

**Oracle® Fusion Middleware**  
User's Guide for Oracle Identity Manager  
11g Release 2 (11.1.2.1.0)  
**E27151-06**

May 2013

Oracle Fusion Middleware User's Guide for Oracle Identity Manager, 11g Release 2 (11.1.2.1.0)

E27151-06

Copyright © 1991, 2013, Oracle and/or its affiliates. All rights reserved.

Primary Author: Debapriya Datta

Contributing Author: Prakash Hulikere

Contributors: Rajesh Pakkath, Sanjay Rallapalli

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 is software or related documentation that 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 END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware 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 that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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

---

---

# Contents

<b>Preface</b> .....	xiii
Audience.....	xiii
Documentation Accessibility .....	xiii
Related Documents .....	xiii
Conventions .....	xiv
<b>Part I Concepts</b>	
<b>1 Feature Overview</b>	
1.1 Features of Oracle Identity Manager .....	1-1
1.1.1 Business User-Friendly Usage .....	1-1
1.1.2 Business Friendly Request Interface .....	1-2
1.1.3 Business User Friendly Request Tracking.....	1-2
1.1.4 Unified Interface for Self Service and Delegated Administration.....	1-2
1.1.5 Organization-Scoped Security .....	1-2
1.1.6 Business User Friendly Personalization .....	1-2
1.1.7 User Administration.....	1-2
1.1.8 Password Management.....	1-3
1.1.9 User Provisioning .....	1-4
1.1.10 Organization and Role Management.....	1-4
<b>2 Oracle Identity Self Service Interface</b>	
2.1 Logging in to Oracle Identity Self Service .....	2-1
2.2 Overview of the Oracle Identity Self Service Interface .....	2-1
2.2.1 Links .....	2-3
2.2.1.1 Accessibility.....	2-3
2.2.1.2 Sandboxes .....	2-4
2.2.1.3 Customize .....	2-4
2.2.1.4 Help .....	2-4
2.2.1.4.1 Top Pane .....	2-5
2.2.1.4.2 Lower Left Pane.....	2-6
2.2.1.4.3 Lower Right Pane .....	2-6
2.2.1.5 Sign Out .....	2-6
2.2.2 Left and Right Panes .....	2-6

2.2.2.1	Home .....	2-7
2.2.2.2	Inbox .....	2-7
2.2.2.3	My Profile .....	2-7
2.2.2.4	Requests .....	2-7
2.2.2.5	Certifications .....	2-8
2.2.2.6	Administration.....	2-8

## Part II Getting Started With Oracle Identity Manager User Interface

### 3 Registering to Self Service

3.1	Submitting Registration Requests .....	3-1
3.2	Tracking Registration Requests .....	3-2

### 4 Accessing Oracle Identity Self Service

4.1	Connecting to Oracle Identity Self Service.....	4-1
4.2	Retrieving Forgotten User Login.....	4-2
4.3	Resetting Forgotten Password .....	4-2

### 5 Personalizing Self Service

5.1	Personalizing the Home Page .....	5-1
5.1.1	Adding a Container .....	5-1
5.1.2	Editing a Container.....	5-3
5.1.3	Removing a Container .....	5-3
5.1.4	Moving Containers.....	5-4
5.1.5	Changing the Layout of the Home Page .....	5-4
5.2	Adding and Removing Attributes in Search Criteria .....	5-5
5.3	Personalizing the Search Result .....	5-5
5.4	Using Saved Search.....	5-6
5.4.1	Creating a Saved Search .....	5-6
5.4.2	Personalizing Saved Search.....	5-7
5.4.3	Deleting a Saved Search.....	5-7
5.4.4	Using Saved Search to Perform a Search Operation.....	5-7
5.5	Sorting Data in Search Results .....	5-7
5.6	Using Query By Example .....	5-8

### 6 Managing Profile Information

6.1	Managing Profile Attributes.....	6-1
6.2	Changing Password.....	6-2
6.3	Setting Challenge Questions and Response.....	6-3
6.4	Viewing Direct Reports.....	6-4
6.4.1	Viewing and Modifying Direct Reports .....	6-4
6.5	Managing Proxies .....	6-4
6.5.1	Adding a Proxy .....	6-5
6.5.2	Editing a Proxy.....	6-5
6.5.3	Removing a Proxy.....	6-6

## 7 Managing Access

7.1	Managing Roles.....	7-1
7.1.1	Requesting for Roles.....	7-1
7.1.2	Modifying Role Details .....	7-2
7.1.3	Removing Roles .....	7-2
7.2	Managing Entitlements.....	7-2
7.2.1	Requesting for Entitlements.....	7-2
7.2.2	Removing Entitlements.....	7-3
7.3	Managing Accounts.....	7-3
7.3.1	Requesting for Accounts.....	7-3
7.3.2	Modifying Accounts.....	7-4
7.3.3	Removing Accounts .....	7-4
7.3.4	Disabling an Account .....	7-4
7.3.5	Enabling an Account .....	7-4
7.4	Viewing Admin Roles .....	7-5

## 8 Using the Access Request Catalog

8.1	Viewing and Modifying the Access Request Catalog for Catalog Items.....	8-1
8.1.1	Refining Search Results.....	8-2
8.1.2	Supported Search Operators .....	8-3
8.2	Adding and Removing Catalog Items to and from the Cart .....	8-4

## 9 Managing Requests

9.1	Request Stages .....	9-3
9.2	Bulk Requests and Child Requests.....	9-8
9.3	Heterogeneous Requests.....	9-10
9.4	Request vs. Direct Operation .....	9-10
9.5	Request Categories .....	9-11
9.6	Common Reasons for Request Failure.....	9-13
9.7	Request Profiles.....	9-13
9.7.1	Creating a Request Profile.....	9-14
9.7.2	Modifying a Request Profile.....	9-14
9.7.3	Deleting a Request Profile .....	9-15
9.8	Creating Requests .....	9-15
9.8.1	Creating a Request to Register Yourself in Oracle Identity Manager.....	9-15
9.8.2	Creating a Request By Using the Request Catalog .....	9-15
9.8.3	Creating a Request By Using a Request Profile.....	9-19
9.9	Tracking a Request.....	9-20
9.10	Withdrawing a Request .....	9-21
9.11	Closing a Request.....	9-22

## 10 Managing Tasks

10.1	Using the Unified Inbox.....	10-2
10.1.1	Creating a View Definition.....	10-2
10.1.2	Editing User Preferences.....	10-3

10.1.3	Deleting a View .....	10-3
10.1.4	Editing the Task Chart .....	10-4
10.2	Managing Approval Tasks .....	10-4
10.2.1	Viewing Approval Tasks .....	10-5
10.2.2	Searching Tasks .....	10-6
10.2.2.1	Performing Simple Search for Tasks.....	10-6
10.2.2.2	Performing Advanced Search for Tasks.....	10-6
10.2.3	Viewing Task Details.....	10-9
10.2.4	Adding Comments and Attachments .....	10-9
10.2.5	Approving a Task .....	10-10
10.2.6	Rejecting a Task.....	10-10
10.2.7	Reassigning a Task .....	10-10
10.2.8	Suspending a Task.....	10-11
10.2.9	Withdrawing a Task .....	10-11
10.3	Managing Certification Review Tasks .....	10-11
10.3.1	Searching and Viewing Certifications .....	10-12
10.3.1.1	Searching Certifications in the Inbox.....	10-12
10.3.1.2	Accessing Certification Tasks From the Inbox .....	10-13
10.3.1.2.1	Viewing User Certification Details .....	10-13
10.3.1.2.2	Viewing Role Certification Details.....	10-15
10.3.1.2.3	Viewing Application Instance Certification Details.....	10-16
10.3.1.2.4	Viewing Entitlement Certification Details.....	10-17
10.3.2	Completing Certifications .....	10-18
10.3.2.1	Completing User Certifications .....	10-18
10.3.2.1.1	Making Certification Decision on the Users.....	10-18
10.3.2.1.2	Reviewing Roles and Entitlements .....	10-19
10.3.2.1.3	Finishing the User Certification .....	10-20
10.3.2.2	Completing Role Certifications .....	10-20
10.3.2.2.1	Making Certification Decisions on the Roles .....	10-20
10.3.2.2.2	Reviewing the Contents of the Roles.....	10-22
10.3.2.2.3	Finishing the Role Certification.....	10-22
10.3.2.3	Completing Application Instance Certifications.....	10-23
10.3.2.3.1	Making Certification Decisions on the Application Instances.....	10-23
10.3.2.3.2	Reviewing Account and Entitlement Assignments.....	10-24
10.3.2.3.3	Finishing the Application Instance Certification.....	10-25
10.3.2.4	Completing Entitlement Certifications.....	10-25
10.3.2.4.1	Making Certification Decisions on the Entitlements.....	10-25
10.3.2.4.2	Reviewing the Entitlement Assignments.....	10-27
10.3.2.4.3	Finishing the Entitlement Certification .....	10-27
10.4	Managing Provisioning Tasks.....	10-28
10.4.1	Searching Provisioning Tasks .....	10-28
10.4.2	Viewing Provisioning Task Details.....	10-29
10.4.3	Setting Response for a Task.....	10-30
10.4.4	Adding Notes to a Task .....	10-30
10.4.5	Reassigning a Task .....	10-31
10.4.6	Viewing Task Assignment History .....	10-32
10.4.7	Viewing Form Details .....	10-33

10.4.8	Modifying Form Details.....	10-33
10.4.9	Retrying a Task .....	10-34
10.4.10	Manually Fulfilling Tasks.....	10-34
10.5	Managing Attestation Tasks.....	10-35
10.5.1	Searching Attestation Tasks .....	10-35
10.5.2	Viewing Attestation Request Detail.....	10-36

## Part III Identity Administration

### 11 Managing Users

11.1	User Lifecycle .....	11-1
11.1.1	OIM Account .....	11-2
11.1.2	Organization.....	11-3
11.1.3	Role .....	11-3
11.2	User Entity Definition .....	11-3
11.3	Default User Accounts .....	11-29
11.4	User Management Tasks.....	11-29
11.4.1	Searching Users.....	11-30
11.4.1.1	Operations on Search Results .....	11-31
11.4.2	Creating a User.....	11-32
11.4.3	Viewing User Details.....	11-34
11.4.4	Modifying Users .....	11-35
11.4.4.1	Editing User Attributes.....	11-35
11.4.4.2	Adding and Removing Roles.....	11-36
11.4.4.3	Adding and Removing Entitlements.....	11-37
11.4.4.4	Modifying Accounts.....	11-37
11.4.4.4.1	Requesting for an Account.....	11-38
11.4.4.4.2	Modifying an Account.....	11-38
11.4.4.4.3	Removing an Account .....	11-39
11.4.4.4.4	Marking an Account as Primary .....	11-39
11.4.4.4.5	Disabling an Account.....	11-40
11.4.4.4.6	Enabling an Account.....	11-40
11.4.4.5	Modifying Details of Direct Reports.....	11-40
11.4.5	Disabling a User .....	11-40
11.4.6	Enabling a User .....	11-41
11.4.7	Deleting a User.....	11-41
11.4.8	Locking an Account.....	11-41
11.4.9	Unlocking an Account.....	11-42
11.5	Username Reservation .....	11-42
11.5.1	Enabling and Disabling Username Reservation .....	11-43
11.5.2	Configuring the Username Policy .....	11-44
11.5.3	Writing Custom User Name Policy.....	11-48
11.5.4	Releasing the Username.....	11-50
11.5.5	Configuring Username Generation to Support Microsoft Active Directory .....	11-51
11.6	Common Name Generation .....	11-51
11.6.1	Common Name Generation for Create User Operation .....	11-51

11.6.2	Common Name Generation for Modify User Operation.....	11-52
--------	-------------------------------------------------------	-------

## 12 Managing Roles

12.1	Role Membership Inheritance .....	12-1
12.2	Role Permission Inheritance .....	12-3
12.3	Role Entity Definition.....	12-4
12.3.1	Role Entity.....	12-5
12.3.2	Role Category Entity .....	12-7
12.3.3	Role Grant Relationship.....	12-8
12.3.4	Role Parent Relationship .....	12-9
12.3.5	Role Organization Relationship.....	12-9
12.4	Default Roles.....	12-9
12.5	Role Management Tasks .....	12-10
12.5.1	Creating Roles .....	12-11
12.5.2	Managing Roles.....	12-11
12.5.2.1	Searching for Roles.....	12-11
12.5.2.2	Viewing and Administering Roles.....	12-13
12.5.2.2.1	The Attributes Tab .....	12-13
12.5.2.2.2	The Hierarchy Tab.....	12-13
12.5.2.2.3	Adding a Parent Role to a Child Role .....	12-14
12.5.2.2.4	Removing a Parent Role from a Role.....	12-14
12.5.2.2.5	Opening a Parent/Child Role.....	12-14
12.5.2.2.6	The Members Tab .....	12-15
12.5.2.2.7	Assigning Members to a Role.....	12-15
12.5.2.2.8	Revoking Members from a Role.....	12-16
12.5.2.2.9	Adding, Modifying, and Deleting Membership Rules .....	12-16
12.5.2.2.10	The Organizations Tab .....	12-18
12.5.2.2.11	Publishing Roles to an Organization.....	12-18
12.5.2.2.12	Revoking Organizations From a Role .....	12-18
12.5.2.3	Viewing Access Policies.....	12-18
12.5.2.4	Deleting Roles .....	12-19
12.5.3	Creating and Managing Role Categories .....	12-19
12.5.3.1	Creating a Role Category.....	12-20
12.5.3.2	Searching Role Categories .....	12-20
12.5.3.3	Modifying a Role Category .....	12-20
12.5.3.4	Deleting a Role Category.....	12-21
12.6	Request-Based Role Grants.....	12-21

## 13 Managing Organizations

13.1	Delegated Administration Model.....	13-1
13.2	Organization Entity Definition .....	13-3
13.3	Organization Scoping and Hierarchy .....	13-4
13.4	Publishing Entities to Organizations .....	13-4
13.5	Admin Roles .....	13-5
13.6	Delegable and Nondelegable Operations.....	13-17
13.7	Evaluating Password Policies .....	13-17
13.8	Organization Management Tasks.....	13-18

13.8.1	Searching Organizations.....	13-18
13.8.2	Creating an Organization .....	13-19
13.8.3	Viewing and Modifying Organizations.....	13-21
13.8.3.1	Modifying Organization Attributes.....	13-22
13.8.3.2	Managing Child Organizations .....	13-22
13.8.3.2.1	Creating a Child Organization .....	13-22
13.8.3.2.2	Deleting a Child Organization .....	13-22
13.8.3.2.3	Disabling a Child Organization .....	13-22
13.8.3.2.4	Enabling a Child Organization.....	13-23
13.8.3.2.5	Opening a Child Organization .....	13-23
13.8.3.3	Viewing Organization Membership .....	13-23
13.8.3.4	Viewing Available Roles .....	13-23
13.8.3.5	Managing Admin Roles.....	13-23
13.8.3.5.1	Granting an Admin Role .....	13-23
13.8.3.5.2	Revoking an Admin Role .....	13-24
13.8.3.6	Viewing Available Accounts .....	13-24
13.8.3.7	Viewing Provisioned Accounts .....	13-24
13.8.3.7.1	Provisioning an Account.....	13-25
13.8.3.7.2	Revoking an Account.....	13-25
13.8.3.7.3	Viewing the Details of a Provisioned Account .....	13-25
13.8.3.7.4	Disabling a Provisioned Account.....	13-25
13.8.3.7.5	Enabling a Provisioned Account.....	13-25
13.8.3.8	Viewing Available Entitlements.....	13-26
13.8.4	Disabling and Enabling Organizations .....	13-26
13.8.5	Deleting an Organization .....	13-27

## 14 Using the Attestation Dashboard

14.1	Viewing Attestation Request Details .....	14-1
14.2	E-Mail Notification .....	14-3
14.3	Attestation Grace Period Checker Scheduled Task .....	14-3

## 15 Using Identity Certification

15.1	Identity Certification Overview .....	15-1
15.1.1	What Is Identity Certification?.....	15-1
15.1.2	Who Is Involved in Completing Identity Certifications?.....	15-3
15.2	Certification UI.....	15-4
15.3	Certification Name Formats .....	15-5
15.4	Searching and Viewing Certifications.....	15-6
15.4.1	Searching Certifications in the Dashboard.....	15-6
15.4.2	Viewing Certifications From the Dashboard.....	15-7
15.5	Completing User Certifications in Offline Mode .....	15-8
15.6	Generating Certification Reports .....	15-10
15.6.1	Generating Certification Reports From the Dashboard .....	15-12
15.6.2	Generating Exported Certification Reports From the Certification Pages.....	15-13

**Glossary**

**Index**

## List of Figures

2-1	Login Page of Oracle Identity Self Service .....	2-2
2-2	Layout of Oracle Identity Self Service.....	2-3
2-3	Layout of the Help Interface.....	2-4
5-1	The Add Box Above Icon on the Toolbar .....	5-2
5-2	A New Container .....	5-2
5-3	The Component Properties Dialog Box .....	5-3
5-4	Dragging and Dropping a Container.....	5-4
5-5	Home Page Layout .....	5-5
5-6	Query By Example.....	5-8
8-1	The Request Cart.....	8-5
9 1	Request Process Flow .....	9-2
9 2	Request Stages .....	9-4
9 3	Bulk Request and Child Request Stages.....	9-9
9 4	The Catalog Page.....	9-16
9 5	The Request Cart.....	9-17
9 6	The Cart Details Page .....	9-18
9 7	The Request Summary Page.....	9-19
10 1	The Task Type Browser Dialog Box .....	10-7
10 2	The Identity Browser .....	10-8
10 3	The Advanced Search Dialog Box .....	10-8
10 4	The Add Notes for Task Window .....	10-31
10 5	The Select User Assignee for Task Window .....	10-32
10 6	The Task History Window .....	10-33
10 7	The Attestation Request Detail Window .....	10-36
11-1	User Life Cycle .....	11-1
11-2	The System Property Detail Page .....	11-44
11-3	The Default Username Policy Configuration .....	11-47
12-1	Role Membership and Permission Inheritance.....	12-3
12-2	The Expression Builder .....	12-17
13-1	Delegated Administration .....	13-2
13-2	Organization Search Results .....	13-19
13-3	The Create Organization Page .....	13-20
13-4	The Organization Details Page .....	13-21
15-1	The Certification Tab .....	15-9

## List of Tables

8-1	Fields in the Detailed Information Section.....	8-2
9 1	Request Stages .....	9-4
9 2	Default Operations and Request Types for Catalog-Based Requests .....	9-12
9 3	Default Operations and Request Types for Non-Catalog-Based Requests .....	9-12
10 1	Columns in the Approval Details Page .....	10-5
10 2	Fields in the Provisioning Tasks Search Results Table.....	10-29
10 3	Fields in the Task Details Window.....	10-29
10 4	Fields in the Task History Window.....	10-33
10 5	Fields in the Attestation Task Search Results Table.....	10-36
10 6	Fields in the Attestation Request Detail Window .....	10-36
11-1	User Life Cycle and Business Objectives Sample Scenarios .....	11-2
11-2	Attributes Defined for User Entity .....	11-4
11-3	Default User Accounts .....	11-29
11-4	Fields in the Create User Page .....	11-32
11-5	Predefined Username Policies .....	11-44
11-6	Constants Representing Policy IDs .....	11-46
11-7	RDN Modification Scenarios.....	11-53
12-1	Default Attributes for the Role Entity .....	12-5
12-2	Default Attributes for the Role Category Entity.....	12-8
12-3	Default Attributes for Role Grant Relationship.....	12-8
12-4	Default Attributes for Role Parent Relationship .....	12-9
12-5	Default Roles in Oracle Identity Manager.....	12-10
12-6	Fields in the Create Role Page.....	12-11
13-1	Default Attributes of the Organization Entity .....	13-3
13-2	Admin Roles in Oracle Identity Manager .....	13-6
13-3	Admin Roles and Permissions .....	13-7
15-1	The Four Types of Identity Certification .....	15-2
15-2	Identity Certification Reviewers .....	15-3
15-3	Certification Name Formats .....	15-5
15-4	Default Certification Reports .....	15-10

---

---

# Preface

The Oracle Fusion Middleware User's Guide for Oracle Identity Manager introduces you to Oracle Identity Self Service tasks, and delegated administration functionalities.

## Audience

This guide is intended for users who can log in to Oracle Identity Self Service and perform self-service operations, request for roles and resources, and manage various approval, provisioning, and attestation tasks. This guide is also intended for delegated administrators who can perform identity administration tasks and define authorization policies to delegate administration privileges. In addition, a user with any role can refer to this guide for an introduction and conceptual information about Oracle Identity Manager.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## Related Documents

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

- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Quick Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Suite Integration Overview*

- *Oracle Fusion Middleware User Reference for Oracle Identity Management*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- *Oracle Fusion Middleware Administrator's Guide for Authorization Policy Manager*

## Conventions

The following text conventions are used in this document:

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

# Part I

---

## Concepts

This part introduces Oracle Identity Manager and describes the concepts related to Oracle Identity Manager.

It contains the following chapters:

- [Chapter 1, "Feature Overview"](#)
- [Chapter 2, "Oracle Identity Self Service Interface"](#)



---

---

# Feature Overview

Oracle Identity Manager is a user provisioning and administration solution, which automates the process of adding, updating, and deleting user accounts from applications and directories. It also improves regulatory compliance by providing granular reports that attest to who has access to what. Oracle Identity Manager is available as a stand-alone product or as part of Oracle Identity and Access Management Suite.

Automating user identity provisioning can reduce Information Technology (IT) administration costs and improve security. Provisioning also plays an important role in regulatory compliance. Key features of Oracle Identity Manager include password management, workflow and policy management, identity reconciliation, reporting and auditing, and extensibility.

## 1.1 Features of Oracle Identity Manager

The features of Oracle Identity Manager can be divided into the following categories:

- [Business User-Friendly Usage](#)
- [Business Friendly Request Interface](#)
- [Business User Friendly Request Tracking](#)
- [Unified Interface for Self Service and Delegated Administration](#)
- [Organization-Scoped Security](#)
- [Business User Friendly Personalization](#)
- [User Administration](#)
- [Password Management](#)
- [User Provisioning](#)
- [Organization and Role Management](#)

### 1.1.1 Business User-Friendly Usage

In earlier releases of Oracle Identity Manager, the usage of Oracle Identity Manager was IT centric. To request for a role, entitlement, or application, business users had to know details, such as which request template, resource object, or IT resource to use. From this release onward, Oracle Identity Manager is easy to use. Business users do not need to know about IT-related details. Instead, business users can search for an item in the request catalog and add it in the shopping cart.

Oracle Identity Manager provides ease of use to business users through simplified request interface that includes shopping cart and catalog-based experience, business-friendly request tracking, unified inbox for approval and certification tasks, and unified interface for self service and delegated administration tasks.

## 1.1.2 Business Friendly Request Interface

In earlier releases of Oracle Identity Manager, complex request scenarios could be implemented by using role requests, request templates and SOA approval processes. However, the request management engine did not offer the ability to request application entitlements. In addition, the overall request process was cumbersome.

The shopping cart pattern has been introduced to simplify the request interface. End users can request for entities such as roles, entitlements, and application instances from the access request catalog by using the shopping cart pattern.

## 1.1.3 Business User Friendly Request Tracking

Administrators and end users can track all requests easily by using the simplified and user-friendly request tracking interface. By using the Track Requests page in Oracle Identity Self Service, you can view or close requests by searching for requests based on request ID, status, request type, requested date, beneficiary, and requester.

## 1.1.4 Unified Interface for Self Service and Delegated Administration

Unlike earlier releases, the current release of Oracle Identity Manager provides a unified interface for the end user self-service for self and others, and user delegated-administration flows. In this release, delegated-administration functions on users are nothing but requests raised on behalf of other users that are automatically approved based on security configuration.

## 1.1.5 Organization-Scoped Security

Oracle Identity Manager provides an organizational-level scoping mechanism for delegated administration and data security of various entities. Every entity is published to a set of organizations and only the users in the published organizations are allowed to receive access.

## 1.1.6 Business User Friendly Personalization

Oracle Identity Manager allows users to personalize Oracle Identity Self Service for their respective logins. Users can rearrange or hide regions in the Home Page, save and reuse regularly searched items, save sorting preferences, and so on.

## 1.1.7 User Administration

By deploying self-service features and delegating administrative functions, an organization can increase user productivity, user satisfaction, and operational efficiency.

### **Single Interface for Self Service and System Administration**

Oracle Identity Manager provides a single Web-based interface for performing all types of operations related to self, identity administration, and system administration and configuration.

### **User Profile Management**

Users can view and edit their own profiles by using Oracle Identity Self Service. This reduces administrative overhead and provides users with control over their identity profiles.

Administrators can view and manage the profiles of other users subject to access permissions by using the user interface for Oracle Identity Manager administration. This allows administrators to create and edit user profiles, change passwords of users, and perform other delegated administration tasks.

### **Request Management**

Oracle Identity Self Service also enables users to create provisioning requests for resources with fine-grained entitlements, profile management requests, and role membership requests. The items to be requested can be selected from a Web-based catalog interface. Business approvers, such as team leaders, line managers, and department heads, can use the same Web-based interface to examine and approve incoming requests. This helps organizations in reducing effort and cost.

### **Delegated Administration**

Oracle Identity Manager features a highly flexible security framework that supports delegation of most administrative functions to any group or user. By moving administration points as close to the user as possible, an organization can achieve tighter control and better security, increasing productivity at the same time.

## **1.1.8 Password Management**

Password management is one of the foremost issues in organizations nowadays. Implementing a password management solution reduces cost and overhead related to raising tickets or calling help desks. The password management features of Oracle Identity Manager discussed in this section aim to help organizations in this area.

### **Self-Service Password Management**

Users can manage their own enterprise passwords, which might then be synchronized with their managed accounts depending on how the managed accounts are individually configured. The enterprise passwords are managed by using the self-service capabilities of Oracle Identity Manager. If a user forgets the password, Oracle Identity Manager can present customizable challenge questions to enable self-service identity verification and password reset. Research shows that the bulk of help desk calls are related to password reset and account lockout. By reducing the need for help desk calls, this self-service capability lowers costs.

### **Advanced Password Policy Management**

Most best practices are supported out of the box and are configurable through an intuitive user interface. Supported password complexity requirements include: password length, alphanumeric and special characters usage, uppercase and lowercase usage, full or partial exclusion of user name, minimum password age, and historical passwords. Oracle Identity Manager lets you define complex password policies that control the passwords set by users. In addition, Oracle Identity Manager allows the application of multiple policies for each resource. For instance, users with fewer privileges can be subjected to a more relaxed password policy, whereas privileged administrators can be subjected to a more stringent policy.

### **Password Synchronization**

Oracle Identity Manager can synchronize or map passwords across managed resources and enforce differences in password policies among these resources. In addition, if an organization is using the desktop-based password reset feature of Microsoft Windows, the Active Directory (AD) connector of Oracle Identity Manager can intercept password changes at the AD server and subsequently propagate these changes to other managed resources in accordance with policies. Similar bidirectional password synchronization capability is offered in most Oracle Identity Manager connectors for directory servers and mainframes.

## **1.1.9 User Provisioning**

Provisioning provides outward flow of user information from Oracle Identity Manager to a target system. Provisioning is the process by which an action to create, modify, or delete user information in a resource is started from Oracle Identity Manager and passed into the resource. The provisioning system communicates with the resource and specifies changes to be made to the account.

Provisioning includes the following:

- **Automated user identity and account provisioning:** This manages user identities and accounts in multiple systems and applications. For example, when an employee working in the payroll department is created in the human resources system, accounts are also automatically created for this user in the e-mail, telephone, accounting, and payroll reports systems.
- **Workflow and policy management:** This enables identity provisioning. Administrators can use interfaces provided by provisioning tools to create provisioning processes based on security policies.
- **Reporting and auditing:** This enables creating documentation of provisioning processes and their enforcement. This documentation is essential for audit, regulatory, and compliance purposes.
- **Attestation:** This enables administrators to confirm users' access rights on a periodic basis.
- **Access deprovisioning:** When the access for a user is no longer required or valid in an organization, Oracle Identity Manager revokes access on demand or automatically, as dictated by role or attribute-based access policies. This ensures that a user's access is promptly terminated where it is no longer required. This is done to minimize security risks and prevent paying for access to costly resources, such as data services.

## **1.1.10 Organization and Role Management**

An organization entity represents a logical container of other entities such as users, roles, and policies in Oracle Identity Manager. In other words, organizations are containers that can be used for delegated administrative model. In addition, organizations define the scope of other Oracle Identity Manager entities, such as users. Oracle Identity Manager supports a flat organization structure or a hierarchical structure, which means that an organization can contain other organizations. The hierarchy can represent departments, geographical areas, or other logical divisions for easier management of entities.

Roles are logical groupings of users to whom you can assign access rights within Oracle Identity Manager, provision resources automatically, or use in common tasks such as approval and attestation. Roles can be independent of organizations, span multiple organizations, or can contain users from a single organization.

---

---

# Oracle Identity Self Service Interface

This chapter will help you familiarize with Oracle Identity Self Service. This will enable you to quickly find the information you need and complete the required tasks easily.

This chapter discusses the following topics:

- [Logging in to Oracle Identity Self Service](#)
- [Overview of the Oracle Identity Self Service Interface](#)

## 2.1 Logging in to Oracle Identity Self Service

To log in to Oracle Identity Self Service:

1. Browse to the following URL by using a Web browser:

```
http://HOSTNAME:PORT/identity
```

In this URL, *HOSTNAME* represents the name of the computer hosting the application server and *PORT* refers to the port on which the server is listening.

---

---

**Note:** The application name, *identity*, is case-sensitive.

---

---

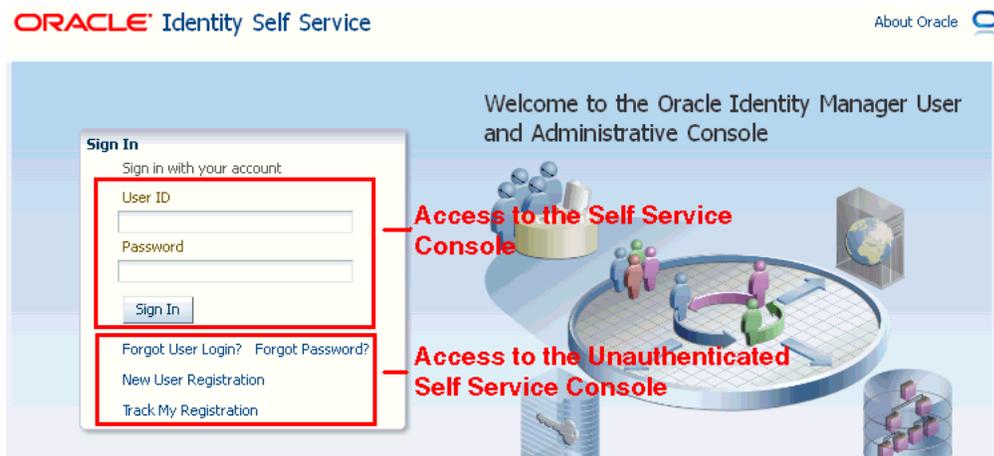
2. After the Identity Self Service login page is displayed, log in with your user name and password.

**See Also:** "[Accessing Oracle Identity Self Service](#)" on page 4-1 for detailed information on logging in

## 2.2 Overview of the Oracle Identity Self Service Interface

Oracle Identity Self Service provides user self-service and delegated identity administration features that serve most of the users of Oracle Identity Manager. This console provides access to the self service console and unauthenticated self service console. [Figure 2-1](#) shows these two consoles.

**Figure 2–1 Login Page of Oracle Identity Self Service**



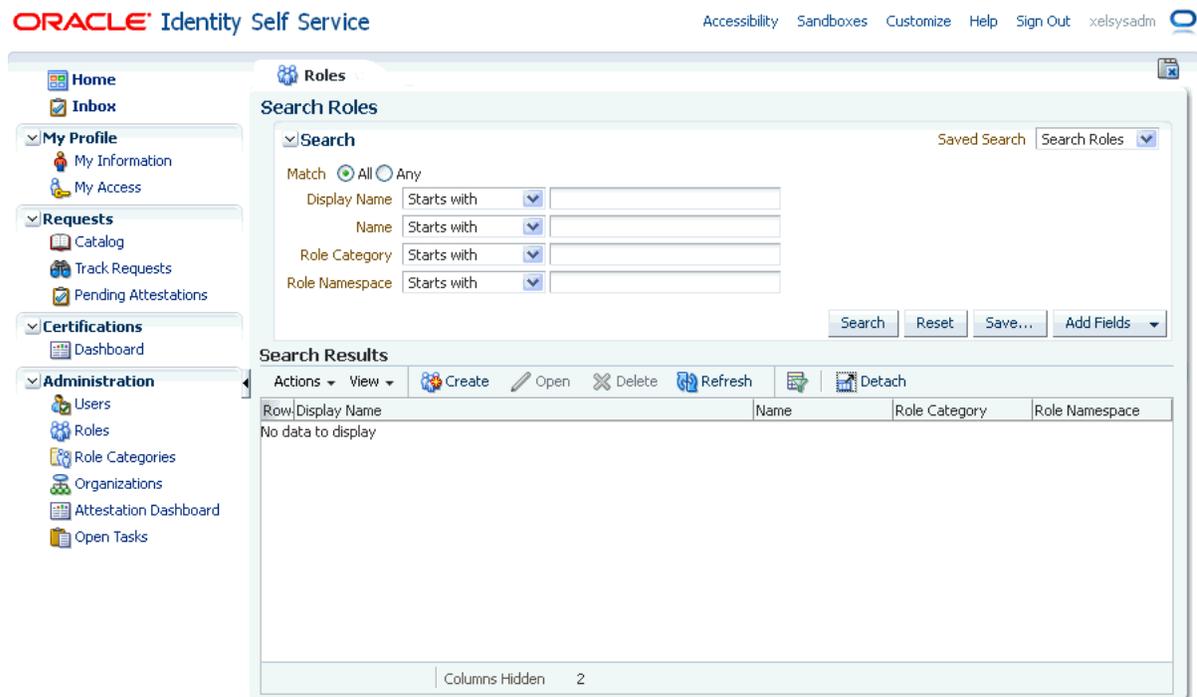
Identity Self Service supports access to unauthenticated self-service tasks in the Unauthenticated Self Service Console. Users who have not authenticated into, or not logged in to Identity Self Service can access the Unauthenticated Self Service Console by clicking the [Forgot User Login?](#), [Forgot Password?](#), [New User Registration](#), or [Track My Information](#) links. This console enables an unauthenticated user to retrieve a forgotten user login ID or password, register to the Oracle Identity Manager environment, and track the registration. See ["Registering to Self Service"](#) on page 3-1 and ["Accessing Oracle Identity Self Service"](#) on page 4-1 chapters for more information.

Access to authenticated self-service tasks is available by logging in to Identity Self Service. The interface of Identity Self Service is composed of the following areas:

- [Links](#)
- [Left and Right Panes](#)

[Figure 2–2](#) shows a sample page and the layout of Identity Self Service.

Figure 2–2 Layout of Oracle Identity Self Service



## 2.2.1 Links

This area consists of the following links in the upper-right-hand corner of the interface:

- [Accessibility](#)
- [Sandboxes](#)
- [Customize](#)
- [Help](#)
- [Sign Out](#)

### 2.2.1.1 Accessibility

Identity Self Service has been designed to adhere to the standards set in Section 508 of the Rehabilitation Act and the World Wide Web Consortium's Web Content Accessibility Guidelines 2.0 AA (WCAG 2.0 'AA').

When you click the Accessibility link in the upper right corner of the page, the Accessibility dialog box is displayed. You can select one of the following options from the Accessibility dialog box:

- **I use a screen reader**

Select this option if you want to use a screen reader.

- **I use high contrast colors**

Select this option to use the high-contrast color scheme that you have specified in your operating system, rather than using the default color scheme specified in Identity Self Service.

- **I use large fonts**

Select this option if you want to change the font size for easy viewing and readability.

### 2.2.1.2 Sandboxes

A sandbox represents an area where metadata objects can be modified without affecting their mainline usage. In other words, a sandbox is a temporary storage area to save a group of runtime page customizations before they are either saved and published to other users, or discarded.

In the Manage Sandboxes page, you can create, delete, activate, deactivate, and publish sandboxes. See the "Managing Sandboxes" section in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information.

### 2.2.1.3 Customize

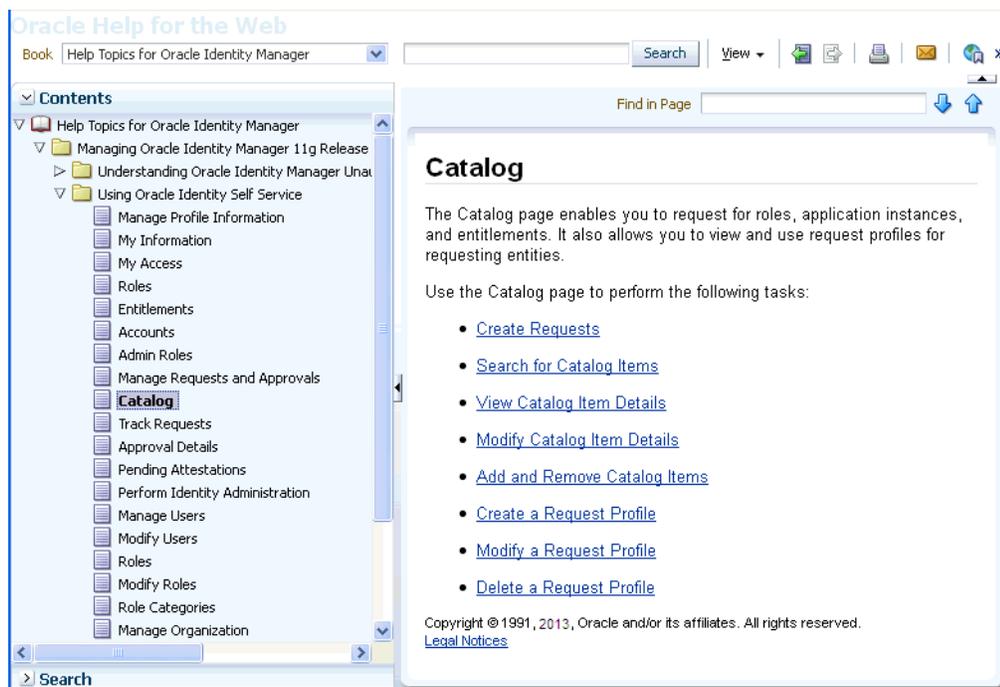
This is used for customizing the user interface (UI). Clicking the Customize link opens Oracle Web Composer that allows you to customize the screen components. See "Customizing the Interface" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about UI customization.

### 2.2.1.4 Help

Identity Self Service includes a help system. Clicking the Help link opens the help system in a new window. In addition, Identity Self Service provides context-sensitive help. For example, if you are in the Catalog page and click the Help link, then help content related to catalog is displayed.

Figure 2–3 shows a sample page and default layout of the help interface.

**Figure 2–3** Layout of the Help Interface



The default view of the help system consists of three panes:

- [Top Pane](#)

- [Lower Left Pane](#)
- [Lower Right Pane](#)

#### 2.2.1.4.1 Top Pane

The top pane consists of the following:

- Book drop-down list: From this drop-down list you can select one of the following values:
  - **Help Topics for Oracle Identity Manager:** Select this value to open all help topics for Oracle Identity Manager.
  - **Administrator's Guide for Oracle Identity Manager:** Select this value to open the online help version of Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager.
  - **Developer's Guide for Oracle Identity Manager:** Select this value to open the online help version of Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.
  - **User's Guide for Oracle Identity Manager:** Select this value to open the online help version of Oracle Fusion Middleware User's Guide for Oracle Identity Manager.
  - **Custom Help Topics for Oracle Identity Manager:** Select this value to open any custom help topics.
- Search field: Specify any word or term to search for in the help system.
- View: From the View menu, you can select any one of the following options:
  - **Maximize Reading Pane:** Collapses the lower left pane to maximize the reading pane, which is the lower right pane.
  - **Restore Default Window Layout:** Restore the current layout of the help system to the default layout.
  - **Contents:** Restores the lower left pane to display the Contents region along with the help topics, if it is not already being displayed.
  - **Search:** Displays the Search region in the lower left pane. In the Search region, you can search for help topic and the search results are displayed in a tabular format. Here are a few guidelines on performing a search:
    - \* Search criterion specified in the Search field can be made case sensitive by selecting the **Case Sensitive** option.
    - \* To define your search precisely, you can specify the boolean operators & (for AND), | (for OR), ! (for NOT) in your search criterion, select the **Boolean expression** option, and then click **Search**.
    - \* To search for help topics containing all words specified in the search criterion, select **All words**.
    - \* To search for help topics containing any word specified in the search criterion, select **Any words**.
  - **Show permanent link for this topic page:** If you want to save the link to a help topic for future reference, then from the View menu, select **Show permanent link for this topic page**. In the dialog box that is displayed, right-click the link to the help topic and select one of the following options:

- \* **Bookmark This Link:** Adds the help topic URL to the browser bookmarks.
- \* **Copy Link Location:** Copies the help topic URL to the clipboard.
- **Toolbar:** The help system contains a toolbar that provides action buttons for certain tasks. You can view the name of the button by moving the mouse pointer over the button. The following buttons are available:
  - **Go back one page:** Takes you back to the page containing the previous help topic.
  - **Go forward one page:** This icon is enabled only if you have clicked the **Go back one page** icon. Clicking the **Go forward one page icon** takes you to the next page in the sequence of topics you visited.
  - **Print this topic page:** Prints the current help topic.
  - **Email this topic page:** Drafts an email with a link to the help topic currently displayed in the help system. This draft can be sent to the desired email recipient.
  - **Link to this topic page:** Saves the link to a help topic for future reference by right-clicking the link to the help topic in the dialog box that is displayed, and then selecting one of the following options:
    - \* **Bookmark This Link:** Adds the help topic URL to the browser bookmarks.
    - \* **Copy Link Location:** Copies the help topic URL to the clipboard.

#### 2.2.1.4.2 Lower Left Pane

The left pane contains the Contents and Search regions. By default, the Contents region is expanded. The Contents region displays links to help topics depending on the option you select from the Book drop-down list in the top pane. You can click the arrow icon beside Contents to expand or collapse the Contents region.

#### 2.2.1.4.3 Lower Right Pane

The lower right pane displays any help topic that you search for or open from the Contents and Search regions in the lower left pane. This pane is also known as the reading pane.

#### 2.2.1.5 Sign Out

Click the Sign Out link to log out of Identity Self Service.

## 2.2.2 Left and Right Panes

Every page in Identity Self Service is divided into two panes. The left pane consists of sections that contain links to regions using which a variety of tasks can be accomplished. The left pane is the primary navigation tool and is displayed on all web pages of Identity Self Service. Depending on the link that you click in the left pane, corresponding details are displayed in the right pane.

The left pane consists of these regions:

- [Home](#)
- [Inbox](#)
- [My Profile](#)

- [Requests](#)
- [Certifications](#)
- [Administration](#)

### 2.2.2.1 Home

The Home page provides you a snapshot of the various functions in Identity Self Service. By default, this page contains the Pending Requests, Pending Approvals, My Accounts, Direct Reports, Getting Started Help Topics, and Change Password containers. You can personalize the Home page by rearranging, hiding, removing, or modifying containers.

See "[Personalizing Self Service](#)" on page 5-1 for more information.

### 2.2.2.2 Inbox

Use the Inbox to perform the following:

- View and manage approval tasks that correspond to requests that are in the user or administrator's queue to be approved. See "[Managing Approval Tasks](#)" on page 10-4 for more information.
- View and manage certification review tasks assigned to the logged-in user. See "[Using the Unified Inbox](#)" on page 10-2 and "[Managing Certification Review Tasks](#)" on page 10-11 for details.

### 2.2.2.3 My Profile

The My Profile region contains the following:

- My Information

Use this page to view and modify personal details of your profile such as changing passwords, setting challenge questions and response, and so on.

See "[Managing Profile Information](#)" on page 6-1 for more information.

- My Access

This page displays entities such as Roles, Entitlements, Accounts, and Admin Roles, to which you have access. In this section, you can request for, remove, or modify entities.

See "[Managing Access](#)" on page 7-1 for more information.

### 2.2.2.4 Requests

The Request region contains the following:

- Catalog

Use this page to search for, view, and request catalog items such as roles, entitlements, and application instances.

See "[Using the Access Request Catalog](#)" on page 8-1 for more information.

- Track Requests

Use this page to search for and track requests raised by you and requests raised for you. You can search for requests based on request ID, status, request type, requested date, beneficiary, and requester.

See "[Tracking a Request](#)" on page 9-20 for more information.

- Pending Attestations

Use this page to view and manage attestation tasks that correspond to outstanding attestation process in the user or administrator's queue.

See "[Managing Attestation Tasks](#)" on page 10-35 for more information.

### 2.2.2.5 Certifications

The Certifications region contains the Dashboard link. The Identity Certification Dashboard provides an overview of in-progress and completed certifications in Oracle Identity Manager.

See "[Using Identity Certification](#)" on page 15-1 for detailed information about the Dashboard.

### 2.2.2.6 Administration

The Administration region contains the following:

- Users

Use this page to view and manage users. Some of the user management tasks that you can perform in this page include creating, modifying, deleting, enabling, and disabling users.

See "[Managing Users](#)" on page 11-1 for more information.

- Roles

Use this page to view and manage roles. Some of the role management tasks that you can perform in this page include creating, viewing, administering, and deleting roles.

See "[Managing Roles](#)" on page 12-1 for more information.

- Role Categories

Use this page to view and manage role categories. See "[Creating and Managing Role Categories](#)" on page 12-19 for more information.

- Organizations

Use this page to view and manage organizations. Some of the organization management tasks include creating, viewing, modifying, and deleting organizations.

See "[Managing Organizations](#)" on page 13-1 for more information.

- Attestation Dashboard

Use this page to view the state of attestation processes that are owned by any group of which you are a member.

See "[Using the Attestation Dashboard](#)" on page 14-1 for more information.

- Open Tasks

Use this page to view and manage provisioning tasks that correspond to tasks instantiated by requests, or pending manual provisioning tasks, or failed automatic provisioning tasks in the user or administrator's queue.

See "[Managing Provisioning Tasks](#)" on page 10-28 for more information.

# Part II

---

## Getting Started With Oracle Identity Manager User Interface

This part describes the various self service tasks that you can perform in Oracle Identity Manager.

It contains the following chapters:

- [Chapter 3, "Registering to Self Service"](#)
- [Chapter 4, "Accessing Oracle Identity Self Service"](#)
- [Chapter 5, "Personalizing Self Service"](#)
- [Chapter 6, "Managing Profile Information"](#)
- [Chapter 7, "Managing Access"](#)
- [Chapter 8, "Using the Access Request Catalog"](#)
- [Chapter 9, "Managing Requests"](#)
- [Chapter 10, "Managing Tasks"](#)



---

---

## Registering to Self Service

This chapter discusses the following topics:

- [Submitting Registration Requests](#)
- [Tracking Registration Requests](#)

### 3.1 Submitting Registration Requests

Oracle Identity Manager requires you to register yourself with an identity to perform certain tasks on Oracle Identity Self Service or Oracle Identity System Administration.

---

---

**Note:** A user is allowed to self register only if the value of the `XL.SelfRegistrationAllowed` system property is set to true. See "System Properties in Oracle Identity Manager" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about this system property.

---

---

To register yourself with Oracle Identity Manager:

1. In the Oracle Identity Self Service login page, click **New User Registration**. The User Registration page is displayed.
2. In the Basic Information section, enter first name, middle name, last name, email, common name, and display name in the respective fields.  
  
Display name is the name of the user displayed in the UI. If not specified, then it is autogenerated while creating the user.
3. In the Enter User ID and Password section, enter the user login name, password, and confirm password in the respective fields.
4. In the Select your challenge questions and answers section, select the challenge question and set an answer for each question.

---

**Note:**

- Challenge questions and answers are asked if the attribute for this is defined in the template for self registration.
  - All Oracle Identity Manager deployments do not support self-registration. This is especially true of internal deployments that manage the identities of employees and contractors, where the identities are added through reconciliation and not self-registration.
- 

5. Click **Register**. You are provided a tracking ID for the registration activity that is used for the tracking the registration feature.

## 3.2 Tracking Registration Requests

You can track your request to register as an identity in Oracle Identity Manager. If the current status indicates success, then you can go to Identity Self Service, and then enter your username and password to log in.

1. In the Identity Self Service login page, click **Track My Registration**. The Track Requests page is displayed.
2. In the Tracking ID field, enter the tracking ID that has been assigned to your registration request. Then click **Submit**. The registration request status is displayed with the following details:

- Tracking request ID
- Request submission date

When the request is submitted and approval is not done, the date shown is the request submission date. In all cases, the date always reflects the last update date.

- Current status of the request

Every self-registration request that is submitted has to go through approvals for it to be processed completely.

If a user tracks the current status of the request, the status is shown with a description of the stage the request is in. The status would be one of the following:

- \* **Pending:** This state indicates that the request is submitted and the approval is pending. In case of default approval, the following status message is displayed:

"Obtaining request-level approval for registration."

If the request level approval is pending. Once the request level approval is obtained, the following status message is displayed:

"Obtaining operation-level approval for registration."

- \* **Rejected:** This state indicates that the request is rejected during approval. The description indicates the reason of rejection. In case of default approval levels, if the request got disapproved at the request approval level, then the following status message is displayed:

"Request rejected. Please call Help-Desk."

If the request gets disapproved at the operation level or request level, then the following status message is displayed:

"Operation approval rejected for registration."

- \* **Completed:** This state indicates that the request is completed. If all the approvals have been provided and the request is successfully completed, the following status message is displayed:

"Request has been completed."

- \* **Failed:** This state indicates that the request is failed during submission. If the request submission is failed, the following status message is displayed:

"The request registration failed."

3. Click **Track Another Registration** to display the status of another registration request.

Or, click **Back to Login** to display the login page.

---

---

**Note:** You can only track the status of Self Registration Requests from this page.

---

---



---

---

## Accessing Oracle Identity Self Service

The login page provides the ability to log in, and provides a starting point for all unauthenticated operations. This page is displayed when you access Oracle Identity Self Service without authenticating either natively to Oracle Identity Manager or by using SSO.

Typical tasks you can perform before logging in to Identity Self Service include:

- [Connecting to Oracle Identity Self Service](#)
- [Retrieving Forgotten User Login](#)
- [Resetting Forgotten Password](#)

### 4.1 Connecting to Oracle Identity Self Service

To log in to Oracle Identity Self Service:

---

---

**Note:**

- If Oracle Identity Manager is configured to support native authentication, then the login link redirects you to a form in which you can authenticate by using your Oracle Identity Manager username and password.
  - If Oracle Identity Manager is configured to support Single Sign-On (SSO), then the login link redirects you to the SSO application login page.
- 
- 

1. Go to the Identity Self Service login page.
2. In the User ID field, enter your username.
3. In the Password field, enter your password.
4. Click **Sign In**. If you are successfully authenticated, then you are logged in and directed to the main page in the authenticated context.

The login attempt might generate an error because of the following reasons:

- **Incorrect credentials:** If the user name and password entered are not correct, then an error message is displayed. This may be because of the following reasons:

Username does not exist

Password is incorrect

Username exists but the user is deleted

- **Locked account:** If the account is locked, then you are not allowed to log in even if the credentials are correct.
  - **Disabled user:** If your user account is disabled, then you are not allowed to log in.
5. If your password has expired, then the Change Password form is displayed. You are not allowed to proceed to the main page of the console without changing the password. Enter a new password, and click **Sign In**.
  6. If the system requires you to specify challenge responses, then specify it and click **Submit**.

Alternatively, you can click **Cancel** if you want to avoid setting challenge questions and logging on to Identity Self Service. You set challenge questions to reset your password without calling the helpdesk. Note that these challenge questions are a unique set of questions and answers. See "[Setting Challenge Questions and Response](#)" on page 6-3 for more information about setting challenge questions and response.

If you attempting to access a page, for example the Pending Approvals page, and you are checking for the pending approvals from a link and you are not logged in already, then you are redirected to the login page. Follow the login instruction provided in this section to log in to Oracle Identity Manager. However, you will be directed to the page you are attempting to access, the Pending Approvals page, instead of the main page of Identity Self Service.

## 4.2 Retrieving Forgotten User Login

If you have forgotten your user login, then you can retrieve it by performing the following steps:

1. In the Identity Self Service login page, click **Forgot User Login**. The Forgot User Login page is displayed.
2. In the Email Address field, enter the email address associated with your user login.
3. Click **Submit**. An email is sent to the specified email address with further instructions.

If you enter an incorrect email address, then an error message is displayed stating that the specified email address does not exist.

## 4.3 Resetting Forgotten Password

To reset your forgotten password:

1. In the Identity Self Service login page, click **Forgot Password?**. The Forgot Password page is displayed.
2. In the User Login field, enter your user name to allow Oracle Identity Manager to locate your user record. Then click **Next**. The Please answer your challenge questions page is displayed.
3. In this step, the wizard provides the challenge questions that you set during user registration to verify your user identity. Enter your responses to the challenge questions, and then click **Next**. The Please enter new password page is displayed.

4. In this step, enter the new password that you want to set, and click **Save**. The following are the possible outcomes of these steps:
  - If Oracle Identity Manager does not find the username you provided, then an error message stating that the user account is invalid is displayed.
  - If the challenge responses specified do not match the ones set during user registration, then an error message stating that the number of questions answered correctly does not match the number of correct answers required.
  - If you satisfy the identity verification criteria (in other words, identifying yourself and answering the challenge questions), but the new password failed to satisfy configured password policies, then an error message is displayed along with details about the password policy.
  - If you satisfy the identity verification criteria and the password is successfully set, then the next page is displayed with a message that the password has been changed. This also unlocks your user account if it was locked by self (not locked by the system administrator manually). Click **Back to Login** to view the login screen from where you can log in to Oracle Identity Manager.



---

---

## Personalizing Self Service

This chapter describes the personalization features of the Oracle Identity Self Service. It contains the following sections:

- [Personalizing the Home Page](#)
- [Adding and Removing Attributes in Search Criteria](#)
- [Personalizing the Search Result](#)
- [Using Saved Search](#)
- [Sorting Data in Search Results](#)
- [Using Query By Example](#)

---

---

**Note:** Personalization of the Self Service is allowed for all users, and is applicable on a per user basis. In other words, the personalization that is saved for a user, is not applicable when another user logs in to Identity Self Service.

