

Oracle® Fusion Middleware
Administrator's Guide for Oracle Identity Manager
11g Release 2 (11.1.2.1.0)
E27149-22

June 2015

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

E27149-22

Copyright © 1991, 2015, Oracle and/or its affiliates. All rights reserved.

Primary Author: Debapriya Datta

Contributing Author: Prakash Hulikere

Contributors: Javed Beg, 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, then 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	xxvii
Audience.....	xxvii
Documentation Accessibility	xxvii
Related Documents	xxvii
Conventions	xxviii

Part I Overview

1 Oracle Identity System Administration Interface

1.1	Logging in to Oracle Identity Manager System Administration Console.....	1-1
1.2	Overview of the Oracle Identity Manager System Administration Console	1-1
1.2.1	Links	1-2
1.2.1.1	Accessibility.....	1-2
1.2.1.2	Sandboxes	1-3
1.2.1.3	Help	1-3
1.2.1.3.1	Top Pane	1-3
1.2.1.3.2	Lower Left Pane.....	1-5
1.2.1.3.3	Lower Right Pane	1-5
1.2.1.4	Sign Out	1-5
1.2.2	Left and Right Panes	1-5
1.2.2.1	Event Management	1-6
1.2.2.2	Certifications	1-6
1.2.2.3	Policies.....	1-6
1.2.2.4	Configuration.....	1-7
1.2.2.5	System Management.....	1-7
1.2.2.6	Upgrade	1-8

Part II Policy Administration

2 Managing Approval Policies

2.1	Approval Selection Methodologies	2-2
2.1.1	Request-Level Methodology	2-2
2.1.2	Operation-Level Methodology: Organization-Based Selection	2-3
2.1.3	Operation-Level Methodology: Role-Based Selection.....	2-3

2.1.4	Operation-Level Methodology: Application Instance-Based Selection.....	2-4
2.2	Creating Approval Policies.....	2-4
2.3	Searching Approval Policies	2-7
2.4	Modifying Approval Policies.....	2-8
2.5	Modifying the Priority of an Approval Policy.....	2-9
2.6	Deleting Approval Policies.....	2-9
2.7	General Guidelines	2-10

3 Managing Access Policies

3.1	Terminologies Used in Access Policies.....	3-1
3.2	Features of Access Policies	3-2
3.2.1	Provisioning Options	3-3
3.2.2	Revoking or Disabling the Policy.....	3-3
3.2.3	Denying a Resource.....	3-4
3.2.4	Evaluating Policies	3-4
3.2.5	Access Policy Priority.....	3-5
3.2.6	Access Policy Data.....	3-6
3.2.7	Provisioning Multiple Instances of the Same Resource via Access Policy by Using Account Discriminator	3-6
3.3	Creating Access Policies.....	3-7
3.4	Managing Access Policies.....	3-10
3.5	Provisioning Multiple Instances of the Same Resource via Access Policy.....	3-10
3.5.1	Creating Separate Accounts for the Same User and Same Resource on a Single Target System	3-11
3.5.2	Enabling Multiple Account Provisioning.....	3-12
3.5.3	Provisioning Multiple Instances of a Resource to Multiple Target Systems	3-12
3.5.4	Limitation of Provisioning Multiple Instances of a Resource via Access Policy.....	3-14

4 Managing Password Policies

4.1	Searching Password Policies	4-1
4.2	Creating a Password Policy.....	4-2
4.3	Setting Password Policy Rules.....	4-3
4.4	Deleting a Password Policy.....	4-9

5 Managing Attestation Processes

5.1	About Attestation.....	5-1
5.1.1	Definition of an Attestation Process.....	5-2
5.1.1.1	Attestation Process Control.....	5-2
5.1.1.1.1	Disabling Processes.....	5-2
5.1.1.1.2	Deleting Processes.....	5-2
5.1.2	Components of Attestation Tasks	5-3
5.1.2.1	Attestation Inbox	5-4
5.1.3	Attestation Request	5-4
5.1.4	Delegation.....	5-4
5.1.5	Attestation Lifecycle Process.....	5-5
5.1.5.1	Stage 1: Creation of an Attestation Task	5-5

5.1.5.2	Stage 2: Acting on an Attestation Task.....	5-7
5.1.5.3	Stage 3: Processing a Submitted Attestation Task.....	5-7
5.1.6	Attestation Engine	5-9
5.1.7	Attestation Scheduled Task.....	5-10
5.1.8	Attestation-Driven Workflow Capability	5-10
5.1.9	Attestation E-Mail.....	5-10
5.1.9.1	Notify Attestation Reviewer	5-10
5.1.9.1.1	Variables	5-10
5.1.9.1.2	Subject Line	5-11
5.1.9.1.3	Body.....	5-11
5.1.9.2	Notify Delegated Reviewers	5-11
5.1.9.2.1	Variables	5-11
5.1.9.2.2	Subject Line	5-11
5.1.9.2.3	Body.....	5-11
5.1.9.3	Notify Process Owner About Declined Attestation Entitlements.....	5-12
5.1.9.3.1	Variables	5-12
5.1.9.3.2	Subject Line	5-12
5.1.9.3.3	Body.....	5-12
5.1.9.3.4	Special Comments	5-12
5.1.9.4	Notify Process Owner About Reviewers with No E-Mail Defined.....	5-12
5.1.9.4.1	Variables	5-12
5.1.9.4.2	Subject Line	5-13
5.1.9.4.3	Body.....	5-13
5.1.9.4.4	Special Comments	5-13
5.2	Attestation Process Configuration.....	5-13
5.2.1	Menu Structure	5-13
5.2.2	System Control.....	5-14
5.3	Creating Attestation Processes.....	5-14
5.4	Managing Attestation Processes.....	5-16
5.4.1	Editing Attestation Processes.....	5-17
5.4.2	Disabling Attestation Processes.....	5-17
5.4.3	Enabling Attestation Processes.....	5-18
5.4.4	Deleting Attestation Processes.....	5-18
5.4.5	Running Attestation Processes	5-18
5.4.6	Managing Attestation Process Administrators	5-18
5.4.7	Viewing Attestation Process Execution History	5-18
5.5	Using the Attestation Dashboard	5-19
5.5.1	Viewing Attestation Request Details	5-20
5.5.2	E-Mail Notification	5-21
5.5.3	Attestation Grace Period Checker Scheduled Task	5-21

Part III Identity Certification

6 Managing Identity Certification

6.1	Certification Concepts.....	6-1
6.1.1	Line of Business and Line Item.....	6-1

6.1.2	Certification Task.....	6-1
6.1.3	Certification Object.....	6-2
6.1.4	Certification Definition	6-2
6.1.5	Certification Jobs.....	6-2
6.1.6	Closed-Loop Remediation.....	6-2
6.1.7	Remediation Tracking.....	6-2
6.1.8	Event Listener.....	6-3
6.1.9	Certification Authorization	6-3
6.2	Configuring Certifications.....	6-3
6.2.1	Prerequisites for Configuring Certifications.....	6-3
6.2.1.1	Marking a Catalog Item as Certifiable.....	6-4
6.2.1.2	Setting the Certifier in the Request Catalog	6-4
6.2.1.3	Setting User Manager and Organization Certifier.....	6-5
6.2.1.4	Setting Risk Levels for Individual Entities	6-5
6.2.1.5	Tagging Attributes	6-6
6.2.1.6	Configuring the Availability of Identity Certification	6-6
6.2.1.7	Configuring Reminders, Notifications, Escalations, and Expiry for Certifications (Optional) 6-7	
6.2.2	Configuring Certification Options in Identity System Administration.....	6-8
6.3	Managing Certification Definitions.....	6-9
6.3.1	Creating Certification Definitions	6-9
6.3.1.1	Creating a User Certification Definition	6-10
6.3.1.2	Creating a Role Certification Definition.....	6-12
6.3.1.3	Creating an Application Instance Certification Definition.....	6-14
6.3.1.4	Creating an Entitlement Certification Definition.....	6-16
6.3.2	Modifying Certification Definitions.....	6-18
6.3.3	Deleting Certification Definitions	6-18
6.4	Scheduling Certifications.....	6-19
6.5	Understanding How Risk Summaries are Calculated.....	6-19
6.5.1	Understanding Item Risk and Risk-Factor Mappings.....	6-20
6.5.1.1	Setting Item Risk.....	6-20
6.5.1.2	Understanding Risk-Level Mappings (Risk Factors)	6-21
6.5.2	Understanding Risk Aggregation and Risk Summaries	6-21
6.5.3	Understanding How Changing Risk Configuration Values Impacts the System...	6-22
6.6	Understanding Closed-Loop Remediation and Remediation Tracking	6-24
6.6.1	Configuring Challenge Workflows.....	6-24
6.7	Understanding Event Listeners	6-25
6.8	Configuring Event Listeners and Certification Event Trigger Jobs.....	6-26
6.8.1	Creating an Event Listener	6-27
6.8.2	Modifying an Event Listener	6-28
6.8.3	Deleting an Event Listener	6-28
6.8.4	Configuring Certification Event Trigger Jobs.....	6-28
6.8.4.1	Setting the Event Listener Name List	6-29
6.8.4.2	Adding More Trigger Jobs	6-29
6.9	Configuring Certification Reports.....	6-29
6.10	Understanding Multi-Phased Review in User Certification.....	6-31
6.10.1	Multiple Phases of Review	6-31
6.10.2	Delegation to Multiple Reviewers Within Each Phase.....	6-32

6.10.3	Stages of Certification in TPAD.....	6-32
6.10.3.1	Phase One With Verification.....	6-33
6.10.3.2	Phase Two With Verification.....	6-37
6.10.3.3	Final Review.....	6-39
6.11	Troubleshooting Identity Certification.....	6-41

Part IV Form Management

7 Managing Forms

7.1	Creating Forms By Using the Form Designer.....	7-1
7.2	Searching Forms By Using the Form Designer.....	7-2
7.3	Modifying Forms By Using the Form Designer.....	7-3
7.3.1	Removing or Hiding Form Attributes.....	7-4

8 Configuring Custom Attributes

8.1	Creating a Custom Attribute.....	8-1
8.2	Creating a Custom Child Form.....	8-5
8.3	Creating a Custom Child Form Attribute.....	8-6
8.4	Modifying a Custom Attribute.....	8-8
8.5	Adding a Custom Attribute.....	8-9
8.5.1	Enabling the Submit Button After Adding a UDF to the Modify User Form.....	8-20
8.6	Adding a Custom Attribute to an Application Instance Form.....	8-21
8.6.1	Regenerating View.....	8-22
8.6.2	Updating the Application Instance Form By Using WebCenter Composer.....	8-22
8.7	Moving UDFs from Test to Production.....	8-23
8.7.1	Moving UDFs Added to Catalog Entities.....	8-23
8.7.2	Moving UDFs Added to User Forms.....	8-24
8.7.2.1	Exporting the UDF from the Test Environment.....	8-24
8.7.2.2	Importing the UDF into the Production Environment.....	8-24
8.8	Synchronizing User-Defined Fields Between Oracle Identity Manager and LDAP.....	8-25
8.9	Attribute Definitions.....	8-25
8.10	Creating Cascaded LOVs.....	8-149

Part V Application Management

9 Managing Application Instances

9.1	Application Instance Architecture and Concepts.....	9-2
9.1.1	Multiple Accounts Per Application Instance.....	9-2
9.1.2	Entitlements.....	9-3
9.1.3	Disconnected Application Instances.....	9-4
9.1.4	Application Instance Security.....	9-4
9.2	Managing Application Instances.....	9-4
9.2.1	Creating Application Instances.....	9-4
9.2.2	Searching Application Instances.....	9-5
9.2.3	Modifying Application Instances.....	9-7

9.2.3.1	Modifying Application Instance Attributes.....	9-7
9.2.3.2	Managing Organizations Associated With Application Instances	9-8
9.2.3.2.1	Publishing an Application Instance to Organizations	9-8
9.2.3.2.2	Revoking Organizations From an Application Instance	9-9
9.2.3.3	Managing Entitlements Associated With Application Instances	9-10
9.2.4	Deleting Application Instances.....	9-10
9.2.5	Creating and Modifying Forms	9-12
9.2.5.1	Creating Forms Associated With Application Instances.....	9-12
9.2.5.2	Modifying Forms Associated With Application Instances.....	9-13
9.2.5.3	Localizing Application Instance Form	9-14
9.3	Configuring Application Instances	9-15
9.3.1	Configuring Provisioning for Connected Application Instances	9-16
9.3.2	Configuring a Resource Object	9-16
9.3.3	Configuring IT Resource.....	9-16
9.3.4	Configuring Password Policies for Application Instances	9-17
9.4	Developing Entitlements	9-18
9.4.1	Available Entitlements and Assigned Entitlements	9-19
9.4.2	Entitlement Data Capture Process	9-20
9.4.2.1	Capture of Data About Available Entitlements	9-20
9.4.2.2	Capture of Data About Assigned Entitlements	9-20
9.4.3	Marking Entitlement Attributes on Child Process Forms	9-21
9.4.4	Duplicate Validation for Entitlements or Child Data.....	9-24
9.4.5	Configuring Scheduled Tasks for Working with Entitlement Data.....	9-25
9.4.5.1	Entitlement List.....	9-26
9.4.5.2	Entitlement Assignments	9-26
9.4.6	Deleting Entitlement	9-26
9.4.7	Refreshing the Entitlement List Post Delete for New Entries	9-28
9.4.8	Disabling the Capture of Modifications to Assigned Entitlements.....	9-28
9.4.9	Entitlement-Related Reports	9-29
9.4.9.1	Entitlement Access List.....	9-30
9.4.9.2	Entitlement Access List History	9-30
9.4.9.3	User Resource Entitlement.....	9-30
9.4.9.4	User Resource Entitlement History	9-30

10 Managing Disconnected Resources

10.1	Disconnected Resources Architecture.....	10-1
10.2	Managing Disconnected Application Instance.....	10-2
10.2.1	Creating a Disconnected Application Instance	10-3
10.2.2	Creating a Disconnected Application Instance for an Existing Disconnected Resource ..	10-5
10.3	Provisioning Operations on a Disconnected Application Instance	10-5
10.3.1	Process Form Updates.....	10-6
10.4	Managing Entitlement for Disconnected Resource.....	10-6
10.4.1	Configuring Entitlement Grant.....	10-6
10.4.1.1	Creating a Child Form and Configuring Entitlement Lookup via Form Designer	10-7
10.4.1.2	Configuring the Process Task that Invokes the SOA Composite	10-9

10.4.2	Configuring for Entitlement Revoke.....	10-12
10.5	Status Changes in Manual Process Task Action.....	10-13
10.6	Customizing Provisioning SOA Composite	10-13
10.6.1	Customizing Human Task Assignment via SOA Composer	10-13
10.6.2	Customizing by Modifying the Out of the Box Composite.....	10-14
10.7	Troubleshooting Disconnected Resources	10-15

11 Managing Lookups

11.1	Searching a Lookup Type	11-1
11.2	Creating a Lookup Type	11-2
11.3	Modifying a Lookup Type.....	11-3

12 Managing Connector Lifecycle

12.1	Lifecycle of a Connector	12-2
12.2	Connector Lifecycle and Change Management Terminology.....	12-4
12.3	Viewing Connector Details.....	12-5
12.4	Installing Connectors.....	12-6
12.4.1	Overview of the Connector Deployment Process.....	12-6
12.4.2	Creating the User Account for Installing Connectors	12-7
12.4.3	Installing a Connector	12-8
12.4.4	Post Installation Steps	12-11
12.5	Defining Connectors.....	12-13
12.6	Cloning Connectors	12-22
12.6.1	Guidelines for Cloning a Connector	12-23
12.6.2	Cloning a Connector.....	12-23
12.6.3	Postcloning Steps	12-35
12.7	Exporting Connector Object Definitions in Connector XML Format.....	12-35
12.8	Upgrading Connectors.....	12-36
12.8.1	Upgrade Use Cases Supported by the Connector Upgrade Feature.....	12-37
12.8.2	Connector Object Changes Supported by the Upgrade Connectors Feature	12-39
12.8.2.1	Resource Object Changes	12-39
12.8.2.2	Process Definition Changes	12-40
12.8.2.3	Resource Object Changes	12-41
12.8.2.4	Process Form Changes.....	12-41
12.8.2.5	Lookup Definition Changes.....	12-41
12.8.2.6	Adapter Changes.....	12-42
12.8.2.7	Rule Changes.....	12-42
12.8.2.8	IT Resource Type Changes.....	12-42
12.8.2.9	IT Resource Changes.....	12-42
12.8.2.10	Scheduled Task Changes.....	12-43
12.8.3	What Happens When You Upgrade a Connector.....	12-43
12.8.4	Summary of the Upgrade Procedure.....	12-43
12.8.5	Procedure to Upgrade a Connector	12-45
12.8.5.1	Preupgrade Procedure	12-45
12.8.5.2	Upgrade Procedure	12-45
12.8.5.3	Postupgrade Procedure	12-60

12.8.6	Procedure to Upgrade a 9.x Connector Version to an ICF Based Connector.....	12-66
12.9	Uninstalling Connectors	12-67
12.9.1	Use Cases Supported by the Uninstall Connectors Utility	12-68
12.9.2	Overview of the Connector Uninstall Process.....	12-68
12.9.3	Setting Up the Uninstall Connector Utility.....	12-70
12.9.4	Uninstalling Connectors and Removing Connector Objects.....	12-70
12.9.4.1	Uninstalling a Connector.....	12-70
12.9.4.2	Removing Adapters, Lookup Definitions, Resource Objects, and Scheduled Tasks . 12-71	
12.9.4.3	Running the Script to Uninstall Connectors and Connector Objects.....	12-71
12.9.4.3.1	Preuninstall	12-71
12.9.4.3.2	Uninstall.....	12-72
12.9.4.3.3	Postuninstall.....	12-74
12.10	Troubleshooting Connector Management Issues.....	12-74

13 Managing Reconciliation

13.1	Types of Reconciliation	13-2
13.1.1	Reconciliation Based on the Object Being Reconciled.....	13-2
13.1.1.1	Trusted Source Reconciliation	13-3
13.1.1.2	Account Reconciliation	13-4
13.1.1.3	Reconciliation Process Flow	13-6
13.1.2	Mode of Reconciliation	13-8
13.1.3	Approach Used for Reconciliation	13-9
13.2	Managing Reconciliation Events	13-10
13.2.1	Searching Events.....	13-10
13.2.1.1	Performing a Simple Search for Events.....	13-10
13.2.1.2	Performing an Advanced Search for Events	13-11
13.2.2	Displaying Event Details	13-12
13.2.3	Determining Event Actions	13-14
13.2.4	Re-evaluating Events.....	13-14
13.2.5	Closing Events.....	13-15
13.2.6	Linking Reconciliation Events	13-15
13.2.6.1	Ad Hoc Linking	13-16
13.2.6.2	Manual Linking.....	13-16
13.2.6.3	Linking Orphan Accounts.....	13-16
13.2.6.3.1	For an Event With Multiple Matches	13-17
13.2.6.3.2	For an Event With No Matches	13-17

Part VI Managing Infrastructure Services

14 Managing Notification Service

14.1	Managing Notification Providers.....	14-2
14.1.1	Using UMS for Notification	14-2
14.1.1.1	Enabling Oracle Identity Manager to Use UMS for Notification	14-2
14.1.1.2	Applying OWSM Policy to the UMS Web Service	14-4
14.1.2	Using SMTP for Notification.....	14-6
14.1.3	Using SOA Composite for Notification.....	14-8

14.1.4	Configuring Custom Notification Provider.....	14-10
14.1.5	Disabling and Enabling Notification Providers	14-11
14.2	Managing Notification Templates.....	14-11
14.2.1	Creating a Notification Template.....	14-12
14.2.2	Searching for a Notification Template.....	14-14
14.2.3	Modifying a Notification Template	14-15
14.2.4	Deleting a Notification Template	14-15
14.2.5	Adding and Removing Locales from a Notification Template.....	14-16
14.2.6	Configuring Notification for a Proxy.....	14-17
14.3	Configuring Default Email Provider.....	14-17
14.4	Configuring SOA Email Notification.....	14-17
14.4.1	Configuring Actionable Email Notification on SOA	14-17
14.4.2	Troubleshooting SOA Email Notification	14-19
14.5	Disabling Email Notification.....	14-19
14.6	Testing Notification Configuration	14-21
14.6.1	Testing UMS Email Notification.....	14-21
14.6.2	Testing SMTP Connectivity.....	14-22

15 Managing the Scheduler

15.1	Configuring the oim-config.xml File.....	15-2
15.2	Starting and Stopping the Scheduler	15-3
15.2.1	Controlling Scheduler Start or Stop in a Clustered Environment.....	15-4
15.2.1.1	Adding the Server Side Property for Oracle Identity Manager.....	15-4
15.2.1.2	Restarting Oracle Identity Manager Managed Servers from the Node Manager.....	15-4
15.2.1.3	Modifying the Server Side Property for Oracle Identity Manager.....	15-5
15.3	Disabling and Enabling the Scheduler on a Node in Cluster Setup.....	15-5
15.3.1	Adding the Server-Level Property	15-5
15.3.2	Restarting the Managed Server from the Node Manger.....	15-6
15.4	Scheduled Tasks.....	15-6
15.4.1	Predefined Scheduled Tasks	15-7
15.4.2	LDAP Scheduled Tasks.....	15-15
15.4.2.1	Using Attribute-Level Filtering for Running LDAP Sync Incremental Reconciliation Jobs	15-20
15.4.3	Creating Custom Scheduled Tasks	15-20
15.5	Jobs.....	15-21
15.5.1	Creating Jobs	15-22
15.5.2	Searching Jobs	15-23
15.5.2.1	Performing a Simple Search for Jobs	15-23
15.5.2.2	Performing an Advanced Search for Jobs	15-24
15.5.3	Viewing Jobs.....	15-24
15.5.4	Modifying Jobs.....	15-26
15.5.5	Disabling and Enabling Jobs	15-26
15.5.6	Starting and Stopping Jobs	15-27
15.5.7	Deleting Jobs.....	15-27

16 Managing System Properties

16.1	System Properties in Oracle Identity Manager.....	16-1
16.2	Creating and Managing System Properties	16-22
16.2.1	Creating System Properties	16-23
16.2.2	Purging Cache	16-27
16.2.3	Searching for System Properties.....	16-27
16.2.3.1	Performing a Simple Search.....	16-27
16.2.3.2	Performing an Advanced Search.....	16-28
16.2.4	Modifying System Properties	16-29
16.2.5	Deleting System Properties	16-30

Part VII Requests

17 Managing the Access Request Catalog

17.1	Access Request Catalog.....	17-1
17.1.1	Access Request Challenges.....	17-1
17.1.2	Concepts.....	17-2
17.1.3	Catalog Use cases.....	17-3
17.2	About the Access Request Catalog.....	17-5
17.2.1	Features and Benefits	17-5
17.2.2	Architecture	17-6
17.3	Administering the Access Request Catalog.....	17-7
17.3.1	Pre-requisites	17-7
17.3.1.1	Setting up the Catalog System Administrator	17-7
17.3.1.2	Defining the Catalog Metadata	17-8
17.3.2	Common Tasks.....	17-10
17.3.2.1	Onboard Applications and Roles	17-10
17.3.2.1.1	Prepare an Onboarding checklist	17-10
17.3.2.1.2	Onboarding Roles.....	17-10
17.3.2.1.3	Onboarding Application Instances.....	17-11
17.3.2.1.4	Onboarding Entitlements.....	17-11
17.3.2.2	Bootstrapping the Catalog.....	17-12
17.3.2.2.1	Bootstrapping the Catalog with Roles.....	17-13
17.3.2.2.2	Bootstrapping the Catalog with Application Instances.....	17-13
17.3.2.2.3	Bootstrapping the Catalog with Entitlements.....	17-14
17.3.2.3	Ongoing Synchronization	17-14
17.3.2.4	Enrich the Catalog	17-14
17.3.2.4.1	Editing a Catalog Item Online	17-15
17.3.2.4.2	Enriching the Catalog in bulk from external sources.....	17-15
17.3.2.4.3	Loading data from an external source.....	17-15
17.3.2.5	Managing Catalog Items.....	17-16
17.3.2.5.1	Deleting a Catalog Items of Type Roles	17-16
17.3.2.5.2	Deleting Catalog Items of Type Application Instances	17-17
17.3.2.5.3	Deleting Catalog Items of type Entitlements	17-17
17.3.3	Database Best Practices for Access Request Catalog	17-17
17.3.3.1	One-Time Optimizations for Oracle Text Index	17-18

17.3.3.2	Text Index Optimization.....	17-19
17.4	Managing the Lifecycle of the Catalog	17-20
17.4.1	Overview of Catalog Customization	17-21
17.4.2	Test to Production procedures for Catalog customizations	17-22
17.4.2.1	Exporting using the Sandbox and Deployment Manager	17-23
17.4.2.2	Importing Using the Deployment Manager and Sandbox.....	17-24
17.4.3	Limitations of the Test to Production procedures	17-24
17.5	Troubleshooting	17-25
17.5.1	Catalog synchronization issues	17-25
17.5.2	Catalog security issues.....	17-28
17.5.3	Catalog Search Issues	17-30

Part VIII Auditing and Reporting

18 Configuring Auditing

18.1	Overview	18-1
18.1.1	Auditing Design Components	18-1
18.1.2	Profile Auditing	18-2
18.1.3	Standard and Customized Reports.....	18-2
18.2	User Profile Auditing	18-2
18.2.1	Data Collected for Audits.....	18-3
18.2.1.1	Capture of User Profile Audit Data	18-3
18.2.1.2	Storage of Snapshots	18-5
18.2.1.3	Trigger for Taking Snapshots	18-6
18.2.2	Post-Processor Used for User Profile Auditing.....	18-6
18.2.3	Tables Used for User Profile Auditing	18-6
18.2.4	Archival.....	18-7
18.3	Role Profile Auditing.....	18-7
18.3.1	Data Collected for Audits.....	18-7
18.3.1.1	Capture and Archiving of Role Profile Audit Data.....	18-8
18.3.1.2	Storage of Snapshots	18-8
18.3.1.3	Trigger for Taking Snapshots	18-8
18.4	Enabling and Disabling Auditing.....	18-9
18.4.1	Disabling Auditing.....	18-9
18.4.2	Enabling Auditing	18-9

19 Using Reporting Features

19.1	Reporting Features.....	19-1
19.2	Starting Oracle Identity Manager Reports	19-2
19.3	Running Oracle Identity Manager Reports.....	19-2
19.4	Supported Output Formats	19-3
19.5	Reports for Oracle Identity Manager	19-3
19.5.1	Access Policy Reports.....	19-3
19.5.1.1	Access Policy Details.....	19-4
19.5.1.2	Access Policy List by Role	19-4
19.5.2	Attestation, Request, and Approval Reports.....	19-5

19.5.2.1	Approval Activity.....	19-5
19.5.2.2	Attestation Process List.....	19-6
19.5.2.3	Attestation Request Details.....	19-7
19.5.2.4	Attestation Requests by Process.....	19-8
19.5.2.5	Attestation Requests by Reviewer.....	19-10
19.5.2.6	Request Details.....	19-11
19.5.2.7	Request Summary.....	19-12
19.5.2.8	Task Assignment History.....	19-13
19.5.3	Role and Organization Reports.....	19-14
19.5.3.1	Role Membership History.....	19-14
19.5.3.2	Role Membership Profile.....	19-15
19.5.3.3	Role Membership.....	19-16
19.5.3.4	Organization Details.....	19-17
19.5.3.5	User Membership History.....	19-18
19.5.4	Password Reports.....	19-19
19.5.4.1	Password Expiration Summary.....	19-19
19.5.4.2	Password Reset Summary.....	19-20
19.5.4.3	Resource Password Expiration.....	19-21
19.5.5	Resource and Entitlement Reports.....	19-22
19.5.5.1	Account Activity In Resource.....	19-23
19.5.5.2	Delegated Admins and Permissions by Resource.....	19-24
19.5.5.3	Delegated Admins by Resource.....	19-24
19.5.5.4	Entitlement Access List.....	19-26
19.5.5.5	Entitlement Access List History.....	19-27
19.5.5.6	Financially Significant Resource Details.....	19-28
19.5.5.7	Resource Access List History.....	19-29
19.5.5.8	Resource Access List.....	19-30
19.5.5.9	Resource Account Summary.....	19-31
19.5.5.10	Resource Activity Summary.....	19-31
19.5.5.11	User Resource Access History.....	19-32
19.5.5.12	User Resource Access.....	19-33
19.5.5.13	User Resource Entitlement.....	19-34
19.5.5.14	User Resource Entitlement History.....	19-36
19.5.6	User Reports.....	19-37
19.5.6.1	User Profile History.....	19-37
19.5.6.2	User Summary.....	19-39
19.5.6.3	Users Deleted.....	19-40
19.5.6.4	Users Disabled.....	19-40
19.5.6.5	Users Unlocked.....	19-41
19.5.7	Certification Reports.....	19-42
19.5.8	Exception Reports.....	19-42
19.5.8.1	Fine Grained Entitlement Exceptions By Resource.....	19-43
19.5.8.2	Orphaned Account Summary.....	19-45
19.5.8.3	Rogue Accounts By Resource.....	19-45
19.5.9	Best Practices for Running Oracle Identity Manager Reports.....	19-46
19.6	Creating Reports Using Third-Party Software.....	19-46
19.7	Required Scheduled Tasks for BI Publisher Reports.....	19-47

20 Using the Archival Utilities

20.1	Using the Reconciliation Archival Utility	20-1
20.1.1	Understanding the Reconciliation Archival Utility	20-1
20.1.2	Prerequisite for Running the Reconciliation Archival Utility	20-3
20.1.3	Archival Criteria	20-3
20.1.4	Running the Reconciliation Archival Utility	20-4
20.1.5	Log File Generated by the Reconciliation Archival Utility.....	20-6
20.2	Using the Task Archival Utility	20-6
20.2.1	Understanding the Task Archival Utility.....	20-6
20.2.2	Preparing Oracle Database for the Task Archival Utility	20-7
20.2.3	Running the Task Archival Utility	20-8
20.2.4	Reviewing the Output Files Generated by the Task Archival Utility	20-10
20.3	Using the Requests Archival Utility.....	20-10
20.3.1	Understanding the Requests Archival Utility	20-10
20.3.2	Prerequisites for Running the Requests Archival Utility	20-11
20.3.3	Input Parameters.....	20-12
20.3.4	Running the Requests Archival Utility.....	20-12
20.3.5	Log Files Generated by the Utility	20-14
20.4	Using the Audit Archival and Purge Utility	20-14
20.4.1	Overview	20-15
20.4.2	Prerequisites for Using the Utility	20-15
20.4.3	Preparing the UPA Table for Archival and Purge	20-16
20.4.4	Archiving or Purging the UPA Table	20-20
20.4.4.1	Partitions That Must Not Be Archived or Purged	20-20
20.4.4.2	Ongoing Partition Maintenance	20-20
20.4.4.3	Archiving or Purging Partitions in the UPA Table	20-21

Part IX Diagnostics and Troubleshooting

21 Configuring Logging

21.1	Logging in Oracle Identity Manager By Using ODL.....	21-1
21.1.1	Message Types and Levels	21-2
21.1.2	Log Handler and Logger Configuration	21-3
21.1.3	Configuring Log Handlers	21-4
21.1.3.1	Log Handler Configuration Tools.....	21-4
21.1.4	Configuring Loggers	21-5
21.1.5	Sample ODL Log Output.....	21-9
21.2	Logging in Oracle Identity Manager By Using log4j.....	21-9
21.2.1	Log Levels	21-10
21.2.2	Loggers	21-10
21.2.3	Configuring and Enabling Logging	21-10
21.3	Setting Warning State	21-10

22 Managing Asynchronous Execution

22.1	Overview of AsyncService.....	22-1
22.2	Async Routing and Configuration	22-1

22.2.1	Configuration Parameters	22-2
22.3	Troubleshooting Failed Async Tasks	22-2
22.3.1	Automated Retry Error Handling Mechanism	22-3
22.3.2	Manual Retry Error Handling Mechanism	22-3
22.4	Working with the Diagnostic Dashboard UI	22-3
22.4.1	Starting the Diagnostic Dashboard UI.....	22-3
22.4.2	Viewing Failed Async Tasks	22-4
22.4.2.1	To view failed async tasks.....	22-4
22.4.3	Retrying Failed Async Tasks.....	22-5
22.4.3.1	To retry failed Async task	22-5
22.4.4	Resubmitting Failed Async Tasks	22-5
22.4.5	Purging Failed Async Tasks.....	22-5
22.4.5.1	To purge failed Async tasks.....	22-5

23 Using Enterprise Manager for Managing Oracle Identity Manager Configuration

23.1	Using MBeans for Configuration Changes	23-1
23.2	Exporting and Importing Configuration Files.....	23-1

24 Setting the Language for Users

25 Working with the Diagnostic Dashboard

25.1	Overview of the Diagnostic Dashboard	25-1
25.2	Installing the Diagnostic Dashboard.....	25-1
25.2.1	Installing the Diagnostic Dashboard on Oracle WebLogic Server	25-1
25.3	Starting the Diagnostic Dashboard	25-2
25.4	Using the Diagnostic Dashboard	25-2
25.5	Running Tests By Using the Diagnostic Dashboard.....	25-3
25.5.1	Oracle Database Prerequisites Check	25-4
25.5.2	Database Connectivity Check	25-4
25.5.3	Account Lock Status	25-4
25.5.4	Data Encryption Key Verification	25-5
25.5.5	Scheduler Service Status	25-5
25.5.6	Remote Manager Status	25-5
25.5.7	JMS Messaging Verification	25-5
25.5.8	Target System SSL Trust Verification	25-5
25.5.9	Java VM System Properties Report.....	25-6
25.5.10	Oracle Identity Manager Libraries and Extensions Version Report	25-6
25.5.11	Oracle Identity Manager Libraries and Extensions Manifest Report.....	25-6
25.5.12	Test Basic Connectivity	25-6
25.5.13	Test Provisioning	25-7
25.5.14	Test Reconciliation.....	25-7
25.5.15	SOA-Oracle Identity Manager Configuration Check	25-7
25.5.16	Request Diagnostic Information.....	25-8
25.5.17	Orchestration Status	25-8
25.5.18	Retry Failed Orchestration	25-9

25.5.19	SPML Web Service.....	25-9
25.5.20	Test OWSM Setup.....	25-9
25.5.21	Test SPML to Oracle Identity Manager Request Invocation	25-9
25.5.22	SPML Attributes to Oracle Identity Manager Attributes.....	25-9
25.5.23	Username Test.....	25-10
25.5.24	Diagnose Creation of User and Role in Oracle Identity Manager and LDAP	25-10
25.5.25	Diagnose LDAP Reserve Container	25-10
25.5.26	Validate Recon Profile.....	25-11
25.5.27	Notification Configuration Test.....	25-11
25.5.28	Diagnose LDAP Connection	25-11
25.5.29	Diagnose OIM Callback Webservice.....	25-11

26 Enabling Diagnostics

26.1	Enabling Diagnostics in Oracle Identity Manager	26-1
26.2	Troubleshooting Dynamic Configuration-Related Problems.....	26-2
26.2.1	Roles in Oracle Identity Manager and Identity Store in Inconsistent State	26-3
26.2.2	Postenablement of the oamEnabled Flag Causes Issues	26-5
26.2.3	Run-time Evaluation of LDAP Containers Defined in LDAPContainerRules.xml	26-5

27 Handling Errors

Part X Additional Components

28 Installing and Configuring a Remote Manager

28.1	Overview of the Remote Manager Configuration	28-1
28.2	Configuring the Remote Manager.....	28-1
28.2.1	Adding the Trust Relation.....	28-2
28.2.2	Configuring the Remote Manager by Using Your Own Certificate.....	28-3
28.2.3	Testing the Remote Manager Connection.....	28-5
28.2.4	Updating the xlconfig.xml File to Change the Port for Remote Manager.....	28-5
28.3	Stopping and Starting the Remote Manager.....	28-6
28.4	Troubleshooting Remote Manager.....	28-6

29 Using the Form Version Control Utility

29.1	Use Cases Supported by the FVC Utility	29-1
29.2	Use Cases That Are Not Supported by the FVC Utility	29-2
29.3	Summary of the Form Version Control Process.....	29-2
29.4	Components of the FVC Utility	29-3
29.5	Using the FVC Utility	29-3
29.5.1	Preparing the Properties File	29-3
29.5.2	Addressing Prerequisites for Using the FVC Utility	29-7
29.5.3	Running the Utility	29-8
29.6	Troubleshooting	29-8

30 Starting and Stopping Servers

30.1	Configuring the Node Manager	30-1
30.2	Starting the Node Manager	30-2
30.3	Starting or Stopping WebLogic Administration Server	30-2
30.4	Starting or Stopping WebLogic Managed Servers	30-2
30.4.1	Starting or Stopping the Managed Servers By Using Command Prompt.....	30-3
30.4.2	Starting or Stopping the Managed Server By Using Oracle Enterprise Manager Fusion Middleware Control	30-3
30.4.3	Starting or Stopping Servers By Using Oracle WebLogic Server Administration Console	30-4

31 Enabling Secure Cookies

32 Integrating with Other Oracle Components

32.1	Oracle Access Manager	32-2
32.2	Oracle Adaptive Access Manager	32-2
32.3	Oracle Identity Analytics	32-2
32.3.1	Integration Configuration in Oracle Identity Analytics.....	32-3
32.3.2	Integration Configuration in Oracle Identity Manager.....	32-3
32.3.2.1	The DataCollectionOperationsIntf API Interface.....	32-3
32.3.2.2	Staging Tables	32-4
32.3.2.3	Data Collection Process	32-4
32.4	Oracle Identity Navigator.....	32-5
32.5	Oracle Virtual Directory.....	32-5
32.6	Oracle Service-Oriented Architecture.....	32-6
32.7	Oracle Business Intelligence Publisher	32-6

33 Handling Lifecycle Management Changes

33.1	URL Changes Related to Oracle Identity Manager.....	33-1
33.1.1	Oracle Identity Manager Host and Port Changes.....	33-1
33.1.1.1	Changing OimFrontEndURL in Oracle Identity Manager Configuration.....	33-2
33.1.1.2	Changing backOfficeURL in Oracle Identity Manager Configuration.....	33-2
33.1.2	Oracle Identity Manager Database Host and Port Changes.....	33-3
33.1.3	Oracle Virtual Directory Host and Port Changes	33-4
33.1.4	BI Publisher Host and Port Changes	33-5
33.1.5	SOA Host and Port Changes.....	33-5
33.1.6	OAM Host and Port Changes	33-6
33.2	Password Changes Related to Oracle Identity Manager	33-6
33.2.1	Changing Oracle WebLogic Administrator Password.....	33-7
33.2.2	Changing Oracle Identity Manager Administrator Password.....	33-7
33.2.3	Changing Oracle Identity Manager Administrator Database Password	33-8
33.2.3.1	Resetting System Administrator Database Password in Oracle Identity Manager Deployment	33-8
33.2.3.2	Resetting System Administrator Database Password When Oracle Identity Manager Deployment is Integrated With Access Manager	33-9
33.2.4	Changing Oracle Identity Manager Database Password.....	33-11

33.2.5	Changing Oracle Identity Manager Passwords in the Credential Store Framework	33-12
33.2.6	Changing OVD Password	33-13
33.2.7	Changing Oracle Identity Manager Administrator Password in LDAP	33-13
33.2.8	Unlocking Oracle Identity Manager Administrator Password in LDAP	33-14
33.3	Configuring SSL for Oracle Identity Manager.....	33-14
33.3.1	Generating Keys.....	33-15
33.3.2	Signing the Certificates	33-15
33.3.3	Exporting the Certificate.....	33-15
33.3.4	Importing the Certificate	33-16
33.3.5	Enabling SSL for Oracle Identity Manager and SOA Servers	33-16
33.3.5.1	Enabling SSL for Oracle Identity Manager	33-16
33.3.5.1.1	Enabling SSL for Oracle Identity Manager By Using Default Setting	33-16
33.3.5.1.2	Enabling SSL for Oracle Identity Manager By Using Custom Keystore..	33-17
33.3.5.2	Changing OimFrontEndURL to Use SSL Port	33-18
33.3.5.3	Changing backOfficeURL to Use SSL Port	33-18
33.3.5.4	Changing SOA Server URL to Use SSL Port	33-19
33.3.5.5	Configuring SSL for Design Console.....	33-20
33.3.5.6	Configuring SSL for Oracle Identity Manager Utilities	33-21
33.3.5.7	Configuring SSL for SPML/Callback Domain.....	33-22
33.3.5.8	Connecting Oracle Identity Manager With SOA	33-23
33.3.6	Enabling SSL for Oracle Identity Manager DB.....	33-23
33.3.6.1	Setting Up DB in Server-Authentication SSL Mode	33-23
33.3.6.2	Creating KeyStores and Certificates	33-25
33.3.6.3	Updating Oracle Identity Manager.....	33-27
33.3.6.4	Updating WebLogic Server.....	33-27
33.3.7	Enabling SSL for LDAP Synchronization.....	33-29
33.3.7.1	Enabling OVD-OID with SSL	33-29
33.3.7.2	Updating Oracle Identity Manager for OVD Host/Port	33-30
33.3.7.3	Enabling Managed WebLogic Server with SSL	33-30

34 Managing Identity and Resource Information

34.1	Overview of User Management.....	34-1
34.2	Managing Organization Information.....	34-1
34.3	Viewing Resources Allowed or Disallowed for Users	34-2
34.3.1	Policy History Tab	34-3
34.4	Assigning Role Entitlements	34-4

35 Securing a Deployment

Part XI Appendixes

A Configuring SSO Providers for Oracle Identity Manager

A.1	Enabling Oracle Identity Manager to Work With OpenSSO	A-1
A.1.1	Prerequisites	A-1
A.1.2	Integrating Oracle Identity Manager with OpenSSO.....	A-2

A.1.3	Running Validation Tests to Verify the Configuration.....	A-5
A.2	Enabling Oracle Identity Manager to Work With IBM Tivoli Access Manager	A-6
A.2.1	Prerequisites	A-6
A.2.2	Integrating Oracle Identity Manager with IBM Tivoli Access Manager	A-6
A.2.3	Running Validation Tests to Validate the Configuration	A-8
A.3	Enabling Oracle Identity Manager to Work With CA SiteMinder	A-9
A.3.1	Prerequisites	A-9
A.3.2	Integrating Oracle Identity Manager with CA SiteMinder	A-9
A.3.3	Running Validation Tests to Validate the Configuration	A-12
A.4	Configuring SSO for XIMDD	A-12

B Localizing Challenge Questions and Responses

Index

List of Examples

8-1	The User.xml Configuration File	8-25
8-2	Entity XML Schema Definition	8-142
22-1	Sample Configuration File.....	22-1
22-2	Configuring Max Retries.....	22-3

List of Figures

1-1	Layout of the Oracle Identity System Administration Console	1-2
1-2	Layout of the Help Interface.....	1-3
4-1	The Create Password Policy Page	4-3
5-1	Delegate Attestation	5-5
5-2	Creating an Attestation Task: Workflow	5-6
5-3	Flow of Events When Reviewer Responds to Entitlement	5-7
5-4	Flow of Events After Attestation Task Response Is Submitted.....	5-8
5-5	Follow-Up Action Sub-Flow.....	5-9
6-1	Rule for Auto-approval.....	6-25
6-2	Stages of Certification in TPAD	6-33
6-3	Phase One With Verification	6-34
6-4	Phase Two With Verification.....	6-38
6-5	Final Review Phase.....	6-40
7-1	The Manage Form Page	7-3
7-2	The Edit Standard Field Dialog Box.....	7-4
8-1	The Create Text Field Page.....	8-3
8-2	The Create Lookup Field Page.....	8-7
8-3	Users Page.....	8-10
8-4	Create User Page.....	8-10
8-5	Create User Page in Customization Mode	8-11
8-6	Object Tree Page in Customization Mode.....	8-12
8-7	Confirm Task Flow Edit Dialog Box	8-13
8-8	Add Content Dialog Box.....	8-14
8-9	Add Content Dialog Box Displaying the Data Component - Manage Users Folder	8-16
8-10	Options for Adding a UDF of Text Type.....	8-18
8-11	Component Properties Dialog Box.....	8-19
9-1	Application Instance Architecture.....	9-2
9-2	Application Instance Search	9-7
9-3	The Select Organizations Dialog Box.....	9-9
9-4	Application Instance Soft Deletion Flow	9-12
9-5	The Manage Form Page	9-14
9-6	Connected Application Instance.....	9-16
9-7	Password Policy for Application Instance	9-17
9-8	Attach Password Policy to Application Instance	9-18
9-9	Entitlement Soft-Deletion Flow.....	9-28
10-1	Disconnected Resource Architecture	10-2
10-2	Create Application Instance Attributes	10-4
10-3	Provision Operation for Disconnected Resources.....	10-6
10-4	Create Process Task	10-10
10-5	Edit Entitlement	10-10
10-6	Sample Adapter Variable Mapping	10-11
10-7	Add Manual Provisioning Rule	10-14
11-1	The Search and Select: Lookup Type Window.....	11-2
11-2	The Create Lookup Type Dialog Box.....	11-3
11-3	The Edit Lookup Type Dialog Box	11-4
12-1	Connector Lifecycle	12-4
12-2	Search Results Table Showing Details of Connectors.....	12-6
12-3	The Select Connector to Install Page	12-9
12-4	Connector History and Dependency	12-10
12-5	The Connector Installation Page.....	12-10
12-6	Connector Management Wizard for Defining Connectors.....	12-15
12-7	Step 1 of the Connector Management Wizard.....	12-16
12-8	Step 2 of the Connector Management Wizard.....	12-17
12-9	Step 3 of the Connector Management Wizard.....	12-18

12-10	Step 4 of the Connector Management Wizard.....	12-19
12-11	Options to Select More Objects or Exit	12-20
12-12	Selected Connector Objects.....	12-21
12-13	Connector Name and Release Number	12-22
12-14	The XML Selection from File System Page.....	12-24
12-15	Searching the Connector	12-25
12-16	The Provide New Names for Resource Objects Page	12-25
12-17	The Provide New Names for Process Definitions Page	12-26
12-18	The Provide New Names for Process Forms Page.....	12-26
12-19	The Provide New Names for IT Resource Type Definitions Page	12-27
12-20	The Provide New Names for IT Resources Page	12-28
12-21	The Provide New Names for Scheduled Tasks Page.....	12-28
12-22	The Provide New Names for Lookup Type Definitions Page.....	12-29
12-23	The Provide a Prefix for Adapters Page	12-30
12-24	The Provide New Names for Reconciliation Rules Page	12-30
12-25	The Object Names Summary Page	12-32
12-26	The Object Clone Generation Page.....	12-34
12-27	The File Download Dialog Box	12-34
12-28	The Connector Management Page	12-36
12-29	The Select Connector XML to Upgrade Page.....	12-49
12-30	The Resource Object Mapping Page	12-50
12-31	The Define Resource Scope Page	12-50
12-32	The Define Process Definition Mapping Page	12-51
12-33	The Process Definition Mapping Summary Page	12-52
12-34	The Define Form Mappings Page	12-52
12-35	The Form Mapping Summary Page	12-53
12-36	The Define IT Resource Type Definition Mappings Page.....	12-54
12-37	The IT Resource Type Definition Mapping Summary Page.....	12-54
12-38	The Preupgrade Steps Page	12-55
12-39	The Select Connector Objects to Be Upgraded Page.....	12-55
12-40	The Connector Upgrade Status Page	12-56
12-41	The Select Connector XML to Upgrade Page.....	12-58
12-42	The Preupgrade Steps Page	12-59
12-43	The Select the Connector Objects to be Upgraded Page	12-59
12-44	The Connector Upgrade Status Page	12-60
12-45	The Variable List Tab of the Adapter Factory Form	12-62
12-46	The Edit Adapter Factory Task Parameters Dialog Box.....	12-63
12-47	The Integration Tab of the Editing Task Dialog Box	12-64
12-48	The Editing Data Mapping for Variable Dialog Box	12-64
12-49	The Pre-Populate Adapters Dialog Box.....	12-65
12-50	The Map Adapter Variable Dialog Box	12-65
13-1	Provisioning and Reconciliation.....	13-1
13-2	Trusted Source Reconciliation from Single and Multiple Authoritative Sources	13-4
13-3	Account Reconciliation From a Target System.....	13-5
13-4	Identity and Account Reconciliation.....	13-5
13-5	Reconciliation Process Flow	13-6
14-1	Sample Mapping of Composite Payload.....	14-8
14-2	SOAEmailNotificationProviderMBean Properties	14-9
14-3	The Create Notification Template Page.....	14-14
14-4	Notification Search Result	14-14
14-5	Notification Template Modification.....	14-15
16-1	Create System Property Page	16-23
16-2	List of System Properties	16-28
16-3	Advanced Search Result	16-29
16-4	System Property Detail Page.....	16-30

17-1	High-Level Catalog Architecture.....	17-6
17-2	Test to Production Process for Catalog.....	17-21
17-3	Catalog Synchronization Diagnostic Flowchart.....	17-26
17-4	Trouble Shooting Synchronization Application Instances Flowchart	17-27
17-5	Trouble Shooting Synchronizing Entitlements Flowchart.....	17-28
17-6	Diagnostic Flowchart With Security Issues.....	17-30
17-7	Catalog Search	17-31
18-1	Design Components of the Auditing Process.....	18-2
22-1	Failed Async Tasks	22-4
25-1	Sample Output for Orchestration Status Test.....	25-8
32-1	Integration with Other Components.....	32-1
34-1	Organizational Default Form	34-2
34-2	Policy History Form.....	34-3
34-3	Roles Form	34-5
A-1	The Resources Screen	A-14

List of Tables

4-1	Fields in the Policy Rules Section	4-4
4-2	Fields in Custom Policy Section.....	4-6
6-1	Configuration Properties	6-8
6-2	Risk Factors	6-21
6-3	Actions or System Events That can Impact Risk Summary Values.....	6-23
6-4	Troubleshooting Identity Certification Issues	6-41
8-1	Fields in the Create Text Field Page	8-3
8-2	Fields in the Create Lookup Field Page	8-7
8-3	Entities and Corresponding Data Components and View Objects	8-14
9-1	Fields in the Create Application Instance Page	9-5
9-2	Possible Scenarios and Duplicate Validation Basis.....	9-24
9-3	Duplicate Validation Based on Operation.....	9-25
10-1	Manual Provisioning SOA Composite Payload Attributes	10-2
10-2	Adapter Variable Mappings for Entitlement Grant.....	10-11
10-3	Adapter Variable Mappings for Entitlement Revoke.....	10-12
10-4	Manual Process Task Action Statuses	10-13
10-5	Troubleshooting Disconnected Resources	10-15
13-1	Types of Reconciliation	13-2
13-2	Regular and Changelog Reconciliation Modes	13-9
13-3	Advanced Search Fields	13-12
13-4	Columns in the Matched Accounts Table	13-13
13-5	Columns in the History Table	13-13
13-6	Actions for Event Status and Types	13-14
14-1	UMSEmailProviderMBean Properties	14-5
14-2	Default SMTP Email Notification Provider Properties	14-7
14-3	SOA Email Notification Provider Properties	14-9
14-4	Default Notification Templates.....	14-11
15-1	Child Elements of the Scheduler Element	15-2
15-2	Predefined Scheduled Tasks	15-7
15-3	LDAP Scheduled Jobs	15-16
15-4	Fields in the Search Results Table.....	15-24
16-1	Default System Properties in Oracle Identity Manager	16-2
16-2	Nondefault System Properties	16-22
16-3	Fields of the Create System Property Form	16-24
16-4	Data Levels Associated with a System Property	16-24
17-1	Catalog Metadata Loader Sample	17-16
17-2	Catalog Customization Steps	17-22
18-1	User Group Membership Tables.....	18-3
18-2	User Resource Instance Tables.....	18-4
18-3	Resource Lifecycle Process Tables	18-4
18-4	Definition of the UPA Table	18-5
18-5	User Profile Audit Tables.....	18-6
18-6	Definition of the GPA Table	18-8
19-1	Scheduled Tasks for BI Publisher Reports	19-47
20-1	Active and Archive Reconciliation Tables	20-2
20-2	Output Files Generated by the Task Archival Utility.....	20-10
20-3	Archival Tables.....	20-11
20-4	Input Parameters.....	20-12
20-5	Logs Generated by the DB Archival Utility	20-14
21-1	Oracle Identity Manager Diagnostic Message Types	21-2
21-2	Oracle Identity Manager Loggers.....	21-6
21-3	Log Levels for log4j.....	21-10
26-1	Troubleshooting Inconsistent Roles	26-4

28-1	Troubleshooting Remote Manager	28-6
29-1	Error Messages and Solutions	29-9
33-1	CSF Keys.....	33-12
34-1	Fields of the Organizational Defaults Form.....	34-2
34-2	Fields of the Policy History Form.....	34-3
35-1	Securing a Deployment.....	35-1
A-1	Authentication Chain	A-10

Preface

The *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* describes how to perform system administration tasks in Oracle Identity Manager.