---

---

### 5.1 Personalizing the Home Page

The Home page provides you a snapshot of the various functions in Identity Self Service. All personalization in the Home page, such as rearranging the containers or hiding containers, are saved automatically. After personalizing the Home page, when you log out of Identity Self Service and log in again, all the changes that you did in the Home page are retained. When any other user logs in to Identity Self Service, the logged in user will see the default settings in the Home page.

You can personalize the Home page in the following ways:

- [Adding a Container](#)
- [Editing a Container](#)
- [Removing a Container](#)
- [Moving Containers](#)
- [Changing the Layout of the Home Page](#)

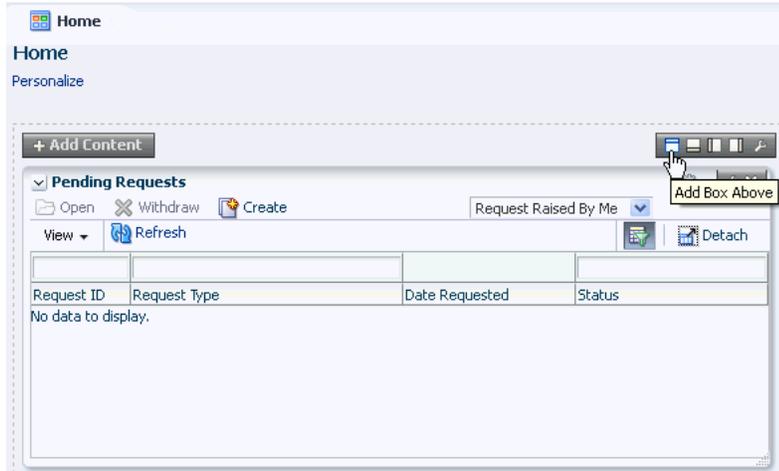
#### 5.1.1 Adding a Container

To add containers in the Home page:

1. Log in to Identity Self Service and navigate to the Home page.

2. On the left navigation pane, click Home. The Home page is displayed.
3. Click **Personalize**. The Home is displayed in customization mode with toolbars that consist of icons.
4. Click the Add Box Above icon on the toolbar. [Figure 5-1](#) shows the Add Box Above icon on the toolbar.

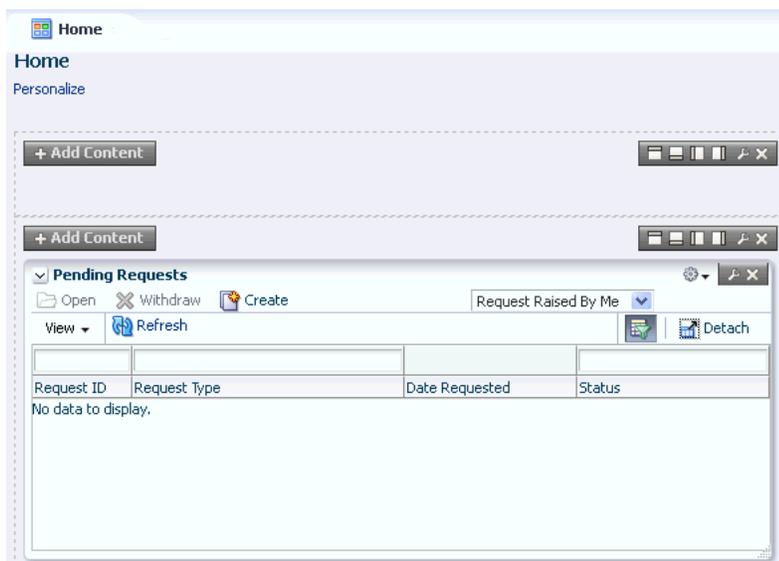
**Figure 5-1 The Add Box Above Icon on the Toolbar**



You can click the respective icons to add a box below, right, or left of the container in which you are clicking the icon.

After clicking the icon, a container is added to the Home page, as shown in [Figure 5-2](#):

**Figure 5-2 A New Container**



5. Click **Close** on the navigation bar at the top to quit customization mode.

---

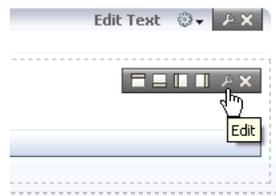
**Note:** After you add a container, you must add UI components to use it. For information about adding UI components to a container, see "Customizing the Home Page" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

---

## 5.1.2 Editing a Container

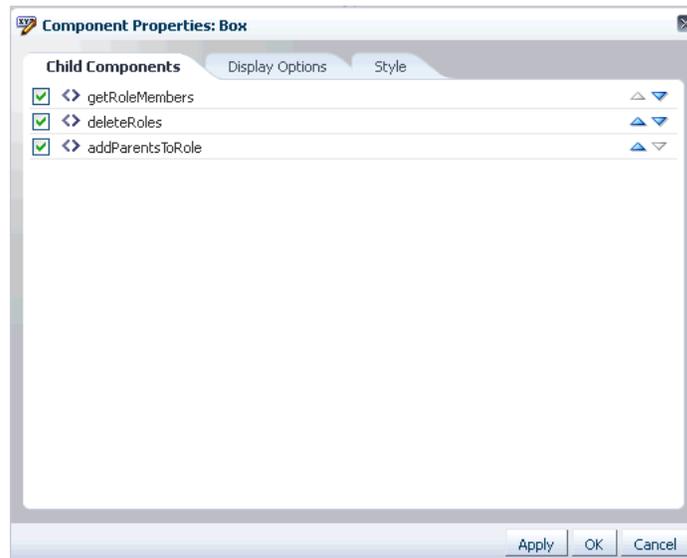
To edit a container in the Home page:

1. In the container that you want to edit, click the Edit icon on the toolbar, as shown in the following figure:



The Component Properties dialog box is displayed with the Child Components tab active, as shown in [Figure 5-3](#):

**Figure 5-3** The Component Properties Dialog Box



2. Use the up and down arrows to move the components up or down in the container.
3. Deselect a component to hide it. Only the selected components are displayed in the container.
4. Click the **Style** tab. In this tab, you can change the properties of the container, such as background color and image, font properties, and margin.
5. Click **Apply**, and then click **OK**.

## 5.1.3 Removing a Container

To remove a container from the Home page:

1. In the container that you want to remove, click the Delete icon, as shown in the following figure:



A message is displayed asking for confirmation.

2. Click **Delete**. The container is deleted from the Home page.

### 5.1.4 Moving Containers

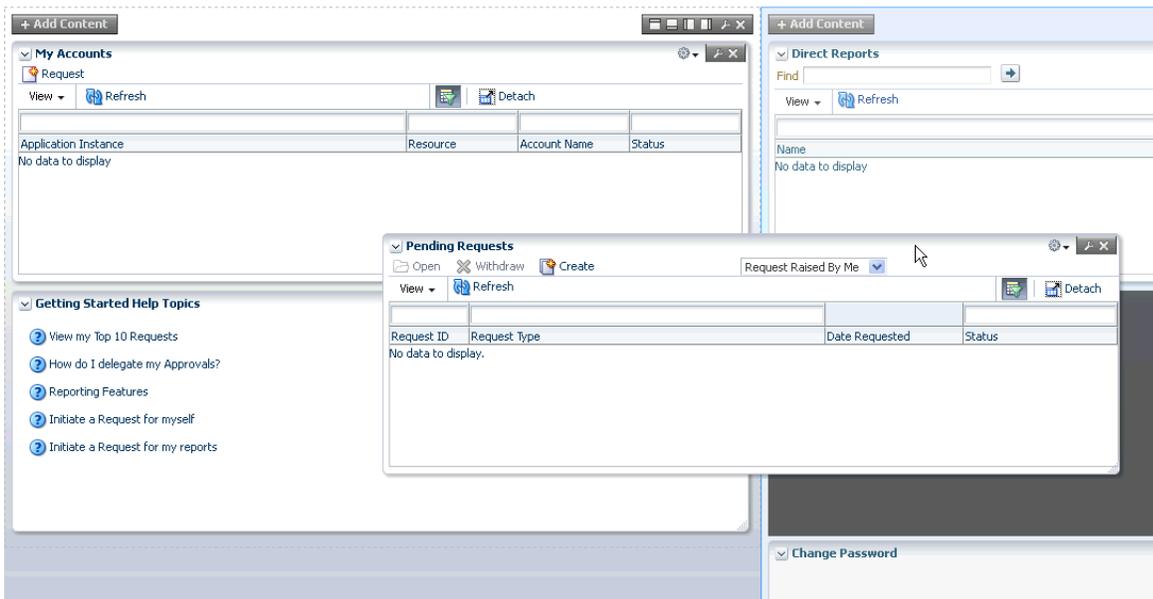
To move the containers in the Home page:

1. To move the containers up or down in the Home page, click the down arrow icon on the top of the container, and select **Move Up** or **Move Down**.

You can move the containers up or down by using the down arrow icon in both customization and noncustomization modes.

2. To move a container across the Home page, in the customization mode, drag the container and drop it in the location where you intend to place it, as shown in [Figure 5-4](#):

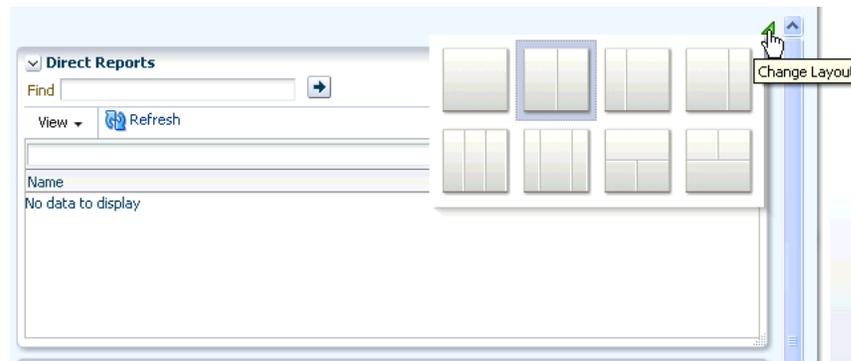
**Figure 5-4 Dragging and Dropping a Container**



### 5.1.5 Changing the Layout of the Home Page

To change the layout of the Home page:

1. In the Home page, click the Change Layout icon on the top right of the containers, as shown in [Figure 5-5](#):

**Figure 5–5 Home Page Layout**

If you are in customization mode, then you can click **Change Layout**.

The current layout is selected by default.

2. Change the layout by selecting a layout, such as one column or two columns below wide area.

If you are in customization mode, then click **Save**, and then click **Close**.

The Home page is displayed in the selected layout.

## 5.2 Adding and Removing Attributes in Search Criteria

Identity Self Service allows you to search for records in various pages, such as the Users page or the Roles page. Default attributes are available in the search pages based on which you can perform the search. In addition to the default search attributes, you can add search attributes based on which you can perform the search.

To add attributes in search criteria:

1. Navigate to a page in Identity Self Service with search option, such as the Users page or the Roles page. For example, to open the Roles page, under Administration, click **Roles**.
2. Click **Add Fields**. The list of attributes that you can add to the search criteria is displayed.
3. Select an attribute from the list, for example, Role Description. The selected attribute is added to the Search section.

Note that a cross icon is displayed with the attribute that you added in the Search section. To remove the attribute from the search criteria, click the cross icon.

## 5.3 Personalizing the Search Result

You can personalize the search result to display or hide search attributes that are displayed as columns in the search results table. You can also change the order in which the columns are displayed in the search results table.

To personalize the search result:

1. To show or hide columns in the search results table:
  - a. On the toolbar of the search results page, click **View**, and then select **Columns**. A list of column names for the search results table are displayed. The column names that are already displayed in the search results table have a check mark.



## 5.4.2 Personalizing Saved Search

To personalize saved search:

1. From the Save Search list, select **Personalize**. The Personalize Saved Searches dialog box is displayed.
2. From the Personalize Saved Searches list, select the saved search that you want to personalize.
3. In the Name field, edit the name of the saved search.
4. Select any one or more of the following options:
  - **Set as Default:** Selecting this option sets the save search as a the default search for the page.
  - **Run Automatically:** Selecting this option runs the saved search when you open the page.
  - **Show in Search List:** Selecting this option displays the saved search in the Saved Search list.
5. Click **Apply**, and then click **OK**.

## 5.4.3 Deleting a Saved Search

To delete a saved search:

1. From the Save Search list, select **Personalize**. The Personalize Saved Searches dialog box is displayed.
2. From the Personalize Saved Searches list, select the saved search that you want to delete.
3. Click **Delete**. A warning message is displayed.
4. Click **Yes** to confirm deletion.
5. Click **OK** to close the Personalize Saved Searches dialog box.

## 5.4.4 Using Saved Search to Perform a Search Operation

If you select the **Set as Default** option when creating the saved search, then the saved search is displayed in the Saved Search list when you open the page. To search for records by using the default saved search, click **Search**.

If you select the **Run Automatically** option when creating the saved search, then the search operation based on the saved search is performed automatically when you open the page.

If you have not selected the **Set as Default** and **Run Automatically** options, then to perform the search by using the saved search, select the saved search from the Saved Search list.

## 5.5 Sorting Data in Search Results

You can sort the data in the search results table in ascending or descending order. When you place the mouse pointer on the column names in the search results table, up and down arrow keys are displayed. Clicking the up arrow key sorts the data in ascending order, and clicking the down arrow key sorts the data in descending order.

The sort is restored as a preference in the Self Service. As a result, when you logout, and login again and perform a search, sorted data is displayed in the search result. The sort preference works only for the logged in user. For other users, the search results table is displayed with default settings.

## 5.6 Using Query By Example

In many Self Service pages, data is displayed in a tabular format. Users can have hundreds of roles and resources, and thousands of entitlements provisioned to them. When you are looking at a large number of records, you need to scroll through multiple pages of results to find specific role, resources, and entitlements. By using the Query By Example feature, you can refine the search results by providing additional filters. Oracle Identity Manager allows you to turn this feature on and off based on your requirement.

When looking for a few records in a list of large number of records, you can use Query By Example to refine the search. To do so:

1. In the search results table, click **View** on the toolbar, and then select **Query By Example**. Text fields are displayed on top of each column of the search results table.
2. Enter a value in a text field for a column. For example, to refine the search for all users with Disabled status, enter Disabled on the text field above the Status column.

Instead of entering the complete value, you can enter a few letters that match the values you are searching, such as Di. Users with Disabled status are displayed. If you enter D as the value, then all users with Disabled or Deleted are displayed (because both the Disabled and Deleted status begin with the letter "D").

3. Press **Enter**. All records that match the Query By Example value are displayed, as shown in :

**Figure 5–6 Query By Example**

The screenshot shows a table titled 'Direct Reports' with a search filter 'Di' applied to the Status column. The table has columns for User Name, userLogin, Status, and Organization. Two rows are visible: Richard Smith (RICHARD.SMITH@AE, Disabled, Org1) and Jane Lee (JANE.LEE@ABC.COM, Disabled, %ellerate Users).

User Name	userLogin	Status	Organization
Richard Smith	RICHARD.SMITH@AE	Disabled	Org1
Jane Lee	JANE.LEE@ABC.COM	Disabled	%ellerate Users

4. To disable Query By Example, click **View**, and then select **Query By Example**.

---

---

## Managing Profile Information

The My Information page in Oracle Identity Self Service enables you to view and modify personal details.

To open the My Information page:

1. Log in to Identity Self Service.
2. In the left pane, under My Profile, click **My Information**.

The My Information page is displayed with sections for modifying profile attributes, changing password, setting challenge questions, viewing direct reports and their attributes, and viewing and modifying proxy users.

The My Information page has the following sections:

- [Managing Profile Attributes](#)
- [Changing Password](#)
- [Setting Challenge Questions and Response](#)
- [Viewing Direct Reports](#)
- [Managing Proxies](#)

### 6.1 Managing Profile Attributes

When you open the My Information page, your profile attributes are displayed in the Basic User Information section. If the section is not expanded by default, then click the arrow icon beside Basic User Information to expand the section.

Editable attributes are displayed in editable text boxes or appropriate UI widgets, such as lookup fields. You can provide new values and click the **Apply** button to submit a change.

When the profile update is submitted, a request is created for the profile update, and a message is displayed along with a tracking number for the request. Workflow rules determine the approval workflow to start and obtain approval before allowing the changes in attributes. The status of the request can be seen on the Tracking Requests page of Identity Self Service. For more information about requests and tracking, see [Chapter 9, "Managing Requests."](#)

---

---

**Note:** The language preference of the user for the UI is not set according to the locale specified by the user in the Basic User Information section of the Self Service. The UI locale is determined as described in "Setting the Language for Users" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

---

---

After submitting the request for modifying profile attributes, you can click the down arrow icon beside Basic User Information to collapse the section.

## 6.2 Changing Password

The Change Password section allows you to reset your enterprise password or target system account password (for example, the Microsoft Active Directory account) that you have been provisioned to. To specify a new password, enter and re-confirm the new passwords. The new password is evaluated for compliance against the applicable password policy. If the new password does not comply with the password policies, then the password change is rejected and you are informed of the failing condition(s). If the password evaluates successfully against all policies, then the password is changed.

To change the password:

1. In the My Information page, expand the Change Password section.
2. From the Account Type list, select one of the following options:
  - **Oracle Identity Manager** - This specifies that the Oracle Identity Manager password is being reset.
  - **Target system account** - This specifies that the password of the target system account that has been selected is being reset. For example, if you have been provisioned to both Microsoft Active Directory and Lotus Notes and Domino, and you want to reset the password of the Lotus Notes and Domino account, then select **Lotus Notes and Domino**.
3. If you selected Oracle Identity Manager in the preceding step, then specify values for the following fields:
  - **Old Password:** Enter the existing password.
  - **New Password:** Enter the new password that you want to set. Click the icon to the right of the New Password field. A list of conditions to set the password is displayed. These conditions are being specified in the password policy, and you must comply with the conditions to specify a password.
  - **Confirm New Password:** Re-enter the new password.

For information about password policies, see the "Managing Password Policies" chapter in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

4. If you selected a target system account in Step 2, then specify values for the following fields:
  - **New Password:** Enter the new password that you want to set. Click the icon to the right of the New Password field. A list of conditions (as specified on the target system) to set the password is displayed. If no conditions to set the password are available on the target system, then the conditions set for the enterprise account are displayed. These conditions are being specified in the

password policy, and you must comply with the conditions to specify a password.

- **Confirm New Password:** Re-enter the new password.

For information about password policies, see the "Managing Password Policies" chapter in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

5. Click **Apply**. If the old password is valid and the new password is in compliance with the password policy, then the password is changed. Otherwise, an error message is displayed.

## 6.3 Setting Challenge Questions and Response

The challenge-response service allows you to set up a series of challenge questions that are used to validate the user's identity to reset a forgotten password. Only the user should know the correct answers to the challenge questions.

Questions and answers are stored as part of the user's profile as a name-value pair list, where the name is the question, and the value is the answer to that question. For example, for user John Doe, the challenge-response set could be as follows:

Challenge	Response
What is your favorite color?	Blue
What is the name of your pet?	Rex
What is the city of your birth?	New York

---

**Note:** Oracle recommends defining answers to challenge questions that cannot be guessed easily by collecting information about the user from the Internet or other public sources.

---

When a user's identity needs to be validated without relying on the authentication scheme, the challenge questions are asked, and the user must provide the necessary number of correct answers.

To set the challenge questions and responses:

1. In the My Information page, expand the **Challenge Questions** section.
2. Select questions from the Question 1, Question 2, and Question 3 fields.
3. In the corresponding Answer 1, Answer 2, and Answer 3 fields, enter the answers.
4. Click **Apply**.

---

**Note:** Challenge questions and responses once set are not visible in this section. If you see the following message in the Challenge Questions section, then you have already set your challenge questions and responses:

Your secret questions and answers are already set.

You can modify the challenge questions and responses that you have already set by performing the procedure described earlier in this section.

---

## 6.4 Viewing Direct Reports

The Direct Reports section in the My Information page lists the direct reports of the user in the management hierarchy, in a tabular format. This section allows you to view the details of each direct report. For each user in the list, the following are displayed:

- Display Name
- User Login
- Identity Status
- Organization

**Tip:** You can add or remove users to and from organizations by using the Attributes tab of the user details page.

If there are a large number of users as your direct reports, then you can query and find a direct report by using the Query By Example feature. See "[Using Query By Example](#)" on page 5-8 for more information about the Query By Example feature.

### 6.4.1 Viewing and Modifying Direct Reports

To view and modify direct reports:

1. In the My Information page, expand the Direct Reports section.
2. Select a user or direct report by clicking the record of the direct report.
3. From the Actions menu, select **Open**. Alternatively, click the **Open** icon on the toolbar. The details of the user is displayed in a new tab. This tab displays the details of the user in various subtabs, such as Attributes, Roles, Entitlements, Accounts, and so on. You can click each tab to review the details of the user.

When you open the user details of a direct report, you can perform certain tasks for the user, such as reset password for the user, and unlock or lock the user's account. You can also view the details of the direct reports of the open user, and perform certain tasks for the user, who is your indirect report. For more details, see "[Modifying Users](#)" on page 11-35.

## 6.5 Managing Proxies

The Proxies section in the My Information page allows you to view and manage the proxy information. It displays the proxies currently set up within Oracle Identity Manager for you, and also allows you to view previously set up proxies. The past proxies view, which displays all proxies that were added in the past, is read-only, and no modifications are allowed.

The existing proxy view allows you to cancel an upcoming proxy whose start date is in the future. You can also edit only the end date of an in-progress proxy whose start date is in the past and end date is in future or not specified.

In the section for current proxies, you can also add new proxies. When adding new proxies, you must specify a start date, an end date, and the proxy user.

This section contains the following topics:

- [Adding a Proxy](#)
- [Editing a Proxy](#)
- [Removing a Proxy](#)

## 6.5.1 Adding a Proxy

To add a proxy:

1. In the My Information page, expand the Proxies section.  
The Current section displays a list of users currently set up as your proxy. The Past section displays a list of past proxies.
2. In the Current section, from the Actions menu, select **Add**. Alternatively, you can click **Add** on the toolbar.  
The Add Proxy dialog box is displayed.
3. For Proxy Name, select any one of the following:
  - **My Manager:** To specify your manager as proxy.
  - **Other User:** To specify any other user as proxy. To do so, click the lookup icon to search for the user you want to specify as proxy.
4. In the Start Date field, specify a start date. To do so, click the Select Date icon to the right of the Start Date field, and select a date from the calendar.
5. In the End Date field, specify an end date.
6. Click **Apply**. The proxy is added to the list of proxies in the Proxies section.

---

---

**Note:** Oracle Identity Manager does not allow adding another proxy whose start and end dates overlap with the existing proxy.

---

---

## 6.5.2 Editing a Proxy

To edit a proxy:

1. In the Current section, select a proxy that you want to edit.
2. From the Actions menu, select **Edit**. Alternatively, you can click **Edit** on the toolbar.  
The Edit Details dialog box is displayed.
3. In the Proxy Name field, select **My Manager** to specify your manager as proxy. Otherwise, select **Other User** to specify any other user as proxy. You can search for the user name.

---

---

**Note:**

- To change the proxy user, you can search only those users for which you have search permission.
  - You cannot modify the Proxy Name field for proxy that is in the "In Progress" state.
- 
- 

4. In the Start Date and End Date fields, if required, specify revised dates.

---

---

**Note:** You cannot modify the Start Date field for a proxy that is in the "In Progress" state.

---

---

5. Click **Apply**. The edited proxy information is saved.

### 6.5.3 Removing a Proxy

To remove a proxy:

1. In the Current section, select a proxy that you want to remove.
2. From the Actions menu, select **Remove**. Alternatively, you can click **Remove** on the toolbar.

When a current proxy is deleted, its end date is set as the date when it is deleted and when a future proxy is deleted, it is removed from the system.

To remove all proxies, click **Remove All** on the toolbar, or select **Remove All** from the Actions menu.

A message is displayed asking for confirmation.

3. Click **Yes**. The selected proxy is removed from the Current section.

---

---

## Managing Access

In Oracle Identity Manager, you have access to entities, such as roles, entitlements, accounts, and admin roles. Access to these entities is governed by authorization policies. For information about authorization policies, see "Security Architecture" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

The entities to which you have access are displayed in the My Access section of the Oracle Identity Self Service. Typical tasks you perform in the My Access section are described in the following topics:

- [Managing Roles](#)
- [Managing Entitlements](#)
- [Managing Accounts](#)
- [Viewing Admin Roles](#)

**Tip:** Adding and removing entities, such as roles, entitlements, and accounts, go through requests that are subject to approval. Before you perform the steps to manage your access to entities, it is recommended that you see [Chapter 9, "Managing Requests"](#) for detailed information about requests in Oracle Identity Manager.

### 7.1 Managing Roles

The Roles tab in the My Access section displays the roles assigned to you. In this tab, you can perform the following:

- [Requesting for Roles](#)
- [Modifying Role Details](#)
- [Removing Roles](#)

#### 7.1.1 Requesting for Roles

To request for roles from the My Access page:

1. Log in to Identity Self Service.
2. Under My Profile, click **My Access**. The My Access page is displayed.
3. Click the **Roles** tab. A list of roles assigned to you is displayed.

---

---

**Note:** In all the tabs in the My Access page, you can refine your search by using Query By Example. For information about using Query By Example, see ["Using Query By Example"](#) on page 5-8.

---

---

4. From the Actions menu, select **Request**. Alternatively, click **Request Roles** on the toolbar.

The Catalog page is displayed. You use the Catalog page to create requests. For information about request catalog, and how to create requests from the Catalog page, see ["Creating Requests"](#) on page 9-15.

When you submit your request for roles, and the request is approved at all approval levels, the roles will be assigned to you.

## 7.1.2 Modifying Role Details

Modification of selected role is possible only if the user is a Role Administrator for the organization to which the role is published. If the user is of any other role or an end-user, then the user can only view the role details.

To modify the details of a role assigned to you:

1. In the Roles tab of the My Access page, select a role whose details you want to modify.
2. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar.

The Role: *ROLE\_NAME* page is displayed with details of the selected role. In this page, you can modify role attributes, role hierarchy, role membership, and publish the role to organizations. For details about these tasks, see ["Managing Roles"](#) on page 12-1.

## 7.1.3 Removing Roles

To remove roles assigned to you:

1. In the Roles tab of the My Access page, select a role that you want to remove.
2. From the Actions menu, select **Remove**. Alternatively, click **Remove Roles** on the toolbar. The Remove Roles catalog page is displayed.
3. Submit the request to remove roles. The role will be removed after the request is approved.

## 7.2 Managing Entitlements

The Entitlements tab in the My Access page displays the entitlements assigned to you. In this tab, you can perform the following:

- [Requesting for Entitlements](#)
- [Removing Entitlements](#)

### 7.2.1 Requesting for Entitlements

To request for entitlements:

1. In the My Access page, click the **Entitlements** tab. A list of entitlements assigned to you is displayed.

---

---

**Note:** In an upgraded deployment of Oracle Identity Manager 11g Release 2 (11.1.2.1.0), the entitlements provisioned to the users before the upgrade are not displayed in the Entitlements tab. To display the entitlements in the Entitlements tab after the upgrade, login to Oracle Identity System Administration, and run the Entitlement Assignments scheduled job. See "Predefined Scheduled Tasks" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about the Entitlement Assignments scheduled job.

---

---

2. From the Actions menu, click **Request**. Alternatively, click **Request Entitlements** on the toolbar. The Catalog page is displayed.
3. Submit the request from the Catalog page. The entitlement will be assigned after the request is approved.

For information about creating a request, see "[Creating Requests](#)" on page 9-15.

## 7.2.2 Removing Entitlements

To remove entitlements assigned to you:

1. In the Entitlements tab, select the entitlements that you want to remove.
2. From the Actions menu, select **Remove**. Alternatively, click **Remove Entitlements** from the toolbar. The Catalog page is displayed.
3. Submit the request to remove entitlements. The entitlement will be removed after the request is approved.

## 7.3 Managing Accounts

The Accounts tab in the My Access page displays the accounts assigned to you. In this tab, you can perform the following:

- [Requesting for Accounts](#)
- [Modifying Accounts](#)
- [Removing Accounts](#)
- [Disabling an Account](#)
- [Enabling an Account](#)

### 7.3.1 Requesting for Accounts

To request for accounts:

1. In the My Access page, click the **Accounts** tab. A list of accounts assigned to you is displayed.
2. From the Actions menu, click **Request**. Alternatively, click **Request Accounts** on the toolbar. The Catalog page is displayed.
3. Submit the request from the Catalog page. The account will be assigned after the request is approved.

For information about creating a request, see "[Creating Requests](#)" on page 9-15.

---

---

**Note:** If you request for an entitlement and application instance together in a single request, and if the beneficiary does not have an account provisioned at the time of entitlement provisioning, then entitlement provisioning fails. However, application instance provisioning succeeds. Therefore, if you request for entitlement and application instance together in a single request, then you must have a primary account provisioned to the target on which the entitlement is stored.

---

---

### 7.3.2 Modifying Accounts

To modify accounts assigned to you:

1. In the Accounts tab, select an account that you want to modify.
2. From the Actions menu, select **Modify**. Alternatively, click **Modify Accounts** on the toolbar. The Catalog page is displayed.
3. Edit the attributes of the account and submit the request from the Catalog page. The account will be modified after the request is approved.

### 7.3.3 Removing Accounts

To remove accounts assigned to you:

1. In the Accounts tab, select the account that you want to remove.
2. From the Actions menu, select **Remove**. Alternatively, click **Remove Accounts** from the toolbar. The Catalog page is displayed.
3. Submit the request to remove accounts. The accounts will be removed after the request is approved.

### 7.3.4 Disabling an Account

To disable an account:

1. In the Accounts tab, select an account that you want to disable.
2. From the Actions menu, select **Disable**. Alternatively, select **Disable** on the toolbar. The Catalog Page is displayed.
3. Submit the request to disable accounts. The accounts will be disabled after the request is approved.

### 7.3.5 Enabling an Account

To enable an account:

1. In the Accounts tab, select an account that you want to enable.
2. From the Actions menu, select **Enable**. Alternatively, select **Enable** on the toolbar. The Catalog Page is displayed.
3. Submit the request to enable accounts. The accounts will be enabled after the request is approved.

## 7.4 Viewing Admin Roles

The Admin Roles tab of the My Access page displays the admin roles you have. Admin roles determine the operations you can perform on each entity. This is governed by authorization policies based on organizations and admin roles. For details on admin roles and authorization in Oracle Identity Manager, see "Security Architecture" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.



---

---

# Using the Access Request Catalog

Oracle Identity Manager supports requesting for entities such as roles, application instances, and entitlements. You can request for these entities by using an access request catalog. All entities that can be requested are published to the catalog, using which you can request for the entities. Publishing is a term used for making an entity available for requesting or provisioning by the users of a particular organization. Users of that organization with Viewer admin role, can request for the entity through the request catalog. In addition, users can request for entities that are published to the home organization.

This section discusses the following topics:

- [Viewing and Modifying the Access Request Catalog for Catalog Items](#)
- [Adding and Removing Catalog Items to and from the Cart](#)

---

---

**Note:** At some places in this guide, access request catalog has been referred to as **catalog** or **request catalog**.

---

---

## 8.1 Viewing and Modifying the Access Request Catalog for Catalog Items

Based on permissions, you can view and modify catalog items in a request catalog as follows:

1. Log in to Oracle Identity Self Service.
2. In the left pane, under Requests, click **Catalog**. The Catalog page is displayed.
3. Search for a catalog item that you want to view or modify as follows:

In the Catalog field, enter a search keyword, and click the search icon on the right. The search results are displayed. The catalog items that match the search condition are listed in the Catalog Items section. Search results are filtered and displayed depending on the authorization policy granted to the user that is performing the search. See "[Supported Search Operators](#)" on page 8-3 for more information about supported search operators.

4. To view the catalog item, from the search results, select a catalog item. The details of the catalog item are displayed in the Detailed Information section.
5. To modify the catalog item, in the Detailed Information section, modify the attributes of the catalog item and then click **Apply** to save the changes. [Table 8-1](#) lists the fields in the Detailed Information section.

**Note:**

- You can modify attribute values if the fields are editable. If you do not have the required permission to modify the details, then these fields are displayed as read-only.
- To see the edit changes, you must log out and relogin to the Catalog edit page.

**Table 8–1 Fields in the Detailed Information Section**

Fields	Description
Name	Base entity name
Display Name	Base entity display name
Description	Description of the base entity
Category	Category of the catalog item  By default, category can be either Role, Entitlement, or Application Instance. You can edit the value of this field to create a new user-defined category. This is illustrated by the following example:  Suppose the category is Role. If you want to specify a new category (for example, <i>My_Roles</i> ) for the current catalog item, then change the value of this field to <i>My_Roles</i> .
Audit Objective	A text field in which any relevant value or description that is use for Oracle Identity Analytics (OIA) certification
Risk Level	Level of risk for the entity  The values that you can set for this field are Low Risk, Medium Risk, and High Risk.
User Defined Tags	Any value that describes the catalog item and used for searching the entity in future
Approver User	User who can approve the catalog item  This is used at the time of processing the request for the catalog item or during attestation
Approver Role	Role that can approve the catalog item
Certifier User	User that can certify the catalog item
Certifier Role	Role that can certify the catalog item
Fulfillment User	User that can complete or fulfill the request for the catalog item
Fulfillment Role	Role that can complete or fulfill the request for the catalog item
Certifiable	Specifies whether a catalog item is certifiable

6. If you want to revert the changes made, then click **Revert**.

### 8.1.1 Refining Search Results

After searching for catalog items, as described in "[Viewing and Modifying the Access Request Catalog for Catalog Items](#)" on page 8-1, you can refine your search results to make it more precise. To do so, in the Refine Search section of the Catalog page, select one or more categories to display the catalog items of those categories. You can select

or deselect the **Select All** checkbox to display or hide all items belonging to the categories.

Categories are a way of organizing entities in a request catalog. Each catalog item is associated with one and only one category. Categories of a catalog can be roles, entitlements, or application instances. For example, you can refine your search result to display catalog items belonging to the entitlements category only by selecting **Entitlements** in the Categories section.

## 8.1.2 Supported Search Operators

You use the Catalog field to specify a keyword to search or browse through the request catalog for catalog items. A search keyword is case insensitive. Here are the supported search operators:

- One or more keywords: You can specify one or more keywords as a search condition.

Sample value for one keyword: administrator

This search condition finds all catalog items that contain the term "administrator."

Sample value for more than one keyword: web administrator

This search condition finds all catalog items that contain the terms web and administrator. This search automatically applies the AND operator to the search keywords. This is because a space character between keywords behaves as an AND operator. Alternatively, you can use an & operator to denote an AND relationship explicitly.

For example, web administrator and web & administrator return catalog items that contain both web and administrator.

- Phrase search: To search for catalog items that contain the exact phrase that you enter, you must specify the search condition within double quotes ("").

For example, searching for "web administrator" returns catalog items containing the phrase "web administrator"

- OR [|] search: Use the OR [|] operator to search for catalog items containing any of the search keywords.

Sample value 1: web | administrator

This search condition returns catalog items containing the term web or administrator.

Sample value 2: "vision purchasing" | administrator

This search condition returns catalog items containing the phrase "vision purchasing" or the term administrator.

- Wildcard search: You can use the asterisk (\*) symbol as the wildcard to perform search operations. However, the catalog search does not support a search condition that begins with or contains only the asterisk (\*) symbol.

For example, admin\* returns catalog items beginning with admin such as administrator and administration.

---

---

**Note:**

- If the number of records are huge in the catalog table, and if you use the hash symbol (#) and add the asterisk (\*) symbol to it, you get an error.
  - You must use only double quote while performing search.
- 
- 

## 8.2 Adding and Removing Catalog Items to and from the Cart

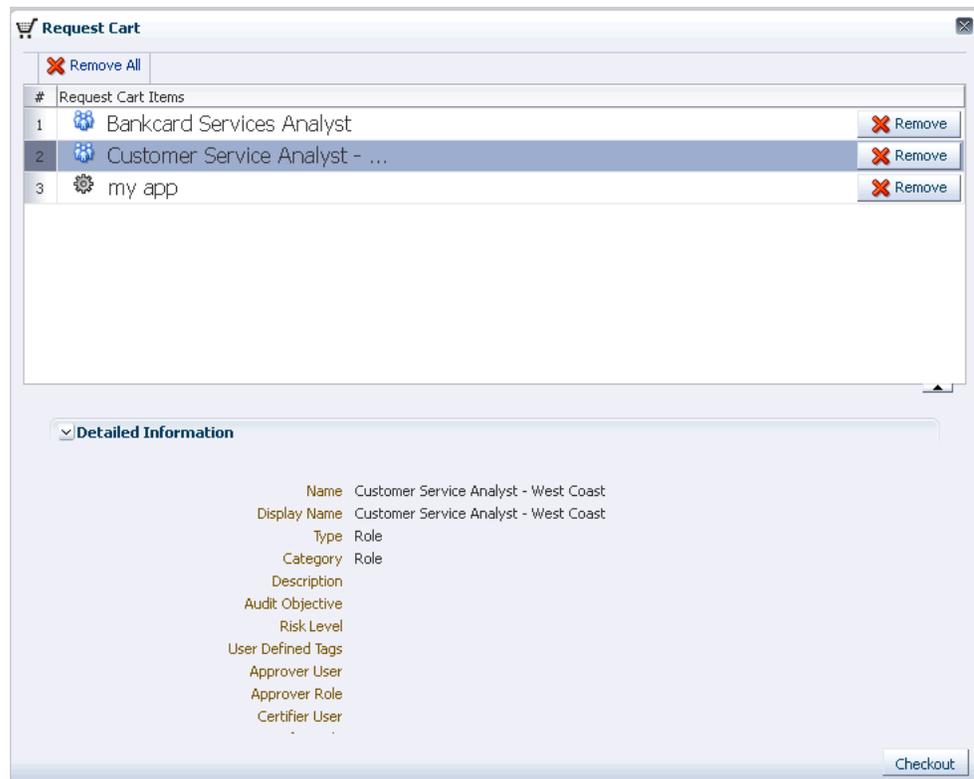
A request cart, also known as a cart, contains a set of catalog items that the user selects from the request catalog. Users can add catalog items to the request cart to submit a request for entities such as roles, entitlements, and application instances. The request cart does not persist across user sessions.

To add catalog items to the cart:

1. Log in to Identity Self Service.
2. Search for the catalog items that you want to add to the cart. See "[Viewing and Modifying the Access Request Catalog for Catalog Items](#)" on page 8-1 for the procedure to search for catalog items.
3. If required, narrow down your search result by selecting or deselecting one or more categories in the Refine Search section. You can select or deselect the **Select All** checkbox to display or hide all the items belonging to the categories.
4. Select a catalog item that you want to request, and then click **Add to Cart**. The information of the selected catalog item is displayed in the Detailed Information section.

You can also select multiple items by pressing **Ctrl** and clicking the items, and then clicking **Add Selected to cart**.

5. Click **Edit**. The Request Cart dialog box is displayed with a list of catalog items in the cart, as shown in [Figure 8-1](#):

**Figure 8–1 The Request Cart**

6. Select a catalog item to display detailed information about the item. Review the details, and if required, you can remove the item from the cart by clicking **Remove** for the corresponding item.

Alternatively, you can click **Remove All** to delete all items from the cart.



---

---

## Managing Requests

In Oracle Identity Manager, various operations, such as adding a role to self or provisioning an application instance, is performed through requests. A request is an entity created by the users or administrators performing a specific action that requires a discretionary permission to be gained by someone or some process before the action can be performed. For example, a user can create a request to gain access to a laptop computer, and a manager can create an open requisition based on the request.

A request has a requester, a beneficiary (optional), and a target entity. A *requester* is an entity that creates or raises a request. A requester can be a user or the system itself. The functional component decides on the requester for system-generated requests. An example of a system-generated request is a request created by the system based on access policy. Here, the functional component is access policy. For unauthenticated requests, the requester is not authenticated to Oracle Identity Manager and is therefore, not present in the system.

A *beneficiary* is an entity that benefits from the action performed after the request is completed and the request is completed only if it is executed successfully.

In Oracle Identity Manager, terms such as role, application instance, and entitlements are defined as entities. Each one of these entities maintains a list of attributes belonging to this entity. Each entity also defines a list of operations that it supports.

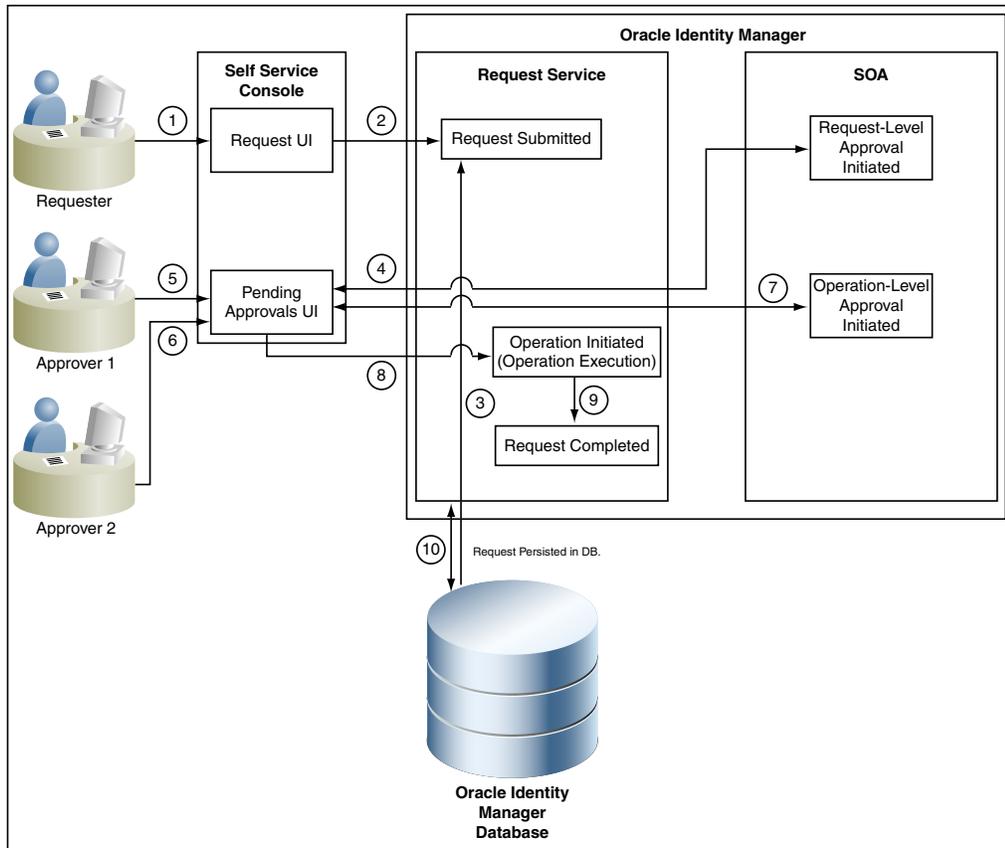
*Target entity* is the resource or entity that is requested for the beneficiary.

For instance, you create a request to provision a UNIX account for the user John Doe. Here, you are the requester, John Doe is the beneficiary, and the UNIX account is the target entity that is requested for John Doe.

As discussed earlier in this guide, Oracle Identity Manager supports requesting for entities such as roles, application instances, and entitlements. You can request for these entities by using a request catalog.

Each request goes through a specific lifecycle after it is created in the system. This lifecycle is managed and controlled by the Request Service. The lifecycle transitions the request through various stages. The stage that a request is in determines what action the controller takes in that step, what operations are available on the request, and what possible stage the transitions are in at that time. [Figure 9 1](#) outlines the process flow of a request:

**Figure 9 1 Request Process Flow**



The request process flow is described with the help of an example of provisioning a laptop computer to a user through a request. The steps are:

1. The requester raises a request to assign a laptop computer to a user by using the Request UI.

---

**Note:** Requests can be raised by using Oracle Identity Self Service.

---

2. The request is submitted to the request service.
3. The request is also stored in Oracle Identity Manager database.
4. Request-Level Approval workflow is initiated by request service in Service-Oriented Architecture (SOA). Based on the workflow configuration, associated tasks are assigned to the corresponding approvers.

**See Also:** "Developing Workflows for Approval and Manual Provisioning" for information about approval workflows in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

5. The request-level approver approves the request by using the Inbox in Identity Self Service. In this example, the requester's manager (Approver 1) is the request-level approver who decides whether to assign a laptop to user 1. If the request-level approver rejects the request, the request goes to a Rejected stage.

---

---

**Note:** When a user requests for an item, Oracle Identity Manager checks if the requester can view the catalog items, but does not check if the items can be granted to the beneficiary. When the request is approved, then Oracle Identity Manager checks if the requested access can be granted to the beneficiary.

---

---

6. If the Approver1 has designated his role to Approver 2, then Approver 2 is the request-level approver who decides whether to assign a laptop to user 1. If Approver 2 rejects the request, the request goes to a Rejected stage.
7. The operation-level approver approves the request by using the Inbox. In this example, the IT admin for the organization is the operation-level approver (Approver 2) who is responsible for issuing a laptop to the user. If the operation-level approver rejects the request, then the request goes to a Rejected stage.

---

---

**Note:** Operation-level request is not initiated if the request is rejected at the request level.

---

---

8. The request operation is initiated in the request service, and the request is executed.
9. The request operation is completed. At this stage, the request operation has the Completed status.
10. The request status is updated in Oracle Identity Manager database.

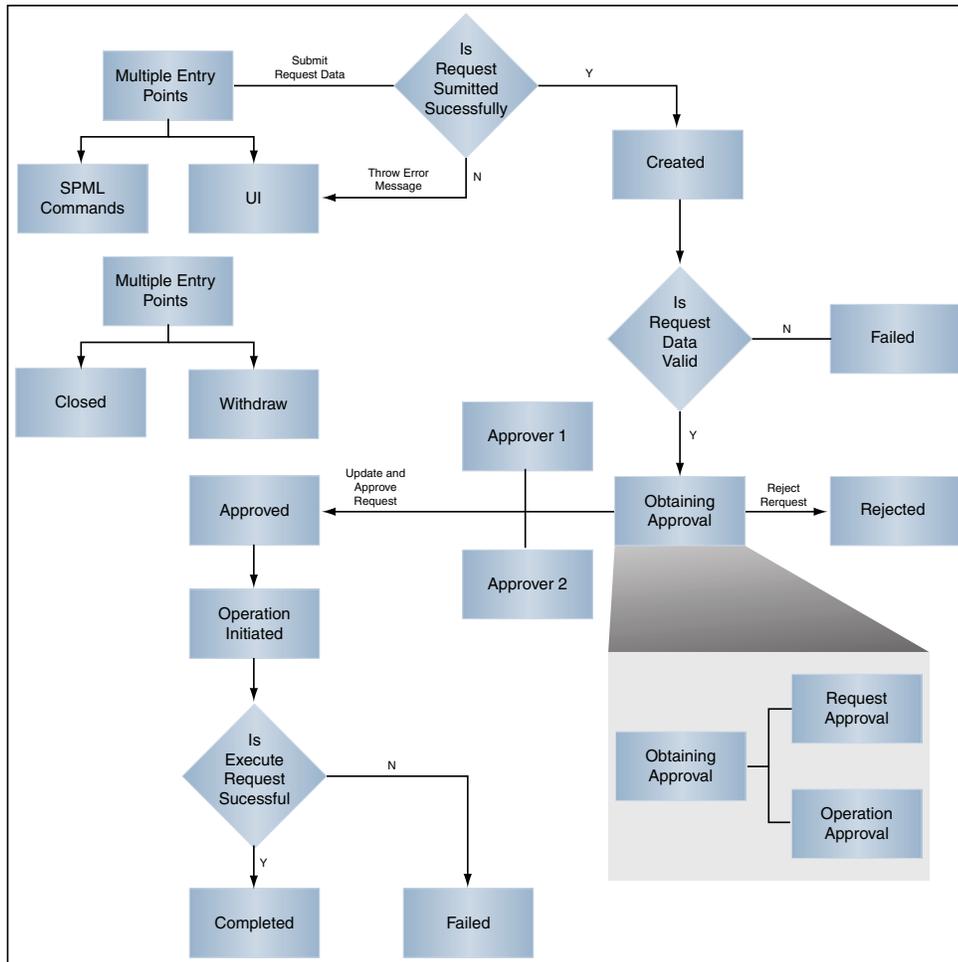
This chapter describes request management in the following sections:

- [Request Stages](#)
- [Bulk Requests and Child Requests](#)
- [Heterogeneous Requests](#)
- [Request vs. Direct Operation](#)
- [Request Categories](#)
- [Common Reasons for Request Failure](#)
- [Request Profiles](#)
- [Creating Requests](#)
- [Tracking a Request](#)
- [Withdrawing a Request](#)
- [Closing a Request](#)

## 9.1 Request Stages

Each request goes through a specific lifecycle after it is created in the system. This lifecycle is managed and controlled by the request service. The lifecycle transits the request through various stages. The stage a request is in determines what action the controller takes in that step, what operations are available on the request at that time, and what the possible stage transitions are. [Figure 9 2](#) outlines the lifecycle flow of a request in the request service:

**Figure 9 2 Request Stages**



**Note:** If a request is not submitted successfully, then the error messages are displayed in the UI. For SPML-initiated requests, the error messages are thrown to SPML.

Figure 9 2 shows all the stages that a request can go through. This diagram specifies stages for a simple request. For information about bulk request, refer to Figure 9 3, "Bulk Request and Child Request Stages".

Each stage represents the logical next step in the request lifecycle. Only the successful execution of an operation can take the request from one stage to the next.

Table 9 1 describes how a request functions at various stages through its life cycle and how a request attains these stages:

**Table 9 1 Request Stages**

Request Stage	Description
Request Created	After successful submission of the request, the request moves to the Request Created stage.

**Table 9 1 (Cont.) Request Stages**

Request Stage	Description
Obtaining Approval	<p>After the request is created, the request engine moves the request to "Obtaining Approval" stage automatically if there are approvals defined for this request. At this stage, the corresponding approvals are initiated through the request service. Upon completion of the same, the request engine looks at the model defined for this request to find out the approval selection methodology to find out the exact approval process to instantiate.</p> <p>When the request engine finds out the approvals that are required to be initiated, it again calls request service to instantiate the workflow.</p> <p>If a request is withdrawn or closed at this stage, then the request engine calls cancel workflow on each workflow instance. Notifications are sent to approvers about the withdrawn tasks.</p> <p>For request notification level 2, notifications are sent for request creation and change of status to any of the Request End statuses. Request End statuses include Request Failed and other failure related statuses, Request Completed, Request Withdrawn, and Request Closed.</p> <p><b>Note:</b> Configuration of notification can be done in the human task of a SOA composite.</p> <p>The following request statuses are associated with Obtaining Approval stage:</p> <ul style="list-style-type: none"> <li>■ Obtaining Request Approval</li> <li>■ Obtaining Operation Approval</li> </ul> <p>For information about these request statuses, refer "<a href="#">Bulk Requests and Child Requests</a>" on page 9-8.</p> <p>After the request successfully completes these statuses, it will attain the Request Approved stage.</p> <p>If an SoD validation check is plugged-in after the request has been successfully created, the request is associated with the following statuses.</p> <ul style="list-style-type: none"> <li>■ SoD check not initiated <ul style="list-style-type: none"> <li>A request attains this stage, if the SoD validation is not initiated for provisioning resource based request. The request engine moves the request to this stage after submission of request and before Obtaining Approval.</li> </ul> </li> <li>■ SoD check initiated <ul style="list-style-type: none"> <li>A request attains this stage, if the SoD validation is initiated asynchronously for provisioning resource based request. The request engine moves the request to this stage after submission of request and before Obtaining Approval.</li> </ul> </li> <li>■ SoD check completed <ul style="list-style-type: none"> <li>A request attains this stage, if the SoD validation is completed for provisioning resource based request. The request engine moves the request to this stage after submission of request and before Obtaining Approval.</li> </ul> </li> </ul> <p><b>Note:</b> These SoD request statuses are possible in case the request is any of the following request types:</p> <ul style="list-style-type: none"> <li>■ Provision Application Instance</li> <li>■ Modify Account</li> <li>■ Provision Entitlement</li> <li>■ Revoke Entitlement</li> <li>■ Assign Roles</li> <li>■ Remove from Roles</li> </ul>

**Table 9 1 (Cont.) Request Stages**

Request Stage	Description
Approved	<p>Only after an Operation Approval is approved, the request is moved to the next stage and the request engine is updated with the current status. The outcome that the request engine finds is Approved, Rejected, or Pending.</p> <p>The following request statuses are associated with this stage:</p> <ul style="list-style-type: none"> <li>■ Request Approval Approved</li> <li>■ Operation Approval Approved</li> </ul>
Rejected	<p>Each time a workflow instance is updated, request service updates the request engine with the current status of that instance. The outcome that the request engine expects from request service is Approved or Rejected. If any of the workflow instances that are instantiated are rejected, then request engine moves the request to Rejected stage. If any workflow instance is rejected, then the controller calls cancel on all the pending workflows and moves the request to Rejected stage.</p> <p>The following request statuses are associated with this stage:</p> <ul style="list-style-type: none"> <li>■ Request Approval Rejected</li> <li>■ Operation Approval Rejected</li> </ul>
Operation Initiated	<p>After the request is approved, the request engine moves the request to the Operation Initiated stage and initiates the operation.</p> <p>The following request statuses are associated with this stage:</p> <ul style="list-style-type: none"> <li>■ Operation Completed <ul style="list-style-type: none"> <li>After completing the actual requested operation, the request engine moves the request to the Operation Completed stage. This happens after Operation Initiated status and is associated with Completed stage.</li> </ul> </li> <li>■ Post Operation Processing Initiated <ul style="list-style-type: none"> <li>After the actual requested operation is completed, if there exists any additional operation that needs to be executed as post-processing, the request engine moves the request to the Post Operation Processing Initiated stage, before initiating those operations. This happens after Operation Completed status.</li> </ul> </li> </ul> <p><b>Note:</b> In case of a bulk operation, child requests are created after request level approval, and the parent request moves to the "Request Awaiting Child Requests Completion" status.</p>

**Table 9 1 (Cont.) Request Stages**

<b>Request Stage</b>	<b>Description</b>
Request Failed	<p>When the associated operations specified in the request fails to execute, the request cancels any pending operations and moves the request to the Request Failed stage.</p> <p>The following request statuses are associated with this stage:</p> <ul style="list-style-type: none"> <li>■ Request Failed When all associated operations specified in a request fail, the request is moved to the Request Failed stage.</li> <li>■ Request Partially Failed When any associated operation specified in a request fails, the request is moved to the Request Partially Failed stage.</li> <li>■ Request Fulfillment Failed When a request associated with an application instance or entitlement fails, then the request moves to the Request Fulfillment Failed stage.</li> <li>■ Request Fulfillment Failed After Max Retry When a request associated with an application instance or entitlement that is in the Rejected stage is retried until the maximum number of retries is reached, then request moves to the Request Fulfillment Failed After Max Retry.</li> </ul>
Withdrawn	<p>A request can be withdrawn by the requester. At this stage, the request is associated to the Request Withdrawn status, and the initiation of all approvals are canceled.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>■ A request can be withdrawn before Operation Initiated stage. Once the request attains the Operation Initiated stage, the request cannot be withdrawn.</li> <li>■ A request can always be withdrawn by a requester only, which is done by using Identity Self Service.</li> <li>■ An administrator can close requests, which is similar to the withdraw function.</li> </ul>
Completed	<p>After the execution of all operations specified in the request are completed, the request engine moves the request to the Request Completed stage.</p> <p>The following request statuses are associated with this stage:</p> <ul style="list-style-type: none"> <li>■ Request Completed with Errors A request attains this status, when an actual requested operation executes fine, but fails to execute any of the post-processing operations. The Request Completed with Errors stage is associated with the Failed stage.</li> <li>■ Request Completed A request attains this status, when an actual requested operation executes fine without any errors.</li> <li>■ Request Awaiting Completion When a request is scheduled to be executed on a future date, the request attains Request Awaiting Completion status till the operation is completed on an effective date.</li> </ul>

The successful attainment of a stage also results in the status of the request being updated to the corresponding status.