Audience

This guide is intended for system administrators who can perform system configuration tasks, application servers, JMS, and connectors, scheduled task management, connector installation and deployment, and archival utility management.

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 that have purchased support 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, refer to the following documents:

- *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware User'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:

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

Part I

Overview

This part provides an overview of the Oracle Identity System Administration interface.

It contains the following chapter:

- [Chapter 1, "Oracle Identity System Administration Interface"](#)

Oracle Identity System Administration Interface

This chapter discusses the procedure to access and log in to Oracle Identity Manager System Administration Console. This chapter provides you an overview of the Oracle Identity Manager System Administration Console.

This chapter discusses the following topics:

- [Logging in to Oracle Identity Manager System Administration Console](#)
- [Overview of the Oracle Identity Manager System Administration Console](#)

1.1 Logging in to Oracle Identity Manager System Administration Console

To log in to Oracle Identity Manager System Administration Console:

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

`http://HOSTNAME:PORT/sysadmin`

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, *sysadmin*, is case-sensitive.

2. After the Oracle Identity Manager System Administration Console login page is displayed, log in with your user name and password.

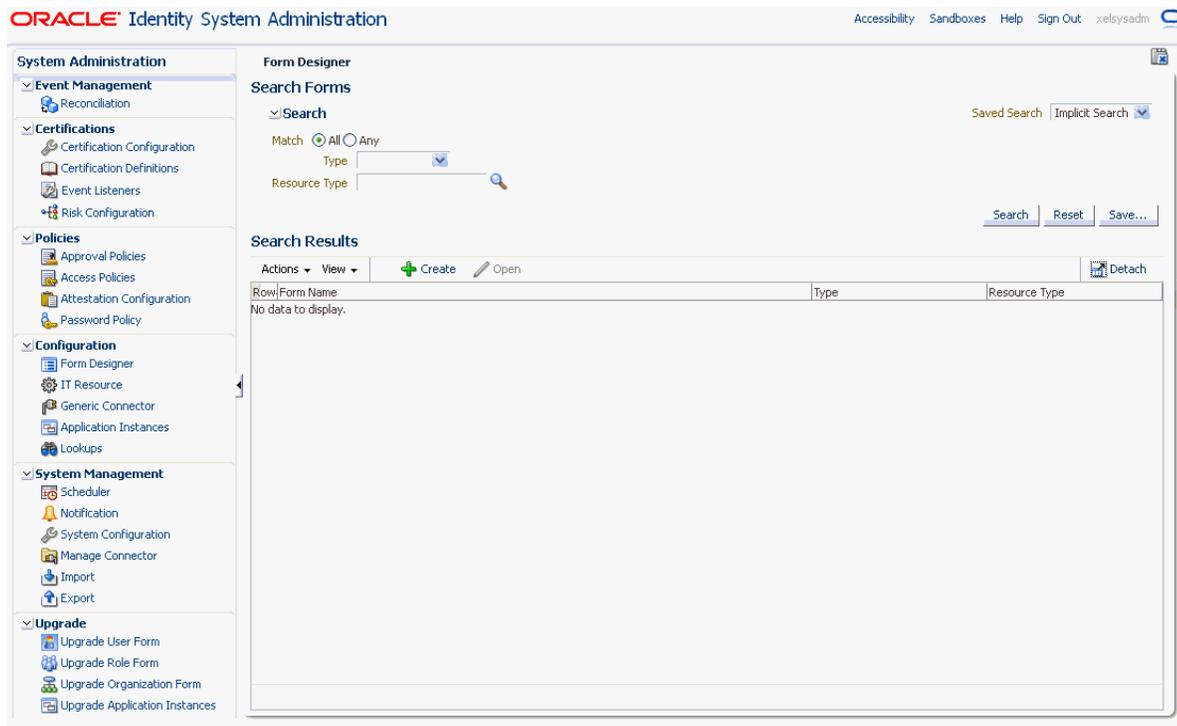
1.2 Overview of the Oracle Identity Manager System Administration Console

The interface of the Oracle Identity Manager System Administration Console is composed of the following areas:

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

[Figure 1–1](#) shows a sample page and the layout of the interface.

Figure 1–1 Layout of the Oracle Identity System Administration Console



1.2.1 Links

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

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

1.2.1.1 Accessibility

The Oracle Identity Manager System Administration Console interface 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 the Oracle Identity Manager System Administration Console.
- **I use large fonts**

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

1.2.1.2 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.

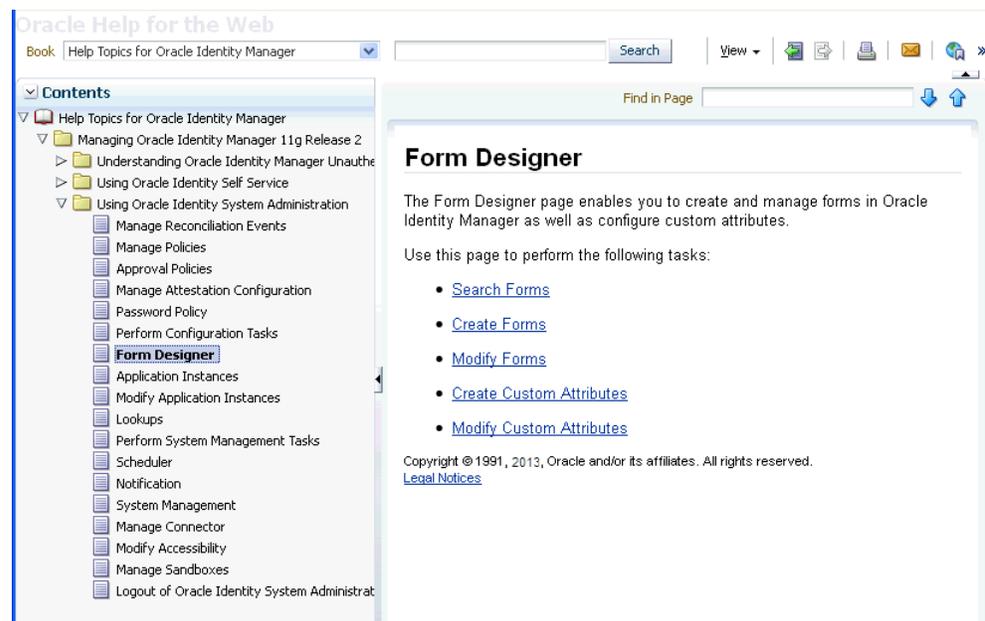
In the Manage Sandboxes page, you can create, delete, activate, deactivate, and publish sandboxes. See the "Managing Sandboxes" section in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information.

1.2.1.3 Help

The Oracle Identity Manager System Administration Console interface includes a help system. Clicking the Help link opens the help system in a new window. In addition, this interface provides context-sensitive help. For example, if you are in the Form Designer page and click the Help link, then help content related to form designer is displayed.

Figure 1–2 shows a sample page and default layout of the help interface.

Figure 1–2 Layout of the Help Interface



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

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

1.2.1.3.1 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:** Restores 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.

1.2.1.3.2 Lower Left Pane

The lower 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.

1.2.1.3.3 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.

1.2.1.4 Sign Out

Click the Sign Out link to log out of the Oracle Identity System Administration Console.

1.2.2 Left and Right Panes

Every page in the Oracle Identity System Administration Console 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 the System Administration Console. 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:

- [Event Management](#)
- [Certifications](#)
- [Policies](#)
- [Configuration](#)
- [System Management](#)
- [Upgrade](#)

1.2.2.1 Event Management

The Event Management region contains the Reconciliation page. Use the Reconciliation page to create and manage reconciliation events. See "[Managing Reconciliation Events](#)" on page 13-10 for more information.

1.2.2.2 Certifications

The Certifications region contains the following:

- **Certification Configuration**

Use this page to set default options that are used during certification creation based on the type of certification. These options can be changed during the certification creation process for each certification definition.

See "[Configuring Certification Options in Identity System Administration](#)" on page 6-8 for more information.
- **Certification Definitions**

Use this page to manage certification definitions for user, role, application instance, and entitlement certifications.

See "[Managing Certification Definitions](#)" on page 6-9 for more information.
- **Event Listeners**

Use this page to manage event listeners that allow an administrator to detect specific business events and store the event details for certification.

See "[Configuring Event Listeners and Certification Event Trigger Jobs](#)" on page 6-26 for more information.
- **Risk Configuration**

Use this page to assign risk levels to roles, application instances, and entitlements, as well as to certain predefined risk factors.

See "[Understanding How Risk Summaries are Calculated](#)" on page 6-19 for more information.

1.2.2.3 Policies

The Policies region contains the following:

- **Approval Policies**

Use this page to create and manage approval policies. An approval policy helps to associate request types with approval processes defined in the workflow service.

See "[Managing Approval Policies](#)" on page 2-1 for more information.
- **Access Policies**

Use this page to create and manage access policies. Access policies define how to automate the provisioning of target systems to users.

See "[Managing Access Policies](#)" on page 3-1 for more information.
- **Attestation Configuration**

Use this page to create, configure and manage attestation processes, and work with the attestation dashboard.

See "[Managing Attestation Processes](#)" on page 5-1 for more information.
- **Password Policy**

Use this page to create and manage password policies. Password policy management includes setting password policy rules, and creating, searching, and deleting password policies.

See "[Managing Password Policies](#)" on page 4-1 for more information.

1.2.2.4 Configuration

The Configuration region contains the following:

- Form Designer

Use this page to create and manage forms of type users, roles, organizations, catalog, and resources that are not predefined in Oracle Identity Manager.

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

- IT Resource

Use this page to create and manage IT resources. An IT resource is composed of parameters that store connection information about a target system. Oracle Identity Manager uses this information to connect to a specific installation or instance of the target system.

See *Managing IT Resources in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information.

- Generic Connector

Use the Generic Connector page to create and manage generic connectors. Generic connectors are basic connectors without advanced features. The connectors utilize generic connectivity technologies, such as SPML and JDBC.

- Application Instances

Use this page to create and manage application instances. An application instance is a combination of an IT resource instance and resource object. Users have accounts and entitlements that are associated with application instance and not with the IT resource instance or resource object.

See "[Managing Application Instances](#)" on page 9-1 for more information.

- Lookups

Use this page to create and manage lookup definitions. See "[Managing Lookups](#)" on page 11-1 for more information.

1.2.2.5 System Management

The System Management region contains the following:

- Scheduler

Use this page to create and manage scheduled jobs. Scheduled jobs are jobs that are run at specified time intervals to manage various activities in Oracle Identity Manager.

See "[Managing the Scheduler](#)" on page 15-1 for more information.

- Notification

Use this page to create and manage notification templates. A notification template is used to send notifications.

See "[Managing Notification Service](#)" on page 14-1 for more information.

- System Configuration

Use this page to create and manage system properties. System properties define the characteristics that control the behavior of Oracle Identity Manager.

See "[Managing System Properties](#)" on page 16-1 for more information.

- Manage Connector

Use this page to define, install, clone, upgrade, and uninstall predefined connectors in an Oracle Identity Manager environment. A predefined connector is designed for commonly used target systems such as Microsoft Active Directory and PeopleSoft Enterprise Applications.

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

- Import

Use this page to import Oracle Identity Manager configurations by using the Deployment Manager.

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

- Export

Use this page to export Oracle Identity Manager configurations by using the Deployment Manager.

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

1.2.2.6 Upgrade

When you upgrade your Oracle Identity Manager environment from 11g Release 1 (11.1.1.5) to 11g Release 2 (11.1.2.1.0), the custom attributes for entities (such as users, roles, organizations, and application instances) exist in the back-end. However, if you want to display these attributes as form fields in the Oracle Identity Manager user interface, then you must customize the associated pages on the interface to add the custom form fields. To do so, use the links in the Upgrade region of the Identity System Administration Console.

The Upgrade region contains the following:

- Upgrade User Form

Use this page to create and manage custom form fields for the user entity.

- Upgrade Role Form

Use this page to create and manage custom form fields for the role entity.

- Upgrade Organization Form

Use this page to create and manage custom form fields for the organization entity.

- Upgrade Application Instances

Use this page to create and manage custom form fields for the application instance entity.

For detailed information about upgrading Oracle Identity Manager 11g Release 1 (11.1.1.5.0) environment to Oracle Identity Manager 11g Release 2 (11.1.2.1.0), see *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management*.

Part II

Policy Administration

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

It contains the following chapters:

- [Chapter 2, "Managing Approval Policies"](#)
- [Chapter 3, "Managing Access Policies"](#)
- [Chapter 4, "Managing Password Policies"](#)
- [Chapter 5, "Managing Attestation Processes"](#)

Managing Approval Policies

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.

You can define multiple approval policies for a request type. Each approval policy is associated with an approval process. When the request is submitted, in the approval initiation phase, all the approval processes associated with the request type are picked up dynamically. Each approval policy has a priority in the backend. Each approval policy decides on what process to invoke based on approval policy priority and approval policy rule.

Approval policy priorities are based on the following:

- For request level, request type + request level
- For operation level, request type + operation level + scope, which is the specific entity associated with the request

When the request engine tries to initiate the approval workflow, it picks up all the available approval policies for that request type in the order of priority. The approval policy with highest priority is taken up and its approval policy rule is evaluated. If the evaluation fails, then the approval policy rule of the approval policy with the next priority is evaluated. If the outcome of the evaluation is true, then the corresponding approval process associated with the approval policy is selected to be the workflow for that request. For information about creating approval policy rules, see "[Creating Approval Policies](#)" on page 2-4.

Note: There is only one approval policy rule per approval policy. The rules can be complex, containing multiple conditions and other rules. The rules do not exist as independent entities and cannot be reused in any other approval policy. There is no default rule for an approval policy.

Approval Policy creation and modification supports request types, such as Provision Application Instance, Grant Entitlement, and Revoke Entitlements. In addition, approval policies support the heterogeneous request type, in which multiple entities are being requested in the same request. For the heterogeneous request type, approval

policies can be created only at the request level. At the operation level, the appropriate request type is set based on the entity type and operation associated with the child request. For more information about heterogeneous requests, see "Heterogeneous Requests" in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

This chapter describes the following topics:

- [Approval Selection Methodologies](#)
- [Creating Approval Policies](#)
- [Searching Approval Policies](#)
- [Modifying Approval Policies](#)
- [Modifying the Priority of an Approval Policy](#)
- [Deleting Approval Policies](#)
- [General Guidelines](#)

2.1 Approval Selection Methodologies

An approval process selection methodology is an algorithm that selects the approval workflow to be initiated. Based on the request type and the approval level, the request engine decides which methodology to be used and evaluates the approval process accordingly.

If no approvals are defined at the request level, it means that a default approval process is invoked. This default approval process is shipped with Oracle Identity Manager and is assigned to the administrator. If no approvals are defined at the operation level, it means that a default approval process is invoked. If no template-level approvals are defined, then it is assumed that no approvals are required at that level.

Note: If the requester has authorizer permissions on an entity, then operation-level approval request is not generated irrespective of the approval policies. See "Admin Role Assignment" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for authorizer permissions.

The following methodologies are used:

- [Request-Level Methodology](#)
- [Operation-Level Methodology: Organization-Based Selection](#)
- [Operation-Level Methodology: Role-Based Selection](#)
- [Operation-Level Methodology: Application Instance-Based Selection](#)

2.1.1 Request-Level Methodology

This methodology is used for all request types at the request level of approval. The determination algorithm of the request-level selection methodology is as follows:

1. Search for all the approval policies configured for the request level and for the request type with which the request is associated in ascending order of approval policy priority. If the approval policies matching this criteria are found, then:

- a. Evaluate the approval policy rules associated with each approval policy to determine the approval workflow. When evaluating the approval policy rules, for the first approval policy rule whose evaluation results in true, the corresponding approval workflow associated with that approval policy is selected. If automatic approval is specified in the approval policy, then request level approval is automatically approved.
 - b. If none of the approval policy rules are satisfied, then it is considered that no approval workflow is configured at the request level.
2. If no approval workflow is determined, then the default request-level approval is selected.

2.1.2 Operation-Level Methodology: Organization-Based Selection

This methodology is used for all user-related request types, such as Create User, Modify User, Disable User, Enable User, and Delete User, at the operation level of approval. The determination algorithm for the organization-based selection methodology at operation level is as follows:

1. Get the user's organization entity for which request is created.
2. Search for all the approval policies configured for the operation level, for the request type associated with the request, or for all organizations in ascending order of the approval policy priority. If the approval policies matching this criteria is found, then:
 - a. Evaluate the approval policy rules associated with each approval policy to determine the approval workflow. When evaluating approval policy rules, for the first approval policy rule whose evaluation results in true, the corresponding approval workflow associated with that approval policy is selected. If automatic approval is specified in the approval policy, then the request is automatically approved at the operation level.
 - b. If none of the approval policy rules are satisfied, then it is considered that no approval workflow is configured at the operation level for this organization.
3. If no approval workflow is configured for that organization entity, then follow the organization hierarchy till either the root node or the domain boundary, which is the root organization in the organization hierarchy. Repeat step 2 for each organization node.
4. If no approval workflow is determined, then the default operation-level approval is selected.

2.1.3 Operation-Level Methodology: Role-Based Selection

This methodology is used for all role-related request types at the operation level of approval. The determination algorithm for the role-based selection methodology at operation level is as follows:

1. Get the role entity being assigned to or removed from the user.
2. Search for all the approval policies configured for the operation level, for the request type associated with the request, or for all roles being assigned or removed in ascending order of the approval policy priority. If the approval policies matching this criteria is found, then:
 - a. Evaluate the approval policy rules associated with each approval policy to determine the approval workflow. When evaluating approval policy rules, for the first approval policy rule whose evaluation results in true, the

- **Policy Name:** Enter a name for the approval policy. This is a mandatory attribute.
- **Description:** Enter the details about what this approval policy will do.
- **Request Type:** Select the request type by selecting from the LOV, for example, Assign Roles. This is a mandatory attribute.

Note: The following request types have been deprecated and do not appear in the LOV:

- Provision Resource
 - De-Provision Resource
 - Enable Provisioned Resource
 - Disable Provisioned Resource
 - Modify Provisioned Resource
-

- **Level:** Select the approval level that you want to implement for this approval policy. This is a mandatory attribute. For more information about approval levels, see "Approval Levels" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
- **Scope Type:** Set automatically based on the request type selection. For example:
 - If request type is set to Create User, then Scope Type is automatically set to Organization.
 - If request type is set to Provision Resource, then Scope Type is automatically set to Resource.
 - If request type is set to Assign Roles, then Scope Type is automatically set to Role.
 - If request type is set to provision application instance or entitlement, then scope type is automatically set to "Application Instance".

Note: The Scope Type, All Scope, and Scope fields are applicable only if the Level field is set to Operation Level. These fields are disabled if the Level field is set to Request Level.

- **All Scope:** Select this option to specify the approval policy associated with all entities for a particular entity type. For example, for the Create User request type, Scope Type is Organization. If you select All Scope, then this approval policy is applicable to all organizations in Oracle Identity Manager. This is same for Resource and Role scopes.
- **Scope:** Select this option to specify the approval policy associated with the specific entity for a particular entity type. An approval policy can be associated with a specific Scope based on the Scope Type.
The Scope field is disabled if All Scope field is set. If All Scope field is not set, then this field becomes mandatory and must be set with some value.
- **Auto Approval:** Select this option to specify automatic approval at the request level or operation level that you select in the Level field.

- **Approval Process:** Select the workflow that you want to associate with this approval policy. If Auto Approval is selected, then this field is disabled and you cannot set any value. If Auto Approval is not set, then this field becomes mandatory.
- 5. On the Step 2. Set Approval Rule and Component page, enter the name of the approval policy rule in the Rule Name field, for example, RuleTest1.
- 6. In the Rule Components section, you can define the parameters of the approval policy rule. To do so, click the icon next to the View list. The Add Simple Rule dialog box is displayed. In this dialog box, you must select values for the following fields, and then click **Save**.
 - **Entity:** Entity, such as Requester, Beneficiary, or Resource, with which the approval policy rule is associated. This varies based on the selected request type and the approval level.
 - **Attribute:** Attribute of the above selected entity.

Note:

- If an entity attribute is a UDF, then the name of the UDF is displayed in the Attribute field. If you want the display name to be visible in the Attribute field, then perform the following procedure:
 1. In a text editor, open the customResources.properties file located in the *OIM_HOME*/server/customResources directory.
 2. Add an entry in the following syntax:


```
global.udf.<udf_column_name>=<unicoded_label_string>
```

In this entry, replace:

udf_column_name with the name of the UDF

unicoded_label_string with the display name of the UDF

For example,

```
global.udf.usr_udf_jobcode=Job Code
```
 3. Save and close the file.
- When writing simple rule expressions, if an entity attribute has an encoded value, then create the expression by using the encoded value, not the lookup-code definition. For example, for the account status attribute, create the expression by using the encoded value 1 or 0, not the decoded value Locked or Unlocked.

-
-
- **Condition:** Condition of the approval policy rule, such as Equals, Not Equals, or Starts With.
 - **Value:** Value of the condition.

Note: If you use the User Login attribute in a rule expression, the corresponding User Login ID value must be entered in all uppercase letters, otherwise the expression will not evaluate to true.

- **Parent Rule Container:** The rule container with which this approval policy rule needs to be associated with.
- 7. Rule containers can be used for modeling complex conditions with And and Or combinations. To add a rule container for the approval policy rule, in the Rule Components section, from the Actions menu, select **Add Rule Container**. The Add Rule Container dialog box is displayed. In this dialog box, enter or select values for the following fields, and then click **Add**.
 - **Rule Container Name:** The name of the rule container.
 - **Parent Rule Container:** The name of the rule container under which you want to create this rule container. A rule container can hold either another rule container or rule elements with the AND or OR operators in a hierarchical order.
 - **Operator:** The operators are AND and OR.
- 8. After the approval rule creation is complete, click **Next**.
- 9. On the Step 3. Review Approval Policy Summary page, verify the information that you have specified for the approval policy. You can click the Back button to modify any information if you want. Click **Finish** to create the approval policy.
- 10. A message is displayed confirming that the approval policy has been created. Click **OK**.

2.3 Searching Approval Policies

To search for approval policies:

1. In the Oracle Identity Manager Advanced Administration, on the left pane of the Approval Policies tab, in the Search field, enter a search criterion to search for approval policies. You can specify the asterisk (*) wildcard character to specify the search criterion.

Note: In simple and advanced search for approval policies, searching with translated approval policy names is not supported. Oracle Identity Manager supports only English string search for approval policies. For default approval policies, you can search with English policy names as stored in the database. However, if you create an approval policy by specifying its name in another language, then you can search it by using the same string, and not in any other language.

2. Click the Search icon. A list of approval policies is displayed in a search results table, with the following fields:
 - **Policy Name:** The name of the approval policy.
 - **Request Type:** The name of the request type associated with the approval policy.

Note: As mentioned earlier in this chapter, the following request types have been deprecated:

- Provision Resource
- De-Provision Resource
- Enable Provisioned Resource
- Disable Provisioned Resource
- Modify Provisioned Resource

If you have upgraded to the current release, then these deprecated request types can appear when you search for or modify approval policies that were created (based on the deprecated request types) in the earlier release. In addition, requests based on any of the deprecated request types that were created in the earlier release can appear in the Track Request page of Oracle Identity Self Service.

- **Scope:** The associated application instance, organization, or role name. The scope is populated only for the approval policies associated with the operation level request.
- **Level:** The approval level.
- **Rule Name:** The name of the approval policy rule.
- **Approval Process:** The approval process associated with the approval policy.
- **Priority:** Priority of the approval policy.

You can also use the Advanced Search option in the Approval Policies tab to search for approval policies based on advanced search criteria. To do so:

1. On the left pane of the Approval Policies tab, click **Advanced Search**. The Advanced Search: Approval Policies page is displayed.
2. Enter values in the fields to specify a search criteria. You can specify a combination of approval policy name, name of the request type associated with the approval policy, approval level, scope type such as resource, organization, or role, and scope to specify the search criteria.
3. Click **Search**. The search result displays a list of approval policies with information about priority, policy name, request type, scope, level, rule name, and approval process.

2.4 Modifying Approval Policies

To modify approval policies:

1. On the search results table, select a policy.
2. From the Actions menu, select **Open**. The Approval Policy Details form is displayed.
3. In the Policy Details section, edit the fields to modify the approval policy.

Note: You cannot modify the approval policy rule name and approval policy priority attribute.

4. In the Approval Rules section, modify approval policy rules, if required. To modify an approval policy rule, you can add a simple rule, add a rule container, modify rule components, or delete a rule component. For detailed information about adding approval policy rules and rule containers, see steps 5 through 7 in ["Creating Approval Policies"](#) on page 2-4.
5. To modify rule components:
 - a. Select the approval policy rule.
 - b. From the Actions menu, select **Modify Rule Components**. The Modify Rule Components dialog box is displayed.
 - c. Edit the values in the fields provided, and click **Apply**.
6. To delete rule components:
 - a. Select the approval policy rule that you want to delete.
 - b. From the Actions menu, select **Delete Rule Components**. A message box is displayed asking for confirmation.
 - c. Click **Yes** to confirm the deletion.
7. Click **Save** to save the changes in the approval policy.

2.5 Modifying the Priority of an Approval Policy

To modify the priority of an approval policy:

1. From the approval policies search result, select a policy whose priority you want to modify.
2. From the Actions menu, select **Set Priority**. The Modify Approval Policy priority wizard is displayed.
3. In the Set Policy Details page, specify values in the fields as required. For information about the fields in this page, see step 4 in ["Creating Approval Policies"](#) on page 2-4. Then, click **Next**.
4. In the Set Policy Priorities page, enter a number to specify the priority of the approval policy. Then, click **Next**.
5. In the Review and Confirm page, the policy name and the priority that you set are displayed for your review. If you want to change the current priority, then click **Back**.

Otherwise, click **Finish**. A message is displayed stating the approval policy priority has been changed successfully.
6. Click **OK**.

Note: Oracle Identity Manager does not perform any validation and allows you to set the same priority to multiple approval policies. It is not recommended to set the same priority to multiple approval policies.

2.6 Deleting Approval Policies

To delete an approval policy:

1. From the approval policies search results, select the approval policy that you want to delete.
2. From the Actions menu, select **Delete**. A message box is displayed asking for confirmation.
3. Click **Yes** to confirm the deletion.

2.7 General Guidelines

Oracle recommends leveraging Oracle Business Rules (OBR) in SOA instead of using approval policies. See "Developing Workflows for Approval and Manual Provisioning" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about using Business Rules in SOA.

In addition, follow these guidelines:

- Review all approval requirements and distill to a set of flows.
- Evaluate if request-level approval is required.
- In the operational composite, leverage the request web service to have a high-level split based on the type of request, such as grant, revoke, or modify, followed by fine-grained split. Here, you can again leverage the request web service and the default payload to make decisions. The evaluation can also be externalized for ease of use or maintenance by using OBR.
- Add one or more Human Tasks and a decision point to pick between the Human Tasks. The Human Task represents the actual approval workflow.
- Create a new composite only as a last option.

Managing Access Policies

Access policies are a list of roles and resources to be provisioned or deprovisioned. Access policies are used to automate the provisioning of target systems to users. This is explained with the help of the following example:

A user belongs to multiple roles created in Oracle Identity Manager. Suppose a role Role1 has a membership rule assigned to it. Membership rules can be designed based on the organization that the user belongs to, such as "Organization Name = "Org1". Roles can have access policies assigned to them. An access policy states which resource would be provisioned and/or denied to a role when the access policy is applicable. Therefore, when a user is created in the Org1 organization, it satisfies a membership rule and grants the Role1 role to the user. This in turn triggers the access policy assigned to the role and then provisions or denies the resources mentioned in the access policy.

This chapter describes how to create and use access policies for users and resources in Oracle Identity Manager. It contains the following sections:

- [Terminologies Used in Access Policies](#)
- [Features of Access Policies](#)
- [Creating Access Policies](#)
- [Managing Access Policies](#)
- [Provisioning Multiple Instances of the Same Resource via Access Policy](#)

3.1 Terminologies Used in Access Policies

The following terminologies are associated with access policies:

Resource

A resource is a logical entity in Oracle Identity Manager that can be provisioned to a user or an organization in Oracle Identity Manager. For example, Microsoft Active Directory (AD), Microsoft Exchange, SAP, UNIX, and Database is modeled as a resource in Oracle Identity Manager.

Resources are templated definitions that are associated with one or more workflows called Provisioning Process in Oracle Identity Manager, which model the lifecycle management, such as how to provision, revoke, enable, and disable.

Resources also have entities called forms associated with them. Forms represent a collection of attributes associated with the resource. For instance, a form associated with AD server includes attributes such as SAM Account Name, Common Name, and

User Principal Name. Forms also contain an attribute of type IT Resource (see "[IT Resource Type](#)" on page 3-2 for details).

Resources can be marked Allow Multiple, which would allow multiple instances of a resource to be provisioned to a user or an organization.

Account

Accounts are actual instances of a resource that are created and provisioned to a user or organization in Oracle Identity Manager. For example, an e-mail account on an Exchange server is an account (instance) of resource type Exchange.

Accounts have specific values for the attributes of the associated form.

IT Resource Type

IT resource type is a logical entity in Oracle Identity Manager used to model a physical target and all its attributes including (but not limited to) the connectivity information and the credentials required to connect to the physical computer. For example, IT resource type AD server is used to model an actual AD server.

IT Resource Instance

These are actual instances of specific IT resource type that represent the actual physical target. They also have specific values for all the attributes of the physical target, such as IP address, port, user name, and password. Two physical AD servers in a deployment are represented by two instances of IT resource type AD Server.

Account Discriminator

Account discriminator is a collection of attributes on a form that uniquely identifies the logical entity on which accounts are created. This term is sometimes loosely referred to as a target. For instance, for an AD server, an account discriminator can be a combination of AD server (an attribute of type IT Resource) and Organization Name.

Typically, account discriminators are attributes of type IT Resource.

Attributes are marked as account discriminators by setting the Account Discriminator property of a Form field to True.

3.2 Features of Access Policies

This section describes the various features offered by the policy engine in the following sections:

- [Provisioning Options](#)
- [Revoking or Disabling the Policy](#)
- [Denying a Resource](#)
- [Evaluating Policies](#)
- [Access Policy Priority](#)
- [Access Policy Data](#)
- [Provisioning Multiple Instances of the Same Resource via Access Policy by Using Account Discriminator](#)

3.2.1 Provisioning Options

Whenever an access policy is applied, provisioning of resources can take place in any one of the following ways:

- The resources are directly provisioned to the user without any request being generated.
- A request is created, and provisioning of resources is subject to request approval.

By using the System Administration Console, you can specify whether you want to create the access policy with request approval or without request approval.

In an access policy with request:

- The default process form for access policy is supported. This means that the data entered for default process form while creating access policy is used to populate request dataset.
- Mandatory fields of request dataset must be populated by one of the following:
 - Process form defaults of access policy while defining access policy: This is because process form access policy defaults are used to populate corresponding request dataset.
 - Prepopulate adapters defined for request dataset.
 - Default data in the request dataset.
- Access policy-based request is not created if all mandatory fields of request dataset are not populated by any one of process form defaults, prepopulate adapters, or default data in request dataset.
- If request has already been created for a user for a specific resource and it is NOT in one of the following status, then new request is not created for the same user and resource combination:
 - Request Closed
 - Request Completed
 - Request Withdrawn
 - Request Failed
 - Template Approval Rejected
 - Request Approval Rejected
 - Operation Approval Rejected

3.2.2 Revoking or Disabling the Policy

Oracle Identity Manager access policies are not applied to subroles. Policies are only applied to direct-membership users (that is, users who are not in subroles) in the roles that are defined on the access policies. You must specify whether a resource in a policy must be revoked or disabled when the policy no longer applies. Based on your selection, the resources are automatically revoked from the users or disabled when the policy no longer applies to the users.

In earlier releases of Oracle Identity Manager, to revoke an account and its entitlements, you had to select the Revoke if no longer applies option in the policy definition. If you left the Revoke if no longer applies option deselected, then no action was performed on the accounts provisioned by the policy. From this release onward,

accounts and entitlements can either be revoked or disabled if policy no longer applies. There is no longer an option to leave any option deselected.

For each resource associated with an access policy, you must select any one of the following options:

- **Revoke if no longer applies:** Selecting this option revokes the account and the entitlements associated with the access policy when the access policy is no longer applicable.
- **Disable if no longer applies:** Selecting this option disables the account and the entitlements associated with the access policy when the access policy is no longer applicable.

Entitlements are always revoked when the policy with the **Revoke if no longer applies** option or **Disable if no longer applies** option enabled no longer applies. When a policy that has the **Disable if no longer applies** option enabled no longer applies, then the entitlements associated with the resource are revoked because the entitlements have been originally granted because of the role grant. The entitlements are added to the resource instance when the role is granted once again.

Note: During an upgrade to Oracle Identity Manager 11g Release 2 (11.1.2.1.0), policies which had the **Revoke if no longer applies** option deselected will be converted to **Disable if no longer applies**. Users associated with these policies will not be updated, but any future updates to the policy will result in the user being marked with a **Disable if no longer applies** flag.

3.2.3 Denying a Resource

While creating an access policy, you can select resources to be denied along with resources to be provisioned for roles. If you first select a resource for provisioning and then select the same resource to be denied, then Oracle Identity Manager removes the resource from the list of resources to be provisioned. If two policies are defined for a role in which one is defined to provision a resource and the other is defined to deny the resource, then Oracle Identity Manager does not provision the resource irrespective of the priority of the policies.

Note: If a resource is denied by an access policy, then the resource is always denied, even if a different policy provisions it. Denying of resources is irrespective of access policy priority. Even if an access policy with lower priority denies a resource, it takes precedence over an access policy with higher priority.

3.2.4 Evaluating Policies

In Oracle Identity Manager, access policies are evaluated during the run of the Evaluate User Policies scheduled job. By default, this task is enabled and scheduled to run every 10 minutes. See "[Predefined Scheduled Tasks](#)" on page 15-7 for more information about the Evaluate User Policies scheduled task.

Access policies can be evaluated in the following scenarios:

- When a user is made a part of a role or removed from a role
The policy for the user is evaluated as part of the add or remove operation.
- If the retrofit flag is set for the policy

The evaluations can happen in the following scenarios:

- Policy definition is updated so that the retrofit flag is set to ON. Policies are evaluated for all applicable users.
- A role is added or removed from the policy definition. Policies are evaluated only for roles that is added or removed.

Note: In 11g Release 2 (11.1.2.1.0), after the role is applicable to the user, you must run the Evaluate User Policies scheduled job to make access policy applicable.

- A resource is added, removed, or the **Revoke If No Longer Applies** or **Disable If No Longer Applies** options are changed for the resource.

When you change the **Revoke if no longer applies** and **Disable if no longer applies** options from one to the other, the existing resource instances are not re-evaluated immediately. This policy change takes effect only the next time the policy is evaluated by the Evaluate User Policies scheduled task.

- When policy data is updated or deleted. This includes both parent and child form data. Policies are evaluated for all applicable users.

3.2.5 Access Policy Priority

Policy priority is a numeric field containing a number that is unique for each access policy you create. The lower the number, the higher is the priority of the access policy. For example, if you specify Priority =1, it means that the policy has the highest priority. When you define access policies through Oracle Identity System Administration, the value 1 is always added to the value of the current lowest priority and the resultant value is automatically populated in the Priority field. Changing this value to a different number might result in readjusting the priority of all the other access policies, thus ensuring that the priorities remain consistent. The following actions are associated with the priority number:

- If the priority number entered is less than 1, then Oracle Identity Manager will change the value to 1 (highest priority).
- If the priority number entered is greater than M, in which M is the current lowest priority, then Oracle Identity Manager will specify the value as less than or equal to M+1.
- Two access policies cannot have the same priority number. Therefore, assigning an already existing priority number to an access policy will lower the priority by 1 for all policies of lesser priority.

Conflicts can arise from multiple access policies being applied to the same user. Because a single instance of a resource is provisioned to the user through access policies, Oracle Identity Manager uses the highest priority policy data for a parent form. For child forms, Oracle Identity Manager uses cumulative records from all applicable policies.

If there is more than one access policy created for the same resource but granting different sets of entitlements and having different behavior when policy no longer applies, then the access policy with **Disable if no longer applies** (DLNA) option enabled has the highest priority irrespective of the access policy priorities. For example, if there is an access policy with **Revoke if no longer applies** (RLNA) option enabled and another policy with DLNA option enabled, then the policy with DLNA

option enabled has higher precedence. Irrespective of the order in which the policies are applied, as long as a policy with DLNA option enabled is applied to the user, the account is always disabled when the policy no longer applies.

If a policy with Disable if no longer applies is later converted to Revoke if no longer applies, then existing accounts that are associated with the policy are not updated to RLNA. The change is effective only for accounts to be created in future.

If a policy with RLNA is later converted to DLNA, then the accounts that are already revoked are not impacted. The change is effective only for accounts currently associated with this policy or accounts to be created in the future.

3.2.6 Access Policy Data

There are multiple ways in which process form data is supplied for resources during provisioning. The following is the order of preference built into Oracle Identity Manager:

1. Default values from the form definition
2. Organization defaults
3. Values obtained through data flow from dataset to process form
4. Prepopulate adapters
5. Access policy data if resource is provisioned because of a policy
6. Data updated by Process Task or Entity Adapters

If a given option is available, then the rest of the options that are at a lower order of preference are overridden. For example, if Option 4 is available, then Options 3, 2, and 1 are ignored.

3.2.7 Provisioning Multiple Instances of the Same Resource via Access Policy by Using Account Discriminator

In earlier releases of Oracle Identity Manager, access policies can be used to manage only a single account for a resource object. In other words, if you already have resource provisioned to user (account has been created in the target system) and if another instance of the same resource is to be provisioned to the same user via access policy, then it is not possible in earlier releases of Oracle Identity Manager. To achieve the functionality of provisioning multiple instances of resource to a user, prior to access policy enhancement in Oracle Identity Manager 11g Release 2 (11.1.2.1.0), you must clone the connector that represents the target system in Oracle Identity Manager. Cloning of connector was error prone needed lot of effort for testing/maintenance of cloned resource. Access Policy enhancement done for provisioning of multiple instances of resource in Oracle Identity Manager 11g Release 2 (11.1.2.1.0) saves the time and effort on cloning connectors.

A target system, such as UNIX server, Active Directory (AD) server, database, SAP, or JD Edwards, is the external system to Oracle Identity Manager that must be provisioned to users in Oracle Identity Manager. The target system is represented by an entity called resource in Oracle Identity Manager. The server on which target system is installed is represented by IT resource in Oracle Identity Manager. And the login credentials provided to user accessing this target system is represented by an account in Oracle Identity Manager. A user can have multiple accounts on a single target system. For example, one account can be a service (administrator) account and another a regular account. Therefore, it is mandatory to have two accounts for a same user in a single target system. In addition, it is possible to have different instances of

target system, such as multiple UNIX servers, database servers, and AD servers. As a result, it is required to create accounts on each instance of the target system for the same user. For implementation details, see "[Creating Separate Accounts for the Same User and Same Resource on a Single Target System](#)" on page 3-11.

In Oracle Identity Manager 11g Release 2 (11.1.2.1.0), access policies can provision multiple accounts in the same target system as well as a single account in multiple instance of the same target system. While evaluating access policies and provisioning resources to user, Oracle Identity Manager checks if the resource has already been provisioned to the user or not. This is determined by checking the resource key (OBJ_KEY) of the resource provisioned to user. To have multiple instances to be provisioned through access policy, another criteria called *account discriminator* along with OBJ_KEY is required to distinguish the multiple instances of the same resource. Therefore, access policy checks the resource key as well as account discriminator to decide if the resource has been provisioned or not.

The account discriminator is a field on a process form (account data) that distinguishes two accounts of the same user, which can be present on the same target system or different target systems. For example:

- If user Jane.Doe is to be provisioned two accounts on two different UNIX servers, then IT resource can be used as account discriminator.
- If user John.Doe is to be provisioned two accounts on the same database instance, then distinct login IDs can be used as account discriminator.

If there are multiple resources that need to be provisioned because of access policy evaluation, a single bulk request is created. The bulk request requires a single request-level approval, but multiple operation-level approvals for which approver can approve each request individually at operation level.

See Also:

- "Approval Levels" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about various levels of request approval
- "[Provisioning Multiple Instances of the Same Resource via Access Policy](#)" on page 3-10 for the steps to provision data from multiple target systems

3.3 Creating Access Policies

You can define an access policy for provisioning resources to users who have roles defined in the policy by using the Access Policy Wizard.

To create an access policy:

1. Login to the Oracle Identity System Administration, and go to Advanced Administration.
2. To open the Create Access Policies page, under Policies, click **Create Access Policy**.
3. Enter information in the required fields indicated with an asterisk (*), such as access policy name and description.

Note: The following special characters are not allowed in the access policy name:

Semicolon (;)

Hash (#)

Percentage (%)

Equal to (=)

Bar (|)

Plus (+)

Comma (,)

Forward slash (/)

Back slash (\)

Single quote (')

Double quote (")

Less than (<)

Greater than (>)

4. For the Provision field, select any one of the following options:
 - **Without Approval:** Selecting this option creates the access policy without request approval. The resources are directly provisioned to the user without any request being generated.
 - **With Approval:** Selecting this option creates the access policy with request approval. When an access policy become applicable, a request is created, and provisioning of resources is subject to request approval.
5. Select **Retrofit Access Policy** to retrofit this access policy when it is created.

Note: If you select Retrofit Access Policy, then the access policy is applied to all existing roles that you select in Step 13 of this procedure, after the Evaluate User Policies job is run.

If you do not select this option, then existing role memberships are not taken into consideration.

6. Click **Continue**.

The Create Access Policy - Step 2: Select Resources (to provision) page is displayed.
7. Specify the resource to be provisioned for this access policy.

Search for resources by using the filter search menu.

 - Select the name of the resource from the results table, and then click **Add**.
 - The names of the desired resources to provision appear in the Selected list. If you want to create an access policy that only denies resources, click **Continue** without selecting a resource.

- To unassign the selected resources, highlight the resource in the Selected list and click **Remove**.

8. Click *Continue*.

If there is a form associated with this resource, the subsequent pages display the required fields. Otherwise, the Create Access Policy - Step 2: Select Resources to Revoke or Disable page is displayed.

Note: Oracle recommends that you do not specify policy defaults for passwords and encrypted attributes.

9. For each resource listed in the page, select any one of the following options:

- **Revoke if no longer applies:** Selecting this option revokes the account and the entitlements associated with the access policy when the access policy is no longer applicable.
- **Disable if no longer applies:** Selecting this option disables the account and the entitlements associated with the access policy when the access policy is no longer applicable.

See "[Revoking or Disabling the Policy](#)" on page 3-3 and "[Evaluating Policies](#)" on page 3-4 for more information about revoking or disabling accounts and entitlements when access policies no longer apply.

10. Click *Continue*.

The Create Access Policy - Step 3: Selected Resources (to deny) page is displayed.

11. Use this page to select resources to be denied by this access policy.

To select resources to be denied:

- a. Select the resources from the results table.
- b. Click **Add** to place the resource in the Selected list.

You must select at least one resource to deny if you have not selected any resources to be provisioned. Selecting the same resources to be denied as to be provisioned will automatically unassign them from the resources to be provisioned selection.

Similarly, in Step a, assigning the same resources to be provisioned as you have already selected to be denied will automatically remove them from the resources to be denied selection. You can remove the resources that were selected to be denied. You do this by selecting those resources from the **Selected** list, and clicking **Remove**.

- c. Click **Continue**.

The Create Access Policy - Step 4: Select Roles page is displayed.

12. Use the Create Access Policy - Step 4: Select Group page to associate a group with the access policy.

13. To associate a role with this access policy:

- Select the role from the results table, and then click **Add**. You must select at least one role. The names of the selected roles appear in the Selected list.
- You can delete the role name by clicking **Remove**.

14. Click *Continue*.

The Create Access Policy - Step 5: Verify Access Policy Information page is displayed.

15. If you want to modify any of the selections you made in the preceding steps of this procedure, then click **Change** to go to the corresponding page of the wizard. After making the required modifications, click **Continue** to return to the Step 5: Verify Access Policy Information page.
16. Click **Create Access Policy** to create the access policy.

Note: When you create an access policy on a resource having a process form with Password field, the password policy is not evaluated. For information about password policies, see *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

3.4 Managing Access Policies

You can use Oracle Identity System Administration to modify information in existing access policies.

To manage access policies:

1. In the Advanced Administration, click **Manage Access Policies** under the Policies menu.

The Manage Access Policies page is displayed.

Use the menu in the search criteria field to select an access policy attribute. You can use the asterisk (*) wildcard character to search for all access policy instances that have any value for the attribute selected. Click **Search Access Policies**.

The Manage Access Policies page is displayed with your search results.

2. To view the details of the Access Policy you want, click **Access Policy Name**.

The Access Policy Details page is displayed.

To make modifications to this access policy, use the **Change** link at the end of each selection category.

Note: You can change the **Revoke if no longer applies** and **Disable if no longer applies** options as a part of the access policy modification. See "[Revoking or Disabling the Policy](#)" on page 3-3 and "[Evaluating Policies](#)" on page 3-4 for information about the effects of changing these options in access policies.

3. After you make the required modifications, click **Update Access Policy**.

This access policy is updated, and the updated information is displayed on the Access Policy Details page.

3.5 Provisioning Multiple Instances of the Same Resource via Access Policy

Provisioning multiple instances of the same resource via access policy by using account discriminator involves the following:

- [Creating Separate Accounts for the Same User and Same Resource on a Single Target System](#)
- [Enabling Multiple Account Provisioning](#)
- [Provisioning Multiple Instances of a Resource to Multiple Target Systems](#)
- [Limitation of Provisioning Multiple Instances of a Resource via Access Policy](#)

3.5.1 Creating Separate Accounts for the Same User and Same Resource on a Single Target System

Two distinct accounts can be created for the same user and same resource on a single target system via access policy. For example, it is required to create two accounts, a user account and service account on a single AD instance. The Active Directory target system is represented by the AD User resource in Oracle Identity Manager. This is implemented in the following way:

1. Create a AD User resource.
2. Create the user, such as JohnD.
3. In the process form, mark UD_ADUSER and UD_ADUSER_UID as the discriminator field so that two distinct accounts have different login IDs.
4. Create two access policies as follows:
 - **For regular account:**

Access policy name: AP1

Associated to role: Role1

Resource to provision: AD User

Process form having Discriminator field: User ID (UD_ADUSER_UID)

Default value in access policy: Account1
 - **For service account:**

Access policy name: AP2

Associated to role: Role2

Resource to provision: AD User

Process form having Discriminator field: User ID (UD_ADUSER_UID)

Default value in access policy: Account2

Note: You must create a prepopulate adapter associated with dataset to generate the values for User ID so that unique values are generated for this field.

5. Assign Role1 and Role2 to JohnD. Note that you will not see the resource provisioned right after completion of role assignment. You must either wait for the Evaluate User Policies scheduled task to run automatically or you run this scheduled task manually.

When Role1 is assigned to JohnD, the Account1 account is created in the AD User target system via the AP1 access policy. When Role2 is assigned to JohnD, Account2 is created in AD User via AP2. Therefore, two distinct accounts can be

created for the same user and same resource on a single target system via access policy.

3.5.2 Enabling Multiple Account Provisioning

By default, Oracle Identity Manager does not support multiple account provisioning. To enable multiple account provisioning:

Set the value of the `XL.AllowAPBasedMultipleAccountProvisioning` system property to `TRUE`. See ["System Properties in Oracle Identity Manager"](#) on page 16-1 for information about this system property. See ["Creating and Managing System Properties"](#) on page 16-22 for information about setting the value of a system property.

When multiple account provisioning is enabled, you must define the appropriate account discriminator attributes. To do so:

1. Log in to the Design Console.
2. Update the process form as follows:
 - a. Expand Development Tools, and then double-click **Form Designer**.
 - b. Search and open the process form.
 - c. On the Form Designer tab, click **Create New Version**.
 - d. In the Create a New Version dialog box, enter a label in the Label field, and then click **Save**.
 - e. From the Current Version list, select the version that you created.
 - f. On the Properties tab, select the field that you want to designate as the discriminator field, and then click **Add Property**.
 - g. In the Add Property dialog box, select **Account Discriminator** as the property name, enter `True` in the Property Value field, and then click **Save**.
 - h. Click **Make Version Active**, and then click **OK**.
 - i. Click **Save**.
3. Run the Form Version Control (FVC) utility if you modified existing process forms. See ["Using the Form Version Control Utility"](#) for information about running the FVC utility.

3.5.3 Provisioning Multiple Instances of a Resource to Multiple Target Systems

The following are the broad-level steps to provision multiple instances of a resource object to multiple target systems via access policy:

1. Create an IT resource type by using the IT Resources Type Definition Form in the Oracle Identity Manager Design Console. For information about using this form, see ["IT Resources Type Definition Form"](#) in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
2. Create multiple IT resource instances of the IT resource type that you created in step 1. For information about creating IT resources, see ["Creating IT Resources"](#) in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Here, IT resource instance is the account discriminator. See ["Provisioning Multiple Instances of the Same Resource via Access Policy by Using Account Discriminator"](#) on page 3-6 for information about account discriminator.

Note: Display the process form default for ITResource. It is mandatory to display it. By doing so, you can successfully provision an application instance via access policy.

3. Create a process form with a field of type that you created in step 1. For information about creating process forms, see "Developing Process Forms" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
4. Create a resource object. For information about creating a resource object, see "Creating a Resource Object" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
5. Create a process definition, and associate the resource object and process form. For information about creating a process definition, see "Creating a Process Definition" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
6. Create access policies associating a role and resource object. See "[Creating Access Policies](#)" on page 3-7 for details.

When you have two instances of the same resource on different physical server, you can use access policy to provision both the instances of a resource to the same user, JohnD. This is described with the help of the following scenario:

You have two AD instances, one hosted on server with IP as 10.151.14.82 and another hosted on server with IP 130.35.66.254. The user is to be provisioned to both the instances via access policy-based provisioning. To achieve this:

1. Create a AD User resource.
2. Create an IT resource with name ADServer1 that represents the server with IP address as 10.151.14.82.
3. Create an IT resource with name ADServer2 that represents the server with IP address as 130.35.66.254.
4. Mark the AD Server (UD_ADUSER_AD) process form field as the discriminator field.
5. Create two access policies as follows:
 - **For the account to be created on ADServer1:**
 - Access policy name: AP3
 - Associated to role: Role3
 - Resource to provision: AD User
 - Process form having Discriminator field: AD Server (UD_ADUSER_AD)
 - Default value for ITResourceLookup field: ADServer1
 - **For the account to be created on ADServer2:**
 - Access policy name: AP4
 - Associated to role: Role4
 - Resource to provision: AD User
 - Process form having Discriminator field: AD Server (UD_ADUSER_AD)
 - Default value for ITResourceLookup field: ADServer2
6. Assign Role3 and Role4 to the user JohnD.

When Role3 is assigned to JohnD, the account is created in the target system on ADServer1 via the AP3 access policy. When Role4 is assigned to JohnD, the account is created in the target system on ADServer2 via the AP4 access policy. Therefore, two distinct accounts are created for the same user and same resource on two different instances of the target system via access policy.

3.5.4 Limitation of Provisioning Multiple Instances of a Resource via Access Policy

Provisioning multiple instances of a resource via access policy has the following limitations:

- A single access policy cannot provision multiple instances of a resource to a user. Multiple access policies must be created to provision multiple instances of resource. You must create the same number of access policies as that of instances of same resource that is to be provisioned.
- If a resource object has a process form that has fields marked as account discriminator fields, then the value of these fields must be specified in any access policy that provisions that resource. Not doing this can result in behavior that cannot be determined, for example, provisioning of multiple accounts the next time policies are evaluated.
- If a resource object has a process form that has fields marked as account discriminator fields and if you use the access policy engine to provision this resource to one or more users, then the values of the account discriminator fields must remain constant throughout the lifecycle of the account. In other words, the values of the account discriminator fields must not be changed. This is because the access policy engine uses the resource object key and the account discriminator values to decide whether or not to provision a new account to the user.

By modifying account discriminator values, you modify the basis on which the provisioning decision had been taken. and the behavior of the access policy engine cannot be determined. Therefore, it is recommended that you do not modify account discriminator values. And the process form values of the account discriminator fields must not be changed.

- If access policies are configured with different account discriminator values, they provision different accounts to the user. A resource object of this type must have the Allow Multiple flag set. Otherwise, provisioning fails.

Note: Account discriminator values that are different only in casing (for example, abc and aBc) are also treated as different values. With this data, two accounts are provisioned to the end user.

Consider the following scenario:

Two access policies are provisioning the same resource with the same account discriminator data. The policies are applied through a request.

These two policies apply to a user, and policies are re-evaluated for the user. Here, only one resource is provisioned to the user through a request. Now, suppose request approval is in progress. In the meantime, the priorities of these two policies are swapped, which means that the higher priority policy becomes the lower one and the other becomes the higher priority policy.

While the request is in progress, if policies are re-evaluated for the user, a second request is created to provision the same resource but through the current higher priority policy. This issue is not currently handled by the policy engine. To avoid this issue, you must ensure that all pending requests for a specific resource are either approved or rejected before modifying the properties of the access policy that provision the resource, especially through a request.

Managing Password Policies

Organization administrators can associate a password policy to an organization. All password policies are created by System Administrators only. The organization administrators can select a relevant password policy from the password policies created by system administrators. A password policy set for an organization is applicable for that organization and all its suborganizations. If the suborganization-level administrator sets a different password policy for that organization, then the parent organization password policy is overridden by the new one, and is applicable to all suborganizations under this organization.

Password policy priority determines which password policy is applicable for a user if the user is a member of multiple organizations. If the organizations are in hierarchy, then the password policy of the organization that is closest to the user is applicable even if the password policy associated with the parent organization has higher priority.

During user creation, Oracle Identity Manager validates the password provided manually or autogenerated against the default password policy which is attached to the Top organization. When a user logs in for the first time and changes the password, the password policy with the highest priority that is applicable to the user's organization is applied.

This chapter describes password policy management in the following sections:

- [Searching Password Policies](#)
- [Creating a Password Policy](#)
- [Setting Password Policy Rules](#)
- [Deleting a Password Policy](#)

4.1 Searching Password Policies

To search for password policies:

1. Login to Oracle Identity System Administration.
2. In the left pane, under Policies, click **Password Policy**. The Password Policy page is displayed.
3. For the Policy Name field, select a search operator from the list.
4. In the Policy Name field, enter the policy name you want to search. If you want to list all existing password policies, then leave this field blank.

5. Click **Search**. The password policies that match your search condition are displayed.

4.2 Creating a Password Policy

By creating password policies, you can:

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

Note: In an environment in which LDAP synchronization is enabled, you must ensure one of the following:

- Password policies set on Oracle Identity Manager must be more restrictive than password policies set on the LDAP server.
 - Password policies set on Oracle Identity Manager must match the password policies set on the LDAP server.
-
-

To create a password policy:

1. In the Password Policy page, from the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Password Policy page is displayed, as shown in [Figure 4-1](#):

Figure 4–1 The Create Password Policy Page

2. In the Policy Name field, enter the name of the password policy.
3. In the Policy Description field, enter a short description of the password policy.
4. In the Policy Rules tab, specify value in the fields to set the rules for the password policy. For a description of each field in the Policy Rules tab, see ["Setting Password Policy Rules"](#) on page 4-3.

Note: You can leave the fields blank in the Policy Rules tab, and click **Apply** to save the password policy. You can later open the password policy and set the policy rules by following the instructions in ["Setting Password Policy Rules"](#) on page 4-3.

5. Click **Apply**.

Note: A password policy is not applied during the creation of an Oracle Identity Manager user through trusted source reconciliation.

4.3 Setting Password Policy Rules

Setting password policy rules involve specifying criteria for your password policy, for example, the minimum and maximum length of passwords.

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

- Enter information in the appropriate fields, or select the required check boxes. For example, to indicate that a password must have a minimum length of four characters, enter **4** in the Minimum Length field.
- In the Password File field, enter the directory path and name of the password policy file (for example, c:\Xellerate\userlimits.txt). This file contains predefined words that you do not want to be used as passwords. The delimiter specified in the File Delimiter field separates these words. The predefined words in the file cannot be used as passwords. For example, if the file contains the word welcome, then welcome, Welcome, and welcome123 are invalid passwords.

To set the rules for a password policy:

1. In the Password Policy page, search and select the password policy that you want to open.
2. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar. The password policy details page is displayed.

Note: You can also set the password policy rules at the time of creating the password policy.

3. In the Policy Rules section, enter values in the fields, as listed in [Table 4-1](#):

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

Table 4-1 Fields in the Policy Rules Section

Field Name	Description
Minimum Length	<p>The minimum number of characters that a password must contain for the password to be valid.</p> <p>For example, if you enter 4 in the Minimum Length field, then the password must contain at least four characters.</p> <p>This field accepts values from 0 to 999.</p>
Minimum Password Age (Days)	<p>The minimum duration in days for which users can use a password.</p> <p>For example, if you enter 2 in the Minimum Password Age (Days) field, then the user cannot change the password before 2 days of creating the password.</p> <p>The value of this field must be less than the value of the Expires After (Days) field. For example, if you enter 30 in the Expires After (Days) field and 31 in the Minimum Password Age (Days) field, then an error is displayed.</p>
Warn After (Days)	<p>The number of days that must pass before a user is notified that the user's password will expire on a designated date.</p> <p>For example, you enter 30 in the Expires After (Days) field, and 20 in the Warn After (Days) field, and the password is created on November 1. On November 21, the user will be informed that the password will expire on December 1.</p> <p>This field accepts values from 0 to 999.</p>

Table 4–1 (Cont.) Fields in the Policy Rules Section

Field Name	Description
Disallow Last Passwords	<p>The frequency at which old passwords can be reused. This policy ensures that users do not change back and forth among a set of common passwords.</p> <p>For example, if you enter 10 in the Disallow Last Passwords field, then users are allowed to reuse a password only after using 10 unique passwords.</p> <p>This field accepts values from 0 to 24.</p>
Expires After (Days)	<p>The maximum duration in days for which users can use a password.</p> <p>For example, if you enter 30 in the Expires After Days field, then users must change their passwords by the thirtieth day from when it was created or last modified.</p> <p>This field accepts values from 0 to 999.</p> <p>Note: After the number of days specified in the Expires After Days field passes, a message is displayed asking the user to change the password.</p>

4. Select any one of the following options:

Note: You can configure either a default complex password policy or a custom password policy. If you select the **Complex Password** option, then you cannot use the Custom Policy option setup, and passwords will be evaluated against the complex password criteria.

- **Complex Password:** Selecting this option sets the following complex password criteria:
 - The password is at least six characters long. This password length overrides the Minimum Length field if the value entered in the Minimum Length field is less than 6. For example, if you enter 2 in the Minimum Length field, at least six characters will be required for the password because it must have at least six characters according to the complex password criteria.
 - The password contains characters from at least three of the following five categories:
 - English Uppercase Characters (A - Z)
 - English Lowercase Characters (a - z)
 - Base 10 digits (0 - 9)
 - Non-alphanumeric characters (for example: !, \$, #, or %)
 - Unicode characters
 - The password does not contain any of User ID, first name, or last name when their length is larger than 2.

The names are parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, then the names are split and all sections are verified not to be included in the password. For example, if the user name is john-d, then d will not be checked in the password because its length is less than 2. Simi-

larly, if the name is John Richard Doe, then the password cannot contain john, richard, or doe.

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

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

- **Custom Policy:** If you select the **Custom Policy** option, you can set a custom password policy by using the fields listed in [Table 4-2](#).

Table 4-2 *Fields in Custom Policy Section*

Field Name	Description
Maximum Length	The maximum number of characters that a password can contain. For example, if you enter 8 in the Maximum Length field, then a password is not accepted if it has more than eight characters. This field accepts values from 1 to 999.
Maximum Repeated Characters	The maximum number of times a character can be repeated in a password. For example, if you enter 2 in the Maximum Repeated Characters field, then a password is not accepted if any character is repeated more than two times. For example, RL112211 would not be a valid password because the character 1 is repeated three times. Note: In this example, there are four occurrences of the character 1, which means that it is repeated three times. This field accepts values from 1 to 999.
Minimum Numeric Characters	The minimum number of digits that a password must contain. For example, if you enter 1 in the Minimum Numeric Characters field, then a password must contain at least one digit. This field accepts values from 0 to 999.
Minimum Alphanumeric Characters	The minimum number of letters or digits that a password must contain. For example, if you enter 6 in the Minimum Alphanumeric Characters field, then a password must contain at least six letters or numbers. This field accepts values from 0 to 999.

Table 4–2 (Cont.) Fields in Custom Policy Section

Field Name	Description
Minimum Unique Characters	<p>The minimum number of nonrepeating characters that a password must contain.</p> <p>For example, if you enter 1 in the Minimum Unique Characters field, then a password is accepted if at least one character in the password is not repeated. For example, 1a23321 would be a valid password because the character a in the password is not repeated although the remaining characters are repeated.</p> <p>This field accepts values from 0 to 999.</p>
Minimum Alphabet Characters	<p>The minimum number of letters that a password must contain.</p> <p>For example, if you enter 2 in the Minimum Alphabet Characters field, then the password is not accepted if it has less than two letters.</p> <p>This field accepts values from 0 to 999.</p>
Special Characters: Minimum	<p>The minimum number of non-alphanumeric characters (for example, #, %, or &) that a password must contain.</p> <p>For example, if you enter 1 in the Special Characters: Minimum field, then a password must have at least one non-alphanumeric character.</p> <p>This field accepts values from 0 to 999.</p>
Special Characters: Maximum	<p>The maximum number of non-alphanumeric characters that a password can contain.</p> <p>For example, if you enter 3 in the Special Characters: Maximum field, then a password is not accepted if it contains more than three non-alphanumeric characters.</p> <p>This field accepts values from 1 to 999.</p>
Minimum Uppercase Characters	<p>The minimum number of uppercase letters that a password must contain.</p> <p>For example, if you enter 8 in the Uppercase Characters: Minimum field, then a password is not accepted if it contains less than eight uppercase letters.</p> <p>This field accepts values from 0 to 999.</p>
Minimum Lowercase Characters	<p>The minimum number of lowercase letters that a password must contain.</p> <p>For example, if you enter 8 in the Minimum Lowercase Characters field, then a password is not accepted if it has less than eight lowercase letters.</p> <p>This field accepts values from 0 to 999.</p>
Characters Required	<p>The characters that a password must contain.</p> <p>For example, if you enter x in the Characters Required field, then a password is accepted only if it contains the character x.</p> <p>The character you specify in the Characters Required field, must be mentioned in the Characters Allowed field. If you enter a character in the Characters Required field that is not mentioned in the Characters Allowed field, then an error is displayed stating that the required characters must be in the list of allowed characters, and required characters must not be in the list of not allowed characters.</p> <p>In addition, if you specify more than one character, then do not provide delimiters. Commas and white spaces are also considered as characters in this field. For example, if you specify characters such as a,x,c, then the password is not accepted unless it contains comma.</p>

Table 4–2 (Cont.) Fields in Custom Policy Section

Field Name	Description
Characters Allowed	<p>The characters that a password can contain.</p> <p>For example, if you enter the percent sign (%) in the Characters Allowed field, then a password is accepted if it contains a percent sign, given that all other criteria are met.</p> <p>Note: If any character is used in the password and that character is not in the Characters Allowed field, then the password will be rejected. For example, if the Characters Allowed field has "abc" and the password is "dad", then the password is rejected because "d" is not in the Characters Allowed field.</p> <p>If you specify the same character in the Characters Allowed and Characters Not Allowed fields, then an error message is returned when you create the password policy.</p>
Characters Not Allowed	<p>The characters that a password must not contain.</p> <p>For example, if you enter an exclamation point (!) in the Characters Not Allowed field, then a password is not accepted if it contains an exclamation point.</p>
Substrings Not Allowed	<p>A series of consecutive alphanumeric characters that a password must not contain.</p> <p>For example, if you enter IBM in the Substrings Not Allowed field, then a password is not accepted if it contains the letters I, B, and M, in successive order.</p>
Special Characters: Min	<p>The minimum number of special characters that a password must contain.</p> <p>For example, if you enter 2 in the Special Characters: Min field, then the password is not accepted if it has less than two special characters.</p> <p>The field accepts values from 0 to 999.</p>
Special Characters: Max	<p>The maximum number of special characters that a password can contain.</p> <p>For example, if you enter 5 in the Special Characters: Max field, then a password is not accepted if it has more than five special characters.</p> <p>This field accepts values from 1 to 999.</p>
Unicode Characters: Min	<p>The minimum number of Unicode characters that a password must contain.</p> <p>For example, if you enter 3 in the Unicode Characters: Minimum field, then the password is not accepted if it has less than three Unicode characters.</p> <p>This field accepts values from 0 to 999.</p>
Unicode Characters: Max	<p>The maximum number of Unicode characters that a password can contain.</p> <p>For example, if you enter 8 in the Unicode Characters: Maximum field, then a password is not accepted if it has more than eight Unicode characters.</p> <p>This field accepts values from 1 to 999.</p>
Start With Alphabet	<p>Whether or not the password must begin with a letter.</p> <p>For example, if you select this option, then the password 123welcome is not accepted because the password does not begin with a letter. However, if you do not select this option, then the password can begin with a letter, numeric digit, or special character.</p>

Table 4–2 (Cont.) Fields in Custom Policy Section

Field Name	Description
Disallow User ID	<p>This check box specifies if the user ID will be accepted as the whole password or as part of the password.</p> <p>When this check box is selected, a password will not be valid if the user ID is entered in the Password field. In addition, the password is not valid if the user ID occurs as a part of the password specified in the Password field.</p> <p>If you deselect this check box, the password will be accepted, even if it contains the user ID.</p>
Disallow First Name	<p>This check box specifies if the user's first name will be accepted as the whole password or as part of the password.</p> <p>When this check box is selected, a password will not be valid if the user's first name is entered in the Password field. In addition, the password is not valid if the first name is entered as a part of the password.</p> <p>If you deselect this check box, then the password will be accepted, even if it contains the user's first name.</p>
Disallow Last Name	<p>This check box specifies if the user's last name will be accepted as the whole password or as part of the password.</p> <p>When this check box is selected, a password will not be valid if the user's last name is entered in the Password field. In addition, the password is not valid if the last name is entered as a part of the password.</p> <p>If you deselect this check box, then the password is accepted, even if it contains the user's last name.</p>
Password File	<p>The path and name of a file that contains predefined terms, which are not allowed as passwords. The file must be stored on the same host on which Oracle Identity Manager is deployed.</p> <p>Note: The settings on the Policy Rules tab get precedence over the specifications in the password file. For example, a disallowed term of the password file is used in the policy when no disallowed term is specified in the Policy Rules tab.</p>
Password File Delimiter	<p>The delimiter character used to separate terms in the password file.</p> <p>For example, if a comma (,) is entered in the Password File Delimiter field, then the terms in the password file will be separated by commas.</p> <p>Note: There are no escape characters defined to be used in password policies.</p>

5. Click **Apply** to save the password policy.

Note: After creating a password policy, you must associate the policy with an organization. The rules of the policy will be applied for the users of that organization and its suborganizations. For information about associating password policies to organizations, see "Creating an Organization" in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

4.4 Deleting a Password Policy

To delete a password policy:

1. In the Password Policy page, search and select a password policy that 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 deletion.

Managing Attestation Processes

This chapter is divided into the following sections:

- [About Attestation](#)
- [Attestation Process Configuration](#)
- [Creating Attestation Processes](#)
- [Managing Attestation Processes](#)
- [Using the Attestation Dashboard](#)

5.1 About 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. 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**.

In Oracle Identity Manager, attestation is supported through the definition of scheduled attestation processes. An attestation process is not the same as an Oracle Identity Manager workflow. It is implemented as a configurable business process in Oracle Identity Manager, and it creates an attestation task for a user. The user acts as a reviewer, and must complete this process to provide correct audit information.

Tracking of attestation activity for a provisioned resource instance is done through tasks in the provisioning processes of resource objects. You can initiate workflow activity based on attestation actions. Additional activities to be started, and a workflow that can be modeled in the process definition form or workflow designer can be initiated, based on an initial attestation action. This is possible due to attestation subflows in the provisioning processes defined in Oracle Identity Manager.

Attestation activity can be initiated on a periodic basis or when required.

A reviewer can delegate specific entitlements in an attestation task to another user for review. This action creates another attestation task that is assigned to the delegated user.

This section discusses the following topics:

- [Definition of an Attestation Process](#)
- [Components of Attestation Tasks](#)

- [Attestation Request](#)
- [Delegation](#)
- [Attestation Lifecycle Process](#)
- [Attestation Engine](#)
- [Attestation Scheduled Task](#)
- [Attestation-Driven Workflow Capability](#)
- [Attestation E-Mail](#)

5.1.1 Definition of an 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. This definition is also the basis on which the attestation task can be initiated when required. An attestation process definition includes:

- **User Scope or Resource Scope:** This defines the algorithm by which the target user entitlements of the attestation process are determined.
- **Reviewer Setup:** This specifies the reviewer, who attests the entitlements of other users. An attestation process can specify a particular user as the reviewer, or can specify more abstractly how to select the reviewer. For example, the reviewer can be specified as the user's manager, as an administrator of the resource, as an authorizer of access to the resource, or as a member of the role that grants the entitlement.
- **Definition of Attestation Schedule:** This specifies the schedule for running the attestation process.
- **Process Owner:** This is a designated group of users that are responsible for monitoring activities related to the process.
 - They will be notified of any issues that occur when the process runs.
 - They will have permissions to view the process definition, but will not have administrative permissions by default.
 - They will be able to execute the process whenever required.

A single attestation process could result in multiple attestation tasks, if that process defines a set of reviewers. In such a case, the process would result in one attestation task for each reviewer in the set.

5.1.1.1 Attestation Process Control

The following sections describe how you can control attestation processes.

5.1.1.1.1 Disabling Processes An attestation process can be disabled by the system administrator to prevent it from running at its preconfigured schedule. This gives an administrator better control over the environment. A system administrator attestation process can be enabled, but it cannot be enabled if its Next Run Time value is in the past. A user who enables an attestation process must set its next run time in the future.

5.1.1.1.2 Deleting Processes An attestation process can be deleted. This is called a soft-delete. It does not actually delete the records because the records must be

maintained for audit purposes. Instead, the attestation process will be marked as deleted.

A deleted process is not displayed in Oracle Identity System Administration. Because process names and codes are unique, a name once used is no longer available, and no new attestation process can be created with the same name.

5.1.2 Components of Attestation Tasks

The basic purpose of the attestation process is to set up an attestation task in Oracle Identity Manager. The attestation task is displayed in the Attestation tab of the TaskList in the Oracle Identity Manager Self Service, where you can manage this task or delegate it to someone else to manage. The following are the basic components of an attestation task:

- **Reviewer:** This specifies the user who performs the attestation.
- **Task Source:** This specifies whether or not the attestation task is a result of a process or because of delegation by another reviewer. In the case of delegation, the task must track the reviewer who delegated the task, and which task is the source of the entitlements.
- **Attestation Data:** This is detailed data about user entitlements in the attestation scope. This data is from the process form of the provisioned resource instance.
- **Attestation Date:** This defines the date on which the attestation task is initiated.
- **Attestation Actions:** These are the actions that the reviewer can take on the attestation scope. The action is not at the level of attestation task overall, but rather against each entitlement in the attestation scope. The following are attestation actions:
 - **Certify:** The reviewer agrees that the user being reviewed is allowed to have the entitlement in its current form, including any specific data or fine-grained permissions.
 - **Reject:** The reviewer does not think that the user must have this entitlement in the form.
 - **Decline:** The reviewer does not want to accept the responsibility of attesting to the entitlement. This action is usually for cases in which processes have been configured incorrectly, and is useful in the early stages of a rollout.

A reviewer declines a task when the reviewer wants someone else to act upon the task. When a task is declined, it gets assigned to a random user in the System Administrator role.
 - **Delegate:** The reviewer wants to reassign the attestation of this entitlement to another qualified person.

Note: The attestation tasks are not workflow tasks in Oracle Identity Manager definition. They are not created as part of workflow. Attestation tasks do not support all the task management features that the workflow engine supports such as dynamic assignment, escalation, and proxy management.

5.1.2.1 Attestation Inbox

From the Attestation tab of the TaskList in the Self Service, a reviewer can view the details of each attestation task. Within an attestation task, the reviewer can provide responses or comments for individual entitlements.

5.1.3 Attestation Request

When an attestation process is executed, an attestation request is created and recorded in Oracle Identity Manager database. This request records for audit purposes, when an attestation process is executed. The attestation request record consists of basic identity and audit data and statistical data that is used in reports. The data includes the following items:

- A request ID: Each attestation request has a unique identifier. Each attestation task that Oracle Identity Manager creates as a result of a request, stores as part of its record, the request ID of the associated attestation request.
- Date and time of execution of the process.
- Date and time of completion of the process: The date and time of completion of the process is considered to be the date and time for that request.
- Total number of entitlements identified for attestation.

The number of provisioned resources that matched the selection criteria (of the resource scope of the attestation process) during this particular execution of the attestation process.

- Number of entitlements certified.
- Number of entitlements rejected.
- Number of entitlements declined.

5.1.4 Delegation

The reviewer who is assigned to an attestation task may not be able to attest to all the entitlements in the task. There may be multiple reasons for this. For example:

- There may be too many entitlements covering too many users in the attestation task
- The reviewer is not sure about the reasons for which the entitlements were provisioned

In these cases, the reviewer may want to involve other people in the review. A reviewer can delegate attestation of certain entitlements in the task.

To delegate attestation, the reviewer selects a set of entitlements in the task and delegates them to another user. This creates a new attestation task that is assigned to the selected reviewer.

The new task contains only those entitlements that the original reviewer selected. The original reviewer is no longer responsible for providing an attestation response for those entitlements. The new attestation task assigned to the delegate would track who performed the delegation, which task it was created from, and some other information, for example, the request ID. The new attestation task is treated in the same manner as any other attestation task. It can even be delegated. [Figure 5–1](#) shows delegate attestation page.

Figure 5–1 Delegate Attestation

Attestation Request >> Save Actions

Process: AD Process

Request Time: August 13, 2010 10:35:36 AM IST

Designate a reviewer for delegated items and enter optional notes for all.
Use the default feature at bottom of the page for bulk action.

User	Resource	Reviewer Action	Delegated Reviewer	Comments
james.hopes [JAMES HOPES]	AD User	Delegate	<input type="text"/> Clear	<input type="text"/>
thomas.muller [THOMAS MULLER]	AD User	Delegate	<input type="text"/> Clear	<input type="text"/>

Default Comment (to be used when no comments are provided):

Default Delegated Reviewer (to be used when no comments are provided): Clear

Back Save Actions

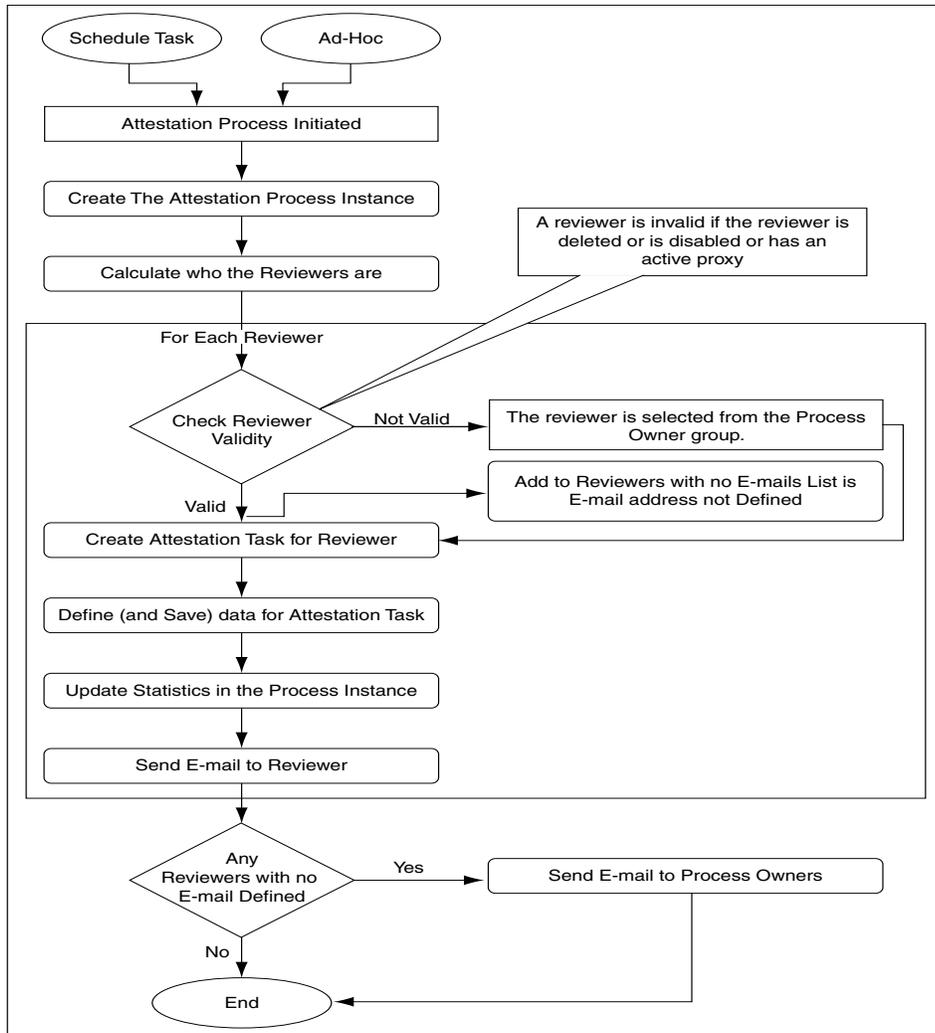
5.1.5 Attestation Lifecycle Process

The following is a description of the attestation lifecycle in Oracle Identity Manager.

5.1.5.1 Stage 1: Creation of an Attestation Task

This stage starts when an attestation process is run. [Figure 5–2](#) describes the workflow involved in this stage.

Figure 5–2 Creating an Attestation Task: Workflow



When the attestation process is run, it first creates a corresponding attestation process instance. It then identifies the reviewers for this run of the process. In most cases, there is only one reviewer. There can even be a set of reviewers.

Whenever an invalid reviewer is found, a new reviewer is fetched from the process owner group. Oracle Identity Manager will select, if possible, a member of the process owner group who has not yet been used as a reviewer for this attestation request. If this is not possible, then Oracle Identity Manager will select a member of the process owner group who has already been selected to act as a reviewer. If Oracle Identity Manager cannot find a member of the process owner group, then it will assign XELSYSADM as the reviewer for the attestation task.

For each valid reviewer, the process calculates all the user entitlements that the reviewer must attest to as part of that task, as determined by the attestation scope defined in the process. The process then adds a reference and any related information regarding those user entitlements to the attestation data of the task. It also adds the number of entitlements covered by that task to the statistical field for the total number of entitlements identified for attestation in the process instance. The process then sends an e-mail message to the reviewer. It also sends e-mail to process owners about the reviewers with no e-mail address defined.

At the end of this stage, all the attestation tasks are in the attestation inboxes of the reviewers.

5.1.5.2 Stage 2: Acting on an Attestation Task

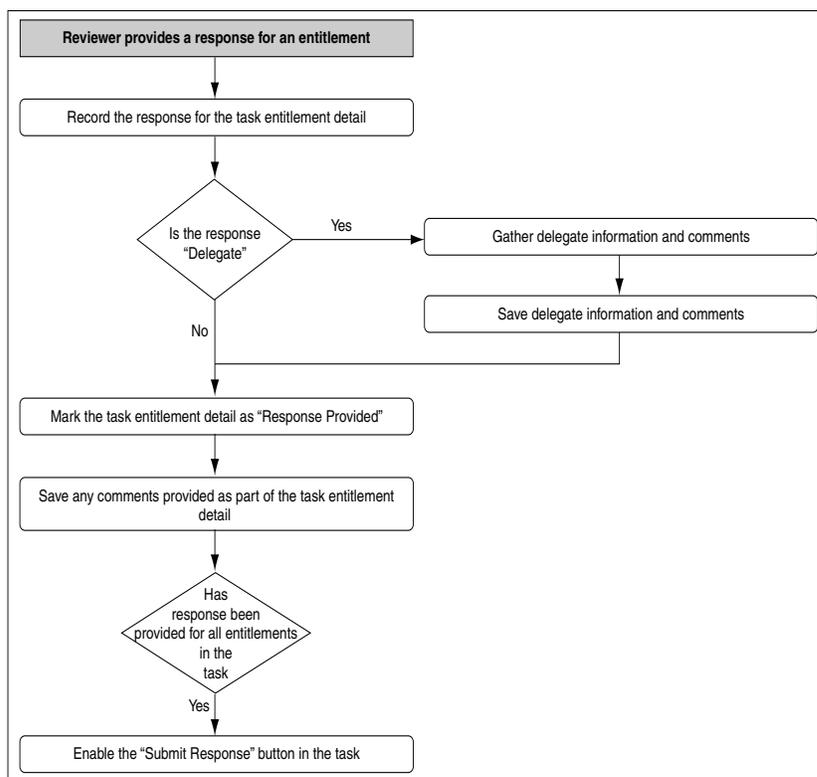
When an attestation task is assigned to a reviewer, the reviewer receives an e-mail, and the task is displayed in the reviewer's attestation inbox. The reviewer views task details in this inbox.

From the task details page, the reviewer provides a response and, if required, a comment for each entitlement. This marks the attestation entitlement detail in the task as **Response Provided**.

If the reviewer's response includes delegating the attestation activity for a specific entitlement, then the reviewer must provide a delegated user. Optionally, the reviewer can provide comments explaining why the reviewer is delegating the attestation activity to that user.

After the reviewer provides responses to all entitlements, the reviewer can commit their action for the attestation task by submitting all responses.

Figure 5-3 Flow of Events When Reviewer Responds to Entitlement



At this point, the next stage of the Attestation Business Process begins.

5.1.5.3 Stage 3: Processing a Submitted Attestation Task

The Attestation Task is marked as **Submitted**. At this point the attestation task is frozen, and cannot be acted on further. For each entitlement in the attestation task, the response is examined by the system. If the response is to either certify or reject, then the provisioned resource instance corresponding to that entitlement is updated accordingly. At the provisioned resource instance level, the last attestation result, the

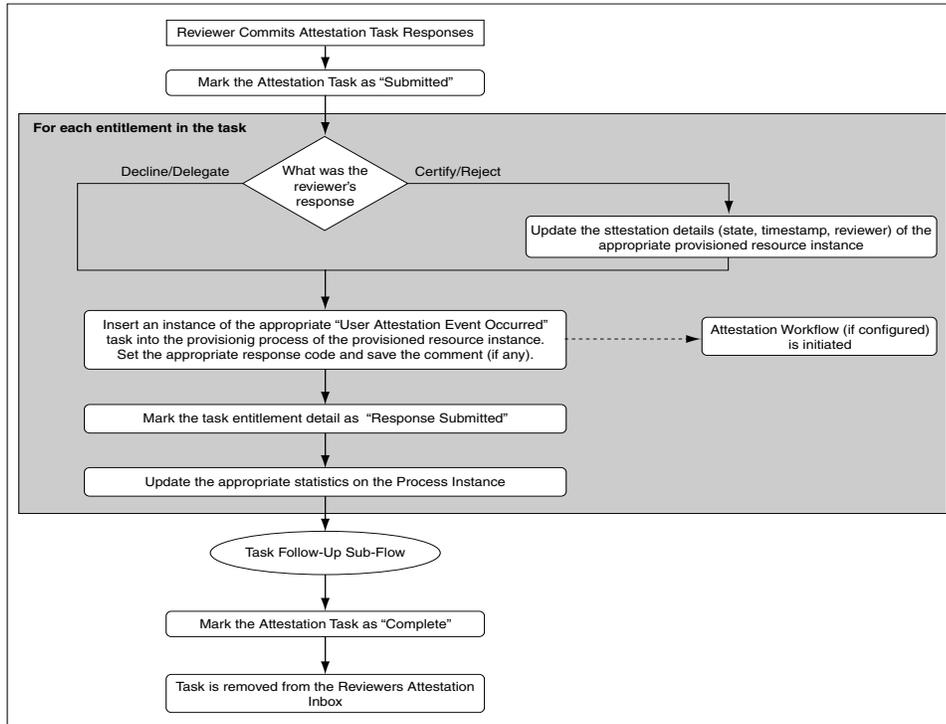
time at which last attestation occurred, and who the reviewer was are recorded. If the response is to decline or delegate, then the attestation detail at the provisioned resource level is not changed.

The **User Attestation Event Occurred** task is inserted into the provisioning process of the resource instance. This starts any attestation-driven workflows that may have been defined. Any comments are saved to the notes field of the task.

The attestation entitlement detail in the task is marked as **Response Submitted**.

Figure 5-4 shows the flow of events after the attestation task response is submitted.

Figure 5-4 Flow of Events After Attestation Task Response Is Submitted



The following statistics are updated on the process instance:

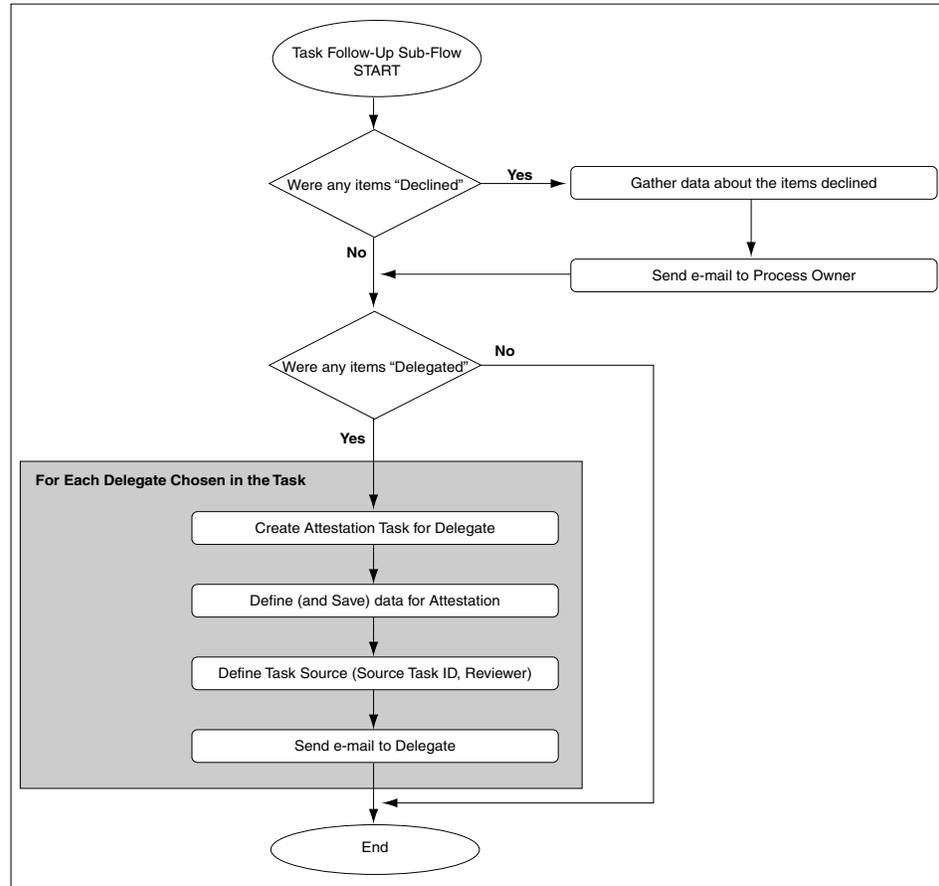
- Number of entitlements certified
- Number of entitlements rejected
- Number of entitlements declined
- Number of entitlements delegated

After all entitlements are covered, a subflow for follow-up action is initiated. In this flow, the process examines if the response for any of the entitlements in the task was declined. If there were any such entitlements, then the process sends e-mail to the Process Owner outlining the details of the decline action.