Operations can be executed manually or automatically by the system in response to an event. Examples of manual operations are:

- Submit request
- Close/cancel (withdraw) request
- Approve request when the service is notified that the approval workflow is successfully approved

Examples of automatic operations are:

- Start approvals when the request is submitted
- Execute request when the request is approved and execution date is in the future or not specified

## 9.2 Bulk Requests and Child Requests

A bulk request is a request with multiple beneficiaries, multiple entities, or both. For example, a request to assign multiple roles to user John Doe generates a bulk request. Provisioning requests to provision a resource, such as AD User, to users John Doe and Jane Doe also generates a bulk request. A bulk request has two parts:

- Parent requests: A request submitted with multiple beneficiaries, multiple target entities, or both is a parent request
- Child requests: When the request level approval happens for a parent request, multiple child requests are created. The parent request is divided into multiple child requests containing one beneficiary and one target entity.

The entity data in bulk requests must be same for different beneficiaries specified in the request. For example, for a 'provision application instance' type of request, if multiple beneficiaries are selected, then the form field that is marked as 'Bulk-update' will only be shown and that value is common for all beneficiaries.

The number of child requests generated depends on the number of target entities associated with each beneficiary. For each beneficiary, one of its associated target entities is used to generate for each child request. A child request contains only one beneficiary and one target entity.

For a request with no beneficiaries, each child request is spawned for each target entity. Consider the following example:

For a modify-user bulk request that modifies the attributes of two users, two child requests are created (one for each user).

Consider another example. For a "provision application instance" type of request, there are two beneficiaries. Two application instances are to be provisioned for each beneficiary. In this scenario, there are two child requests for the first beneficiary and two child requests for the second beneficiary. Each application instance and its associated beneficiary are present in each child request. Therefore, for this bulk request, there are a total of one parent request and four child requests.

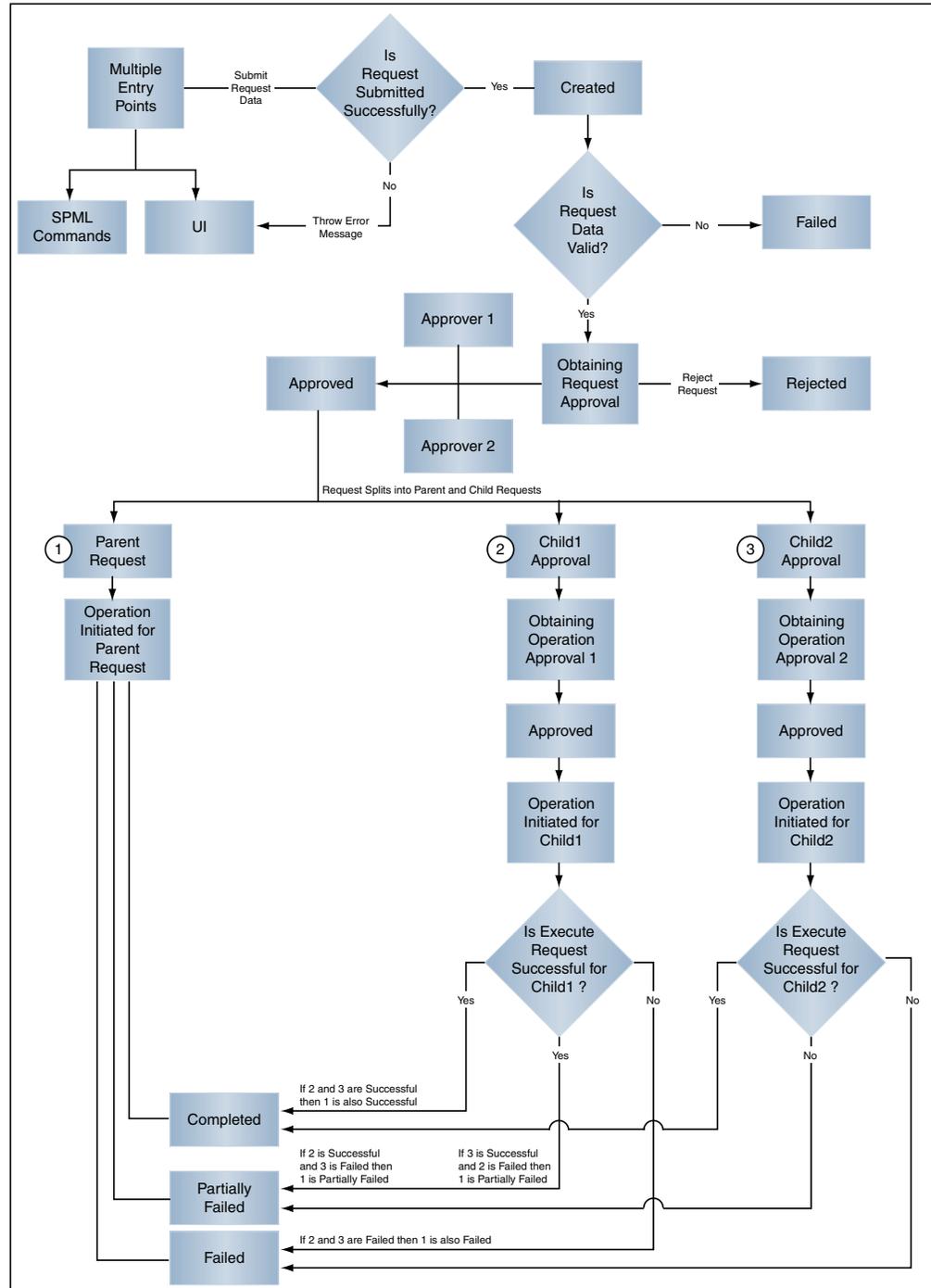
Request-level approval is performed as a part of parent request. After the parent request spawns child requests, the parent request goes to the Request Awaiting Child Requests Completion stage, where in the request awaits for the child requests to complete the operation-level approval. After all the child requests complete, the parent request moves to the Completed stage.

Operation-level approval is performed for child requests only. Approvers can approve or reject child requests individually. If all the child requests are approved or rejected,

then the parent request attains the Completed stage. If one or more (but not all) of the child requests fail, then the parent request attains the Request Partially Failed stage. If all the child requests fail, the parent request attains the Failed stage.

Figure 9 3 outlines the lifecycle flow of a request in the request service:

Figure 9 3 Bulk Request and Child Request Stages



See Also: Table 9 1, "Request Stages" for information about request stages

## 9.3 Heterogeneous Requests

Heterogeneous request is a request created for entities of different types. Oracle Identity Manager supports requesting roles, application instances, and entitlements in a single request, which is heterogeneous in nature.

The following request types are supported in a heterogeneous request:

- Provision Application Instance
- Assign Role
- Provision Entitlement

For a request that is submitted for different entities, the request type is set as "Heterogeneous request". For example, if you submit a single request for two separate entities such as roles and entitlements, then the request type is "Heterogeneous request".

For a request that is submitted for multiple entities of same type, the request type is set according to the entity selected. For example, if you submit a request for multiple roles, then the request type is "Assign Roles".

## 9.4 Request vs. Direct Operation

Users in Oracle Identity Manager can perform various operations in the application. Any operation that you can perform in Oracle Identity Manager is controlled by the authorization policies that have been defined. The admin roles granted to a user in an organization determine whether an operation that a user can perform in Oracle Identity Manager happens directly or through a request. For example, if you are a user administrator, then all operations such as create user, modify user, grant account, enable user account, and so on are direct operations. Similarly, if you have been assigned the User Viewer admin role, then operations such as create user, enable user, delete user, grant role, revoke entitlements, and so on result in a request being created. For more information about admin roles in Oracle Identity Manager, the corresponding permissions allowed to users of that admin role and whether the operation is direct or results in a request, see the "Security Architecture" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Whether an operation results in a request or is performed directly depends on:

- The admin roles granted to the user who is performing the operation. Based on the admin roles granted to the user, an authorization check is performed to determine whether the operation results in a request or direct operation.
- Whether it is a bulk operation or single operation. Irrespective of the admin roles granted to the user, a bulk operation always results in a request.
- Whether a value has been provided in the Effective Date field. If a value is specified in the Effective Date field, the operation results in a request, irrespective of single or bulk operation.

For a single operation without effective date:

If you are performing an operation on yourself, then it results in a request.

If you are performing an operation on others and you are an authorizer, then the operation is direct.

All operations in Oracle Identity Manager do not go through the authorization check to determine if it is a direct operation or a request. Determining whether an operation

is a request or not will be done only for requestable operations. See the tables in ["Request Categories"](#) on page 11 for information about default requestable operations.

The check for direct operation or request is applicable to an operation only if it has a corresponding request model. As a result, this authorization check is performed for creating a user, but not for creating an organization because there is no request model for creating an organization. Similarly, locking and unlocking user accounts are also operations that do not go through the authorization check to determine request or direct operation. Therefore, these operations are direct.

Note that creation of a request does not always mean that the SOA workflow is invoked and manual approval is obtained. There are scenarios in which a request is created, but approval is not required. Consider the following sample scenarios:

**Scenario 1:**

A request is created when the operation is bulk, but at the operational level, if the requester is determined to be the admin of the entity, then it is considered auto-approved.

**Scenario 2:**

If an SoD check is enabled, then the approval workflow has to be initiated always. This is because SoD check happens in the approval workflow only.

End users can submit request for entities such as application instances, entitlements, and roles published to home organization for self or others in the same organization. To submit requests for users in other organizations, you must be granted the User Viewer admin role (in each of the organizations to which the users belong), and the corresponding Application Instance Viewer, Entitlement Viewer, or Role Viewer roles.

## 9.5 Request Categories

There are two categories of request in Oracle Identity Manager:

- **Catalog-based requests:** This type of request focuses on granting access to users by using the access request catalog. A catalog-based request is a request created for entities such as roles, application instances, and entitlements. The following are the types of catalog-based requests:
  - **Role request:** This is a request for enterprise role, which in turn has one or more access policies associated with it.
  - **Application instance request:** This is a request for accounts in target applications. An application instance represents an account in a target application, typically known as an IT resource instance in Oracle Identity Manager. Requesting for and provisioning an application instance means that an account has been created for you in the target application.
  - **Entitlement request:** This is a request for additional access in target applications. For example, for an E-Business Suite account, you can request for entitlements such as CRM administrator or payroll supervisor. When a user requests for entitlements, the entitlements are appended to the primary account. See ["Requesting for an Account"](#) on page 11-38 for information about primary and non-primary accounts.

By default, the catalog is categorized by the type of entity. You can modify catalog items and specify your own category. See ["Using the Access Request Catalog"](#) on page 8-1 for more information on viewing and modifying catalog items.

You create catalog-based requests by adding request items to a request cart. The request cart can contain items of the same or different entity types.

After you add the request items to the cart, you proceed to checkout where you select the target users and then submit the request. The users that you can select (in other words, beneficiaries of the request) depends on the User Viewer admin role that you have across organizations.

Some application instances have forms associated with them for which you have to provide additional information. You cannot submit such application instance requests without completing the form.

Oracle Identity Manager provides a set of predefined request types. [Table 9 2](#) lists the operations and request types that Oracle Identity Manager supports by default for catalog-based requests.

**Table 9 2 Default Operations and Request Types for Catalog-Based Requests**

Catalog Entity	Request Types	Bulk	Beneficiary
Application Instance	Provision Application Instance	Y	Y
Entitlement	Provision Entitlement	Y	Y
Role	Assign Roles	Y	Y

- Non-catalog-based requests:** This type of request is created without using the request catalog. Examples of non-catalog-based requests include self registration, create user, modify user, modify account, revoke account, enable or disable an account, enable or disable users, and bulk modification of users.

Oracle Identity Manager provides a set of predefined request types. [Table 9 3](#) lists the operations and request models that Oracle Identity Manager supports by default for non-catalog-based requests.

**Table 9 3 Default Operations and Request Types for Non-Catalog-Based Requests**

Category	Request Type	Bulk	Beneficiary
User Management	Create User	N	N
	Self-Register User	N	N
	Modify User Profile	Y	N
	Enable User	Y	N
	Disable User	Y	N
	Delete User	Y	N
Provisioning	Modify Account	Y	Y
	Enable Account	Y	Y
	Disable Account	Y	Y
	Revoke Account	Y	Y
Role Management	Create Role	N	N
	Delete Role	Y	N
	Modify Role	Y	N
	Assign Roles	Y	Y
	Remove from Roles	Y	Y

---

---

**Note:** The following request types are deprecated in the current release:

- Request types related to "Self"
- Request types related to "Resource"

No new requests can be created based on these deprecated request types.

---

---

## 9.6 Common Reasons for Request Failure

When the associated operations specified in a request fail to execute, the request cancels any pending operations and moves the request to the Request Failed stage. Clicking the Request Failed hyperlink displays the reason for request failure.

A request can fail for any one of the following reasons:

- If you are requesting a role, then your request can fail due to an SoD violation.
- If you are requesting an application instance and that application instance depends on another application instance, then the request moves to 'Request Approved Fulfillment Pending' status because the parent application instance is not provisioned. For example, to successfully provision a user to a Microsoft Exchange account, the user must have a Microsoft Active Directory account in the domain controller that is managing the users of the Exchange server.
- When you request for an entitlement, the entitlement is provisioned to the primary account. Therefore, if you are requesting an entitlement, but you do not have a primary account provisioned to you, the entitlement request fails.

In addition to the preceding reasons, failures can occur because of incorrect password, password policy violation, target system being unavailable, and so on.

## 9.7 Request Profiles

When you select catalog items for requesting, the items are added to a request cart. The request cart is similar to the shopping cart in Web sites that sell products to customers. You can view the selected items in the cart, or edit the request cart to add or remove items.

Request profiles are request carts that are saved for future reuse by the users. The request cart is saved by the catalog administrator or system administrator so that the user can use it to request for entities without searching through thousands of catalog items.

---

---

**Note:** When a user creates a request through request profile, the items are filtered based on authorization policies. This means that the items for which the user does not have the required privileges to request, are automatically removed from the cart. If the user is not authorized to request any item in the profile, then the cart items will be empty.

---

---

This section discusses the following topics:

- [Creating a Request Profile](#)
- [Modifying a Request Profile](#)

- [Deleting a Request Profile](#)

---

---

**Note:** Creating, modifying, or deleting a request profile can be performed only by catalog administrators or system administrators.

---

---

## 9.7.1 Creating a Request Profile

To create a request profile:

1. In the Catalog page, select one or more catalog items, and click **Add to Cart**. The catalog items are added to the request cart.
2. Click **Checkout**. The Cart Details page is displayed. The select catalog items are displayed in the Cart Items section.
3. Click **Save As Profile**. The Request Cart dialog box is displayed with the catalog items in the request profile.
4. In the Save Profile Name field, enter a name for the request profile.
5. In the Description field, enter a description of the request profile.
6. Click **Save**. The request profile is created.

## 9.7.2 Modifying a Request Profile

To modify a request profile:

1. In the Request Profiles section of the Catalog page, click the request profile that you want to modify. The Cart details page is displayed.
2. In the Cart Items section, select a cart item to display the details of the item.
3. In the Details section, modify the request details, if required. To do so, set or modify values in the Details section, and then click **Ready to Submit**.
4. If you want to add more items to the cart, then:
  - a. Click **Back to Catalog**.
  - b. On the Catalog page, search for and select items to be added to the cart, and then click **Add to Cart**.
5. Click **Checkout**. The Cart Details page is displayed.
6. Click **Save As Profile**. The Save as Profile dialog box is displayed.
7. In the Save Profile Name field, enter the name for the request profile that is being modified. If you enter a new name, then a new request profile is created. If you enter the name of an existing request profile, then that request profile is updated with the latest changes.
8. In the Description field, enter a description of the request profile.
9. Click **Save**. Depending on whether you have entered the name of an existing request profile or new name, the request profile is created or updated, respectively.

---

---

**Note:** Values that you add or specify for Target Users, Justification, or Effective Date will not saved in a request profile.

---

---

### 9.7.3 Deleting a Request Profile

To delete a request profile:

1. In the Request Profiles section of the Catalog page, click the red cross mark preceding the name of the request profile.
2. In the Confirmation dialog box that is displayed, click **Yes**.

The request profile is deleted.

## 9.8 Creating Requests

This section describes how to create requests in the following topics:

- [Creating a Request to Register Yourself in Oracle Identity Manager](#)
- [Creating a Request By Using the Request Catalog](#)
- [Creating a Request By Using a Request Profile](#)

### 9.8.1 Creating a Request to Register Yourself in Oracle Identity Manager

Using the login page of Identity Self Service, you can create a request to register yourself in Oracle Identity Manager. This is called a self-registration request and can be raised by users not present in Oracle Identity Manager (anonymous users). To create a self-registration request, see "[Submitting Registration Requests](#)" on page 3-1. After submitting the self-registration request, you can track it by navigating to the login page, and clicking **Track My Registration**.

### 9.8.2 Creating a Request By Using the Request Catalog

---

---

**Note:** The procedure discussed in this section is applicable for requesting roles, entitlements, and application instances.

---

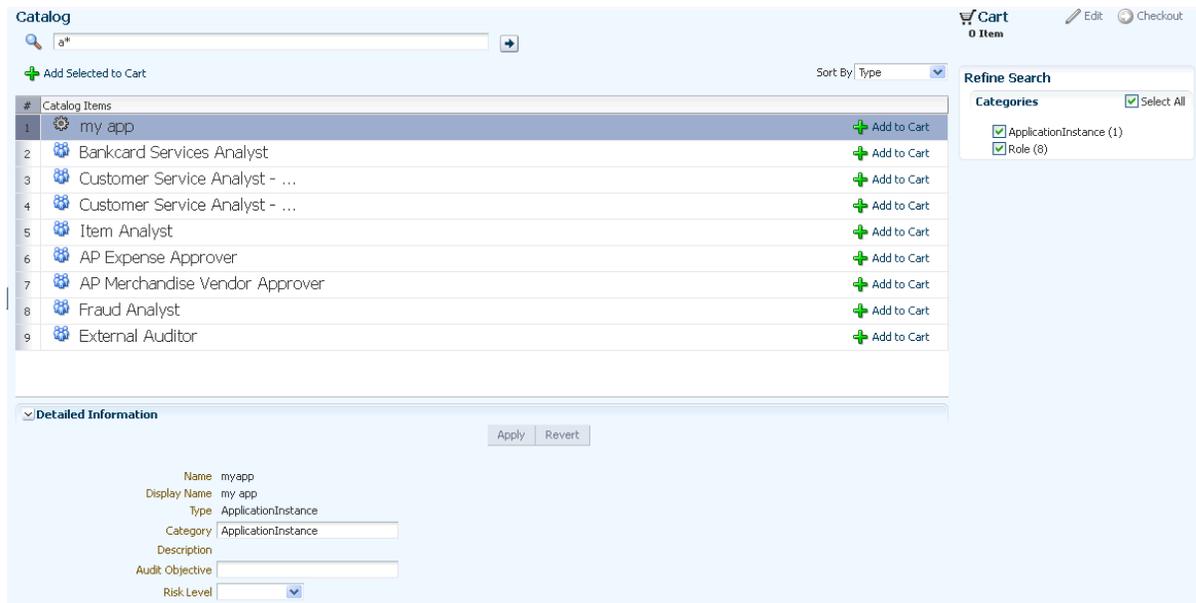
---

In Identity Self Service, you can create requests from various pages, such as the Home page, My Access page, and the entity detail pages for users and roles. Irrespective of the page or tab from where you are creating the request, you go through the request catalog to create requests.

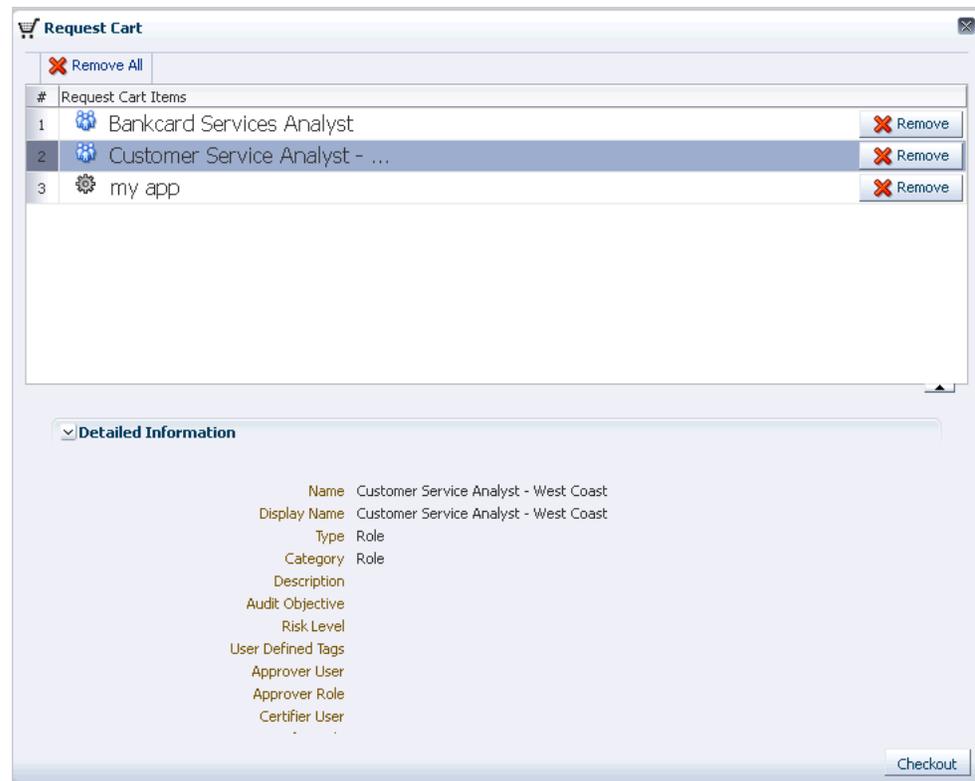
To create a request by using the request catalog:

1. Log in to Identity Self Service.
2. Under Requests, click **Catalog**. The Catalog page is displayed.
3. Search for the item that you want to request. To do so, enter a keyword in the search field, and click the search icon on the right. The search results are displayed. The catalog items that match the search condition are listed in the Catalog Items section, as shown in [Figure 9 4](#):

**Figure 9 4 The Catalog Page**



4. In the Refine Search section, select one or more categories to display the catalog items of those categories. You can click **Select All** to display or hide all the items belonging to the categories.
5. Select a catalog item that you want to request. The summary information of the item is displayed below the Catalog Items section.  
You can also select multiple items by pressing **Ctrl** and clicking the items.
6. Click **Add Selected to Cart**.  
The selected items are added to the request cart.
7. Optionally, click **Edit** to view the catalog items added to the cart. The Request Cart dialog box is displayed with a list of catalog items in the cart, as shown in [Figure 9 5](#):

**Figure 9 5 The Request Cart**

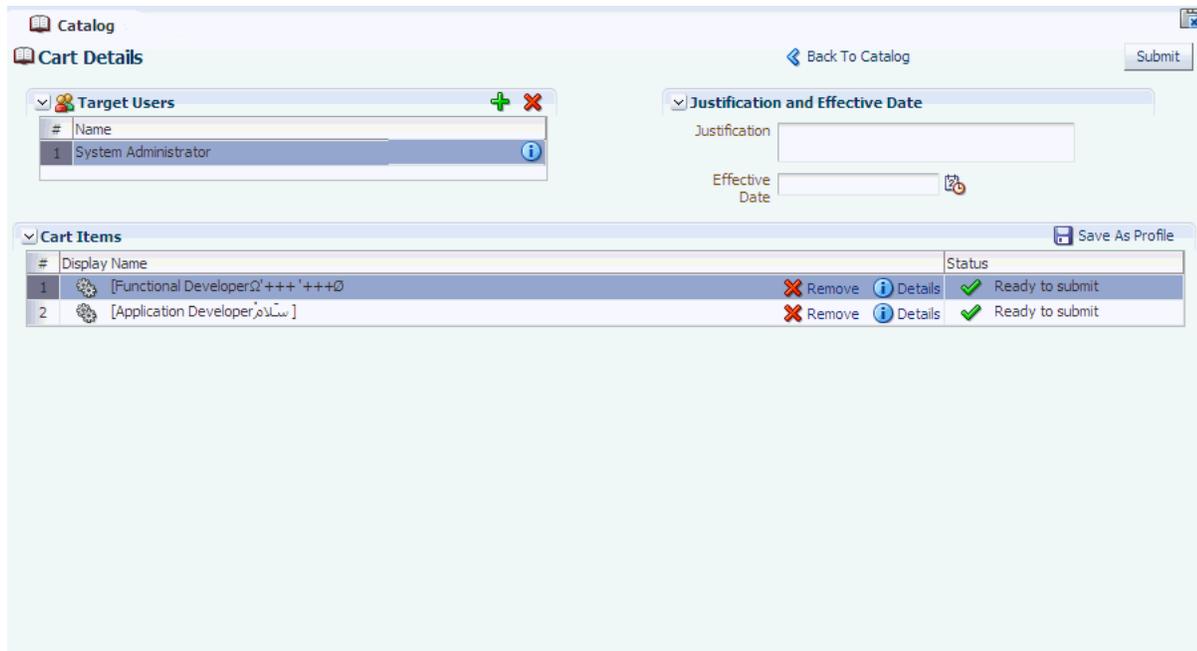
8. If required, select a catalog item to display detailed information about the item. Review the details, and if required, you can remove the item from the cart by clicking **Remove** for the corresponding item.

Alternatively, click Remove All to delete all items from the cart.

9. Click **Checkout**. Alternatively, you can click **Checkout** on the Catalog page.

The Cart Details page is displayed, as shown in [Figure 9 6](#):

Figure 9 6 The Cart Details Page



10. The Target Users section displays the usernames of beneficiaries for the request. You can click user details icon for a user to view the details of the user.
11. To add beneficiaries to the request:
  - a. Click the green plus symbol. The Advanced Search for Target Users dialog box is displayed.
  - b. Search and select one or more users that you want to add.
  - c. Click **Add Selected** to add the selected users to the Selected Users list. Alternatively, click **Add All** to add all the users in the Selected Users list.
  - d. Click **Add**. The selected users or beneficiaries are added to the Target Users section of the Request Cart Details page.
- You can also select a user that you want to remove from the list of beneficiaries, and click **Remove**.
12. If required, in the Justification and Effective Date section, in the respective fields, specify a justification and effective date when the request will be active.
13. In the Cart Items section, if required, select a cart item and click **Details** to display the details of the item.
14. After reviewing and modifying the details or each item in the cart, click **Submit**.

The request is submitted for approval, and the Request Summary page is displayed with summary information, target user or beneficiary information, and request and approval details. Figure 9 7 shows the Request Summary page:

Figure 9-7 The Request Summary Page

**Request Summary : 3** Withdraw Request

**Summary Information**

Request Id 3  
 Requested Date 2/21/2012  
 Effective Date  
 Justification

Requester XELSYSADM  
 Status Obtaining Request Approval  
 Parent Request ID  
 Request Type Provision Entitlement

**Request Details** Approval Details

**Target Users**

User Login	Email
XELSYSADM	donotreply@orad...

**Related Requests**

Beneficiary	Request Id	Requested Item
No data to display.		

**Cart Items**

#	Display Name	Details
1	[Functional DevelopersΩ+++ '+++⓪	Details
2	[Application Developerسلام ]	Details

---

**Note:** In the Request Summary page, if you want to withdraw the request, then click **Withdraw Request**, and click **Yes** to confirm. To withdraw requests from other pages in Identity Self Service, see "[Withdrawing a Request](#)" on page 9-21.

---

### 9.8.3 Creating a Request By Using a Request Profile

To create a request by using the request profile:

1. In Identity Self Service, under Requests, click **Catalog**. The Catalog page is displayed with the request profiles created for you.
2. Click the request profile name that you want to use to create the request. The Cart Details page is displayed.
3. The Target Users section displays the usernames of beneficiaries for the request. You can click information icon against each user to view the details.
4. To add beneficiaries to the request:
  - a. Click the Add icon. The Advanced Search for Target Users dialog box is displayed.
  - b. Search and select one or more users that you want to add.
  - c. Click **Add Selected** to add the selected users to the Selected Users list. Alternatively, click **Add All** to add all the users in the Selected Users list.
  - d. Click **Add**. The selected users or beneficiaries are added to the Users section of the Request Cart Details page.

You can also select a user that you want to remove from the list of beneficiaries, and click the Remove icon.

5. If required, in the Justification and Effective Date section, in the respective fields, specify a justification and effective date when the request will be active.

6. In the Cart Items section, select a cart item to display the details of the item.
7. After reviewing and modifying the details of each request in the cart, click **Submit**.

The request is submitted for approval, and the Request Summary page is displayed with summary information, target user or beneficiary information, and request and approval details.

## 9.9 Tracking a Request

To track a request:

1. In Identity Self Service, under Requests, click **Track Requests**. The Track Requests page is displayed.
2. Search for the requests you want to track. To do so:
  - a. Select any one of the following:

**All:** On selecting this option, the search is performed with the AND condition. This means that the search operation returns requests that match all the search criteria that is specified.

**Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation returns requests that match the search criterion that is specified.

- b. In the searchable request attribute fields, such as Request ID, specify a value. You can include wildcard characters (\*) in the attribute value.

For some attributes, select the attribute value from the lookup. For example, to search all requests with the Obtaining Operation Approval status, from the Status list, select the **Equals** search operator, and the select **Obtaining Operation Approval** from the adjacent list.

- c. For each attribute value that you specify, select a search operator from the list. For example, the following search operators are available for Request ID:

Starts with

Ends with

Equals

Does not equal

Contains

Does not contain

For other fields, for example Status or Request Type, only Equals and Does not equal operators are available.

For fields of date type, the search operators are:

Equals

Does not equal

Before

After

On or before

On or after

- d. To add a searchable request attribute to the Track Requests page, click **Add Fields**, and select the attribute from the list of attributes.  
For example, if you want to track all requests by a requester, then you can add the Requester attribute as a searchable field and specify a search condition.
  - e. Optionally, click **Reset** to reset the search conditions that you specified. Typically, you perform this step to remove the specified search conditions and specify a new search condition.
  - f. Click **Search**. The search results is displayed in a tabular format.
3. If the request search you performed displays a large number of records, then you can filter the request search result. To do so:
    - a. From the Show list, select any of the following:
      - Requests Raised By Me:** This is selected by default. Returns requests created by logged-in user.
      - Requests Raised For Me:** Returns requests where login user exists as beneficiary or target user.
      - For Reportee:** This option is available if the logged-in user is a manager of a user.
      - For User:** This option is available if the logged-in user has been granted the User Administrator or the HelpDesk admin role.
      - All:** Returns all requests in the search result. This option is available if the logged-in user has been granted the System Administrator role.
    - b. To sort the requests in the search result by any of the columns such as Request ID or Status, click the **Sort Ascending** or **Sort Descending** arrows in the column. The requests in the search result are sorted by the selected column.
  4. In the request search result, click a request to view the details of the request. The details of the request is shown in a page with the following information:
    - Summary information: This section shows general request details, such as request ID, request status, and effective date.
    - Target Users: This section lists the beneficiaries or target users for the request.
    - Related Requests: This section lists requests that are related to the open request, if any.
    - Request Details: This tab lists the requested catalog items. You can select an item to display a summary information of the item.
    - Approval Details: This tab displays the status of request approval by each approver to whom the request has been assigned.

## 9.10 Withdrawing a Request

A request can be withdrawn by the requester and only the requests that have not started the execution phase can be withdrawn. Also, beneficiaries cannot withdraw requests. Requests having the following stages can be withdrawn:

- Obtaining Approval
- Approved

---

---

**Note:** Approved requests cannot be closed unless the request has the Request Awaiting Completion status.

---

---

To withdraw a request:

1. In Identity Self Service, under Requests, click **Track Requests**. The Track Requests page is displayed.
2. Search for the requests that you want to withdraw. The search results display a list of requests that match your search criteria with a Withdraw Request button for each request.
3. For a request that you want to withdraw, click **Withdraw Request**. Alternatively, you can open the details of a request by clicking the request ID, and subsequently clicking **Withdraw Request** on the request details page.
4. Click **Yes** in the confirmation message box. The request is withdrawn and a notification is sent to the beneficiary and requester of the request. If the withdrawal is successful, then request moves to the Request Withdrawn stage. Any pending approval tasks associated with the request are canceled.

---

---

**Note:**

- Configuration of notification can be done in the human task of a SOA composite.
  - For more information about request-related tasks, such as approving a request, reassigning a task, and rejecting a task, see "[Managing Tasks](#)" on page 10-1.
- 
- 

## 9.11 Closing a Request

Administrators can prematurely close any request that has not started the execution phase. This includes all requests waiting for approvals or has completed approvals but no operation has been started. Requests with the following state can be closed:

- Obtaining Approval
- Approved

---

---

**Note:**

- Approved requests cannot be closed unless the request has the Request Awaiting Completion status.
  - If a request is closed while the request is in the Obtaining Approval stage, then all the approvals that are still pending in the approver task list are removed.
- 
- 

To close a request:

1. In Identity Self Service, under Requests, click **Track Requests**. The Track Request page is displayed.
2. Search for the requests that you want to close. The requests that match the search condition are displayed in a tabular format.
3. Select the request that you want to close.

4. From the Actions menu, select **Close Request**. Alternatively, you can click the **Close Request** icon on the toolbar.
5. Click **Yes** in the confirmation message box. The request is closed and a notification is sent to the requestor and target user of this request. When a request is closed successfully, the request moves to the Request Closed stage.

---

---

**Note:**

- Configuration of notification can be done in the human task of a SOA composite.
  - For more information about request-related tasks, such as approving a request, reassigning a task, and rejecting a task, see "[Managing Tasks](#)" on page 10-1.
- 
-



---

---

## Managing Tasks

In Oracle Identity Self Service, you can view task instances of specific types. These types are associated with specific Oracle Identity Manager components. The task types are approval, certification, provisioning, and attestation tasks.

The approval tasks can be viewed and managed from the Inbox section of Identity Self Service. These tasks are instantiated by request service and correspond to associated requests that are in the user or administrator's queue to be approved.

The certification review tasks can be viewed and managed from the Inbox section of Identity Self Service. These tasks correspond to the certification process in the reviewer's queue.

The provisioning tasks can be viewed and managed from the Open Tasks section of Identity Self Service. These tasks correspond to tasks instantiated by requests, or pending manual provisioning tasks, or failed automatic provisioning tasks in the user or administrator's queue.

The attestation tasks can be viewed and managed from the Pending Attestations section of Identity Self Service. These tasks correspond to outstanding attestation process in the user or administrator's queue.

---

---

**Note:** The attestation feature has been deprecated in Oracle Identity Manager 11g Release 2 (11.1.2.1.0). However, this feature is available if you upgrade from Oracle Identity Manager Release 9.x or 11g Release 1 (11.1.1) or 11g Release 2 (11.1.2).

---

---

The approval, provisioning, and attestation tasks can be used by both administrators and end-users. For example, an IT department personnel responsible for delivering a laptop to an employee may not be an Oracle Identity Manager administrator, but needs to view and change provisioning tasks.

This chapter contains the following topics:

- [Using the Unified Inbox](#)
- [Managing Approval Tasks](#)
- [Managing Certification Review Tasks](#)
- [Managing Provisioning Tasks](#)
- [Managing Attestation Tasks](#)

## 10.1 Using the Unified Inbox

The Inbox lists all the approval and certification-review tasks assigned to the logged-in user in a single screen. It enables the logged-in user to filter task views into user preferences, such as assigned tasks, completed tasks, and tasks for which information has been requested. The user can select a task to open it in a new tab and then perform necessary actions on the task. This allows you to work on multiple tasks at a time by opening them in different tabs. To access the Inbox, login to Oracle Identity Self Service, and click **Inbox** on the left navigation pane.

The Inbox also allows the user to search tasks, organize them in views, and create shared views. The Worklist Views section of the Inbox lists the available views. You can click a view to display its contents, which are filtered representations of tasks that match the view definition.

Managing views is described in the following sections:

- [Creating a View Definition](#)
- [Editing User Preferences](#)
- [Deleting a View](#)
- [Editing the Task Chart](#)

### 10.1.1 Creating a View Definition

To create a view definition in the Inbox:

1. In the Worklist Views section of the Inbox, click the **Add View** icon (plus icon). The Create User View dialog box is displayed.
2. Select any one of the following options:
  - **Create View:** Select to create a new view. Enter a name of the view in the Name field.
  - **Use Public View:** Select to create a view based on an already existing view that is publicly available to users. On selecting this option, a lookup icon is displayed adjacent to the Name field. Click the lookup icon to open the Select Public View dialog box, select a view based on which you want to create the new view, and click **OK**.

---

---

**Note:** If you log in as a domain admin user, then you can create the view as public so that all users can see the view. When you create a public view, it is displayed under the Standard Views section. For more information, refer to SOA documentation.

---

---

3. In the Assignee, Task Type, and Add Condition fields, specify a search condition based on which certifications will be displayed in the view. See "[Searching Certifications in the Inbox](#)" on page 10-12 for information about specifying a search condition.
4. In the Share View section, select any one of the following:
  - Definition only:** Select this option to share the view definition with other users and groups.
  - Data:** Select this option to share the data or search result in your view.

5. Click the lookup icon adjacent to the Users and Groups fields to select users and groups respectively with whom you want to share the view.
6. Click **OK**. The view is added in the My Views list of the Worklist Views section.

## 10.1.2 Editing User Preferences

You can modify the columns in the Inbox that lists the certification tasks assigned to you or for which you are the reviewer. To edit the way columns are displayed or hidden in the Inbox:

1. In the Worklist Views section of the Inbox, click the **Edit User Preferences** icon. The Edit User Preferences dialog box is displayed.

**Tip:** If the Worklist Views section is not displayed by default, then click the arrow next to Worklist Views to expand the Worklist View. To collapse the Worklist Views, you can click the arrow again.

2. In the Available Columns list, select the columns that you want to display. You can hold the Ctrl key and select multiple columns.
3. Click the **Move selected items to other list** button to move the selected columns to the Selected Columns list. To move all the columns in the Available Columns list to the Selected Columns list, you can click the **Move all items to other list** button.
4. To remove columns from the Selected Columns list, select the columns by holding the Ctrl key, and click the **Remove selected items from list** button.

---

---

**Note:** You cannot remove the Title column from the Selected Columns list. The title column is always displayed as the first column in the Inbox.

---

---

5. Click the up and down arrow key to the right of the Selected Columns list to move the columns up or down the order.
6. From the Sort By Column list, select a column name based on which you want the certification data to be sorted. For example, if you select Priority from this list, then the certification tasks in the Inbox will be sorted based on the priority.
7. Select the Sort Order as Ascending or Descending.
8. From the Number of tasks per fetch list, select the number of certification tasks that you want to display in the Inbox at a time.
9. For User language setting of, select Browser or Identity Provider to select the language settings of the web browser or Identity provider respectively.
10. Click **OK**. The certification tasks are listed according to the options you selected in the Edit User Preferences dialog box.

## 10.1.3 Deleting a View

To delete a view in the Inbox:

1. In the Worklist Views section of the Inbox, select a view that you want to delete.
2. Click the **Delete View** icon (cross icon). A message is displayed asking for confirmation.
3. Click **Yes** to confirm.

### 10.1.4 Editing the Task Chart

To show or hide the task status information in the Inbox:

1. In the Task Status section of the Inbox, click the **Edit Task Chart** icon. The Chart Display States dialog box is displayed.

**Tip:** If the Task Status section is not displayed by default, then click the arrow next to Task Status to expand the Task Status. To collapse the Task Status, you can click the arrow again.

2. Select the task status options that you want to display in the Task Status section of the Inbox. To hide the task status, deselect the task status options.
3. Click **OK**.

## 10.2 Managing Approval Tasks

Oracle Identity Manager request service interacts with SOA Server to handle various aspects of human interaction in Oracle Identity Manager workflows. This request service is used to assign tasks to roles and users. You can perform various operations upon tasks assigned to you. For example, you can approve, reject, or claim a task, or request for more information. The process flow in corresponding Oracle Identity Manager workflow is dependent on the outcome of given tasks.

**See Also:** "Developing Workflows for Approval and Manual Provisioning" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about approval workflows

When a request is submitted, the request service initiates the approval as a task in Oracle SOA Server. This task is assigned to the approver. Further processing of this request by request service remains pending, which is subject to the outcome of the corresponding task. The approver must be able to access the Inbox section that lists all the tasks assigned to the approver. The approver can now act upon this task and set its outcome, for example, approve or reject. After the task outcome has been set, the request service resumes the processing of the request that is based on the task outcome.

On successful submission of requests, the request service creates Human Tasks in SOA and assigns them to users or roles in Oracle Identity Manager. Authenticated users can view the tasks waiting for action in the Inbox section.

This section describes some of the task actions you can perform in the Inbox section:

- [Viewing Approval Tasks](#)
- [Searching Tasks](#)
- [Viewing Task Details](#)
- [Approving a Task](#)
- [Rejecting a Task](#)
- [Reassigning a Task](#)
- [Suspending a Task](#)
- [Withdrawing a Task](#)

---



---

**Note:** The features related to performing task actions in the Inbox section are provided by Oracle SOA. For detailed information about the task actions, see *Oracle Fusion Middleware Developer's Guide for Oracle SOA Suite*.

---



---

## 10.2.1 Viewing Approval Tasks

To view for approval details:

1. Log in to Identity Self Service.
2. In the left pane, click **Inbox**.

The Worklist Views page is displayed. By default, all types of tasks are displayed in an unified inbox view.

The Worklist Views page displays the details of your tasks in columns described in [Table 10 1](#):

**Table 10 1 Columns in the Approval Details Page**

Column	Description
Title	The title of the task.
Number	The number of the task.
Priority	The priority of the task.
Assignees	The user to whom the task is assigned.
State	The state in which the task is in, such as Assigned or Completed.
Created	The time stamp of the task when it was created.
Expires	The time stamp of the task when it expires.

3. From the Worklist Views menu, expand **My Work Queues**, if not already expanded.
4. From the My Work Queues menu, you can select any one of the following views:
  - **Due Soon:** Displays all tasks that are due in a few days.
  - **High Priority:** Display all tasks with high priority.
  - **Past Day:** Displays all tasks assigned in the previous day.
  - **Past Week:** Displays all tasks assigned in the previous week.
  - **Past Month:** Displays all tasks assigned in the previous month.
  - **Past Quarter:** Displays all tasks assigned in the previous quarter.
  - **Manual Provisioning:** Displays all tasks created for manual provisioning.
  - **New Tasks:** Displays all new tasks that have been created.
  - **Pending Approvals:** Displays all tasks that are pending approvals.
  - **Pending Certifications:** Displays all tasks that are pending certifications.
5. From the Assignee list, select any of the following:
  - **Me:** Displays all tasks assigned to you.
  - **My Group:** Displays all tasks assigned to the role you have.

- **Me & My Group:** Displays all tasks assigned to you and the role you have.
  - **Me & My Group All:** Displays all tasks assigned to you and all the roles you have.
  - **Me (Previously):** Displays all tasks that were previously assigned to you, but are not assigned to you now.
  - **Me (Review Only):** Displays all tasks that are assigned to you for review.
6. From the State list, select any one of the following:
- **Any:** Displays all tasks in your queue irrespective of the state.
  - **Assigned:** Displays all tasks that are currently assigned to you.
  - **Completed:** Displays all tasks in your queue that have been completed.
  - **Suspended:** Displays all tasks in your queue that have been suspended.
  - **Withdrawn:** Displays all tasks in your queue that have been withdrawn.
  - **Expired:** Displays all tasks in your queue that have expired.
  - **Errored:** Displays all tasks in your queue that generated an error.
  - **Alerted:** Displays all tasks in your queue for which the assignees have been alerted.
  - **Information Requested:** Displays all tasks in your queue for which information has been requested.

You can select appropriate options from the My Work Queues menu, the Assignee list, and the State list to display a list of task shown as a combination of your selection.

## 10.2.2 Searching Tasks

In the Approval Details page, you can perform the following search operations:

- [Performing Simple Search for Tasks](#)
- [Performing Advanced Search for Tasks](#)

### 10.2.2.1 Performing Simple Search for Tasks

To perform simple search for tasks:

1. In the left pane, click **Inbox**.
2. In the Search field of any tab, enter a search criterion. For example, if you enter `request` in the Search field, all tasks with the word 'request' in the task title are displayed.

---

---

**Note:** The simple search does not support wildcard characters.

---

---

3. Click the icon next to the Search field. The tasks that match the search criterion you specified are displayed.

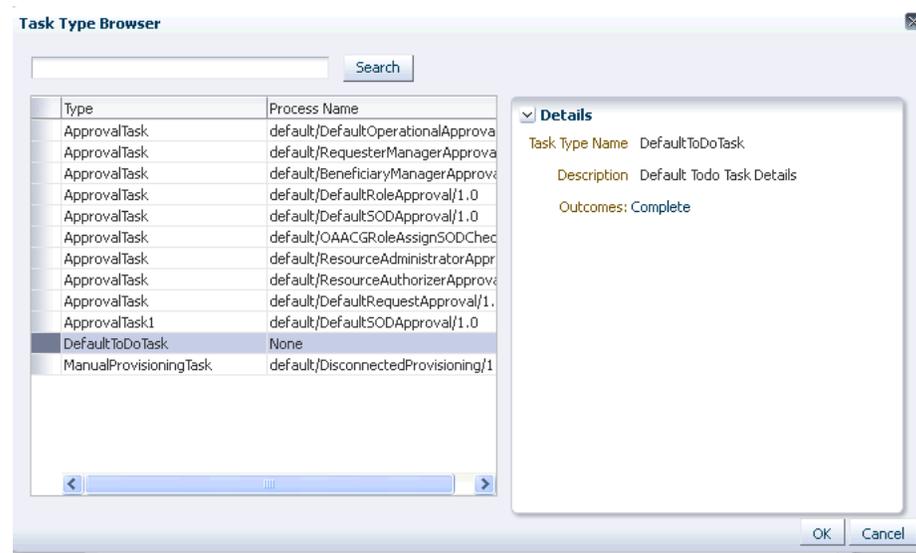
### 10.2.2.2 Performing Advanced Search for Tasks

To perform advanced search for tasks:

1. Open the Inbox section.

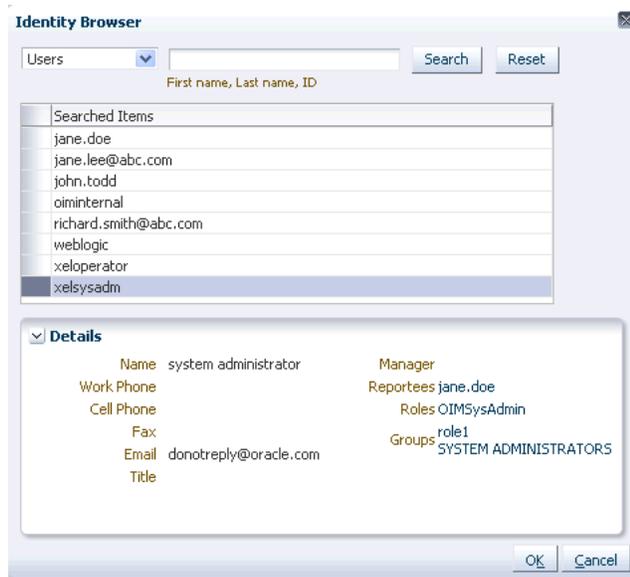
2. In any tab, click **Advanced**. The Advanced Search dialog box is displayed.
3. To specify a task type to search, click the lookup icon next to the Task Type field. The Task Type Browser dialog box is displayed.
4. Click **Search**. The available task types along with process names are displayed.
5. Select a task type. The details of the process type are displayed in the right panel, as shown in [Figure 10 1](#):

**Figure 10 1 The Task Type Browser Dialog Box**



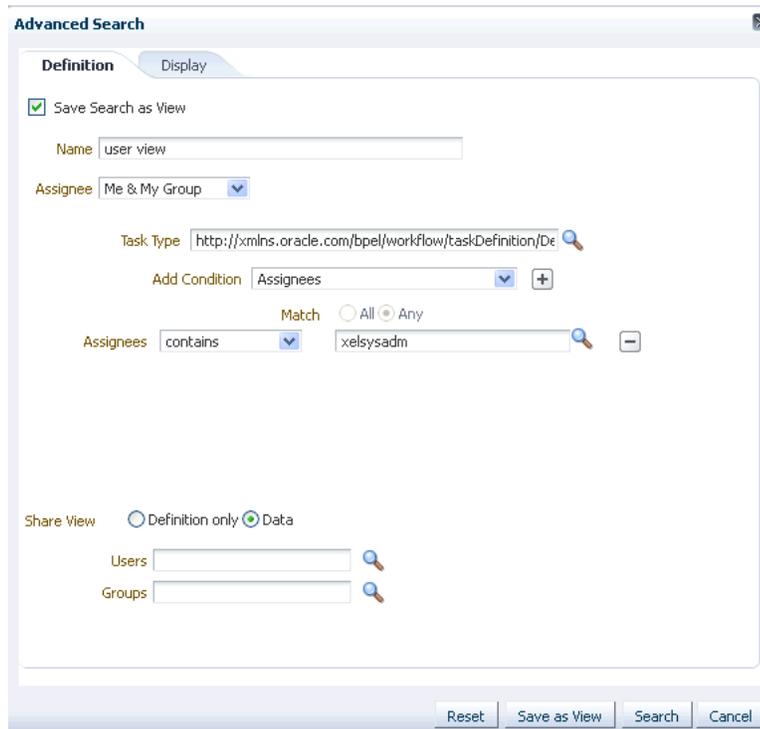
6. Click **OK**. The task type is added in the Task Type field.
7. From the Add Condition list, select a condition. For the purpose of this example, select **Assignees**.
8. To add more conditions, click the plus icon next to the Add Condition list. The Assignees field is added.
9. For the Assignees field, select a search operator, such as contains or does not contain.
10. To search and select an assignee, click the lookup icon next to the Assignees field. The Identity Browser dialog box is displayed.
11. From the list, select Users to display the users as assignees.
12. Specify a search condition, such as first name, last name, or user ID, in the field, and click **Search**. A list of users that match the search condition is displayed.
13. Select the user that you want to specify as assignee. The details of the user is displayed, as shown in [Figure 10 2](#):

**Figure 10 2 The Identity Browser**



14. Click **OK**. The selected user is added to the Assignee field in the Advanced Search dialog box.
15. If you want to save the search condition you specified as a view for future use, then perform the following:
  - a. Select the **Save Search as View** option. Some fields related to saved search are displayed, as shown in [Figure 10 3](#):

**Figure 10 3 The Advanced Search Dialog Box**



- b. Select any one of the following to share the view:
    - Definition only:** Shares the definition of the view without the data that is searched.
    - Data:** Shares the data as well as the definition of the saved search.
  - c. In the Users and Group fields, search and select users and groups with whom you want to share the saved search as a view.
  - d. Click **Save as View**. The search is saved as a view.
16. Click **Search**. The tasks that match the search condition you specified are displayed.

### 10.2.3 Viewing Task Details

When you click the request title link of any of the approval tasks in any of the tabs in the Inbox section, task details are shown for that approval task in a new tab.

The task details page displays a detailed view of the request in the Summary Information section, the Request Details tab, the Approvals tab, and the Cart Details section. It allows complete management of the listed task.

In the Cart Details section, the approver can provide data, without which (if the field is marked as mandatory) the approver will not be allowed to approve a request. For example, when an approver opens a task related to self-registration request, the organization field is marked as mandatory, but no value is specified for this field by the requester. Therefore, the approver must specify a value for this mandatory field.

In the next level of approval, the approver can modify the data, if required. Similarly, if the approver sends the task to another user for more information (using the Request Information operation), then the user to whom it is assigned can see an additional section called "Additional Request Information" in Task details and the user can send a response to the information requested.

In addition, the following tabs display details associated to the request:

- **Request Details:** This tab displays the target users or beneficiary information, and related requests, if any.
- **Approvals:** The complete approval flow with all approvers. You can select the **Future participants** option to display the next level approvers. You can select the **Full task actions** option to display all the approvals for the task.

The various operation that you can perform in the task details page are described in the subsequent sections.

### 10.2.4 Adding Comments and Attachments

After you view the task details, you can add comments and attachments prior to performing any operation on the task such as approving, rejecting, or reassigning the request. An attachment can either be a hyperlink or an actual file. It is recommended that the size of the file attachment that you upload be less than 2 MB. If you want to upload file attachments of size greater than 2 MB, then you must change the ADF configuration and increase the size limit. For more details, see *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.