Next, the process examines if the response for any of the entitlements in the task was delegated. If there were any such entitlements, then the process identifies all the users that the reviewer selected as delegates and creates an attestation task for each. Each attestation task is only for the entitlements that the reviewer delegated to the user. The delegated user receives e-mail notification about the delegation.

After all the delegated attestation tasks are created, the subflow is completed and it merges back into the main flow. [Figure 5-5](#) shows the flow of events of the follow-up action subflow.

Figure 5-5 Follow-Up Action Sub-Flow



With the follow-up subflow complete, the attestation task is marked as **Complete**.

5.1.6 Attestation Engine

The attestation engine implements the attestation lifecycle. It is a service in Oracle Identity Manager architecture that exposes APIs to receive instructions to initiate a particular attestation process. The API is called from the attestation scheduled task as well as from the Run Now button on the Attestation Process Detail page to support on-demand execution. It supports both drivers for initiation of attestation processes.

The attestation engine uses the JMS messaging service to perform offline, queued processing. This ensures better performance.

Note: Attestation depends on the entry in the user profile audit data. If the audit entry is not generated for a user who is part of the attestation process, then the reviewer would not be able to see the user and process form information in attestation. To avoid such situations, ensure that the Issue Audit Messages Task scheduled task is run before performing the attestation run.

5.1.7 Attestation Scheduled Task

This new system scheduled task is responsible for examining the attestation processes defined in Oracle Identity Manager, and creating the necessary attestation tasks in the system.

Features of this scheduled task are:

- By default, this scheduled task is set to run every night. You can change the schedule according to your requirements.
- This scheduled task examines the attestation process definition table for all active (not system administrator) attestation processes
- If the scheduled task finds that the next scheduled start time of a process is in the past, then the task sends a call to the Attestation Engine to initiate the attestation process.

5.1.8 Attestation-Driven Workflow Capability

You can enhance the provisioning processes predefined in Oracle Identity Manager to listen to triggers coming from attestation activity. In this way, you can define custom workflows as part of the provisioning workflow that would respond to attestation taking place (or not taking place, in case of a refusal), and therefore be initiated when attestation takes place. This serves two purposes:

- The default attestation task in the flow, User Attestation Event Occurred, would provide the audit trail for the attestation history of the specific user entitlement.
 - There is one instance of this task for each time that resource instance is attested by the appropriate type of attestation process.
 - The response code set on the task indicates what the response provided by the reviewer is.
 - The user tagged as the person creating the task indicates who the reviewer is.
 - Any comment provided by the user is in the notes field for the task.
- Using response-generated tasks, the default task can start the workflow to respond to a particular attestation response received. Therefore, for a particular resource, you can specify that the Reject response must start the appropriate workflow tasks in the provisioning process for disabling the account, as an example.

5.1.9 Attestation E-Mail

As part of the attestation processes, the Attestation Engine sends out e-mail to various interested parties. To make the e-mail configurable with respect to the content, they are made available as e-mail templates of the General type in Oracle Identity Manager Email Definition store. For context-sensitivity, the e-mail contain a set of variables that can be replaced with the required values.

5.1.9.1 Notify Attestation Reviewer

This template is used to build the e-mail to send to the reviewer when an attestation task is assigned to the reviewer.

5.1.9.1.1 Variables The following are variables in the Notify Attestation Reviewer template:

Variable	Description
Attestation Definition.Process Name	Name of the attestation process
Attestation Definition.Process Code	Code for the attestation process
Attestation Task.Task Assigned Date	Date the attestation task was assigned

5.1.9.1.2 Subject Line The following is the Subject line of e-mail messages defined by the Notify Attestation Reviewer template:

A new attestation task for attestation process *Attestation Definition.Process Name* has been added to your attestation inbox

5.1.9.1.3 Body The body of the e-mail message contains the following information:

The attestation task details are as follows
 Process Name: *Attestation Definition.Process Name*
 Process Code: *Attestation Definition.Process Code*
 Data Type: Access Rights
 Assigned Date: *Attestation Task.Task Assigned Date*

5.1.9.2 Notify Delegated Reviewers

This template is used to build the e-mail to send to a reviewer when an attestation task is delegated to the reviewer.

5.1.9.2.1 Variables The following are variables in the Notify Delegated Reviewers template:

Variable	Description
Attestation Definition.Process Name	Name of the attestation process
Attestation Definition.Process Code	Code for the attestation process
Attestation Task.Task Assigned Date	Date the attestation task is assigned
Attestation Task.Delegated By First Name	First name of the reviewer who performed the delegation
Attestation Task.Delegated By Last Name	Last name of the reviewer who performed the delegation
Attestation Task.Delegated By User Id	User ID of the reviewer who performed the delegation action

5.1.9.2.2 Subject Line The following is the Subject line of e-mail messages defined by the Notify Delegated Reviewers template:

Attestation Task.Delegated By User Id has delegated to you an attestation task from attestation process *Attestation Definition.Process Name*

5.1.9.2.3 Body The body of the message contains the following information:

The attestation task details are as follows
 Process Name: *Attestation Definition.Process Name*
 Process Code: *Attestation Definition.Process Code*
 Data Type: Access Rights
 Assigned Date: *Attestation Task.Task Assigned Date*
 Delegated By: *Attestation Task.Delegated By First Name Attestation Task.Delegated By Last Name [Attestation Task.Delegated By User Id]*

5.1.9.3 Notify Process Owner About Declined Attestation Entitlements

The Notify Declined Attestation Entitlements template is used to build the e-mail to send to process owners notifying them of any declined entitlement attestations.

5.1.9.3.1 Variables The following are variables in the Notify Process Owner about Declined Attestation Entitlements template:

Variable	Description
Attestation Request.Request Id	ID of the attestation request
Attestation Definition.Process Name	Name of the attestation process
Attestation Task.Reviewer First Name	First name of the reviewer
Attestation Task.Reviewer Last Name	Last name of the reviewer
Attestation Task.Reviewer User Id	User ID of the reviewer
Attestation Data.Provisioned User First Name	First name of the user being attested
Attestation Data.Provisioned User Last Name	Last name of the user being attested
Attestation Data.Provisioned User Id	User ID of the user being attested
Attestation Data.Resource Name	Name of the resource being attested
Attestation Data.Entitlement Descriptive Data	Descriptive data of the entitlement being attested

5.1.9.3.2 Subject Line The following is the Subject line of e-mail messages defined by the Notify Process Owner About Declined Attestation Entitlements template:

User access rights in attestation request *Attestation Request.Request Id* have been declined by *Attestation Task.Reviewer User Id*

5.1.9.3.3 Body The following is displayed in the body of the message:

Attestation of the following user access rights were declined by the reviewer.
 Reviewer: *Attestation Task.Reviewer First Name* *Attestation Task.Reviewer Last Name* [*Attestation Task.Reviewer User Id*]
 Attestation Process: *Attestation Definition.Process Name*
 Attestation Request ID: request *Attestation Request.Request Id*
 Access Rights Data: *Attestation Data.Provisioned User First Name* *Attestation Data.Provisioned User Last Name* [*Attestation Data.Provisioned User User Id*] - *Attestation Data.Resource Name* - *Attestation Data.Entitlement Descriptive Data*

5.1.9.3.4 Special Comments Each entitlement data item will appear on a new line.

5.1.9.4 Notify Process Owner About Reviewers with No E-Mail Defined

The Attestation Reviewers With No Email Defined template is used to build the e-mail to send to process owners notifying them of reviewers for whom there is no e-mail address defined.

5.1.9.4.1 Variables The following are variables in the Notify Process Owner About Reviewers with No Email Defined template:

Variable	Description
Attestation Request.Request Id	ID of the attestation request

Variable	Description
Attestation Definition.Process Name	Name of the attestation process
Attestation Request.Request Creation Date	Date when the attestation request was created
Attestation Task.Reviewer First Name	First name of the reviewer that is invalid
Attestation Task.Reviewer Last Name	Last name of the reviewer that is invalid
Attestation Task.Reviewer User Id	User ID of the reviewer that is invalid

5.1.9.4.2 Subject Line The following is the Subject line for e-mail defined by the Notify Process Owner About Reviewers with No Email Defined template:

E-mail address is not defined for some of the reviewers in attestation process
Attestation Definition.Process Name, request *Attestation Request.Request Id*

5.1.9.4.3 Body The following is the body of the message:

The following attestation reviewers do not have e-mail addresses defined. Attestation requests have been generated for these reviewers and can be accessed by logging in to Oracle Identity Manager. However, notification e-mails were not sent.

Attestation process: *Attestation Definition.Process Name*
 Attestation Request ID: request *Attestation Request.Request Id*
 Request date: *Attestation Request.Request Creation Date*
 Reviewers Without Email: *Attestation Task.Reviewer First Name Attestation Task.Reviewer Last Name* [*Attestation Task.Reviewer User Id*]

5.1.9.4.4 Special Comments Each reviewer detail appears on a new line.

5.2 Attestation Process Configuration

A menu item in Oracle Identity System Administration provides access to the Attestation Process Configuration pages. Oracle Identity Manager administrators can use these pages to:

- Define new attestation processes.
- Manage existing processes.
- Initiate ad-hoc attestation processes.

5.2.1 Menu Structure

The top-level Attestation menu contains the following links in the Policies section of Oracle Identity Manager Advanced Administration:

- Create Attestation Process
- Manage Attestation Process

These menu items are governed by the same delegated administration permissions that govern all menu items in the Advanced Administration.

These menu items are defined but not assigned to any group in Oracle Identity Manager. They will be assigned to the System Administrators group in Oracle Identity Manager if audit compliance components are installed.

5.2.2 System Control

Attestation has the following dependencies:

- The User Profile Audit feature must be enabled.
- Historical data must be collected at least up to the Process Form level.

If the auditing level is set below the required levels, then clicking menu item links related to attestation generates the Attestation Feature Not Available page, and prevents the user from defining any attestation processes.

Audit levels are controlled by the system property called `XL.UserProfileAuditDataCollection` and the attestation feature expects this value to be set to at least Resource Form.

5.3 Creating Attestation Processes

Note: Oracle Identity Manager Permission model applies to the procedure described in this section. This model restricts any list of targets (for example, users) to only those targets for which the logged-in user has read access.

To create an attestation process:

1. Login to Oracle Identity System Administration.
2. In the left pane, under Policies, click **Attestation Configuration**. The Manage Attestation Process page is displayed.
3. Click **Create Attestation** Process. The Step1: Define Process page is displayed.
4. Enter values for the fields described in the following table, and then click **Continue**:

Field	Description
Name	A unique name for the attestation process. The name must be unique across system administrator and deleted attestation processes.
Code	An identifying code (up to 32 characters) for the process. The code must be unique across system administrator and deleted attestation processes. Note: A code enhances the identification of the attestation process definition. However, if you do not specify a value in the Code field, then the attestation process is identified by the unique name.
Description	Detailed description of the attestation process.

5. On the Step 2: Define User Scope page:
 - a. Select an attribute from the **Attribute** list. The Attribute list displays the user attributes given in the `FormMetaData.xml` file and the user-defined attributes from the user form. The attribute that you select is used to specify the criteria that must be met by users on whom the attestation process is applied.
 - b. From the **Condition** list, select a condition. The Condition list of values will change based on the type of attribute selected. For example, if you select User

ID in the **Attribute** field, then the conditions displayed are **Contains**, **Does Not Contain**, **Is Exactly**, and **Is Not Exactly**. If you select the **Start Date** attribute, then the conditions displayed are **Before**, **After**, and **Between**.

- c. In the **Value** field, enter a value for the user attribute.
 - d. Select the **Recursive** option. The **Recursive** check box is used for the entities for which you want to include the child entities while defining user scope. For example, if you select **Organization** in the user scope and then select **Recursive**, then the operation also includes all the suborganizations.
 - e. Click **Add** to add a new row to the user scope table, and click **Continue**. If you add multiple rows to the user scope table, then the attestation process will apply only to users who match all of the attribute conditions in the user scope.
6. On the Step 3: Define Resource Scope page, select a resource for the attestation process as follows:
- a. From the **Attribute** list, select one of the resource attributes listed in the following table:

Attribute	Expression	Description
Name	Full text or wildcard	The name of the resource.
Type	Lookup values with the option to select all or a subset	The type of resource.
Resource Audit Objectives	Lookup values with the option to select all or a subset	The audit objectives assigned for a resource, which is provisioned. For example, whether or not the resource is financially significant. For more information about Resource Audit Objectives, see "Viewing Resource Details" on page 12-1.
Administrator User Groups	Lookup values with the option to select all or a subset	The user groups that have administrative permissions for a resource.
Authorized User Groups	Lookup values with the option to select all or a subset	The user groups that are authorizers or approvers for the resources.
Resource Status	Full text or wildcard	The status displayed when a resource is provisioned to a user, such as Certify , Reject , Open , or Closed .

- b. From the **Condition** list, select a search condition.
 - c. In the **Value** field, enter a value for the resource attribute.
 - d. Click **Add** to add a new row to the resource scope table, and then click **Continue**. If you add multiple rows to the resource scope table, then the attestation process will apply only to resources that match all of the attribute conditions in the resource scope.
7. On the Step 4: Define Administration Details page, define the reviewer to attest data, the attestation process schedule, grace period, and the process owner by performing the following steps:
- a. From the **Reviewer** list, select the type of reviewer for the attestation process, such as a single specific user, role member, or resource administrator. Then, select the reviewer from the adjoining lookup field.

When you select "Role Member" as the reviewer type, you must select a role for reviewing a particular attestation task. Once the attestation task has been created and run, it will be assigned to the role you selected based on the following conditions:

- All users who are not in Deleted and Disabled state will be assigned the attestation task.
 - If the reviewer in that role happens to be the beneficiary as well, then that user will not be assigned the attestation task.
 - If after the above checks, there is no eligible user in that role, then the task is assigned to all the users in the System Administrator role.
- b. Specify the attestation process schedule to run the attestation process once or repeatedly after a specific number of days, months, or years.
 - c. Specify the grace period, the number of days in which each reviewer must respond to any attestation task that is generated by this attestation process.
 - d. In the **Starting on** field, specify a start date for the attestation process.
 - e. In the **Process owner group lookup** field, specify a group that is the process owner for the attestation process.
 - f. If you want the process owner to be notified by e-mail if the reviewer refuses the attestation process, select **Email process owner if reviewer refuses attestation request**. Then, click **Continue**.
8. On the Step 5: Verify Info page, review the details of the attestation process, and then click **Create Process**.

You are redirected to a page with a message that you have successfully created an attestation process definition. Clicking the process name takes you to the Attestation Process Detail page. To create another attestation process, click **Create Another Attestation Process Definition**.

The Attestation Process Detail page is described in the "[Managing Attestation Processes](#)" section.

5.4 Managing Attestation Processes

To manage attestation processes:

1. In the left pane of Oracle Identity System Administration, under Policies, click **Attestation Configuration**. The Manage Attestation Process page is displayed.
2. On the Manage Attestation Process page, enter the search criteria for the attestation process you want to manage. You can search by attestation process name, process code, reviewer type, or process owner. After you enter your search criteria, click **Search**. The Attestation Process Details page is displayed with the attestation processes that match your search criteria. The attestation processes displayed are the ones that the logged-in administrator is allowed to view based on permissions, or by virtue of being a member of the Process Owner group. This page does not show any deleted processes. The columns displayed on the page are listed in the following table:

Column	Description
Names	Specifies the name of the process.
Code	Specifies the attestation process code.

Column	Description
Description	Specifies a description for the process.
Status	Indicates whether the attestation process is active or system administrator.
Type	Specifies the type of resource.
User Scope	Specifies the scope of the user who will be a part of the attestation process.
Resource Scope	Specifies the resources that are within the scope of the attestation process.
Reviewer Type	Indicates the type of the reviewer.
Reviewer Name	Indicates the name of the reviewer.
Schedule	Indicates if the process is scheduled to run only once, or on a daily, monthly, or yearly basis.
Last Start	Specifies the last time an attestation process was run.
Next Start	Specifies when the process is scheduled to run next.
Process Owner Group	Indicates the process owner group. In addition, it specifies whether or not the process owner will be notified by e-mail if the reviewer refuses the attestation request.
Last Completion	Specifies the last time an instance of this process was completed.

The rest of this section discusses the following topics:

- [Editing Attestation Processes](#)
- [Disabling Attestation Processes](#)
- [Enabling Attestation Processes](#)
- [Deleting Attestation Processes](#)
- [Running Attestation Processes](#)
- [Managing Attestation Process Administrators](#)
- [Viewing Attestation Process Execution History](#)

5.4.1 Editing Attestation Processes

To edit an attestation process:

1. On the Attestation Process Detail page, click **Edit**.
2. On the Edit Attestation Process page, make the required changes to the attestation process, and then click **Save**.

The fields on the Edit Attestation Process page are the same as those displayed in the "[Creating Attestation Processes](#)" section.

5.4.2 Disabling Attestation Processes

To disable an active attestation process:

1. On the Attestation Process Detail page, click **Disable**.

Note that the Disable button is displayed only when a process is active.

2. On the Disable Attestation Confirmation page, click **Confirm Disable**.

5.4.3 Enabling Attestation Processes

An attestation process can be enabled only if its next start time is in the future and if the process is disabled.

To enable an attestation process:

1. On the Attestation Process Detail page, click **Enable**.

Note that the Enable button is displayed only when the process is disabled.

2. On the Enable Attestation Confirmation page, click **Confirm Enable**.

5.4.4 Deleting Attestation Processes

You can edit, disable, or delete an attestation process only as a process administrator with the required permissions.

To delete an attestation process:

1. On the Attestation Process Detail page, click **Delete**.
2. On the page, click **Confirm Delete**.

5.4.5 Running Attestation Processes

This feature enables you to run unscheduled attestation processes. To run an attestation process, click **Run Now** on the Attestation Process Detail page. This starts the attestation process independent of the attestation schedule.

Only users in the process owner group can start unscheduled attestation processes.

5.4.6 Managing Attestation Process Administrators

The tasks of adding, deleting, and updating administrative groups for attestation processes are similar to the tasks of adding, deleting, and updating administrative groups for users and organizations.

To manage the administrators of an attestation process, select **Administrators** from the Additional Details list on the Attestation Process Detail page. The Administrative Groups page is displayed. You can use this page to add and remove administrators for an attestation process and update administrator permissions.

The permission model for an attestation process definition is as follows:

- To view the attestation process definition, the user must be either of the following:
 - A member of a group that has the appropriate read permissions in the administrators group
 - A member of the group that is the process owner
- To edit the attestation process definition, the user must be a member of a group that has the required write permissions in the administrators group.
- To delete the attestation process definition, the user must be a member of a group that has the required delete permissions in the administrators group.

5.4.7 Viewing Attestation Process Execution History

To view the execution history of an attestation process, select **Execution History** from the Additional Details list on the Attestation Process Detail page. The Attestation Process Execution History page is displayed.

The following are the columns in the Attestation Process Execution History table:

Column	Description
Request ID	ID for the attestation process instance that was run
Reviewer	Name of the reviewer for the attestation process
Initiated On	Date and time when the request was started
Completed On	Date and time when the request was completed If the request is still pending, then it shows Not Completed.

On the Attestation Process Execution History page, click the request ID link to open the Request Detail page. On this page, you can filter the requests according to the certified, rejected, open, and closed state.

5.5 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, login 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.

5.5.1 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"> ▪ Certify ▪ Reject ▪ Open ▪ Closed
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.
Comments	Reviewer comments. Long comments are truncated, and tooltips are used to show the full text of the comments.

5.5.2 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.

5.5.3 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.

Part III

Identity Certification

This part describes identity certification in Oracle Identity Manager.

It contains the following chapter:

- [Chapter 6, "Managing Identity Certification"](#)

Managing Identity Certification

This chapter describes the concepts related to identity certification, the configuration tasks required for identity certification. It contains the following topics:

- [Certification Concepts](#)
- [Configuring Certifications](#)
- [Managing Certification Definitions](#)
- [Scheduling Certifications](#)
- [Understanding How Risk Summaries are Calculated](#)
- [Understanding Closed-Loop Remediation and Remediation Tracking](#)
- [Understanding Event Listeners](#)
- [Configuring Event Listeners and Certification Event Trigger Jobs](#)
- [Configuring Certification Reports](#)
- [Understanding Multi-Phased Review in User Certification](#)
- [Troubleshooting Identity Certification](#)

6.1 Certification Concepts

The concepts related to identity certification is described in the following sections.

6.1.1 Line of Business and Line Item

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.

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.

6.1.2 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.

6.1.3 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

6.1.4 Certification Definition

Certification definition is a named set of parameters that is used as input to a certification job to generate certification objects. A certification definition specifies the following:

- The type of certification to generate, such as user certification, role certification, application instance certification, or entitlement certification
- Selection criteria that describe which line items, for example users, to select
- Content-restriction criteria that describe which details to select for each line item
- Other parameters that control the generation of certification objects or the behavior of review tasks

6.1.5 Certification Jobs

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 jobs can be:

- Scheduled to run at regular intervals, such as weekly, monthly, or quarterly, as required
- Run immediately from the Scheduler section of Oracle Identity System Administration
- Triggered from an event-listener action

You can create and run certification-generation jobs to create certifications as requested or as scheduled. You can enable and run the risk-aggregation job to calculate the risk-values of entities, such as users, accounts, role-assignments, and entitlement-assignments.

6.1.6 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.

6.1.7 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.

6.1.8 Event Listener

Event listener is a service that responds to changes in users. Event listeners are supported for user and application instance certifications.

Each event listener for certification contains:

- The selection-criteria specified by an administrator
- The certification definition to use in response

6.1.9 Certification Authorization

The following Oracle Identity Manager admin roles grant the assignee privileges required to administer the certification feature and monitor the progress of certification instances:

- **Certification Administrator:** The Certification Administrator admin role grants the assignee super-user privileges for the certification feature. In particular, this admin role grants access to the certification configuration and scheduler in the Oracle Identity Manager System Administration. This role also grants full access to certification where you can view or take action on any certifications.
- **Certification Viewer:** The Certification Viewer is a read-only role, allowing a compliance administrator to view new, in progress, and completed certifications.

See "Security Architecture" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the permissions and associated authorization policies of the Certification Administrator and Certification Viewer admin roles.

6.2 Configuring Certifications

This section contains the following topics:

- [Prerequisites for Configuring Certifications](#)
- [Configuring Certification Options in Identity System Administration](#)

6.2.1 Prerequisites for Configuring Certifications

Configuring certifications has the following prerequisite steps:

- [Marking a Catalog Item as Certifiable](#)
- [Setting the Certifier in the Request Catalog](#)
- [Setting User Manager and Organization Certifier](#)
- [Setting Risk Levels for Individual Entities](#)
- [Tagging Attributes](#)
- [Configuring the Availability of Identity Certification](#)
- [Configuring Reminders, Notifications, Escalations, and Expiry for Certifications \(Optional\)](#)

Note: Some of the preconfiguration steps require you to use the request catalog. For detailed information about the request catalog, see the following sections:

- "Using the Access Request Catalog" in the Oracle Fusion Middleware User's Guide for Oracle Identity Manager
 - ["Managing the Access Request Catalog"](#) on page 17-1
-
-

6.2.1.1 Marking a Catalog Item as Certifiable

A requestable entity, such as user account, role assignment, role membership, application instance, or entitlement, is available for certification only after it is marked as certifiable in the request catalog. Any entity that is not marked as certifiable does not appear in the certification.

To mark an entity as certifiable:

1. Login to Oracle Identity Self Service.
2. On the left pane, under Requests, click **Catalog**.
3. Search and select the role, application instance, or entitlement that you want to set as certifiable.
4. Under Detailed Information, select the **Certifiable** option.
5. Click **Apply**.

Note: By default, all items in the catalog are marked as certifiable. You can deselect the **Certifiable** option if you do not want a certification task to be generated for that entity.

6.2.1.2 Setting the Certifier in the Request Catalog

When you set a user as the certifier for an entity and select some of the options for selecting reviewers, such as Role Certifier or Application Instance Certifier, the user is automatically set as the certifier or primary reviewer for certifying that entity. For example, if user John Doe is selected as the certifier for the Vision Developers role, then John Doe is automatically set as the primary reviewer for certifying the Vision Developers role depending on the selection in the Reviewers screen of creating certifications. In this example, after the user is set as the certifier for the Vision Developers role and you are creating a Role Certification, selecting the Role Certifier option will pick up this field.

Note: Setting the certifier in the request catalog is required if you want to use some of the options for selecting reviewers in the certification creation screen, such as Role Certifier or Application Instance Certifier.

To set the certifier in the catalog:

1. In Oracle Identity Self Service, navigate to the Catalog page.
2. Search and select the role, application instance, or entitlement for which you want to set the certifier.

3. For the Certifier User field, click the lookup icon. From the lookup, search and select a user that you want to set as certifier for the selected entity.

Note: The Certifier Role field available in the Detailed Information section of the catalog is not used in Oracle Identity Manager 11g Release 2 (11.1.2.1.0).

4. Click **Apply**.

6.2.1.3 Setting User Manager and Organization Certifier

The user manager and organization certifier are available for selection as the primary reviewer in the certification creation process.

User manager is the user selected in the Manager field in the Attributes tab of the User Details page in Oracle Identity Self Service. If Jane Doe is specified as the manager for Terence Hill, then while creating a user certification definition, as described in ["Creating Certification Definitions"](#) on page 6-9, when you select user manager as the primary reviewer, Jane Doe is automatically set as the primary reviewer for the certification tasks generated for Terence Hill.

The organization certifier is the user selected in the Certifier User Login field in the Attributes tab of the Organization Details page in Oracle Identity Self Service. If Robert Klein is specified as the organization certifier for the Vision North organization, then while creating the certification definition, when you select organization certifier as the primary reviewer, Robert Klein is automatically set as the primary reviewers for the certifications tasks generated for Vision North.

Note:

- Setting the user manager or organization certifier is required if you want to use the Reviewer option of User Manager or Organization Certifier. Otherwise, this is not required.
 - Role organization certifier does not support the Hierarchy aware option. For the organization certifier, the role must be available in the organization. In other words, the specific organization must be specified for the role. Otherwise, certification will not be generated. Make sure that the role and organization are linked and organization has the certifier user assigned.
-

6.2.1.4 Setting Risk Levels for Individual Entities

To set the risk levels for individual entities:

1. In Oracle Identity Self Service, navigate to the Catalog page.
2. Search and select the role, application instance, or entitlement for which you want to set the risk level.
3. Under Detailed Information, from the Risk Level list, select **High Risk**, **Medium Risk**, or **Low Risk**.
4. Click **Apply**.

After setting the risk level for an individual entity, you must run the Risk Aggregation scheduled job so that final and correct risk level is pick up.

6.2.1.5 Tagging Attributes

Accounts, IT resources, and entitlements must be tagged for certification in the Design Console. Without tagging, certification for the entities are not generated.

To configure account and IT resource tagging:

1. Login to the Design Console.
2. Under Development Tools, click **Form Designer**.
3. Click the search icon on the top. The Form Designer Table is displayed with a list of all available forms.
4. Open the child process form, and click **Create New Version**.
5. Click the **Properties** tab.
6. Locate only one entitlement field per form, click **Add Property**, and add the `Entitlement = true` property setting.
If there are multiple entitlement child forms, then add one `Entitlement = true` property setting per entitlement form.
7. Save the child form, and click **Make Version Active**.

Note: If there are multiple child forms, update all of them by repeating steps 4 through 7 before going to the next step.

8. Select the parent forms for each connector that is installed. The parent form has the User ID fields to store the account name in the target system, for example, UD_ADUSER and UD_EBS_USER.
9. Select a form. A new Form Designer tab opens.
10. Click **Create New Version**. In the popup, enter a name, for example, v2. Click the save icon. Close the popup.
11. In the Current version list, make sure that the newly created version v2 is selected.
12. Click the **Properties** tab.
13. Locate the field that uniquely identifies the account in the target system, such as UserID, UserName, and AccountName, which are typical fields in the default connectors. Click **Add Property**, and add the `AccountName = true` property setting.
14. Locate the IT resource field. For most connectors, this is identified by the text `ITResourceLookupField` as a property for the target system. Click **Add Property**, and add the `ITResource = true` property setting.
15. Save the parent form. Click **Make Version Active**.
16. Repeat steps 3 through 11 for each IT resource.

6.2.1.6 Configuring the Availability of Identity Certification

Oracle Identity Manager enables you to use the identity certification feature along with the legacy attestation feature. You can also choose to hide attestation or certification if you do not want to use one of them. To configure the usage of certification and attestation, provide any one of the following values for the 'Display Certification or Attestation' system property:

- **both:** This value specifies that all the attestation and identity certification navigation menus and pages are displayed in Oracle Identity Self Service and Oracle Identity System Administration.
- **attestation:** This is the default value. This value specifies that only attestation feature can be used, and all identity certification navigation menus and pages are hidden in Oracle Identity Self Service and Oracle Identity System Administration.
- **certification:** This value specifies that only identity certification feature can be used, and all attestation navigation menus and pages are hidden in Oracle Identity Self Service and Oracle Identity System Administration.

Note: You must have the license for the Certification component in order to set the value of the Display Certification or Attestation system property to both or certification.

After setting the value of this system property, you must restart Oracle Identity Manager.

Note: For information about system properties and setting the values of system properties, see "[Managing System Properties](#)" on page 16-1.

6.2.1.7 Configuring Reminders, Notifications, Escalations, and Expiry for Certifications (Optional)

If email notifications is configured in SOA, as described in "[Configuring SOA Email Notification](#)" on page 14-17, then email notifications are sent by default in the following scenarios:

- When a task is assigned to a user
- When a task is completed

By default, two reminders are sent one day after and two days after the certification has been created. There is no escalation or expiry set for the certifications by default.

To change the default configuration for certification:

1. Login to Oracle SOA Composer with Admin credentials, such as weblogic, by navigating to the following URL:

```
http://HOST_NAME:PORT_NUMBER/soa/composer
```
2. Click **Open**, and select **Open Tasks**. The Select a Task to open dialog box is displayed.
3. Select CertificationProcess_rev1.0, and click **Open**. The CertificationTask : Event Driven Configuration page is displayed.
4. In the Notification Settings section, perform the following:
 - a. The assignees of the task are selected as recipients of the notification for Assign and Complete tasks. To change the default setting, you can select the task status in the Task Status column, and select the notification recipient in the Recipient column. You can click the pencil icon for each task to edit the default notification message, and click **OK**.
 - b. In the drop-down below, change the default setting for reminders.

5. In the Expiry and Escalation Policy section, you can change the default value for escalation and expiry.
6. Click **OK**.
7. Click **Save**, and then click **Commit**.

6.2.2 Configuring Certification Options in Identity System Administration

You can set default options in Oracle Identity System Administration that are used during certification creation based on the type of certification. These options can be changed during the certification creation process for each certification definition.

To configure certification options in Oracle Identity System Administration:

1. In the left pane of Oracle Identity System Administration, under Certifications, click **Certification Configuration**. The Certification Configuration page is displayed.
2. Set the configuration properties, as listed in [Table 6–1](#).

Note: All the options listed in [Table 6–1](#) set the default configuration that is picked up during certification creation based on the type of certification. These can be changed during the certification creation process for each certification definition.

Table 6–1 Configuration Properties

Property	Description
Password required on sign-off	Select to require users to sign off in order to complete a certification.
Allow comments on certify operations	Select to allow the user to type a comment if a certify action is selected. By default, a comment is required.
Allow comments on all non-certify operations	Select to allow the user to type a comment if a revoke action is selected. By default, a comment is required.
Verify employee access	Select to control if you want to view Page 1 in the user certification view. By default, this option is selected. This option is used in user certification.
Prevent self certification	Select to prevent reviewers from being able to certify their own access. Enabling this option allows the certification creator to assign the certification to an alternate reviewer. When the Prevent self certification option is enabled, the User Manager option is selected by default, which means that the assignee is the user's manager. To select any other user, select Select User . Click the Search icon to search and select an alternate reviewer.
User and Account Selections	Select any one of the following: <ul style="list-style-type: none"> ■ Include only active users and active accounts: ■ Include any user with active accounts: ■ Include all users and all accounts:

Table 6–1 (Cont.) Configuration Properties

Property	Description
Allow advanced delegation	Select to enable the ability to delegate a line item to others. This option is not selected by default. When delegation is enabled, there is a verification stage, in which the certification is routed to the primary reviewer with all the decisions of the delegates as well as the primary reviewer's own decisions for final sign off.
Allow multi-phased review	Select to enable collaborative certification, for which in phase 1 the business review is completed and that is followed by a phase 2 for the technical review followed by an optional final review, which is completed by the business reviewer again. This is used only in user certification only.
Allow reassignment	Select to reassign the line items in page 1 of certifications to other users. When a certification task is reassigned, the item disappears from the list of the original assignee and is not visible within the review cycle.
Allow auto-claim	Select to mark all the items in page 1 as claimed by default. By default, auto claim is enabled. If you deselect this option, then users have to manually claim each item before they can view the item details.
Perform closed loop remediation	Select any one of the following: <ul style="list-style-type: none"> ■ Never: Select to prevent closed-loop remediation. ■ When certification is completed: Select to specify closed-loop remediation when certification is completed.
Enable Interactive Excel	Select to enable ADF DeskTop Integration (DI) for user certification that provides the user the option to download certification data to Microsoft Excel worksheet and work on it in offline mode. See "Completing User Certifications in Offline Mode" in the <i>Oracle Fusion Middleware User's Guide for Oracle Identity Manager</i> for information about working on certifications in an offline mode.

3. Click **Save**.

6.3 Managing Certification Definitions

This section contains the following topics:

- [Creating Certification Definitions](#)
- [Modifying Certification Definitions](#)
- [Deleting Certification Definitions](#)

6.3.1 Creating Certification Definitions

Creating certification definitions is described in the following sections:

- [Creating a User Certification Definition](#)
- [Creating a Role Certification Definition](#)
- [Creating an Application Instance Certification Definition](#)
- [Creating an Entitlement Certification Definition](#)

6.3.1.1 Creating a User Certification Definition

To create a user certification definition:

1. Log in to Oracle Identity System Administration.
2. On the left pane, under Certifications, click **Certification Definitions**. The Certification Definitions page is displayed.
3. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The General Details page of the New Certification wizard is displayed.
4. Enter values as follows:
 - **Certification Name:** Enter a name for the certification.
 - **Type:** Select **User** to create a user certification.
 - **Description:** Optionally enter a description for the new user certification.
5. Click **Next**. The Base Selection page of the New Certification wizard is displayed.
6. Select a user-selection strategy in the Base Selection section, as follows:
 - **Users from All Organizations:** Selects users from all organizations in Oracle Identity Manager.
 - **Only Users from Selected Organizations:** Allows you to manually select specific organizations. You can select the organizations by clicking Add. To remove a selected organization, click Remove.

Note: When completing a certification, a certifier cannot see the organization name or any other details about the organization unless that person is also the organization administrator for that organization. If the certifier is not the organization administrator, only the users in the organization are displayed.

- **All users:** Selects all the users in Oracle Identity Manager.
 - **Users criteria:** Selects all the users that meet the given search condition. For help with search, See "Searching Users" in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about searching. You can preview the results of this selection.
 - **Selected users:** Allows you to select specific users from a list of users in the system. To select users, click **Add**. To remove selected users, click **Remove**.
7. Select any one of the following options to specify constraints to the base selection:
 - Users with Any Level of Risk
 - Only Users with High Risk Summaries
 - Only Users with High Risk Roles
 - Only Users with High Risk Application Instances
 - Only User with High Risk Entitlements
 8. Click **Next**. The Content Selection page is displayed.
 9. Select the following:
 - **Include users with no accounts:** This option includes the users who have no access within the certification.

- **Limit the role-assignments to certify for each user:** The list of roles per user can be restricted to the selected option. For example, if you select selected roles and add one role, then that role only will show up in the certification if it is marked as certifiable in the catalog even if the user has other roles.
 - **Include accounts with no certification attributes:** This includes the accounts in the selected application instances even if there are no certifiable entitlements (access) within the target system. If you deselect this option, then accounts in the target system that do not have any entitlements do not appear in the certification.
 - **Limit the application-instance-assignments to certify each user:** Similar to roles, you can restrict the application instances you want to see within the certification.
 - **Limit the entitlement-assignments to certify for each user:** You can limit the entitlements that you can see within the certification.
10. Click **Next**. The Configuration page is displayed.
11. Select the options, as described in [Table 6–1, "Configuration Properties"](#), and click **Next**. The Reviewers page is displayed.

If you want to enable multi-phased review with advanced delegation, then select the **Allow advanced delegation** and **Allow multi-phased review** options.

12. From the Reviewer list, select a primary reviewer. The primary reviewer can be user manager, organization certifier, or any other user that you select.

For multi-phased review, perform the following:

- a. In the Phase 1 section, select any one of the following to select the Phase 1 reviewer:
 - **User Manager:** Selects the user's manager as the Phase 1 reviewer.
 - **Organization Certifier:** Selects the organization certifier as the Phase 1 reviewer.
 - **Search for a User:** Selects any user as the Phase 1 reviewer that you search and specify by clicking the lookup icon.
 - b. In the Phase 2 (Optional) section, select the **Enable Phase 2 review process** option to specify that the privilege certifier will be the primary Phase 2 reviewer for each user privilege, such as role, account, and entitlement assignments.
 - c. In the Final Review (Optional) section, select the **Enable Final Review process** option to enable a final review process by the Phase 1 reviewer for final validation and sign off.
13. Click **Next**. The Incremental page is displayed.
14. Select **Enabled** for Generate Incremental Data. This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

When Incremental Certification is enabled, it takes the following parameters:

- **Incremental Date Range** (required): This includes:
 - **Since Last Base** (default): When this option is selected, current access of the user is compared against the last certification of the same type, which was created without enabling incremental and all the incremental

certifications since then, to the current date when the certification is created.

- **Since Date:** When this option is selected, current access of the user is compared against all the certifications of the same type since the given date and when the certification is created.
 - Show Previous Value (optional): This includes:
 - **Disabled** (default): When this is deselected, then the values that have already appeared in the previous certifications based on the Incremental Date Range parameter are not included in the certification.
 - **Enabled:** When this is selected, all the current values that existed in previous certifications are displayed with the last decisions taken for those access.
15. Click **Next**. The Summary page is displayed with the details of the user certification.
16. Click **Create** to create the user certification. A message is displayed asking if you want to create a certification job based on the definition and run it now. You can edit the job name, and click **Yes** to run the certification job.

Alternatively, click **No** to create a certification definition without creating and running the scheduled job. With this option, you must manually create a certification job later.

The new user certification definition is displayed in the Certification Definition page.

Note: For multi-phased review with advanced delegation:

- The certification is not 100% complete till the Phase 2 reviewers or technical reviewers have completed all the reviews. The certification status displays the phase and percentage completion in each phase the certification is in during the two phased review. To view this status, click the In Progress certification in the Inbox or Dashboard.
 - The certification goes to the Phase 1 primary reviewer for final review. In Page 2, the Phase 1 primary reviewer can review the actions made by the users in the first and second phases (greyed out) as well as the system-generated default actions, which the Phase 1 primary reviewer can override.
-

6.3.1.2 Creating a Role Certification Definition

To create a role certification definition:

1. On the left pane of Oracle Identity System Administration, under Certifications, click **Certification Definitions**. The Certification Definitions page is displayed.
2. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The General Details page of the New Certification wizard is displayed.
3. Enter values as follows:
 - **Name:** Enter a name for the certification.
 - **Type:** Select **Role** to create a role certification definition.

- **Description:** Optionally enter a description for the new role certification definition.
4. Click **Next**. The Base Selection page of the New Certification wizard is displayed.
 5. In the Base Selection section of the page, select a role selection strategy from the list, as shown:
 - **All Roles in All Organizations:** Selects all roles in all the organizations in Oracle Identity Manager.
 - **Roles from Selected Organizations:** Selects the roles from the organizations that you specify. Click Add to search and select an organization. To remove a selected organization, click Remove.

Note: When completing a certification, a certifier cannot see the organization name or any other details about the organization unless that person is also the organization administrator. If the certifier is not the organization administrator, only the users in the organization are displayed.

- **All Roles:** Selects all roles in Oracle Identity Manager.
- **Role criteria:** Selects all of the roles that meet the given search condition. You can preview the results of this selection.

Tip: You can save the search and use it for specifying role criteria while creating another role certification definition. The saved search is not mapped to a specific certification. To use the role criteria saved search for another role certification definition:

1. During certification creation, after selecting the **Role Criteria** option and specifying the search condition, you must click **Update and Preview Results**. This associates the selected criteria with the definition.
 2. If you want to save this search criteria as a template, then click **Save**. You are prompted to enter a name for the template that you are saving. You can then save this template and reuse it.
 3. The saved template is not specific to a certification. While creating another certification, this template is displayed by default. If you create another new template, then that template is displayed. In other words, the latest template is displayed for all criteria screens associated with a type of certification.
 4. If you do not want to use the generated template, then change the value in the Saved Search list to something else that you want to use.
- **Selected roles:** Allows you to manually select the roles.
6. Select any one of the following options to specify constraints:
 - Roles with Any Level of Risk:
 - Only High Risk Roles:
 7. Click **Next**. The Content Selection page is displayed.
 8. Select **Certify Policies** to specify the certification of policies. Select **Certify Members** to specify the certification of role members.
 9. Click **Next**. The Configuration page is displayed.

10. Select the configuration options, as described in [Table 6-1, "Configuration Properties"](#), and click **Next**. The Reviewers page is displayed.

From the Reviewer list, select a primary reviewer. The primary reviewer can be organization certifier, role certifier, or any other user that you select.

11. Click **Next**. The Incremental page is displayed.

12. Select **Enabled** for Generate Incremental Data. This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

When Incremental Certification is enabled, it takes the following parameters:

- **Incremental Date Range** (required): This includes:
 - **Since Last Base** (default): When this option is selected, current access of the user is compared against the last certification of the same type, which was created without enabling incremental and all the incremental certifications since then, to the current date when the certification is created.
 - **Since Date**: When this option is selected, current access of the user is compared against all the certifications of the same type since the given date and when the certification is created.
- **Show Previous Value** (optional): This includes:
 - **Disabled** (default): When this is deselected, then the values that have already appeared in the previous certifications based on the Incremental Date Range parameter are not included in the certification.
 - **Enabled**: When this is selected, all the current values that existed in previous certifications are displayed with the last decisions taken for those access.

13. Click **Next**. The Summary page is displayed with the details of the user certification.

14. Click **Create**. A message is displayed asking if you want to create a certification job based on the definition and run it now. You can edit the job name, and click **Yes** to run the certification job.

Alternatively, click **No** to create a certification definition without creating and running the scheduled job. With this option, you must manually create a certification job later.

The new role certification definition is displayed in the Certification Definition page.

6.3.1.3 Creating an Application Instance Certification Definition

To create an application instance certification definition:

1. On the left pane of Oracle Identity System Administration, under Certifications, click **Certification Definitions**. The Certification Definitions page is displayed.
2. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The General Details page of the New Certification wizard is displayed.
3. Enter values as follows:
 - **Name**: Enter a name for the certification.

- **Type:** Select **Application Instance** to create an application instance certification definition.
- **Description:** Optionally enter a description for the new application instance certification definition.
4. Click **Next**. The Base Selection page of the New Certification wizard is displayed.
5. In the Base Selection section of the page, select an application instance selection strategy from the list, as shown:
 - **All Application Instances:** Selects all application instances in Oracle Identity Manager.
 - **Selected application instances only:** Allows you to manually select the application instances. Click **Add** to search and select the application instances. To remove any selected application instance, click **Remove**.
6. Select any one of the following options to specify constraints:
 - Application Instances with Any Level of Risk
 - Only High Risk Application Instances
7. Click **Next**. The Content Selection page is displayed.
8. Select any one of the following:
 - **Accounts of Users from All Organizations:** Selects the accounts of users from all organizations in Oracle Identity Manager.
 - **Accounts of Users from Selected Organizations:** Allows you to manually select the organizations whose user accounts will be certified.
 - **Accounts of All Users:** Selects the accounts of all users in Oracle Identity Manager.
 - **Accounts of Selected Users:** Allows you to manually select the users whose accounts will be certified.
9. Click **Next**. The Configuration page is displayed.
10. Select the configuration options, as described in [Table 6-1, "Configuration Properties"](#), and click **Next**. The Reviewers page is displayed.
11. From the Reviewer list, select a primary reviewer. The primary reviewer can be application instance certifier, user manager, application instance certifier, organization certifier, or any other user that you select.
12. Click **Next**. The Incremental page is displayed.
13. Select **Enabled** for Generate Incremental Data. This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

When Incremental Certification is enabled, it takes the following parameters:

- **Incremental Date Range** (required): This includes:
 - Since Last Base (default): When this option is selected, current access of the user is compared against the last certification of the same type, which was created without enabling incremental and all the incremental certifications since then, to the current date when the certification is created.

- **Since Date:** When this option is selected, current access of the user is compared against all the certifications of the same type since the given date and when the certification is created.
 - Show Previous Value (optional): This includes:
 - **Disabled** (default): When this is deselected, then the values that have already appeared in the previous certifications based on the Incremental Date Range parameter are not included in the certification.
 - **Enabled:** When this is selected, all the current values that existed in previous certifications are displayed with the last decisions taken for those access.
14. Click **Next**. The Summary page is displayed with the details of the user certification.
15. Click **Create**. A message is displayed asking if you want to create a certification job based on the definition and run it now. You can edit the job name, and click **Yes** to run the certification job.
- Alternatively, click **No** to create a certification definition without creating and running the scheduled job. With this option, you must manually create a certification job later.
- The new application instance certification definition is displayed in the Certification Definition page.