To add comments and attachments:

1. Open the Inbox section.

2. On any tab, search for and select the task for which you want to add comments or attachments. The details of the task are displayed in a new tab.
3. To add a comment:
  - a. Click the Approvals tab.
  - b. Click the **Create Comment** icon. The Create Comment dialog box is displayed.
  - c. In the Comment field, enter the comments related to the task, and then click **OK**.
  - d. Click **Save** to save the comment.
4. To add an attachment:
  - a. Expand the Attachments section if it not already expanded.
  - b. Click the **Add Attachment** icon. The Add Attachment dialog box is displayed.
  - c. Select one of the following options as the attachment type:
    - URL:** Specify the URL to an attachment.
    - Desktop File:** Allows you to select and upload a file from the desktop.
  - d. Click **OK**.

### 10.2.5 Approving a Task

To approve a task that is assigned to you:

1. Open the Inbox section.
2. Search for and select the task that you want to approve.
3. Click the task to view its details in a new tab, and then click **Approve**.

The task is approved and is no longer displayed in the tasks table.

---

---

**Note:** A self-registration request is assigned to the System Administrator role by default. Before you can approve a self-registration request, as a member of the System Administrator role, you must claim a self-registration task, provide the organization name, and update the request before approval.

---

---

### 10.2.6 Rejecting a Task

To reject a request that is assigned to you:

1. Open the Inbox section.
2. Search for and select the task that you want to reject.
3. Click the task to view its details in a new tab and provide any comments. Then, click **Reject**. The task is rejected and is no longer displayed in the tasks table of the Approval Details page.

### 10.2.7 Reassigning a Task

To reassign a request that is assigned to you:

1. Open the Inbox section.
2. Search for and select the task that you want to reassign.

3. Click the task to view its details in a new tab. Then, from the Task Actions menu, select **Reassign**.  
The Reassign Task dialog box is displayed.
4. Select any one of the following options:
  - **Reassign (transfer task to another user or group):** To reassign the task to another user, group, or application role. On selecting this option, you can search and select users, groups, or application roles for reassigning.
  - **Delegate (allow specified user to act on my behalf):** To delegate the task to a user that you can search and select. The delegated user will take actions on the task on your behalf. The privileges of the delegatee are based on the delegator's privileges.
5. Search for user or groups to which you want to assign the task, and click the **Move selected items to other list** icon to include the selection in the Selected list.
6. Click **OK**. The task is assigned.

### 10.2.8 Suspending a Task

To suspend a task:

1. In the Approval Details page, search and select the request that you want to suspend.
2. Click the task to view its details in a new tab. Then, from the Task Actions menu, select **Suspend**.

A message is displayed stating that the task is successfully suspended.

### 10.2.9 Withdrawing a Task

To withdraw a task:

1. In the Approval Details page, search and select the request that you want to withdraw.
2. Click the task to view its details in a new tab. Then, from the Task Actions menu, select **Withdraw**.

A message is displayed stating that the task is successfully withdrawn.

## 10.3 Managing Certification Review Tasks

You can view and make decisions on certifications by using the Inbox. This section describes working with certifications in the Inbox in the following topics:

- [Searching and Viewing Certifications](#)
- [Completing Certifications](#)

---

---

**Note:** This section describes the actions you can perform in the Inbox. For an overview of identity certification and information about operations you can perform by using the Dashboard, see "[Chapter 15, "Using Identity Certification"](#)".

---

---

## 10.3.1 Searching and Viewing Certifications

This section describes how to search and filter certifications in the Inbox and Dashboard, and how to view the details of certifications in the following sections:

- [Searching Certifications in the Inbox](#)
- [Accessing Certification Tasks From the Inbox](#)

### 10.3.1.1 Searching Certifications in the Inbox

The Inbox enables you to perform simple search and advanced search based on search criteria that you specify.

To perform simple search for certifications:

1. Login to Oracle Identity Self Service.
2. On the left pane, click **Inbox**. The Inbox is displayed with a list of certification review tasks (and other approval tasks) assigned to you.
3. From the State list, select the certification status that you want to search for, for example, Assigned or Completed. Select Any to search for any certification irrespective of the status.
4. In the Search box, specify a search criterion, for example, the certification name.
5. Click the Search icon. The certifications that match your search criteria are listed in the search results table.

To perform advanced search for certifications:

1. Login to Oracle Identity Self Service.
2. On the left pane, click **Inbox**. The Inbox is displayed with a list of certification review tasks (and other approval tasks) assigned to you.
3. Click **Advanced** adjacent to the Search icon. The Advanced Search dialog box is displayed.
4. Click the lookup icon next to the Task Type field. The Task Type Browser is displayed.
5. Click **Search**. A list of available task types are displayed.
6. Select the task type that you want to specify as a search criteria. The details of the task type is displayed in the Details pane.
7. Click **OK**. The selected task type is populated in the Task Type field.
8. From the Add Condition list, select a field name, for example, Start Date.
9. Click the plus (+) icon. The fields to specify the search condition are displayed.
10. In the Start Date list, select a condition, such as on, equals, or greater than.
11. In the adjacent date field, specify a date based on which the search condition is formed.
12. (Optional) Select the **Save Search as View** option if you want to save the search criteria as a view in the Inbox. To save the search as a view:
  - a. In the Name field, enter a name for the view.
  - b. In the Share View section, select any one of the following:

**Definition only:** Select this option to share the view definition with other users and groups.

**Data:** Select this option to share the data or search result in your view.

- c. Click the lookup icon adjacent to the Users and Groups fields to select users and groups respectively with whom you want to share the view.
  - d. Click **Save as View**. The view is added in the My Views section in the list of worklist views.
13. After specifying the complete search criteria, click **Search**. The certifications that match your search criteria are listed in the search results table.

**Tip:** To sort the data in the search results table, place the mouse pointer on a column name. Up and down arrows are displayed on the column names. Click the up arrow to sort in ascending order. Click the down arrow to sort in descending order.

### 10.3.1.2 Accessing Certification Tasks From the Inbox

This section describes how to access certification tasks for each type of certification:

- [Viewing User Certification Details](#)
- [Viewing Role Certification Details](#)
- [Viewing Application Instance Certification Details](#)
- [Viewing Entitlement Certification Details](#)

---

**Note:** The pages that display certification details and the details for user access rights, role content and membership, account details for application instances and entitlements enable you to personalize the contents of the pages. For example, you can use saved search, show/hide columns, and sort the data in columns. These personalization features are similar in all pages in Oracle Identity Self Service. See [Chapter 5, "Personalizing Self Service"](#) for information about personalizing pages in Oracle Identity Self Service.

---

#### 10.3.1.2.1 Viewing User Certification Details

To view user certification details:

1. On the left pane of the Oracle Identity Self Service, click **Inbox**. The Inbox is displayed with a list of certification tasks assigned to you, and for which you are the primary reviewer or delegated reviewer.
2. Click a certification task name to open it in a new page. Page 1 or the user certification summary page of the certification task opens in a new page.
3. Review the following sections of the user details:
  - The user certification name and certification creation date appears at the top of the page. Clicking the information icon adjacent to the certification name displays a pop-up with detailed statistics of the current certification being reviewed.
  - In the table that lists the users, the user name is a hyperlink. Clicking this hyperlink opens the access details of the user.
  - The Detailed Information section consists of the following tabs:

**User Information:** This tab displays user attributes that are included in the certification snapshot during certification generation. The user name is a hyperlink. Click the user name to display the user details in a new tab.

**Risk Summary:** This tab identifies why a user's Risk Summary is High/Medium/Low based on various factors. The pie chart in this tab displays the overall breakdown of a user's risk. Click any area of the chart to open the detail screen of the user certification. To view the risk items in a tooltip, place your mouse pointer over the charts.

This tab also displays a graph that breaks down the risk levels based on the roles, accounts, and entitlements the user has, as well as their associated risk levels. Click any area of the graph to open the detail screen of the user certification. To view the risk items in a tooltip, place your mouse pointer over the graph.

**Action History:** This tab displays the various delegation paths available on the user details page, and a trail of the actions taken by the reviewers as well as by Oracle Identity Manager. Possible details displayed include all the actions that are available in the Actions menu, as well as proxy, escalate, and expire.

4. Review the following sections of the role details:

- The User Detail section displays the user attributes that are included in the certification snapshot during certification generation.
- The table lists the roles with Display Name, Action, and Risk Summary.
- The Detailed Information section consists of the following tabs:

**Catalog Information:** This tab displays the default catalog attributes that are included as part of the default snapshot creation. The Name and Owner fields are hyper-linked. Clicking these hyperlinks opens the role detail and user details pages in new tabs.

**Risk Summary:** This tab identifies why a role Risk Summary is High, Medium, or Low based on various factors, such as Item Risk, Last Certification Decision, and Provisioning Method. The Provisioning Method field is hyper-linked. Clicking this hyperlink opens the appropriate access policy or access request details in a new tab.

**Certification History:** This tab displays the various certification decisions made by reviewers in the past on the given line-item.

**Action History:** This tab displays the phase in which the reviewer made a given decision. Possible values include all the actions that are available in the Actions menu, as well as proxy, escalate, and expire..

5. Review the following sections of the account details:

- The account name and the application instance name are displayed in the table, along with the underlying entitlements associated to the account. Accounts and entitlements are indicated by different icons.
- The Detailed Information section consists of the following tabs:

**Catalog Information:** This tab displays the account details that are the default catalog attributes. These attributes must be included as part of the default snapshot creation. The Name and Certifier fields are hyper-linked. Clicking these hyperlinks opens the account detail and user details pages in new tabs.

**Risk Summary:** This tab identifies why an account Risk Summary is High, Medium, or Low based on various factors, such as Item Risk, Last Certification Decision, and Provisioning Method. The Provisioning

Method field is hyper-linked for an access request. Clicking this hyperlink opens the appropriate access policy or access request details in a new tab.

**Certification History:** This tab displays the various certification decisions made by reviewers in the past on the given line-item.

**Action History:** This tab displays the phase in which the reviewer made a given decision. Possible values include all the actions that are available in the Actions menu, as well as proxy, escalate, and expire..

6. Review the following sections of the entitlement details:

- The account name and the application instance name are displayed in the table, along with the underlying entitlements associated to the account. Accounts and entitlements are indicated by different icons.

- The Detailed Information section consists of the following tabs:

**Catalog Information:** This tab displays the entitlement details that are the default catalog attributes. These attributes must be included as part of the default snapshot creation. The Display Name and Certifier fields are hyper-linked. When you click the Display Name of the entitlement, the granular entitlement hierarchy, if it is being captured in the catalog for a given entitlement, is displayed in a new tab. Clicking the Certifier name opens the user details page in a new tabs.

**Risk Summary:** This tab identifies why an entitlement Risk Summary is High, Medium, or Low based on various factors, such as Item Risk, Last Certification Decision, and Provisioning Method. The Provisioning Method field is hyper-linked. Clicking this hyperlink opens the appropriate access policy or access request details in a new tab.

**Certification History:** This tab displays the various certification decisions made by reviewers in the past on the given line-item.

**Action History:** This tab displays the phase in which the reviewer made a given decision. Possible values include all the actions that are available in the Actions menu, as well as proxy, escalate, and expire..

7. To display the details of the access rights for the next user in the certification task, click **Next** at the top of the page. You can click **First**, **Previous**, **Next**, and **Last** buttons to navigate between the pages for the access rights of each user. You can click **Back to Summary** to go back to the user certification detail page.

**10.3.1.2.2 Viewing Role Certification Details** To view role certification details:

1. On the left pane of the Oracle Identity Self Service, click **Inbox**. The Inbox is displayed with a list of certification tasks assigned to you, and for which you are the primary reviewer or delegated reviewer.
2. Click a certification task name to open it in a new page. Page 1 or the role certification summary page of the certification task opens.
3. Review the following sections of the role certification details page:
  - The role certification name and certification creation date appears at the top of the page. Clicking the information icon adjacent to the certification name displays a pop-up with detailed statistics of the current certification being reviewed.
  - In the table that lists the roles, the user name is a hyperlink. Clicking this hyperlink opens the role details. The table also displays the Members and Policies columns.

- Select a role in the certification table. The Detailed Information section displays the following tabs:
  - **Catalog Information:** This tab displays all catalog attributes of the selected role. The Role Name and Certifier fields are hyperlinked. Clicking these hyperlinks opens the role details and user details in new tabs.
  - **Action History:** This tab displays the various delegation paths available on the role details page, and a trail of the actions taken by the reviewers as well as by Oracle Identity Manager. Possible actions include delegate, re-assign, escalate, or proxy.
- 4. In the certification table, click a role name to open the role detail. The role detail page consists of the following tabs:
  - **Members:** This tab lists the role membership of the open role. Select a row in the members table to display the Detailed Information section, which consists of the User Information, Risk Summary, Certification History, and Action History tabs.
  - **Policies:** This tab lists the policies associated with the open role. Select a row in the policies table to display the Detailed Information section, which consists of the Policy Information, Certification History, and Action History tabs.
- 5. In the Policies tab, expand a policy by clicking the icon adjacent to the policy. The entitlements associated with the policy are listed in the table. Select the entitlement to display the entitlement details in the Detailed Information section. The entitlement details are displayed in the Catalog Information, Certification History, and Action History tabs.
- 6. To display the role contents and role members for the next role in the certification task, click **Next** at the top of the page. You can click First, Previous, Next, and Last buttons to navigate between the pages for the role contents and role member details of each role. You can click **Back to Summary** to go back to the role certification detail page.

**10.3.1.2.3 Viewing Application Instance Certification Details** To view application instance certification details:

1. On the left pane of the Oracle Identity Self Service, click **Inbox**. The Inbox is displayed with a list of certification tasks assigned to you, and for which you are the primary reviewer or delegated reviewer.
2. Click a certification task name to open it in a new page. Page 1 or the application instance certification summary page of the certification task opens.
3. Review the following sections of the application instance certification details page:
  - The application instance certification name and certification creation date appears at the top of the page. Clicking the information icon adjacent to the certification name displays a pop-up with detailed statistics of the current certification being reviewed.
  - In the table that lists the application instances, the application instance name is a hyperlink. Clicking this hyperlink lists the accounts belonging to the selected application instance.
  - Select an application instance in the certification table. The Detailed Information section displays the following tabs:

**Catalog Information:** This tab displays all catalog attributes of the selected application instance. The Certifier field is hyperlinked. Clicking this hyperlink opens the user details in a new tab.

**Action History:** This tab displays the various delegation paths available on the application instance details page, and a trail of the actions taken by the reviewers as well as by Oracle Identity Manager. Possible values include all the actions that are available in the Actions menu, and delegate, re-assign, escalate, or proxy.

4. In the certification table, click an application instance name to open the application instance detail. This page lists the application instance names and account names along with the underlying entitlements associated to the account.
5. Click an account to display the account details in the Detailed Information section. This section displays the account details in the Catalog Information, Risk Summary, Certification History, and Action History tabs.
6. Click an entitlement to display the entitlement details in the Detailed Information section. This section displays the entitlement details in the Catalog Information, Risk Summary, Certification History, and Action History tabs.
7. To display the set of users who have accounts for the next the application instance in the certification task, click **Next** at the top of the page. You can click First, Previous, Next, and Last buttons to navigate between the pages for the account details of each application instance. You can click **Back to Summary** to go back to the application instance certification detail page.

**10.3.1.2.4 Viewing Entitlement Certification Details** To view entitlement certification details:

1. On the left pane of the Oracle Identity Self Service, click **Inbox**. The Inbox is displayed with a list of certification tasks assigned to you, and for which you are the primary reviewer or delegated reviewer.
2. Click a certification task name to open it in a new page. Page 1 or the entitlement certification detail page of the certification task opens.
3. Review the following sections of the entitlement certification details page:
  - The entitlement certification name and certification creation date appears at the top of the page. Clicking the information icon adjacent to the certification name displays a pop-up with detailed statistics of the current certification being reviewed.
  - In the table that lists the entitlements, the entitlement name is a hyperlink. Clicking this hyperlink displays the entitlement assignment details of the selected entitlement.
  - Select an entitlement in the certification table. The Detailed Information section displays the following tabs:

**Catalog Information:** This tab displays all catalog attributes of the selected application instance. The Display Name and Certifier fields are hyperlinked. Clicking these hyperlinks opens the entitlement details and user details in new tabs.

**Action History:** This tab displays the various delegation paths available on the entitlement details page, and a trail of the actions taken by the reviewers as well as by Oracle Identity Manager. Possible values include all the actions in the Actions menu, and delegate, re-assign, escalate, or proxy.

4. In the certification table, click an entitlement name to open the entitlement assignment detail. This page lists the account names of the selected entitlement.
5. Click an account to display the account details in the Detailed Information section. This section displays the account details in the Account-Owner Information, Risk Summary, Certification History, and Action History tabs.
6. Click an entitlement to display the entitlement details in the Detailed Information section. This section displays the entitlement details in the Catalog Information, Risk Summary, Certification History, and Action History tabs.
7. To display the set of users who have accounts for the next entitlement in the certification task, click **Next** at the top of the page. You can click First, Previous, Next, and Last buttons to navigate between the pages for the account details of each entitlement. You can click **Back to Summary** to go back to the entitlement certification detail page.

## 10.3.2 Completing Certifications

Completing certifications is described in the following sections:

- [Completing User Certifications](#)
- [Completing Role Certifications](#)
- [Completing Application Instance Certifications](#)
- [Completing Entitlement Certifications](#)

### 10.3.2.1 Completing User Certifications

User certification enables managers to verify their employees and the role assignments, accounts and entitlement assignments for each. Completing a user certification involves the following steps:

1. [Making Certification Decision on the Users](#)
2. [Reviewing Roles and Entitlements](#)
3. [Finishing the User Certification](#)

**10.3.2.1.1 Making Certification Decision on the Users** When a certification task is opened, you may be required to verify the access of each user. This verification step is optional based on the configuration settings set in the certification definition. If verification is not required, then the initial summary view of users are skipped and you are presented with the user detail view.

If verification is required, then a decision must be made on each of the users that you have been asked to review. To do so:

1. In the Inbox, open the new or in progress certification review task. Page 1 of the certification task is displayed with a list of users.
2. Review the list of users and verify that each employee works for you, and that you are responsible for verifying their access.
3. From the Actions menu, select any one of the following for each user:
  - **Claim:** Select to restore a user to your verification queue for certification. This might happen automatically, depending on the values in certification configuration. See "Configuring Certification Options in Identity System Administration" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about the certification configuration options.

However, even if each user is claimed automatically, you are free to choose another action.

- **Revoke:** Select if the user is no longer part of the organization. This action removes the user from the certification process, and you will not approve or revoke roles and entitlements for this user. To return a user to your verification queue, select the user name, and select **Claim** from the Actions menu.
- **Re-assign:** Select if the user works for someone else who should now be responsible for verifying the user's assigned roles and entitlements. This action removes the selected user(s) from the current certification, creates a new certification with the selected user(s), and assigns the person you specify as the primary reviewer for that new certification.
- **Abstain:** Select if the employee does not work for you and you do not know who should be responsible for verifying the user's assigned roles and entitlements. This action on the user records on each role and entitlement assigns to the user your decision to abstain, that is, to leave each assignment as it is. If you know who should be responsible, then you can reassign the user instead.

After you have taken a verification action on each user, you must make certification decisions on each role and entitlement assigned to the users you have claimed. You do not need to make any further certification decisions on a user that you have revoked or reassigned or abstained. Normally, this means that you will open each user and then review its roles and entitlements, as described in ["Reviewing Roles and Entitlements"](#) on page 10-19. However, you may also choose to delegate one or more users to another person, which allows that person to make certification decisions on the roles and entitlements assigned to that user. The following actions are available from the Actions menu:

- **Open:** Select this action to review the details of each user and to make certification decisions on the roles and entitlements assigned to the user. See ["Reviewing Roles and Entitlements"](#) on page 10-19.
- **Delegate:** Select this action to allow another person to make decisions on the access privileges of each selected user. This action will create a new delegated-review task that contains the selected user(s) and will assign the task to the person you specify as delegate. Responsibility still remains with you, the primary reviewer.
- **Un-delegate:** This action applies only to delegated users. This action removes each selected user from the delegated-review task and returns decision-making rights to you, the primary reviewer.

The Actions menu offers two additional convenience actions that are useful after you have made some certification decisions on the details of a user. These actions affect the decisions on multiple details, that is, accesses of each selected user:

- **Complete:** Sets any missing decisions on role-assignments, accounts, or entitlement-assignments to Certify.
- **Reset:** Clears all decisions made on the user including decisions on the user's access.

**10.3.2.1.2 Reviewing Roles and Entitlements** Use the details view of the certification to review a user's role assignments, accounts, and entitlement assignments. The details view can be accessed by selecting a user in the summary view, and clicking **Open** from the Actions menu, or by clicking the user name.

After your selections are made, you can use the Actions menu to select the appropriate action. The Actions menu contains the following options:

- **Certify:** You approve each selected assignment.
- **Revoke:** You disapprove each selected assignment. This decision indicates that the user no longer needs the privilege and the assignment should be removed. When you select this option, a dialog box might be displayed that asks for comments. Type a note in the Comments pop-up, and click **OK**.
- **Certify Conditionally:** You approve each selected assignment, but only temporarily. This action also requires you to specify an end date on which your approval expires.
- **Abstain:** You take no position on each selected assignment. This records your decision to leave the assignment as it is.
- **Reset:** Use this to clear any decision you have made on the selected assignment.

For each action, optional comments can be added. By default, every decision other than to certify, such as Revoke, Certify Conditionally, and Abstain, allow optional comments.

**10.3.2.1.3 Finishing the User Certification** The final step in the certification cycle is the sign-off action. Signing off can only be done when every access privilege has a decision assigned to it. When this state is reached, Oracle Identity Manager automatically prompts you to sign-off on all the decisions taken. If you choose not to sign-off at that time, then you can manually invoke the sign-off dialog box later assuming that all access privileges are still completed. The process for signing off is the same whether automatically prompted by the system or manually activated.

To manually sign-off:

1. From the Actions menu, select **Sign-off**. The Sign-off dialog box is displayed asking to complete the certification.
2. To complete the certification, select **Yes**, and enter a password in the Password Required field. The password option is configurable and set in the certification definition. If disabled, the password field is not displayed in the Sign-off dialog box.

Alternatively, to complete the certification later, select **No**.

3. Click **OK**.

Upon successful sign-off, the tab displaying the certification is closed automatically and a confirmation message is displayed.

### 10.3.2.2 Completing Role Certifications

Role certification enables role owners to certify roles and role content. Completing a role certification involves the following steps:

1. [Making Certification Decisions on the Roles](#)
2. [Reviewing the Contents of the Roles](#)
3. [Finishing the Role Certification](#)

**10.3.2.2.1 Making Certification Decisions on the Roles** When a certification task is opened, you may be required to verify the access of each role. This verification step is optional based on the configuration settings set in the certification definition. If verification is

not required, then the initial summary view of role will be skipped, and you will be presented with the role detail view.

If verification is required, then a decision must be made on each of the roles for which you are the role owner. To do so:

1. In the Inbox, open the new or in progress certification review task. Page 1 of the certification task is displayed with a list of roles.
2. From the Actions menu, select any one of the following for each role:
  - **Claim:** Select to restore a role to your verification queue for certification. This might happen automatically, depending on the values in certification configuration. See "Configuring Certification Options in Identity System Administration" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about the certification configuration options. However, even if each role is claimed automatically, you are free to choose another action.
  - **Revoke:** Select if the role is no longer appropriate. This action removes the role from the certification process, and you will not approve or revoke assignments for this role. To return a role to your verification queue, select the role name, and select **Claim** from the Actions menu.
  - **Re-assign:** Select to remove the role from the current certification and create a new one with the selected role. This action removes the selected role(s) from the current certification, creates a new certification with the selected role(s), and assigns the person you specify as the primary reviewer for that new certification.
  - **Abstain:** Select if the role is not appropriate and you do not know who should be responsible for verifying the role's assigned accounts, memberships, and entitlements. This action on the role records on each account and entitlement assigns to the role your decision to abstain, that is, to leave each assignment as it is. If you know who should be responsible, then you can reassign the role instead.

After you have taken a verification action on each role, you must make certification decisions on each policy and entitlement assigned to the roles you have claimed. You do not need to make any further certification decisions on a role that you have revoked or reassigned or abstained. Normally, this means that you will open each role and then review its policies and entitlements, as described in ["Reviewing the Contents of the Roles"](#) on page 10-22. However, you may also choose to delegate one or more roles to another person, which allows that person to make certification decisions on the policies and entitlements assigned to that role. The following actions are available from the Actions menu:

- **Open:** Select this action to review the details of each role and to make certification decisions on the policies and entitlements assigned to the role. See ["Reviewing the Contents of the Roles"](#) on page 10-22.
- **Delegate:** Select this action to allow another person to make decisions on the access privileges of each selected role. This action will create a new delegated-review task that contains the selected role(s) and will assign the task to the person you specify as delegate. Responsibility still remains with you, the primary reviewer.
- **Un-delegate:** This action applies only to delegated roles. This action removes each selected role from the delegated-review task and returns decision-making rights to you, the primary reviewer.

The Actions menu offers two additional convenience actions that are useful after you have made some certification decisions on the details of a role. These actions affect the decisions on multiple details, that is, accesses of each selected role:

- **Complete:** Sets any missing decisions on account or entitlement assignments to Certify.
- **Reset:** Clears all decisions made on the role including decisions on the role's access.

**10.3.2.2.2 Reviewing the Contents of the Roles** Use the details view of the certification to review a role's policies, memberships, and entitlements. The details view can be accessed by selecting a role in the summary view and clicking the **Open** button from the Actions menu, or by clicking the role name.

After your selections are made, you can use the Actions menu to select the appropriate action. The Actions menu contains the following options:

- **Certify:** You approve each selected assignment.
- **Revoke:** You disapprove each selected assignment. This decision indicates that the role no longer needs the privilege and the assignment should be removed. When you select this option, a dialog box might be displayed that asks for comments. Type a note in the Comments pop-up, and click **OK**.
- **Certify Conditionally:** You approve each selected assignment, but only temporarily. This action also requires you to specify an end date on which your approval expires.
- **Abstain:** You take no position on each selected assignment. This records your decision to leave the assignment as it is.
- **Reset:** Use this to clear any decision you have made on the selected assignment.

For each action, optional comments can be added. By default, every decision other than to certify, such as Revoke, Certify Conditionally, and Abstain, allow optional comments.

Click the **Members** tab to review the users who have this role assigned. Revoke, Certify Conditionally, Certify, and/or Abstain the role's members as required. In this tab, an additional **Approve** option is available for two-phased user certification. Selecting this option copies the decision from Phase 1 to Phase 2. See "Understanding Multi-Phased Review in User Certification" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about two-phased review.

**10.3.2.2.3 Finishing the Role Certification** The final step in the certification cycle is the sign-off action. Signing off can only be done when every access privilege has a decision assigned to it. When this state is reached, Oracle Identity Manager automatically prompts you to sign-off on all the decisions taken. If you choose not to sign-off at that time, then you can manually invoke the sign-off dialog box later assuming that all access privileges are still completed. The process for signing off is the same whether automatically prompted by the system or manually activated.

To manually sign-off:

1. From the Actions menu, select **Sign-off**. The Sign-off dialog box is displayed asking to complete the certification.
2. To complete the certification, Select **Yes**, and enter a password in the Password Required field. The password option is configurable and set in the certification

definition. If disabled, the password field is not displayed in the Sign-off dialog box.

Alternatively, to complete the certification later, select **No**.

3. Click **OK**.

Upon successful sign-off, the tab displaying the certification is closed automatically and a confirmation message is displayed.

### 10.3.2.3 Completing Application Instance Certifications

Application instance certification involves certifying or revoking employee entitlements on one or more application instances. These entitlements are assigned directly to an employee and are not assigned as part of a role. Completing an application instance certification involves the following steps:

1. [Making Certification Decisions on the Application Instances](#)
2. [Reviewing Account and Entitlement Assignments](#)
3. [Finishing the Application Instance Certification](#)

**10.3.2.3.1 Making Certification Decisions on the Application Instances** When a certification task is opened, you may be required to verify the access of each application instance. This verification step is optional based on the configuration settings set in the certification definition. If verification is not required, then the initial summary view of application instances is skipped, and you are presented with the application instance detail view.

If verification is required, then a decision must be made on each of the application instances. To do so:

1. In the Inbox, open the new or in-progress certification review task.
2. From the Actions menu, select any one of the following for each application instance:
  - **Claim:** Select to restore an application instance to your verification queue for certification. This might happen automatically, depending on the values in certification configuration. See "Configuring Certification Options in Identity System Administration" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about the certification configuration options. However, even if each application instance is claimed automatically, you are free to choose another action.
  - **Revoke:** Select if the application instance is no longer appropriate. This action removes the application instance from the certification process, and you will not approve or revoke assignments for this application instance. To return an application instance to your verification queue, select the application instance name, and select **Claim** from the Actions menu.
  - **Re-assign:** Select to remove the application instance from the current certification and create a new one with the selected application instance. This action removes the selected application instance(s) from the current certification, creates a new certification with the selected application instance(s), and assigns the person you specify as the primary reviewer for that new certification.
  - **Abstain:** Select if the application instance is not appropriate and you do not know who should be responsible for verifying the application instance's assigned accounts and entitlements. This action on the application instance

records on each account and entitlement assigns to the application instance your decision to abstain, that is, to leave each assignment as it is. If you know who should be responsible, then you can reassign the application instance instead.

After you have taken a verification action on each application instance, you must make certification decisions on each account and entitlement assigned to the application instances you have claimed. You do not need to make any further certification decisions on an application instance that you have revoked or reassigned or abstained. Normally, this means that you will open each application instance and then review its accounts and entitlements, as described in "[Reviewing Account and Entitlement Assignments](#)" on page 10-24. However, you may also choose to delegate one or more application instances to another person, which allows that person to make certification decisions on the accounts and entitlements assigned to that application instance. The following actions are available from the Actions menu:

- **Open:** Select this action to review the details of each application instance and to make certification decisions on the accounts and entitlements assigned to the application instance. See "[Reviewing Account and Entitlement Assignments](#)" on page 10-24.
- **Delegate:** Select this action to allow another person to make decisions on the access privileges of each selected application instance. This action will create a new delegated-review task that contains the selected application instance(s) and will assign the task to the person you specify as delegate. Responsibility still remains with you, the primary reviewer.
- **Un-delegate:** This action applies only to delegated application instances. This action removes each selected application instance from the delegated-review task and returns decision-making rights to you, the primary reviewer.

The Actions menu offers two additional convenience actions that are useful after you have made some certification decisions on the details of an application instance. These actions affect the decisions on multiple details, that is, accesses of each selected application instance:

- **Complete:** Sets any missing decisions on account or entitlement assignments to Certify.
- **Reset:** Clears all decisions made on the role including decisions on the application instance's access.

**10.3.2.3.2 Reviewing Account and Entitlement Assignments** Use the details view of the certification to review an application instance's accounts and entitlements. The details view can be accessed by selecting an application instance in the summary view and clicking the **Open** button from the Actions menu, or by clicking the application instance name.

After your selections are made, you can use the Actions menu to select the appropriate action. The Actions menu contains the following options:

- **Certify:** You approve each selected assignment.
- **Revoke:** You disapprove each selected assignment. This decision indicates that the application instance no longer needs the privilege and the assignment should be removed. When you select this option, a dialog box might be displayed that asks for comments. Type a note in the Comments pop-up, and click **OK**.

- **Certify Conditionally:** You approve each selected assignment, but only temporarily. This action also requires you to specify an end date on which your approval expires.
- **Abstain:** You take no position on each selected assignment. This records your decision to leave the assignment as it is.
- **Reset:** Use this to clear any decision you have made on the selected assignment.

For each action, optional comments can be added. By default, every decision other than to certify, such as Revoke, Certify Conditionally, and Abstain, allow optional comments.

An additional **Approve** option is available for two-phased user certification. Selecting this option copies the decision from Phase 1 to Phase 2. See "Understanding Multi-Phased Review in User Certification" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about two-phased review.

**10.3.2.3 Finishing the Application Instance Certification** The final step in the certification cycle is the sign-off action. Signing off can only be done when every access privilege has a decision assigned to it. When this state is reached, Oracle Identity Manager automatically prompts you to sign-off on all the decisions taken. If you choose not to sign-off at that time, then you can manually invoke the sign-off dialog box later assuming that all access privileges are still completed. The process for signing off is the same whether automatically prompted by the system or manually activated.

To manually sign-off:

1. From the Actions menu, select **Sign-off**. The Sign-off dialog box is displayed asking to complete the certification.
2. To complete the certification, Select **Yes**, and enter a password in the Password Required field. The password option is configurable and set in the certification definition. If disabled, the password field is not displayed in the Sign-off dialog box.

Alternatively, to complete the certification later, select **No**.

3. Click **OK**.

Upon successful sign-off, the tab displaying the certification is closed automatically and a confirmation message is displayed.

### 10.3.2.4 Completing Entitlement Certifications

Entitlement certifications enable you to certify whether employees should be able to access entitlements. Completing an entitlement certification involves the following steps:

1. [Making Certification Decisions on the Entitlements](#)
2. [Reviewing the Entitlement Assignments](#)
3. [Finishing the Entitlement Certification](#)

**10.3.2.4.1 Making Certification Decisions on the Entitlements** When a certification task is opened, you may be required to verify the access of each entitlement. This verification step is optional based on the configuration settings set in the certification definition. If verification is not required, then the initial summary view of the entitlements is skipped, and you are presented with the entitlement detail view.

If verification is required, then a decision must be made on each of the entitlements. To do so:

1. In the Inbox, open the new or in-progress certification review task.
2. From the Actions menu, select any one of the following for each entitlement:
  - **Claim:** Select to restore an entitlement to your verification queue for certification. This might happen automatically, depending on the values in certification configuration. See "Configuring Certification Options in Identity System Administration" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about the certification configuration options. However, even if each entitlement is claimed automatically, you are free to choose another action.
  - **Revoke:** Select if the entitlement is no longer appropriate. This action removes the entitlement from the certification process, and you will not approve or revoke assignments for this entitlement. To return an entitlement to your verification queue, select the entitlement name, and select **Claim** from the Actions menu.
  - **Re-assign:** Select to remove the entitlement from the current certification and create a new one with the selected entitlement. This action removes the selected entitlement(s) from the current certification, creates a new certification with the selected entitlement(s), and assigns the person you specify as the primary reviewer for that new certification.
  - **Abstain:** Select if the entitlement is not appropriate and you do not know who should be responsible for verifying the entitlement's assigned accounts. This action on the entitlement records on each account assigns to the entitlement your decision to abstain, that is, to leave each assignment as it is. If you know who should be responsible, then you can reassign the entitlement instead.

After you have taken a verification action on each entitlement, you must make certification decisions on each user account assigned to the entitlements you have claimed. You do not need to make any further certification decisions on an entitlement that you have revoked or reassigned or abstained. Normally, this means that you will open each entitlement and then review its user accounts, as described in "[Reviewing the Entitlement Assignments](#)" on page 10-27. However, you may also choose to delegate one or more entitlements to another person, which allows that person to make certification decisions on the user accounts assigned to that entitlement. The following actions are available from the Actions menu:

- **Open:** Select this action to review the details of each entitlement and to make certification decisions on the user accounts assigned to the entitlement. See "[Reviewing the Entitlement Assignments](#)" on page 10-27.
- **Delegate:** Select this action to allow another person to make decisions on the access privileges of each selected entitlement. This action will create a new delegated-review task that contains the selected entitlement(s) and will assign the task to the person you specify as delegate. Responsibility still remains with you, the primary reviewer.
- **Un-delegate:** This action applies only to delegated entitlements. This action removes each selected entitlement from the delegated-review task and returns decision-making rights to you, the primary reviewer.

The Actions menu offers two additional convenience actions that are useful after you have made some certification decisions on the details of an entitlement. These

actions affect the decisions on multiple details, that is, accesses of each selected entitlement:

- **Complete:** Sets any missing decisions on account assignments to Certify.
- **Reset:** Clears all decisions made on the entitlement including decisions on the entitlement's access.

**10.3.2.4.2 Reviewing the Entitlement Assignments** Use the details view of the certification to review an entitlement's user accounts. The details view can be accessed by selecting an entitlement in the summary view and clicking **Open** from the Actions menu, or by clicking the entitlement name.

After your selections are made, you can use the Actions menu to select the appropriate action. The Actions menu contains the following options:

- **Certify:** You approve each selected assignment.
- **Revoke:** You disapprove each selected assignment. This decision indicates that the entitlement no longer needs the privilege and the assignment should be removed. When you select this option, a dialog box might be displayed that asks for comments. Type a note in the Comments pop-up, and click **OK**.
- **Certify Conditionally:** You approve each selected assignment, but only temporarily. This action also requires you to specify an end date on which your approval expires.
- **Abstain:** You take no position on each selected assignment. This records your decision to leave the assignment as it is.
- **Reset:** Use this to clear any decision you have made on the selected assignment.

For each action, optional comments can be added. By default, every decision other than to certify, such as Revoke, Certify Conditionally, and Abstain, allow optional comments.

An additional **Approve** option is available for two-phased user certification. Selecting this option copies the decision from Phase 1 to Phase 2. See "Understanding Multi-Phased Review in User Certification" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about two-phased review.

**10.3.2.4.3 Finishing the Entitlement Certification** The final step in the certification cycle is the sign-off action. Signing off can only be done when every access privilege has a decision assigned to it. When this state is reached, Oracle Identity Manager automatically prompts you to sign-off on all the decisions taken. If you choose not to sign-off at that time, then you can manually invoke the sign-off dialog box later assuming that all access privileges are still completed. The process for signing off is the same whether automatically prompted by the system or manually activated.

To manually sign-off:

1. From the Actions menu, select **Sign-off**. The Sign-off dialog box is displayed asking to complete the certification.
2. To complete the certification, Select **Yes**, and enter a password in the Password Required field. The password option is configurable and set in the certification definition. If disabled, the password field is not displayed in the Sign-off dialog box.

Alternatively, to complete the certification later, select **No**.

3. Click **OK**.

Upon successful sign-off, the tab displaying the certification is closed automatically and a confirmation message is displayed.

## 10.4 Managing Provisioning Tasks

This Open Tasks section of the Identity Self Service displays all provisioning tasks assigned to you or pending actions in your inbox. In addition, failed automatic provisioning tasks that you must review to take corrective action are displayed in your inbox. You must take corrective action, such as retry and manually complete, on those tasks.

The provisioning tasks feature is used by administrators as well as users. For example, the person in IT administration who is responsible for delivering a laptop computer to an employee may not be an administrator in Oracle Identity Manager, but must view and change provisioning tasks.

A provisioning operation such as creating or updating an account, or granting or revoking an entitlement can fail due to one of the following reasons:

- Mandatory information in the process form associated with the provisioning task is missing.
- Password specified for the account does not comply with the password policies configured on the target application.
- Target system is unavailable.

When a provisioning operation fails, you can configure the provisioning workflow to assign the failed task to an administrator or resource owner for taking an action. These tasks are visible in the Open Tasks page under the Administration region. When you click Open Tasks, all tasks assigned to you for remediation are displayed. In this page, you can perform actions such as viewing the details of a rejected task and retrying it. If the task is no longer valid, you can manually complete it.

You can perform the following tasks in the Provisioning tab:

- [Searching Provisioning Tasks](#)
- [Viewing Provisioning Task Details](#)
- [Adding Notes to a Task](#)
- [Reassigning a Task](#)
- [Viewing Task Assignment History](#)
- [Viewing Form Details](#)
- [Modifying Form Details](#)
- [Retrying a Task](#)
- [Manually Fulfilling Tasks](#)

### 10.4.1 Searching Provisioning Tasks

The first section in the Provisioning tab page allows you to search for the provisioning tasks assigned to you or on which your action is pending. Specify values in the following fields to search for the provisioning tasks:

- **Match:** The **All** and **Any** options are read-only.

- **Task Name:** Specify a task name that you want to search. To do so, select any one of the Starts with, Ends with, Equals, Does not equal, Contains, or Does not contain search operations.
- **Task Status:** Select **Pending** or **Rejected** to search for tasks for which your action is pending or for rejected tasks respectively.

After specifying the search criteria, when you click **Search**, the search results table is displayed. [Table 10 2](#) lists the fields in the search results table:

**Table 10 2 Fields in the Provisioning Tasks Search Results Table**

Field	Description
Task Name	The name of the task
Task Status	The status of the task, which is Pending or Rejected
Application Instance	The name of the application instance, which is affected by this task
Beneficiary	The user whose provisioned application instance will get affected because of this task
Date Assigned	The date and time when the Provisioning task has been assigned to the Assignee
Assignee	The user to whom the task is assigned
Request ID	The ID of the provisioning request task
Account Name	The name of the account being provisioned

## 10.4.2 Viewing Provisioning Task Details

To view provisioning task details:

1. Under Administration, open the Open Tasks section.
2. In the Provisioning Tasks page, search for and select the task whose detail you want to view.
3. From the Actions menu, select **Open**. Alternatively, you can click **Open** on the toolbar. The Task Details page is displayed in a new window.

[Table 10 3](#) lists the fields in the Task Details window:

**Table 10 3 Fields in the Task Details Window**

Field	Description
Task Name	The name of the task
Resource Name	The name of the resource, which is affected by this task
Description	A description of the task
User	The beneficiary user name
Status	The status of the task, Pending or Rejected
Response	The response set by the user on the Set Response page <b>Note:</b> For information about setting response, see " <a href="#">Setting Response for a Task</a> " on page 10-30.
Response Description	The description of the response that is defined in the Response tab of the Task Definition section in Oracle Identity Manager Design Console

**Table 10 3 (Cont.) Fields in the Task Details Window**

Field	Description
Notes	The additional comments entered by the approver
Assigned to	The user to whom or role to which the task is assigned <b>Note:</b> If the task is assigned to a role, this property will come as "Assigned to Role" with the role details.
Error Details	The error, if any, while setting the response
Projected Start	The date when the task is scheduled to start
Projected End	The date when the task is suppose to end
Actual Start	The date when the task was started
Actual End	The date when the task was ended
Last Update	The date when the task was last updated

### 10.4.3 Setting Response for a Task

As an approver, you can set a response for the task while taking an action on the task. To set a response for a task:

---



---

**Note:** Response cannot be set if there are no response codes defined for the corresponding tasks. Response codes are defined by using Oracle Identity Manager Design Console. For more information about defining response codes, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

---



---

1. Under Administration, open the Open Tasks section.
2. In the Provisioning Tasks page, search for and select a task for which you want to set a response.
3. From the Actions menu, select **Open**. Alternatively, you can click **Open** on the toolbar. The Task Details window is displayed.
4. In the Task Details window, click **Set Response**.
5. In the Specify Task Responses page, select one of the multiple responses defined, and click **OK**. The response is set.

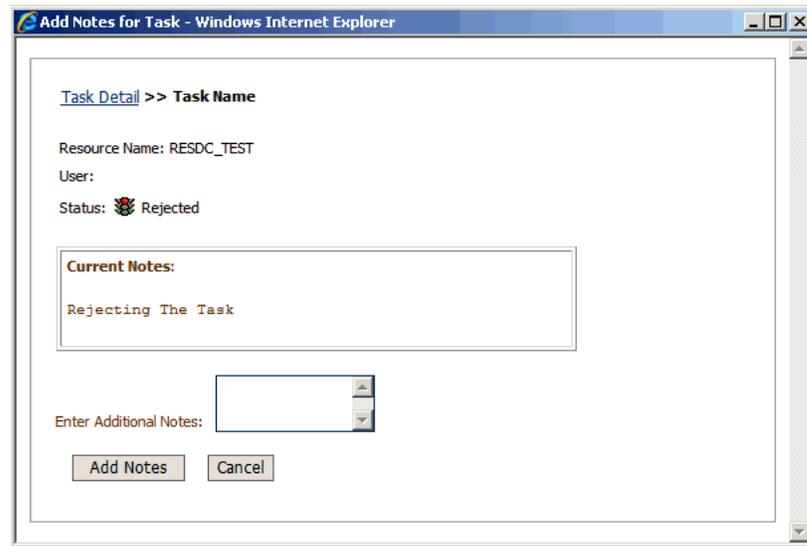
### 10.4.4 Adding Notes to a Task

Notes are additional comments provided by the approver. These comments are optional.

To add notes to a task:

1. Under Administration, open the Open Tasks section.
2. In the Provisioning Tasks page, search for and select a task for which you want to add notes.
3. From the Actions menu, select **Open**. Alternatively, you can click **Open** on the toolbar. The Task Details window is displayed.
4. In the Task Details window, click **Add Notes**. The Add Notes for Task window is displayed, as shown in [Figure 10 4](#):

**Figure 10 4 The Add Notes for Task Window**



5. In the Enter Additional Notes field, enter the note that you want to add to the task.
6. Click **Add Notes**.

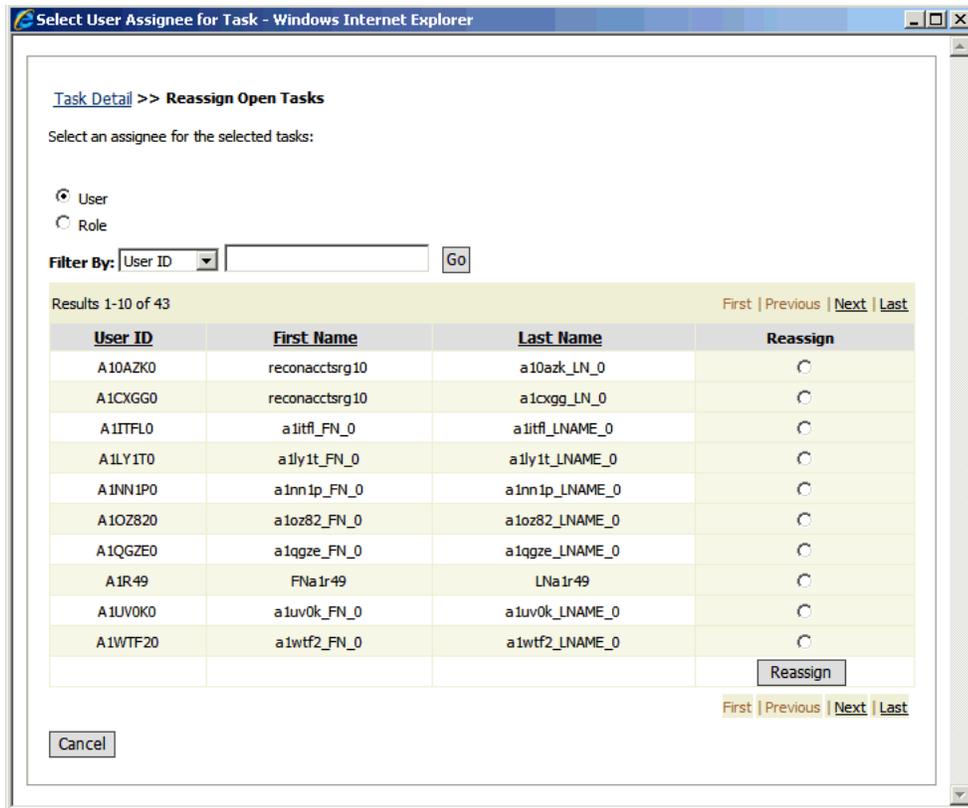
### 10.4.5 Reassigning a Task

As the approver, you can reassign a task to another user or role for taking appropriate action on the task. When the task is reassigned to another user, the assignee becomes the approver. When the task is reassigned to a role, any one member of that role can approve or reject the task.

To reassign a task to another user or role:

1. Under Administration, open the Open Tasks section.
2. In the Provisioning Tasks page, search for and select the task that you want to reassign.
3. From the Actions menu, select **Open**. Alternatively, you can click **Open** on the toolbar. The Task Details window is displayed.
4. In the Task Details window, click **Reassign**. The Select User Assignee for Task window is displayed, as shown in [Figure 10 5](#):

**Figure 10 5 The Select User Assignee for Task Window**

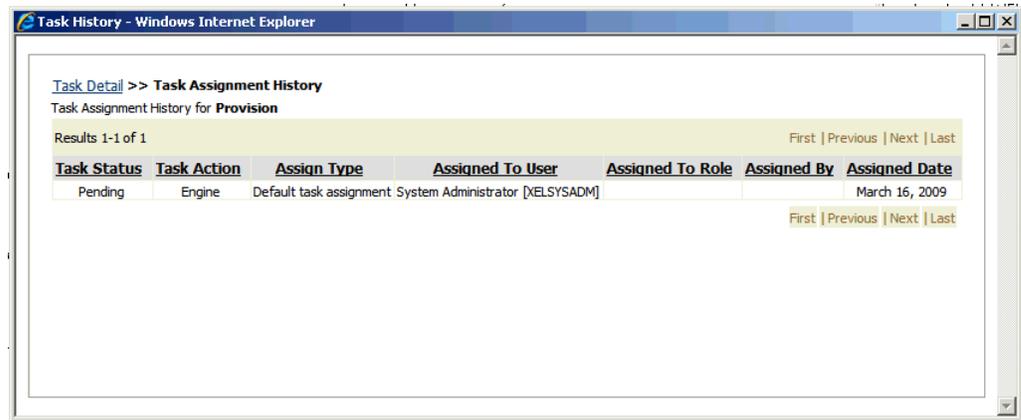


5. Select **User** or **Role** depending on what you want to search for. A list of users or roles is displayed, depending on your selection. You can also filter the search by specifying a criteria for filtering and entering a value in the Filter By field.
6. In the Reassign column, select a user or role to whom you want to assign the task.
7. Click **Reassign**.
8. In the Confirm Tasks to Reassign page, read the details of the action that you are performing and select **Confirm Re-assign Task** to reassign the task or select **Cancel Re-assign Task** to cancel the task reassignment.
9. Check whether the value in the Assigned to section is properly updated according to the above reassignment action.

### 10.4.6 Viewing Task Assignment History

To view the assignment history of a task:

1. Under Administration, open the Open Tasks section.
2. In the Provisioning Tasks page, search for and select a task for which you want to view the task assignment history.
3. From the Actions menu, select **Open**. Alternatively, you can click **Open** on the toolbar. The Task Details window is displayed.
4. In the Task Details window, click **Task Assignment History**. The Task History window is displayed, as shown in [Figure 10 6](#):

**Figure 10 6 The Task History Window**

The task assignment history is displayed in the fields, as shown in [Table 10 4](#):

**Table 10 4 Fields in the Task History Window**

Field	Description
Task Status	The status of the task, Pending or Rejected
Task Action	The source details of the task, for example, when the task is first created it will be "Engine". If the user reassigns the task, it will be "User".
Assign Type	The type of the assignee of the task, for example, when the task is assigned for the first time, it is "Default Task Assignment". If the task is reassigned, then its value is either user or role.
Assigned to User	The user to whom the task is assigned
Assigned to Role	The role to which the task is assigned
Assigned By	The user who assigned the task
Assigned Date	The date when the task was assigned

### 10.4.7 Viewing Form Details

You can view the process form attached with a task. These are process forms associated with the underlying process definition. A task is embedded in the process definition.

To view the process form attached with a task:

1. Under Administration, open the Open Tasks section.
2. In the Provisioning Tasks page, search for and select a task whose process form you want to view.
3. From the Actions menu, select **View Form**. Alternatively, you can click **View Form** on the toolbar. The View Form window is displayed.

### 10.4.8 Modifying Form Details

You can edit the process form associated with a provisioning workflow to provide missing information, if any.

To modify the process form details:

1. Under Administration, open the Open Tasks section.

2. In the Provisioning Tasks page, search for and select a task whose process form you want to modify.
3. From the Actions menu, select **Edit Form**. Alternatively, you can click **Edit Form** on the toolbar.
4. In the Edit Form window, modify the required details and click **Save**.

### 10.4.9 Retrying a Task

As the approver, you can retry a task when an error was generated while setting the response in the first attempt. To retry a task:

---

---

**Note:** Only automated tasks can be retried, and an adapter must be attached to the task. Manual tasks cannot be retried.

---

---

1. Under Administration, open the Open Tasks section.
2. In the Provisioning Tasks page, search for and select a task that you want to retry.
3. From the Actions menu, select **Retry**. Alternatively, you can click **Retry** on the toolbar.
4. A warning message is displayed prompting you to confirm whether you want to retry the task.
5. Click **Retry**.

### 10.4.10 Manually Fulfilling Tasks

There are two types of provisioning operations:

- **Automated:** These are provisioning operations that take place in an automated manner by using an Oracle Identity Manager connector for a particular target application.
- **Manual:** These are provisioning operations that are manually performed with human intervention.

A manual fulfillment task is created during manual provisioning operations. In addition, a manual fulfillment task is created during automated provisioning operation if you want to introduce manual steps to mandate an administrator to take some action either before or after the provisioning operation.

To complete a manual fulfillment task:

1. Log in to Identity Self Service.
2. In the left pane, click **Inbox**. The Worklist Views page is displayed.
3. In the My Work Queues menu, click Manual Provisioning to view the manual fulfillment tasks. Select a task to view the details. The manual task details are displayed in a new window with sections such as Details, Contents, Cart Details, History, Comments, and Attachments.
4. In the Details section, change any value as desired, and then click **Fulfill**. A message confirming that the account data has been successfully updated is displayed.
5. If required, in the Comments and Attachments sections, add comments and attachments, respectively. See "[Adding Comments and Attachments](#)" on page 10-9 for more information.

6. Click **Complete**.

## 10.5 Managing Attestation Tasks

---

---

**Note:** The attestation feature has been deprecated in Oracle Identity Manager 11g Release 2 (11.1.2.1.0). However, this feature is available if you upgrade from Oracle Identity Manager Release 9.x or 11g Release 1 (11.1.1) or 11g Release 2 (11.1.2).

---

---

Attestation enables users designated as reviewers to be notified of reports they must review. These reports describe provisioned resources of other users. A reviewer can attest to the accuracy of the entitlements by providing a response. The attestation action, along with the response the reviewer provides, any associated comments, and an audit view of the data that the reviewer views and attests to, is tracked and audited to provide a complete trail of accountability. In Oracle Identity Manager, this process is known as an attestation task.