6.3.1.4 Creating an Entitlement Certification Definition

To create an entitlement certification definition:

1. On the left pane of Oracle Identity System Administration, under Certifications, click **Certification Definitions**. The Certification Definitions page is displayed.
2. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The General Details page of the New Certification wizard is displayed.
3. Enter values as follows:
 - **Name:** Enter a name for the certification.
 - **Type:** Select **Entitlement** to create an entitlement certification definition.
 - **Description:** Optionally enter a description for the new entitlement certification definition.
4. Click **Next**. The Base Selection page of the New Certification wizard is displayed.
5. In the Base Selection section of the page, select a role selection strategy from the list, as shown:
 - **Selected entitlements** - Allows you to manually select the entitlements. Click Add to search and select the entitlements. To remove any selected entitlement, click **Remove**.
 - **All Entitlements with Selected Certifiers:** Allows you to select a list of users including all the entitlements for which they are the certifier user in the catalog.
6. Select any one of the following options to specify constraints:
 - Entitlements with Any Level of Risk
 - Only High Risk Entitlements

7. Click **Next**. The Content Selection page is displayed.
8. Select any one of the following:
 - **Accounts of Users from All Organizations:** Selects the accounts of users from all organizations in Oracle Identity Manager.
 - **Accounts of Users from Selected Organizations:** Allows you to manually select the organizations whose user accounts will be certified.
 - **Accounts of All Users:** Selects the accounts of all users in Oracle Identity Manager.
 - **Accounts of Selected Users:** Allows you to manually select the users whose accounts will be certified.
9. Click **Next**. The Configuration page is displayed.
10. Select the configuration options, as described in [Table 6-1, "Configuration Properties"](#), and click **Next**. The Reviewers page is displayed.
11. From the Reviewer list, select a primary reviewer. The primary reviewer can be entitlement certifier or any other user that you select.
12. Click **Next**. The Incremental page is displayed.
13. Select **Enabled** for Generate Incremental Data. This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

When Incremental Certification is enabled, it takes the following parameters:

- **Incremental Date Range** (required): This includes:
 - **Since Last Base** (default): When this option is selected, current access of the user is compared against the last certification of the same type, which was created without enabling incremental and all the incremental certifications since then, to the current date when the certification is created.
 - **Since Date:** When this option is selected, current access of the user is compared against all the certifications of the same type since the given date and when the certification is created.
 - **Show Previous Value** (optional): This includes:
 - **Disabled** (default): When this is deselected, then the values that have already appeared in the previous certifications based on the Incremental Date Range parameter are not included in the certification.
 - **Enabled:** When this is selected, all the current values that existed in previous certifications are displayed with the last decisions taken for those access.
14. Click **Next**. The Summary page is displayed with the details of the user certification.
 15. Click **Create**. A message is displayed asking if you want to create a certification job based on the definition and run it now. You can edit the job name, and click **Yes** to run the certification job.

Alternatively, click **No** to create a certification definition without creating and running the scheduled job. With this option, you must manually create a certification job later.

The new entitlement certification definition is displayed in the Certification Definition page.

6.3.2 Modifying Certification Definitions

To modify a certification definition:

1. In the left pane of Oracle Identity System Administration, under Certifications, click **Certification Definitions**. The Certification Definitions page is displayed with a list of all certification definitions.
2. Select the certification definition that you want to modify.

Note: If there is a periodic scheduled task tied to this definition, then the next execution of the scheduled task will be run by using the modified changes.

3. From the Actions menu, select **Edit**. Alternatively, you can click **Edit** on the toolbar.

A message is displayed stating that the definition is referenced by scheduled jobs and event listeners and asking for confirmation. This message is not displayed if you try to edit a certification definition for which you have not created certification jobs.

4. Click **Edit** to confirm. The Certification Definition pages are displayed on which you can edit the values in the fields.
5. Edit the fields to modify the certification definition by navigating through the pages by clicking the **Next** and **Back** buttons.
6. When finished, click **Save**. A message is displayed stating that the definition has been successfully updated.
7. Click **OK**.

6.3.3 Deleting Certification Definitions

To delete a certification definition:

1. In the left pane of Oracle Identity System Administration, under Certifications, click **Certification Definitions**. The Certification Definitions page is displayed with a list of all certification definitions.
2. Select the certification definition that you want to delete.
3. From the Actions menu, select **Delete**. Alternatively, you can click **Delete** on the toolbar.

A message is displayed stating that the definition is referenced by scheduled jobs and event listeners and asking for confirmation. This message is not displayed if you try to delete a certification definition for which you have not created certification jobs.

4. Click **Delete** to confirm. A message is displayed asking for confirmation.
5. Click **OK**.

6.4 Scheduling Certifications

Certifications are scheduled as part of the certification creation process. For more information, see ["Creating Certification Definitions"](#) on page 6-9. Certifications can be scheduled to run once, or to repeat on a daily, weekly, or monthly basis.

Note: You must create a certification definition before you can schedule it. See ["Creating Certification Definitions"](#) on page 6-9.

After you create a certification definition by clicking Create on the Summary page of the New Certification wizard, a message is displayed asking if you want to create a certification job and run it. You can edit the scheduled job name in the Job Name box. When you click Yes, the certification job is created for the new certification definition and is run. You can go to the Scheduler section in Oracle Identity System Administration and search for the job. The default name of the job is `Cert_DEFINITION_NAME`.

The certification job is created based on the Certification Creation Task scheduled task. This scheduled task is used to create new certification jobs for a defined certification definition. When the job runs, the certification definition is used and certifications are generated.

See ["Predefined Scheduled Tasks"](#) on page 15-7 for information about the Certification Creation Task scheduled task. You can modify the certification jobs from the Scheduler section of Oracle Identity System Administration. See ["Modifying Jobs"](#) on page 15-26 for details.

You can also schedule a certification from the Scheduler section of Oracle Identity System Administration. To do so, follow the instructions in ["Creating Jobs"](#) on page 15-22. In this method, select Certification Creation Task in the Task field in the Create Job page.

When you modify a certification job, specify the certification definition name in the Certification Definition Name field of the Job Details page.

6.5 Understanding How Risk Summaries are Calculated

You can directly assign high, medium, and low risk levels to roles, application instances, and entitlements, as well as to certain predefined risk factors. A risk-aggregation job calculates Risk Summaries for the remaining higher-order data objects that are required to support identity certification. These objects include every user, user-role assignment, account, and entitlement-assignment in Oracle Identity Manager. During identity certification, certifiers use Risk Summaries to separate high-risk certification items from medium-risk and low-risk items.

This section describes how the system processes risk levels to arrive at Risk Summaries. It also describes the risk-aggregation job, which you can run manually or on a scheduled basis.

Note: Roles, application instances, and entitlements are *metadata* objects, whereas users, accounts, and entitlement-assignments are *instance-data* objects.

Metadata objects are structural objects that represent and describe your information systems within Oracle Identity Manager, whereas instance-data objects are the individual instances of application data that populate the systems. For example, consider a customer service application (a resource) that has a predefined role that enables users to create trouble tickets (an entitlement). In this example, a single resource object represents the application and a single entitlement object represents a specific privilege within that application.

Now consider there might be thousands of user accounts on this resource, some subset of which has the entitlement-assignment that allows the user to create a trouble ticket. A single resource (metadata object) can have multiple accounts (instance-data objects), and a single entitlement (metadata object) can have multiple assignment instances (instance-data objects). Oracle Identity Manager calculates the risk levels for instance-data objects because it would not be feasible for a human to process risk levels for every user, account, and entitlement-assignment on a recurring basis.

6.5.1 Understanding Item Risk and Risk-Factor Mappings

Item risk and the risk-factor mappings are settings that are under your direct control.

6.5.1.1 Setting Item Risk

Item risk refers to the risk levels that you and other administrators can assign to specific roles, application instances, and entitlements.

Note: Three bars signifies high risk, two bars signifies medium risk, one bar signifies low risk.

If you do not directly assign an item-risk level to a metadata object, then Oracle Identity Manager assigns a default item-risk level for you. Roles, application instances, and entitlements can each have a default value.

To set the default item-risk level for the metadata objects:

1. Login to Oracle Identity System Administration.
2. On the left pane, under Certifications, click **Risk Configuration**.
3. Select the High, Medium, or Low risk radio buttons for each item.
4. Click **Save**.

You should reserve high item-risk levels for metadata objects that confer highly-restricted privileges to users. Note that setting a high item-risk level on an object will cause its parent object to also have a high Risk Summary value. Similarly, setting a medium item-risk level on an object will cause its parent object to have at least a medium Risk Summary value. In order for a higher-order object to have a low Risk Summary value, all of the objects under it in the system hierarchy would have to have low risk settings.

6.5.1.2 Understanding Risk-Level Mappings (Risk Factors)

Risk-Factor Mappings are settings that map risk levels to certain predefined conditions. For example, you might configure "items with open audit violations" as high risk, whereas "items that are closed as risk-accepted" you might configure as medium risk.

Generally speaking, you should reserve high Risk-Factor levels for conditions in which privileges are being extended to users that may be irregular or dangerous.

There are three Risk-Factor categories in Oracle Identity Manager, and each category contains multiple settings. Risk-Factor categories are described in the following table.

Table 6–2 Risk Factors

Risk Factor	Description
Provisioning Scenarios / Assignment Scenarios	<p><i>Provisioning Scenarios</i> define the risk levels that should be associated with the method or mechanism used to assign a role, account, or entitlement-assignment to a user.</p> <p>For example, you might configure a risk level of <i>Medium</i> for objects that are provisioned directly by an administrator, and a risk level of <i>Low</i> for objects that are provisioned based on Policies that are tied to Roles. You might configure a risk-level of <i>High</i> for objects that are pulled into Oracle Identity Manager via reconciliation.</p>
Last Certification Action	<p>Defines risk level based on the status of the last certification for the account, entitlement-assignment, or user-role assignment under consideration.</p> <p>For example, configure a risk level of <i>Low</i> for any item for which the previous certification decision was to approve, and configure a risk level of <i>Medium</i> for any item for which the previous certification decision was to <i>Certify Conditionally</i>. Finally, you might configure a value of <i>High</i> for any item for which the previous certification decision was <i>Abstain</i> or <i>Revoke</i>.</p>

Note: Changing Risk-Level mappings on the Configuration page in the UI can cause major ripple effects that impact Risk Summaries throughout Oracle Identity Manager. During your initial setup you should configure mappings on the Risk Level configuration page, and then avoid making additional unnecessary changes. See ["Understanding How Changing Risk Configuration Values Impacts the System"](#) on page 6-22 for more information about the ripple effects that impact Risk Summaries.

6.5.2 Understanding Risk Aggregation and Risk Summaries

The Risk Aggregation Task scheduled job processes Item-Risk levels and Risk-Factor levels, and calculates Risk Summaries for each higher-order object that supports identity certification.

Risk aggregation Task is used to seed the predefined Risk Aggregation Job. You do not need to create new jobs using this task. When a job of this task type runs, it calculates the risk of all the users in Oracle Identity Manager since they have been last updated. See ["Predefined Scheduled Tasks"](#) on page 15-7 for information about this scheduled task. You can enable the Risk Aggregation Task scheduled job by following the instructions in ["Disabling and Enabling Jobs"](#) on page 15-26.

In the first phase of risk aggregation, the Risk Aggregation Task scheduled job evaluates each individual object's Item-Risk level and its three Risk-Factor levels, and assigns the highest of the four levels to the object's Risk Summary property. A Risk Summary value is calculated for each individual User object, User-Role Assignment object, Account object, and entitlement-assignment object. The following diagram illustrates this process.

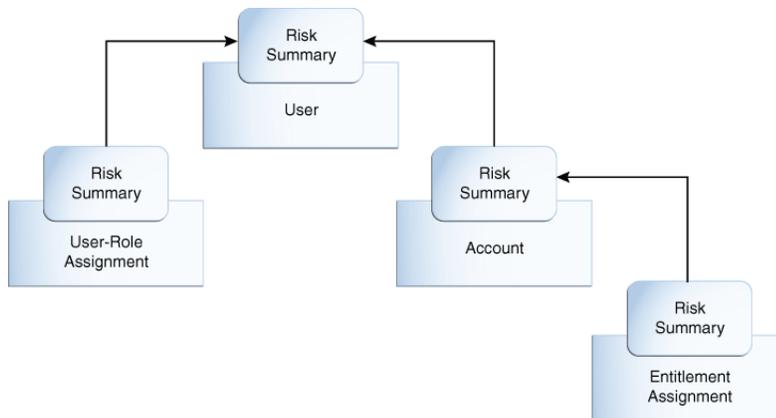


Once Risk Summaries are calculated for every object, the next phase of aggregation begins, in which the Risk Summary of each individual object rolls up to the Risk Summary of the parent object that contains it.

Above the entitlement-assignment level, each data object's Risk Summary value contributes to the Risk Summary of the parent-object that contains it. For example, Account objects are one hierarchy-level up from entitlement-assignment objects, and User objects are one hierarchy level up from there. So, the Risk Summary of every entitlement-assignment object within an Account object contributes to the Risk Summary for that Account, and, similarly, the Risk Summary for every Account object within the User object contributes to the Risk Summary for that User.

User objects are also one level above User-Role Assignment objects, so the Risk Summary for every User-Role Assignment object contributes to the Risk Summary for that User.

The following diagram illustrates this process.



In the diagram, the Risk-Summary value of the entitlement-assignment rolls up to the Account object. The Risk-Summary values of Accounts and the Risk-Summary values of User-Role Assignments roll up to the Risk Summary of any associated User.

6.5.3 Understanding How Changing Risk Configuration Values Impacts the System

There are three main actions or system events that can impact Risk Summary values. Depending on the action or system event, the impact can be minor, moderate, or major. Each action or event and its consequences is described in the following table.

Table 6–3 *Actions or System Events That can Impact Risk Summary Values*

Action or Event	Impact	Description
Users and/or Oracle Identity Manager make changes to individual entitlements	Minor	<p>Applies to changes to individual data objects, such as accounts, entitlements, and user-role assignments. These values might change frequently. For example, the following types of changes are included in this category:</p> <ul style="list-style-type: none"> ■ An attribute value is added to or removed from an account. ■ An account is added to or removed from a user. ■ A role assignment is added to or removed from a user. ■ A risk factor on an individual data object changes. <p>The impact within Oracle Identity Manager is relatively minor because the changes happen at the level of each individual entitlement.</p>
An administrator makes item-risk changes to roles, resources, and entitlements	Moderate	<p>Applies to situations where you or another administrator change the risk-level of a role, an application instances, or an entitlement.</p> <p>The ripple-effect of these changes can be large. Changing the risk level on a metadata object can change the item-risk level on every data-object associated with the metadata object. Changing the risk level on a data-object may affect its risk summary and, in turn, the risk summary of every other data-object that contains it.</p> <p>For example, changing the risk level on an entitlement definition will change the Item Risk on every assignment of that entitlement that corresponds to it. Changing the Item Risk on an entitlement-assignment may change its Risk Summary. Changing the Risk Summary of an entitlement-assignment may affect the Risk Summary of the parent Account. Changing the Risk Summary of an Account may affect the Risk Summary of the User who owns the Account.</p>
An administrator makes configuration changes to the Risk-Level Mappings	Major	<p>Applies to situations where you or another administrator change the Risk-Level Mappings on the Risk Configuration page in Oracle Identity System Administration.</p> <p>Changing the risk level associated with a specific value of a specific risk factor could affect the risk summary of any user-role assignment, account, or entitlement-assignment that has that risk-factor value. Changing the risk summary of any user-role assignment, account, or entitlement assignment could in turn affect every user associated with an affected user-role assignment, account, or entitlement assignment.</p> <p>For this reason, you should change risk-level mappings only rarely.</p>

6.6 Understanding Closed-Loop Remediation and Remediation Tracking

Closed-loop remediation is a feature that allows you to directly revoke roles and entitlements from the provisioning solution as a result of roles and entitlements revoked during the certification process.

When a certification is complete and all primary review tasks have been signed off, Oracle Identity Manager attempts to remove every user and privilege for which the final decision was to revoke. Requests are created to de-assign any role-assignment that is revoked, to de-provision any account that is revoked, to remove any entitlement-assignment that is revoked, and to delete or disable any user that is revoked. Specifically:

- Revoking a user deletes/disables the user and removes all privileges of that user.
- Revoking a user's role-assignment removes that member from the role. This might eventually cause provisioning to remove accounts and entitlement-assignments granted by the role (if those accounts and entitlement-assignments are not otherwise granted to the user.)
- Revoking a user's account deletes/disables the account. This implicitly removes/disables any entitlement-assignments associated with that account.
- Revoking a user's entitlement-assignment removes the assignment from the account that contains it.

The remediation status can be tracked in the request catalog for auditing purposes. Each remediation-request contains the certification ID of the certification that spawned the request, which allows the Dashboard to link to the Track Requests page of Oracle Identity Self Service to display the status of all the requests associated with the certification that is being displayed.

6.6.1 Configuring Challenge Workflows

By default, closed-loop remediation functions in the following way:

- If the person who signed-off the certification (final reviewer) is the user's (beneficiary's) manager, then the requests are auto-approved.
- If the final reviewer is not the user's manager, then the requests go through a challenge workflow, which is as follows:
 1. A request is sent to the user (beneficiary) whose access is revoked.
 2. If the beneficiary accepts the revoke by approving the request, then closed-loop remediation takes place and access is revoked.
 3. If the beneficiary challenges the revoke by rejecting the request, then the request is sent back to the person who signed off the certification (final reviewer).
 - a. If the final reviewer accepts the challenge, then the process stops and the beneficiary's access is not revoked.
 - b. If the final reviewer rejects the challenge, then closed-loop remediation takes place and the access is revoked.

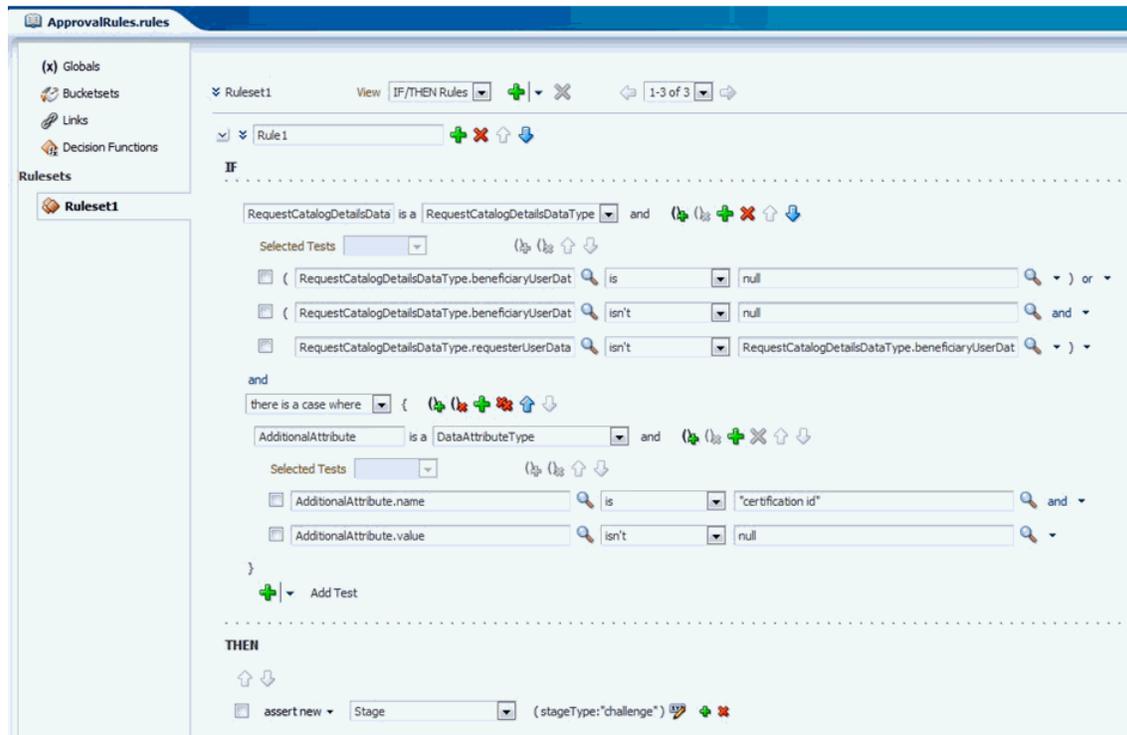
This logic is defined within the DefaultRequestApproval composites in SOA by using rules. You can modify the rules to have all the closed-loop remediation requests to be auto-approved. To do so:

1. Login to Oracle SOA Composer with Admin credentials, such as weblogic, by navigating to the following URL:

`http://HOST_NAME:PORT_NUMBER/soa/composer`

2. Click **Open**, and select **Open Rules**. The Select a Dictionary to open dialog box is displayed.
3. For the DefaultRequestApproval_rev2.0 composite, click **Ruleset1** in the Contents column.
4. Click **Edit**.
5. Expand Rule 1, as shown in [Figure 6-1](#):

Figure 6-1 Rule for Auto-approval



6. Under THEN, click the pencil icon.
7. In the pop-up, change the value from challenge to auto. This value specifies that all the closed-loop remediation requests will be auto-approved, and the challenge workflow will not be invoked.
8. Click **OK**.
9. Click **Save**, and then click **Commit**.

6.7 Understanding Event Listeners

The Event Listener mechanism allows an administrator that detects specific business events and stores the event details for certification. The stored event details are called Certification Event Triggers, and these are processed into certifications by the Certification Event Trigger Task, running as a scheduled job. The business events currently detected by event listeners are modifications of OIM users, either individually or in bulk. Listeners currently generate user certifications or application instance certifications.

Every event listener contains a ruleset and a certification definition, as described in ["Managing Certification Definitions"](#) on page 6-9. The ruleset contains one or more rules, each of which tests one or more conditions and specifies an action to take if its conditions are met. The standard action for event listener rules is to store a Certification Event Trigger that identifies the event listener, the user or users that were modified, and the certification definition that should be generated in response to this event.

Triggers accumulate between runs of the Certification Event Trigger Job. When the job runs, it groups the triggers by their event listener identifiers, and then processes each group according to the corresponding event listener's properties. By default, the trigger job creates a certification for all users in each group of triggers, using the listener's certification definition as the template for the certification. After this, the triggers from the completed group are deleted.

There are several properties that affect how an event listener's triggers will be processed by the trigger job. The first property determines whether the listener is in active or disabled state. If a listener is disabled, then its rules are no longer evaluated when business events occur, and therefore, no triggers are stored from that listener. If a listener stored triggers before being disabled, then the next trigger job run deletes those triggers without processing them. When a disabled listener is set back to active state, it can once again store triggers that are processed by the trigger job.

Another event listener property that affects trigger processing is its Event Count, which limits how many triggers may be processed for the listener during a single run of the trigger job. This setting is optional. If it is not specified, then the number is unlimited. If the event count is specified, then it represents the maximum number of triggers that may be processed. When the trigger job runs, it checks the listener's event count for each batch of triggers, and if the number of triggers exceeds the event count, then the triggers are discarded without generating a certification. This feature is useful for preventing huge certifications from being created when users are modified in bulk.

Finally, the trigger job itself may be configured to process the triggers from certain event listeners, but not others. This feature is controlled by a Certification Event Trigger Task parameter titled Event Listener Name List. If this parameter is left blank in the definition of the trigger job, then triggers from all listeners are processed when the trigger job runs. If the name list is defined, then only the listeners in that list have their triggers processed when the job runs; triggers from other listeners are ignored and retained for future trigger job runs. When multiple instances of scheduled jobs are defined for the Certification Event Trigger Task, then each list of event listeners can have its triggers processed on the most appropriate schedule.

Note: If a listener name appears in more than one Event Listener Name List, or if one of the trigger jobs has an empty Event Listener Name List, then the first of these jobs to run consumes all of that listener's triggers. Triggers are always discarded after the first time they are processed.

6.8 Configuring Event Listeners and Certification Event Trigger Jobs

This section contains the following topics:

- [Creating an Event Listener](#)
- [Modifying an Event Listener](#)
- [Deleting an Event Listener](#)

- [Configuring Certification Event Trigger Jobs](#)

Note: Event listeners are supported for user and application instance certifications.

6.8.1 Creating an Event Listener

To create a new event listener:

Note: Before creating an event listener, you must create a user certification definition or an application instance definition that will be executed when the Certification Event Trigger job is run.

1. Login to Oracle Identity System Administration.
2. In the left pane, under Certifications, click **Event Listeners**. The Event Listeners page is displayed.
3. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Event Listener page is displayed.
4. In the Listener Properties section, specify the name with which the event will be identified, and the description.
5. From the Certification Definition list, select a certification definition that will be executed.
6. In the Event Count box, enter the maximum number of events that should be processed for this listener at the time the Certification Event Trigger Job runs. Use this to avoid executing an action for bulk updates.
7. From the Status list, select Active or Disabled status.
8. In the Event Trigger section, add a rule containing conditions that will be evaluated when an event takes place. For example, when a user is updated, a condition can check if the user's title property or location property has changed. Another example can be change of manager for a user.

To add a condition:

- a. Click the plus (+) icon, and change Rule 1 to a rule name, for example, Manager Change Condition.
- b. Click the expand icon to the left of the condition.
- c. Click the lookup icon to open the Condition Browser.
- d. Click **Modified User, previousValue**. Select **manager**, and click **OK**. This sets `ModifiedUser.previousValue.Manager`.
- e. Select the condition operation, such as **isn't**.
- f. Click the second lookup icon, search and select the attribute name and click **OK**, so that the following condition is set:
`ModifiedUser.previousValue.Manager isn't ModifiedUser.currentValue.Manager`
- g. Under THEN, click the plus (+) icon to the left of Add Action.
- h. Click the down arrow key and select **call**.
- i. From the list, select **certifyThisUser**.

9. Click **Create** to create the event listener.

When the Certification Event Trigger job is run, a certification will be created for a user whose manager has changed.

An example of the event listener rule can be to check for an attribute's change to a specific value. For example:

```
ModifiedUser.previousValue.country isn't ModifiedUser.currentValue.country and  
ModifiedUser.currentValue.country is "Brazil"
```

`ModifiedUser.previousValue.country isn't ModifiedUser.currentValue.country` checks for a change in the Country attribute. Any change causes this condition to evaluate to TRUE. Then, `and ModifiedUser.currentValue.country is "Brazil"` adds a second condition to the rule. This checks whether the attribute has changed to a specific value, for example Brazil. This condition is applicable if some special certification is required for employees moving to Brazil. For other employees who have moved to some other place, the rule's action is not triggered.

6.8.2 Modifying an Event Listener

To modify an event listener:

1. On the left pane of Oracle Identity System Administration, under Certifications, click **Event Listeners**. The Event Listeners page is displayed with a list of event listeners.
2. Select the event listener that you want to modify.
3. From the Actions menu, select **Edit**. Alternatively, click **Edit** on the toolbar. The event listener details page is displayed.
4. Edit the values in the fields to modify the event listener.
5. Click **Save**.

6.8.3 Deleting an Event Listener

To delete an event listener:

1. On the left pane of Oracle Identity System Administration, under Certifications, click **Event Listeners**. The Event Listeners page is displayed with a list of event listeners.
2. Select the event listener 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 **Yes** to confirm.

6.8.4 Configuring Certification Event Trigger Jobs

As mentioned in "[Understanding Event Listeners](#)" on page 6-25, the Certification Event Trigger Job offers an optional parameter called Event Listener Name List. If one or more event listener names are supplied in this field, then the trigger job will only process the triggers for those listeners, which implies that you will need multiple trigger jobs to cover processing for your full set of listeners. The sections describes how to set this parameter and how to define multiple trigger jobs. It contains the following sections:

- [Setting the Event Listener Name List](#)

- [Adding More Trigger Jobs](#)

6.8.4.1 Setting the Event Listener Name List

To set the Event Listener Name List:

1. Login to Oracle Identity System Administration.
2. On the left pane, under System Management, click **Scheduler**.
3. In the search field, enter `Certification Event Trigger Job`, and perform the search.
4. Click the job name in the search result to display the trigger job details.
5. Scroll down to the Parameters section, where you can see a parameter titled Event Listener Name List (comma separated).
6. Enter one or more event listener names in this field, separated by commas. Make sure to type each listener's name exactly as it appears in the Name column of the Event Listeners table.
7. Click **Apply** to save the changes.

6.8.4.2 Adding More Trigger Jobs

In addition to the predefined instance of the Certification Event Trigger Job, you can create new trigger job instances by performing the following steps:

1. Login to Oracle Identity System Administration.
2. On the left pane, under System Management, click **Scheduler**.
3. On the left pane, from the Actions menu, select **Create**. Alternatively, you can click the icon with the plus (+) sign beside the View list.
4. In the Create Job panel, expand the Task field by clicking the icon to its right.
5. In the Search field, enter `Certification Event Trigger Task`, and perform the search.
6. In the search result, click the Certification Event Trigger Task row, and then click **Confirm**.
7. Enter the Job Name and any desired scheduling details for this trigger job instance.
8. In the Event Listener Name List field, enter a comma-separated list of the listener names that this trigger job instance will process.

Every instance of the trigger job can have its own schedule or can be run manually, and can be restricted to handling triggers for a specified subset of listeners. This enables you to trigger different event listeners at different intervals.

6.9 Configuring Certification Reports

Certification reports are implemented in Oracle BI Publisher. When you configure BI Publisher reports for certification, the Reports tab is displayed in the Detailed Information section of the Dashboard.

Note:

- Oracle Identity Manager reports must be deployed on BI Publisher. See "Generating Certification Reports" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about the default certification reports and generating certification reports.
 - If BI Publisher credentials and URL are not configured in Oracle Identity Manager, then the Reports tab in the Dashboard and the Export to PDF or Excel option in the Certification page are not available.
-

To configure BI Publisher URL:

1. Login to Oracle Enterprise Manager.
2. Click **Identity and Access**.
3. Select **OIM cluster, OIM node, System MBean Browser**.
4. In the System MBean Browser, navigate to **Application Defined MBeans, oracle.iam, Server: oim server, Application: oim, XMLConfig, Config, XMLConfig.DiscoveryConfig, Discovery**.
5. Update the value of the BIPublisherURL attribute with BI Publisher URL.
6. Click **Apply**.

To configure BIP credentials in Oracle Identity Manager:

1. Log in to Oracle Enterprise Manager.
2. In left pane, expand **Weblogic Domain**. The domain name is displayed.
3. Right-click the domain name, and navigate to **Security, Credentials**. A list of maps in the credential store, including the oim map, is displayed.
4. Expand the oim map. A list of entries of type Password is displayed.
5. Create a new CSF entry in the oim credential store map, as follows:
 - Select Map: oim
 - Key: BIPWSKey
 - Type: Password
 - Username: *ADMINISTRATOR_USER_NAME*
 - Password: *ADMINISTRATOR_PASSWORD*
 - Description: Login credentials for BI Publisher web service.

Reports can be generated in the following formats:

- PDF
- RTF
- HTML
- Microsoft Excel
- CSV

6.10 Understanding Multi-Phased Review in User Certification

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.

Note: Oracle Identity Manager supports TPAD for user certification only. TPAD is not supported for role certification, application instance certification, and entitlement certification.

This section describes TPAD in the following sections:

- [Multiple Phases of Review](#)
- [Delegation to Multiple Reviewers Within Each Phase](#)
- [Stages of Certification in TPAD](#)

6.10.1 Multiple Phases of Review

Multiple phases of review combines multiple perspectives on the same set of user-access-privileges. For user certification, the phases are:

- **Business Review:** This is the required first phase of review. The business reviewer, typically the manager of each user, views all the certifiable access privileges of a user. First, the manager confirms that the user is a valid holder of privileges, such as an employee, within that enterprise. Then the manager confirms that the user's position within the enterprise justifies the user's access privileges, such as role assignments, account assignments, and entitlement assignments. The business reviewer certifies or approves any privilege that seems appropriate and revokes any privilege that seems unnecessary or unreasonable.
- **Technical Review:** This is an optional second phase of review. The technical reviewer, typically the owner or an authorizer of each privilege, reviews the members of the privilege or the assignments of that privilege to specific users or to specific accounts of specific users. The technical reviewer certifies or approves any privilege that seems appropriate and revokes any assignment of that privilege that seems unnecessary or unreasonable.
- **Final Review:** This is an optional final phase review. If the certification is configured to enable final review, then the primary reviewer from the first phase, for example the manager of each user, can see the decisions that reviewers made in the first two phases and can override those decisions if required.

See Also: "Who Is Involved in Completing Identity Certifications?" in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about primary reviewer, technical reviewer, final reviewer, and delegated reviewer.

6.10.2 Delegation to Multiple Reviewers Within Each Phase

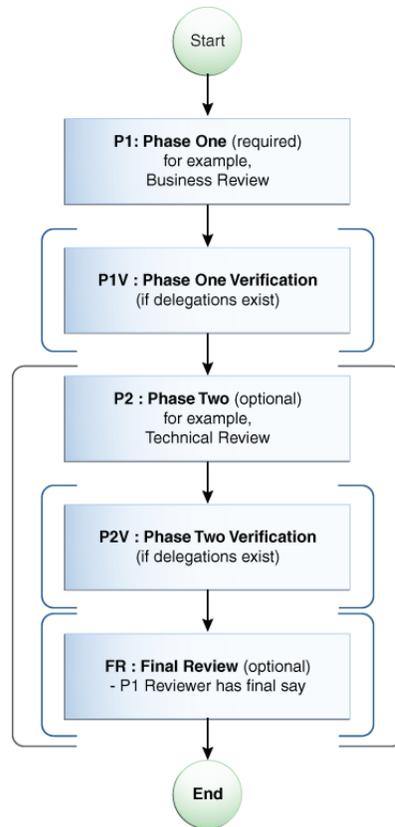
The primary reviewer in Phase One or Phase Two can spread the work to other users in the following ways:

- The primary reviewer can reassign responsibility for any set of line items to another user. Reassignment transfers the responsibility to another person, whereas delegation retains the responsibility with the primary reviewer. Reassignment of a certification task in Phase One creates a new certification.
- The primary reviewer can delegate each line-item, or any set of line-items, to any user that the primary reviewer selects. This user is called a delegated reviewer. Delegating a line-item marks that line-item as delegated in the primary reviewer's task, and prevents the primary reviewer from acting on that line-item.
- The primary reviewer can undelegate any delegated line-item at any time within the phase before signing off the certification task. Undelegating a line-item removes it from the delegated reviewer's task, and allows the primary reviewer to act on the line-item, for example, by making certification-decisions or delegating or reassigning it.

In Phase One or Phase Two, whenever the primary reviewer delegates line-items and signs off with at least one line-item still delegated, which means that the primary reviewer has not undelegated all of those line-items before signing off, then Oracle Identity Manager generates a review task for Phase-One Verification or Phase-Two Verification, and assigns this task to the primary reviewer. This task allows the primary reviewer to see and override any decision that a delegated reviewer made in that phase.

6.10.3 Stages of Certification in TPAD

[Figure 6–2](#) illustrates the stages of certification in TPAD by combining the required Phase One, the optional Phase Two, and the optional Final Review phase that depends on Phase Two, with the conditional verification tasks.

Figure 6–2 Stages of Certification in TPAD

As shown in [Figure 6–2](#), the overall sequence of stages within TPAD certification are:

1. **start:** Certification is created, and certification task is generated by running the Certification Creation Task scheduled job.
2. **Phase One Review:** This is always required.
3. **Phase One Verification:** This takes place only if Phase One is completed with delegations.
4. **Phase Two Review:** This is optional depending on configuration.
5. **Phase Two Verification:** This takes place only if Phase Two is completed with delegations.
6. **Final Review:** This is optional depending on configuration and takes place only if Phase Two is completed.
7. **end:** Certification task is completed. If any access has been revoked as a part of the certification completion, then closed-loop remediation takes place.

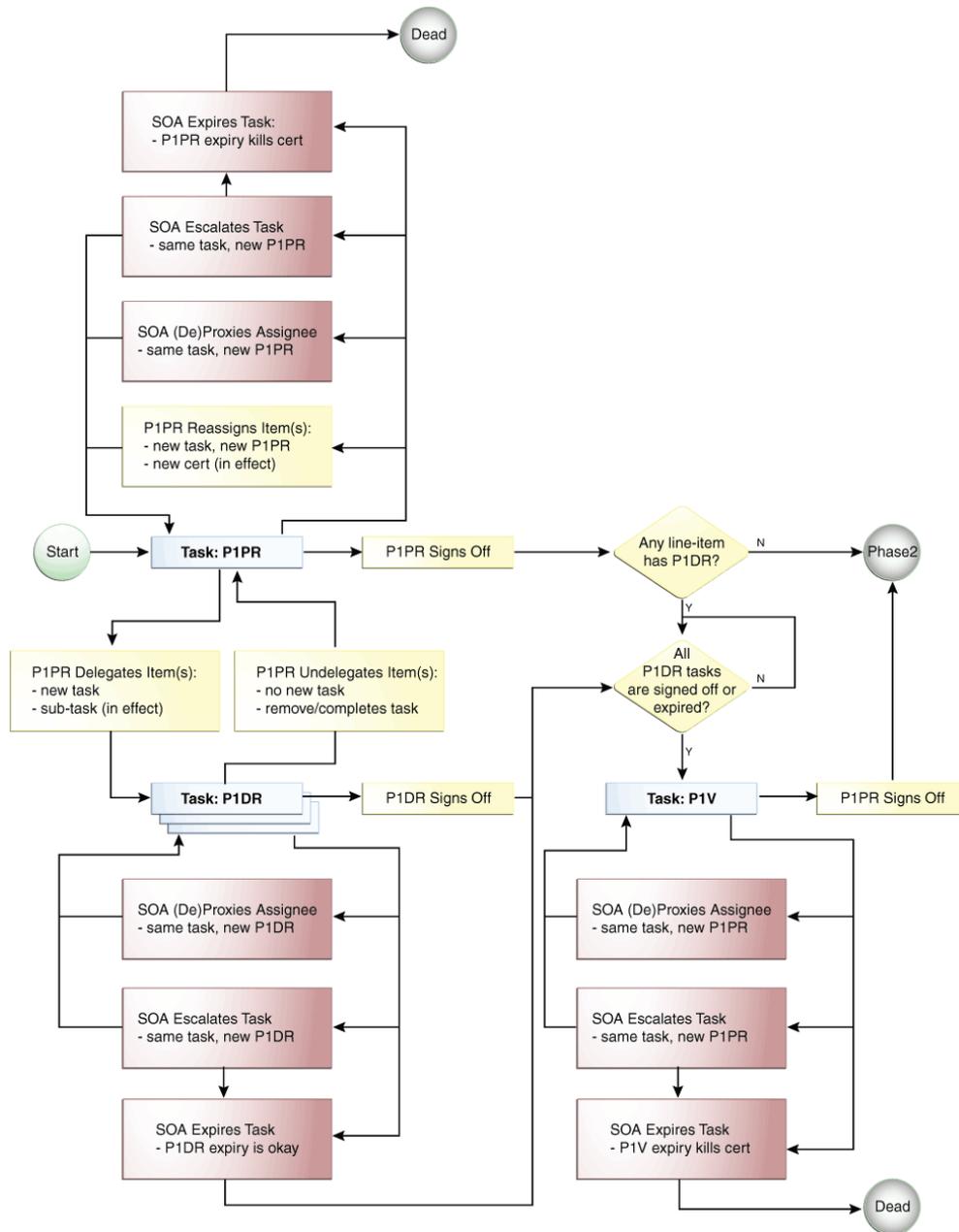
The certification stages in TPAD are described in the following sections:

- [Phase One With Verification](#)
- [Phase Two With Verification](#)
- [Final Review](#)

6.10.3.1 Phase One With Verification

[Figure 6–3](#) shows the first phase of certification review with TPAD.

Figure 6-3 Phase One With Verification



Following is the process flow of the Phase One review with verification in TPAD:

1. **Start:** A set of certification objects are generated, and the review process starts. Every line-item within each particular certification object is assigned to a Phase One Primary Reviewer (P1PR).
2. **Task P1PR:** When the scheduled jobs for certification generation are run, Oracle Identity Manager uses Service-Oriented Architecture (SOA) to create a task, for each certification object, which is assigned to the Phase One Primary Reviewer (P1PR).

When the primary reviewer opens the task, the primary reviewer can see every line-item within the certification object. If the primary reviewer opens any

particular line-item, then the primary reviewer can see every line-item-detail for that line-item.

The primary reviewer can act on any line-item within the task. The primary reviewer can delegate any line-item to another person, or can reassign any line-item to another person. By default, the primary reviewer owns every line-item and can decide, such as certify or revoke, the line-item-details.

After decision has been made for each line-item, or each detail for the line-item has a Phase-One Decision, or has been delegated or reassigned, the primary reviewer can sign off or complete the task.

3. **P1PR Reassigns Item(s):** If the primary reviewer during Phase One reassigns any set of line-items to another person, then Oracle Identity Manager removes those reassigned line-items (and their details) from the original certification and puts them into a new and separate certification. The person to whom the line-items were reassigned becomes the P1PR for that new and separate certification.

The reassigned line-items disappear from the task of the original P1PR, and does not reappear within this review process. Even if the new P1PR reassigns or delegates the line-items back to the original P1PR, this creates a new task for the original P1PR so that it is part of a different review process in the following way:

- If the new P1PR reassigns line-items back to the original P1PR, this will be a new certification with its own P1PR task.
 - If the new P1PR delegates the line-items back to the original P1PR, then this will be a new delegated review (P1DR) task within the review-process of the new P1PR.
4. **P1PR Delegates Item(s):** If the primary reviewer delegates any set of line-items to another person, then that person is the phase one delegated reviewer (P1DR) for each of those line-items. A new task is created and assigned to the new P1DR.

Note: In order to minimize the number of tasks, it is recommended that you select the set of line-items that you intend to delegate to a particular reviewer. Otherwise, the delegated reviewer can receive any number of tasks, each of which contains some subset of line-items from the same phase of the same certification object.

When the primary reviewer delegates a particular set of line-items, the line-items are marked as delegated within the task from which the primary reviewer delegated them. The primary reviewer can no longer act within that task on those line-items unless the primary reviewer undelegates them. The primary reviewer has an opportunity during Phase One Verification to see and override the decisions made by any delegated reviewer.

5. **P1PR Undelegates Item(s):** The primary reviewer can undelegate or take back from a delegated reviewer any line-item that is delegated. Undelegating a line-item allows the primary reviewer to act on that line-item and removes that line-item from the task of the current delegated reviewer, which prevents the delegated reviewer from acting on it further.
6. **P1PR Signs Off:** After every line-item has been completed or delegated or reassigned, the primary reviewer can sign off on the task, which completes the task. A line-item is completed when all of its details have a decision for the current phase. At this point, Oracle Identity Manager determines whether or not Phase One Verification (P1V) is required.

7. **SOA (De)Proxies Assignee (P1PR):** A proxy can be assigned for the assigned reviewer, such as P1PR. For example, when the reviewer is scheduled to go on vacation, the reviewer can activate a proxy. When the reviewer returns from vacation, the proxy is deactivated. When the newly assigned (proxy) reviewer opens the task, the proxy reviewer can view and act on each line-item and line-item-details. See "Managing Proxies" in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about adding, modifying, and removing proxies.
8. **SOA Escalates Task (P1PR):** The certification task can be escalated depending on configuration of the SOA composite that Oracle Identity Manager uses for certification-review tasks. For example, if the reviewer has not signed off or completed a task within a configured time-limit, SOA can escalate the task and reassign it to the manager of the currently-assigned reviewer. After the task is escalated the maximum number of times or has reached some other condition that terminates escalation, the task expires.
9. **SOA Expires Task (P1PR):** A certification review task can expire in certain conditions. For example, if the reviewer has not signed off a task within a configured time-limit, then the task can expire. If the task is configured to escalate before expiring, then SOA expires the task only after it has escalated the maximum number of times or reaches some other condition that terminates escalation. When a task expires, it cannot be acted upon.
10. **Task: P1DR:** Each delegated-review task contains a set of line-items that the primary reviewer has delegated to the delegated reviewer. When the delegated reviewer opens the task, the delegated reviewer can see only the line-items that are delegated in the particular delegation-event that produced the task. If the phase-one delegated reviewer (P1DR) opens any particular line-item, P1DR can see every detail for that line-item.

The delegated reviewer can act on any line-item within the task. The delegated reviewer cannot delegate any line-item to another person, cannot undelegate any line-item, and cannot reassign any line-item to another person. By default, the delegated reviewer owns every line-item and can decide, such as certify or revoke, its line-item-details. After every line-item has been decided, or all the details for the line-item has a Phase-One Decision, the delegated reviewer can sign off or complete the task.

11. **P1DR Signs Off:** After every line-item within a delegated-review task has been decided, the delegated reviewer can sign off or the task. Every delegated-review task must complete or must expire before the certification review process can proceed to Phase-One Verification.
12. **Any line-item has P1DR:** This branch-point decides whether the Phase One Verification stage is required. This depends on whether any line-item is delegated:
 - If any line-item that is not reassigned remains delegated when the P1PR signs off, then the review process moves to Phase One Verification.
 - If no line-item that is not reassigned remains delegated when the P1PR signs off, then the review-process moves to Phase Two.
13. **All P1DR tasks are signed off or expired:** This branch loops until every Phase One delegated-review task has either been signed off (completed) or has expired.
14. **Task: P1V:** After the primary-reviewer (P1PR) has signed off and every delegated-review-task (P1DR) has either completed or expired, Phase One Verification begins. Another task for the same certification-object is created and assigned to the primary reviewer. Within this task, the primary reviewer can see

and override any decision made in Phase One. The primary reviewer also can complete any line-item that no delegated reviewer has completed. The primary reviewer cannot reassign and delegate, and therefore, cannot undelegate any line-item within this task.

15. **P1PR Signs Off (P1V):** After every line-item-detail within the certification-object for every line-item that has not been reassigned to another primary reviewer has a decision, the Phase-One Primary Reviewer can sign off. When the reviewer signs off on the Phase-One Verification task, the certification review process proceeds to Phase Two.
16. SOA can proxy the assignee, and escalate or expire the P1V task (similar to the P1PR task). See steps 7 through 9 for details.

6.10.3.2 Phase Two With Verification

Phase Two is an optional, plural, and rotated version of Phase One.

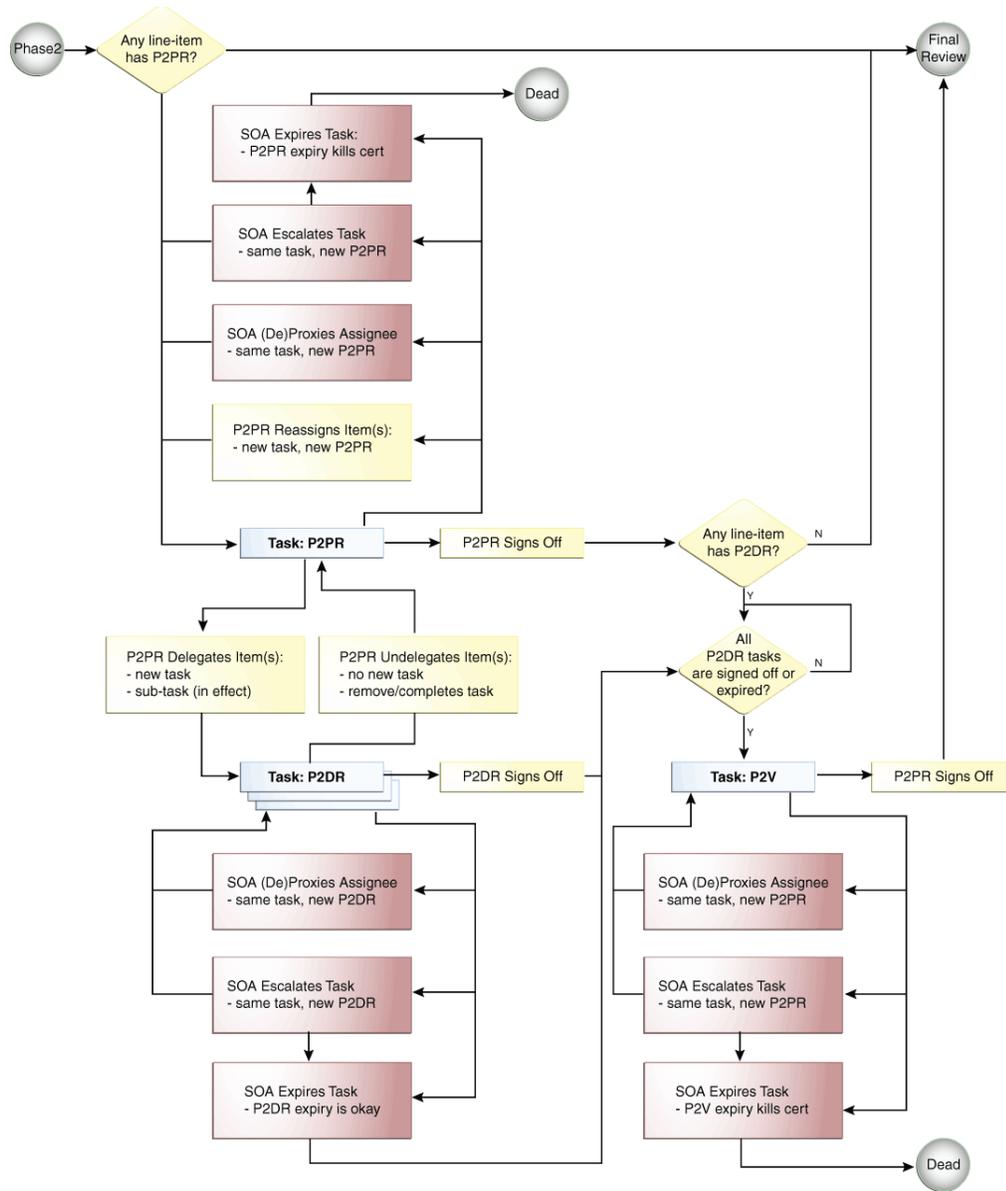
Optional: Phase Two is optional because it occurs only if Phase Two is enabled in configuration, the administrator specified a strategy to select a Phase Two Primary Reviewer, and the specified strategy assigned a Phase Two Primary Reviewer to at least one line-item within the certification.