An attestation process is the mechanism by which an attestation task is set up. Input that an attestation process requires includes information about how to define the components that constitute the attestation task and how to associate the attestation task with a schedule at which the task must be run. This definition is also the basis on which the attestation task can be initiated when required.

The Pending Attestations section in Identity Self Service displays all attestation processes assigned to you or pending your actions in your inbox.

---

---

**Note:** Using Oracle Identity Manager integrated with Oracle Identity Analytics (OIA) replaces the attestation functionality.

---

---

You can perform the following tasks in the Pending Attestations section:

- [Searching Attestation Tasks](#)
- [Viewing Attestation Request Detail](#)

### 10.5.1 Searching Attestation Tasks

To search for attestation tasks:

1. Log in to Identity Self Service.
2. In the left pane, under Requests, click **Pending Attestations**. The Pending Attestations page is displayed.
3. Select any one of the following options:
  - **All:** To search all the tasks that match the criteria you specify.
  - **Any:** To search any task that matches your criteria.
4. In the Task Name field, enter the name of the task that you want to search. To do so, select the Starts with, Ends with, Equals, or Contains search operators.
5. In the Start Date field, specify a start date of the task by using the Start Date icon next to the field. To do so, select the Equals, Before, or After search operators.
6. Click **Search**. The attestation tasks that match the search criteria are displayed in a search results table. [Table 10 5](#) shows the fields in the search results table:

**Table 10 5 Fields in the Attestation Task Search Results Table**

Field	Description
Task Name	The name of the task.
Process Code	An unique identifier for the task that is entered by the user.
Start Date	The start date of the attestation task.
Type	The type of task. This is hard coded as 'Access Right'.
No of records	The number of records displayed as the search result.

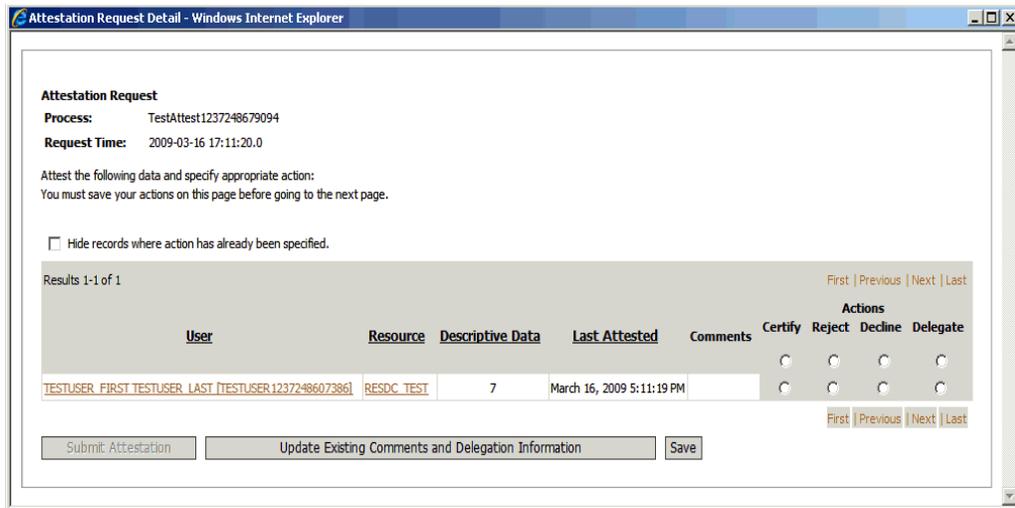
### 10.5.2 Viewing Attestation Request Detail

To view attestation request detail:

1. In Identity Self Service, under Request, click **Pending Attestations**. The Pending Attestations page is displayed.
2. Search for and select the task that you want to view.
3. From the Actions menu, select **Open Task Details**. Alternatively, you can click Open Task Details on the toolbar. The Attestation Request Detail window is displayed, as shown in [Figure 10 7](#):

**Note:** Multiple users, designated as reviewers can view the attestation request details. However, only one user, whoever does it first, can submit the attestation.

**Figure 10 7 The Attestation Request Detail Window**



[Table 10 6](#) lists the fields in the Attestation Request Detail window:

**Table 10 6 Fields in the Attestation Request Detail Window**

Field	Description
Process	Name of your attestation process created.
Request Time	The time when the request is created.

**Table 10 6 (Cont.) Fields in the Attestation Request Detail Window**

<b>Field</b>	<b>Description</b>
Hide records where action has already been specified	Whether or not the records for which action has been specified must be hidden from the list of attestation requests.
User	User whose entitlement is being attested. The data is displayed as a link. When you click the link, the user profile page is displayed with the user details for the attestation date.
Resource	Resource that is the basis for the entitlement being attested. The data is displayed as a link. When you click the link, a page is displayed with the process form data of the entitlement for the attestation date.
Descriptive Data	Description of the provisioned resource instance.
Last Attested	Last response that was provided for the attestation.
Comments	Reviewer comments. The comments will be updated in this field, when you click <b>Update Existing Comments and Delegation Information</b> . Long comments are truncated, and tooltips are used to show the full text of the comments.
Actions	Action to be performed on the request. The value can be one of the following: <ul style="list-style-type: none"> <li>▪ Certify</li> <li>▪ Reject</li> <li>▪ Decline</li> <li>▪ Delegate</li> </ul>
Submit Attestation	Click this button to submit the attestation request.
Save	Click this button to save the attestation request for future submission.



# Part III

---

## Identity Administration

This part describes Oracle Identity Manager delegated administration functionalities by using the identity administration features.

It contains the following chapters:

- [Chapter 11, "Managing Users"](#)
- [Chapter 12, "Managing Roles"](#)
- [Chapter 13, "Managing Organizations"](#)
- [Chapter 14, "Using the Attestation Dashboard"](#)



The user management feature in Oracle Identity Manager includes creating, updating, deleting, enabling and disabling, locking, and unlocking of user accounts. This feature is described in the following sections:

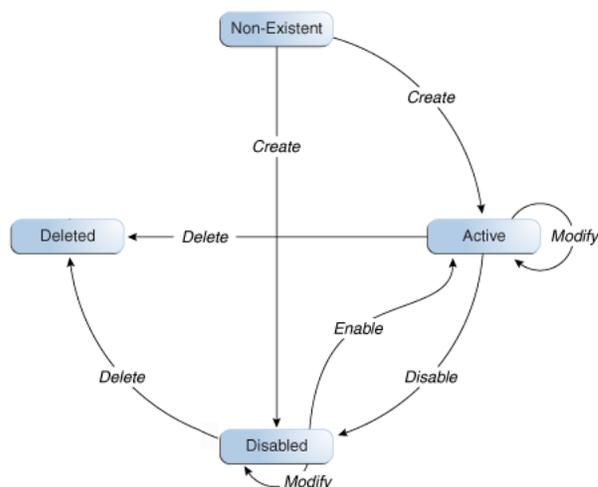
- [User Lifecycle](#)
- [User Entity Definition](#)
- [Default User Accounts](#)
- [User Management Tasks](#)
- [Username Reservation](#)
- [Common Name Generation](#)

## 11.1 User Lifecycle

User lifecycle is a term to describe the process flow of how a user entity is created, managed, and terminated in the system based on certain events or time factors.

A user entity goes through various stages in the lifecycle. The stages are non-existent, disabled, active, and deleted. [Figure 11-1](#) depicts the different lifecycle stages, all possible transitions, and the operations that set up those transitions:

**Figure 11-1 User Life Cycle**



There is a possibility of process rules or business requirements being defined for each transition of the user lifecycle. You can use the sample scenarios listed in [Table 11–1](#) to establish the link between user lifecycle transitions and business objectives.

**Table 11–1 User Life Cycle and Business Objectives Sample Scenarios**

Current State	Operation	Sample Scenario	Process Description
Non-existent	Create	HR enters user profile information for a new hire. If the new hire is not introduced to the system immediately, then HR sets a future start date for the user.	If the start is not a future date then the user is introduced into the system in an Active state.  If the Start Date is in future then the create process creates the user in a disabled state.
Disabled	Enable	User's start date is in effect. The system initiates provisioning for the new hire.	User is marked enabled in the system and the user is now able to login and use the system. By default, all necessary memberships and accounts are established as part of the workflow.
Active	Modify	User is promoted to a new position. As a result, HR changes the job title of the user.	New resources are provisioned to the user, and old irrelevant resources are deprovisioned from the user.
Active	Disable	User takes one year sabbatical from the company. HR manually disables the user on the last working day of the user. The user re-joins the company after some period. HR can make the user Active again.	User is marked disabled in the system, and the user is no longer able to login to the system. The disabled users can be made Active again.
Active	Deleted	User retires from the company. HR manually deletes the user on the last working day of the user.	User is marked deleted in the system, and the user is no longer able to login to the system. By default, all users' accounts are deprovisioned as part of the workflow.

The following concepts are integral to user lifecycle management:

- [OIM Account](#)
- [Organization](#)
- [Role](#)

### 11.1.1 OIM Account

OIM Account is an abstraction representing a means to be authenticated to access Oracle Identity Manager. In Oracle Identity Manager, the cardinality of relationship between user and OIM account is one-to-one. By default, users are associated with OIM accounts that allow users to access Oracle Identity Manager. However, there may be users who do not need to access Oracle Identity Manager, and therefore, may not be provisioned with an OIM account.

Some user operations, such as lock and unlock, are explicitly account operations. When locking or unlocking a user, you lock or unlock the user's OIM account.

## 11.1.2 Organization

Organization is a logical container for authorization and permission data. A user in Oracle Identity Manager must belong to one organization only. For detailed information about organizations in Oracle Identity Manager, see [Chapter 13, "Managing Organizations"](#).

## 11.1.3 Role

Oracle Identity Manager provides easy and controlled privilege management through roles. Roles are named groups of related privileges that you grant to users or other roles. Roles are designed to ease the administration of end-user system and schema object privileges. For detailed information about roles, see [Chapter 12, "Managing Roles"](#).

## 11.2 User Entity Definition

Attributes are defined for the user entity in Oracle Identity Manager. These attributes are the same for all entities. You can add your own attributes to the user entity.

For each attribute of an entity, the following properties are defined in Oracle Identity Manager:

- **Attribute Name:** The name of the attribute.
- **Type:** Indicates the type of data in the attribute. Supported types are string, number, date, boolean, and lookup.
- **Properties:** For each attribute, the properties such as Use in bulk (specifies whether the attribute is available in bulk operations), Encrypt (determines whether the attribute must be encrypted), Searchable (determines whether the attribute can be searched by a user), and so on can be defined.

**See Also:** "Configuring Custom Attributes" in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about adding custom attributes and their properties

[Table 11-2](#) lists the attributes defined for the user entity in Oracle Identity Manager:

**Table 11-2 Attributes Defined for User Entity**

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
usr_key	Account Settings	The GUID of the user. It is autogenerated when the user is created.	number	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: Yes Max-Size: 19 Visible: No Display-Type: ENTITY	N/A
act_key	Basic User Information	The GUID of the organization to which the user belongs. This is a mandatory field.	number	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: 19 Visible: Yes Display-Type: ENTITY	N/A
Last Name	Basic User Information	The last name of the user. This is a mandatory field.	string	Required: Yes System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A
First Name	Basic User Information	The first name of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A

Table 11-2 (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
Middle Name	Basic User Information	The middle name of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A
Display Name	Basic User Information	The display name of the user. If not specified, then it is autogenerated while creating the user.	string	Required: No MLS: No Multi-represented: Yes System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 382 Visible: Yes Display-Type: TEXT	N/A
Xellerate Type	Basic User Information	The type of end-user or administrator.	string	Required: Yes System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: 30 Visible: Yes Display-Type: CHECKBOX	Lookup.Users.XellerateType End-User End-User Administrator

**Table 11–2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
usr_password	Account Settings	The password of the user. It is stored as an encrypted value.	string	Required: Yes System-Controlled: No Encryption: Encrypt User-Searchable: No Bulk-Updatable: No Read-Only: No Max-Size: 128 Visible: Yes Display-Type: SECRET	N/A
usr_disabled	Account Settings	Indicates whether the user is disabled or enabled. 0 indicates that the user is enabled. 1 Indicates that the user is disabled.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: Yes Read-Only: Yes Max-Size: 1 Visible: Yes Display-Type: CHECKBOX	N/A
Status	Account Settings	The status of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: Yes Max-Size: 25 Visible: Yes Display-Type: LOV	Lookup.Web Client.Users.Status Active Disabled Deleted Disabled Until Start Date

Table 11-2 (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
Role	Basic User Information	The type of user in the system.	string	Required: Yes System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: 255 Visible: Yes Display-Type: LOV	Lookup.Users.Role Full-Time Part-Time Temp Intern Consultant EMP CWK NONW OTHER Contractor
User Login	Account Settings	The login ID of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 256 Visible: Yes Display-Type: TEXT	N/A
usr_manager_key	Basic User Information	The GUID of the user's manager.	number	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: 19 Visible: Yes Display-Type: ENTITY	N/A

**Table 11-2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
Start Date	Account Effective Dates	The start date of the user.	date	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: - Visible: Yes Display-Type: DATE_ONLY	N/A
End Date	Account Effective Dates	The end date of the user.	date	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: - Visible: Yes Display-Type: DATE_ONLY	N/A
usr_provisioning_date	Provisioning Dates	The date on which the user profile has been created in Oracle Identity Manager.	date	Required: No System-Controlled: No Encryption: Clear Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: - Visible: Yes Display-Type: DATE_ONLY	N/A

**Table 11-2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
usr_deprovisioning_date	Provisioning Dates	The date when the resources will be deprovisioned from the user.	date	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: - Visible: Yes Display-Type: DATE_ONLY	N/A
usr_provisioned_date	System	The date when the resources have been provisioned to the user.	date	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: Yes Max-Size: - Visible: No Display-Type: DATE_ONLY	N/A
usr_deprovisioned_date	System	The date when the resources are deprovisioned from the user.	date	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: Yes Max-Size: - Visible: No Display-Type: DATE_ONLY	N/A

**Table 11-2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
Email	Basic User Information	The e-mail address of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 256 Visible: Yes Display-Type: TEXT	N/A
usr_locked	Account Settings	Indicates whether the user account is locked or unlocked.  The value 0 indicates that the account is unlocked.  The value 1 indicates that the account is locked.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Update: No Read-Only: Yes Max-Size: 1 Visible: Yes Display-Type: LOV	Users.Lock User 0 1
Locked On	Lifecycle	The date on which the user account has been locked.	date	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: - Visible: No Display-Type: DATE_ONLY	N/A
Automatically Delete On	Lifecycle	The date on which the user account will be automatically deleted.	date	Required: No System-Controlled: No Encryption: Clear Searchable: Yes Bulk-Updatable: Yes Read-Only: Yes Max-Size: - Visible: No Display-Type: DATE_ONLY	N/A

**Table 11-2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
Manually Locked	Lifecycle	Indicates whether the user account has been automatically or manually locked.  1 indicates that the account has been manually locked by an administrator.  0 indicates that the account has been automatically locked, for instance, on exceeding the maximum number of login attempts with incorrect password.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 1 Visible: No Display-Type: TEXT	N/A
usr_login_attempts_ctr	System	The number of times the user has tried logging in with incorrect password. It is set to 0 at every successful login.	number	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 19 Visible: No Display-Type: NUMBER	N/A
usr_create	System	The date on which the user has been created.	date	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: Yes Max-Size: - Visible: No Display-Type: DATE_ONLY	N/A

**Table 11-2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
usr_update	System	The date on which the user has been last updated.	date	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: Yes Max-Size: - Visible: No Display-Type: DATE_ONLY	N/A
usr_timezone	Preferences	The timezone preference of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: 100 Visible: Yes Display-Type: TIME_ZONE	N/A

Table 11–2 (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
usr_locale	Preferences	The locale preference of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: 100 Visible: Yes Display-Type: LOV	Notification.Languages English French German Italian Spanish Brazilian Portuguese Japanese Korean Simplified Chinese Traditional Chinese Arabic Czech Danish Dutch Finnish Greek Hebrew Hungarian Norwegian Polish Portuguese Romanian Russian Slovak Swedish Thai Turkish
usr_pwd_change	System	This field is currently not used.	string	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 1 Visible: No Display-Type: CHECKBOX	N/A

**Table 11-2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
usr_pwd_must_change	System	This field is currently not used. The value 0 indicates that the password is not required to be changed. The value 1 mandates that the user changes the password.	string	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 1 Visible: No Display-Type: CHECKBOX	N/A
usr_pwd_never_expires	System	This field is currently not used. The value 0 indicates that the password will expire. The value 1 indicates that password never expires.	string	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 1 Visible: Yes Display-Type: CHECKBOX	N/A
usr_pwd_expire_date	System	The date on which the password will expire. Valid if Password Never Expires is 0.	date	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: - Visible: No Display-Type: DATE_ONLY	N/A

**Table 11-2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
usr_pwd_warn_date	System	The date after which the user will be warned to change the password.	date	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Update: No Read-Only: Yes Max-Size: - Visible: No Display-Type: DATE_ONLY	N/A
usr_pwd_expired	System	Indicates whether the user password has expired. If so, then the password must be reset.  The value 0 indicates that password has not expired.  The value 1 indicates that password has expired.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Update: No Read-Only: Yes Max-Size: 1 Visible: No Display-Type: CHECKBOX	N/A
usr_pwd_warned	System	Indicates whether the user has been warned to change the password.  0 indicates that the user has not been warned to change the password yet.  1 indicates that the user has been warned to change the password.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Update: No Read-Only: Yes Max-Size: 1 Visible: No Display-Type: CHECKBOX	N/A

**Table 11-2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
usr_pwd_reset_attempts_ctr	System	The number of times the user has tried resetting the password with incorrect answers to challenge questions. It is set to 0 at every successful reset password.	number	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 19 Visible: No Display-Type: NUMBER	N/A
usr_change_pwd_at_next_logon	System	Indicates whether the user must change his password at next login.  The value 1 indicates that the user must reset password at next login. The value 0 indicates that user does not need to reset password at next login.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Update: No Read-Only: Yes Max-Size: 1 Visible: No Display-Type: CHECKBOX	N/A
usr_data_level	System	Indicates the kind of operation, such as add, modify, or delete, supported on this record.  The possible values for this column are:  0: Indicates that this row can be updated or deleted  1: Indicates that this row cannot be updated and deleted  2: Indicates that the row can only be modified and cannot be deleted  3: Indicates that the row can only be deleted and cannot be modified	string	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 1 Visible: No Display-Type: TEXT	N/A

**Table 11–2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
usr_pwd_min_age_date	System	If set, then it indicates the date before which the user password cannot be changed.	date	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: - Visible: No Display-Type: DATE_ONLY	N/A
usr_createby	System	The GUID of the user who created this user.	number	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 19 Visible: No Display-Type: ENTITY	N/A
usr_updateby	System	The GUID of the user who updated this user.	number	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 19 Visible: No Display-Type: ENTITY	N/A

**Table 11–2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
usr_created	System	This is not currently used in Oracle Identity Manager.	date	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 19 Visible: No Display-Type: DATE_ONLY	N/A
usr_policy_update	System	This is used to re-evaluate the user's policies. To re-evaluate object policies for any user to whom the current policy applies, evaluate the UPP and UPD tables to get list of users for the current policy. For each user found, set the policy_update flag. Attach as a post-insert, post-update and post_delete event handler to tcPOP.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: Yes Read-Only: Yes Max-Size: 1 Visible: No Display-Type: TEXT	N/A
Country	Other User Attributes	The country of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 100 Visible: Yes Display-Type: TEXT	N/A
Department Number	Other User Attributes	The department number of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A

**Table 11–2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
Description	Other User Attributes	The description of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 2000 Visible: Yes Display-Type: TEXT	N/A
Common Name	Other User Attributes	The common name of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 240 Visible: Yes Display-Type: TEXT	N/A
Employee Number	Other User Attributes	The employee number of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A
Fax	Other User Attributes	The FAX number of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: Yes Display-Type: TEXT	N/A

**Table 11–2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
Generation Qualifier	Other User Attributes	The Generation Qualifier for the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: Yes Display-Type: TEXT	N/A
Hire Date	Other User Attributes	The hire date of the user.	date	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: - Visible: Yes Display-Type: DATE_ONLY	N/A
Home Phone	Other User Attributes	The home phone number of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: Yes Display-Type: TEXT	N/A
Locality Name	Other User Attributes	The locality name of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A

Table 11-2 (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
Mobile	Other User Attributes	The mobile number of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: Yes Display-Type: TEXT	N/A
Pager	Other User Attributes	The pager number of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: Yes Display-Type: TEXT	N/A
Home Postal Address	Other User Attributes	The home postal address of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 256 Visible: Yes Display-Type: TEXT	N/A
Postal Address	Other User Attributes	The postal address of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 256 Visible: Yes Display-Type: TEXT	N/A

**Table 11–2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
Postal Code	Other User Attributes	The postal code of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 230 Visible: Yes Display-Type: TEXT	N/A
PO Box	Other User Attributes	The PO box number of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: Yes Display-Type: TEXT	N/A
State	Other User Attributes	The state of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A
Street	Other User Attributes	The street name in the user's address.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A

Table 11-2 (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
Telephone Number	Other User Attributes	The telephone number of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: Yes Display-Type: TEXT	N/A
Title	Other User Attributes	The title of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A
Initials	Other User Attributes	The initials of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 10 Visible: Yes Display-Type: TEXT	N/A
Password Generated	System	This flag indicates whether the password has been autogenerated for the user.	string	Required: No System-Controlled: Yes Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: Yes Max-Size: 1 Visible: No Display-Type: TEXT	N/A

**Table 11–2 (Cont.) Attributes Defined for User Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Description</b>	<b>Data Type</b>	<b>Properties</b>	<b>Lookup Code and its Entries</b>
LDAP Organization	Other User Attributes	User organization name in LDAP.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A
LDAP Organization Unit	Other User Attributes	User organization unit in LDAP, such as department or any subentity of a larger entity.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 80 Visible: Yes Display-Type: TEXT	N/A
LDAP GUID	Other User Attributes	User global unique identifier in LDAP.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 256 Visible: Yes Display-Type: TEXT	N/A
LDAP DN	Other User Attributes	User distinguished name in LDAP.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 256 Visible: Yes Display-Type: TEXT	N/A

Table 11-2 (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
FA Language	Preferences	Language of the user for LDAP environment.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: 100 Visible: No Display-Type: TEXT	NA
Embedded Help	Other User Attributes	Indicates whether to suppress the help popups on rollover. This attribute is not interpreted by Oracle Identity Manager and is used to persist values in LDAP.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: No Max-Size: 10 Visible: No Display-Type: LOV	Lookup.Users.EmbeddedHelp true false
Number Format	Other User Attributes	The number format preference of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: No Max-Size: 30 Visible: No Display-Type: LOV	Lookup.Users.NumberFormat ###0.##[.,] ###0.###[\u00A0,] ###0.### ###0.###;### 0.###- ###0.###[.,] ###0.###;(#,##0.###)[.,] ###0.##[\u00A0,] ###0.###[.] ###0.###[',]

**Table 11-2 (Cont.) Attributes Defined for User Entity**

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
Date Format	Other User Attributes	The date format preference of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: No Display-Type: LOV	Lookup.Users.DateFormat MM-dd-yyyy MM-dd-yy MM.dd/yyyy MM.dd.yy MM/dd/yyyy y MM/dd/yy M-d-yyyy M-d-yy M.d/yyyy M.d.yy M/d/yyyy M/d/yy dd-MM-yyyy dd-MM-yy d-M-yyyy d-M-yy dd.MM/yyyy dd.MM.yy d.M/yyyy d.M.yy dd/MM/yyyy y dd/MM/yy d/M/yyyy d/M/yy yyyy-MM-dd yy-MM-dd yyyy-M-d yy-M-d yyyy.MM.dd yy.MM.dd yyyy.M.d yy.M.d yy. M. d yyyy/MM/d d yy/MM/dd yyyy/M/d yy/M/d

Table 11-2 (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
Time Format	Other User Attributes	The time format preference of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: No Display-Type: LOV	Lookup.Users .TimeFormat HH:mm HH:mm:ss HH:mm HH:mm:ss H:mm H:mm:ss H:mm H:mm:ss a hh:mm a hh:mm:ss a hh:mm a hh:mm:ss ah:mm ah:mm:ss hh:mm a hh:mm:ss a hh:mm a hh:mm:ss a
Currency	Other User Attributes	The preferred currency code of the user.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: No Display-Type: LOV	Lookup.Users .Currency
Font Size	Other User Attributes	The preferred font size of the user, such as large or medium. This is related to the Accessibility feature. This attribute is not interpreted by Oracle Identity Manager and is used to persist values in LDAP.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: No Max-Size: 10 Visible: No Display-Type: LOV	Lookup.Users .FontSize LARGE MEDIUM

Table 11–2 (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Description	Data Type	Properties	Lookup Code and its Entries
Color Contrast	Other User Attributes	The preferred color contrast of the user, such as standard or high. This is related to the Accessibility feature. This attribute is not interpreted by Oracle Identity Manager and is used to persist values in LDAP.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: No Max-Size: 10 Visible: No Display-Type: LOV	Lookup.Users.ColorContrast STANDARD HIGH
Accessibility Mode	Other User Attributes	The preferred accessibility feature of the user, such as Screen Reader Optimized or Standard Accessibility. This attribute is not interpreted by Oracle Identity Manager and is used to persist values in LDAP.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: No Bulk-Updatable: No Read-Only: No Max-Size: 20 Visible: No Display-Type: Text	Lookup.Users.AccessibilityMode screenReader inaccessible default
FA Territory	Preferences	Region of the user for LDAP environment.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No Read-Only: No Max-Size: 100 Visible: No Display-Type: LOV	NA
User Name Preferred Language	Preferences	The preference language of the user used to show only the display name of the user in that language.  <b>Note:</b> The preference can be stored in Oracle Identity Manager, but it is not honored on Oracle Identity Manager UI.	string	Required: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes Read-Only: No Max-Size: 20 Visible: No Display-Type: LOV	Select MLS_LOCAL E_CODE as USR_NAME_ PREFERRED _LANG from mls_locale where locale_flag=0 OR locale_flag 1 order by mmls_locale_co de asc

## 11.3 Default User Accounts

Table 11–3 lists the default user accounts that are created in Oracle Identity Manager.

**Table 11–3** Default User Accounts

Account	Description
XELSYSADM	This account is the Oracle Identity Manager administrator (super-user) and is created during installation. You create a password for this account during installation. To change the password at any later point in time after installation, see "Changing Oracle Identity Manager Administrator Password" in <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager</i> .
WEBLOGIC	This account is used for integrating SOA and Oracle Identity Manager by using the 'User Role Provider' implementation. When SOA is reconfigured to use LDAP-based user-role provider, Oracle Identity Manager does not require this account.  This account is created during installation. You create a password for this account during installation. To change the user name of this account at any later point in time after installation, see "Enabling Oracle Identity Manager to Connect to SOA Using the Administrative Users Provisioned in LDAP" in <i>Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management</i> .
OIMINTERNAL	This account is set to a 'run as' user for Message Driven Beans (MDBs) executing JMS messages. This account is created during installation and is used internally by Oracle Identity Manager.  The password of this account is set to a single space character in Oracle Identity Manager database to prevent user login through Oracle Identity Manager Design console or Oracle Identity Manager System Administration Console.  Do <i>not</i> change the user name or password of this account.

## 11.4 User Management Tasks

You can perform the following user management tasks by using Oracle Identity Self Service:

---

**Note:** For more information about the tasks listed in this section, see "Security Architecture" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

---

- [Searching Users](#)
- [Creating a User](#)
- [Viewing User Details](#)
- [Modifying Users](#)
- [Disabling a User](#)
- [Enabling a User](#)
- [Deleting a User](#)
- [Locking an Account](#)
- [Unlocking an Account](#)

## 11.4.1 Searching Users

The search operation lets you search user entities based on the search criteria that you specify. Each search criterion consists of:

- The attribute to search against
- The search operators, such as Equals and Starts with
- The values to search for

To search for users:

1. Log in to Identity Self Service.
2. On the left pane, under Administration, select **Users**. The Manage Users page is displayed.
3. Select any one of the following options:
  - **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.
  - **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.
4. In the searchable user attribute fields, such as User Login, specify a value. You can include wildcard characters (\*) in the attribute value.

For some attributes, select the attribute value from the list. For example, to search all users with locked accounts, select **Locked** from the Account Status list.

5. For each attribute value that you specify, select a search operator from the list. The following search operators are available:
  - Starts with
  - Ends with
  - Equals
  - Does not equal
  - Contains
  - Does not contain

The search operator can be combined with wildcard characters to specify a search condition. The asterisk (\*) character is used as a wildcard character. For example, you can specify the value of the User Login attribute to be Jo\* as the search criteria, and select Equals as the search operator. The users with login names that begins with Jo are displayed.

6. To add a searchable user attribute to the Manage Users page, click **Add Fields**, and select the attribute from the list of attributes.

For example, if you want to search all users with the Country attribute as US, then you can add the Country attribute as a searchable field and specify a search condition.

---

---

**Note:** You can configure the attributes that are searchable. The attributes available for search must be a subset of the attributes defined for the user entity that are marked with the Searchable = Yes property.

---

---

7. Optionally click **Reset** to reset the search conditions that you specified. Typically, you perform this step to remove the specified search conditions and specify a new search condition.
8. Click **Search**. The search results is displayed in a tabular format.
9. If you want to hide columns in the search results table, then perform the following steps:
  - a. Click **View** on the toolbar, select **Columns, Manage Columns**. The Manage Columns dialog box is displayed.
  - b. From the Visible Columns list, select the columns that you want to hide.
  - c. Click the left arrow icon to add the columns in the Hidden Columns list.
  - d. Click **OK**. The selected columns are not displayed in the search results. A status message displays along the bottom of the search table to identify how many columns are currently hidden. Figure shows that three columns are hidden:

#### 11.4.1.1 Operations on Search Results

This section describes the operations that you can perform based on selection of row(s) in the search results table. It is divided into single selection operations and bulk or multiple selection operations.

You can perform the following single selection operations by selecting a user from the search results table:

- View detail
- Modify, only if the user status is active
- Enable, only if the user status is disabled
- Disable, only if the user status is enabled
- Lock, only if the selected user's account is unlocked
- Unlock, only if the selected user's account is locked
- Reset password
- Delete

You can perform the following bulk or multiple selection operations by selecting multiple users from the search results table:

- Modify
- Enable, only if the user status is disabled
- Disable, only if the user status is enabled
- Lock, only if the selected user's account is unlocked
- Unlock, only if the selected user's account is locked
- Delete

---



---

**Note:** Operations can be direct or request-based that is subject to approval, based on the authorization privileges you have determined by the admin roles of the user.

---



---

## 11.4.2 Creating a User

You can create a new user in Oracle Identity Manager by using the Create User page. You can open this page only if you are authorized to create users as determined by the authorization policy on the Create User privilege on any organization in Oracle Identity Manager.

---



---

**Note:** The create user operation can be a direct operation or generate a request, which is subject to approval, based on the authorization privileges you have.

---



---

To create a user:

1. In Identity Self Service, under Administration, click **Users**. The Search Users page is displayed.
2. From the Actions menu, select **Create**. Alternatively, you can click **Create** on the toolbar. The Create User page is displayed with input fields for user profile attributes.
3. Enter details of the user in the Create User page. [Table 11–4](#) describes the fields in the Create User page:

**Table 11–4** *Fields in the Create User Page*

Section	Field	Description
Justification and Effective Date	Justification	Justification for creating the user.
	Effective Date	Date on which the user must be created.
Basic User Information	First Name	First name of the user.
	Middle Name	Middle name of the user.
	Last Name	Last name of the user.
	Email	E-mail address of the user.
	Manager	The reporting manager of the user.
	Organization	The organization to which the user belongs. This is also known as the home organization.
	User Type	The type of employee, such as consultant, contractor, contingent worker, employee, full-time employee, intern, non-worker, other, part-time employee, or temporary.
Account Settings	Display Name	It can have localized values, which can be added by clicking Manage Localizations, and selecting from a list of languages. Display Name is available in 33 languages.
	User Login	The user name to be specified for logging in to the Administration Console.

**Table 11–4 (Cont.) Fields in the Create User Page**

Section	Field	Description
	Password	The password to be specified for logging in to the Administration console.
	Confirm Password	Re-enter the password to be specified for logging in to the Administration console.
Account Effective Dates	Start Date	The date when the user will be activated in the system.
	End Date	The date when the user will be deactivated in the system.
Provisioning Dates	Provisioning Date	Date when user is getting provisioned into the system.
	Deprovisioning Date	Date when the user is getting deprovisioned from the system.
Contact Information	Telephone Number	The telephone number of the user.
	Home Phone	The telephone number of the user's residence.
	Home Postal Address	The postal address of the user's residence.
	Fax	The fax number of the user.
	Mobile	The mobile number of the user.
	Pager	The pager number of the user.
	Postal Address	The postal address of the user.
	Postal Code	The postal code number of the user's address.
	PO Box	The post box number of the user's address.
	State	The state name of the user.
	Street	The street name where the user resides.
	Country	The country where user resides.
Preferences	Locale	The locale code of the user.
	Timezone	The timezone of the user.
Other Attributes	Common Name	The common name of the user.
	Department Number	The department number of the user.
	Employee Number	The employee number of the user.
	Generation Qualifier	Whether the user qualifies the generation.
	Hire Date	The hiring date of the user.
	Locality Name	The name of the locality where user resides.
	Initials	The initials of the user.
	Title	The title for the user.

4. Click **Submit**. A message is displayed stating that the user is created successfully.

**Tip:** Users can be created by any one of the following methods:

- By using Oracle Identity Administration
- By self registration
- By using SPML Web service or APIs

For all the above methods, Oracle Identity Manager uses the default password policy or Password Policy against Default Rule. If you want to use a different password policy, then you must attach the new password policy to the default rule by using Oracle Identity System Administration. To do so, see "Managing Password Policies" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

### 11.4.3 Viewing User Details

The view user operation allows you to view detailed user profile information in the User Details page. You can open this page if you are authorized to view the user's profile as determined by the authorization policy through the View User Details privilege.

To display user details:

1. In Identity Self Service, under Administration, click **Users**. The Search Users page is displayed.
2. Search for the user for which you want to display the details.
3. In the search results table, click the user login name in the User Login column. The User Details page is displayed.

The user details are displayed in the following tabs:

- **The Attributes Tab:** Displays the attribute profile that includes details about basic user information, account effective dates, and provisioning dates. For more details, see "Editing User Attributes".

- **The Roles Tab:** Displays a list of roles to which the user belongs. You can click each role to display summary information about the role.

In the Roles tab, you can assign roles to the user and remove roles from the user. For more details, see "[Adding and Removing Roles](#)" on page 11-36.

- **The Entitlements Tab:** Displays a list of entitlements for the user. You can click each entitlement to display a summary of the entitlement.

In the Entitlements tab, you can request for entitlements and remove entitlements from the user. For more details, see "[Adding and Removing Entitlements](#)" on page 11-37.

- **The Accounts Tab:** Displays a list of accounts for the user. You can click each account to display a summary of the account.

Typical tasks you perform in this tab are request for an account, modify and remove accounts, mark an account as primary, and disable and enable accounts. For more details, see "[Modifying Accounts](#)" on page 11-37.

- **The Direct Reports Tab:** Displays a read-only table of users for whom the user is set as the manager. In other words, this tab lists the direct reportees of the user. For each user in the table, it displays the following:

- Display Name

- User Login
- Status
- Organization

If you select a row in the table, then summary information about the direct reportee is displayed at the bottom.

Direct reports allows you to open the user details of the direct reportees. To do so, select a row in the table of direct reportees, and click the open icon on the toolbar.

- **The Admin Roles Tab:** Displays a list of admin roles assigned to the user. You can select an admin role to display a summary of the admin role.

Using the admin role detail information, you can select or deselect the **include sub-orgs** option. When this option is selected, it specifies that the admin role is applicable to the users of the organization and all the suborganizations of the organization. When this option is not selected, it specifies that the admin role is applicable to the users of the organization only. See "[Managing Admin Roles](#)" on page 13-23 for more information.

## 11.4.4 Modifying Users

You can perform administrative user modification tasks from the user details. The modification is broken up across the different tabs in the page that displays user details, which means that modifications done in each tab are independent of each other and must be saved individually. The modifications you can perform in each tab is outlined in the following sections:

---



---

**Note:** The modify user operation can be a direct operation or generate a request, which is subject to approval, based on the authorization privileges you have.

---



---

- [Editing User Attributes](#)
- [Adding and Removing Roles](#)
- [Adding and Removing Entitlements](#)
- [Modifying Accounts](#)
- [Modifying Details of Direct Reports](#)

### 11.4.4.1 Editing User Attributes

To edit the attributes of a user:

1. In the Users section under Administration, search for the user for which you want to modify the attributes.
2. Select the user in the search results table.
3. Modify the user in one of the following ways:
  - Click **Edit** on the toolbar.
  - From the Actions menu, select **Edit**.
  - Click the user login of the user record that you want to disable. On the User Details page, click **Modify User** on the toolbar.

4. In the Modify User page, change values of the attributes in the respective fields as required.
5. Click **Submit**. The modify attribute operation is completed successfully.

#### 11.4.4.2 Adding and Removing Roles

In the Roles tab of the User Details page, you can add and remove roles. To assign roles for a user:

1. In the User Details page, click the **Roles** tab. The Roles tab is displayed with the list of roles assigned to the user.
2. From the Actions menu, select **Request**. Alternatively, you can click **Request Roles** on the toolbar. The Catalog page is displayed.
3. Click the search icon next to the Catalog field. A list of catalog items available for requesting is displayed.

---

---

**Note:** The catalog items that are available for requesting by a user is governed by authorization privileges defined for the admin roles of the user.

---

---

4. Select the catalog item for the role that you want to request.
5. Click **Add Selected to Cart**. The selected role catalog item is added to the request cart.
6. Click **Checkout**. The role will be assigned to the user when an approver approves the request.

You can edit the catalog item by clicking **View & Edit**.

To remove roles from a user:

1. In the User Details page, click the **Roles** tab. The Roles tab is displayed with the list of roles assigned to the user.
2. Select the role that you want to remove.
3. From the Actions menu, select **Remove**. Alternatively, you can click **Remove Roles** on the toolbar. The Catalog page is displayed.
4. Click the search icon next to the Catalog field. A list of catalog items available for requesting is displayed.

---

---

**Note:** The catalog items that are available for requesting by a user is governed by authorization privileges defined for the admin roles of the user.

---

---

5. Select the catalog item for the role that you want to remove.
6. Click **Add Selected to Cart**. The selected role catalog item is added to the request cart.
7. Click **Checkout**. The role is either removed immediately or a request is raised depending on authorization privileges granted to the user.

You can edit the catalog item by clicking **View & Edit**.

### 11.4.4.3 Adding and Removing Entitlements

To request entitlements for a user:

1. In the User Details page, click **Entitlements**. The Entitlements tab is displayed with the list of entitlements assigned to the user.
2. From the Actions menu, select **Request**. Alternatively, you can click **Request Entitlements** on the toolbar. The Catalog page is displayed.
3. Click the search icon next to the Catalog field. A list of catalog items available for requesting is displayed.

---

---

**Note:** The catalog items that are available for requesting by a user is governed by authorization privileges defined for the admin roles of the user.

---

---

4. Select the catalog item for the entitlement that you want to request.
5. Click **Add Selected to Cart**. The selected entitlement catalog item is added to the request cart.
6. Click **Checkout**. The entitlement will be assigned to the user when an approver approves the request.

You can edit the catalog item by clicking **View & Edit**.

To remove entitlements from a user:

1. In the User Details page, click **Entitlements**. The Entitlements tab is displayed with the list of entitlements assigned to the user.
2. Select the entitlement that you want to remove.
3. From the Actions menu, select **Remove**. Alternatively, you can click **Remove Entitlements** on the toolbar. The Catalog page is displayed.
4. Click the search icon next to the Catalog field. A list of catalog items available for requesting is displayed.

---

---

**Note:** The catalog items that are available for requesting by a user is governed by authorization privileges defined for the admin roles of the user.

---

---

5. Select the catalog item for the entitlement that you want to remove.
6. Click **Add Selected to Cart**. The selected entitlement catalog item is added to the request cart.
7. Click **Checkout**. The entitlement will be removed from the user when an approver approves the request.

You can edit the catalog item by clicking **View & Edit**.

### 11.4.4.4 Modifying Accounts

You can perform the following account modification operations from the Accounts tab of the User Details page:

- [Requesting for an Account](#)
- [Modifying an Account](#)

- [Removing an Account](#)
- [Marking an Account as Primary](#)
- [Disabling an Account](#)
- [Enabling an Account](#)

#### 11.4.4.4.1 Requesting for an Account

You can request accounts by requesting an application instance. You can request for the following types of accounts (application instances):

- **Primary account:** A primary account is the first account created for a user in a target application. In other words, a primary account is the first application instance that is being requested. Oracle Identity Manager supports multiple accounts for a single application instance. The first account that is created is tagged as primary account, and there can be only one primary account for a user. The other accounts (non-primary accounts) are associated with the primary account. When the user requests entitlements, the entitlements are appended to the primary account.
- **Non-primary account:** If a user already has a primary account and requests for another account in the same target application, then that account is a non-primary account. A user can have multiple non-primary accounts, but only one primary account.

**See Also:** "[Marking an Account as Primary](#)" on page 11-39 for more information on marking an account as primary

To request for an account:

1. In the User Details page, click the **Accounts** tab. This tab lists the accounts of the user.
2. From the Actions menu, select **Request**. Alternatively, click **Request Accounts** on the toolbar. The Catalog page is displayed.
3. Click the search icon next to the Catalog field. A list of catalog items available for requesting is displayed.

---

---

**Note:** The catalog items that are available for requesting by a user is governed by authorization privileges defined for the admin roles of the user.

---

---

4. Select the catalog item for the account that you want to request. In other words, select the application instance that you want to request.
5. Click **Add Selected to Cart**. The selected account catalog item is added to the request cart.
6. Click **Checkout**. The account will be granted to the user when an approver approves the request.

You can edit the catalog item by clicking **View & Edit**.

#### 11.4.4.4.2 Modifying an Account

To modify an account for the user:

1. In the Accounts tab, select the account that you want to modify.

2. From the Actions menu, select **Modify**. Alternatively, click **Modify Accounts** on the toolbar. The account details is displayed which is available for editing.
3. Edit the fields that you want to modify.
4. Click **OK**.

#### 11.4.4.3 Removing an Account

To remove an account from the user:

1. In the Accounts tab, from the Actions menu, select **Remove**. Alternatively, click **Remove Accounts** on the toolbar. The Catalog page is displayed.
2. Click the search icon next to the Catalog field. A list of catalog items available for requesting is displayed.

---

---

**Note:** The catalog items that are available for requesting by a user is governed by authorization privileges defined for the admin roles of the user.

---

---

3. Select the catalog item for the account that you want to remove.
4. Click **Add Selected to Cart**. The selected account catalog item is added to the request cart.
5. Click **Checkout**. The account will be removed from the user when an approver approves the request.

You can edit the catalog item by clicking **View & Edit**.

#### 11.4.4.4 Marking an Account as Primary

Oracle Identity Manager supports multiple accounts in a single application instance. The first account that is created is tagged as the primary account, and there can be only one primary account for a user. The other accounts (non-primary accounts) are associated with the primary account.

All types of entitlements are available for request in the request catalog. If the request for an entitlement is approved, it is associated with the primary account and not the non-primary account.

When the user gets provisioned to an application instance, Oracle Identity Manager checks if it is the first account provisioned for the user in that application instance. If so, the account is marked as primary. When existing user accounts are reconciled from application instances, the first account that gets reconciled is marked as primary.

A user can have only one primary account. However, Oracle Identity Manager supports multiple accounts for a single application instance. If the account marked as primary is not supposed to be the actual primary account, you can manually change the primary tag for the account and mark another account as primary. By doing so, you can ensure that when the user requests entitlements, the entitlements are appended to the primary account.

To mark an account as a primary account:

1. In the Accounts tab, select the account that you want to mark as primary.
2. From the Actions menu, select **Make Primary**. Alternatively, click **Make Primary** on the toolbar.

A message is displayed asking for confirmation.

3. Click **Yes** to confirm. The account is marked as primary.

#### 11.4.4.4.5 Disabling an Account

You can disable an account that is in enabled state. To disable an account:

1. In the Accounts tab, select the account that you want to disable.
2. From the Actions menu, select **Disable**. Alternatively, click **Disable** on the toolbar.  
A message is displayed asking for confirmation.
3. Click **Yes** to confirm. The account is disabled.

#### 11.4.4.4.6 Enabling an Account

You can enable an account that is in disabled state. To enable an account:

1. In the Accounts tab, select the account that you want to enable.
2. From the Actions menu, select **Enable**. Alternatively, click **Enable** on the toolbar.  
A message is displayed asking for confirmation.
3. Click **Yes** to confirm. The account is enabled.

#### 11.4.4.5 Modifying Details of Direct Reports

The modify the details of direct reports:

1. In the User Details page, click the **Direct Reports** tab. This tab lists the direct reports of the open user.
2. Select the user or direct report you want to modify.
3. Click the edit icon on the toolbar. The User details page of the selected direct report is displayed. Use the toolbar and tabs to modify the details of the direct report.

### 11.4.5 Disabling a User

To disable a user that is in enabled state:

1. In the Users section under Administration, search for and select the user you want to disable.
2. Disable the user in one of the following ways:
  - Click **Disable** on the toolbar.
  - From the Actions menu, select **Disable**.
  - Click the user login of the user record that you want to disable. On the User Details page, click **Disable User** on the toolbar.
3. In the Target Users section, click the plus icon to search for more target users and add to the list of users that you want to disable. You can also view the user details by clicking the **User Details** link for each user.
4. In the Justification and Effective Date section, specify a justification and effective date for disabling the selected user.
5. Click **Submit**. A message is displayed stating that the user is successfully disabled.

## 11.4.6 Enabling a User

To enable a disabled user:

1. In the Users section under Administration, search for and select the user you want to enable.
2. Enable the user in one of the following ways:
  - Click **Enable** on the toolbar.
  - From the Actions menu, select **Enable**.
  - Click the user login of the user record that you want to enable. On the User Details page, click **Enable User** on the toolbar.
3. In the Target Users section, click the plus icon to search for more target users and add to the list of users that you want to enable. You can also view the user details by clicking the **User Details** link for each user.
4. In the Justification and Effective Date section, specify a justification and effective date for enabling the selected user.
5. Click **Submit**. A message is displayed stating that the user is successfully enabled.

## 11.4.7 Deleting a User

To delete a user:

1. In the Users section under Administration, search for and select the user you want to delete.
2. Delete the user in one of the following ways:
  - Click **Delete** on the toolbar.
  - From the Actions menu, select **Delete**.
  - Click the user login of the user record that you want to delete. On the User Details page, click **Delete User** on the toolbar.
3. Verify that the selected user is displayed in the Target Users section.
4. If required, in the Target Users section, click the plus icon to search for more target users and add to the list of users that you want to delete. You can also view the user details by clicking the **User Details** link for each user.
5. In the Justification field, enter a justification for deleting the user.
6. In the Effective Date field, specify a date from which the user account must be removed.
7. Click **Submit**. A request to delete the user is created, which is subject to approval.

## 11.4.8 Locking an Account

To lock the account of a user:

1. In the Users section under Administration, search for and select the user you want to lock.
2. Lock the user in one of the following ways:
  - Click **Lock Account** on the toolbar.
  - From the Actions menu, select **Lock Account**.

- Click the user login of the user record that you want to lock. On the User Details page, click **Lock Account** on the toolbar.
3. In the confirmation message that is displayed, click **Lock**. The account of the selected user is locked.

### 11.4.9 Unlocking an Account

To unlock the account of a user:

1. In the Users section under Administration, search for and select the user you want to unlock.
2. Unlock the user in one of the following ways:
  - Click **Unlock Account** on the toolbar.
  - From the Actions menu, select **Unlock Account**.
  - Click the user login of the user record that you want to unlock. On the User Details page, click **Unlock Account** on the toolbar.
3. In the confirmation message that is displayed, click **Unlock**. The account of the selected user is unlocked.

## 11.5 Username Reservation

When the request for user creation is submitted, the following scenarios are possible:

- While the request is pending, another create user request is submitted with the same username. If the second request is approved and the user is created, then the first request, when approved, fails because the username already exists in Oracle Identity Manager.
- While the request is pending, another user with the same username is directly created in the LDAP identity store. When the create user request is approved, it fails while provisioning the user entity to LDAP because an entry already exists in LDAP with the same username.

To avoid these problems, you can reserve the username in both Oracle Identity Manager and LDAP while the create user request is pending for approval. If a request is created to create a user with the same username, then an error message is displayed and the create user request is not created.

---

---

**See Also:** ["Creating Requests"](#) on page 9-15 for information about creating requests to create a user

---

---

For reserving the username:

- The USER ATTRIBUTE RESERVATION ENABLED system property must be set to TRUE for the functionality to be enabled. For information about searching and modifying system properties, see "Managing System Properties" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.
- Reservation in LDAP is done only if reservation functionality is enabled, and LDAP is in sync with Oracle Identity Manager database. For information about synchronization between Oracle identity Manager and LDAP identity store, see "Integration Between LDAP Identity Store and Oracle Identity Manager" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

---

---

**Note:**

- If LDAP provider is not configured, then the reservation is done only in Oracle Identity Manager.
  - When LDAP synchronization and user attribute reservation features are enabled, it is recommended to enable UID uniqueness in the directory server. Without this, user reservation in the directory does not work properly because while the user is reserved in the reservation container, the user with the same user ID can be created in the user container. This results in user creation failure when Oracle Identity Manager tries to move the user from the reservation container to the user container.
- 
- 

If user attribute reservation is enabled, the reservation happens in two phases:

In the first phase, an entry is created in Oracle Identity Manager database and a user is created in reservation container. This entry in Oracle Identity Manager database is removed after successful creation of user, rejection by approver, or request failure.

In the second phase, in LDAP, on successful creation, the user is moved to the reservation container. In other cases such as rejection by approver or request failure, the user is removed from the reservation container.

After the request-level and operation-level approvals are obtained for the create user request, the username is no longer reserved in the username container in LDAP. The username is moved to the container in which the existing users are stored. The user is also created in Oracle Identity Manager.

This section consists of the following topics:

- [Enabling and Disabling Username Reservation](#)
- [Configuring the Username Policy](#)
- [Writing Custom User Name Policy](#)
- [Releasing the Username](#)
- [Configuring Username Generation to Support Microsoft Active Directory](#)

## 11.5.1 Enabling and Disabling Username Reservation

The username reservation functionality is enabled by default in Oracle Identity Manager. This is done by keeping the value of the USER ATTRIBUTE RESERVATION ENABLED system property to TRUE. You can verify the value of this system property in the System Configuration section of the Oracle Identity Manager System Administration Console.

To disable username reservation:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **System Configuration**. The Advanced Administration opens in a new window.
3. In the left pane, click the search icon to search for all existing system properties. A list of system properties are displayed in the search results table.
4. Click **User Attribute Reservation Enabled**. The System Property Detail page for the selected system property is displayed, as shown in [Figure 11-2](#):

**Figure 11–2 The System Property Detail Page**

The screenshot shows a web browser window titled 'System Property Detail: User Attribute Reservation Enabled'. The page contains a form with the following fields:

- \* Key: 53
- \* Property Name: User Attribute Reservation Enabled
- \* Keyword: XL.IsUsrAttribReservEnabled
- \* Value: TRUE
- Log In Required:

There are two 'Save' buttons: one in the top right corner and one at the bottom right of the form area.

5. In the Value field, enter **False**.
6. Click **Save**. The username reservation functionality is disabled.

## 11.5.2 Configuring the Username Policy

Username Policy is a plugin implementation for username operations such as username generation and username validation. You can change the default policies from the System Configuration section in Oracle Identity System Administration.

In case of a Create User usecase, the plugins are invoked only if the user login is not provided. In such a case, the plugin to be invoked is picked up from the system property, "Default policy for username generation".

Table 11–5 lists the predefined username policies provided by Oracle Identity Manager. In this table, the dollar (\$) sign in the username generation indicates random alphabet:

**Table 11–5 Predefined Username Policies**

Policy Name	Expected Information	Username Generated
oracle.iam.identity.usermgmt.impl.plugins.EmailIDPolicy	E-mail	E-mail value is used as the auto-generated user name
oracle.iam.identity.usermgmt.impl.plugins.LastNameFirstInitialLocalePolicy	First name, last name, and locale	last name + first initial_locale, last name + middle initial + first initial_locale, last name + \$ + first initial_locale (all possibilities of single random alphabets), last name + \$\$ + first initial_locale
oracle.iam.identity.usermgmt.impl.plugins.FirstInitialLastNameLocalePolicy	Firstname, Lastname, Locale	first initial + lastname_locale, first initial + middle initial + first name_locale, first initial + \$ + lastname_locale, first initial + \$\$ + lastname_locale
oracle.iam.identity.usermgmt.impl.plugins.LastNameFirstInitialPolicy	Firstname, Lastname	lastname+firstInitial, lastname+middleinitial+firstInitial, lastname+\$+firstInitial ( all possibilities of single random alphabets) , lastname+\$\$+firstInitial
oracle.iam.identity.usermgmt.impl.plugins.FirstInitialLastNamePolicy	Firstname, Lastname	firstInitial+lastname, firstInitial+middleInitial+firstname, firstInitial+\$+lastname, firstInitial+\$\$+lastname

**Table 11–5 (Cont.) Predefined Username Policies**

Policy Name	Expected Information	Username Generated
oracle.iam.identity.usermgmt.impl.plugin.LastNameFirstNamePolicy	Firstname, Lastname	lastname.firstname, lastname.middleinitial.firstname, lastname.\$.firstname ( all possibilities of single random alphabets) , lastname.\$\$.firstname
oracle.iam.identity.usermgmt.impl.plugin.FirstNameLastNamePolicy	Firstname, Lastname	firstname.lastname, firstname.middleinitial.lastname, firstname.\$.lastname (all possibilities of single random alphabets) , firstname.\$\$.lastname
oracle.iam.identity.usermgmt.impl.plugin.DefaultComboPolicy	Any one of the following: - Email - Firstname, Last Name - Last name.	If e-mail is provided, then username is generated based on the e-mail. If e-mail is not available, then it generates username based on firstname and lastname by appending a user domain to it. If first name is not available, then it generates the username based of the last name only by appending a user domain to it.  The user domain is configured as the Default user name domain system property, and the default value is @oracle.com
oracle.iam.identity.usermgmt.impl.plugin.LastNamePolicy,	Lastname	lastname, middle initial + lastname , \$ + lastname, \$\$ + lastname
oracle.iam.identity.usermgmt.impl.plugin.LastNameLocalePolicy	Lastname, Locale	lastname_locale, middle initial + lastname_locale , \$ + lastname_locale, \$\$ + lastname_locale
oracle.iam.identity.usermgmt.impl.plugin.FirstNameLastNamePolicyForAD	Firstname, Lastname	firstname+lastname, substring of firstname+lastname+\$, substring of firstname+ substring of lastname+\$
oracle.iam.identity.usermgmt.impl.plugin.LastNameFirstNamePolicyForAD	Lastname, Firstname	lastname+firstname, lastname+substring of firstname+\$, substring of lastname+ substring of firstname+\$

The policy implementations generate the username, check for its availability, and if the username is not available, then generate other username based on the policy in the order mentioned in [Table 11–5](#), and repeat the procedure. The dollar (\$) sign in the username generation indicates random alphabet. If any of the expected information is missing, then the policies generate errors.

Values must be provided for all the parameters of the username generation format. If any of the parameters are not provided, then Oracle Identity Manager generates an error. For example, If the `firstname.lastname` policy is configured and the `firstname` is not provided, then the error would be "An error occurred while generating the Username. Please provide `firstname` as expected by the `firstname.lastname` policy".

The username generation is exposed as public APIs in User Manager. Oracle Identity Manager provides an utility class for accessing the functionality of generating user names. The class that contains utility methods is as shown:

```
oracle.iam.identity.usermgmt.api.UserManager
```

The `UserManager` class exposes the following public API for username generation and validation:

```
//Method that will generate username based on default policy

    public String generateUserNameFromDefaultPolicy(Map<String, Object> attrMap)
        throws UserNameGenerationException, UserManagerException;

//Method that will generate username based on policy

    public String generateUserNameFromPolicy(String policyId, Map<String, Object>
attrMap) throws UserNameGenerationException, UserManagerException;

//Method that will check whether username is valid against default policy

    public boolean isUserNameValidForDefaultPolicy(String userName, Map<String,
Object> attrMap) throws UserManagerException;

//Method that will check whether username is valid against given policy

    public boolean isUserNameValidForPolicy(String userName, String policyId,
Map<String, Object> attrMap) throws UserManagerException;

//Method to return all policies (including customer written)

    public List<Map<String, String>> getAllUserNamePolicies(Locale locale)

//Method that will return policy description in given locale

    public String getPolicyDescription(String policyID, Locale locale)
```

[Table 11–6](#) lists the constants defined in the `UserManager` class to represent the policy ID of the default username policies:

**Table 11–6 Constants Representing Policy IDs**

Policy Name	Constant
EmailIDPolicy	EMAIL_ID_POLICY
LastNameFirstInitialLocalePolicy	FIRSTNAME_LASTNAME_POLICY
FirstInitialLastNameLocalePolicy	LASTNAME_FIRSTNAME_POLICY
LastNameFirstInitialPolicy	FIRSTINITIAL_LASTNAME_POLICY
FirstInitialLastNamePolicy	LASTNAME_FIRSTINITIAL_POLICY
LastNameFirstNamePolicy	FIRSTINITIAL_LASTNAME_LOCALE_POLICY
FirstNameLastNamePolicy	LASTNAME_FIRSTINITIAL_LOCALE_POLICY
DefaultComboPolicy	DEFAULT_COMBO_POLICY
LastNamePolicy	LASTNAME_POLICY
LastNameLocalePolicy	LASTNAME_LOCALE_POLICY
FirstNameLastNamePolicyForAD	FIRSTNAME_LASTNAME_POLICY_FOR_AD
LastNameFirstNamePolicyForAD	LASTNAME_FIRSTNAME_POLICY_FOR_AD

When called to generate username, the policy classes expect the attribute values to be set in a map by using the key constants defined in the `oracle.iam.identity.utils.Constants` class. This means that a proper parameter value must be passed to call the method by using the appropriate constant defined for it, for example, the `FirstName` parameter has a constant defined for it.

The default username policy can be configured by using the Oracle Identity System Administration. To do so:

1. Navigate to the System Configuration section.
2. Search for all the system properties.
3. Click **Default policy for username generation**. The System Property Detail page for the selected property is displayed, as shown in [Figure 11-3](#):

**Figure 11-3 The Default Username Policy Configuration**

The screenshot shows a web browser window titled "System Property Detail: Default policy for username generation". The page content includes the following fields:

- \* Key:
- \* Property Name:
- \* Keyword:
- \* Value:
- Log In Required:

There are "Save" buttons in the top right and bottom right corners of the form area.

The `XL.DefaultUserNameImpl` system property is provided for picking up the default policy implementation. By default, it points to the default username policy, which is `oracle.iam.identity.usermgmt.impl.plugins.DefaultComboPolicy` displayed in the Value field.

4. In the Value field, enter **`oracle.iam.identity.usermgmt.impl.plugins.POLICY`**. Here, *POLICY* is one of the policy implementations.

---

**Note:** All the plug-ins must be registered with Oracle Identity Manager by using the `/identity/metadata/plugin.xml` file. A sample `plugin.xml` file is as shown:

```
<plugins
  pluginpoint="oracle.iam.identity.usermgmt.api.UserNamePolicy">
  <plugin
    pluginclass="oracle.iam.identity.usermgmt.impl.plugins.LastNameFirs
tNamePolicy"
    version="1.0" name="LastNameFirstNamePolicy"/>
  </plugins>
```

---

5. Click **Save**.

### 11.5.3 Writing Custom User Name Policy

You can write your own policies by adding new plug-ins and changing the default policies from the System Configuration section in Oracle Identity System Administration.

**See Also:** "Developing Plug-ins" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about the plug-in framework

The UserManager exposes APIs for username operations. The APIs take the user data as input and return a generated username. The APIs make a call to plug-ins that return the username. This allows you to replace the default policies with custom plug-ins with your implementation for username operations.

---

---

**Note:**

- For user name generation and validation, public APIs are exposed in UserManager.
  - While creating the policy, ensure that the attributes used in generating the username are defined in the request data set. For information about request data set, see the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
- 
- 

You can write your own username policies by implementing the plug-in interface, as shown:

```
package oracle.iam.identity.usermgmt.api;

public interface UserNameGenerationPolicy extends
    oracle.iam.identity.usermgmt.api.UserNamePolicy {
    public String getUsername(Map<String, Object> reqData) throws
        UserNameGenerationException;
    public boolean isGivenUserNameValid(String userName, Map<String, Object> reqData);

    //methods inherited from old user name policy interface
    //oracle.iam.identity.usermgmt.api.UserNamePolicy
    public String getUsernameFromPolicy(HashMap<String, String> reqData) throws
        UserNameGenerationException;
    public boolean isUserNameValid(String userName, HashMap<String, String> reqData);
    public String getDescription(Locale locale);
}
```

This plug-in point is exposed as a kernel plug-in that takes request data as input and returns the username. Each plug-in expects some information and generates username based on that information provided.

---

**Note:** Oracle Identity Manager provides an abstract implementation of the `oracle.iam.identity.usermgmt.api.UserNameGenerationPolicy` interface as the `oracle.iam.identity.usermgmt.api.AbstractUserNameGenerationPolicy` class name. Therefore, you need not implement the following two methods:

```
public String getUserFromPolicy(HashMap<String, String>
reqData) throws UserNameGenerationException;

public boolean isUserNameValid(String userName, HashMap<String,
String> reqData);
```

---

All the plug-ins must be registered with Oracle Identity Manager by using the `/identity/metadata/plugin.xml` file. A sample `plugin.xml` file is mentioned below:

```
<plugins pluginpoint="oracle.iam.identity.usermgmt.api.UserNamePolicy">
<plugin
pluginclass="oracle.iam.identity.usermgmt.impl.plugins.CustomDepartmentNumberEmplo
yeNumberPolicy "
version="1.0" name="CustomDepartmentNumberEmployeeNumberPolicy"/>
</plugins>
```

The following are the guidelines on while writing custom user name policies:

- Policies should implement the new interface `oracle.iam.identity.usermgmt.api.UserNameGenerationPolicy`.
- Custom user name policies must be re-entrant. This means that the custom code in the policy should return the same user login if approver has updated an attribute that does not contribute in generating the user login.

For sample implementation please refer below:

```
package oracle.iam.identity.usermgmt.impl.plugins;

import java.util.Locale;
import java.util.Map;

import oracle.iam.identity.exception.UserNameGenerationException;
import oracle.iam.identity.usermgmt.api.AbstractUserNameGenerationPolicy;
import oracle.iam.identity.usermgmt.api.UserManagerConstants;
import oracle.iam.identity.usermgmt.api.UserNameGenerationPolicy;

public class CustomDepartmentNumberEmployeeNumberPolicy extends
AbstractUserNameGenerationPolicy implements UserNameGenerationPolicy {

    private String departmentNumberKey =
UserManagerConstants.AttributeName.DEPARTMENT_NUMBER.getId();

    private String employeeNumberKey =
UserManagerConstants.AttributeName.EMPLOYEE_NUMBER.getId();

    @Override
    public String getUserName(Map<String, Object> reqData)
        throws UserNameGenerationException {

        String departmentnumber = reqData.get(departmentNumberKey) == null ?
null : reqData.get(departmentNumberKey).toString();
```

```
        String employeeNumber = reqData.get(employeeNumberKey) == null ? null :
reqData.get(employeeNumberKey).toString();

        // Required in case of approver edit. If approver has not modified any
attribute which contributes in user name generation , then return same old user
login

        //Check if user data is not changed using checkForSameUserLogin method
present in AbstractUserNameGenerationPolicy, then return same user login

        //OR use Map<String, Object> existingData = (Map<String, Object>)
reqData.get(oracle.iam.identity.usermgmt.api.UserManagerConstants.EXISTING_DATA )
to implement your own comparison logic

        // If existingData is NULL, it means generate a new user login. If it is
not NULL, then it means policy is invoked during approver edit.

        // If it is NOT NULL, Compare value of participating attributes from
existingData and reqData. If same, return same user login as present in
existingData ; otherwise generate a new user login.

        String oldUserLogin = checkForSameUserLogin(reqData , new
String[]{departmentNumberKey , employeeNumberKey});
        if(oldUserLogin!=null)
            return oldUserLogin;

        // TODO: DO basic validations. Also, Ensure newly generated user
name is unique and not reserved. You may use utility methods in
oracle.iam.identity.usermgmt.utils.UserNamePolicyUtil for preforming validations.
        return departmentnumber + "-" + employeeNumber;
    }

    @Override
    public boolean isGivenUserNameValid(String userName, Map<String, Object>
reqData) {
        // TODO : custom implementation
        return true;
    }

    @Override
    public String getDescription(Locale locale) {
        return "User Name Generation Policy using department number and
employee number";
    }
}
```

## 11.5.4 Releasing the Username

The username is released in the following scenarios:

- When the request is approved, and the user is successfully created in Oracle Identity Manager and provisioned to LDAP, and the username from the reserved table is removed. The reserved username is removed after successful user creation after the approvals. The reserved entry in LDAP is removed and the actual user is created.

- If the request is rejected, then the reserved entry of username in LDAP and Oracle Identity Manager is removed.
- If the request fails while or before creating a user in Oracle Identity Manager or LDAP, then the reserved username is deleted.

### 11.5.5 Configuring Username Generation to Support Microsoft Active Directory

In Oracle Identity Manager deployment with LDAP synchronization is enabled, where Microsoft Active Directory (AD) is the data store, the User Login attribute in Oracle Identity Manager is mapped to the uid attribute in LDAP, which in turn is mapped to the sAMAccountName attribute. The sAMAccountName attribute is used as login for all AD-based applications. There is a limitation on the maximum length supported for value contained in the sAMAccountName attribute in AD. It cannot exceed 20 characters.

Oracle Identity Manager accepts user name as an input at the time of user creation and it can be more than 20 characters. Because AD does not support user name of more than 20 characters, Oracle Identity Manager can be configured to generate the user name, which consists of less than 20 characters.

When AD is used as data store, you can configure the autogeneration of user name by setting the value of the XL.DefaultUserNamePolicyImpl system property to any one of the following:

- **FirstNameLastNamePolicyForAD:** Generates the user login by prefixing a substring from the first name to that of the last name
- **LastNameFirstNamePolicyForAD:** Generates the user login by prefixing a substring from last name to that of the first name

See "Administering System Properties" for information about the XL.DefaultUserNamePolicyImpl system property and setting values of system properties.

---



---

**Note:** If AD is the data store, then any one of the FirstNameLastNamePolicyForAD or LastNameFirstNamePolicyForAD policies must be used. Any other user name generation policy will fail to generate the user name.

---



---

## 11.6 Common Name Generation

The generation of the Common Name user attribute value in Oracle Identity Manager is described in the following sections:

- [Common Name Generation for Create User Operation](#)
- [Common Name Generation for Modify User Operation](#)

### 11.6.1 Common Name Generation for Create User Operation

In an LDAP-enabled deployment of Oracle Identity Manager, Fusion applications such as Human Capability Management (HCM) does not pass the common name via SPML request. Given that the common name is a mandatory attribute in LDAP and Oracle Identity Manager is setup to use it as the RDN, Oracle Identity Manager must generate a unique common name.

Based on the description on Common Name, it is the user's display name consisting of first name and last name. Therefore, Oracle Identity Manager generates the Common

Name with the help of a common name generation policy that specifies the Common Name in the "firstname lastname" format.

To configure common name generation in Oracle Identity Manager, set the value of the `XL.DefaultCommonNamePolicyImpl` system property to `oracle.iam.identity.usermgmt.impl.plugins.FirstNameLastNamePolicy`. For information about the `XL.DefaultCommonNamePolicyImpl` system property and setting the value of a system property, see "Managing System Properties" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

The following are the details of the `FirstNameLastNamePolicy`:

- Expected information: Firstname, Lastname
- Common Name generated: `firstname.lastname`, `firstname.$.lastname` (all possibilities of single random alphabets), `firstname.$$lastname` and so on until a unique common name is generated

---

---

**Note:** The common name must be reserved until the user is created by the request so that multiple requests generated simultaneously having same first and last names do not generate the same common name.

---

---

## 11.6.2 Common Name Generation for Modify User Operation

When the user profile is modified, one or more attributes can change. HCM cannot filter out and send only the modified data to Oracle Identity Manager because it does not have the old user attributes and cannot determine which ones are modified. Therefore, all attributes including the common name (CN) are passed to Oracle Identity Manager by the SPML request. Because the CN changed, Oracle Identity Manager attempts a modify operation (`modrdn`) in the directory resulting in DN change. Because of this unintended DN change, the group membership DN becomes stale resulting in the user losing membership in that group. This subsequently results in authorization failure. This happens when referential integrity is turned off in the LDAP server, and therefore, the referenced groups are not updated when the RDN of the user changes. Therefore, referential integrity must be turned on in the target LDAP server. Otherwise, the group memberships become stale. The referential integrity issue is also applicable to roles. Groups are also members of other groups and any RDN changes must be reflected as well.

You can turn on the referential integrity by setting the value of the `XL.IsReferentialIntegrityEnabled` system property to `TRUE`. For information about this system property, see "Managing System Properties" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

[Table 11-7](#) lists the possible scenarios when RDN is modified:

**Table 11–7 RDN Modification Scenarios**

<b>Referential Integrity in LDAP</b>	<b>XL.IsReferentialIntegrity Enabled</b>	<b>Result of Modify Operation (modrdn)</b>
Disabled	FALSE	Oracle Identity Manager generates an error and operation fails.
Disabled	TRUE	Modify operation passes from Oracle Identity Manager and RDN is changed in LDAP. However, the group references are not updated and are stale. This configuration is not recommended.
Enabled	FALSE	Oracle Identity Manager generates an error and modify operation fails. This property must be set to TRUE in Oracle Identity Manager because referential integrity is enabled in LDAP.
Enabled	TRUE	Modify operation passes and RDN is updated. In addition, the references for the DN are updated in LDAP.
Multiple directories with roles and users stored in separate directories. Referential integrity property is not relevant here.	FALSE	Modify operation fails from Oracle Identity Manager. This is not supported by LDAP. Therefore, FALSE is the recommended value in Oracle Identity Manager for the property.
Multiple directories with roles and users stored in separate directories. Referential integrity property is not relevant here.	TRUE	Modify operation passes and RDN is modified. However, because LDAP does not support referential integrity in multiple directories, the group references are stale and must be manually updated.



---

---

## Managing Roles

You use roles to create and manage the records of a collection of users to whom you want to permit access to common functionality, such as access rights, roles, or permissions.

Roles can be independent of an organization, span multiple organizations, or contain users from a single organization.

Using roles, you can:

- Assign users to roles.
- Assign a role as a parent role to an existing role.
- Designate provisioning policies for a role. These policies determine if a resource object is to be provisioned to or requested for a member of the role.
- Assign or remove membership rules to or from the role. These rules determine which users can be assigned or removed as direct membership to or from the role.
- Map users (via roles) to access policies for automating the provisioning of target systems to the users. See "Managing Access Policies" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for details.
- Publish or unpublish roles to organizations.
- View the menu items that the users can access through Oracle Identity Manager Administration Web interface.

This chapter describes roles and functionalities related to roles in the following sections:

- [Role Membership Inheritance](#)
- [Role Permission Inheritance](#)
- [Role Entity Definition](#)
- [Default Roles](#)
- [Role Management Tasks](#)
- [Request-Based Role Grants](#)

### 12.1 Role Membership Inheritance

Membership inheritance means that the members of the inheritor role inherit from the inherited role. For example:

---

---

**Note:** The role that inherits membership is called the member-inheritor role. The role from which the member-inheritor role inherits membership is called the inherited-member role

---

---

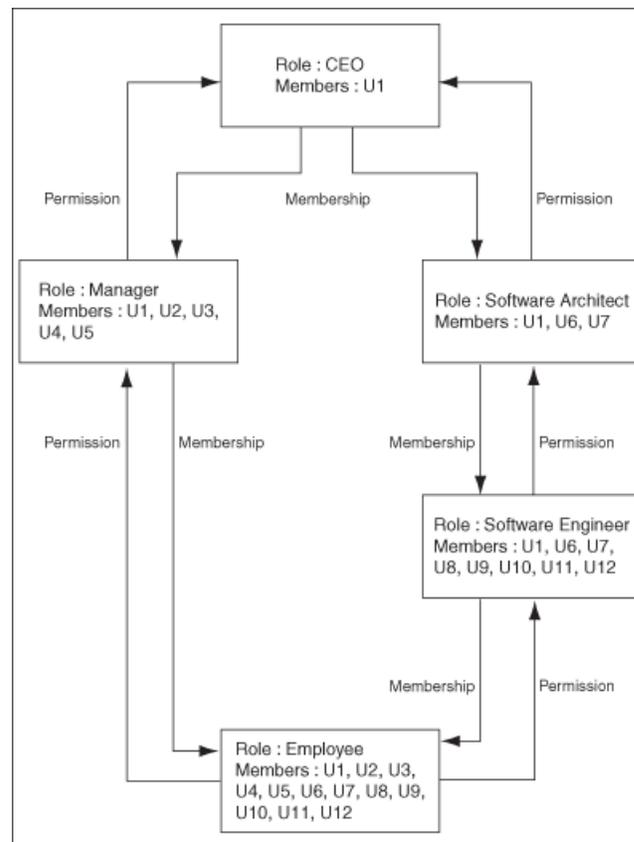
- Role B inherits memberships from Role A. Role B is the member-inheritor role to Role A.
- Role C also inherits memberships from Role A. Role C is also a member-inheritor role of Role A.

In this example, all members of Role A are also implicit or indirect members of Role B and Role C, but members of Role B are not automatically members of Role A. In other words, Roles B and C are the member-inheritor roles of Role A, and Role A is the inherited-member role of Role B and Role C. A real example for this is that the Employee Role (Role B) inherits memberships from the Manager Role (Role A).

Role membership inheritance is described with the help of the following scenario:

- The role of CEO is an inherited-member role of the Manager role, as a list of managers will include the CEO role.
- The role Manager is an inherited-member role of the Employee role.
- The role Software Architect is an inherited-member role of the Software Engineer role.
- The role Software Engineer is an inherited-member role of the Employee role.
- The Employee role has two inherited-member roles - the Manager role and the Software Engineer role.

Figure 12-1 shows the parent and child roles in this example, along with the membership inheritance:

**Figure 12–1 Role Membership and Permission Inheritance**

Each user in an inherited-member role automatically becomes a member in any of its member-inheritor roles. If that member-inheritor role is itself an inherited-member role, then the user is also added to its member-inheritor roles, and so on. This continues until there are no more member-inheritor roles in the inheritance chain. For example, a CEO is a manager and is automatically a member of the Manager role. Similarly, a manager is automatically an employee. This is why a member added to an inherited-member role gets inherited by its member-inheritor roles, and so on. This explains why the direct membership of the Employee role is empty, and considering membership inheritance, the Employee role has more members than all other roles.

A user can be a member of a role in one of the following ways:

- The member has been inherited from the inherited-member role, which is called indirect membership.
- The user is directly assigned to the role (by using membership rules), which is called direct membership.

An indirect member can be assigned as a direct member as well. If a user's direct membership in a role is revoked, the user is still a member of that role because of inheritance.

## 12.2 Role Permission Inheritance

Permission inheritance means that the permissions of the inheritor role inherit from the inherited role. For example:

- Role B inherits permissions from Role A.

- Role C also inherits permissions from Role A.

In this example, Role B and Role C are permissions-inheritor roles of Role A. In the Hierarchy tab, this relationship is denoted by "child" - Role B and Role C are the children of Role A. Similarly, Role A is the inherited-permissions role of Role B and Role C. In the Hierarchy tab, Role A is the "parent" of Role B and Role C.

A real example for this is that the Manager role inherits permissions from the Employee role.

Oracle Identity Self Service represents role permission inheritance through the following sections in the Hierarchy tab:

**See Also:** ["The Hierarchy Tab"](#) on page 12-13 for more information about the Hierarchy tab

- **Inherited From:** Displays the parent roles from which the open role is inherited. The base role has the same permissions and privileges on the members as the inherited roles. Only inherited roles can be added or removed from the base role, but the base role cannot be added or removed from the inherited role.
- **Inherited By:** Lists the child roles that are inherited by the open role. This is a read-only display of the roles. You can use the Open Role action to modify the relationship from the base role.

For example, you create three roles: role1, role2, and role3. Open role3 and assign role2 as the parent role. Similarly, open role2 and assign role1 as the parent role. When you open role3, the Inherited From section displays the role2 parent role, and role1 is displayed under role2. When you open role1, the Inherited By section displays the role2 child role, and role3 is displayed under role2.

[Figure 12-1](#) illustrates that a permission on Employee is a permission that a Manager will have. Similarly, a permission a Manager will have is a permission a CEO will have. And this is why permissions inherit upwards. In addition, a parent role can inherit permissions from multiple child roles. For example, a CEO inherits the permissions of the Manager and Software Architect roles. Therefore, membership inheritance and permission inheritance go in different directions.

## 12.3 Role Entity Definition

Attributes are defined for the role entity in Oracle Identity Manager. These attributes are the same for all entities, such as user, organization, role, role hierarchy, and role membership. For a list of attributes defined for the entities, see ["User Entity Definition"](#) on page 11-3.

---

---

**Note:** You cannot add your own attributes for the role entity.

---

---

This section describes the default attribute definition of the following entities:

- [Role Entity](#)
- [Role Category Entity](#)
- [Role Grant Relationship](#)
- [Role Parent Relationship](#)
- [Role Organization Relationship](#)

### 12.3.1 Role Entity

The Role.xml file contains the attribute definition for the role entity. You can add your own attributes to the role entity.

Attributes of an entity associated with a role can be made available through the Role API, when retrieving role details. This can be done without incurring the cost of an additional API call to retrieve the joined entity. Examples of these attributes are configured out-of-the-box in Role.xml, where the parameters with names beginning 'foreign\_search\_' collectively make available the attributes 'Role Category Name', 'Owner First Name', 'Owner Last Name', 'Owner Display Name', 'Owner Email', and 'Owner Login'.

Note that the role entity definition contains the entity keys (Role Category Key and User Key), which enable these 'additional' attributes to be provided.

Table 12-1 lists the default attributes for the role entity.

**Table 12-1 Default Attributes for the Role Entity**

Attribute Name	Category	Type	Data Type	Properties	LOV
Role Key	Basic	Single	Numeric	Required: Yes System-Can-Default: Yes System-Controlled: Yes Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA
Role Unique Name	Basic	Single	Text	Required: Yes System-Can-Default: Yes System-Controlled: Yes Encryption: Clear User- searchable: No Bulk-Updatable: No	NA
Role Display Name	Basic	Single	Text (multi-langua ge)	Required: Yes System-Can-Default: Yes System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA
Role Namespace	Basic	Single	Text	Required: Yes System-Can-Default: Yes System-Controlled: Yes Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA

**Table 12–1 (Cont.) Default Attributes for the Role Entity**

<b>Attribute Name</b>	<b>Category</b>	<b>Type</b>	<b>Data Type</b>	<b>Properties</b>	<b>LOV</b>
Role Name	Basic	Single	Text (multi-language)	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA
Role Description	Basic	Single	Text (multi-language)	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA
LDAP GUID	LDAP	Single	Text	Required: Yes System-Can-Default: No System-Controlled: Yes Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA
LDAP DN	LDAP	Single	Text	Required: Yes System-Can-Default: No System-Controlled: Yes Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA

**Table 12–1 (Cont.) Default Attributes for the Role Entity**

Attribute Name	Category	Type	Data Type	Properties	LOV
Role Category Key	Basic	Single	Reference to role category	Required: Yes System-Can-Default: Yes System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes	NA
Role Owner Key	Basic	Single	Reference to Role Owner	Required: Yes System-Can-Default: Yes System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: Yes	NA
Role Email	Basic	Single	Text	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA

### 12.3.2 Role Category Entity

The RoleCategory.xml file contains the attribute definition for the role category entity. You cannot add your own attributes to the role category entity.

[Table 12–2](#) lists the default attributes for the role category entity.

**Table 12–2 Default Attributes for the Role Category Entity**

Attribute Name	Category	Type	Data Type	Properties	LOV
Role Category Key	Basic	Single	Text	Required: Yes System-Can-Default: Yes System-Controlled: Yes Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA
Role Category Name	Basic	Single	Text	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA
Role Category Description	Basic	Single	Text	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA

### 12.3.3 Role Grant Relationship

The RoleRoleRelationship.xml file contains the attribute definition for role grant relationship. You cannot add your own attributes for the role grant relationship.

[Table 12–3](#) lists the default attributes for role grant relationship.

**Table 12–3 Default Attributes for Role Grant Relationship**

Attribute Name	Category	Type	Data Type	Properties	LOV
UGP_KEY	Basic	Single	Reference to role	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA
USR_KEY	Basic	Single	Reference to user	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA

### 12.3.4 Role Parent Relationship

The RoleUserMembership.xml file contains the attribute definitions for role parent relationship. You cannot add your own attributes to the role parent relationship.

Table 12–4 lists the default attributes for the role parent relationship.

**Table 12–4** Default Attributes for Role Parent Relationship

Attribute Name	Category	Type	Data Type	Properties	LOV
UGP_KEY	Basic	Single	Reference to role	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA
GPG_UGP_KEY	Basic	Single	Reference to role	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes Bulk-Updatable: No	NA

---



---

**Note:** UGP\_KEY is a reference to the parent role. GPG\_UGP\_KEY is a reference to the child role.

---



---

### 12.3.5 Role Organization Relationship

A role organization relationship can be established by publishing the role to an organization. See "[Publishing Entities to Organizations](#)" on page 13-4 for more information.

## 12.4 Default Roles

In Oracle Identity Manager, the following types of roles are available:

- Enterprise roles:** These are roles that users (depending on the permissions granted) can create in Oracle Identity Manager and request for by using the request catalog. See "[Role Management Tasks](#)" on page 12-10 and "[Request-Based Role Grants](#)" on page 12-21 for more information about creating and requesting roles.
- Admin roles:** These are predefined roles in Oracle Identity Manager that have a one-to-one mapping with the application roles defined in Oracle Entitlement Server. Admin roles are not visible to the end users. Therefore, admin roles cannot be requested. See "[Admin Roles](#)" on page 13-5 for more information about admin roles.

Table 12–5 lists the default enterprise roles in Oracle Identity Manager. For a list of default admin roles, see "[Admin Roles](#)" on page 13-5.

---



---

**Note:** If you upgrade from Oracle Identity Manager 11g Release 1 (11.1.1), then the default roles of 11g Release 1 (11.1.1) will be available.

---



---

**Table 12–5** *Default Roles in Oracle Identity Manager*

Role	Description
ALL USERS	Members of this role have minimal permissions, including the ability to access the user's own user record. By default, each user belongs to the All Users role.
SYSTEM ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users, and other users can only view it on UI. Members of this role have access to the UI to perform various tasks to manage attestation events.
Administrators	This role is for internal use only, meaning it is for OIM users, and other users can only view it on UI. It is the administrators role for SOA.
OPERATORS	This role is for internal use only, meaning it is for OIM users, and other users can only view it on UI. Members of this role have access to the pages related to organizations, users, and Task List. These users can perform a subset of functions on these pages.
SELF OPERATORS	This role is for internal use only, meaning it is for OIM users, and other users can only view it on UI. It contains one user, XELSELFREG, who is responsible for modifying the privileges that users have when performing self-registration actions within Oracle Identity Manager.  <b>Note:</b> Oracle Identity Manager recommends that you do not modify the permissions associated with the SELF OPERATORS user role. In addition, you should not assign any users to this role.

You can modify the permissions associated with the default roles. You can also create additional roles. However, you cannot assign/remove menu items to/from any roles.

## 12.5 Role Management Tasks

This section discusses the following topics:

- [Creating Roles](#)
- [Managing Roles](#)
- [Creating and Managing Role Categories](#)

---



---

**Note:** A role, SELF OPERATORS, is added to Oracle Identity Manager by default. This role contains one user, XELSELFREG, who is responsible for modifying user permissions for performing self-registration in the Administration Console.

Oracle recommends that you do not modify the permissions associated with the SELF OPERATORS role and do not assign users to this role.

---



---

## 12.5.1 Creating Roles

When you first create a new role, the Role Details page shows the role name. You can add information to a role by using the Additional Detail menu as described in ["Managing Roles"](#) on page 12-11.

To create a role:

1. Log in to Identity Self Service.
2. Under Administration, click **Roles**. The Search Roles page is displayed.
3. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Role page is displayed.
4. Enter values in the fields. [Table 12-6](#) lists the fields in the Create Role page.

**Table 12-6 Fields in the Create Role Page**

Field	Description
Name	The name of the role
Display Name	The role name as displayed in the UI
Role E-mail	The e-mail ID of the role
Role Description	The description for the role
Role Category	The category to which the role belongs If a role category is not specified in this field, then the role is created in the Default category. See <a href="#">"Creating and Managing Role Categories"</a> on page 12-19 for information about role categories.
Owned By	The owner of the role The role owner is a user who has permissions to view, modify, and delete the role without having to create custom authorization policies. For information about authorization policies for role management, see "Security Architecture" in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i> .

5. Click **Save**. The role is created successfully. The role details page for the created role is displayed.

## 12.5.2 Managing Roles

You can find roles, add information to them, and perform other administrative functions for roles.

This section discusses the following topics:

- [Searching for Roles](#)
- [Viewing and Administering Roles](#)
- [Viewing Access Policies](#)
- [Deleting Roles](#)

### 12.5.2.1 Searching for Roles

To search for roles:

1. In Identity Self Service, under Administration, click **Roles**. The Search Roles page is displayed.
2. Select any one of the following:
  - **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.
  - **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.
3. In the searchable user attribute fields, such as Display Name, specify a value. You can include wildcard characters (\*) in the attribute value.

For some attributes, select the attribute value from the lookup. For example, to search all roles in the Default role category, select Default in the Role Category field.

4. For each attribute value that you specify, select a search operator from the list. The following search operators are available:
  - Starts with
  - Ends with
  - Equals
  - Does not equal
  - Contains
  - Does not contain

The search operator can be combined with wildcard characters to specify a search condition. The asterisk (\*) character is used as a wildcard character. For example, you can specify the value of the Display Name attribute to be Jo\* as the search criteria, and select Equals as the search operator. The roles with Display Name that begins with Jo are displayed.

5. To add a searchable role attribute to the Search Roles page, click **Add Fields**, and select the attribute from the list of attributes.

For example, if you want to search all roles in a role namespace, then you can add the Role Namespace attribute as a searchable field and specify a search condition.

---

---

**Note:** You can configure the attributes that are searchable. The attributes available for search must be a subset of the attributes defined for the role entity that are marked with the Searchable = Yes property.

---

---

6. Optionally click **Reset** to reset the search conditions that you specified. Typically, you perform this step to remove the specified search conditions and specify a new search condition.
7. Click **Search**. The search results is displayed in a tabular format, as shown in Figure:
8. If you want to hide columns in the search results table, then perform the following steps:

- a. Click **View** on the toolbar, select **Columns, Manage Columns**. The Manage Columns dialog box is displayed.
- b. From the Visible Columns list, select the columns that you want to hide.
- c. Click the left arrow icon to add the columns in the Hidden Columns list.
- d. Click **OK**. The selected columns are not displayed in the search results. A status message displays along the bottom of the search table to identify how many columns are currently hidden. Figure shows that two columns are hidden:

### 12.5.2.2 Viewing and Administering Roles

You can open the details of a role and edit the role attributes, modify the role inheritance and membership, and then publish roles to organization. To open the details of a role and modify it, perform one of the following:

- In the Search Roles page, search and select the role that you want to open. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar.
- In the search results table of the Search Roles page, click the Display Name of the role.

The details of the role is displayed in a new page. The role display name is displayed at the top of the page. You can display the details of the role and modify role information in the following tabs of this page:

- [The Attributes Tab](#)
- [The Hierarchy Tab](#)
- [The Members Tab](#)
- [The Organizations Tab](#)

#### 12.5.2.2.1 The Attributes Tab

The Attributes tab displays the role attributes. Except for the Role Namespace field (which is a read-only field), the rest of the fields in the Attributes tab are same as available in the Create Role page. The Role Namespace field displays the namespace to which the role is assigned. For information about the rest of the fields in the Attributes tab, see [Table 12-6, "Fields in the Create Role Page"](#).

To modify the role attributes, change the values in the fields, and click **Apply**.

#### 12.5.2.2.2 The Hierarchy Tab

The Hierarchy tab displays the role hierarchy information in the following sections:

- **Inherits From:** This section displays the parent roles from which the open role is inherited. The base role has the same permissions and privileges on the members as the inherited roles. Only inherited roles can be added or removed from the base role, but the base role cannot be added or removed from the inherited role.
- **Inherited By:** This section lists the child roles that are inherited by the open role. This is a read-only display of the roles. You can use the Open Role action to modify the relationship from the base role.

In the Hierarchy tab, you can perform the following:

- [Adding a Parent Role to a Child Role](#)
- [Removing a Parent Role from a Role](#)

- [Opening a Parent/Child Role](#)

#### 12.5.2.2.3 Adding a Parent Role to a Child Role

To add a parent role to a role:

1. Open the role.
2. Click the **Hierarchy** tab. In the Inherits From section, this tab lists the parent roles of the open from which the open role inherits permissions.
3. Verify that Inherits From is active.
4. From the Actions menu, select **Add**. Alternatively, click **Add** on the toolbar. The Search Roles dialog box is displayed.
5. From the Search list, select a role attribute based on which you want to search for the role. Then, select an attribute by using the lookup icon. You can also include wildcard characters (\*) in your search criterion. Then, click the search icon. A list of roles that matches your search criterion is displayed.
6. Select one or more roles that you want to add as parent roles. Then, click **Add Selected** to move the selected roles to the Selected Roles list.  
  
Alternatively, you can click **Add All** to add all the roles in the Selected Roles list.
7. Click **Add**. The selected roles are added as parent roles to the opened role and the role hierarchy is displayed in the Inherits From section of the Hierarchy tab.
8. Select the inherited role that is added. A summary information of the role selected is displayed below the table.

You can click the Display name of the inherited role to open the role details.

#### 12.5.2.2.4 Removing a Parent Role from a Role

To remove a parent role from a role:

1. In the Inherits From section of the Hierarchy tab, select the role that you want to remove.
2. From the Actions menu, select **Remove**. Alternatively, click **Remove** on the toolbar. A message box is displayed asking for confirmation.
3. Click **OK**. The inherited role is removed from the Inherits From section of the Hierarchy tab.

#### 12.5.2.2.5 Opening a Parent/Child Role

You can open parent roles from the Inherits From section and child roles from the Inherited By section of the Hierarchy tab.

You can also open the roles that are linked parent and child roles (similar to grand parent roles and grand child roles) of the current opened role from the Inherited From and Inherited By sections of the Hierarchy tab respectively.

To open a parent role:

1. In the Inherits From section of the Hierarchy tab, select the role that you want to open.
2. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar.

A page with details about the inherited role is displayed. In this page, you can view and edit the role attributes, modify the role inheritance and membership,

assign and remove membership rules, access policies, and permissions, and update permissions.

To open a child role:

1. In the Inherits From or Inherited By section of the Hierarchy tab, select the role that you want to open.
2. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar. A page with details about the inherited role is displayed.

#### 12.5.2.2.6 The Members Tab

The Members tab displays the members assigned to the open role. This information is displayed in the following sections:

- **Direct:** This section displays the members that are directly assigned to the open role. It also displays all members that are assigned via membership rules.
- **Indirect:** This section displays the members that are indirectly inherited by the role.
- **All:** This section displays all the members, direct and indirect, assigned to the open role.

In the Members tab, you can perform the following:

- [Assigning Members to a Role](#)
- [Revoking Members from a Role](#)
- [Adding, Modifying, and Deleting Membership Rules](#)

#### 12.5.2.2.7 Assigning Members to a Role

To assign members to a role:

1. In the Direct section of the Members tab, click **Assign** on the toolbar. The Catalog page is displayed.
2. In the Target Users section, click **Add** to select the members (users) to be assigned to the role. The Advanced Search for Target Users dialog box is displayed.
3. Search and select one or more users that you want to add.
4. Click **Add Selected** to add the selected users to the Selected Users list. Alternatively, click **Add All** to add all the users in the Selected Users list.
5. Click **Add**. The selected users or beneficiaries are added to the Target Users section of the Request Cart Details page.
6. In the Justification and Effective Date section, in the respective fields, specify a justification and effective date when the request will be active.
7. In the Cart Items section, if required, select a cart item and click **Details** to display the details of the item.
8. In the Details section, modify the request details, if required. To do so, set or modify values in the Details section, and then click **Ready to Submit**.
9. After reviewing and modifying the details or each request in the cart, click **Submit**.

The request is submitted for approval, and the Request Summary page is displayed with summary information, target user or beneficiary information, and request and approval details.

### 12.5.2.2.8 Revoking Members from a Role

To revoke members from a role:

1. In any section of the Members tab, select the member that you want to revoke.
2. Click **Revoke** on the toolbar. The Remove Roles page is displayed.
3. In the Target Users section, verify the members to be revoked from the role.
4. Enter values for the Justification and Effective Date fields.
5. Click **Submit**. If you have the required authorization policies for revoking members from a role, then without any approval step, the users are removed from the role. If you do not have the required authorization policies, then the role will be revoked when an approver approves the request.

### 12.5.2.2.9 Adding, Modifying, and Deleting Membership Rules

In the Members tab, you can add, modify, or delete the user membership rules by using the expression builder. The expression builder lets you specify a condition based on which users are dynamically assigned to roles. You can specify simple to complex condition expressions as the user membership rule. When you modify a user membership rule, the existing user memberships are evaluated, and then the existing role memberships that are not valid are revoked and new role memberships are granted.

To add a user membership rule:

1. In the Members tab, in the User Membership Rules section, click **Add Rule**. The Expression Builder is displayed.
2. In the left pane, verify that <ADD> is selected. This is the placeholder to specify a user attribute for the condition.
3. Under Select Operand Value, in the Attributes tab, select a user attribute, for example, **Country**.
4. Click **Add** to add the attribute to the condition in the left pane.
5. From the list of operators, select a comparator, such as = (equals), > (greater than), >= (greater than equal to), < (less than), => (less than equal to), and IN.
6. Under Select Operand Value, in the Literals tab, specify a value in the Value field, such as `United States of America`.

When a checkbox or lookup type UDF or default attribute is used in membership rule, then it must be treated as shown in the following example:

```
( ( ( Last Name = "Klein" ) AND ( First Name Contains "Robert" ) )
OR ( ( User Login Starts with "rob" ) AND ( Common Name Ends with "ein" ) )
OR ( ( Robert2UserUDF111DL != "Robert2UserUDF111DL" ) AND ( Robert2UserNumberDL
>= 99999 )
AND ( RobertUserDateDL =< 2013-12-31 ) AND ( Robert2UsercheckboxDL = "1" )
AND ( Robert2UserLookupDL IN ["RobertLookUpCode3","RobertLookUpCode9"] ) ) )
```

Here:

- Robert2UsercheckboxDL is check box, which must be used in the rule as a string. Use "1" to check for True/yes/Selected/Checked, and use "0" to check for False/no/Unselected/unchecked.
- Robert2UserLookupDL is lookup type. In the default userprofile, "Robert2LookUpMean3" will be displayed. But you must use its code value "Robert2LookUpCode3" in the expression.

- For All type of Attributes, there is no way to check NULL or no value.

---

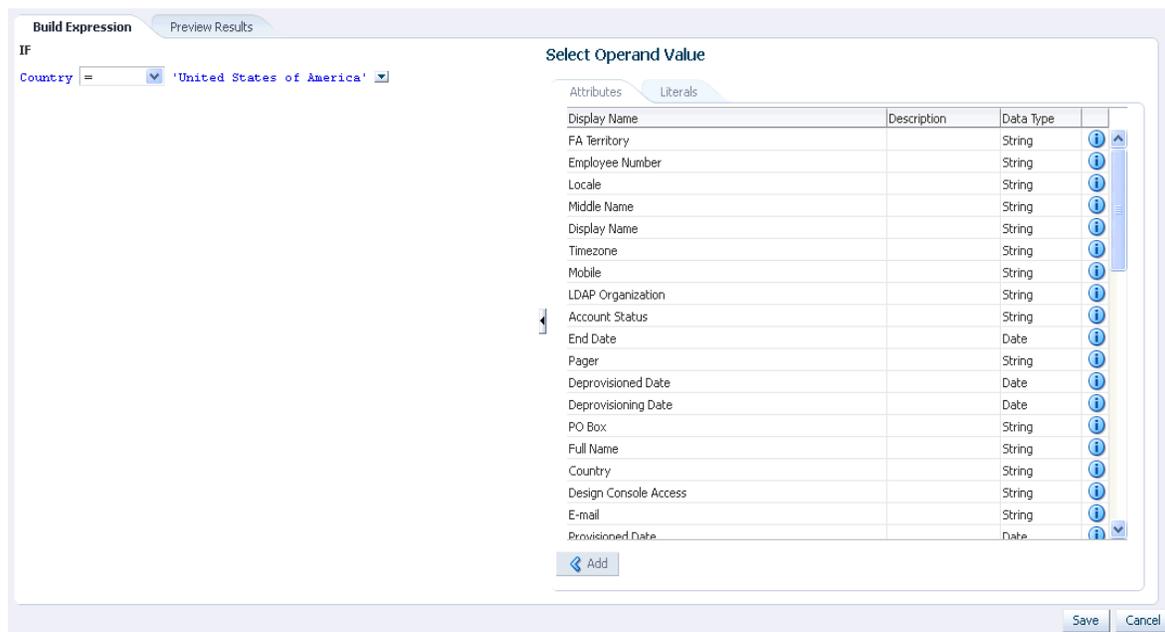
**Note:** Checkbox fields are stored as strings in the backend. The data type for a checkbox field is a String and not Boolean. Therefore, all string operations will be displayed.

---

7. Click **Add** to add the specified value to the condition expression. The expression now means that users belonging to United States of America will be dynamically assigned to the open role.

Figure 12–2 shows the expression builder with the condition.

**Figure 12–2 The Expression Builder**



8. If required, on the Preview Results tab, you can preview members to whom this rule will be applied.
9. Click **Save**. The expression builder closes, and the rule you defined has been applied.

To modify a user membership rule:

1. In the Members tab, in the User Membership Rules section, click **Edit Rule**. The expression builder is displayed.
2. Specify a condition to dynamically assign members, as described in the steps for adding membership rule.
3. If required, on the Preview Results tab, you can preview members to whom the modified rule will be applied.
4. Click **Save**. The modified membership rule is applicable now.

To delete a user membership rule:

1. In the Members tab, in the User Membership Rules section, click **Delete Rule**. A dialog box asking to confirm whether you want to delete the membership rule is displayed.

2. Click **Yes**. The membership rule is deleted and no longer applicable.

#### 12.5.2.2.10 The Organizations Tab

The Organizations tab allows you to assign and revoke organizations to and from the open role. By assigning an organization to the open role, you make the role available to the organization. This is called publishing the role entity to an organization.

All the organizations, to which the open role has been published, are displayed in the Organizations tab. For each organization, the **include sub-orgs** option is available for selection in the Hierarchy Aware column. Select this option if you want the open role to be available to the entire hierarchy of the organization. To make the open role available only to the organization and not its hierarchy, leave this option deselected.

In the Organizations tab, you can perform the following:

- [Publishing Roles to an Organization](#)
- [Revoking Organizations From a Role](#)

#### 12.5.2.2.11 Publishing Roles to an Organization

To publish roles to an organization:

1. In the Role details page, click the **Organizations** tab. This tab displays the organizations that are assigned to the open role.
2. From the Actions menu, select **Assign**. Alternatively, click **Assign** on the toolbar. The Search Organizations dialog box is displayed.
3. Search for the organizations you want to add. The organizations are displayed in the Organization Results section.
4. Select the organizations that you want to add, and click **Add Selected**. The selected organizations are added to the Selected Organizations section.
5. For each selected organization, the **Hierarchy** option is selected by default. If you want to publish the role to the suborganizations of the selected organization, then leave the Hierarchy option selected.

To publish the role to the selected organization only, deselect the **Hierarchy** option.

6. Click **OK**. The role is published to the selected organizations. In other words, the selected organizations are assigned to the role.

#### 12.5.2.2.12 Revoking Organizations From a Role

To revoke an organization from a role:

1. In the Organizations tab, select the organization that you want to revoke.
2. From the Actions menu, select **Revoke**. Alternatively, click **Revoke** on the toolbar. A message is displayed asking for confirmation.
3. Click **Revoke**. The organization is revoked from the role.

#### 12.5.2.3 Viewing Access Policies

You can display all available access policies for this role. To view access policies assigned to the role:

In the Role details page, click **Access Policy**. The Access Policies page is displayed. This page displays the policy name and brief description of the policy.

### 12.5.2.4 Deleting Roles

To delete a role:

1. In the Search Roles page, search for a role as described in ["Searching for Roles"](#) on page 12-11.
2. Select the role that you want to delete.
3. From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar. A message is displayed asking for confirmation.
4. Click **Delete** to confirm.

---

---

**Note:**

- You are not allowed to delete a role, which is the parent/child of some other role. To delete such a role, you must first remove the associated parent-child role relationships. When the role is no longer involved in any role relationships, it can be deleted.
  - You are not allowed to delete a role that has users associated with it.
- 
- 

## 12.5.3 Creating and Managing Role Categories

Role categories are a way of categorizing roles for the purpose of navigation and authorization. Role categories are internally stored in Oracle Identity Manager as an attribute of the role and is reconciled with the multivalued business category attribute in the LDAP identity store. If the value in LDAP is empty, then the role is assigned to the default role category. If the value in LDAP is an unrecognized value, then a role category (with the category name as the unrecognized value) is created, and then the role is assigned to this newly created role category. If the value in LDAP has multiple values, then the role reconciliation process does not reconcile the role and generates reconciliation errors in Oracle Identity Manager.

The default role categories in Oracle Identity Manager are:

- **OIM Roles:** All the predefined roles in Oracle Identity Manager are assigned to this category. These are roles that exist in Oracle Identity Manager by default and are primarily used for managing permissions. There will not be any corresponding entity in LDAP store and catalog for these predefined roles.
- **Default:** A newly created role must have a role category. Therefore, if a role category is not specified at the time of creating the role, then the role is assigned to this category by default.

---

---

**Note:** The default role categories cannot be localized.

---

---

This section describes the following topics:

- [Creating a Role Category](#)
- [Searching Role Categories](#)
- [Modifying a Role Category](#)
- [Deleting a Role Category](#)

### 12.5.3.1 Creating a Role Category

To create a role category:

1. In Identity Self Service, under Administration, click **Role Categories**. The Search Role Categories page is displayed.
2. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Role Category page is displayed.
3. In the Role Category box, enter the name of the role category.
4. In the Role Category Description box, enter a description for the role category. This step is optional.
5. Click **Save**. The role category is created, and the role category details page is displayed. The page consists of the Attributes and Roles tabs.

The Attributes tab displays the attributes of the role category. You can edit the fields in this tab to edit the role category.

The Roles tab displays the list of roles belonging to the role category.

### 12.5.3.2 Searching Role Categories

To search for role categories:

1. Under Administration, click **Role Categories**. The Search Role Categories page is displayed.
2. In the Role Category field, specify a value. You can include wildcard characters (\*) in the attribute value.
3. For the attribute value that you specify, select a search operator from the list. The following search operators are available:
  - Starts with
  - Ends with
  - Equals
  - Does not equal
  - Contains
  - Does not contain

The search operator can be combined with wildcard characters to specify a search condition. The asterisk (\*) character is used as a wildcard character. For example, you can specify the value to be D\* as the search criteria, and select Equals as the search operator. The role categories that begins with D are displayed.

4. To add a searchable attribute to the Role Categories, click **Add Fields**, and select the attribute from the list of attributes.
5. Optionally click **Reset** to reset the search conditions that you specified. Typically, you perform this step to remove the specified search conditions and specify a new search condition.
6. Click **Search**. The search results is displayed in a tabular format.

### 12.5.3.3 Modifying a Role Category

To modify a role category:

1. In the Search Role Categories page, search and select the role category you want to modify.
2. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar. A page with details about the role category is displayed.
3. The Attributes tab is open by default. Edit the fields in this tab to modify basic category information such as name and description. When finished, click **Apply**.
4. Click the **Roles** tab. In this tab, you can view all roles that are assigned to this category.

#### 12.5.3.4 Deleting a Role Category

To delete a role category:

1. In the Search Role Categories page, search and select the role category you want to delete.
2. From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar.  
If the role category detail page is open, then click **Delete** on the toolbar.  
A message box is displayed asking for confirmation.
3. Click **Delete**. The role category is deleted.

---

---

**Note:** You cannot delete a role category that has roles associated with it.

---

---

## 12.6 Request-Based Role Grants

Oracle Identity Manager generates a request when a role grant is performed. This request is subject to approval, and therefore, the role grant takes place only when the role grant request has been approved.

After a role grant request is generated, the request ID is displayed. This is for tracking the request in Identity Self Service or Oracle Identity System Administration.

Role grant requests have the following details:

- Request ID: Automatically generated
- Request Type: Type of request
- Request Status: Assigned
- Date Requested: Current timestamp
- Effective Date: Current timestamp
- Requester: Null
- Beneficiary: Null
- Justification: Null



---

---

## Managing Organizations

An organization entity represents a logical container of entities such as users and other organizations in Oracle Identity Manager. Organization in Oracle Identity Manager is used only for security purposes. It is not an enterprise organization, or an LDAP organization or organization unit.

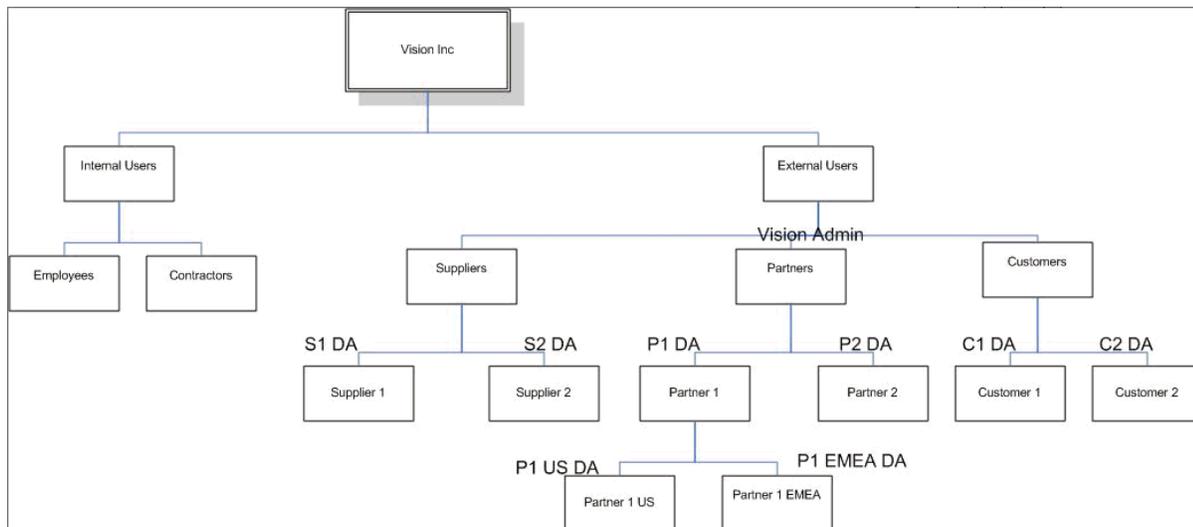
The concepts related to organizations and procedures to manage organizations are described in the following sections:

- [Delegated Administration Model](#)
- [Organization Entity Definition](#)
- [Organization Scoping and Hierarchy](#)
- [Publishing Entities to Organizations](#)
- [Admin Roles](#)
- [Delegable and Nondelegable Operations](#)
- [Evaluating Password Policies](#)
- [Organization Management Tasks](#)

### 13.1 Delegated Administration Model

Vision Inc. is a fictitious company used in this document to depict a typical delegated administration use case. There are five user types: employees, contractors, suppliers, partners, and customers. There are approximately one hundred applications that are to be provisioned to each user. In this example, the proposed solution is called IDM.