Plural: There can be multiple Phase Two Primary Reviewers because each reviewer administers or authorizes a line-item-detail rather than a line-item. For example, in a user certification, each role assignment, account assignment, or entitlement assignment can have a different primary reviewer.

Rotated: Each reviewer in Phase Two can see a rotated view. For example, in Phase One of user certification, the business-reviewer can see users as line-items and each user's access-privileges as line-item-details. In Phase Two of user certification, each technical reviewer can see privilege-definitions, such as role, application instance, or entitlement definitions, as line-items and can see members of each privilege as line-item-details. This privilege-centric view is more useful to a technical-reviewer, who can delegate or reassign responsibility for individual privilege-definitions.

[Figure 6–4](#) shows the second phase of certification review with TPAD.

Figure 6–4 Phase Two With Verification



The stages in Phase Two are similar to Phase One, except for the following:

- Task: P2PR:** A review task is generated for each type of privilege for which each Phase Two primary reviewer (P2PR) must review assignments within that certification. When a Phase Two primary reviewer opens a P2PR task, that primary reviewer can see a list of line-items for which that primary reviewer is responsible within the certification object. For example, in Phase Two of a user certification, the Technical Reviewer who opens a P2PR task can see a list of privileges, such as role definitions, application instance definitions, or entitlement definitions, for which that primary reviewer is the certifier and for which that certification object contains assignments. Because this type of certification is user-centric, the rotated view is privilege-centric.

If the primary reviewer opens any particular line-item, the primary reviewer can see every line-item-detail for that line-item. The primary reviewer can act on any line-item within the task. The primary reviewer can delegate any line-item to

another person or can reassign any line-item to another person. By default, the primary reviewer owns every line-item and can decide, such as certify or revoke, its line-item-details.

- **P2PR Reassigns Item(s):** If the primary reviewer in Phase Two reassigns any set of line-items to another person, then that person becomes the new primary reviewer (P2PR) for those line-items. Oracle Identity Manager creates a new primary-review task and assigns it to the new P2PR.

Note: The Reassign operation in Phase Two does not generate a new certification. For example, if a primary technical reviewer reassigns a (rotated) line-item, then this does not split the certification.

The reassigned line-items disappear from the task of the original P2PR. The line-items are displayed within a separate task that is assigned to the new P2PR.

6.10.3.3 Final Review

Final Review is optional and is a tie-breaker. It is the simplest phase in TPAD.

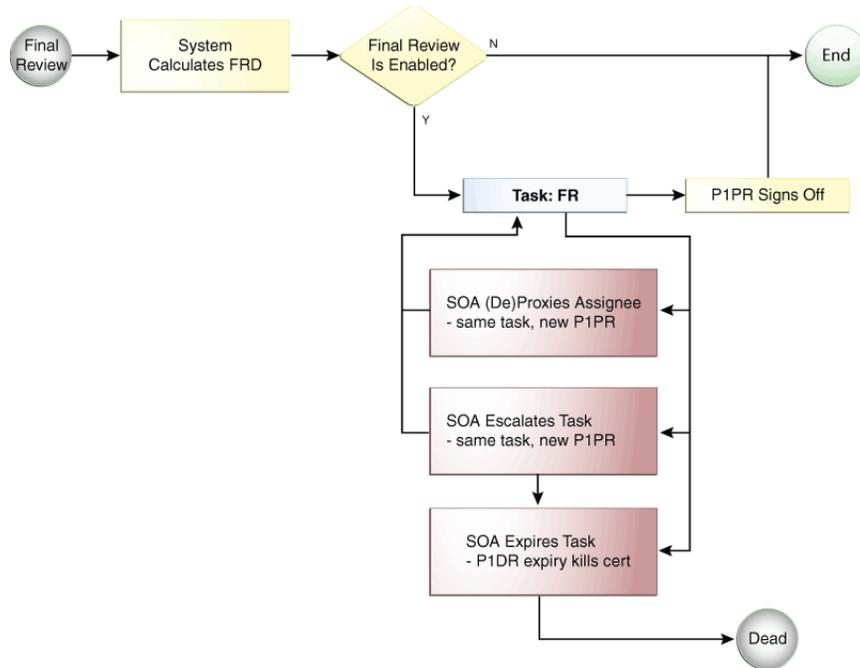
Optional: Final Review occurs only if it is enabled in configuration, the administrator specified in the certification definition that Final Review is to be performed, and Phase Two is performed because at least one line-item had a Phase Two Primary Reviewer.

Tie-breaker: Because the Phase Two reviewers may have made different decisions than the Phase One reviewers, the Phase One primary reviewer can view and override the decisions made in the two earlier phases. Therefore, Final Review is a tie-breaker.

Simplest phase: There is only one Final Reviewer, who is the Phase One Primary Reviewer. The Final Reviewer cannot delegate and cannot reassign. The Final Reviewer can see the decisions made during Phase One, the decisions made during Phase Two, and can override the decisions.

Figure 6–5 depicts the optional Final Review phase of certification review with TPAD.

Figure 6–5 Final Review Phase



In Final Review, the following stages are different from other review phases:

- **System Calculates FRD:** Oracle Identity Manager calculates a Final Review Decision (FRD) in the following manner:
 - For any line-item detail that has a Phase Two decision other than Abstain, the Phase Two decision becomes the Final Review decision.
 - If a particular line-item detail lacks a Phase Two decision, or if the Phase Two decision is to abstain, then the Phase One decision becomes the Final Review decision.
- **Final Review is enabled:** This branch decides whether or not to generate a task for Final Review and assign it to the Phase One Primary Reviewer. If Phase Two is disabled in configuration, or if Phase Two is not used in this certification review, or if Final Review is disabled in configuration, then task for Final Review is not generated. If Phase Two decisions have been made and Final Review is enabled in configuration, then the task for Final Review is generated.
- **Task: FR:** The Final Reviewer opens the Final Review task, and can see the following:
 - The decision made during Phase One on each line-item detail.
 - The decision made during Phase Two on each line-item detail.
 - The Final Review Decision.

The Final Reviewer can override the FRD in the context of the Phase One and Phase Two decisions. The Final Reviewer cannot reassign and delegate, and therefore, cannot undelegate any line-item within the task. The Final Reviewer can sign off after validating each FRD. At that point, the Final Review task is complete and the overall certification process is complete with the exception of closed-loop remediation, which Oracle Identity Manager performs automatically following signoff.. If the Final Reviewer does not sign off and allows the Final Review task to expire, then the certification process is dead.

You can use Final Review to compare the Phase One decision with the Phase Two decisions and make a final decision. If you prefer the Phase Two decision, then do not enable Final Review in configuration.

6.11 Troubleshooting Identity Certification

Table 6–4 lists possible issues encountered while using identity certification and the steps to resolve the issues.

Table 6–4 Troubleshooting Identity Certification Issues

Problem	Solution
You create certification definition and run the Certification Creation Task scheduled job, but no certification tasks are generated.	Make sure that all the certification configuration steps, as described in " Configuring Certifications " on page 6-3, have been performed.
Identity certification does not work	Apply the mandatory patches listed in section "Mandatory Patches Required for Installing Oracle Identity Manager" of the <i>Oracle Fusion Middleware Identity Management Release Notes</i> at the following URL: http://docs.oracle.com/cd/E37115_01/relnotes.1112/e39887/install.htm#ASIRN5213

Part IV

Form Management

This part describes how to manage forms in Oracle Identity Manager to extend users, roles, organizations, request catalogs, and resources.

It contains the following chapters:

- [Chapter 7, "Managing Forms"](#)
- [Chapter 8, "Configuring Custom Attributes"](#)

Managing Forms

You can use Form Designer in Oracle Identity System Administration to create and manage forms and datasets.

See Also: "Understanding Requests" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about request datasets

This section contains the following topics:

- [Creating Forms By Using the Form Designer](#)
- [Searching Forms By Using the Form Designer](#)
- [Modifying Forms By Using the Form Designer](#)

Note: Before you start performing the procedures described in this section, it is recommended that you review the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

7.1 Creating Forms By Using the Form Designer

To create forms by using the Form Designer:

1. Login to Oracle Identity System Administration.
2. Create and activate a sandbox. A warning message is displayed if no sandbox is activated. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
3. In the left pane, under Configuration, click **Form Designer**. The Form Designer page is displayed.
4. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Form page is displayed.
5. In the Resource Type field, specify a resource object with which you want to associate the form. To do so:
 - a. Click the lookup icon next to the Name field. The Search and Select: Name dialog box is displayed.

- b. In the Name field, enter the name of the resource object you want to search. You can leave this field blank if you want to display all resource objects.
 - c. Click **Search**. The resource objects that match the search condition are displayed.
 - d. Select the resource object that you want to associate with the form, and click **OK**. The resource object name is displayed in the Name field of the Create Form page.
6. In the Form Name field, enter a form name.
 7. In the Available form fields section, a list of form field names along with description and Display Name are displayed. These fields are available for the form you are creating. For each available form field, you can select the Bulk Update option. Selecting this option makes the form field available for updating the entities in bulk.
 8. Click **Create**. A message is displayed stating that the form is created.
 9. If required, you can export the sandbox to store all the changes made in your sandbox. For detailed instructions on exporting a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
 10. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

7.2 Searching Forms By Using the Form Designer

To search forms by using the Form Designer:

1. In Oracle Identity System Administration, under Configuration, click **Form Designer**. The Form Designer page is displayed.
2. Select any one of the following options:
 - **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.
3. From the Type list, select the form type, such as User, Role, Organization, Catalog, or Resource. The form type represents the entity type with which the form is associated.

If you want to display all the forms for the selected form type, then leave the other search fields as blank, and click **Search**.
4. From the Resource Type list, select the type of resource object associated with the form. Note that selecting a value for the Resource Type list is mandatory only if you selected **Resource** from the Type list in the preceding step.
5. Enter values in the Form Name or Description fields to specify a search criteria by the form name or description respectively.
6. Click **Search**. The forms that match your search condition are displayed. For each form, the search result displays the form name, form type, resource type, and description.

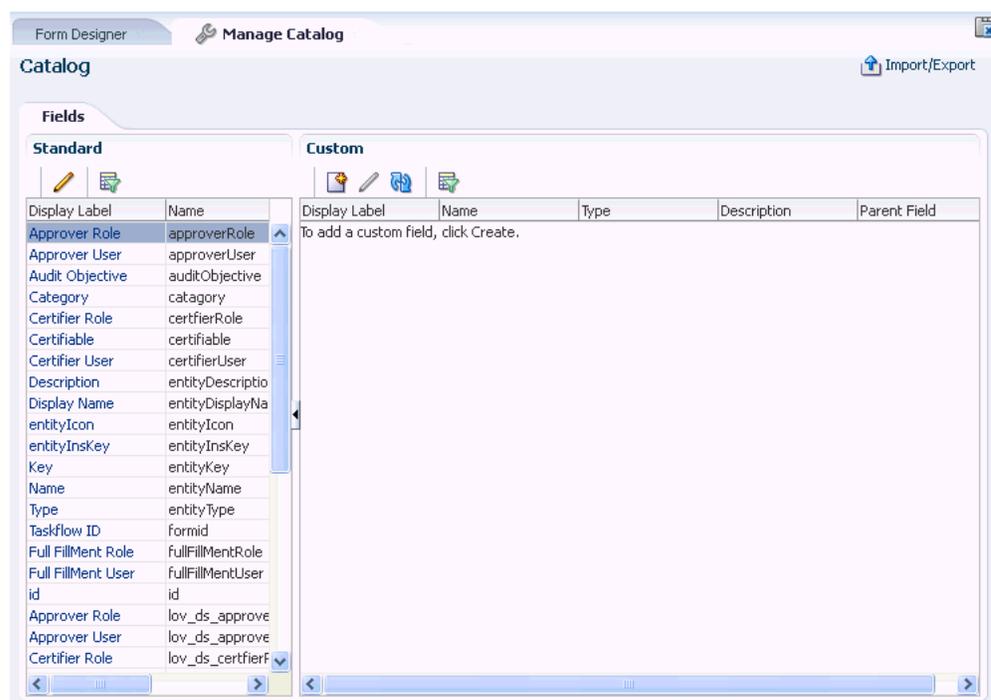
7.3 Modifying Forms By Using the Form Designer

To modify a form by using the Form Designer:

See Also: [Section 7.3.1, "Removing or Hiding Form Attributes"](#)

1. Create and activate a sandbox. A warning message is displayed if no sandbox is activated. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
2. In the Form Designer page, search for the form you want to modify.
3. In the Search Results table, select the form you want to modify.
4. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar. Otherwise, click the form name in the search results table. The Manage Form page is displayed with details of the form, as shown in [Figure 7-1](#):

Figure 7-1 The Manage Form Page



The Manage Form page displays the form attributes in the Object Information section. The Standard and Custom sections list the standard and custom fields of the form. You can edit the standard fields, and create and edit custom fields in these sections.

5. If you want to modify any standard field, then perform the following steps:
 - a. In the Standard section, select the field you want to modify.
 - b. Click the Edit icon on the toolbar. Alternatively, you can click the display label to edit the field.

The Edit Standard Field dialog box is displayed, as shown in [Figure 7-2](#):

Figure 7–2 The Edit Standard Field Dialog Box



- c. Change the values in the fields. You are allowed to edit the display name of the field, and the help text. The Field Name and API Name fields are read-only.
 - d. Click **OK**.
6. If required, you can export the sandbox to store all the changes made in your sandbox. For detailed instructions on exporting a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
 7. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

See Also: ["Configuring Custom Attributes"](#) on page 8-1 for information about creating and modifying custom fields or user-defined fields (UDFs)

7.3.1 Removing or Hiding Form Attributes

To remove or hide a form attribute in Oracle Identity Self Service:

1. Log in to Oracle Identity Self Service.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
3. In the left pane, under Requests, click **Catalog**. The Catalog page is displayed.
4. Search for and select the application instance whose resource form page must be updated, and the click **Add to Cart**.
5. Click **Checkout**.
6. On the Cart Details page, under the Details section, the application instance form and its attributes are displayed.
7. Click **Customize** to open WebCenter Composer. The page opens in customization mode.
8. From the View menu at the upper left corner of the page, select **Source**. The object tree is displayed.
9. If you want to delete a form attribute, select the UI component and click the delete icon in the Composer panel at the top of the page.

If you want to hide a form attribute, click **Edit**. Then, select the UI component and set the rendered property to `false`.

10. Click **Close** to leave customization mode.
11. If required, you can export the sandbox to move the change from the test to production environment. For detailed instructions on exporting a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
12. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Configuring Custom Attributes

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, resource, organization, and catalog entities.

This chapter describes how to create and manage UDFs in the following sections:

- [Creating a Custom Attribute](#)
- [Creating a Custom Child Form](#)
- [Creating a Custom Child Form Attribute](#)
- [Modifying a Custom Attribute](#)
- [Adding a Custom Attribute](#)
- [Adding a Custom Attribute to an Application Instance Form](#)
- [Moving UDFs from Test to Production](#)
- [Synchronizing User-Defined Fields Between Oracle Identity Manager and LDAP](#)
- [Attribute Definitions](#)
- [Creating Cascaded LOVs](#)

Note: Before you start performing the procedures described in this section, it is recommended that you review the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

8.1 Creating a Custom Attribute

To create a custom attribute or UDF:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

3. In the left pane, under Configuration, click **Form Designer**. The Form Designer page is displayed.
4. Search and open the form in which you want to create the UDF. For example, you can open the form "User" to create or modify user to add a UDF to the form.
5. In the Custom section of the Fields tab, click the **Create** icon. The Select Field Type dialog box is displayed.
6. Select a field type you want to create. The available field types are:
 - **Text:** Select this option to create a text field.
 - **Number:** Select this option to create a numeric field.
 - **Checkbox:** Select this option to create a checkbox field.
 - **Date:** Select this option to create a date type field.
 - **Lookup:** Select this option to create a lookup field in which users can search and select the value. Note that there are two types of lookups that you can create:
 - A drop-down list from which you can select a value.
 - A searchable picklist (ADF name input list of value), from which users can search and select the value. If you want to create a searchable picklist, then on the Create Lookup Field page, under the Advanced section, select **Searchable Picklist**.

Note: After you create a UDF for dependent lookups (a lookup field that is created with the **Constrain list by parent field value selection option** selected), you must set the partialTriggers property through WebCenter composer to refresh the values in the dependent lookup. To do so, see the procedure described in "[Creating Cascaded LOVs](#)" on page 8-149.

7. Click **OK**. The page to create a custom field is displayed.

As an example, [Figure 8–1](#) shows the Create Text Field page. The rest of the procedure in this section has been based on creating a custom text field.

Figure 8–1 The Create Text Field Page

Create Text Field Save and Close Cancel

Appearance
Configure how this field will appear when displayed to your users.

* Display Label
Display Width Characters

Name
Each field requires a unique name in the system. Name and description are for internal use only, and are never displayed to your users.

* Name
Description

Constraints

Searchable
Maximum Length Characters

Default Value
Enter the value you want to set for the field when an object is created. Select Expression if you want to set the default dynamically.

Advanced

Encrypt
 Use in Bulk
LDAP Attribute

8. Enter values in the fields of the Create Text Field page. [Table 8–1](#) lists the fields in the Create Text Field page. Depending on the type of field that you are creating, the fields on the listed in the following table varies.

Table 8–1 Fields in the Create Text Field Page

Section	Field	Description
Appearance	Display Label	The custom field label that is displayed in the form.
	Display Width	The display width in characters. If you do not specify a value for this field, then the length of the field is taken as default.
Name	Name	The unique custom field name. This field is of internal use only, and the value of this field is not displayed to the user.
	Description	The description of the custom field. This field is of internal use only, and the value of this field is not displayed to the user.

Table 8–1 (Cont.) Fields in the Create Text Field Page

Section	Field	Description
Constraints	Searchable	<p>Determines if the custom field can be searched by the user.</p> <p>In addition, if the Searchable option is not checked, then the UDF cannot be used throughout the application as it is not displayed.</p> <p>Note: If you select the Searchable checkbox, then in the Advanced section, you cannot select Encrypt. A custom field that is marked as searchable cannot be encrypted.</p> <p>Note: When you create a searchable UDF in the catalog, the searchable UDF is automatically displayed in the advanced search form of the catalog. You can use the UDF for searching in the catalog. But no index will be present on that UDF, and as a result, performance might be compromised. Therefore, you must manually create an index on those fields. To do so, use the following SQL statement:</p> <pre>CREATE INDEX INDEX_NAME ON catalog NAME_OF_CATALOG_UDF;</pre>
	Maximum Length	<p>The maximum length of the field in characters.</p> <p>Note: You can increase the maximum length for default and custom attributes by using the User form. However, decreasing the maximum length is not supported.</p>
Default Value	Text field	<p>The default value of the custom field. The value you specify in this field is set for the field when the object is created by using Oracle Identity Self Service. But if user entities are created through GTC trusted source reconciliation, then these default values are not populated.</p> <p>Note: The field below the text field is grayed out and is not used.</p>
Advanced	Encrypt	<p>Determines whether the custom field must be encrypted.</p> <p>Note: If you select the Encrypt checkbox, then in the Constrains section, you cannot select Searchable. A custom field that is encrypted cannot be searchable.</p>
	Use in Bulk	<p>Determines whether the attribute is available in bulk operations.</p>
	LDAP Attribute	<p>Name of the attribute in the LDAP repository to which this custom attribute must map to.</p> <p>Note: Unless LDAP synchronization is enabled, setting a value for this field has no effect. For more information about enabling LDAP synchronization, see the "Configuring OIM Server" chapter in <i>Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management</i>.</p>

9. Click **Save and Close**. The UDF is created in the backend and is displayed in the Custom section of the Form Details page.
10. If required, you can export the sandbox to store all the changes made in your sandbox. For detailed instructions on exporting a sandbox, see the "Managing

Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

11. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

When you create a UDF by using the Form Designer, it is created in the back-end, and is not available for use. To make it available for use to the user, you must include the UDF in the Oracle Identity Self Service page on which it will be displayed. For information about including a UDF in the Oracle Identity Self Service page, see "[Adding a Custom Attribute](#)" on page 8-9.

8.2 Creating a Custom Child Form

Application instance forms can have child forms. Note that at some places in this guide, the term **resource form** has been used to refer to **application instance forms**.

To create a custom child form:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Note: You must ensure that sandbox in which the application instance form for which you are creating the child form must be published. If it is not published, then you must perform the procedure described in this section in the same sandbox in which the application instance form was created.

3. In the left pane, under Configuration, click **Form Designer**. The Form Designer page is displayed.
4. Search for and open the application instance (resource) form for which you want to create a child form as follows:
 - a. In the Search section, from the Type drop-down list, select **Resource**.
 - b. Specify a value for the Resource Type look field.
 - c. Click **Search**.
A list of all resource forms (application instance forms) that meet the search criteria is displayed.
 - d. From this list, select the form to open. Alternatively, click **Open** on the toolbar.
The Manage <APP_INSTANCE_FORM_NAME> page is displayed.
5. On the Child Objects tab, click the **Add** icon on the toolbar. The Add dialog box is displayed.
6. In the Name field, enter the name of the child form and click **OK**. The child form is created in the backend and is displayed in the Child Objects tab of the application instance form for which it was created.
7. Click **Regenerate View** to regenerate the application instance form associated with the child form. If you do not regenerate the view the child form will not be available in the page for use on which you want it to be displayed.

8. If required, you can export the sandbox to store all the changes made in your sandbox. For detailed instructions on exporting a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
9. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

8.3 Creating a Custom Child Form Attribute

To create a custom child form attribute:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Note: You must ensure that sandbox in which the child form for which you are creating the attribute must be published. If it is not published, then you must perform the procedure described in this section in the same sandbox in which the child form was created.

3. In the left pane, under Configuration, click **Form Designer**. The Form Designer page is displayed.
4. Search for and open the parent form (application instance form) of the child form in which you want to create an attribute. See Step 4 of "[Creating a Custom Child Form](#)" on page 8-5 for information about searching and opening a form.
The Manage <APP_INSTANCE_FORM_NAME> page is displayed.
5. On the Child Objects tab, from the list of child forms, search for and select the child form in which you want to create the attribute. The Manage <CHILD_FORM_NAME> page is displayed.
6. In the Custom section of the Fields tab, click the **Create** icon. The Select Field Type dialog box is displayed.
7. Select a field type you want to create. The available field types are:
 - **Text:** Select this option to create a text field.
 - **Number:** Select this option to create a numeric field.
 - **Checkbox:** Select this option to create a checkbox field.
 - **Date:** Select this option to create a date type field.
 - **Lookup:** Select this option to create a lookup field in which users can search and select the value.
8. Click **OK**. The page to create a custom field is displayed.

As an example, [Figure 8-2](#) shows the Create Lookup Field page. The rest of the procedure in this section has been based on creating a custom lookup field.

Figure 8–2 The Create Lookup Field Page

9. Enter values in the fields of the Create Lookup Field page. [Table 8–2](#) lists the fields in the Create Lookup Field page:

Table 8–2 Fields in the Create Lookup Field Page

Section	Field	Description
Appearance	Display Label	The custom field label that is displayed in the form.
	Help Text	Field-level help text that is displayed to the users as a tooltip.
Name	Name	The unique custom field name. This field is of internal use only, and the value of this field is not displayed to the user.
	Description	The description of the custom field. This field is of internal use only, and the value of this field is not displayed to the user.
Constraints	Searchable	Determines if the custom field can be searched by the user.

Table 8–2 (Cont.) Fields in the Create Lookup Field Page

Section	Field	Description
List of Values	Lookup Type	<p>The lookup whose values are displayed to the user as a list of available values. You can either specify an existing lookup type or create a new one.</p> <p>Note: If you are creating a new lookup, then the name of this new lookup must not be the same as that of the UDF (of type lookup) that you are creating. This ensures that the lookup is displayed in the Manager User page.</p>
Default Value	Drop-down list	<p>The default value of the custom field. The value you specify in this field is set for the field when the object is created.</p> <p>Note: The field below the down-down list is grayed out and is not used.</p>
Advanced	Entitlement	<p>Determines whether the custom field is an entitlement.</p> <p>Note: If you are creating a child form with a lookup field for entitlement (in other words, the Entitlement field is selected), then you must select Searchable and Searchable Picklist options too.</p>
	Use in Bulk	Determines whether the attribute is available in bulk operations.
	Searchable Picklist	Determines whether the custom field is searchable.

10. Click **Save and Close**. The UDF is created in the backend and is displayed in the Custom section of the Form details page.
11. If required, you can export the sandbox to store all the changes made in your sandbox. For detailed instructions on exporting a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
12. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

When you create a UDF by using the Form Designer, it is created in the back-end, and is not available for use. To make it available for use to the user, you must include the UDF in the Oracle Identity Self Service page on which it will be displayed. For information about including a UDF in the Oracle Identity Self Service page, see ["Adding a Custom Attribute"](#) on page 8-9.

8.4 Modifying a Custom Attribute

To modify a custom attribute that you created for a form:

1. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
2. In the Form Designer, search and open the form which contains the custom attribute you want to modify.
3. In the Custom section, select the custom attribute that you want to modify.

4. Click the Edit icon on the toolbar. Alternatively, click the Display Name of the attribute. The page to edit the field is displayed.
5. Modify the values in the fields by referring to [Table 8-1](#).
6. Click **Save and Close**.
7. If required, you can export the sandbox to store all the changes made in your sandbox. For detailed instructions on exporting a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
8. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

8.5 Adding a Custom Attribute

When you create a UDF, it is created only in the backend, and is not available in the page for use on which you want it to be displayed. To display a UDF in a page in Oracle Identity Self Service:

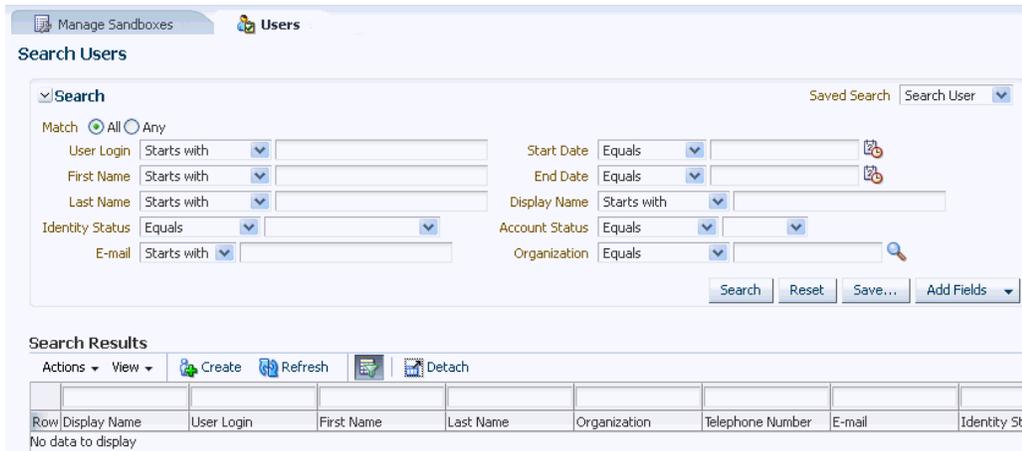
1. Create the UDF by using the Form Designer. For example, you can create a UDF for the Create User page.

See "[Creating a Custom Attribute](#)" on page 8-1 for information about created a UDF.

Note: After adding a UDF through Form Designer, logout of both Oracle Identity System Administration and Oracle Identity Self Service, and then login again to be able to see the newly added UDF and use it for customization.

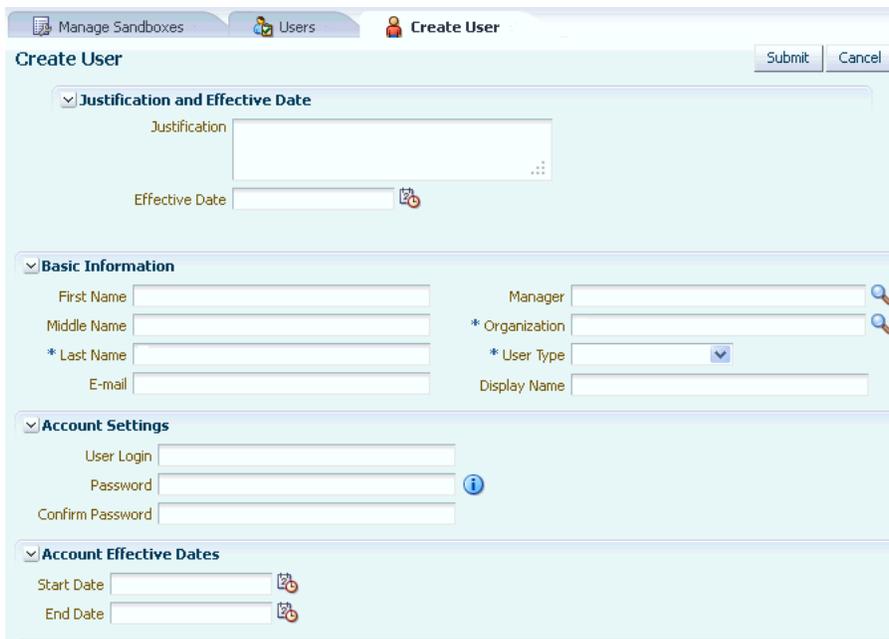
2. Log in to Oracle Identity Self Service.
3. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
4. In the left pane, under Administration, click **Users**. The Users page is displayed as shown in [Figure 8-3](#).

Figure 8–3 Users Page



5. Click **Create User** on the toolbar to display the Create User page. [Figure 8–4](#) displays the Create User page.

Figure 8–4 Create User Page



6. Click **Customize** at the upper right corner of the page to open WebCenter Composer. The Create User page opens in customization mode as shown in [Figure 8–5](#).

Figure 8–5 Create User Page in Customization Mode

Editing Page: Identity Self Service
View ▾ Page Properties Close

ORACLE Identity Self Service Accessibility Sandboxes (customUDF) Customize Help Sign Out

My Profile ▾ Requests ▾ Administration ▾

Manage Sandboxes Users Create User

Create User Submit Cancel

Justification and Effective Date

Justification

Effective Date

Basic Information

First Name

Middle Name

* Last Name

E-mail

Manager

* Organization

* User Type

Display Name

Account Settings

User Login

Password

Confirm Password

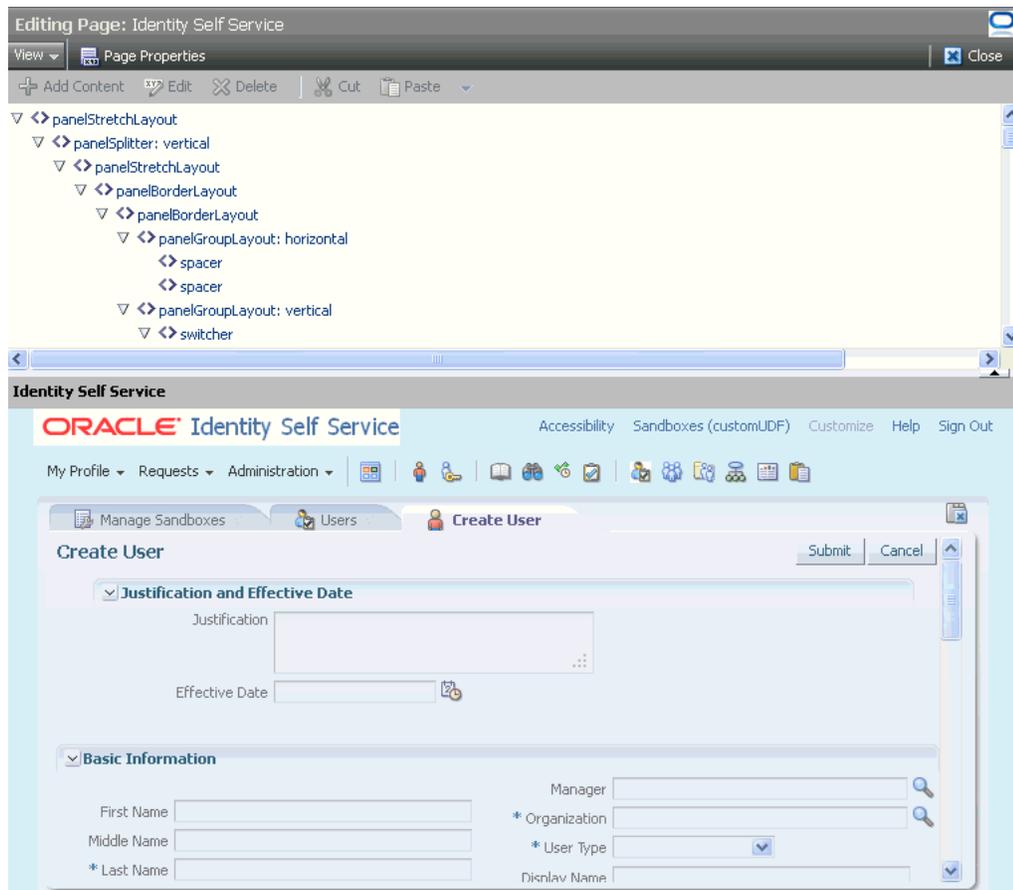
Account Effective Dates

Start Date

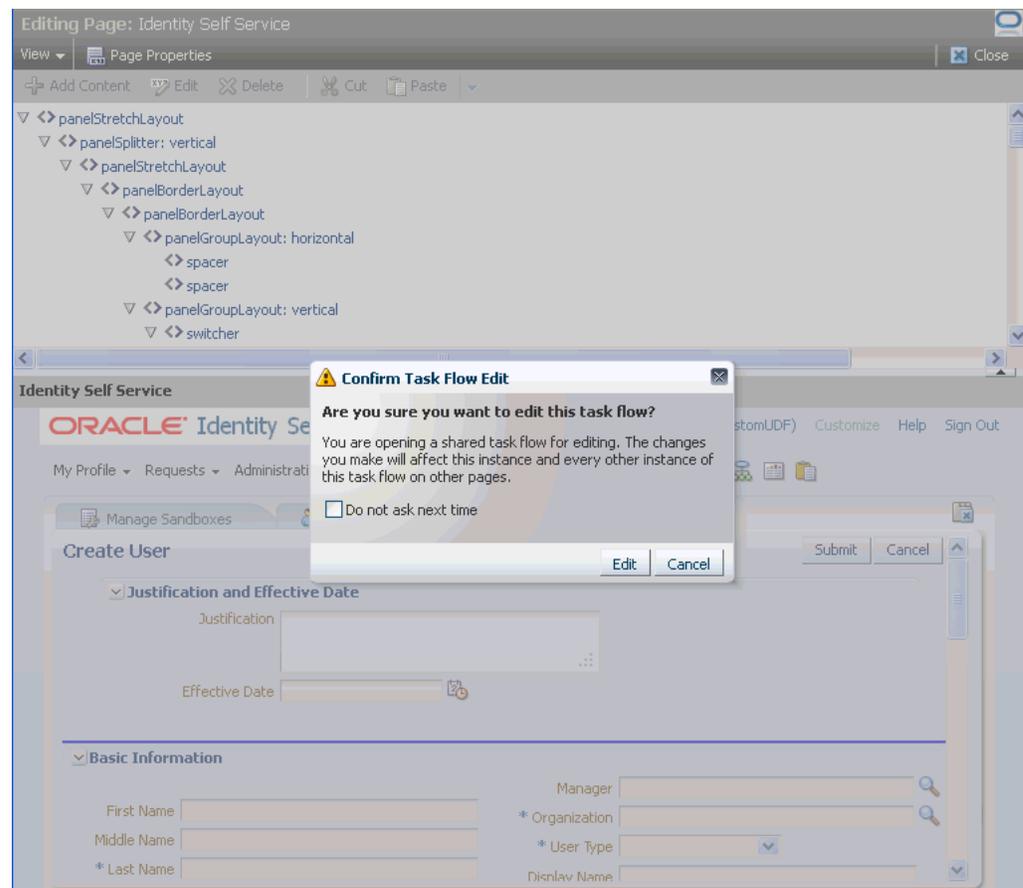
End Date

7. Enter values for all mandatory fields.
8. In the upper-left corner of the page, from the View menu, select **Source**. The object tree is displayed as shown in [Figure 8–6](#).

Figure 8–6 Object Tree Page in Customization Mode

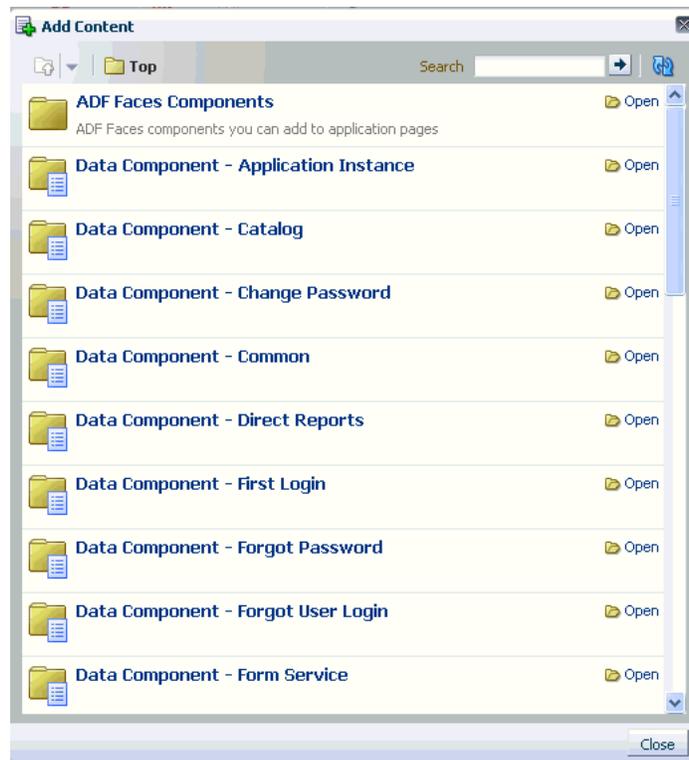


9. Select the section of the page on which you want to add the UDF.
10. In the Confirm Task Flow Edit dialog box, click **Edit** to confirm the edit task. The corresponding ADF component in the object tree is selected. [Figure 8–7](#) displays the Confirm Task Flow Edit dialog box.

Figure 8–7 Confirm Task Flow Edit Dialog Box

11. Select the `panelFormLayout` component, and click **Add Content**. The Add Content dialog box is displayed as shown in [Figure 8–8](#).

Figure 8–8 Add Content Dialog Box



12. Depending on the entity or area on which the UDF was added, select the data component, and then the view object. [Table 8–3](#) lists the entities, pages, data components, and view objects that must be selected.

Table 8–3 Entities and Corresponding Data Components and View Objects

Entity	Page	Data Component	View Object
User	Create User	Data Component - Catalog	userVO
	Modify User	Data Component - Catalog	userVO
	Search Users	Data Component - Manage Users	UserVO1
	View User Details	Data Component - Manage Users	UserVO1
	My Information	Data Component - My Information	UserVO1
	New User Registration	Data Component - User Registration	UserVO1
Role	Create Role	Data Component - Role	RoleDetailsVO
	Modify Role	Data Component - Role	RoleDetailsVO
	Search Roles	Data Component - Role	RoleVO1
Organization	Create Organization	Data Component - Organization	EditOrgVO
	Modify Organization	Data Component - Organization	EditOrgVO

Table 8–3 (Cont.) Entities and Corresponding Data Components and View Objects

Entity	Page	Data Component	View Object
	Search Organizations	Data Component - Organization	OrganizationVO
Catalog	Access Request	Data Component - Catalog	CartItemVO1
Certification	User Certification	Data Component - Certification	UserCertificationUserVO1
			UserCertificationUserEntitlementVO1
	Role Certification	Data Component - Certification	RoleCertificationRoleVO1
			RoleCertificationMemberVO1
			RoleCertificationPolicyVO1
	Application Instance Certification	Data Component - Certification	ApplicationCertificationApplicationVO
			ApplicationCertificationEntitlementVO
	Entitlement Certification	Data Component - Certification	EntitlementCertificationEntitlementVO
			EntitlementCertificationEntitlementMemberVO

Figure 8–9 shows the Add Content dialog box with folder options such as Data Component - Manager Users.

Figure 8–9 Add Content Dialog Box Displaying the Data Component - Manage Users Folder



13. Scroll to find the UDF that you added and click **Add**. If the UDF is not displayed, then refresh the content by clicking the refresh icon at the top right hand corner of the dialog box.
14. Depending on the custom attribute that you created in Step 1 and the type of UDF that you want to display, select one of the following items from the menu:

For a UDF of Text or Number type:

- ADF Output Text
- ADF Output Text w/Label
- ADF Output Formatted
- ADF Output Formatted w/Label
- ADF Input Text
- ADF Input Text w/Label
- ADF Label
- ADF Readonly Input Text w/Label
- ADF Select Boolean Checkbox
- ADF Table Column
- ADF Input List Of Value

For a UDF of Checkbox type:

- ADF Output Text
- ADF Output Text w/Label

- ADF Output Formatted
- ADF Output Formatted w/Label
- ADF Input Text
- ADF Input Text w/Label
- ADF Label
- ADF Readonly Input Text w/Label
- ADF Select Boolean Checkbox
- ADF Select One Radio
- ADF Select One Choice
- ADF Table Column
- ADF Input List Of Value

For a UDF of Date type:

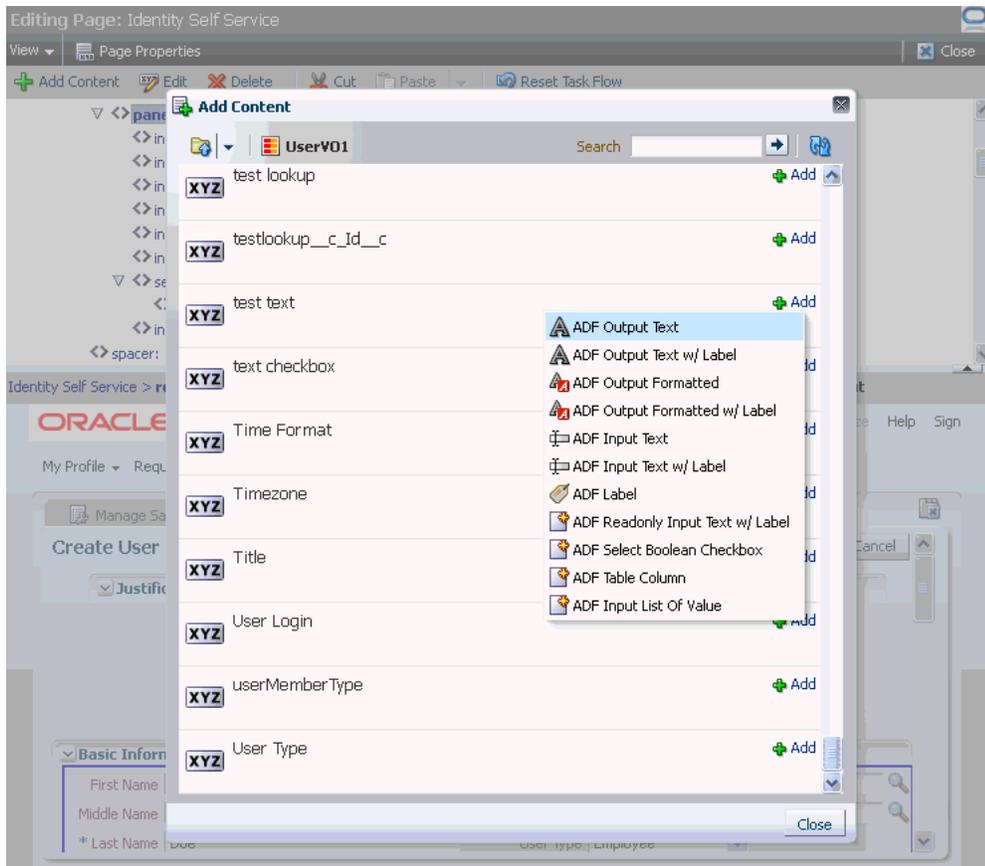
- ADF Output Text
- ADF Output Text w/Label
- ADF Output Formatted
- ADF Output Formatted w/Label
- ADF Input Text
- ADF Input Text w/Label
- ADF Label
- ADF Input Date w/Label
- ADF Readonly Input Text w/Label
- ADF Select Boolean Checkbox
- ADF Table Column
- ADF Input List Of Value

For a UDF of Lookup type:

- ADF Output Text
- ADF Output Text w/Label
- ADF Output Formatted
- ADF Output Formatted w/Label
- ADF Input Text
- ADF Input Text w/Label
- ADF Label
- ADF Readonly Input Text w/Label
- ADF Select Boolean Checkbox
- ADF Table Column
- ADF Input List Of Value

For example, if you have created a UDF of Text type, then select **ADF Input Text w/Label**. Similarly, if you created a UDF of Lookup type, the select **ADF Input List of Value**. As an example, [Figure 8–10](#) shows options for a UDF of Text type.