Vision Inc. has two major sets of users, Internal Users consisting of employees and contractors, and External Users consisting of partners, suppliers, and customers, as illustrated in [Figure 13-1](#):

**Figure 13–1 Delegated Administration**

Internal Users are on-boarded and managed by a HR Administrator directly by using Oracle Identity Self Service. IDM administrator creates various partners, suppliers, and customers, as shown in [Figure 13–1](#), and assigns delegated administrator for each of these organizations. For example, the IDM administrator can create and manage a partner organization called Partner1, create one or more users under Partner1, and assign one or more of these users as the delegated administrator for that organization. The delegated administrator, for example Partner1 DA, can then create additional hierarchy under Partner1, for example Partner1 US and Partner1 EMEA, and can specify a delegated administrator under each of these organizations. For example, Partner1 DA can specify User1 under Partner1 US as delegated administrator of Partner1 US. This hierarchy levels can go to the nth level.

The users created under each of these organizations follow a strict permission model. For example, users in the External Users organization cannot see users Internal Users, but internal users who are a part of IDM Administrator can see both internal and external users. Partner1 DA is not able to see users under Partner2 or vice versa. Similarly, Partner1 US DA is not able to see Partner1 EMEA users. A parent delegated administrator can see all children delegated administrators but not the reverse. For example, Partner1 DA can see Partner1 US and Partner1 EMEA users, but Partner1 US users are able to see only users in Partner1 US. This entire delegation model is achieved through organization hierarchy, viewer admin role assignment to users, and publishing the entities to only those organizations to which the users belong.

The ability of the users in organizations to view and access resources follows hierarchy. For example, all resources/roles that are permitted for Partner1 is visible by default to Partner1 US and Partner1 EMEA. This is achieved by selecting a flag to include suborganizations when publishing the entities, described later in this document. Both publishing and delegation are organization hierarchy-aware. Each of the delegated administrators can further limit the resource availability for their corresponding entities.

The delegated administration model is achieved through the following:

- Organization definition:** Users and entities are defined in logical containers called organizations, and a set of attributes are defined for the organizations. See ["Organization Entity Definition"](#) on page 13-3 for details.

- **Organization scoping with logical organization hierarchy:** Scoping the entities to certain set of users. This means that not all users can view or access all entities. For example, the users in the Partners organization can only view the roles, entitlements, and application instances available to the Partners organization. These users cannot view or access the entities available to the Suppliers and Customers organizations. See "[Organization Scoping and Hierarchy](#)" on page 13-4 for details.
- **Publishing of entities to organizations:** The entities are made available to the users of an organization. See "[Publishing Entities to Organizations](#)" on page 13-4.
- **Admin roles:** The permissions that a user has on a entity is governed by the admin role assignment to the user. See "[Admin Roles](#)" on page 13-5 for details.

## 13.2 Organization Entity Definition

In Oracle Identity Manager, attributes are defined by default for the organization entity. These attributes are the same for all entities, such as user, organization, role, role hierarchy, and role membership. For a list of attributes defined for the entities, see "[User Entity Definition](#)" on page 11-3.

[Table 13-1](#) lists the default attributes of the organization entity:

**Table 13-1** *Default Attributes of the Organization Entity*

Attribute Name	Category	Type	Data Type	Display Type	Properties
Organization Name	Basic	Single	String	Single line text	Required: Yes System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes
Type	Basic	Single	String	LOV	Required: Yes System-Can-Default: Yes System-Controlled: Yes Encryption: Clear User-Searchable: Yes

**Table 13–1 (Cont.) Default Attributes of the Organization Entity**

Attribute Name	Category	Type	Data Type	Display Type	Properties
Parent Organization	Basic	Single	String	Single line text	Required: No System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes
Status	Basic	Single	String	Single line text	Required: Yes System-Can-Default: Yes System-Controlled: Yes Encryption: Clear User-Searchable: Yes
Password Policy	Basic	Single	String	LOV	Required: false System-Can-Default: No System-Controlled: No Encryption: Clear User-Searchable: Yes

### 13.3 Organization Scoping and Hierarchy

In Oracle Identity Manager, the root of the organizational hierarchy is represented by the Top organization. The Top organization is a predefined organization that is available in Oracle Identity Manager. By default, every organization in Oracle Identity Manager extends from the Top organization.

Oracle Identity Manager provides an organizational-level scoping mechanism for delegated administration and data security of various entities. This is achieved by the following:

- **User's admin role memberships in organizations:** User is assigned permissions over an organization by assigning admin role in that organization scope.
- **Entities available in organizations:** Data is secured by confining its availability only in a set of organizations. The process of making data available in organization scope is referred to as publishing. The user is allowed to perform operations on an entity as assigned by the user's admin roles, if those roles are published to the organization and the entity is published to the same organization.

### 13.4 Publishing Entities to Organizations

Publishing an entity to an organization is making the entity available to that organization. The enterprise roles, entitlements, or application instances can be published by respective administrators to a list of organizations to enable these to be granted to the users of those organizations. Enterprise roles, entitlements, and application instances are published to a list of organizations to make these:

- Requestable to users under the list of organizations
- Manageable to the list of organization administrators to manage these roles

You can publish entities to organizations from the Organizations tab of the respective entity details page in Identity Self Service.

When an entity admin creates an entity (for example, a Role Admin creates an enterprise role), then that entity (role, in this example) is automatically made available to all the organizations where the admin has entity admin roles. This avoids creating and then publishing entities for admins in their respective organizations or organization hierarchies). However, if the entity needs to be published to other organizations, then the entity needs to be manually published.

## 13.5 Admin Roles

Admin role is a first class entity in Oracle Identity Manager and is not the same as enterprise role or group entity. The authorization and security model in Oracle Identity Manager works on the basis of the admin role assignment to a user. The assignment can be in the given organization scope or in Top organization scope. As mentioned earlier, the Top organization is at the root of the organization hierarchy in Oracle Identity Manager. Authorization policies are created according to the admin roles. Admin roles are predefined in Oracle Identity Manager, and you cannot add new admin roles. Admin roles cannot be created, updated, deleted, or requested.

Entities have the following admin roles defined for it:

- **Entity Administrator:** Can manage the entire lifecycle of the entity and perform any operation on the entity.
- **Entity Viewer:** Can view the entity in the catalog or request profile and request for the entity
- **Entity Authorizer:** Can view the entity in the catalog or request profiles and request for it, but does not require approval. There is no authorizer on the organization entity because organization membership cannot be requested. Similarly, there is no authorizer for the user. The user admin and user authorizer are the same.

However, there are certain exceptions for the entity administrator. For example, Role Administrators cannot assign or revoke users to or from that role. To assign or revoke users to the role, the role administrator must explicitly have any one of the following:

**Role Viewer role:** To be able to assign or revoke users to that role through requests, which are subject to approval.

**Role Authorizer role:** To be able to assign or revoke users to that role as a direct operation.

Similarly, Application Instance Administrators and Entitlement Administrators cannot assign or revoke users to or from the respective entities. These admin roles must have explicit entity viewer or entity authorizer roles to be able to assign or revoke to or from that entity, through request or direct operation respectively.

Admin roles have no hierarchy. However, admin role memberships are hierarchy-aware and can be cascaded downwards to the child organizations. Admin role membership is always given in an organization scope, and can only be assigned by the System Administrator or System Configurator. Admin roles do not have autogroup membership or role membership rules.

---

---

**Note:** Admin roles cannot be stored in LDAP data store and are stored in Oracle Identity Manager database.

---

---

Admin roles belong to a role category called admin roles. The admin roles cannot be requested and are never exposed to end users. Only the System Administrator and

System Configurator roles, which require users to be assigned to these roles to perform system functions, can access admin roles.

The System Administrator and System Configurator admin roles are available only to the Top organization. Therefore, only System Administrators and System Configurators can assign System Administrator and System Configurator roles because they have access to the Top organization. Only a System Administrator can provision resources to an organization.

Table 13–2 lists the admin roles in Oracle Identity Manager for each entity.

**Note:** In Table 13–2, you will come across implicit permissions called org basic info, role basic info, entitlement basic info, and appinstance basic info. The basic-info permission gives the permission only to view-search the given entity. Consider the following examples:

- View Org permission provides all the permissions defined for the Organization Viewer admin role, but org basic info provides the permissions only to search and view the organization attributes.
- The User Viewer admin role provides the basic info permission on roles, organizations, application instances, and entitlements in that scoped organization.

**Table 13–2 Admin Roles in Oracle Identity Manager**

Entity	Admin Role	Description
	System Administrator	Oracle Identity Manager System Administrator role with all privileges
	System Configurator	Role with privileges to configure Oracle Identity Manager
	SPML Administrator	SPML administrator to manage SPML operations
Role	Role Administrator	Role with privileges to administer all assigned enterprise roles
	Role Authorizer	Role with privileges to authorize all assigned enterprise roles. Role authorizer can grant roles as a direct operation.
	Role Viewer	Role with privileges to view assigned enterprise roles.
Entitlement	Entitlement Administrator	Role with privileges to administer all assigned entitlements
	Entitlement Authorizer	Role with privileges to authorize all assigned entitlements
	Entitlement Viewer	Role with privileges to view all assigned entitlements
Application Instance	Application Instance Administrator	Role with privileges to administer all assigned application instances
	Application Instance Authorizer	Role with privileges to authorize all assigned application instances
	Application Instance Viewer	Role with privileges to view all assigned application instances
Organization	Organization Administrator	Role with privileges to administer all assigned organizations
	Organization Viewer	Role with privileges to view all assigned organizations

**Table 13–2 (Cont.) Admin Roles in Oracle Identity Manager**

Entity	Admin Role	Description
User	User Administrator	Role with privileges to administer all assigned users
	HelpDesk	Help Desk to manage users
	User Viewer	Role with privileges to view all assigned user records
Catalog	Catalog Administrator	Role with privileges to manage all catalog items

**See Also:** "Security Architecture" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information about admin roles

Table 13–3 lists the admin roles in Oracle Identity Manager and the corresponding permissions allowed provided by the admin roles.

**Table 13–3 Admin Roles and Permissions**

Admin Role in Oracle Identity Manager	Implicit Permissions	Organization Scoped Permissions	Request or Direct Operation	
User Administrator	Organization Viewer	Search User (attribute-level security)	NA	
	Role Viewer	View User (attribute-level security)	NA	
	Entitlement Viewer	Create User	Direct	
	AppInstance Viewer		Delete User	Direct
			Modify User (attribute-level security)	Direct
			Lock User	NA
			Unlock User	NA
			Enable User	Direct
			Disable User	Direct
			Grant Role	Direct
			Revoke Role	Direct
			Grant Accounts	Direct
			Revoke Accounts	Direct
			Grant Entitlements	Direct
			Revoke Entitlements	Direct
			Change User Password	NA
			Change Account Passwords	NA
Modify User Account	Direct			
Enable User Account	Direct			
Disable User Account	Direct			
View Org	NA			
View Role	NA			

**Table 13–3 (Cont.) Admin Roles and Permissions**

<b>Admin Role in Oracle Identity Manager</b>	<b>Implicit Permissions</b>	<b>Organization Scoped Permissions</b>	<b>Request or Direct Operation</b>
		View Entitlements	NA
		View Application Instance	NA
		View Requests	NA
		View Admin Role Memberships	NA
		View Role Memberships	NA
		View User Accounts	NA
		View User Entitlements	NA
		View Proxy	NA
		Add Proxy	Direct
		Delete Proxy	Direct
Help Desk	Org Basic Info	Search User (attribute-level security)	NA
	Role Basic Info	View User (attribute-level security)	NA
	Entitlement Basic Info	Enable User	Request
	AppInstance Basic Info	Disable User	Request
		Unlock User ONLY IF locked out due to failed logins	Direct
		Change User Password	Direct
		Change Account Password	Direct
		View Org	NA
		View Role	NA
		View Entitlements	NA
		View Application Instance	NA
		View Requests	NA
		View Role Memberships	NA
		View Proxy	NA
		View User Accounts	NA
		View User Entitlements	NA
User Viewer	Organization Viewer	Create User	Request
	Role Viewer	Delete User	Request
	Entitlement Viewer	Modify User (attribute-level security)	Request
	AppInstance Viewer	Search User (attribute-level security)	NA

**Table 13–3 (Cont.) Admin Roles and Permissions**

<b>Admin Role in Oracle Identity Manager</b>	<b>Implicit Permissions</b>	<b>Organization Scoped Permissions</b>	<b>Request or Direct Operation</b>
		View User (attribute-level security)	NA
		Enable User	Request
		Disable User	Request
		Grant Role	Request
		Revoke Role	Request
		Grant Accounts	Request
		Revoke Accounts	Request
		Grant Entitlements	Request
		Revoke Entitlements	Request
		Modify User Account	Request
		View Org	NA
		View Role	NA
		View Entitlements	NA
		View Application Instance	NA
		View Requests	NA
		View Role Memberships	NA
		View Proxy	NA
		Enable User Account	Request
		Disable User Account	Request
		View Admin Role Memberships	NA
		Add Admin roles	NA
		Delete Admin roles	NA
		Modify Admin Role membership	NA
		View User Accounts	NA
		View User Entitlements	NA
Role Viewer	Org Basic Info	Grant Role	Request
	User Basic Info	Revoke Role	Request
		View Org	NA
		View Role	NA
		View Users	NA
		View Role Memberships	NA
Organization Viewer	Org Basic Info	Search Org	NA
	User Basic Info	View Org	NA

**Table 13–3 (Cont.) Admin Roles and Permissions**

<b>Admin Role in Oracle Identity Manager</b>	<b>Implicit Permissions</b>	<b>Organization Scoped Permissions</b>	<b>Request or Direct Operation</b>
	AppInstance Info	View Users	NA
	Entitlement Info	View Role	NA
		View AppInstance	NA
		View Entitlement	NA
		View All Publications	NA
		View All Org Members	NA
		View Admin Role & memberships	NA
		View Accounts Provisioned to Org	NA
Application Instance Viewer	User Basic Info	Search Application Instance	NA
	Org Basic Info	View Application Instance (excluding passwords)	NA
	Entitlement Info	Grant Account	Request
		Revoke Accounts	Request
		Modify User Account	Request
		Enable User Account	Request
		Disable User Account	Request
		View Org	NA
		View User	NA
		View AppInstance	NA
		View Entitlements	NA
		View User Accounts	NA
		View User Entitlements	NA
Entitlement Viewer	User Basic Info	Search Entitlement	NA
	Org Basic Info	View Entitlement	NA
	AppInstance Basic Info	Grant Entitlement	Request
		Revoke Entitlement	Request
		View Orgs	NA
		View Users	NA
		View AppInstance	NA
		View User Accounts	NA
		View User Entitlements	NA
Role Administrator	User Basic Info	Search Role	NA
	Org Basic Info	View Role	NA
		Create Role	Direct

**Table 13–3 (Cont.) Admin Roles and Permissions**

<b>Admin Role in Oracle Identity Manager</b>	<b>Implicit Permissions</b>	<b>Organization Scoped Permissions</b>	<b>Request or Direct Operation</b>
		Modify Role	Direct
		Delete Role	Direct
		View Role Members	NA
		Manage Role Hierarchy	Direct
		Publish role (only to allowed orgs)	Direct
		Unpublish role (only to allowed orgs)	Direct
		Manage Role Membership Rules	Direct
		Create Role Category	Direct
		Update Role Category	Direct
		Delete Role Category	Direct
		View Users	NA
		View Orgs	NA
		View Role Memberships	NA
Application Instance Administrator	User Basic Info	Create Application instance	Direct
	Org Basic Info	Modify Application instance	Direct
	Entitlement Administrator	Delete Application instance	Direct
		Search Application Instance	NA
		View Application Instance	NA
		Publish Application Instance (only to allowed orgs)	Direct
		Unpublish Application Instance (only to allowed orgs)	Direct
		Publish Entitlements (only to allowed orgs)	Direct
		Unpublish Entitlements (only to allowed orgs)	Direct
		Access Advanced UI	NA
		View accounts	NA
		View Users	NA
		View Orgs	NA
		View User Accounts	NA
		View User Entitlements	NA

**Table 13–3 (Cont.) Admin Roles and Permissions**

<b>Admin Role in Oracle Identity Manager</b>	<b>Implicit Permissions</b>	<b>Organization Scoped Permissions</b>	<b>Request or Direct Operation</b>	
Organization Administrator	User Basic Info	Search Org	NA	
	AppInstance Basic Info	View Org	NA	
	Entitlement Basic Info	Create Organization	Direct	
	Role Basic Info		Modify Organization	Direct
			Delete Organization	Direct
			All Role Admin Privileges for Admin Roles.	Direct
			Update Organization Hierarchy (for a specific organization)	Direct
			Associate password policy	Direct
			View members	NA
			View roles published	NA
			View app instances published	NA
			View entitlements published	NA
			View accounts (provisioned to org)	NA
	<b>Note:</b> Provisioning resources to organization is allowed only to the System Administrator.			
Entitlement Administrator	User Basic Info	Search Entitlements	NA	
	AppInstance Basic Info	View Entitlements	NA	
	Org Basic Info		add Entitlements (API)	Direct
			delete Entitlements (API)	Direct
			update Entitlements (API)	Direct
			Publish Entitlement (only to allowed orgs)	Direct
			Unpublish Entitlement (only from allowed orgs)	Direct
			View orgs	NA
			View User	NA
			View app instance	NA
			View accounts	NA
			View Entitlement Members	NA

**Table 13–3 (Cont.) Admin Roles and Permissions**

<b>Admin Role in Oracle Identity Manager</b>	<b>Implicit Permissions</b>	<b>Organization Scoped Permissions</b>	<b>Request or Direct Operation</b>
		View Published Entitlements (API) org data security applies	NA
Catalog Administrator	AppInstance Basic Info	Edit Catalog metadata	Direct
	Entitlement Basic Info	Create Request Profiles	Direct
	Role Basic Info	Modify Request Profiles	Direct
		Delete Request Profiles	Direct
		View application instances	NA
		View entitlements	NA
		View roles	NA
Role Authorizer	User Basic Info	View Role	NA
	Org Basic Info	Grant Role	Direct
		Revoke Role	Direct
		View Orgs	NA
		View Users	NA
		View Role Memberships	NA
Application Instance Authorizer	User Basic Info	Search Application Instance	NA
	Org Basic Info	View Application Instance (excluding passwords)	NA
		Grant account	Direct
		Revoke account	Direct
		Modify account	Direct
		Enable account	Direct
		Disable account	Direct
		View Org	NA
		View Entitlements	NA
		View Users	NA
		View User Accounts	NA
		View User Entitlements	NA
Entitlement Authorizer	User Basic Info	Search Entitlement	NA
	Org Basic Info	View Entitlement	NA
	AppInstance Basic Info	Grant Entitlement	Direct
		Revoke Entitlement	Direct
		View Users	NA
		View Orgs	NA

**Table 13–3 (Cont.) Admin Roles and Permissions**

<b>Admin Role in Oracle Identity Manager</b>	<b>Implicit Permissions</b>	<b>Organization Scoped Permissions</b>	<b>Request or Direct Operation</b>
		View Application Instance	NA
		View User Accounts	NA
		View User Entitlements	NA
Catalog System Administrator	App Instance Basic Info	Edit Catalog metadata	Direct
	Entitlement Basic Info	Create Request Profiles	Direct
	Role Basic Info	Modify Request Profiles	Direct
		Delete Request Profiles	Direct
		View Application Instances	NA
		View Entitlements	NA
		View Roles	NA
System Configuration Administrator	Role Basic Info	View Forms	NA
	Org Basic Info	Create Forms	NA
	Application Instance Basic Info	Modify Forms	NA
	Entitlement Basic Info	Delete Forms	NA
		Import Connector	NA
		Export Connector	NA
		View Resource Object	NA
		Create Resource Object	NA
		Modify Resource Object	NA
		Delete Resource Object	NA
		View Application Instance	NA
		Create Application Instance	NA
		Modify Application Instance	NA
		Delete Application Instance	NA
		Publish Application Instance	NA
		View Entitlement	NA
		Publish Entitlement	NA
		Delete Entitlement (using APIs)	NA

**Table 13-3 (Cont.) Admin Roles and Permissions**

<b>Admin Role in Oracle Identity Manager</b>	<b>Implicit Permissions</b>	<b>Organization Scoped Permissions</b>	<b>Request or Direct Operation</b>
		Modify Entitlement (using APIs)	NA
		Add Entitlement (using APIs)	NA
		View Approval Policies	NA
		Create Approval Policies	NA
		Modify Approval Policies	NA
		Delete Approval Policies	NA
		Access Advanced UI	NA
		View Password Policy	NA
		Create Password Policy	NA
		Modify Password Policy	NA
		Delete Password Policy	NA
		View Notification	NA
		Create Notification	NA
		Delete Notification	NA
		Modify Notification	NA
		Add Locale to Notification	NA
		Remove Locale To Notification	NA
		Complete Async Event Handlers	NA
		Orchestration Operation	NA
		Register Plugin	NA
		Unregister Plugin	NA
		View scheduled Jobs	NA
		Start Scheduler	NA
		Stop Scheduler	NA
		Add Task	NA
		Modify Task	NA
		Delete Task	NA
		Create Trigger	NA
		Delete Trigger	NA
		Modify Trigger	NA
		View Jobs	NA
		Create Jobs	NA

**Table 13-3 (Cont.) Admin Roles and Permissions**

<b>Admin Role in Oracle Identity Manager</b>	<b>Implicit Permissions</b>	<b>Organization Scoped Permissions</b>	<b>Request or Direct Operation</b>
		Modify Jobs	NA
		Delete Jobs	NA
		Enable Jobs	NA
		Disable Jobs	NA
		Run-now Jobs	NA
		Pause Jobs	NA
		Resume Jobs	NA
		Stop Jobs	NA
		Reset Status	NA
		View System Properties	NA
		Create System Properties	NA
		Modify System Properties	NA
		Delete System Properties	NA
		View Attributes	NA
		Add Attributes	NA
		Modify Attributes	NA
		Delete Attributes	NA
		Add Derived Attributes	NA
SPML Admin		Create, modify, and delete users	Request
		Search users on all the attributes	NA
		Enable user status	Request
		Disable user status	Request
		Add role memberships	Request
		Delete role memberships	Request
		Search roles on all the attributes	NA
		Create, modify, and delete roles	Request

---



---

**Note:** You can add a restriction on home organization permissions such that only a manager can view or modify the manager's reportees. To do so, open and delete the following policies by using the Authorization Policy Management (APM) UI:

- OrclOIMUserHomeOrgDirectWithAttributesPolicy
- OrclOIMUserHomeOrgDirectPolicy
- OrclOIMUserHomeOrgApprovalWithAttributesPolicy
- OrclOIMUserHomeOrgApprovalPolicy

For more information about the authorization policies used to control user's access to Oracle Identity Manager application, see the "Security Architecture" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

---



---

## 13.6 Delegable and Nondelegable Operations

There are some operations that can be delegated to other users (delegated administrators). These operations are:

- Create User
- Modify User
- Enable User
- Disable User
- Change Password
- Assign Roles
- Assign Organizations
- Assign Entitlements
- Provisioning Accounts
- Create and Manage Organization and Organization hierarchy
- Create and Manage Role and Role Hierarchy
- Create and Manage RO and IT Resource Instances

The following operations cannot be delegated to other users:

- Create and Manage Catalog
- Other System Administration Tasks
- Lookup Definition Management
- Password Policy Definition management

## 13.7 Evaluating Password Policies

Password policies are a list of rules or conditions that govern the syntax of the password. Password policies are created by System Administrators. For more information about creating and managing password policies, see the "Managing Password Policies" chapter in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

Organization administrators can attach a password policy to an organization either while creating an organization or at any later point in time. The procedure to create or modify an organization is discussed later in this chapter.

In Oracle Identity Manager, password policies are evaluated in the following scenarios:

- When users register themselves to Oracle Identity Manager to perform certain tasks in Identity Self Service or Oracle Identity System Administration.
- When users reset their password using the Forgot Password? link.
- When users change their enterprise password or target system account password from the Change Password section of the My Information page.
- When an administrator sets or changes the password of a user manually.

The following is the order in which a user's effective password policy is evaluated:

1. The password policy (if available) set for the user's home organization is applicable for the user.
2. If no password policy is set for the user's home organization, then the policy of the organization at the next level in the organization hierarchy of the user's home organization is picked. This procedure of identifying an organization at the next level in the hierarchy of the user's home organization continues until an organization associated with a password policy is determined. This password policy is applicable to the user.
3. If none of the organizations in the hierarchy has password policies set, then the password policy attached to the Top organization is applicable. If no password policy is attached to the Top organization, then the default password policy of the XellerateUsers resource is applicable.

## 13.8 Organization Management Tasks

The tasks related to organization management are performed in the Organizations section of Identity Self Service. The tasks are described in the following sections:

- [Searching Organizations](#)
- [Creating an Organization](#)
- [Viewing and Modifying Organizations](#)
- [Disabling and Enabling Organizations](#)
- [Deleting an Organization](#)

### 13.8.1 Searching Organizations

To search for organizations:

1. Log in to Identity Self Service.
2. In the left pane, under Administration, click **Organizations**. The Organization page is displayed.
3. Select any one of the following:
  - **All:** Search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.

- **Any:** Search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.
- 4. In the Organization Name field, enter the organization name search attribute that you want to search. To do so, select a search comparator. The default search comparator is Starts With. The Equals comparator is available in the list as an alternative.

You can use wildcard characters to specify the organization name.

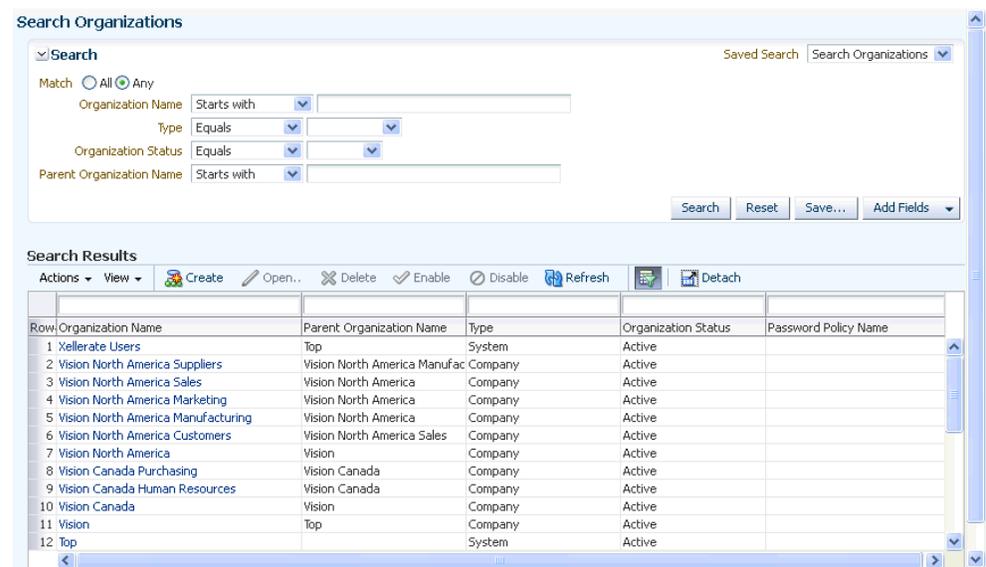
- 5. From the Type list, select the organization type. The organization type can be Branch, Company, or Department.
- 6. To add a field in your search:
  - a. Click **Add Fields**, and select a field, such as Organization Status.
  - b. Enter value for the search attribute that you added. In this example, from the Organization Status list, select the organization status, which can be Active, Deleted, or Disabled.

If you want to remove a field that you added in the search, then click the cross icon next to the field.

- 7. Click **Search**. The results are displayed in the search results table.

The search results table displays the organization name, parent organization name, organization type, and organization status, as shown in [Figure 13-2](#):

**Figure 13-2 Organization Search Results**

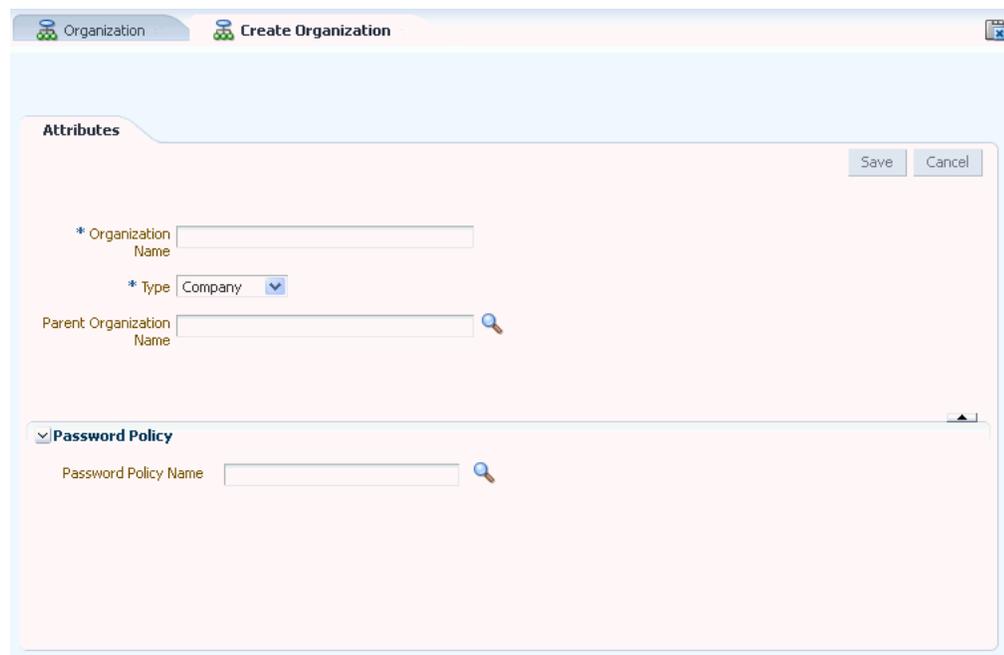


## 13.8.2 Creating an Organization

To create an organization:

1. In Identity Self Service, under Administration, click **Organizations**. The Organization page is displayed.
2. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Organization page is displayed, as shown in [Figure 13-3](#):

**Figure 13–3 The Create Organization Page**



3. In the Organization Name field, enter the name of the organization.
4. From the Type list, select the type of the organization, such as Branch, Company, or Department.
5. Specify the parent organization to which the newly created organization will belong. To do so:
  - a. Click the search icon next to the Parent Organization field. The Search Organizations dialog box is displayed.
  - b. Search and select the organization that you want to specify as the parent organization.
  - c. Click **Select**. The selected organization is added as the parent organization.
6. Specify a password policy name that you want to associate with the organization. To do so:
  - a. Click the search icon next to the Password Policy Name field. The Search Password Policy Name dialog box is displayed.
  - b. Search and select the password policy that you want to associate with the organization. To list all password policies, you can click the search icon, and then you can select the password policy from the search results.
  - c. Click **Add**. The selected password policy name is added to the Password Policy Name field.

**See Also:** "Managing Password Policies" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about creating and managing password policies
7. Click **Save** to create the organization.

### 13.8.3 Viewing and Modifying Organizations

The view organization operation allows you to view detailed organization profile information in the organization details page. You can view this page only if you are authorized to view the organization profile as determined by the authorization policy. If you have the authorization to modify the organization, then you can also modify the organization by using this page.

To open the details of an organization:

1. In Identity Self Service, under Administration, click **Organizations**. The Organization page is displayed.
2. Search and select the organization whose details you want to display.
3. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar. The details of the selected organization is displayed in a new page, as shown in [Figure 13–4](#):

**Figure 13–4** The Organization Details Page

You can perform administrative organization modifications in the organization details page. The modification is divided across the different sections of the organization details page, which means that modifications done in each section are independent of each other and must be saved individually. The modification for each section is described in the following sections:

- [Modifying Organization Attributes](#)
- [Managing Child Organizations](#)
- [Viewing Organization Membership](#)
- [Viewing Available Roles](#)
- [Managing Admin Roles](#)
- [Viewing Available Accounts](#)
- [Viewing Provisioned Accounts](#)
- [Viewing Available Entitlements](#)

### 13.8.3.1 Modifying Organization Attributes

The Attributes tab, as shown in [Figure 13–4](#), of the organization details page displays attributes of the organization. If you are authorized to modify the organization profile as determined by authorization policy, then the organization details page opens in editable mode, and you can modify organization information. You can modify the values for the attributes, and then click **Apply** to save the changes.

Whether or not the logged-in user is allowed to modify the organization is controlled by authorization policies. If you are not allowed to modify the organization, then the organization details page is displayed in read-only mode with no editable fields.

---

---

**Note:** The Status attribute in the organization details page is read-only.

---

---

### 13.8.3.2 Managing Child Organizations

The Children tab displays a list of child organizations that the open organization has. For each child organization in the list, the organization name, organization type, and organization status are displayed.

The Children tab enables you to perform the following:

- [Creating a Child Organization](#)
- [Deleting a Child Organization](#)
- [Disabling a Child Organization](#)
- [Enabling a Child Organization](#)
- [Opening a Child Organization](#)

#### 13.8.3.2.1 Creating a Child Organization

In the Children tab, you can create a child organization or suborganization of the open organization by selecting **Create Sub-org** from the Actions menu. Alternatively, click **Create Sub-org** on the toolbar. The Create organization page is displayed. Perform the steps described in "[Creating an Organization](#)" on page 13-19 to complete creating the child organization.

#### 13.8.3.2.2 Deleting a Child Organization

To delete a child organization:

1. In the Children tab, select the organization you want to delete.
2. From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar. A message is displayed asking for confirmation.
3. Click **Yes** to confirm. The selected child organization is deleted.

#### 13.8.3.2.3 Disabling a Child Organization

To disable a child organization:

1. In the Children tab, select the organization you want to disable.
2. From the Actions menu, select **Disable**. Alternatively, click **Disable** on the toolbar. A message is displayed asking for confirmation.
3. Click **Yes** to confirm. The selected child organization is disabled.

#### 13.8.3.2.4 Enabling a Child Organization

To enable a child organization:

1. In the Children tab, select the organization you want to enable.
2. From the Actions menu, select **Enable**. Alternatively, click **Enable** on the toolbar. A message is displayed asking for confirmation.
3. Click **Yes** to confirm. The selected child organization is enabled.

#### 13.8.3.2.5 Opening a Child Organization

From the Children tab, you can open the details of a child organization by selecting the organization, and selecting **Open** from the Actions menu. Alternatively, you can click **Open** on the toolbar, or simply click the name of the organization.

To modify a child organization, click the child organization name that you want to modify. The organization details page for the selected organization is displayed, by using which you can modify the details of that organization.

#### 13.8.3.3 Viewing Organization Membership

The Members tab is a read-only tab that displays a list of users in the selected organization. For each user in the list, the following are displayed:

- User Login
- Display Name
- First Name
- Last Name
- Email

**Tip:** You can add or remove users to and from organizations by using the Attributes tab of the user details page.

#### 13.8.3.4 Viewing Available Roles

You can view the roles in an organization by clicking the **Available Roles** tab of the organization details page. The role names, role categories, and corresponding organization names are listed in this tab.

#### 13.8.3.5 Managing Admin Roles

You can view the admin roles that are assigned to an organization by clicking the **Admin Roles** tab of the organization details page. The admin roles and their corresponding description are listed in this tab. When you select an admin role, the users who have the selected admin role are displayed in the User Members section. This tab also allows you to grant and revoke admin roles available to the open organization to users.

In the Admin Roles tab, you can perform the following:

- [Granting an Admin Role](#)
- [Revoking an Admin Role](#)

##### 13.8.3.5.1 Granting an Admin Role

To grant an admin role to a user:

1. In the organization details page, click the **Admin Roles** tab. A list of admin roles assigned to the open organization is displayed.
2. Select the admin role that you want to grant to a user.
3. Click **Assign** on the toolbar. The Advanced Search for Target Users dialog box is displayed.
4. Search for the target users to whom you want to grant the selected admin role. You can select the **Just show my directs** option to list only your direct reports.
5. In the User Results section, select the user that you want to grant the admin role.
6. Click **Add Selected** to move the selected user to the Selected Users section. Alternatively, you can click **Add All** to move all the users from the User Results section to the Selected Users section.
7. Click **Add**. The admin role is granted to the selected user. When you click the admin role in the Admin Roles tab, the selected user's record is displayed in the User Members section.
8. In the User Members section, select the user record. Select **include sub-orgs** to grant the admin role to the user's organization and its suborganizations. If you want to grant the admin role to the user's organization only, then do not select this option.

#### 13.8.3.5.2 Revoking an Admin Role

To revoke an admin role from a user:

1. In the Admin Roles tab, select an admin role from which you want to revoke the user.
2. In the User Members section, select the user from whom you want to revoke the admin roles.
3. From the Actions menu, select **Revoke**. Alternatively, click **Revoke** on the toolbar. A message is displayed asking for confirmation.
4. Click **Revoke** to confirm. The user record is no longer displayed when you select the admin role.

#### 13.8.3.6 Viewing Available Accounts

The accounts available to an organization are the accounts that have been published to the organization. This means that the accounts are available for requesting by the users of the organization. You can view the available accounts in an organization by clicking the **Available Accounts** tab in the organization details page.

#### 13.8.3.7 Viewing Provisioned Accounts

The Provisioned Accounts tab displays the accounts that have been provisioned to the open organization.

In the Provisioned Accounts tab, you can perform the following:

- [Provisioning an Account](#)
- [Revoking an Account](#)
- [Viewing the Details of a Provisioned Account](#)
- [Disabling a Provisioned Account](#)
- [Enabling a Provisioned Account](#)

### 13.8.3.7.1 Provisioning an Account

To provision an account to an organization:

1. In the Provisioned Accounts tab, select the account that you want to provision.
2. From the Actions menu, select **Provision**. Alternatively, you can create **Provision** on the toolbar.

The Provision Resource to Organization page is displayed in a new window.

3. On the Step 1: Select a Resource page, select a resource from the list, and then click **Continue**.
4. On the Step 2: Verify Resource Selection page, click **Continue**.
5. On the Step 5: Provide Process Data page, enter the details of the account that you want to provision to the organization, and then click **Continue**.
6. On the Step 6: Verify Process Data page, verify the data that you have provided, and then click **Continue**. The "Provisioning has been initiated" message is displayed.

### 13.8.3.7.2 Revoking an Account

To revoke an account from an organization:

1. In the Provisioned Accounts tab, select the account that you want to revoke.
2. From the Actions menu, select **Revoke**. Alternatively, you can click **Revoke** on the toolbar.

A message is displayed asking for confirmation.

3. Click **Yes**.

### 13.8.3.7.3 Viewing the Details of a Provisioned Account

To view the details of a provisioned account:

1. In the Provisioned Accounts tab, select the account you want to open.
2. From the Actions menu, select **Open**. Alternatively, you can click **Open** on the toolbar.

The details of the account is displayed in a new page.

### 13.8.3.7.4 Disabling a Provisioned Account

To disable a provisioned account:

1. In the Provisioned Accounts tab, select the account you want to disable.
2. From the Actions menu, select **Disable**. Alternatively, you can click **Disable** on the toolbar.

A message is displayed stating that the provisioned account has been successfully disabled.

### 13.8.3.7.5 Enabling a Provisioned Account

To enable a provisioned account:

1. In the Provisioned Accounts tab, select the account you want to enable.
2. From the Actions menu, select **Enable**. Alternatively, you can click **Enable** on the toolbar.

A message is displayed stating that the provisioned account has been successfully enabled.

### 13.8.3.8 Viewing Available Entitlements

You can view the entitlements published to the open organization by clicking the **Available Entitlements** tab. For each entitlement, the following information is displayed:

- Entitlements name
- Resource associated with the entitlement
- Account name associated with the entitlement
- Organization name

## 13.8.4 Disabling and Enabling Organizations

---

---

**Note:** You cannot disable organizations with child organizations or users. You can force disable it only by setting the system property `ORG.DISABLEDELETEACTIONENABLED` to true. After you set this property, the users and suborganizations will be disabled while disabling the parent organization.

---

---

To disable an organization with enabled state:

1. In the organization details page, click **Disable** on the top of the page. Alternatively, in the search result for organizations in the Organization page, select the organization, and from the Actions menu, select **Disable**.  
A message is displayed asking for confirmation.
2. Click **Disable** to confirm.

To enable an organization with disabled state:

1. In the search result for organizations in the Organization page, select the organization that you want to enable.
2. From the Actions menu, select **Enable**. A message is displayed asking for confirmation.
3. Click **Enable** to confirm.

## 13.8.5 Deleting an Organization

---

---

**Note:**

- You cannot delete organizations with child orgs or users. You can force delete it only by setting the system property `ORG.DISABLEDELETEACTIONENABLED` to true. Once you set the property, the users and sub orgs will be deleted while deleting the parent org.
  - You can delete an organization only if you have the "Delete" permission for that organization.
  - The deleted record would still exist in the database, marked deleted.
- 
- 

To delete an organization:

1. In the search result for organizations in the Organization page, select the organization that you want to delete.
2. From the Actions menu, select **Delete**. Alternatively, you can click Delete on top of the organization details page. A message is displayed asking for confirmation.
3. Click **Delete** to confirm.



---



---

## Using the Attestation Dashboard

You use the Attestation Dashboard to view the state of attestation processes that are owned by any group of which you are a member.

To use the Attestation Dashboard, log in to Oracle Identity Self Service, and under Administration, click **Attestation Dashboard**. The Attestation Dashboard page displays a table listing the state of attestation processes that are owned by any group of which you are a member. The Attestation Dashboard table contains the columns listed in the following table:

Column	Description
Process Code	The attestation process code.
Process Name	The name of the process. The Attestation Process Detail page is displayed when the link for an attestation process name is clicked.
Last Completion	The date and time when the instance was run before the latest one was completed. If it does not exist, then the value must be None. It is a link that takes the user to the Attestation Request Detail page for the required Attestation Request.
Current Request Date	The date and time when the last instance of this Process was run. If it has never been run, then the value is New. It is a link that takes the user to the Attestation Request Detail page for the required Attestation Request.
Current Completion	The date and time when the last instance run was completed. If it has not been completed, then the value is Pending.
Total Records	The total number of entitlements identified for attestation and covered by an attestation task as part of the last process instance.
Certified	The number of entitlements certified in the last attestation process instance.
Rejected	The number of entitlements rejected in the last attestation process instance.
Open	All the open records for which no responses have been provided by the reviewers.

### 14.1 Viewing Attestation Request Details

You can access the drill-down page from the Attestation Dashboard page. The drill-down page displays the attestation details of all entitlements covered by a particular run of the Attestation Process.

To view attestation request details:

1. Click the link for the Last Completion or Current Request Page fields listed in the table on the Attestation Dashboard page.

The Attestation Request Detail page displays the request details for the selected attestation process, along with a table that contains the following columns:

Column	Description
User	User whose entitlement is being attested. The data is displayed as a link. When you click the link, the user profile page is displayed with the user details for the attestation date.
Resource	Resource that is the basis for the entitlement being attested. The data is displayed as a link. When you click the link, a page is displayed with the process form data of the entitlement for the attestation date.
Descriptive Data	Description of the provisioned resource instance.
Comments	Comment or status of the request. The value can be one of the following: <ul style="list-style-type: none"> <li>▪ Certify</li> <li>▪ Reject</li> <li>▪ Open</li> <li>▪ Closed</li> </ul>
Attestation Result	Last response that was provided for the attestation.
Reviewer	User who provided the response. The data is displayed as a link. When you click the link, the user profile page is displayed with the current user details.
Delegation Path	If the attestation of an entitlement goes through any delegation, then you can use the View link in this column to see the Delegation Path Detail page. If no delegation has taken place, then None is displayed.
Comments	Reviewer comments. Long comments are truncated, and tooltips are used to show the full text of the comments.

2. Any attestation requests that require delegation include a link in the Delegation Path column.

Clicking the link displays a Delegation Path page that provides information about the delegation path of the attestation request.

The Data Attested field shows details about the entitlement being attested. It constructs the value by putting together user information, the resource name, and descriptive data in the following format:

*User\_First\_Name User\_Last\_Name [User\_ID] - Resource\_Name - Descriptive\_Data*

The table on the Delegation Path page contains the following fields:

Column	Description
Reviewer	The reviewer to whom the entitlement for attestation is assigned. The data is displayed as a link. When you click the link, the current user profile data is displayed.
Attestation Result	Action supplied by the reviewer. Except for the first record, the value is always Delegated.
Attestation Date	The date and time of the attestation response of the reviewer.

Column	Description
Comments	Reviewer comments. Long comments are truncated, and tooltips are used to show the full text of the comments.

## 14.2 E-Mail Notification

As part of the attestation process, the attestation engine sends e-mail to concerned parties at various stages. You can configure e-mail content by using e-mail templates of the General type in Oracle Identity Manager Email Definition store.

In the templates, the form user is defined as XELSYSADM. You can change it to a different user. You must ensure that the e-mail address is defined for the user selected to use these templates. Otherwise, the system may not be able to send out notifications.

The following e-mail notification templates are available:

- **Notify Attestation Reviewer:** Used for sending e-mail when an attestation task is assigned to a reviewer.
- **Notify Delegated Reviewers:** Used for sending e-mail to reviewers when an attestation task is delegated to them.
- **Notify Declined Attestation Entitlements:** Used for sending e-mail to users in the Process Owner group if a reviewer declines any entitlements.
- **Attestation Reviewers With No E-Mail Defined:** Used for sending e-mail to users in the Process Owner group if an e-mail address is not defined for any of the reviewers.

## 14.3 Attestation Grace Period Checker Scheduled Task

A system scheduled task called Attestation Grace Period Checker is used to examine the attestation processes defined in Oracle Identity Manager and to create the required attestation tasks.

The features of the Attestation Grace Period Checker scheduled task are:

- The scheduled task is set to run every 30 minutes by default. You can change this according to your requirement.
- The scheduled task examines all active attestation processes.



---

---

## Using Identity Certification

This chapter provides an overview of identity certification, describes the identity certification user interface, and includes information about how to complete identity certifications. It contains the following topics:

- [Identity Certification Overview](#)
- [Certification UI](#)
- [Certification Name Formats](#)
- [Searching and Viewing Certifications](#)
- [Completing User Certifications in Offline Mode](#)
- [Generating Certification Reports](#)

### 15.1 Identity Certification Overview

This section describes what, why, and how identity certifications are conducted. It also discusses who is typically involved in the identity certification process.

#### 15.1.1 What Is Identity Certification?

Identity certification is the process of reviewing user entitlements and access-privileges within an enterprise to ensure that users have not acquired entitlements that they are not authorized to have. It also involves either approving (certifying) or rejecting (revoking) each access-privilege.

Certifications can be scheduled to run on a regular basis to meet compliance requirements. Managers use the identity certification feature to review their employees' entitlements to access applications and data. Based on changes reported by the identity certification module, managers can authorize or revoke employee access as needed.

You can create four types of certifications. Each type of certification addresses a particular use-case—a specific type of review that enterprises commonly perform. Each type of reviewer reviews a different subset of access-related data from a specific point of view.

[Table 15-1](#) lists the four types of identity certification that are possible in Oracle Identity Manager.

**Table 15–1 The Four Types of Identity Certification**

Identity Certification Type	Description
User Certification	<p>Allows managers to certify employee access to roles, accounts, and entitlements. Typically, each manager in an organization reviews the access-privileges of the people who report directly to that manager. Each reviewer in a certification of this type is focused on his or her direct-reports, but is expected to review all of the access-privileges for each direct report.</p> <p>User certification optimizes review from the perspective of the line-of-business (LOB) manager, who must review all access-privileges for each user who reports to the LOB manager.</p> <p>User certification also supports a two-phased review, in which user access rights can be reviewed by managers first, and subsequently by any of the other IT owners, such as role owner, application instance owner, or entitlement owner, all within a single certification campaign.</p>
Role Certification	<p>Allows role owners to certify role content and/or role members. This certification is used in organizations that have implemented role-based access control (RBAC). Typically, the owner of a role is the person responsible for reviewing its definition (that is, the set of access-privileges that it conveys) as well as its membership (the set of users to whom the role has been assigned). Each reviewer in a certification of this type is focused on a particular enterprise role.</p> <p>Role certification optimizes review from the perspective of the role authorizer or role administrator, who must review the definition and the membership of each role that are owned by the role authorizer or role administrator.</p>
Application Instance Certification	<p>This certification allows the person who is responsible for a particular system or application to review the set of users who have accounts on that system or application. The reviewer can drill down and view the details of the access-privileges of each account. Each reviewer in a certification of this type is focused on one specific system or application.</p> <p>Application instance certification optimizes review from the perspective of the Application Instance Authorizer or Application Instance Administrator, who must review the membership (accounts) and the set of privileges (entitlement-assignments) for each application that are owned by the Application Instance Authorizer or Application Instance Administrator.</p>
Entitlement Certification	<p>Allows entitlement owners to certify user accounts that have a particular privilege. This certification is used if a specific person is responsible for a particular entitlement (that is, an Attribute Value or a group membership that confers a specific access-privilege). The entitlement owner can review the set of user accounts that have that particular entitlement. Each reviewer in a certification of this type is focused on one specific privilege within one specific resource.</p> <p>Entitlement certification optimizes review from the perspective of the Entitlement Authorizer or Entitlement Administrator, who must review the definition and the membership (entitlement-assignments) for each privilege (entitlement-definition) that are owned by the Entitlement Authorizer or Entitlement Administrator.</p>

A scheduled job generates certifications based on a specified certification definition. Oracle Identity Manager applies the selection criteria within the certification definition

to select the privilege assignments (and/or privilege definitions) that will be reviewed and by whom. Oracle Identity Manager generates a separate certification for each primary reviewer. Oracle Identity Manager also generates a review task for each primary reviewer. Oracle Identity Manager creates a new review task whenever a primary reviewer delegates or reassigns line-items to another reviewer. As each reviewer acts on the review task assigned to that reviewer, this updates the overall certification. Overall progress for each certification is visible from the Dashboard.

## 15.1.2 Who Is Involved in Completing Identity Certifications?

Identity certification allows personnel in an organization to review and certify user entitlement data, role content data, application instance data, and entitlement data. Following are descriptions of the types of users that are typically involved in the identity certification process, as well as the certifications that each user type can authorize or revoke. In Oracle Identity Manager, personnel who participate in the identity certification process are called *reviewers*.

Table 15–2 lists the reviewers involved in identity certification.

**Table 15–2 Identity Certification Reviewers**

Reviewer Name	Description	Certification Types That Can Be Accessed
Certifier	A generic term that signifies a person who is responsible for reviewing and completing any kind of certification.	<ul style="list-style-type: none"> <li>■ User certification</li> <li>■ Role certification</li> <li>■ Application instance certification</li> <li>■ Entitlement certification</li> </ul>
User manager	A manager with direct reports. Users report to a user manager.	<ul style="list-style-type: none"> <li>■ User entitlement</li> </ul>
Business reviewer	<p>A user within an enterprise who reviews the access-privileges of other users from a business-oriented perspective. Typically, this is a Line-Of-Business (LOB) manager who is responsible for the access-privileges of users who report to him/her.</p> <p><b>Note:</b> LOB is a category of industry or business function. For example, an LOB manager is oriented to a business function within an enterprise, such as Sales.</p>	<ul style="list-style-type: none"> <li>■ User certification</li> <li>■ Role certification</li> <li>■ Application instance certification</li> <li>■ Entitlement certification</li> </ul>
Primary Reviewer	The person who is primarily responsible for making certification decisions on a particular set of line-items. The primary reviewer can reassign a line-item to another user, in which case that user becomes the new primary reviewer for that line-item, and the original primary reviewer never sees that line-item again. The primary reviewer can also delegate any of his line-items to another person, in which case that user becomes the delegated reviewer for that line-item, but the primary reviewer still retains responsibility for that line-item.	<ul style="list-style-type: none"> <li>■ User certification</li> <li>■ Role certification</li> <li>■ Application instance certification</li> <li>■ Entitlement certification</li> </ul>

**Table 15–2 (Cont.) Identity Certification Reviewers**

Reviewer Name	Description	Certification Types That Can Be Accessed
Technical Reviewer	A user within an enterprise who reviews the access-privileges of others from a technically-oriented perspective. Typically, this is an IT expert or an application-owner who is responsible for access-privileges being specified correctly, or for limiting access within the enterprise to a specific access-privilege.	<ul style="list-style-type: none"> <li>■ User certification</li> </ul>
Delegated Reviewer	A person who is assigned to help with the certification work. The delegated reviewer is secondarily responsible for making certification-decisions on a particular set of line-items, but the primary reviewer remains ultimately responsible. Any decision made by the delegated reviewer eventually returns to the primary reviewer, who can override that decision.	<ul style="list-style-type: none"> <li>■ User certification</li> <li>■ Role certification</li> <li>■ Application instance certification</li> <li>■ Entitlement certification</li> </ul>
Final Reviewer	<p>The person who has the final say over the certification-decisions. The final reviewer can review and override the certification decisions of other reviewers.</p> <p>Final Review is performed only after a two-phased review (and only when an administrator has configured the certification-definition to enable this). The primary reviewer from the first phase can then make a final review of the certification actions made by all the reviewers in the first two phases.</p>	<ul style="list-style-type: none"> <li>■ User Certification</li> </ul>

## 15.2 Certification UI

You can view and work with certification objects by using the following in Oracle Identity Self Service:

- **Inbox:** The Inbox lists all the tasks assigned to the logged-in user in a single screen. It enables the logged-in user to filter task views into user preferences, such as assigned tasks, completed tasks, and tasks for which information has been requested. The user can select a task to open it in a new tab and then perform necessary actions on the task. This allows the user to work on multiple tasks at a time by opening them in different tabs. The Inbox also allows the user to search tasks, organize them in views, and create shared views.

To access the Inbox, login to Oracle Identity Self Service, and click **Inbox** on the left navigation pane.

**See Also:** "[Managing Certification Review Tasks](#)" on page 10-11 for detailed information about the Inbox and the operations you can perform by using the Inbox

- **Dashboard:** The Identity Certification Dashboard provides an overview of in-progress and completed certifications in the system. The certifications displayed

in the dashboard depends on your role. A user with either the Certification Administrator or Certification Viewer admin role can see all certifications in the system. A non-administrative user, for example, a manager, can see any certification for which that user is assigned as a primary reviewer. A primary reviewer or user with the Certification Viewer admin role can view the certification information. A user assigned the Certification Administrator admin role can view any certification, and take basic actions on in-progress certifications.