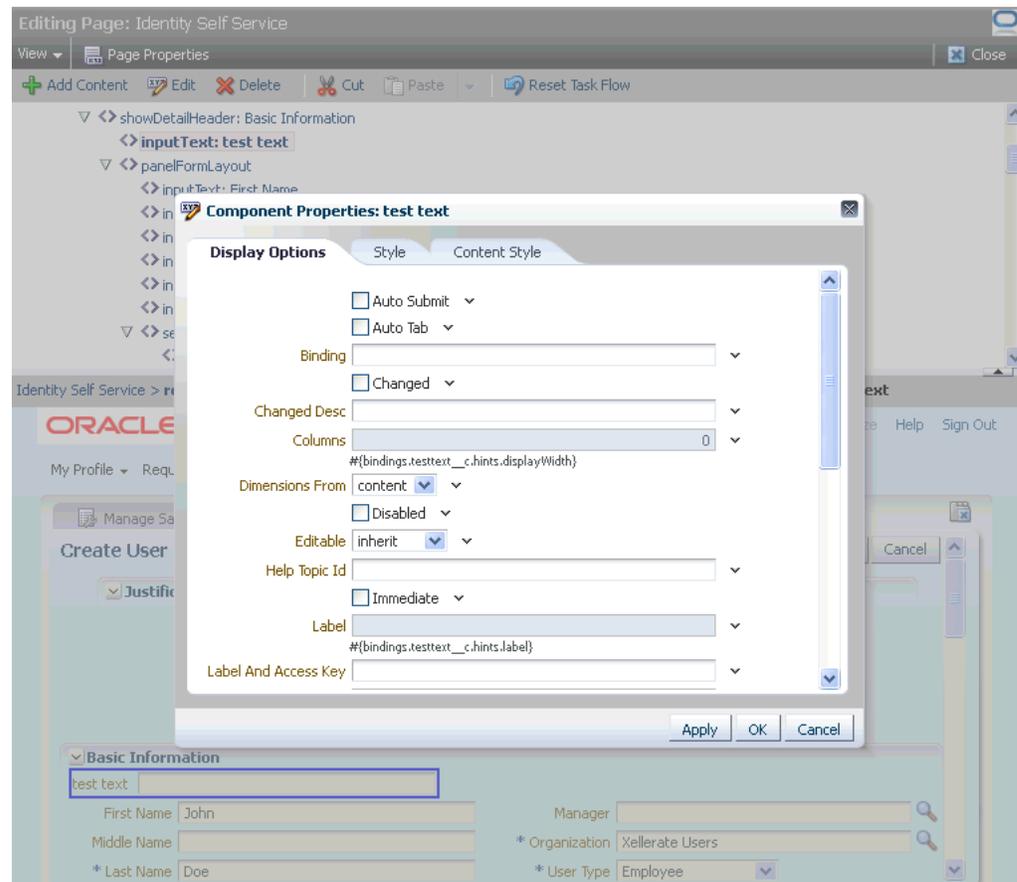
Figure 8–10 Options for Adding a UDF of Text Type



15. Click **Close** to close the Add Content dialog box.

Note: If two attribute labels are displayed for the same field, then add the attribute that does not end with __C.

16. From the object tree on the Editing Page, select the UDF on the page, and click **Edit**. The Component Properties dialog box, as shown in [Figure 8–11](#), is displayed.

Figure 8–11 Component Properties Dialog Box

17. On the Display Options tab:

- a. Select **Auto Submit**.
- b. If you have added the UDF on the user form, then in the Value Change Listener field, enter
`#{pageFlowScope.cartDetailStateBean.attributeValueChangedListener}`.

If you have added the UDF on a form other than the user form, then copy the value of the Value Change Listener field from any of the existing fields on the form and paste it as the value of the Value Change Listener field for the newly added UDF.

Note: An error is encountered when you set a value for the Value Change Listener field by using the Web Composer. As a work around, perform the following steps:

1. Export all changes made to the sandbox (one that is currently active) to a ZIP file.
 2. Extract the contents of the ZIP file and locate the XML file for the form on which the UDF was added. For example, the XML file for the Create User form is
oracle/iam/ui/runtime/form/view/pages/mdssys/cust/site/site/user/CreateForm.jsff.xml.
 3. In a text editor, open the XML file and identify the ADF component (for example, af:inputText) that you selected while adding the UDF to the form.
 4. Set the value of the Value Change Listener field, which is the valueChangeListener property of the ADF component.
 5. Save the changes, repackage the zip file (the sandbox archive) and then import it back to your environment.
-
-

- c. If you want to mark this attribute as mandatory, then change the **Required** and **Show Required** properties to true.

18. Click **OK**.

19. Click **Close** to leave customization mode.

20. If required, you can export the sandbox, in case if you intend to move the change from test to production environment. See "Managing Sandboxes" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed instructions on exporting a sandbox.

21. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

To remove a UDF, you can use the customization mode to open the WebCenter Composer. In the customization mode, select the component or UDF that you want to remove, and then delete it or set the rendered property on that UDF to false.

8.5.1 Enabling the Submit Button After Adding a UDF to the Modify User Form

After adding a new UDF to the modify user form by customizing the UI using Web Composer, the Submit button of the form is not enabled when you try to modify a user. But modification of other user form fields enable the Submit button.

To avoid this issue, when you add a new UDF to the modify user form for the first time:

1. Create a sandbox and activate it. Open the page that contains the UDF, and click **Customize**.
2. Select **View, Source**.
3. Note the value of the valueChangeListener property of a predefined or default field. To do so:
 - a. Click the predefined field, and then click **Edit** to open the Component Properties dialog box.
 - b. Copy the value of the valueChangeListener property.

4. Add the new UDF to the form, as described in ["Adding a Custom Attribute"](#) on page 8-9.
5. Export the sandbox as a ZIP file.
6. Delete the sandbox without publishing it.
7. Extract the ZIP file, and edit the jsff.xml file for the specific screen.
8. Add the following attributes to the ADF tag, for example af:inputText, for the UDFD field, as shown:

```
valueChangeListener=VALUE_COPIED_IN_STEP3
autoSubmit="true"
```

The resulting XML will look similar to the following:

```
<?xml version='1.0' encoding='UTF-8'?>
<mds:customization version="11.1.1.61.92"
xmlns:mds="http://xmlns.oracle.com/mds" motype_local_name="root"
motype_nsuri="http://java.sun.com/JSP/Page">
  <mds:move node="_xg_12" parent="_xg_pf15" position="last"/>
  <mds:insert parent="_xg_pf15" position="last">
    <af:inputText xmlns:af="http://xmlns.oracle.com/adf/faces/rich"
value="#{bindings.JobCode__c.inputValue}"
label="#{bindings.JobCode__c.hints.label}"
required="#{bindings.JobCode__c.hints.mandatory}"
columns="#{bindings.JobCode__c.hints.displayWidth}"
maximumLength="#{bindings.JobCode__c.hints.precision}"
shortDesc="#{bindings.JobCode__c.hints.tooltip}" id="dtrt_dc_628826708"
autoSubmit="true"
valueChangeListener="#{pageFlowScope.cartDetailStateBean.attributeValueChangedL
istener}">
      <f:validator xmlns:f="http://java.sun.com/jsf/core"
binding="#{bindings.JobCode__c.validator}"/>
    </af:inputText>
  </mds:insert>
  <mds:move node="_xg_19" parent="_xg_pf15" position="last"/>
  <mds:move node="_xg_20" parent="_xg_pf15" position="last"/>
  <mds:move node="_xg_27" parent="_xg_pf15" position="last"/>
  <mds:move node="_xg_23" parent="_xg_pf15" position="last"/>
  <mds:move node="_xg_41" parent="_xg_pf15" position="last"/>
</mds:customization>
```

9. Create the ZIP file for the sandbox.
10. Import the sandbox.
11. Publish the sandbox.

8.6 Adding a Custom Attribute to an Application Instance Form

When you create a custom attribute (UDF) on an application instance form, it is created only in the backend, and is not available in the page for use on which you want it to be displayed. The following are the options available to display the UDF in a page in Oracle Identity Self Service:

- [Regenerating View](#)
- [Updating the Application Instance Form By Using WebCenter Composer](#)

8.6.1 Regenerating View

To display the UDF in a page in Oracle Identity Self Service:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Note: You must ensure that sandbox in which the application instance form for which you are adding a custom child attribute must be published. If it is not published, then you must perform the procedure described in this section in the same sandbox in which the application instance form was created.

3. In the left pane, under Configuration, click **Form Designer**. The Form Designer page is displayed.
4. Search for and open the application instance form whose child form (containing the UDFs that you added) must be displayed in a page in Oracle Identity Self Service.
5. On the Child Objects tab, click **Regenerate View**.

Note: Any customization made to the page will be lost when you click **Regenerate View**.

6. If required, you can export the sandbox, in case if you intend to move the change from test to production environment. See "Managing Sandboxes" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed instructions on exporting a sandbox.
7. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

8.6.2 Updating the Application Instance Form By Using WebCenter Composer

To display the UDF in a page in Oracle Identity Self Service:

1. Create the UDF by using the Form Designer.
2. Log in to Oracle Identity Self Service.
3. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
4. In the left pane, under Requests, click **Catalog**. The Catalog page is displayed.
5. Search for and select the application instance whose resource form page must be updated, and the click **Add to Cart**.
6. Click **Checkout**.
7. On the Cart Details page, under the Details section, the application instance form and its attributes are displayed.

8. Click **Customize** to open WebCenter Composer. The page opens in customization mode.
9. Enter values for all mandatory fields.
10. From the View menu at the upper left corner of the page, select **Source**. The object tree is displayed.
11. Under the Details section, select and click the attributes of the application instance form. A message confirming whether you want to edit the page is displayed.
12. Click **Edit**. In the object tree, the ADF component corresponding to the selection made in the preceding step is selected.
13. Click **Add Content**. The Add Content dialog box is displayed.
14. Select the data component. To do so:
 - a. Select **Data Component - Catalog**.
 - b. Search for *APP_INSTANCEVO* and then click **Open**. Here, *APP_INSTANCE* is the name of the application instance for which the attributes are added.
15. Scroll to find the UDF that you added. If the UDF is not displayed, then refresh the page.
16. Select the UDF on the page, and click **Add**.
17. Click **Close** to leave customization mode.
18. If required, you can export the sandbox to move the change from the test to production environment. For detailed instructions on exporting a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
19. Publish the sandbox. For detailed instructions on publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

8.7 Moving UDFs from Test to Production

The following sections discuss the procedure to move a UDF added to a catalog entity or User form from test to production:

- [Moving UDFs Added to Catalog Entities](#)
- [Moving UDFs Added to User Forms](#)

See Also:

- ["Limitations of the Test to Production procedures"](#) on page 17-24 for information about test to production limitations.
- ["Handling Concurrency Conflicts"](#) in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about handling concurrency conflicts when multiple users customize an application by using sandboxes and troubleshooting concurrency issues

8.7.1 Moving UDFs Added to Catalog Entities

The procedure to move a UDF added to a catalog entity from test to production is discussed later in this guide. See ["Test to Production procedures for Catalog customizations"](#) on page 17-22 for more information.

8.7.2 Moving UDFs Added to User Forms

Moving a UDF that is added to a User form from test to production consists of the following steps:

- [Exporting the UDF from the Test Environment](#)
- [Importing the UDF into the Production Environment](#)

Note: Before you perform these procedures, ensure that you do not have any popup blockers enabled in your browser and that you have a supported Java Runtime Environment (JRE) installed in the browser. This is because the Deployment Manager uses a popup window and it requires JRE to be installed in the browser.

8.7.2.1 Exporting the UDF from the Test Environment

To export the UDF from the test environment:

1. Log in to Oracle Identity System Administration.
2. Under System Management, click **Export**.
3. Search for **User Metadata**. A list of all available metadata is displayed.
4. Select the UDF that you want to move from test to production, and then click **Select Children**.
5. Click **Select Dependencies**, and then click **Confirmation**.
6. Click **Add for Export**.
7. In the confirmation message that is displayed, click **OK** to exit the wizard.
8. Click **Export**. Alternatively, provide description and then click **Export**.
9. Specify the location to which the content must be exported. A message confirming that the export was successful is displayed.
10. Export the sandbox from the test environment to store all the changes made in your sandbox. For detailed instructions on exporting a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Note:

- The sandbox exported here must be the same, which has been used while creating and adding custom UDFs.
 - The sandbox must not have been published before exporting, because there is no way to export the published sandbox.
-
-

8.7.2.2 Importing the UDF into the Production Environment

To import UDF into the production environment:

1. In Oracle Identity Manager System Administration, under System Management, click **Import**.
2. Specify the path to the XML file that was exported from the test environment by using the Deployment Manager.

3. Click **Add File, Import**, and then confirm the import. A message confirming that the import was successful is displayed.
4. Import the sandbox exported from the test environment. For information about importing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
5. Activate the sandbox to verify the changes. For information about activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
6. Publish the sandbox after you verify the changes. For information about publishing a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

8.8 Synchronizing User-Defined Fields Between Oracle Identity Manager and LDAP

Note:

- LDAP synchronization can be enabled during or any time after installing Oracle Identity Manager.
 - While creating/modifying an attribute using Form Designer, provide a value against LDAP Attribute. This is the value of LDAP attribute name against which the user-defined field (UDF) will be synchronized, and applicable only in LDAP sync enabled environment.
-
-

If you enable LDAP synchronization anytime after creating one or more user-defined fields (UDFs), then you must synchronize these user-defined fields with the corresponding LDAP attributes. To do so, by using the Form Designer, search for and open the form containing the UDF, and then save it (no need to make any other change). Repeat this process of opening the form containing the UDF and then saving it for all UDFs created before enabling LDAP synchronization.

8.9 Attribute Definitions

For all attribute definitions, there is a configuration file for each entity for maintaining the entity attributes. For example, the configuration file for maintaining the user entity attributes is `User.xml`. This configuration file defines all attributes of user entity and their properties. The mapping of the attribute to the backend attributes or columns is also specified in the file. The attributes to be displayed on the UI are determined based on the attribute properties. For example, if an attribute is system-controlled, then the attribute is not displayed in the UI.

[Example 8-1](#) shows the code for a sample `User.xml` configuration file:

Example 8-1 The User.xml Configuration File

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:entity-definition xmlns:tns="http://www.oracle.com/schema/oim/entity"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.oracle.com/schema/oim/entity ../entity.xsd">
  <entity-type child-entity="false">User</entity-type>
  <!-- Defines the repository and data provider to use for this entity -->
```

```

<provider-instance>
  <repository-instance>OperationalDB</repository-instance>
  <provider-type>UserDataProvider</provider-type>
  <parameters>
    <parameter name="table">
      <value>usr</value>
    </parameter>
    <parameter name="id_column">
      <value>usr_key</value>
    </parameter>
    <parameter name="usr_foreign_key_column">
      <value>usr_manager_key</value>
    </parameter>
    <parameter name="org_table">
      <value>act</value>
    </parameter>
    <parameter name="org_id_column">
      <value>act_key</value>
    </parameter>
    <parameter name="org_foreign_key_column">
      <value>parent_key</value>
    </parameter>
  <parameter name="foreign_search_table">
    <value>act:usr:usr:usr:usr</value>
  </parameter>
  <parameter name="foreign_search_table_alias">
    <value>actorg:usrmgr:usrmgr:usrmgr:usrmgr</value>
  </parameter>
  <parameter name="foreign_search_table_to_join_key">
    <value>actorg.act_key:usrmgr.usr_key:usrmgr.usr_key:usrmgr.usr_key:usrmgr.usr_key</value>
  </parameter>
  <parameter name="foreign_search_table_from_join_key">
    <value>usr.act_key:usr.usr_manager_key:usr.usr_manager_key:usr.usr_manager_key:usr.usr_manager_key</value>
  </parameter>
  <parameter name="foreign_search_column">
    <value>actorg.act_name:usrmgr.usr_login:usrmgr.usr_display_name:usrmgr.usr_first_name:usrmgr.usr_last_name</value>
  </parameter>
  <parameter name="foreign_search_column_label">
    <value>Organization Name:Manager Login:Manager Display Name:Manager First Name:Manager Last Name</value>
  </parameter>
  <parameter name="foreign_search_column_alias">
    <value>actorg_act_name:usrmgr_usr_login:usrmgr_usr_display_name:usrmgr_usr_first_name:usrmgr_usr_last_name</value>
  </parameter>
  <parameter name="foreign_search_column_outer_join">
    <value>false:true:true:true:true</value>
  </parameter>
</parameters>
</provider-instance>
  <container-capability>
    <enabled>>false</enabled>
  </container-capability>

```

```

<!-- entity-attributes define the attributes at the API level. These are the
attribute names that the API will return and expects -->
<entity-attributes>
  <attribute name="usr_key">
    <type>number</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
    <multi-represented>>false</multi-represented>
  </attribute-group>
</entity-attributes>
<!-- The metadata attachment defines the entity attribute properties.
These properties will be common across all entities -->
<metadata-attachment>
  <!-- Whether the attribute is searchable by the user -->
  <metadata>
    <name>user-searchable</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <!-- Whether the attribute can be updated in bulk -->
  <metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <!-- The category in the UI to which this attribute belongs -->
  <metadata>
    <name>category</name>
    <value>Account Settings</value>
    <category>properties</category>
  </metadata>
  <!-- The display type of the attribute on the UI -->
  <metadata>
    <name>display-type</name>
    <value>ENTITY</value>
    <category>properties</category>
  </metadata>
  <!-- Whether the attribute value needs to be encrypted or not -->
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <!-- The maximum size that an attribute value can take -->
  <metadata>
    <name>max-size</name>
    <value>19</value>
    <category>properties</category>
  </metadata>
  <!-- Whether the attribute is single valued or multivalued -->
  <metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>

```

```

<!-- Whether an attribute's value can be modified or not -->
<metadata>
  <name>read-only</name>
  <value>true</value>
  <category>properties</category>
</metadata>
<!-- Whether the value is controlled only by the system -->
<metadata>
  <name>system-controlled</name>
  <value>true</value>
  <category>properties</category>
</metadata>
defined attribute -->
  <!-- Whether the attribute is custom or user
  <metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>
</attribute>
<attribute name="act_key">
  <type>number</type>
  <searchable>true</searchable>
  <required>true</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Basic User Information</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>ENTITY</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>entity-type</name>
    <value>Organization</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>entity-type-attributes</name>
    <value>Organization Name</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>

```

```

        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>256</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
    <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    </metadata-attachment>
</attribute>
<attribute name="Last Name">
    <type>string</type>
    <searchable>true</searchable>
    <required>true</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
    <value>Basic User Information</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>

```

```

        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>visible</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>max-size</name>
    <value>80</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata>
</metadata-attachment>
</attribute>
<attribute name="First Name">
    <type>string</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Basic User Information</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>

```

```

    </metadata>
    <metadata>
      <name>display-type</name>
      <value>TEXT</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value>80</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>
</attribute>
<attribute name="Middle Name">
  <type>string</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>

```

```

    <metadata>
      <name>category</name>
      <value>Basic User Information</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>TEXT</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value>80</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>
</attribute>
<attribute name="Full Name">
  <type>string</type>
  <searchable>true</searchable>
  <required>>false</required>
  <MLS>true</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>

```

```

        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Basic User Information</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>164</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
    <attribute name="Display Name">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>true</multi-represented>
    <attribute-group>Basic</attribute-group>
</metadata-attachment>
    <metadata>
        <name>user-searchable</name>

```

```

        <value>true</value>
        <category>properties</category>
</metadata>
<metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>category</name>
    <value>Basic User Information</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>display-type</name>
    <value>TEXT</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>visible</name>
    <value>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>382</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata>

</metadata-attachment>
</attribute>
<attribute name="Xellerate Type">
    <type>string</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>

```

```

<multi-represented>>false</multi-represented>
  <default-value>End-User</default-value>
  <attribute-group>Basic</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>Basic User Information</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>CHECKBOX</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value>30</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>possible-values-code</name>
      <value>Lookup.Users.XellerateType</value>

```

```

        <category>properties</category>
    </metadata>

</metadata-attachment>
</attribute>
<attribute name="usr_password">
    <type>string</type>
    <searchable>true</searchable>
    <required>false</required>
    <MLS>false</MLS>
<multi-represented>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Account Settings</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>SECRET</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>ENCRYPT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>128</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>

```

```

        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>false</value>
        <category>properties</category>
    </metadata>

</metadata-attachment>
</attribute>
<attribute name="usr_disabled">
    <type>string</type>
    <searchable>true</searchable>
    <required>false</required>
    <MLS>false</MLS>
<multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Account Settings</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>CHECKBOX</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>1</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>

```

```

        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Status">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Account Settings</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>LOV</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>25</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>

```

```

        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>read-only</name>
    <value>true</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>possible-values-code</name>
        <value>Lookup.WebClient.Users.Status</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Role">
    <type>string</type>
    <searchable>true</searchable>
    <required>true</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>bulk-updatable</name>
    <value>true</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>category</name>
    <value>Basic User Information</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>display-type</name>
    <value>LOV</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>visible</name>
    <value>true</value>
    <category>properties</category>

```

```

</metadata>
<metadata>
  <name>max-size</name>
  <value>255</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>multi-valued</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>read-only</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>system-controlled</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>custom</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
  <metadata>
    <name>possible-values-code</name>
    <value>Lookup.Users.Role</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>
</attribute>
<attribute name="User Login">
  <type>string</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Account Settings</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>TEXT</value>
    <category>properties</category>

```

```

</metadata>
<metadata>
  <name>encryption</name>
  <value>CLEAR</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>visible</name>
  <value>>true</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>max-size</name>
  <value>256</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>multi-valued</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>read-only</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>system-controlled</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
  <metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_manager_key">
  <type>number</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Basic User Information</value>
    <category>properties</category>
  </metadata>

```

```

    <metadata>
      <name>display-type</name>
      <value>ENTITY</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>entity-type</name>
      <value>User</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>entity-type-attributes</name>
      <value>Manager Login,Manager Display Name,Manager First
Name,Manager Last Name</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value>382</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>
</attribute>
<attribute name="Start Date">
  <type>date</type>
  <searchable>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
</multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>

```

```

<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Account Effective Dates</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>DATE_ONLY</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value></value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>multi-valued</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>read-only</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>system-controlled</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>custom</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>
</attribute>
<attribute name="End Date">
  <type>date</type>

```

```

    <searchable>true</searchable>
    <required>false</required>
    <MLS>false</MLS>
  <multi-represented>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>Account Effective Dates</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>DATE_ONLY</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value></value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>

```

```

    </metadata-attachment>
  </attribute>
  <attribute name="usr_provisioning_date">
    <type>date</type>
    <searchable>true</searchable>
    <required>false</required>
    <MLS>false</MLS>
  <multi-represented>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>Provisioning Dates</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>DATE_ONLY</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value></value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>

```

```

        </metadata>                <metadata>
            <name>custom</name>
            <value>>false</value>
            <category>properties</category>
        </metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_deprovisioning_date">
    <type>date</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Provisioning Dates</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>DATE_ONLY</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value></value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>

```

```

    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>
</attribute>
<attribute name="usr_provisioned_date">
  <type>date</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>System</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>DATE_ONLY</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value></value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>
</attribute>

```

```

    <metadata>
      <name>read-only</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
  </metadata>
  <metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>

  </metadata-attachment>
</attribute>
<attribute name="usr_deprovisioned_date">
  <type>date</type>
  <searchable>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>System</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>DATE_ONLY</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value></value>
    <category>properties</category>
  </metadata>

```

```

    <metadata>
      <name>multi-valued</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>
</attribute>
<attribute name="Email">
  <type>string</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Basic User Information</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>TEXT</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>

```

```

    <metadata>
      <name>max-size</name>
      <value>256</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>
</attribute>
<attribute name="usr_locked">
  <type>string</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Account Settings</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>LOV</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>

```

```

        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>1</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>possible-values-code</name>
        <value>Users.Lock User</value>
        <category>properties</category>
    </metadata>
</metadata>

</metadata-attachment>
</attribute>
<attribute name="Locked On">
    <type>date</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Lifecycle</value>
        <category>properties</category>
    </metadata>
</metadata>

```

```

        <name>display-type</name>
        <value>DATE_ONLY</value>
        <category>properties</category>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value></value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Automatically Delete On">
    <type>date</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>

```

```

        <name>category</name>
        <value>Lifecycle</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>DATE_ONLY</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value></value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    </metadata-attachment>
</attribute>
<attribute name="Manually Locked">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>

```

```

        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Lifecycle</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>1</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    </metadata-attachment>
</attribute>
<attribute name="usr_login_attempts_ctr">
    <type>number</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>

```

```

        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>NUMBER</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>19</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_create">
    <type>date</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>

```

```
<multi-represented>>false</multi-represented>
  <attribute-group>Basic</attribute-group>
    <metadata-attachment>
      <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>display-type</name>
        <value>DATE_ONLY</value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>max-size</name>
        <value></value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>read-only</name>
        <value>>true</value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>system-controlled</name>
        <value>>true</value>
        <category>properties</category>
      </metadata>
      <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
      </metadata>
    </metadata-attachment>
  </attribute>
```

```

<attribute name="usr_update">
  <type>date</type>
  <searchable>true</searchable>
  <required>false</required>
  <MLS>false</MLS>
<multi-represented>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>System</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>DATE_ONLY</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value></value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>false</value>

```

```

        <category>properties</category>
    </metadata>

</metadata-attachment>
</attribute>
<attribute name="usr_timezone">
    <type>string</type>
    <searchable>true</searchable>
    <required>false</required>
    <MLS>false</MLS>
<multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Preferences</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TIME_ZONE</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>100</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_locale">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Preferences</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>LOV</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>100</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>

```

```

        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>possible-values-code</name>
        <value>Notification.Languages</value>
        <category>properties</category>
    </metadata>

</metadata-attachment>
</attribute>
<attribute name="usr_pwd_cant_change">
    <type>string</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>CHECKBOX</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>1</value>

```

```

        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata>

</metadata-attachment>
</attribute>
<attribute name="usr_pwd_must_change">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>CHECKBOX</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>

```

```

        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>max-size</name>
    <value>1</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_pwd_never_expires">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>CHECKBOX</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>

```

```

        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>1</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata>

</metadata-attachment>
</attribute>
<attribute name="usr_pwd_expire_date">
    <type>date</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>DATE_ONLY</value>

```

```

        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>max-size</name>
    <value></value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_pwd_warn_date">
    <type>date</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>

```

```

        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>display-type</name>
    <value>DATE_ONLY</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>max-size</name>
    <value></value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
</metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_pwd_expired">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>bulk-updatable</name>
    <value>>false</value>

```

```

        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>category</name>
    <value>System</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>display-type</name>
    <value>CHECKBOX</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>max-size</name>
    <value>1</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_pwd_warned">
    <type>string</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>

```

```

        <category>properties</category>
    </metadata>
<metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>category</name>
    <value>System</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>display-type</name>
    <value>CHECKBOX</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>1</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata>

</metadata-attachment>
</attribute>
<attribute name="usr_pwd_reset_attempts_ctr">
    <type>number</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>false</multi-represented>

```

```
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>System</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>NUMBER</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value></value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_change_pwd_at_next_logon">
```

```

<type>string</type>
<searchable>true</searchable>
<required>false</required>
<MLS>false</MLS>
<multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>System</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>CHECKBOX</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value>1</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>multi-valued</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>read-only</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>system-controlled</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>custom</name>
    <value>false</value>
    <category>properties</category>
  </metadata>

```

```
</metadata>

</metadata-attachment>
</attribute>
<attribute name="usr_data_level">
  <type>string</type>
  <searchable>true</searchable>
  <required>false</required>
  <MLS>false</MLS>
<multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>System</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>CHECKBOX</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value>1</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>multi-valued</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>read-only</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>system-controlled</name>
    <value>true</value>
```

```

        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>

</metadata-attachment>
</attribute>

<attribute name="usr_pwd_min_age_date">
    <type>date</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
    <attribute-group>Extended</attribute-group>
    <metadata-attachment>
        <metadata>
            <name>user-searchable</name>
            <value>>false</value>
            <category>properties</category>
        </metadata>
        <metadata>
            <name>bulk-updatable</name>
            <value>>false</value>
            <category>properties</category>
        </metadata>
        <metadata>
            <name>category</name>
            <value>System</value>
            <category>properties</category>
        </metadata>
        <metadata>
            <name>display-type</name>
            <value>DATE_ONLY</value>
            <category>properties</category>
        </metadata>
        <metadata>
            <name>encryption</name>
            <value>CLEAR</value>
            <category>properties</category>
        </metadata>
        <metadata>
            <name>visible</name>
            <value>>false</value>
            <category>properties</category>
        </metadata>
        <metadata>
            <name>max-size</name>
            <value></value>
            <category>properties</category>
        </metadata>
        <metadata>
            <name>multi-valued</name>
            <value>>false</value>
            <category>properties</category>
        </metadata>
        <metadata>
            <name>read-only</name>

```

```

        <value>true</value>
        <category>properties</category>
</metadata>
<metadata>
  <name>system-controlled</name>
  <value>true</value>
  <category>properties</category>
</metadata>
  <metadata>
    <name>custom</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_createby">
  <type>number</type>
  <searchable>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Basic</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>System</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>TEXT</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value></value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>multi-valued</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_updateby">
    <type>number</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>

```

```

        <value></value>
        <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_created">
    <type>date</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>DATE_ONLY</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>max-size</name>
    <value></value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="usr_policy_update">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>

```

```

        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>1</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>

    </metadata-attachment>
</attribute>
<attribute name="Country">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>

```

```

        <value>TEXT</value>
        <category>properties</category>
    </metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>visible</name>
    <value>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>100</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Department Number">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>

```

```

        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>80</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>

    </metadata-attachment>
</attribute>
<attribute name="Description">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>2000</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    </metadata-attachment>
</attribute>
<attribute name="Common Name">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>

```

```

        <value>true</value>
        <category>properties</category>
</metadata>
<metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>category</name>
    <value>Other User Attributes</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>display-type</name>
    <value>TEXT</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>visible</name>
    <value>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>240</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata>

</metadata-attachment>
</attribute>
<attribute name="Employee Number">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>

```

```

<multi-represented>>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>Other User Attributes</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>TEXT</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value>80</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>
</attribute>

```

```
<attribute name="Fax">
  <type>string</type>
  <searchable>true</searchable>
  <required>false</required>
  <MLS>false</MLS>
<multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Other User Attributes</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>TEXT</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value>4000</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>multi-valued</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>read-only</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>system-controlled</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>custom</name>
    <value>false</value>
  </metadata>
</metadata-attachment>
</attribute>
```

```

        <category>properties</category>
    </metadata>

</metadata-attachment>
</attribute>
<attribute name="Generation Qualifier">
    <type>string</type>
    <searchable>true</searchable>
    <required>false</required>
    <MLS>false</MLS>
<multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>20</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>

</metadata-attachment>
</attribute>
<attribute name="Hire Date">
    <type>date</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>DATE_ONLY</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value></value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Home Phone">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>20</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>

```

```

        <value>>false</value>
        <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Locality Name">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>

```

```

        <value>80</value>
        <category>properties</category>
    </metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Mobile">
    <type>string</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>

```

```

        <value>true</value>
        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>max-size</name>
    <value>20</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Pager">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>

```

```

        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
<metadata>
    <name>visible</name>
    <value>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>20</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Home Postal Address">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>

```

```

        <value>TEXT</value>
        <category>properties</category>
    </metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>visible</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>256</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Postal Address">
    <type>string</type>
    <searchable>true</searchable>
    <required>false</required>
    <MLS>>false</MLS>
</multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>

```

```

        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>display-type</name>
    <value>TEXT</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>visible</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>256</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Postal Code">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>30</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>

    </metadata-attachment>
</attribute>
<attribute name="PO Box">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>

```

```

        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>20</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="State">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>

```

```
<multi-represented>>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>Other User Attributes</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>TEXT</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value>80</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>
</attribute>
```

```

<attribute name="Street">
  <type>string</type>
  <searchable>true</searchable>
  <required>false</required>
  <MLS>false</MLS>
<multi-represented>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>Other User Attributes</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>TEXT</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value>80</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>false</value>

```

```

        <category>properties</category>
    </metadata>

</metadata-attachment>
</attribute>
<attribute name="Telephone Number">
    <type>string</type>
    <searchable>true</searchable>
    <required>false</required>
    <MLS>false</MLS>
<multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>4000</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>

</metadata-attachment>
</attribute>
<attribute name="Title">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>80</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>

```

```

        <value>>false</value>
        <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Initials">
    <type>string</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>10</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Common Name Generated">
    <type>number</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>NUMBER</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>

```

```

        <value>1</value>
        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="Password Generated">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>System</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata>
<metadata>
    <name>max-size</name>
    <value>1</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>true</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="LDAP Organization">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>

```

```

        <value>CLEAR</value>
        <category>properties</category>
</metadata>
<metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>80</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="LDAP Organization Unit">
    <type>string</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>

```

```

        <value>TEXT</value>
        <category>properties</category>
</metadata>
<metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>visible</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>max-size</name>
    <value>80</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>multi-valued</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>read-only</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
<metadata>
    <name>system-controlled</name>
    <value>>false</value>
    <category>properties</category>
</metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute>
<attribute name="LDAP GUID">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>

```

```

        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>256</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>

    </metadata-attachment>
</attribute>
<attribute name="LDAP DN">
    <type>string</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>

```

```

        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Other User Attributes</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>TEXT</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>256</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>true</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>system-controlled</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>custom</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    </metadata-attachment>
</attribute>
<attribute name="FA Language">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>

```

```
        <value>true</value>
        <category>properties</category>
</metadata>
<metadata>
  <name>bulk-updatable</name>
  <value>true</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>category</name>
  <value>Preferences</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>display-type</name>
  <value>TEXT</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>encryption</name>
  <value>CLEAR</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>visible</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>max-size</name>
  <value>100</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>multi-valued</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>read-only</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>system-controlled</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>custom</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
</metadata-attachment>
</attribute>
<attribute name="Embedded Help">
  <type>string</type>
  <searchable>true</searchable>
  <required>>false</required>
```

```

    <MLS>false</MLS>
  <multi-represented>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Preferences</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>LOV</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value>10</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>multi-valued</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>read-only</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>system-controlled</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>custom</name>
    <value>false</value>
    <category>properties</category>
  </metadata>

```

```
<metadata>
    <name>possible-values-code</name>
    <value>Lookup.Users.EmbeddedHelp</value>
    <category>properties</category>
</metadata>

</metadata-attachment>
</attribute>
<attribute name="Number Format">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Preferences</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>LOV</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>30</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
</metadata-attachment>
</attribute-group>
</multi-represented>
</attribute>
</attribute-definition>
```

```

</metadata>
<metadata>
  <name>system-controlled</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>custom</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
  <metadata>
    <name>possible-values-code</name>
    <value>Lookup.Users.NumberFormat</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>
</attribute>
<attribute name="Date Format">
  <type>string</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>Preferences</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>LOV</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value>20</value>
      <category>properties</category>
  </metadata-attachment>

```

```

    </metadata>
    <metadata>
      <name>multi-valued</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>read-only</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>possible-values-code</name>
      <value>Lookup.Users.DateFormat</value>
      <category>properties</category>
    </metadata>
  </metadata-attachment>
</attribute>
  <attribute name="Time Format">
    <type>string</type>
    <searchable>>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
  <multi-represented>>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>Preferences</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>LOV</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
  </metadata-attachment>

```

```

</metadata>
<metadata>
  <name>visible</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>max-size</name>
  <value>20</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>multi-valued</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>read-only</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>system-controlled</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>custom</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
  <metadata>
    <name>possible-values-code</name>
    <value>Lookup.Users.TimeFormat</value>
    <category>properties</category>
  </metadata>
</metadata-attachment>
</attribute>
<attribute name="Currency">
  <type>string</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Preferences</value>
    <category>properties</category>

```

```

</metadata>
<metadata>
  <name>display-type</name>
  <value>LOV</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>encryption</name>
  <value>CLEAR</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>visible</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>max-size</name>
  <value>20</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>multi-valued</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>read-only</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>system-controlled</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>custom</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
  <metadata>
    <name>possible-values-code</name>
    <value>Lookup.Users.Currency</value>
    <category>properties</category>
  </metadata>
</metadata>

</metadata-attachment>
</attribute>
<attribute name="Font Size">
  <type>string</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>false</value>
    <category>properties</category>
  </metadata>

```

```

</metadata>
<metadata>
  <name>bulk-updatable</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>category</name>
  <value>Preferences</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>display-type</name>
  <value>LOV</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>encryption</name>
  <value>CLEAR</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>visible</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>max-size</name>
  <value>10</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>multi-valued</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>read-only</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>system-controlled</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>custom</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
  <metadata>
    <name>possible-values-code</name>
    <value>Lookup.Users.FontSize</value>
    <category>properties</category>
  </metadata>
</metadata>

</metadata-attachment>
</attribute>
<attribute name="Color Contrast">
  <type>string</type>

```

```
<searchable>true</searchable>
<required>false</required>
<MLS>false</MLS>
<multi-represented>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Preferences</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>LOV</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>encryption</name>
    <value>CLEAR</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>visible</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>max-size</name>
    <value>10</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>multi-valued</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>read-only</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>system-controlled</name>
    <value>false</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>custom</name>
    <value>false</value>
    <category>properties</category>
  </metadata>

```

```

</metadata>          <metadata>
    <name>possible-values-code</name>
    <value>Lookup.Users.ColorContrast</value>
    <category>properties</category>
</metadata>

    </metadata-attachment>
</attribute>
<attribute name="Accessibility Mode">
    <type>string</type>
    <searchable>true</searchable>
    <required>>false</required>
    <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
    <metadata>
        <name>user-searchable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>bulk-updatable</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>category</name>
        <value>Preferences</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>display-type</name>
        <value>LOV</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>encryption</name>
        <value>CLEAR</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>visible</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>max-size</name>
        <value>20</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>multi-valued</name>
        <value>>false</value>
        <category>properties</category>
    </metadata>
    <metadata>
        <name>read-only</name>
        <value>>false</value>
        <category>properties</category>

```

```

    </metadata>
    <metadata>
      <name>system-controlled</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>custom</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>possible-values-code</name>
      <value>Lookup.Users.AccessibilityMode</value>
      <category>properties</category>
    </metadata>

  </metadata-attachment>
</attribute>
<attribute name="FA Territory">
  <type>string</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
  <attribute-group>Extended</attribute-group>
  <metadata-attachment>
    <metadata>
      <name>user-searchable</name>
      <value>>true</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>bulk-updatable</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>category</name>
      <value>Preferences</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>display-type</name>
      <value>TEXT</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>encryption</name>
      <value>CLEAR</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>visible</name>
      <value>>false</value>
      <category>properties</category>
    </metadata>
    <metadata>
      <name>max-size</name>
      <value>100</value>
      <category>properties</category>
  </metadata-attachment>

```

```

</metadata>
<metadata>
  <name>multi-valued</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>read-only</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>system-controlled</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>custom</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>possible-values-code</name>
  <value></value>
  <category>properties</category>
</metadata>
</metadata-attachment>
</attribute>
<attribute name="User Name Preferred Language">
  <type>string</type>
  <searchable>>true</searchable>
  <required>>false</required>
  <MLS>>false</MLS>
<multi-represented>>false</multi-represented>
<attribute-group>Extended</attribute-group>
<metadata-attachment>
  <metadata>
    <name>user-searchable</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>bulk-updatable</name>
    <value>>true</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>category</name>
    <value>Preferences</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>display-type</name>
    <value>LOV</value>
    <category>properties</category>
  </metadata>
  <metadata>
    <name>lookup-query</name>
    <value>select+MLS_LOCALE_CODE+as+USR_NAME_PREFERRED_LANG+from+mls_locale+where+loc

```

```

ale_flag=0+OR+locale_flag=1+order+by+mls_locale_code+asc</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>lookup-query-display-column</name>
  <value>USR_NAME_PREFERRED_LANG</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>lookup-query-save-column</name>
  <value>USR_NAME_PREFERRED_LANG</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>encryption</name>
  <value>CLEAR</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>visible</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>max-size</name>
  <value>20</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>multi-valued</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>read-only</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>system-controlled</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>custom</name>
  <value>>false</value>
  <category>properties</category>
</metadata>
<metadata>
  <name>possible-values-code</name>
  <value></value>
  <category>properties</category>
</metadata>
</metadata-attachment>
</attribute>
</entity-attributes>

<!-- The target fields define the attribute columns in the DB. These are not
exposed via the User Management APIs. -->
<target-fields>

```

```
<field name="usr_key">
  <type>number</type>
  <required>true</required>
</field>
<field name="act_key">
  <type>number</type>
  <required>true</required>
</field>
<field name="usr_last_name">
  <type>string</type>
  <required>true</required>
</field>
<field name="usr_first_name">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_middle_name">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_full_name">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_display_name">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_type">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_password">
  <type>string</type>
  <required>true</required>
</field>
<field name="usr_disabled">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_pwd_cant_change">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_pwd_must_change">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_pwd_never_expires">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_status">
  <type>string</type>
  <required>false</required>
</field>
<field name="usr_emp_type">
  <type>string</type>
  <required>false</required>
</field>
```

```
<field name="usr_login">
  <type>string</type>
  <required>true</required>
</field>
<field name="usr_pwd_expire_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_pwd_warn_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_manager_key">
  <type>number</type>
  <required>>false</required>
</field>
<field name="usr_pwd_warned">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_pwd_expired">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_start_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_end_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_provisioning_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_deprovisioning_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_provisioned_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_deprovisioned_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_email">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_locked">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_locked_on">
  <type>date</type>
  <required>>false</required>
</field>
```

```
<field name="usr_automatically_delete_on">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_manually_locked">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_login_attempts_ctr">
  <type>number</type>
  <required>>false</required>
</field>
<field name="usr_pwd_reset_attempts_ctr">
  <type>number</type>
  <required>>false</required>
</field>
<field name="usr_data_level">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_change_pwd_at_next_logon">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_pwd_min_age_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_create">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_update">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_timezone">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_locale">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_createby">
  <type>number</type>
  <required>>false</required>
</field>
<field name="usr_updateby">
  <type>number</type>
  <required>>false</required>
</field>
<field name="usr_created">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_policy_update">
  <type>string</type>
  <required>>false</required>
</field>
```

```
<field name="usr_country">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_dept_no">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_description">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_common_name">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_emp_no">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_fax">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_gen_qualifier">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_hire_date">
  <type>date</type>
  <required>>false</required>
</field>
<field name="usr_home_phone">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_locality_name">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_mobile">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_pager">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_home_postal_address">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_postal_address">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_postal_code">
  <type>string</type>
  <required>>false</required>
</field>
```

```
<field name="usr_po_box">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_state">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_street">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_telephone_number">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_title">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_initials">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_pwd_generated">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_cn_generated">
  <type>number</type>
  <required>>false</required>
</field>
<field name="usr_ldap_organization">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_ldap_organization_unit">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_ldap_guid">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_ldap_dn">
  <type>string</type>
  <required>>false</required>
</field>
  <field name="usr_language">
    <type>string</type>
    <required>>false</required>
  </field>
<field name="usr_color_contrast">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_accessibility_mode">
  <type>string</type>
  <required>>false</required>
</field>
<field name="usr_time_format">
```

```
        <type>string</type>
        <required>>false</required>
    </field>
    <field name="usr_date_format">
        <type>string</type>
        <required>>false</required>
    </field>
    <field name="usr_currency">
        <type>string</type>
        <required>>false</required>
    </field>
    <field name="usr_number_format">
        <type>string</type>
        <required>>false</required>
    </field>
    <field name="usr_font_size">
        <type>string</type>
        <required>>false</required>
    </field>
    <field name="usr_embedded_help">
        <type>string</type>
        <required>>false</required>
    </field>
    <field name="usr_territory">
        <type>string</type>
        <required>>false</required>
    </field>
    <field name="usr_name_preferred_lang">
        <type>string</type>
        <required>>false</required>
    </field>
</target-fields>
<!-- The attribute mapping defines which backend DB columns are mapped to the
frontend attributes exposed at the API level -->
<attribute-maps>
    <attribute-map>
        <entity-attribute>usr_key</entity-attribute>
        <target-field>usr_key</target-field>
    </attribute-map>
    <attribute-map>
        <entity-attribute>act_key</entity-attribute>
        <target-field>act_key</target-field>
    </attribute-map>
    <attribute-map>
        <entity-attribute>Last Name</entity-attribute>
        <target-field>usr_last_name</target-field>
    </attribute-map>
    <attribute-map>
        <entity-attribute>First Name</entity-attribute>
        <target-field>usr_first_name</target-field>
    </attribute-map>
    <attribute-map>
        <entity-attribute>Middle Name</entity-attribute>
        <target-field>usr_middle_name</target-field>
    </attribute-map>
    <attribute-map>
        <entity-attribute>Full Name</entity-attribute>
        <target-field>usr_full_name</target-field>
    </attribute-map>
</attribute-maps>
```

```
<entity-attribute>Display Name</entity-attribute>
<target-field>usr_display_name</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Xellerate Type</entity-attribute>
  <target-field>usr_type</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_password</entity-attribute>
  <target-field>usr_password</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_disabled</entity-attribute>
  <target-field>usr_disabled</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_pwd_cant_change</entity-attribute>
  <target-field>usr_pwd_cant_change</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_pwd_must_change</entity-attribute>
  <target-field>usr_pwd_must_change</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_pwd_never_expires</entity-attribute>
  <target-field>usr_pwd_never_expires</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Status</entity-attribute>
  <target-field>usr_status</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Role</entity-attribute>
  <target-field>usr_emp_type</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>User Login</entity-attribute>
  <target-field>usr_login</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_pwd_expire_date</entity-attribute>
  <target-field>usr_pwd_expire_date</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_pwd_warn_date</entity-attribute>
  <target-field>usr_pwd_warn_date</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_manager_key</entity-attribute>
  <target-field>usr_manager_key</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_pwd_expired</entity-attribute>
  <target-field>usr_pwd_expired</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_pwd_warned</entity-attribute>
  <target-field>usr_pwd_warned</target-field>
</attribute-map>
<attribute-map>
```

```
<entity-attribute>Start Date</entity-attribute>
  <target-field>usr_start_date</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>End Date</entity-attribute>
  <target-field>usr_end_date</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_provisioning_date</entity-attribute>
  <target-field>usr_provisioning_date</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_deprovisioning_date</entity-attribute>
  <target-field>usr_deprovisioning_date</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_provisioned_date</entity-attribute>
  <target-field>usr_provisioned_date</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_deprovisioned_date</entity-attribute>
  <target-field>usr_deprovisioned_date</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Email</entity-attribute>
  <target-field>usr_email</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_locked</entity-attribute>
  <target-field>usr_locked</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Locked On</entity-attribute>
  <target-field>usr_locked_on</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Automatically Delete On</entity-attribute>
  <target-field>usr_automatically_delete_on</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Manually Locked</entity-attribute>
  <target-field>usr_manually_locked</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Automatically Delete On</entity-attribute>
  <target-field>usr_automatically_delete_on</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_login_attempts_ctr</entity-attribute>
  <target-field>usr_login_attempts_ctr</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_pwd_reset_attempts_ctr</entity-attribute>
  <target-field>usr_pwd_reset_attempts_ctr</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>usr_data_level</entity-attribute>
  <target-field>usr_data_level</target-field>
</attribute-map>
<attribute-map>
```