To access the Dashboard, login to Oracle Identity Self Service, and click **Dashboard** under Certifications on the left navigation pane.

### 15.3 Certification Name Formats

The certification task names are displayed in different formats depending on the review phase and reviewer. Table 15–3 lists the certification task names in various review phases.

**See Also:** "Understanding Multi-Phased Review in User Certification" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about the review phases in multi-phased review for user certification

**Table 15–3 Certification Name Formats**

Review Phase	Name Format	Example
Phase 1 (P1)	CERT_DEFINITION[ P1_PRIMARY_REVIEWER ]	Q1 Access 2012[ Robert Klein ]
Phase 1 Reassign	CERT_DEFINITION[ P1_PRIMARY_REVIEWER ]Reassigned[ NEW_PRIMARY_REVIEWER ]	Q1 Access 2012[ Robert Klein ]Reassigned[ Jane Doe ]
Phase 1 Delegate	CERT_DEFINITION[ P1_PRIMARY_REVIEWER ]Delegated[ P1_DELEGATED_REVIEWER ]	Q1 Access 2012[ Robert Klein ]Delegated[ Jane Doe ]
Phase 1 Verification	CERT_DEFINITION[ P1_PRIMARY_REVIEWER ]Verification	Q1 Access 2012[ Robert Klein ]Verification
Phase 2 (P2)	CERT_DEFINITION[ P1_PRIMARY_REVIEWER ]Roles[ P2_TECHNICAL_REVIEWER ]	Q1 Access 2012[ Robert Klein ]Roles[ Terence Hill ]
	CERT_DEFINITION[ P1_PRIMARY_REVIEWER ]Application Instances[ P2_TECHNICAL_REVIEWER ]	Q1 Access 2012[ Robert Klein ]Application Instances[ Martha Smith ]
	CERT_DEFINITION[ P1_PRIMARY_REVIEWER ]Entitlements[ P2_TECHNICAL_REVIEWER ]	Q1 Access 2012[ Robert Klein ]Entitlements[ Hattori Hanzo ]
Phase 2 Reassign	CERT_DEFINITION[ P1_PRIMARY_REVIEWER ]Roles[ P2_TECHNICAL_REVIEWER ]Reassigned[ NEW_P2_TECHNICAL_REVIEWER ]	Q1 Access 2012[ Robert Klein ]Roles[ Terrence Hill ]Reassigned[ Jane Doe ]
	CERT_DEFINITION[ P1_PRIMARY_REVIEWER ]Application Instances[ P2_TECHNICAL_REVIEWER ]Reassigned[ NEW_P2_TECHNICAL_REVIEWER ]	Q1 Access 2012[ Robert Klein ]Application Instances[ Martha Smith ]Reassigned[ Jane Doe ]

**Table 15–3 (Cont.) Certification Name Formats**

Review Phase	Name Format	Example
	<i>CERT_DEFINITION</i> [ <i>P1_PRIMARY_REVIEWER</i> ]Entitlements[ <i>P2_TECHNICAL_REVIEWER</i> ]Reassigned[ <i>NEW_P2_TECHNICAL_REVIEWER</i> ]	Q1 Access 2012[ Robert Klein ]Entitlements[ Hattori Hanzo ]Reassigned[ Jane Doe ]
Phase 2 Delegate	<i>CERT_DEFINITION</i> [ <i>P1_PRIMARY_REVIEWER</i> ]Roles[ <i>P2_TECHNICAL_REVIEWER</i> ]Delegated[ <i>NEW_P2_TECHNICAL_REVIEWER</i> ]	Q1 Access 2012[ Robert Klein ]Roles[ Terrence Hill ]Delegated[ Jane Doe ]
	<i>CERT_DEFINITION</i> [ <i>P1_PRIMARY_REVIEWER</i> ]Application Instances[ <i>P2_TECHNICAL_REVIEWER</i> ]Delegated[ <i>NEW_P2_TECHNICAL_REVIEWER</i> ]	Q1 Access 2012[ Robert Klein ]Application Instances[ Martha Smith ]Delegated[ Jane Doe ]
	<i>CERT_DEFINITION</i> [ <i>P1_PRIMARY_REVIEWER</i> ]Entitlements[ <i>P2_TECHNICAL_REVIEWER</i> ]Delegated[ <i>NEW_P2_TECHNICAL_REVIEWER</i> ]	Q1 Access 2012[ Robert Klein ]Entitlements[ Hattori Hanzo ]Delegated[ Jane Doe ]
Phase 2 Verification	<i>CERT_DEFINITION</i> [ <i>P1_PRIMARY_REVIEWER</i> ]Roles[ <i>P2_TECHNICAL_REVIEWER</i> ]Verification	Q1 Access 2012[ Robert Klein ]Roles[ Terrence Hill ]Verification
	<i>CERT_DEFINITION</i> [ <i>P1_PRIMARY_REVIEWER</i> ]Application Instances[ <i>P2_TECHNICAL_REVIEWER</i> ]Verification	Q1 Access 2012[ Robert Klein ]Application Instances[ Martha Smith ]Verification
	<i>CERT_DEFINITION</i> [ <i>P1_PRIMARY_REVIEWER</i> ]Entitlements[ <i>P2_TECHNICAL_REVIEWER</i> ]Verification	Q1 Access 2012[ Robert Klein ]Entitlements[ Hattori Hanzo ]Verification
Final review	<i>CERT_DEFINITION</i> [ <i>P1_PRIMARY_REVIEWER</i> ]Final Review	Q1 Access 2012[ Robert Klein ]Final Review

## 15.4 Searching and Viewing Certifications

This section describes how to search and filter certifications in the Inbox and Dashboard, and how to view the details of certifications in the following sections:

- [Searching Certifications in the Dashboard](#)
- [Viewing Certifications From the Dashboard](#)

### 15.4.1 Searching Certifications in the Dashboard

To search for certifications:

1. Login to Oracle Identity Self Service.
2. On the left pane, under Certifications, click **Dashboard**. The Dashboard is displayed with a list of certifications in a table. The table consists of columns, such as Name, Percent Complete, and Organization.

You can personalize the table to display or hide certification attributes that are displayed as columns in the table. You can also change the order in which the columns are displayed in the table.

3. To show or hide columns and change the order of the columns, follow the instructions in "[Personalizing the Search Result](#)" on page 5-5.

4. From the Show list, select any one of the following to filter the list of certifications displayed in the Dashboard:
  - **New and In Progress:** Lists the certifications that are assigned to you and the certifications in progress.
  - **New:** Lists only the new certifications that are assigned to you.
  - **In Progress:** Lists only the certifications in progress.
  - **Expired:** Lists the certifications whose end date has passed.
  - **Completed:** Lists the certifications that are in the completed state.
  - **All:** Lists all types of certifications including new, in progress, and expired certifications.
5. From the Search list, select any one of the following, and enter a search criterion in the box adjacent to the list:
  - **Certification Name:** To search the certifications by certification name.
  - **Organization Name:** To search the certifications by the organization name selected for the certification.
  - **Create Date:** To search the certifications by certification creation date.
6. Click the Search icon. The certifications that match your search criteria are displayed in the table.

**Tip:** To sort the data in the search results table, place the mouse pointer on a column name. Up and down arrows are displayed on the column names. Click the up arrow to sort in ascending order. Click the down arrow to sort in descending order.

## 15.4.2 Viewing Certifications From the Dashboard

You can open and view certification details from the Inbox or the Dashboard. However, all users cannot see the certifications in the Dashboard. Only the primary reviewers, who have been selected as certifiers during the certification creation process, can see the certifications in the Dashboard. All other users can access certification tasks only from the Inbox. For example, the delegated reviewers cannot see the particular certification in the Dashboard, but can see a certification task in the Inbox. Similarly, phase 2 reviewers for user certification cannot see any certification in the Dashboard.

**See Also:** "Understanding Multi-Phased Review in User Certification" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about the phases of reviews in multi-phased review for user certification

To open and view certification details from the Dashboard:

1. Open the Dashboard.
2. Select the certification for which you want to display the details. A summary of the selected certification is displayed in the Detail Information section, which consists of the following tabs:
  - **Certification Details:** Displays the certification attributes such as name, percentage complete, and number of roles, accounts, entitlements, or users for the selected certification. A link to the requests page is also displayed if closed-loop remediation has been activated for the certification.

For information about closed-loop remediation and remediation tracking, see "Understanding Closed-Loop Remediation and Remediation Tracking" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*. For information about the Track Requests page, see "Tracking a Request" on page 9-20.

- **Reports:** Enables you to generate certification reports. This tab is displayed only if the report option is configured in Oracle Identity Manager. See "Generating Certification Reports" on page 15-10 for details.
- 3. From the Actions menu, select **Open**. Alternatively, you can click **Open** on the toolbar, or click the certification name to open it. The details of the selected certification is displayed in the certification details page.

In both Inbox and the Dashboard, you can also click the certification name to open the details of the certification.

The certification details is displayed in a tabular format. You can hide, unhide, and re-order columns in the table. For details, see "Personalizing the Search Result" on page 5-5. In addition, you can use the saved search feature in this page to search for the details. For information about creating and using saved search, see "Using Saved Search" on page 5-6.

## 15.5 Completing User Certifications in Offline Mode

You have the option to download user certification data to your local computer and work on it in an offline mode by using Microsoft Excel without having an active session with Oracle Identity Manager. After making decisions on the certifications, you can connect to Oracle Identity Manager and upload your decisions. The availability of this option can be controlled by enabling or disabling the **Enable Interactive Excel** option in the Certification Configuration page in Oracle Identity System Administration. For information about this option, see "Configuring Certification Options in Identity System Administration" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

---



---

### Note:

- The option to download user certification data to your local computer and work on it in an offline mode is available for user certifications only. This functionality is not available for role, application instance, and entitlement certifications.
  - For this functionality to work, you must have Microsoft Excel 2007 or 2010. To configure Microsoft Excel for this functionality, perform the steps provided at the following URL:  
[http://docs.oracle.com/cd/E18941\\_01/tutorials/jdtut\\_11r2\\_59/jdtut\\_11r2\\_59\\_1.html](http://docs.oracle.com/cd/E18941_01/tutorials/jdtut_11r2_59/jdtut_11r2_59_1.html)
- 
- 

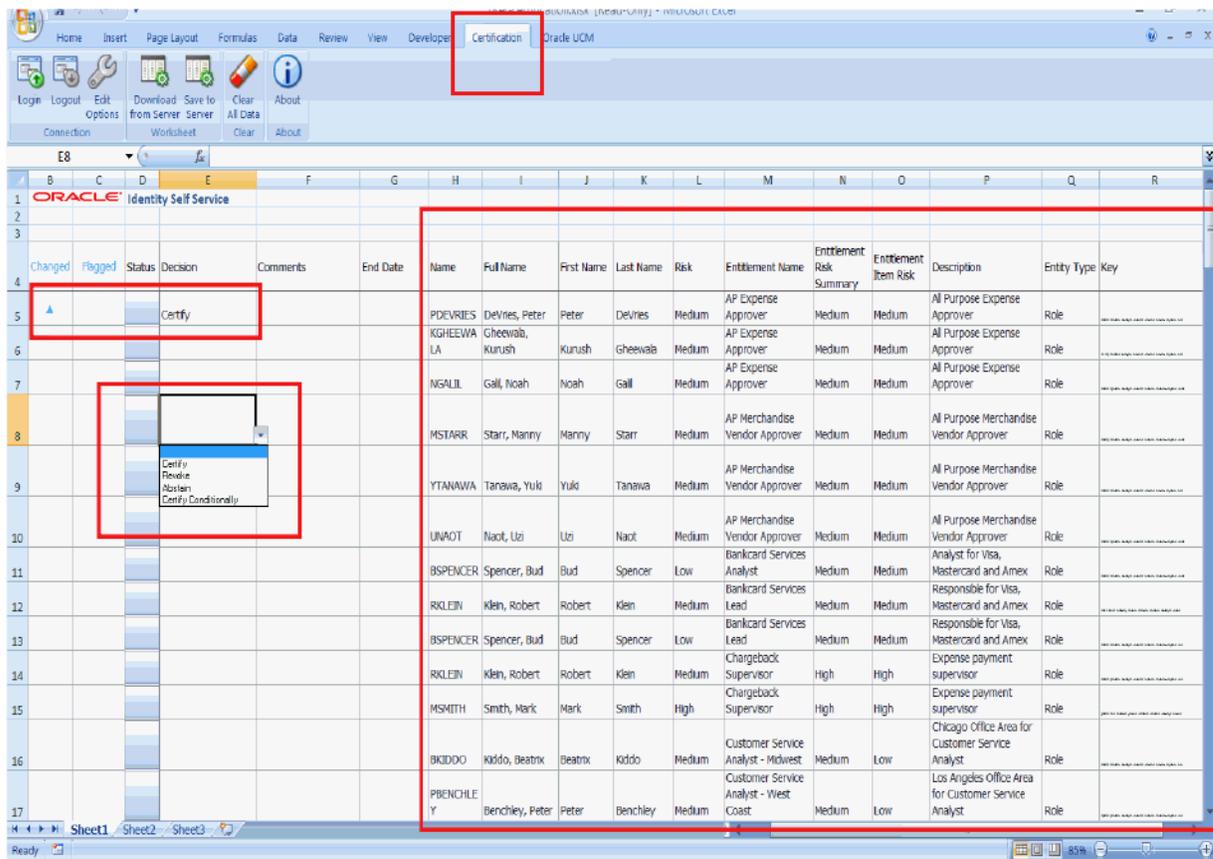
When the **Enable Interactive Excel** option is enabled, the **Download to Editable Excel** menu option is available in the Actions menu in the certification detail and certification summary pages of the user certification.

To work on a user certification in offline mode:

1. Open a user certification from the Dashboard or Inbox.
2. From the Actions menu, select **Download to Editable Excel**. A message box is displayed with the options to open or save the file.

3. Select **Open with**.
4. Make sure that **Microsoft Office Excel** is selected instead of Microsoft Office Excel (Default). Microsoft Office Excel (Default) is the version of Excel for which the plugin for this functionality is not enabled.
5. Click **OK**. A message box is displayed asking whether you want to connect to the corresponding server where the application is running and from where the spreadsheet was downloaded.
6. Click **Yes**. The page to login to Oracle Identity Self Service is displayed. This provides an extra layer of security before you can download the data to work on.
7. Login to Oracle Identity Self Service by providing the credentials. The user certification data is downloaded into a spreadsheet.
8. Click the **Certification** tab. This displays the list of options available when you work on a record. [Figure 15-1](#) shows the Certification tab.

**Figure 15-1 The Certification Tab**



9. Select the decisions from the drop-down for each user. When a decision is selected, the Changed column displays a flag that indicates the change. The area highlighted in grey color is a read-only area and no changes can be made there.

Decisions other than Certify cannot be updated unless certain conditions are met, and as a result, the data upload will fail. To view these errors, double-click the error field under the status column. Then, you can perform the necessary action to fix it before trying to upload again. The actions can be:

- Revoke: Comments are required.

- Abstain: Comments are required.
- Certify Conditionally: Comments and an end date are required.

---



---

**Note:** User-defined field (UDF) data for both user and catalog will show up in the spreadsheet as read-only columns.

---



---

10. When you finish selecting the decisions, you can upload the data back to the server by clicking the **Save to Server**. The user data is updated on the user certification screens.

---



---

**Note:** When you upload the spreadsheet data, if the application instance and entitlement decisions are different, the decisions for entitlements maybe be over-ridden on the server side depending on which data gets uploaded to the server first. In other words, data downloaded in a particular order is uploaded in that particular order.

For example, if you revoke an entitlement and certify the account as Certify Conditionally, the entitlement could also be certified as Certify Conditionally if the account is updated last in the server, after the entitlement has been updated.

As a work around, you can download the Excel file again to verify the final value updated on the server.

---



---

If you try to download the spreadsheet for a certification that has already been completed, then a different version of the spreadsheet is downloaded, in which all the columns are marked as read-only and the **Save to Server** button is not available.

## 15.6 Generating Certification Reports

Oracle BI Publisher reports are used for identity certification. These reports select data from the certification tables of the Oracle Identity Manager database.

There are specific templates to control the format and content of reports. For example, many of the certification reports have a template that includes details from action history for each line-item and detail, and another template that does not.

There are a list of predefined or default certification reports in Oracle Identity Manager. [Table 15-4](#) lists the default certification reports for each type of certification.

**Table 15-4** Default Certification Reports

Certification Type	Certification Report	Description
User certification	Complete Certification Report	Presents comprehensive data of a user certification. This report includes a list of all employees and their access.
	Certified Access Report	Lists access marked as certified.
	Revoked Access Report	Lists access marked as revoked.
	Abstained Access Report	Lists certification items that the certifier declined to complete because the certifier is not responsible for verifying the user's assigned roles and entitlements.

**Table 15–4 (Cont.) Default Certification Reports**

<b>Certification Type</b>	<b>Certification Report</b>	<b>Description</b>
	Certified Conditionally Access Report	Lists access that the certifier approved temporarily, even though the access may not be appropriate or justified in the long term. Reviewers are required to enter an end date, which are included in this report. However, the access is not revoked and notices are not sent out about expired end dates.
	Complete Certification Task Report	Presents user-certification data based on certification tasks. This is a subset of the Complete Certification Report.
Role certification	Complete Certification Report	Presents comprehensive data of a role certification.
	Certified Access Report	Lists entitlements marked as certified.
	Revoked Access Report	Lists entitlements as revoked.
	Abstained Access Report	Lists certification items that the certifier declined to complete because the certifier is not responsible for verifying the role's assigned memberships.
	Certified Conditionally Access Report	Lists access that the certifier approved temporarily, even though the access may not be appropriate or justified in the long term. Reviewers are required to enter an end date, which are included in this report. However, the access is not revoked and notices are not sent out about expired end dates.
	Complete Certification Task Report	Presents role-certification data based on certification tasks. This is a subset of the Complete Certification Report.
Application instance certification	Complete Certification Report	Presents comprehensive data of an application instance certification.
	Certified Access Report	Lists entitlements marked as certified.
	Revoked Access Report	Lists entitlements marked as revoked.
	Abstained Access Report	Lists certification items that the certifier declined to complete because the certifier is not responsible for verifying the application instances's assigned users and accounts.
	Certified Conditionally Access Report	Lists access that the certifier approved temporarily, even though the access may not be appropriate or justified in the long term. Reviewers are required to enter an end date, which are included in this report. However, the access is not revoked and notices are not sent out about expired end dates.
	Complete Certification Task Report	Presents certification data for application instances based on certification tasks. This is a subset of the Complete Certification Report.
Entitlement certification	Complete Certification Report	Presents comprehensive data of an entitlement certification.
	Certified Access Report	Lists access marked as certified.
	Revoked Access Report	Lists access marked as revoked.

**Table 15–4 (Cont.) Default Certification Reports**

Certification Type	Certification Report	Description
	Abstained Access Report	Lists certification items that the certifier declined to complete because the certifier is not responsible for verifying the entitlement's assigned accounts and attributes.
	Certified Conditionally Access Report	Lists access that the certifier approved temporarily, even though the access may not be appropriate or justified in the long term. Reviewers are required to enter an end date, which is included in this report. However, the access is not revoked and notices are not sent out about expired end dates.
	Complete Certification Task Report	Presents entitlement-certification data based on certification tasks. This is a subset of the Complete Certification Report.

This section contains the following topics:

- [Generating Certification Reports From the Dashboard](#)
- [Generating Exported Certification Reports From the Certification Pages](#)

### 15.6.1 Generating Certification Reports From the Dashboard

To generate certification reports by using the Dashboard:

1. In Oracle Identity Self Service, navigate to the Dashboard. A list of certifications is displayed.
2. Select the certification for which you to generate the report. The Detailed Information section is displayed for the selected certification.
3. Click the **Reports** tab.
4. Select Report Type as Complete Certification, Certified, Revoked, Abstained, or Certified Conditionally.
5. From the Report Format Output list, select the format in which you want to generate the report, such as HTML or PDF.
6. Select the **Display Action History** option to include in the report the action history or trail of actions taken by all reviewers on the certification. Deselecting this option does not show the action history in the certification report.
7. Click **Generate Report**. The certification information is exported to the selected option, such as HTML or PDF.

**Tip:** On selecting Excel as the report format in step 5, an error message is displayed on opening the report. This is a security alert from Microsoft and can be ignored. However, if you want to avoid the message, then perform the following steps:

1. Go to Windows registry.
2. Search and navigate to the  
HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Excel\Security  
key.
3. Set the following value:  
(DWORD) "ExtensionHardening" = 0

## 15.6.2 Generating Exported Certification Reports From the Certification Pages

To generate certification reports by using the Inbox:

1. In Oracle Identity Self Service, navigate to the Inbox. A list of certification tasks is displayed.
2. Click an in-progress certification task name to open Page 1 of the certification task.
3. From the Actions menu, select Export to PDF or Excel.

The exported certification tasks in PDF or Excel is equivalent to Complete Certification Report.



---

---

# Glossary

## **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 using the Access Policies menu item in Oracle Identity Manager Web admin console.

## **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, pre-populate 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 runtime application data used by its adapter tasks. An adapter variable may be used multiple times within a single adapter.

## **Admin Roles**

Roles that are predefined in Oracle Identity Manager that have a one-to-one mapping to the Application Roles defined in Oracle Entitlement Server. Application Roles are Oracle Entitlements Server (OES) construct and cannot be viewed or assigned through Oracle Identity Manager. Hence, each Application Role in OES will have a corresponding Admin Role in Oracle Identity Manager

**Application Instance**

An entity that depicts the intersection between an IT resource instance and a resource object. Users are expected to have accounts and entitlements tied to application instance and not to the IT resource instance or resource object. Today, some Oracle Identity Manager features work at IT resource instance level and some work at resource object level. With the introduction of this entity, all accounts and entitlements will be consistently identified at Application Instance level.

**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 the 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 main task of the API may 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.

**Application Roles**

Predefined roles in Oracle Entitlements Server that govern the policies and permissions each of these roles can perform.

**approval policy**

Approval policy is a configurable entity of request management that helps associate various request types with approval processes defined in the request service only for request-level and operation-level approvals. It associates approval workflows to be initiated at request or operation levels for a request type. You can use approval policies to associate various request types with various approval processes, which are the SOA-based workflows. Approval policies control which approval process is to be invoked based on the request data evaluation.

**approval task**

Approval tasks are instantiated by request service and correspond to associated requests that are in the user or administrator's queue to be approved.

**attestation**

Attestation enables users designated as reviewers to be notified of reports they must review. These reports describe entitlements of other users. A reviewer can attest to the accuracy of these entitlements by providing a response.

**attestation process**

An attestation process is the mechanism by which an attestation task is set up. Input that an attestation process requires includes information about how to define the components that constitute the attestation task and how to associate the attestation task with a schedule at which the task must be run.

**attestation task**

The attestation action, along with the response the reviewer provides, any associated comments, and an audit view of the data that the reviewer views and attests to, is tracked and audited to provide a complete trail of accountability. In Oracle Identity Manager, this process is known as an attestation task.

**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.

**beneficiary**

A beneficiary is an entity that benefits from the action performed after the request is completed and the request is completed only if it is executed successfully.

**Bulk Load Utility**

The Bulk Load utility is aimed at automating the process of loading a large amount of data into Oracle Identity Manager. It helps reduce the downtime involved in loading data. You can use this utility after you install Oracle Identity Manager or at any time during the production lifetime of Oracle Identity Manager. Bulk Load utility can be used to load user, account, role, role hierarchy, role membership, and role category data into Oracle Identity Manager.

**business reviewer**

A user within an enterprise who reviews the access-privileges of other users from a business-oriented perspective. Typically, this is a Line-Of-Business (LOB) manager who is responsible for the access-privileges of users who report to the manager.

**callback service**

The callback service invokes deployment-specific logic at predetermined points during Oracle Identity Manager event processing. The callback service triggers notifications and callbacks that allow external applications to perform some action as a part of Oracle Identity Manager event processing.

**Catalog**

Catalog, also known as Request Catalog, offers a consistent and intuitive request experience for customers to request roles, entitlements and application instance following the commonly used Shopping Cart paradigm. The catalog is a structured commodity with its own set of metadata.

**Catalog Item**

A catalog item is an entity, such as roles, entitlements or application instances, that can be requested by a user, either for themselves or on behalf of other users.

**Catalog Item Navigation Category**

A catalog Item Navigation Category is a way to organize the request catalog. Each catalog item is associated with one and only one category. A catalog item navigation category is an attribute of the catalog item. Catalog Administrators can edit a Catalog Item and provide a value for the category.

**certification**

Identity certification is the process of reviewing user entitlements and access-privileges within an enterprise to ensure that users have not acquired entitlements that they are not authorized to have. It also involves either approving (certifying) or rejecting (revoking) each access-privilege.

**certification definition**

Certification definition is a named set of parameters that is used as input to a certification job to generate certification objects.

### **certification object**

Certification object is a generated certification that is assigned to a particular certifier or primary reviewer. Each certification object consists of:

- A unique certification ID
- A set of line-items, each of which contains a set of details

### **certification job**

Certification jobs are used to create certifications as requested or as scheduled. A certification job is a background execution-task that generates certification objects based on a specified certification definition.

### **certification task**

Certification task consists of a set of work to be done within a certification process. Each set of line-items that is assigned to a particular reviewer initiates a Service-Oriented Architecture (SOA) task that contains that particular set of line items and that is routed to SOA Inbox of that particular reviewer. The SOA component also notifies the reviewer that a certification task has been assigned to the reviewer.

### **closed-loop remediation**

Closed-loop remediation is a feature that utilizes the provisioning system of Oracle Identity Manager to automatically revoke accounts, roles, and entitlements based on the results of the Oracle Identity Manager certification process.

### **Connected Resource**

Target systems that are online and have ways to provision directly by using connectors.

### **connector**

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

### **Connector Server**

Connector Servers are implementation of the ICF Framework and allow remote execution of target connector from Oracle Identity Manager. Communication between Oracle Identity Manager and an ICF-based connector server happens over a socket layer.

### **context**

A context is the environment in which an Oracle Identity Manager operation is performed. For example, a user creation operation performed in Oracle Identity Self Service is carried out in the Web context.

### **Dashboard**

The Identity Certification Dashboard provides an overview of in-progress and completed certifications in the system. The certifications displayed in the dashboard depends on your role.

### **data field**

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

**database**

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

**delegated administrators**

This is an Oracle Identity Manager user who has been assigned administrative responsibilities. Administrative rights are assigned using membership within administrative groups. Administrators have access only to those organizations, forms, data, and users for which/whom they are responsible.

**delegated reviewer**

A person who is assigned to help with the certification work. The delegated reviewer is secondarily responsible for making certification-decisions on a particular set of line-items, but the primary reviewer remains ultimately responsible. Any decision made by the delegated reviewer eventually returns to the primary reviewer, who can override that decision.

**Deployment Manager**

The Deployment Manager is a tool for exporting and importing Oracle Identity Manager configurations and customizations. Usually, the Deployment Manager is used to migrate a configuration from one deployment to another, for example, from a test to a production deployment, or to create a backup of the deployment.

**deprovisioning**

The rescinding of a user's, user group's, and/or organization's access to a resource.

**Diagnostic Dashboard**

Diagnostic Dashboard is a stand-alone application that helps you validate some of the Oracle Identity Manager prerequisites and installation.

**disconnected resource**

Disconnected resources are targets for which there is no connector. Therefore, the provisioning fulfillment for disconnected resources is not automated, but manual.

**e-mail definition**

This is a predefined template that is used when generating e-mail notifications. E-mail definitions are created using the E-mail Definition form.

**Enterprise Roles**

Enterprise Roles are customer defined roles that can be requested via the catalog.

**Entities**

Managed entities like User, Organization, Role, Entitlements, Application Instance.

**Entitlement**

An entitlement granted to an account on a target system enables the account owner (user) to perform a specific task or function. An entitlement can be an application role, responsibility, or group membership. For example, if user Richard is granted the Inventory Analyst role on a target system, then Richard can use that entitlement to access and generate inventory-related reports from the target system.

**Entity Owners**

All Owners (Role, Entity, and Application Instance) are additional metadata on the entity, typically used in resolving approvals, certifications, etc. The Owners of an entity have no administrative rights on the entity itself.

**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 runtime. In addition, you can view the reasons for the errors, along with possible solutions. See [adapter task](#).

**error message**

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

**event**

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

**event handler**

An event handler is a piece of code that is registered with an orchestration on various stages. These event handlers are invoked when the relevant orchestration stage is performed.

See [event](#).

**event listener**

Event listener is a service that responds to changes in users. Event listeners are supported for user and application instance certifications.

**final review**

The optional, final phase of certification with TPAD. If Final Review is enabled in configuration, then this phase allows the final reviewer, who is the primary reviewer from Phase One, to view and override the decisions made during Phase Two.

**final reviewer**

The person who has the final say over the certification-decisions. The final reviewer can review and override the certification decisions of other reviewers. Final review is performed only after a two-phased review (and only when an administrator has configured the certification-definition to enable this). The primary reviewer from the first phase can then make a final review of the certification actions made by all the reviewers in the first two phases.

**form**

A graphical user interface layout (i.e., 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.

**Form Designer**

A form used to create customized Forms. Forms created using this form must be associated with a process or a resource object. These forms (and the fields they are

comprised of) are used to provide processes or resource objects with a mechanism for obtaining additional information they require to conduct provisioning.

### **GTC**

Generic Technology Connector (GTC) enables you to create a custom connector to link the target system and Oracle Identity Manager without using the customization features of the Adapter Factory.

### **GTC provider**

The components that constitute a generic technology connector are called providers.

### **heterogeneous request**

Heterogeneous request is a request created for entities of different types. Oracle Identity Manager supports requesting roles, application instances, and entitlements in a single request, which is heterogeneous in nature.

### **Identity connector**

Identity connectors are components developed to link Oracle Identity Manager with external stores of applications, directories, and databases. This release of Oracle Identity Manager provides support for developing and building identity connectors by using the Identity Connector Framework (ICF). Using the ICF decouples Oracle Identity Manager from the other applications to which it connects. Therefore, you can build and test an identity connector before integrating it with Oracle Identity Manager.

### **identity connector server**

An identity connector server is required when an identity connector bundle is not directly executed within your application. By using one or more identity connector servers, the ICF architecture permits your application to communicate with externally deployed identity connector bundles. Identity connector servers are available for Java™ and Microsoft .NET Framework applications.

### **Identity Store**

A Identity Repository which stores all identity data.

### **Inbox**

The Inbox lists all the approval and certification-review tasks assigned to the logged-in user in a single screen. It enables the logged-in user to filter task views into user preferences, such as assigned tasks, completed tasks, and tasks for which information has been requested. The user can select a task to open it in a new tab and then perform necessary actions on the task. This allows you to work on multiple tasks at a time by opening them in different tabs. To access the Inbox, login to Oracle Identity Self Service, and click Inbox on the left navigation pane.

### **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.

### **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](#).

**JavaBean**

JavaBeans allow developers to create reusable software components that can then be assembled together 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 bi-directionally with non-network-aware APIs. See [remote manager](#).

**line item**

A line item is a row of data that appears on Page One of a certification. Each line item collects or groups together according to the type of certification the set of privilege-assignments related to a particular identity or privilege. A reviewer can open any line-item to see its line item details. For example, within phase one of a user certification, each line item represents a user. Opening the user details displays the access-privileges of that user.

**LOB**

Line of Business (LOB) is a category of industry or business function. For example, an LOB manager is oriented to a business function within an enterprise, such as Sales.

**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 combo box and the commands that can be selected from that combo box.

Lookup definitions are created 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, etc.) 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 has 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 Java Client, any updates made by this feature are rendered on the Web Client 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 combo box that represents the lookup definition. See [lookup definition](#).

**Managed Organizations**

The list of Organizations that are explicitly assigned to delegated administrators. These are organization for which the users have been granted the associated Admin Role.

**Management Hierarchy**

Is applicable globally and every manager will be able to manage (User Administration) their reports.

**manual task**

This is any task within a process that requires user action in order to be completed. Approval processes are generally comprised of 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, etc.), records or data structures (length, fields, columns, etc.) or the physical location or permissions of data (where it is located, how it is associated, ownership, etc.). 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.

**non-primary account**

If a user already has a primary account and requests for another account in the same target application, then that account is a non-primary account. A user can have multiple non-primary accounts, but only one primary account.

**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 they need to be productive, and revokes and or prevents unauthorized access to protect proprietary information and enhance security.

**orchestration**

The process of any Oracle Identity Manager operation that goes through a predefined set of stages and executes some business logic in each stage is called an orchestration.

**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.

**Phase One**

The required, first phase of certification with TPAD. For a user certification, this is business review. For a privilege-centric certification, such as role certification, application instance certification, or entitlement certification, this is technical review. The system assigns a task to the Primary Reviewer for Phase One when the system generates a certification. If the Primary Reviewer spreads the work to any delegated reviewer, then the system generates another task for Phase One Verification.

**Phase One Verification**

A conditional stage (or sub-phase) within Phase One. Oracle Identity Manager creates and assigns this task to the primary reviewer if the primary reviewer has delegated any line-item to another person (delegated reviewer). This stage allows the primary reviewer for a line item to override any decision made by a delegated reviewer during Phase One.

**Phase Two**

The optional, second phase of certification with TPAD. For a user certification, this is technical review. For a privilege-centric certification, this is business review. Oracle Identity Manager assigns a task to each primary reviewer for Phase Two when the system generates a certification. If the primary reviewer spreads the work to any delegated reviewer, then the system generates another task for Phase Two verification.

**Phase Two Verification**

A conditional stage or subphase within Phase Two. The system creates and assigns this task to the primary reviewer if the primary reviewer has delegated any line-item to another person (delegated reviewer). This stage allows the primary reviewer for a line-item to override any decision made by a delegated reviewer during Phase Two.

**plug-in**

A plug-in is a logical component that extends the functionality of features provided by Oracle Identity Manager. The plug-in framework enables you to define, register, and configure plug-ins, which extend the functionality provided by features. Plug-ins can be predefined or custom-developed, and they are utilized at plug-in points.

**plug-in point**

A plug-in point is a specific point in the business logic where extensibility can be provided. An interface definition called the plug-in interface accompanies such a point. You can extend the plug-in interface based on the business requirements and register them as plug-ins.

**policy obligation**

If a user has multiple roles that have different authorization policies applicable in the same context, then the user's access rights are the cumulative rights across those policies. For example, the authorization check for the permission to search for users returns a list of obligations. This is a list of obligations from each applicable authorization policy. These obligations from multiple policies are combined to get a unified search result.

**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 using the User Defined Field Definition form and the Form Designer form, respectively.

See [Rule Generator Adapter](#).

**primary account**

A primary account is the first account created for a user in a target application. In other words, a primary account is the first application instance that is being requested. Oracle Identity Manager supports multiple accounts for a single application instance. The first account that is created is tagged as primary account, and there can be only one primary account for a user. The other accounts (non-primary accounts) are associated with the primary account. When the user requests entitlements, the entitlements are appended to the primary account.

**primary reviewer**

The person who is primarily responsible for making certification decisions on a particular set of line-items. The primary reviewer can reassign a line-item to another user, in which case that user becomes the new primary reviewer for that line-item, and the original primary reviewer never sees that line-item again. The primary reviewer can also delegate any of his line-items to another person, in which case that user becomes the delegated reviewer for that line-item, but the primary reviewer still retains responsibility for that line-item.

**process**

This is a collection of one or more process tasks, also, 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.

**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 allows Oracle Identity Manager to automate the execution of a process task. See [process task](#).

**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 may 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](#).

**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 pre-defined 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.

**provisioning task**

Provisioning tasks are tasks instantiated by requests, or pending manual provisioning tasks, or failed automatic provisioning tasks in the user or administrator's queue.

**Publish to Organizations**

A list of roles (in Oracle Identity Manager Enterprise Edition), and entitlements and application instance (in Oracle Identity Manager) that are made available to organizations by the respective entity administrators

**query**

A method of searching for particular data records within a database using a common characteristic. For example, a common query performed on the Organizations page

---

(Oracle Identity Self Service) is to retrieve all records related to a particular organizational unit. Oracle Identity Manager has many powerful built-in query syntax tools.

**reconciliation**

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

**record**

A collection of related items of information organized as a single unit of data (for example, a single record comprised 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).

**remediation tracking**

You can use the request catalog to track the remediation status of revoked accounts, access within accounts, or roles. This records whether and when each revocation request is fulfilled.

**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 needs to perform some function with this third-party application (for example, call a method that resides within the external API).

**request**

A request is an entity created by the users or administrators performing a specific action that requires a discretionary permission to be gained by someone or some process before the action can be performed. For example, a user can create a request to gain access to a laptop computer, and a manager can create an open requisition based on the request. A request has a requester, a beneficiary (optional), and a target entity.

**Request Cart**

A request cart contains a set of request items that a user has requested. The request cart does not persist across user sessions.

**Request Catalog**

A request catalog is a collection of items that can be searched, browsed and requested by a user either for themselves or on behalf of others.

**request dataset**

Request dataset is an XML definition file that dictates what data needs to be collected during various phases of the request lifecycle. In the request dataset, you can define what attributes need to be submitted by the requester and approver, whether or not an attribute is mandatory, and how UI should render the attribute to the user. Every attribute defined as a part of the dataset is associated with a set of properties that define the behavior of the attributes. Request dataset also allows you to define additional attributes, which exist only in the context of the request.

### **Request Profile**

A request profile is a cart that has been saved by an administrator. The administrator can, optionally, enter additional information about the items in the cart, before saving it. For example if an application instance is included in the profile then the request form (data set) for the application instance can be filled during profile creation by the administrator. The end user who is creating request based on the profile can change the information in the form if he wants to. All users have access to all request profiles. However, all users don't have access to all items in the request profile.

### **request stage**

Each request goes through a specific lifecycle after it is created in the system. This lifecycle is managed and controlled by the request service. The lifecycle transits the request through various stages. The stage a request is in determines what action the controller takes in that step, what operations are available on the request at that time, and what the possible stage transitions are. Each stage represents the logical next step in the request lifecycle. Only the successful execution of an operation can take the request from one stage to the next.

### **requester**

A requester is an entity that creates or raises a request. A requester can be a user or the system itself. The functional component decides on the requester for system-generated requests. An example of a system-generated request is a request created by the system based on access policy.

### **reset password**

This is the ability of a user to change his or her password.

When the user first registers with Oracle Identity Manager (using the Oracle Identity Manager Web Application), he/she needs to 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.

### **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 might 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 system-wide options that will determine how the resource is provisioned.

### **resource object**

See [resource](#).

### **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 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.
- **Pre-Populate:** This type of rule is used to determine the pre-populate 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 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.

### sandbox

A sandbox represents an area in the MDS repository where metadata objects can be modified without effecting their mainline usage. Typically, sandboxes are used to test changes to metadata objects before exposing them to the mainline use. Any changes made to a sandbox are visible only in the sandbox. By publishing the sandbox the changes are merged to the mainline.

### scheduled task

A scheduled task configure the metadata for a job, which is to be run, and the parameters required for execution of that task. This metadata is predefined for the predefined tasks. A new task can be added by the user, which will have the new metadata or the existing tasks can be updated to add/update the parameters for other configuration details.

### scheduler

Scheduler enables you to schedule jobs that automatically run predefined scheduled tasks at the specified time.

### self-registration

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

**shceduled job**

A job can be scheduled to run at the specified interval. You can create multiple jobs scheduled to run at different time intervals. A job run is a specific execution of a job. Each job run includes information such as the start time, stop time, exceptions and status of the execution.

**SoD**

Segregation of Duties (SoD) is aimed at applying checks and balances on business processes. The SoD validation process in Oracle Identity Manager occurs when a user creates a request for an entitlement on a particular target system. The request is funneled through a resource approval workflow and, if it passes that initial workflow, a resource provisioning workflow. If the user's request passes SoD validation (and an approver approves the request), the resource provisioning workflow is initiated. If the request fails SoD validation, the resource approval workflow can be configured to take remediation steps.

**SPML**

Oracle Identity Manager provides client applications with the Identity Management service to manage identities, which makes use of the Service Provisioning Markup Language (SPML).

**stored procedure**

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

**stored procedure task**

This is one of several adapter task types. This type of adapter task allows Oracle Identity Manager to map to and execute 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 utilize stored procedures on any Oracle or SQLServer database (assuming it is accessible on its network). This includes retrieving primitive values from stored procedures. See [adapter task](#). See [stored procedure](#).

**system property**

System properties define the characteristics that control the behavior of Oracle Identity Manager. You can define the functionality of consoles such as the Oracle Identity System Administration and Oracle Identity Self Service by using system properties.

**target entity**

Target entity is the resource or entity that is requested for the beneficiary.

**target resource**

The external resource or application to which you wish to provision a user or organization with access 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, or 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 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.

**technical reviewer**

A user within an enterprise who reviews the access-privileges of others from a technically-oriented perspective. Typically, this is an IT expert or an application-owner who is responsible for access-privileges being specified correctly, or for limiting access within the enterprise to a specific access-privilege.

**toolbar**

The set of buttons along the top edge of the Oracle Identity Manager Design Console window that provides access to frequently used functions. Clicking the left mouse button when the pointer is over a button will execute that button's function. Hovering with your mouse over a button will cause a tool tip about that button to be displayed.

**TPAD**

Collaborative certification or two-phased review with advanced delegation (TPAD) provides the following functionalities:

- Two-phased review, which allows to combine within a single certification the perspectives of business-oriented and technical reviewers.
- Advanced delegation, which allows a certifier to retain overall responsibility while delegating decisions to others. Advanced delegation of individual line-items within a certification allows a reviewer to spread the work among several people who can work simultaneously. This allows those who are responsible for reviewing access within an enterprise to spread the burden and thus complete the work more quickly.

**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 may be more than one trusted source and more than one key per trusted source.

**trusted source reconciliation**

See [authoritative identity reconciliation](#).

**UDF**

Entity attributes are properties of the entity. The information about the user entity is stored in the form of attributes, such as first name, last name, user login, and password. There are default user attributes in Oracle Identity Manager. However, you can create custom user attributes by using the Form Designer in the Oracle Identity System Administration. The custom attributes are referred to as user defined fields (UDFs). Oracle Identity Manager lets you create UDFs for the user, role, organization, and catalog entities.

**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 may use either the Java or the Web version 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 Web Application. End-users are generally only able to perform basic functions within Oracle Identity Manager.

---

---

# Index

## A

---

access  
  managing, 7-1  
  roles, 7-1  
    modify, 7-2  
    remove, 7-2  
    request for, 7-1  
access request catalog, 8-1, 9-15  
accessibility, 2-3  
accounts  
  disabling, 7-4, 11-40  
  enabling, 7-4, 11-40  
  locking, 11-41  
  managing, 7-3  
  modifying, 7-4, 11-37, 11-38  
  non-primary, 11-38  
  primary, 11-38, 11-39  
  provisioning, 13-25  
  removing, 7-4  
  removing from user, 11-39  
  requesting, 7-3, 11-38  
  revoking from organizations, 13-25  
  types, 11-38  
  unlocking, 11-42  
admin roles, 7-5, 13-5  
  granting, 13-23  
  managing, 13-23  
  revoking, 13-24  
admin roles, viewing, 7-5  
Administration, 2-8  
approval tasks, 10-4  
  adding attachments, 10-9  
  adding comments, 10-9  
  approving, 10-10  
  delegating, 10-11  
  reassigning, 10-10, 10-11  
  rejecting, 10-10  
  searching, 10-6  
  suspending, 10-11  
  task details, 10-9  
  viewing, 10-5  
  withdrawing, 10-11  
Attestation Dashboard  
  e-mail notifications, 14-3  
  scheduled tasks, 14-3

  viewing attention request details, 14-1  
attestation tasks, 10-35  
  request details, 10-36  
  searching, 10-35

## B

---

beneficiary, 9-1  
bulk request, 9-8

## C

---

catalog  
  refining search results, 8-2  
catalog items  
  adding to cart, 8-4  
  modifying, 8-1  
  removing from cart, 8-4  
  viewing, 8-1  
catalog-based requests, 9-11  
certification, 15-1  
  Dashboard, 15-4  
  generating reports, 15-10  
  Inbox, 15-4  
  name formats, 15-5  
  reports, 15-10  
  reviewers, 15-3  
  types, 15-1  
certification reports, 15-10  
Certifications, 2-8  
certifications  
  completing, 10-18  
  offline mode, 15-8  
  searching and viewing, 10-12, 15-6  
challenge questions and response, 6-3  
child organizations  
  deleting, 13-22  
  disabling, 13-22  
  enabling, 13-23  
  opening, 13-23  
child requests, 9-8  
common name, 11-51  
common name generation, 11-51  
  create user operation, 11-51  
  modify user operation, 11-52  
completing certifications, 10-18

- application instance certifications, 10-23
- entitlement certifications, 10-25
- offline mode, 15-8
- role certifications, 10-20
- user certifications, 10-18
- configure
  - username policy, 11-44
- create
  - child organizations, 13-22
  - custom user name policies, 11-48
  - organizations, 13-19
  - request, 9-15
  - request profile, 9-14
  - role categories, 12-20
  - roles, 12-11
  - saved searches, 5-6
  - users, 11-32
- customize, 2-4

## D

---

- Dashboard, 15-4
- default roles, 12-9
- default roles categories, 12-19
- delegated administration, 1-3
- delete
  - attributes from search criteria, 5-5
  - catalog items, 8-4
  - child organizations, 13-22
  - containers, 5-3
  - organizations, 13-27
  - proxies, 6-6
  - request profile, 9-15
  - role categories, 12-21
  - roles, 12-19
  - saved searches, 5-7
  - user membership rules, 12-17
  - users, 11-41
- direct operation, 9-10
- direct reports
  - modifying, 6-4, 11-40
  - viewing, 6-4
- disable
  - accounts, 7-4, 11-40
  - child organizations, 13-22
  - organizations, 13-26
  - provisioned accounts, 13-25
  - username reservation, 11-43
  - users, 11-40

## E

---

- enable
  - accounts, 7-4, 11-40
  - child organizations, 13-23
  - organizations, 13-26
  - provisioned accounts, 13-25
  - username reservation, 11-43
  - users, 11-41
- entitlements

- managing, 7-2
- remove, 7-3
- request for, 7-2
- entity definition
  - organizations, 13-3
  - roles, 12-4
  - users, 11-3
- evaluating password policies, 13-17

## F

---

- features of Oracle Identity Manager, 1-1
- forgot password, 4-2
- forgot user login, 4-2

## H

---

- help, 2-4
- heterogeneous requests, 9-10

## I

---

- identity certification, 15-1
  - types, 15-1
- Identity Self Service
  - logging in, 2-1
  - login, 4-1
  - overview of, 2-1
  - registering, 3-1
  - registration request, 3-1
  - tracking registration request, 3-2
- Inbox, 2-7, 15-4

## L

---

- layout of pages in UI, 2-3
- lock, accounts, 11-41
- log in to Oracle Identity Self Service, 2-1, 4-1

## M

---

- manage
  - access, 7-1
  - accounts, 7-3
  - admin roles, 13-23
  - approval tasks, 10-4
  - attestation tasks, 10-35
  - entitlements, 7-2
  - organizations, 13-1
  - provisioning tasks, 10-28
  - requests, 9-1
  - roles, 12-1, 12-11
  - tasks, 10-1
  - user profile, 6-1
  - users, 11-1, 11-29
- modify
  - accounts, 11-37, 11-38
  - catalog items, 8-1
  - organizations, 13-21
  - request profile, 9-14
  - role categories, 12-20

- user membership rules, 12-17
- users, 11-35
- modifying
  - direct reports, 11-40
- My Profile, 2-7

## N

---

- non-catalog-based requests, 9-12
- non-primary accounts, 11-38

## O

---

- OIM Account, 11-2
- Oracle Identity Manager, 1-1
  - registering, 3-1
- organization and role management, 1-4
- organizations, 11-3, 13-1
  - attributes, 13-22
  - child organizations, 13-22
  - creating, 13-19
  - creating child organizations, 13-22
  - delegated administration, 13-1
  - deleting, 13-27
  - deleting child organizations, 13-22
  - disabling child organizations, 13-22
  - enabling and disabling, 13-26
  - enabling child organizations, 13-23
  - entity definition, 13-3
  - managing, 13-1
  - members, 13-23
  - opening child organizations, 13-23
  - publishing entities, 13-4
  - scoping and hierarchy, 13-4
  - searching, 13-18
  - viewing and modifying, 13-21

## P

---

- parent request, 9-8
- password management, 1-3
  - advanced, 1-3
  - self-service, 1-3
  - synchronization, 1-4
- password policies, 13-17
- password policies evaluation, 13-17
- personalizing, 2-7, 5-1
  - creating saved searches, 5-6
  - deleting saved searches, 5-7
  - Home page
    - adding containers, 5-1
    - changing the Home page layout, 5-4
    - editing containers, 5-3
    - moving containers, 5-4
    - removing containers, 5-3
  - saved searches, 5-7
  - search criteria, 5-5
  - search result, 5-5
- primary accounts, 11-38, 11-39
- provisioned accounts, 13-24
- provisioning, 1-4

- provisioning tasks, 10-28
  - adding notes, 10-30
  - assignment history, 10-32
  - form details, 10-33
  - manually fulfilling, 10-34
  - modifying form details, 10-33
  - reassigning, 10-31
  - retrying, 10-34
  - searching, 10-28
  - setting response, 10-30
  - task details, 10-29
- publishing, 12-18
- publishing roles, 12-18

## Q

---

- query by example, refine search results, 5-8

## R

---

- registration requests, 3-1
  - submitting, 3-1
  - tracking, 3-2
- remove
  - accounts, 7-4
  - accounts from user, 11-39
  - catalog items, 8-4
  - entitlements, 7-3
  - entitlements from user, 11-37
  - parent role, 12-14
  - roles assigned, 7-2
  - roles from user, 11-36
- request
  - catalog-based
    - application instance request, 9-11
    - entitlement request, 9-11
    - role request, 9-11
  - creating, 9-15
- request catalog, 8-1, 9-15
- request category, 9-11
- request failure, 9-13
- request profiles, 9-13, 9-19
  - creating, 9-14
  - deleting, 9-15
  - modifying, 9-14
- request stages, 9-3
- requester, 9-1
- Requests, 2-7
- requests, 9-1, 9-10
  - applications instances, 9-11
  - beneficiary, 9-1
  - bulk request, 9-8
  - catalog-based, 9-11
  - categories, 9-11
  - child request, 9-8
  - closing, 9-22
  - entitlements, 9-11
  - failure, 9-13
  - heterogeneous, 9-10
  - managing, 9-1

- non-catalog-based, 9-12
- parent request, 9-8
- process flow, 9-1
- requester, 9-1
- role, 9-11
- stages, 9-3
- target entity, 9-1
- tracking, 9-20
- withdrawing, 9-21
- role categories, 12-19
  - creating, 12-20
  - deleting, 12-21
  - modifying, 12-20
  - searching, 12-20
- role categories, default, 12-19
- roles, 11-3, 12-1
  - adding membership rules, 12-16
  - assigning members, 12-15
  - attributes, 12-13
  - creating, 12-11
  - default, 12-9
  - deleting, 12-19
  - deleting membership rules, 12-16, 12-17
  - entity definition, 12-4
  - hierarchy, 12-13
  - inherited by, 12-4, 12-13
  - inherited from, 12-4, 12-13
  - managing, 12-1, 12-11
  - members, 12-15
  - membership inheritance, 12-1
  - modifying membership rules, 12-16, 12-17
  - opening child roles, 12-14
  - opening parent roles, 12-14
  - permission inheritance, 12-3
  - publishing to organizations, 12-18
  - removing parent role, 12-14
  - revoke members, 12-16
  - revoke organizations, 12-18
  - searching, 12-11
  - viewing and administering, 12-13

## S

---

- sandbox, 2-4
- search
  - approval tasks, 10-6
  - attestation tasks, 10-35
  - operations on results, 11-31
  - organizations, 13-18
  - provisioning tasks, 10-28
  - role categories, 12-20
  - roles, 12-11
  - users, 11-30
- search operators, 8-3
- searching and viewing certifications, 10-12, 15-6
- self-service features, 1-2
  - profile management, 1-3
  - request management, 1-3
- simple search
  - operations on results, 11-31

- sort data, 5-7
- supported, 8-3

## T

---

- target entity, 9-1
- task
  - managing, 10-1
- TaskList, 10-1
- tasks, 10-1
  - approval tasks, 10-1, 10-4
  - attestation tasks, 10-1, 10-35
  - certification review tasks, 10-1
  - provisioning tasks, 10-1, 10-28

## U

---

- unlock, accounts, 11-42
- user attributes, 11-3
- user lifecycle, 11-1
- user profile
  - challenge questions and response, 6-3
  - direct reports, 6-4
  - managing, 6-1
  - password, 6-2
  - profile attributes, 6-1
  - proxies, 6-4
    - adding, 6-5
    - editing, 6-5
    - removing, 6-6
- username, 11-42
  - policy configuration, 11-44
  - releasing, 11-50
- username policies, create, 11-48
- username reservation, 11-42
  - enabling and disabling, 11-43
- users, 11-1
  - adding entitlements, 11-37
  - adding roles, 11-36
  - attributes, 11-3
  - creating, 11-32
  - deleting, 11-41
  - disabling, 11-40
  - editing user attributes, 11-35
  - enabling, 11-41
  - entity definition, 11-3
  - lifecycle, 11-1
  - managing, 11-1, 11-29
  - modifying, 11-35
  - OIM Account, 11-2
  - removing entitlements, 11-37
  - removing roles, 11-36
  - requesting entitlements, 11-37
  - searching, 11-30
  - viewing details, 11-34

## V

---

- view
  - admin roles, 7-5
  - approval task details, 10-9

- approval tasks, 10-5
- attestation task request details, 10-36
- catalog items, 8-1
- direct reports, 6-4
- form details, 10-33
- organizations, 13-21
- provisioned account details, 13-25
- provisioned accounts, 13-24
- provisioning task assignment history, 10-32
- provisioning task details, 10-29
- user details, 11-34

## **W**

---

- workflow and policy
  - deprovisioning, 1-4
  - provisioning, 1-4
- writing custom user name policies, 11-48