```

    <entity-attribute>usr_change_pwd_at_next_logon</entity-attribute>
    <target-field>usr_change_pwd_at_next_logon</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>usr_pwd_min_age_date</entity-attribute>
    <target-field>usr_pwd_min_age_date</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>usr_create</entity-attribute>
    <target-field>usr_create</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>usr_update</entity-attribute>
    <target-field>usr_update</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>usr_timezone</entity-attribute>
    <target-field>usr_timezone</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>usr_locale</entity-attribute>
    <target-field>usr_locale</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>usr_createby</entity-attribute>
    <target-field>usr_createby</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>usr_updateby</entity-attribute>
    <target-field>usr_updateby</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>usr_created</entity-attribute>
    <target-field>usr_created</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>usr_policy_update</entity-attribute>
    <target-field>usr_policy_update</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>Country</entity-attribute>
    <target-field>usr_country</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>Department Number</entity-attribute>
    <target-field>usr_dept_no</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>Description</entity-attribute>
    <target-field>usr_description</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>Common Name</entity-attribute>
    <target-field>usr_common_name</target-field>
</attribute-map>
<attribute-map>
    <entity-attribute>Employee Number</entity-attribute>
    <target-field>usr_emp_no</target-field>
</attribute-map>
<attribute-map>

```

```
<entity-attribute>Fax</entity-attribute>
<target-field>usr_fax</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Generation Qualifier</entity-attribute>
  <target-field>usr_gen_qualifier</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Hire Date</entity-attribute>
  <target-field>usr_hire_date</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Home Phone</entity-attribute>
  <target-field>usr_home_phone</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Locality Name</entity-attribute>
  <target-field>usr_locality_name</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Mobile</entity-attribute>
  <target-field>usr_mobile</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Pager</entity-attribute>
  <target-field>usr_pager</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Home Postal Address</entity-attribute>
  <target-field>usr_home_postal_address</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Postal Address</entity-attribute>
  <target-field>usr_postal_address</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Postal Code</entity-attribute>
  <target-field>usr_postal_code</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>PO Box</entity-attribute>
  <target-field>usr_po_box</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>State</entity-attribute>
  <target-field>usr_state</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Street</entity-attribute>
  <target-field>usr_street</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Telephone Number</entity-attribute>
  <target-field>usr_telephone_number</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Title</entity-attribute>
  <target-field>usr_title</target-field>
</attribute-map>
<attribute-map>
```

```
<entity-attribute>Initials</entity-attribute>
<target-field>usr_initials</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Common Name Generated</entity-attribute>
  <target-field>usr_cn_generated</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Password Generated</entity-attribute>
  <target-field>usr_pwd_generated</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>LDAP Organization</entity-attribute>
  <target-field>usr_ldap_organization</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>LDAP Organization Unit</entity-attribute>
  <target-field>usr_ldap_organization_unit</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>LDAP GUID</entity-attribute>
  <target-field>usr_ldap_guid</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>LDAP DN</entity-attribute>
  <target-field>usr_ldap_dn</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>FA Language</entity-attribute>
  <target-field>usr_language</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Embedded Help</entity-attribute>
  <target-field>usr_embedded_help</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Font Size</entity-attribute>
  <target-field>usr_font_size</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Color Contrast</entity-attribute>
  <target-field>usr_color_contrast</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Accessibility Mode</entity-attribute>
  <target-field>usr_accessibility_mode</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Number Format</entity-attribute>
  <target-field>usr_number_format</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Date Format</entity-attribute>
  <target-field>usr_date_format</target-field>
</attribute-map>
<attribute-map>
  <entity-attribute>Time Format</entity-attribute>
  <target-field>usr_time_format</target-field>
</attribute-map>
<attribute-map>
```

```

    <entity-attribute>Currency</entity-attribute>
    <target-field>usr_currency</target-field>
  </attribute-map>
</attribute-map>
  <entity-attribute>FA Territory</entity-attribute>
  <target-field>usr_territory</target-field>
</attribute-map>
</attribute-map>
  <entity-attribute>User Name Preferred Language</entity-attribute>
  <target-field>usr_name_preferred_lang</target-field>
</attribute-map>
</attribute-maps>
<!-- The following section defines various User configurations for the UI -->
<metadata-attachment xmlns="">
  <!-- 1 -->
  <!--
    This section defines the categories that will be available in the UI.
    Each attribute must belong to one of these categories
  -->
  <metadata>
    <!-- The unique ID of the category -->
    <name>Basic User Information</name>
    <!-- The display name of the category. This will be a key in a bundle
    which will be fetched by the config API -->
    <value>Basic User Information</value>
    <category>categories</category>
  </metadata>
  <metadata>
    <name>Account Settings</name>
    <value>Account Settings</value>
    <category>categories</category>
  </metadata>
  <metadata>
    <name>Account Effective Dates</name>
    <value>Account Effective Dates</value>
    <category>categories</category>
  </metadata>
  <metadata>
    <name>Provisioning Dates</name>
    <value>Provisioning Dates</value>
    <category>categories</category>
  </metadata>
  <metadata>
    <name>Lifecycle</name>
    <value>Lifecycle</value>
    <category>categories</category>
  </metadata>
  <metadata>
    <name>System</name>
    <value>System</value>
    <category>categories</category>
  </metadata>
  <metadata>
    <name>Other User Attributes</name>
    <value>Other User Attributes</value>
    <category>categories</category>
  </metadata>
  <metadata>
    <!-- The unique ID of the category -->
    <name>CustomAttributes</name>

```

```

        <!-- The display name of the category. This will be a key in a bundle
which will be fetched by the config API -->
        <value>Custom Attributes</value>
        <category>categories</category>
</metadata>
<metadata>
    <name>Preferences</name>
    <value>Preferences</value>
    <category>categories</category>
</metadata>

<!-- 2 -->
<!--
    This section defines the ordering amongst the categories
-->

<metadata>
    <name>1</name>
    <value>Basic User Information</value>
    <category>categories.order</category>
</metadata>
<metadata>
    <name>2</name>
    <value>Account Settings</value>
    <category>categories.order</category>
</metadata>
<metadata>
    <name>3</name>
    <value>Account Effective Dates</value>
    <category>categories.order</category>
</metadata>
<metadata>
    <name>4</name>
    <value>Provisioning Dates</value>
    <category>categories.order</category>
</metadata>
<metadata>
    <name>5</name>
    <value>Lifecycle</value>
    <category>categories.order</category>
</metadata>
<metadata>
    <name>6</name>
    <value>System</value>
    <category>categories.order</category>
</metadata>
<metadata>
    <name>7</name>
    <value>Other User Attributes</value>
    <category>categories.order</category>
</metadata>
<metadata>
    <name>8</name>
    <value>CustomAttributes</value>
    <category>categories.order</category>
</metadata>
<metadata>
    <name>9</name>
    <value>Preferences</value>
    <category>categories.order</category>

```

```
</metadata>

<!-- 3 -->
<!--
    This section defines the ordering of the attributes within each
    category. The attributes will be displayed on the UI in the order defined here.
-->
<metadata>
  <name>1</name>
  <value>User Login</value>
  <category>categories.Account Settings</category>
</metadata>
<metadata>
  <name>2</name>
  <value>usr_password</value>
  <category>categories.Account Settings</category>
</metadata>
<metadata>
  <name>3</name>
  <value>Status</value>
  <category>categories.Account Settings</category>
</metadata>
<metadata>
  <name>4</name>
  <value>usr_locked</value>
  <category>categories.Account Settings</category>
</metadata>
<metadata>
  <name>5</name>
  <value>usr_key</value>
  <category>categories.Account Settings</category>
</metadata>

<metadata>
  <name>1</name>
  <value>First Name</value>
  <category>categories.Basic User Information</category>
</metadata>
<metadata>
  <name>2</name>
  <value>Middle Name</value>
  <category>categories.Basic User Information</category>
</metadata>
<metadata>
  <name>3</name>
  <value>Last Name</value>
  <category>categories.Basic User Information</category>
</metadata>
<metadata>
  <name>4</name>
  <value>Xellerate Type</value>
  <category>categories.Basic User Information</category>
</metadata>
<metadata>
  <name>5</name>
  <value>Email</value>
  <category>categories.Basic User Information</category>
</metadata>
<metadata>
```

```
<name>6</name>
<value>usr_manager_key</value>
<category>categories.Basic User Information</category>
</metadata>
<metadata>
  <name>7</name>
  <value>act_key</value>
  <category>categories.Basic User Information</category>
</metadata>
<metadata>
  <name>8</name>
  <value>Role</value>
  <category>categories.Basic User Information</category>
</metadata>
<metadata>
  <name>9</name>
  <value>Full Name</value>
  <category>categories.Basic User Information</category>
</metadata>

<metadata>
  <name>10</name>
  <value>Display Name</value>
  <category>categories.Basic User Information</category>
</metadata>
<metadata>
  <name>1</name>
  <value>Start Date</value>
  <category>categories.Account Effective Dates</category>
</metadata>

<metadata>
  <name>2</name>
  <value>End Date</value>
  <category>categories.Account Effective Dates</category>
</metadata>
<metadata>
  <name>1</name>
  <value>usr_provisioning_date</value>
  <category>categories.Provisioning Dates</category>
</metadata>

<metadata>
  <name>2</name>
  <value>usr_deprovisioning_date</value>
  <category>categories.Provisioning Dates</category>
</metadata>
<metadata>
  <name>1</name>
  <value>Manually Locked</value>
  <category>categories.Lifecycle</category>
</metadata>
<metadata>
  <name>2</name>
  <value>Locked On</value>
  <category>categories.Lifecycle</category>
</metadata>

<metadata>
  <name>3</name>
```

```
        <value>Automatically Delete On</value>
        <category>categories.Lifecycle</category>
</metadata>
<metadata>
    <name>1</name>
    <value>usr_provisioned_date</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>2</name>
    <value>usr_deprovisioned_date</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>3</name>
    <value>usr_login_attempts_ctr</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>4</name>
    <value>usr_create</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>5</name>
    <value>usr_update</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>6</name>
    <value>usr_pwd_cant_change</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>7</name>
    <value>usr_pwd_must_change</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>8</name>
    <value>usr_pwd_never_expires</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>9</name>
    <value>usr_pwd_expire_date</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>10</name>
    <value>usr_pwd_warn_date</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>11</name>
    <value>usr_pwd_expired</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>12</name>
```

```

        <value>usr_pwd_warned</value>
        <category>categories.System</category>
</metadata>
<metadata>
    <name>13</name>
    <value>usr_pwd_reset_attempts_ctr</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>14</name>
    <value>usr_change_pwd_at_next_logon</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>15</name>
    <value>usr_pwd_min_age_date</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>16</name>
    <value>usr_createby</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>17</name>
    <value>usr_updateby</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>18</name>
    <value>usr_created</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>19</name>
    <value>usr_policy_update</value>
    <category>categories.System</category>
</metadata>

<metadata>
    <name>20</name>
    <value>Password Generated</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>21</name>
    <value>usr_data_level</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>22</name>
    <value>Common Name Generated</value>
    <category>categories.System</category>
</metadata>
<metadata>
    <name>1</name>
    <value>Country</value>
    <category>categories.Other User Attributes</category>
</metadata>
<metadata>

```

```
<name>2</name>
<value>Department Number</value>
<category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>3</name>
  <value>Description</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>4</name>
  <value>Common Name</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>5</name>
  <value>Employee Number</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>6</name>
  <value>Fax</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>7</name>
  <value>Generation Qualifier</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>8</name>
  <value>Hire Date</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>9</name>
  <value>Home Phone</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>10</name>
  <value>Locality Name</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>11</name>
  <value>Mobile</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>12</name>
  <value>Pager</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>13</name>
  <value>Home Postal Address</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
```

```
<name>14</name>
<value>Postal Address</value>
<category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>15</name>
  <value>Postal Code</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>16</name>
  <value>PO Box</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>17</name>
  <value>State</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>18</name>
  <value>Street</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>19</name>
  <value>Telephone Number</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>20</name>
  <value>Title</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>21</name>
  <value>Initials</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>22</name>
  <value>LDAP Organization</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>23</name>
  <value>LDAP Organization Unit</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>24</name>
  <value>LDAP GUID</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
  <name>25</name>
  <value>LDAP DN</value>
  <category>categories.Other User Attributes</category>
</metadata>
<metadata>
```

```
<name>1</name>
<value>usr_locale</value>
<category>categories.Preferences</category>
</metadata>
<metadata>
  <name>2</name>
  <value>usr_timezone</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>3</name>
  <value>Number Format</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>4</name>
  <value>Currency</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>5</name>
  <value>Date Format</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>6</name>
  <value>Time Format</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>7</name>
  <value>Accessibility Mode</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>8</name>
  <value>Color Contrast</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>9</name>
  <value>Font Size</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>10</name>
  <value>Embedded Help</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>11</name>
  <value>FA Language</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
  <name>12</name>
  <value>FA Territory</value>
  <category>categories.Preferences</category>
</metadata>
<metadata>
```

```

        <name>13</name>
        <value>User Name Preferred Language</value>
        <category>categories.Preferences</category>
</metadata>
<!-- 4 -->
<!--
    This section defines the attributes that will be available in advanced
search
-->
<metadata>
    <name>User Login</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>First Name</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>Middle Name</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>Last Name</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>Display Name</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>Role</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>act_key</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>usr_manager_key</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>Start Date</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>End Date</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>

```

```

        <name>Status</name>
        <value></value>
        <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>Xellerate Type</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>usr_locked</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>Email</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<!--<metadata>
    <name>Phone</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata-->
<metadata>
    <name>usr_locale</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>usr_timezone</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>usr_provisioning_date</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>usr_deprovisioning_date</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<metadata>
    <name>usr_provisioned_date</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>

<metadata>
    <name>usr_deprovisioned_date</name>
    <value></value>
    <category>Advanced Search.Attributes</category>
</metadata>
<!-- 5 -->
<!--
    This section defines attributes that will be used for simple search
-->
<metadata>

```

```

        <name>Display Name</name>
        <value></value>
        <category>Simple Search.Attributes</category>
</metadata>
<metadata>
    <name>User Login</name>
    <value></value>
    <category>Simple Search.Attributes</category>
</metadata>
<metadata>
    <name>First Name</name>
    <value></value>
    <category>Simple Search.Attributes</category>
</metadata>
<metadata>
    <name>Last Name</name>
    <value></value>
    <category>Simple Search.Attributes</category>
</metadata>

<!-- 6 -->
<!--

```

This section defines attributes and their ordering in the advanced search results table. The simple search results table will use the first two defined here.

```

-->
<metadata>
    <name>1</name>
    <value>Display Name</value>
    <category>Search Results.Attributes</category>
</metadata>
<metadata>
    <name>2</name>
    <value>User Login</value>
    <category>Search Results.Attributes</category>
</metadata>
<metadata>
    <name>3</name>
    <value>First Name</value>
    <category>Search Results.Attributes</category>
</metadata>
<metadata>
    <name>4</name>
    <value>Last Name</value>
    <category>Search Results.Attributes</category>
</metadata>
<metadata>
    <name>5</name>
    <value>act_key</value>
    <category>Search Results.Attributes</category>
</metadata>
<metadata>
    <name>6</name>
    <value>usr_manager_key</value>
    <category>Search Results.Attributes</category>
</metadata>
<metadata>
    <name>7</name>
    <value>Status</value>
    <category>Search Results.Attributes</category>

```

```

    </metadata>
    <metadata>
      <name>8</name>
      <value>usr_locked</value>
      <category>Search Results.Attributes</category>
    </metadata>

    <!-- 7 -->
    <!--
      This section defines derived attributes. That is, attributes whose
      value is based on other attribute values.
    -->
    <!--
    <metadata>
      <name>Full Name</name>
      <value></value>
      <category>Derived Attributes</category>
    </metadata>
    -->
    <!--<metadata>
      <name>1</name>
      <value>Last Name</value>
      <category>Derived Attributes.Full Name</category>
    </metadata>
    <metadata>
      <name>2</name>
      <value>, </value>
      <category>Derived Attributes.Full Name</category>
    </metadata>
    <metadata>
      <name>3</name>
      <value>First Name</value>
      <category>Derived Attributes.Full Name</category>
    </metadata>-->

  </metadata-attachment>
</tns:entity-definition>

```

The User.xml file must be compliant to the entity schema file (Entity.xsd).

[Example 8-2](#) shows the code for a sample Entity.xsd file:

Example 8-2 Entity XML Schema Definition

```

<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.oracle.com/schema/oim/entity"
xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://www.oracle.com/schema/oim/entity">
<element name="entity-definition"
type="tns:entity-definition-type">
</element>

<complexType name="entity-definition-type">
  <all>
    <element name="entity-type" minOccurs="1" maxOccurs="1">
      <complexType>
        <simpleContent>
          <extension base="string">
            <attribute name="child-entity"
type="boolean">
          </attribute>

```

```

</extension>
</simpleContent>
</complexType>
</element>
<element name="description" type="string" maxOccurs="1"
minOccurs="0">
</element>
<element name="provider-instance"
type="tns:provider-instance-type" minOccurs="1"
maxOccurs="1">
</element>
<element name="container-capability"
type="tns:container-definition-type" maxOccurs="1"
minOccurs="1">
</element>
<element name="entity-attributes" maxOccurs="1"
minOccurs="1">
<complexType>
<sequence>
<element name="attribute"
type="tns:attribute-definition-type" maxOccurs="unbounded"
minOccurs="1">
</element>
</sequence>
</complexType>
</element>
<element name="target-fields" maxOccurs="1" minOccurs="1">
<complexType>
<sequence>
<element name="field"
type="tns:field-definition-type" maxOccurs="unbounded"
minOccurs="1">
</element>
</sequence>
</complexType>
</element>
<element name="attribute-maps" maxOccurs="1"
minOccurs="0">
<complexType>
<sequence>
<element name="attribute-map"
type="tns:attribute-map-definition-type"
maxOccurs="unbounded" minOccurs="1">
</element>
</sequence>
</complexType>
</element>
<element name="child-entities" maxOccurs="1"
minOccurs="0">
<complexType>
<sequence>
<element name="entity"
type="tns:attribute-definition-type" maxOccurs="unbounded"
minOccurs="1">
</element>
</sequence>
</complexType>
</element>
<element name="metadata-attachment" maxOccurs="1"
minOccurs="0">

```

```
<complexType>
  <sequence>
    <element name="metadata"
      type="tns:metadata-attachment-type" maxOccurs="unbounded"
      minOccurs="0">
    </element>
  </sequence>
</complexType>
</element>
<element name="control-attributes" minOccurs="0" maxOccurs="1">
  <complexType>
    <sequence>
      <element name="attribute" minOccurs="1" maxOccurs="unbounded">
        <complexType>
          <sequence>
            <element name="type" type="string"
              minOccurs="1" maxOccurs="1">
            </element>
            <element name="description"
              type="string" minOccurs="0" maxOccurs="1">
            </element>
            <element name="required"
              type="boolean" minOccurs="1" maxOccurs="1">
            </element>
          </sequence>
          <attribute name="name"
            type="string" use="required">
          </attribute>
        </complexType></element>
      </sequence>
    </complexType></element>
  </all>
</complexType>

<complexType name="provider-instance-type">
  <all>
    <element name="repository-instance" type="string" maxOccurs="1"
      minOccurs="0"></element>
    <element name="provider-type" type="string" maxOccurs="1" minOccurs="1"></element>
    <element name="parameters" minOccurs="0" maxOccurs="1">
      <complexType>
        <sequence>
          <element name="parameter" maxOccurs="unbounded" minOccurs="1">
            <complexType>
              <sequence>
                <element name="value" type="string" maxOccurs="unbounded" minOccurs="1">
                </element>
              </sequence>
            </complexType>
          </element>
          <attribute name="name" type="string">
          </attribute>
        </complexType>
      </element>
    </sequence>
  </complexType>
</element>
</all>
</complexType>

<complexType name="parameter-definition-type">
  <all>
```

```

<element name="type" type="string" maxOccurs="1" minOccurs="1">
</element>
<element name="description" type="string" maxOccurs="1" minOccurs="0">
</element>
<element name="required" type="boolean" maxOccurs="1" minOccurs="1">
</element>
<element name="multi-valued" type="boolean" maxOccurs="1" minOccurs="0">
</element>
</all>
<attribute name="name" type="string"></attribute>
</complexType>

<complexType name="attribute-definition-type">
  <all>
    <element name="type" type="string" maxOccurs="1"
minOccurs="1">
</element>
    <element name="description" type="string" maxOccurs="1"
minOccurs="0">
</element>
    <element name="required" type="boolean" maxOccurs="1"
minOccurs="1">
</element>
    <element name="searchable" type="boolean" maxOccurs="1"
minOccurs="1">
</element>
    <element name="MLS" type="boolean" minOccurs="0" maxOccurs="1"></element>
    <element name="default-value" type="string" maxOccurs="1"
minOccurs="0">
</element>
    <element name="attribute-group" type="string" maxOccurs="1"
minOccurs="1">
</element>
    <element name="metadata-attachment" maxOccurs="1"
minOccurs="0">
<complexType>
<sequence>
<element name="metadata"
type="tns:metadata-attachment-type" maxOccurs="unbounded"
minOccurs="0">
</element>
</sequence>
</complexType>
</element>
  </all>
  <attribute name="name" type="string"></attribute>
</complexType>

<complexType name="field-definition-type">
  <all>
    <element name="type" type="string" maxOccurs="1" minOccurs="1">
</element>
    <element name="description" type="string" maxOccurs="1" minOccurs="0">
</element>
    <element name="required" type="boolean" maxOccurs="1" minOccurs="1">
</element>
  </all>
  <attribute name="name" type="string"></attribute>
</complexType>

```

```

<complexType name="attribute-map-definition-type">
  <all>
    <element name="entity-attribute" type="string" maxOccurs="1" minOccurs="1">
    </element>
    <element name="target-field" type="string" maxOccurs="1" minOccurs="1">
    </element>
  </all>
</complexType>

<element name="repository-definition"
type="tns:repository-definition-type">
</element>

<complexType name="repository-definition-type">
  <all>
    <element name="name" type="string" maxOccurs="1" minOccurs="1">
    </element>
    <element name="class" type="string" maxOccurs="1" minOccurs="1">
    </element>
    <element name="parameters" maxOccurs="1" minOccurs="0">
    <complexType>
    <sequence>
    <element name="parameter-def" type="tns:parameter-definition-type"
maxOccurs="unbounded" minOccurs="1">
    </element>
    </sequence>
    </complexType>
    </element>
    <element name="description" type="string" maxOccurs="1" minOccurs="0"></element>
  </all>
</complexType>

<element name="provider-definition"
type="tns:provider-definition-type">
</element>

<complexType name="provider-definition-type">
  <all>
    <element name="name" type="string" maxOccurs="1" minOccurs="1"></element>
    <element name="type" maxOccurs="1" minOccurs="1">
    <complexType>
    <choice>
    <element name="DataProvider" type="string"></element>
    <element name="RelationProvider" type="string">
    </element>
    </choice>
    </complexType>
    </element>
    <element name="class" type="string" maxOccurs="1" minOccurs="1"></element>
    <element name="description" type="string" maxOccurs="1" minOccurs="0"></element>
    <element name="parameters" maxOccurs="1" minOccurs="0">
    <complexType>
      <sequence>
    <element name="parameter-def" type="tns:parameter-definition-type"
maxOccurs="unbounded" minOccurs="1">
    </element>
    </sequence>
    </complexType>
    </element>
  </all>

```

```

</complexType>

<element name="repository-instance">
<complexType>
  <all>
<element name="name" type="string"></element>
<element name="type" type="string"></element>
<element name="parameters" maxOccurs="1" minOccurs="0">
<complexType>
<sequence>
<element name="parameter" maxOccurs="unbounded" minOccurs="1">
<complexType>
<sequence>
<element name="value" type="string" maxOccurs="1" minOccurs="1">
</element>
</sequence>
<attribute name="name" type="string">
</attribute>
</complexType>
</element>
</sequence>
</complexType>
</element>
</all>
</complexType>
</element>

<complexType name="container-definition-type">
  <sequence>
<element name="enabled" type="boolean" maxOccurs="1" minOccurs="1"></element>
<element name="contained-entity" type="string" maxOccurs="unbounded"
minOccurs="0">
</element>
</sequence>
</complexType>

<complexType name="relation-definition-type">
  <all>
<element name="relation-type" type="string" maxOccurs="1" minOccurs="1"></element>
<element name="description" type="string" maxOccurs="1" minOccurs="0"></element>
<element name="provider-instance" type="tns:provider-instance-type" maxOccurs="1"
minOccurs="1">
</element>
<element name="entity1" type="tns:relation-entity-type" maxOccurs="1"
minOccurs="1">
</element>
<element name="entity2" type="tns:relation-entity-type" maxOccurs="1"
minOccurs="1"></element>
<element name="relation-attributes" maxOccurs="1" minOccurs="1">
<complexType>
<sequence>
<element name="attribute" type="tns:attribute-definition-type"
maxOccurs="unbounded" minOccurs="0">
</element>
</sequence>
</complexType>
</element>
<element name="target-fields" maxOccurs="1" minOccurs="1">
<complexType>
<sequence>

```

```
<element name="field" type="tns:field-definition-type" maxOccurs="unbounded"
minOccurs="0">
</element>
</sequence>
</complexType>
</element>
<element name="attribute-maps" maxOccurs="1" minOccurs="0">
<complexType>
<sequence>
<element name="attribute-map" type="tns:attribute-map-definition-type"
maxOccurs="unbounded" minOccurs="1">
</element>
</sequence>
</complexType>
</element>
</all>
</complexType>

<element name="relation-definition"
type="tns:relation-definition-type">
</element>

<complexType name="relation-entity-type">
<all>
<element name="entity-type" type="string"></element>
<element name="attribute" type="string"></element>
<element name="attribute-in-entity" type="string"></element>
<element name="attribute-group" type="string" maxOccurs="1"
minOccurs="1"></element>
</all>
</complexType>

<element name="datatype-definition"
type="tns:datatype-definition-type">
</element>

<complexType name="datatype-definition-type">
<all>
<element name="name" type="string" maxOccurs="1" minOccurs="1"></element>
<element name="class" type="string" maxOccurs="1" minOccurs="1"></element>
<element name="base-type" type="string" maxOccurs="1" minOccurs="1"></element>
</all>
</complexType>

<complexType name="metadata-attachment-type">
<all>
<element name="name" type="string"></element>
<element name="value" type="string"></element>
<element name="category" type="string"></element>
</all>
</complexType>

<element name="derived-datatype-definition"
type="tns:derived-datatype-definition-type">
</element>

<complexType name="derived-datatype-definition-type">
<all>
<element name="name" type="string" maxOccurs="1" minOccurs="1">
```

```

</element>
<element name="class" type="string" maxOccurs="1" minOccurs="1">
</element>
<element name="parameters" minOccurs="0" maxOccurs="1">
<complexType>
<sequence>
<element name="parameter" maxOccurs="unbounded" minOccurs="1">
<complexType>
<sequence>
<element name="value" type="string" maxOccurs="1" minOccurs="1">
</element>
</sequence>
</complexType>
</element>
</sequence>
</complexType>
</element>
</all>
</complexType>
</schema>

```

The entity XML files are stored in MDS. When a new attribute is added, the database schema is updated along with the entity XML in MDS. The configuration service APIs can be used to fetch the attribute information and can be leveraged while building custom UI.

8.10 Creating Cascaded LOVs

To create cascaded LOVs on the My Information page and Self-Registration Page:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox, for example `SUJ`. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
3. In the left pane, under Configuration, click **Form Designer** and then select **User**.
4. Create the following UDFs of Lookup Type:
 - parent - ParentChoice
 - dependent - DepChoice
5. Make the UDF DepChoice dependent on the UDF ParentChoice, and map the values.
6. Export the sandbox.

The sandbox is stored as `sandbox_SUJ.zip`.
7. Unzip the `sandbox_SUJ.zip` file, and perform the following steps:
 - a. Search for the following text in `\persdef\sessiondef\oracle\iam\ui\runtime\form\model\user\view\mdssys\cust\site\site\userVO.xml.xml` file under `<ViewAttribute Name="DepChoice__c">` tag:

```

<Property Name="CascadingParentChoiceList"
Value="ParentChoice__c"/>

```

```
<Property Name="CascadingRelationshipId" Value="100000000002523"/>
```

- b. Copy the text in Step 7 a to
 \persdef\oracle\iam\ui\common\model\user\view\mdssys\cust\site\site\userVO.xml file under <ViewAttribute Name="DepChoice__c" tag.
- c. Search for the following text
 \persdef\sessiondef\oracle\iam\ui\runtime\form\model\user\view\mdssys\cust\site\site\userVO.xml.xml file:

```
</mds:insert>
  <mds:insert parent="UserVO" position="last">
    <ViewAccessor Name="LOVVA_For_DepChoice__c"
    ViewObjectName="oracle.adf.businesseditor.model.views.CascadingLookups "
    xmlns="http://xmlns.oracle.com/bc4j">
      <ParameterMap>
        <PIMap Variable="Bind_RelationshipId">

<TransientExpression><![CDATA[viewObject.findAttributeDef("DepChoice__c").get
Property("CascadingRelationshipId")]]></TransientExpression>

        </PIMap>
        <PIMap Variable="Bind_ParentLookupCode">

<TransientExpression><![CDATA[ParentChoice__c]]></TransientExpression>
        </PIMap>
      </ParameterMap>
    </ViewAccessor>
  </mds:insert>
```

- d. Copy the text in Step 7.c to
 \tmp\persdef\oracle\iam\ui\common\model\user\view\mdssys\cust\site\site\userVO.xml.xml file by replacing the following text:

```
</mds:insert>
  <mds:insert parent="UserVO" position="last">
    <ViewAccessor Name="LOVVA_For_DepChoice__c"
    ViewObjectName="oracle.adf.businesseditor.model.views.Lookups"
    xmlns="http://xmlns.oracle.com/bc4j">
      <ParameterMap>
        <PIMap Variable="Bind_LookupType">

<TransientExpression><![CDATA['Lookup.Conditions.Severity']]></TransientExp
ression>

        </PIMap>
      </ParameterMap>
    </ViewAccessor>
  </mds:insert>
```

8. Recreate the zip file with same name as in Step 6.
9. Delete the sandbox SUJ from Oracle Identity System Administration.
10. Import the modified sandbox_SUJ.zip created in Step 8.
11. Log in to Oracle Identity Self Service.
12. Activate the sandbox, SUJ.

13. Customize the My Information page to add the two UDFs created in Step 4.
14. Click the sandbox and perform the following steps:
 - a. Select `/oracle/iam/ui/myinformation/pages/my-information.jsff` file and then click **Export Sandbox**.
 - b. Open the preceding file and copy the id of the UDF, `ParentChoice`.
 ex: `id="dtrt_dc_3742570725"`
15. Click **Customize** to customize the My Information page while the sandbox is active in Oracle Identity Self Service.
16. Select **DepChoice** and click Edit Property to add the `partialTrigger` value. value of the `ParentChoice` UDF copied in Step 14.b in `partialTrigger` value of `DepChoice`.
17. Enter the value of `ParentChoice` UDF copied in Step 14.b in `partialTrigger` value of `DepChoice`.
18. Select **ParentChoice** and set the auto **submit** property to **true**.
19. Publish the sandbox.

Note: For any LOV, the user details page displays the lookup code as the output text value. To display the LOV lookup value on the user details page, create a searchable picklist (ADF name input list of value), and then make it read-only.

Specifying Cascaded LOVs Without NULL Value

When you set the value of the required property to true in the attributes on the create user or modify user form, you can still submit a request without selecting a value. To make the user select a value for the required attribute, you must modify the request dataset to mark the attribute as mandatory. To do so:

1. When the administrative server and at least one Oracle Identity Manager managed server is running, login to Oracle Enterprise Manager Fusion Middleware Control by using the URL in the following format:
2. Navigate to **Identity and Access, oim**. Right-click and navigate to **System MBean Browser**.
3. Under Application Defined MBeans, navigate to **oracle.mds.lcm, Server:oim_server1, Application:OIMAppMetadata**.
4. To export the request dataset:
 - a. Click the **Operations** tab, and then click **exportMetadata**.
 - b. In the `toLocation` field, enter `/tmp` or the name of another directory.
 - c. Select `createSubDir` as **false**.
 - d. Specify the doc location as the following:

```
/metadata/iam-features-requestactions/model-data/CreateUserDataSet.xml.
```

```
/metadata/iam-features-requestactions/model-data//ModifyUserDataset.xml
```

Note: Multiple documents can be set in the doc location while invoking operations `exportMetaData` or `importMetaData`.

- e. Also select **false** for `excludeAllCust`, `excludeBaseDocs`, and `excludeExtendedMetadata`. Then, click **Invoke**.

This exports the file specified in the docs field to the directory specified in the `toLocation` field.

- 5. Edit the `CreateUserDataSet.xml` file, and change the value of the 'required' property to `true` for the Location and BusinessUnit AttributeReferences.
- 6. To import the request dataset:
 - a. Click **importMetaData**.
 - b. In the `fromLocation` field, enter `/tmp` or the name of the directory in which you have the configuration files.
 - c. Select `createSubDir` as **false**.
 - d. Specify the doc location as the following:

```
/metadata/iam-features-requestactions/model-data/CreateUserDataSet.xml
/metadata/iam-features-requestactions/model-data//ModifyUserDataset.xml
```
 - e. Also select **false** for `excludeAllCust`, `excludeBaseDocs`, and `excludeExtendedMetadata`. Then, click **Invoke**.

This imports the file specified in the docs field to MDS in the `toLocation` field.
- 7. Restart Oracle Identity Manager.

Part V

Application Management

This part describes application management in Oracle Identity Manager.

It contains the following chapters:

- [Chapter 9, "Managing Application Instances"](#)
- [Chapter 10, "Managing Disconnected Resources"](#)
- [Chapter 11, "Managing Lookups"](#)
- [Chapter 12, "Managing Connector Lifecycle"](#)
- [Chapter 13, "Managing Reconciliation"](#)

Managing Application Instances

Application instance is a new abstraction used in 11g Release 2 (11.1.2.1.0). It is a combination of IT resource instance (target connectivity and connector configuration) and resource object (provisioning mechanism).

In pre-R2 releases, requests creation was based on name of resources and it was Administrator-centric, which needed good knowledge of technology. However in 11g Release 2 (11.1.2.1.0), accounts and entitlements of users are associated with application instances, and not with the IT resource instance or resource object. This makes it easier for an end user to operate.

Application instance will be published to organizations and can be requested by users of those organizations. Suppose Microsoft Active Directory (AD) is to be provisioned to users across different organizations or departments across the world. You can define application instances consisting of the following:

- AD as the resource object
- Each AD server instance with the connectivity information, such as URL and password, as IT resources

This is because the resource object is same for all users, but the connectivity information, such as port number, can be different for users who are part of different organizations. Therefore, the AD resource object can be provisioned as an application instance without the user being aware of the connectivity information.

Application Instance is the provisionable entity. In order to get an account in a specific target, end users will need to request for the application instance. Instead of requesting for a resource and configuring IT resource instance separately, end user can request for an application instance. The request is subject to approval by an approver. When the request is approved, the resource is provisioned to the user, and an account is created in the target system.

Note: If the request is coming from an administrator, then it may not require approval, where as a request coming from an end user needs approval by approver.

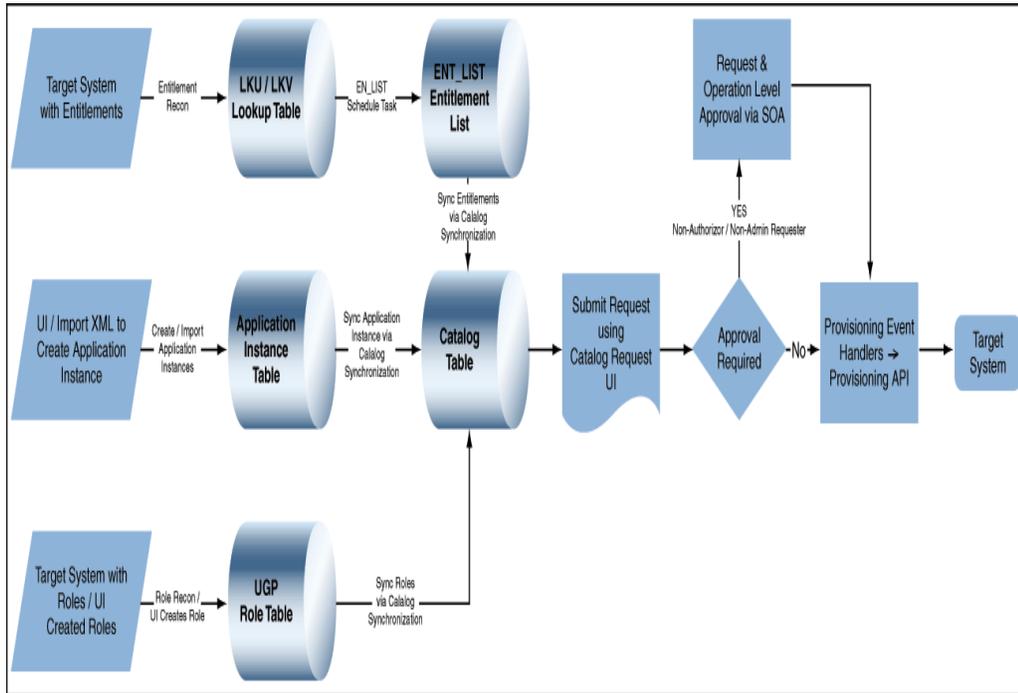
This chapter describes application instances in the following topics:

- [Section 9.1, "Application Instance Architecture and Concepts"](#)
- [Section 9.2, "Managing Application Instances"](#)
- [Section 9.4, "Developing Entitlements"](#)

9.1 Application Instance Architecture and Concepts

An Application Instance is the provisionable entity which will be published to the catalog. 11g Release 2 (11.1.2.1.0) provides the functionality to create catalog-based request to grant application instance, entitlements, and roles. The architecture includes enhancements required in provisioning module to support request for application instances and entitlements. [Figure 9-1](#) illustrates the Application Instance architecture.

Figure 9-1 Application Instance Architecture



The application instance concepts are described in the following sections:

- [Section 9.1.1, "Multiple Accounts Per Application Instance"](#)
- [Section 9.1.2, "Entitlements"](#)
- [Section 9.1.3, "Disconnected Application Instances"](#)
- [Section 9.1.4, "Application Instance Security"](#)

9.1.1 Multiple Accounts Per Application Instance

Users in an enterprise can have multiple accounts in a single application instance. This is required in a scenario in which an HR administrator performs various tasks for other employees in the organization by using an administrative account. The same HR administrator logs in by using a separate user account when performing certain tasks for self. In this example, the same user requires two different accounts for logging in to the system and performs different types of operations.

In addition, supporting multiple accounts for users is required to prevent potential security threats. Suppose a user uses the same account for logging in to the environment, and performs administrative tasks, regular business tasks for self and others, and tasks related to IT infrastructure. If there is an intrusion in the system and the account is hacked, the hacker can access infrastructure data and other confidential information. If the user has multiple accounts for each type of task and the regular

account is hacked, the confidential information related to IT infrastructure and other sensitive resources are secured from the hacker.

Oracle Identity Manager supports multiple accounts in 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 subsequent accounts created on the same application instance would be tagged as Other. When the user requests entitlements, the entitlements are appended to the primary account.

When the user gets provisioned to an application instance, the Oracle Identity Manager checks if it is the first account getting provisioned for the user in that application instance. If it is the first account, then 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. If the account marked as primary is not the actual primary account, then you can manually change the primary tag for the account and mark another account as primary.

9.1.2 Entitlements

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 a role, responsibility, or group membership. For example, if user Richard is granted the Inventory Analyst role on a target system, then Richard has a child process form that holds Inventory Analyst role data.

In Oracle Identity Manager, there is one process form for each account (resource) provisioned to an OIM User. Entitlement data is stored in child process form. In the example described earlier, the process form for Richard's account on the target system has a child process form that holds Inventory Manager role data.

Note: To reconcile entitlements created in the target system into Oracle Identity Manager, you must first run the scheduled job for lookup field synchronization, and then run the Entitlement List scheduled job.

Attributes that constitute entitlement data stored on a child process form may vary from one target system to another. In addition, different types of entitlements, such as roles and responsibilities, may have different attributes.

Entitlements that are required to be associated to the administrative accounts are provisioned by requesting a modify resource on the administrative account. From the user's resource (account) profile, the administrator can request for modifying the administrative account and add the administrative entitlements to this account's child table, which then provisions this entitlement to the respective administrative account. Entitlements can also be requested through Entitlement request.

All types of entitlements are available for request in the request catalog. If the request for an administrative entitlement is approved, then it is associated to the primary account and not the administrative account.

You can edit the entitlements by using the Application Instances section of the Oracle Identity System Administration.

See "[Developing Entitlements](#)" on page 9-18 for detailed information about entitlements.

9.1.3 Disconnected Application Instances

You might deploy self service, delegated administration, request management, and role-based provisioning features in Oracle Identity Manager, and might not deploy provisioning and reconciliation connectors to automate provisioning. After completion of delegated administration operation, request-approval, or role-based provisioning, a manual provisioning task is assigned to an administrator. The administrator then manually performs the provisioning in the target application instance. An example of this is provisioning of an access card, which is physical. Because Oracle Identity Manager cannot provision a physical access card, the application instance of the disconnected resource is to be provisioned.

Oracle Identity Manager supports provisioning of disconnected resources by using the SOA worklist for manual provisioning of disconnected resources. After the role-based provisioning decision or SOA request approval is complete and the corresponding application instance is determined to be a disconnected application instance, a new SOA workflow is started. This new SOA workflow is assigned to the manual provisioning administrator.

To achieve provisioning of disconnected resource, you can create application instances of the disconnected type. The manual provisioning administrator can use the Pending Approvals section of the Oracle Identity Self Service to update all fields in the request. After the manual provisioning administrator submits the manual provisioning worklist item, the provisioning infrastructure marks the underlying provisioning task to be completed based on the response of the manual provisioning administrator. If the administrator specifies that task is manually completed, then the status is changed to provisioned.

9.1.4 Application Instance Security

The Application Instance is also the entity with which security primitives are associated via the organization publishing mechanism. In multi-tenant environments, resource definitions can be shared by multiple organizations, but only those organizations that have the application instance published to them will be actually able to provision to the targets.

9.2 Managing Application Instances

You manage application instances by using Oracle Identity System Administration. This includes:

- [Creating Application Instances](#)
- [Searching Application Instances](#)
- [Modifying Application Instances](#)
- [Deleting Application Instances](#)
- [Creating and Modifying Forms](#)

See Also: ""Converting a Disconnected Application Instance to Connected" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for information about converting a disconnected application instance to a connected application instance

9.2.1 Creating Application Instances

To create an application instance:

1. Login to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **Application Instances**. The Application Instances page is displayed.
3. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Application Instance page is displayed.
4. Enter the values of the attributes, as listed in [Table 9-1](#):

Table 9-1 Fields in the Create Application Instance Page

Attribute	Description
Name	The name of the application instance. This is a required field. Note: If you enter non-ASCII characters in the Name field, then an error message is displayed when you try to save the application instance. It is recommended that you enter only ASCII or alphanumeric characters in the Name field.
Display Name	The display name of the application instance. This is a required field.
Description	A description of the application instance.
Disconnected	Select if you want to specify the application instance as disconnected. Selecting this option creates a new approval process that is assigned to the manual provisioning administrator. See " Disconnected Application Instances " on page 9-4 for more information. Note: Disconnected application instance can only be created when a sandbox is active. See "Managing Sandboxes" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for more information about sandbox.
Resource Object	The resource object name. You can click the search icon next to this field to search and select a resource object.
IT Resource Instance	The IT resource instance name. You can click the search icon next to this field to search and select an IT resource instance.
Form	Select the form or dataset name. The forms associated with the selected resource object are populated in the Forms list. Here, you can create a new form, or edit an existing form. See " Creating and Modifying Forms " on page 9-12 for more information.
Parent AppInstance	The application instance name that you want to specify as a parent to the new application instance. The new application instance inherits all the properties of the parent application instance.

5. Click **Save**. The application instance is created, and the details of the application instance is displayed in a page.

9.2.2 Searching Application Instances

To search for application instances:

1. In the Oracle Identity System Administration, under Configuration, click **Application Instances**. The Application Instances 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 application instance 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 application instances with a particular resource object, specify the resource object name in the Resource Object 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

The search operator can be combined with wildcard characters to specify a search condition. The asterisk (*) character is used as a wildcard character.
- 5. To add a searchable application instance attribute to the Application Instances page, click **Add Fields**, and select the attribute from the list of attributes.
For example, if you want to search all application instances under a parent application instance, then you can add the Parent AppInstance attribute as a searchable field and specify a search condition.
- 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 result is displayed in a tabular format, as shown in [Figure 9-2](#):

Figure 9–2 Application Instance Search

R...	Display Name	Description	Resource Object	IT Resource Instance
1	Vision Purchasing	Vision Purchasing	eBusiness Suite User	EBS-APPS 12
2	Vision Employees Domain	Vision Employees Domain	AD User	ADITResource

Tip: You can use the Query By Example feature to refine your search based on specific values. For more information, see "Query By Example" in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

9.2.3 Modifying Application Instances

You can open an application instance and modify the attributes, assign and revoke organizations to which the application instance is available, and edit the entitlements associated with the application instance. These tasks are described in the following sections:

- [Modifying Application Instance Attributes](#)
- [Managing Organizations Associated With Application Instances](#)
- [Managing Entitlements Associated With Application Instances](#)

9.2.3.1 Modifying Application Instance Attributes

To modify the attributes of an application instance:

1. In the Application Instances page, search and select the application instance that you want to open.
2. From the Actions menu, click Open. Alternatively, click Open on the toolbar. You can also click the Display Name of the application instance.

The Application Instance details page is displayed.

3. Ensure that the Attributes tab is displayed. The fields that you are not allowed to modify are grayed out.
4. Edit the values in the fields, such as Display Name, Description, Form, and Parent AppInstance.
5. Click **Apply**. The attribute modifications are saved.

Note: After modifying an application instance, if the modified details are reflected in the Catalog page of Oracle Identity Self Service, but are not reflected in the User Details page, then close and reopen the User Details page. The updated application instance details will be reflected now.

9.2.3.2 Managing Organizations Associated With Application Instances

You must make an application instance available for requesting and subsequent provisioning to users by publishing the application instance to an organization. The users in that organization or the users who has User Viewer role in that organization or the users who has Application Instance Viewer role + User Viewer Role in that organization can request for application instance. For information about authorization in Oracle Identity Manager, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

In the Organizations tab of the Application Instance details page, you can publish the application instance to organizations, and revoke organizations from the application instance.

In addition, you can publish the application instance to an organization and its suborganizations so that users of the suborganizations can also request for the application instance. You can also publish an application instance to organizations with entitlements so that users of the organization can request for the application instance with the entitlements associated with it.

Note: An administrator user can publish an entity to any organization that the administrator can view. For example, an Entitlement Administrator can publish entitlements with administrative permissions to any organization on which the Entitlement Administrator has view permission.

This section describes the following tasks:

- [Publishing an Application Instance to Organizations](#)
- [Revoking Organizations From an Application Instance](#)

9.2.3.2.1 Publishing an Application Instance to Organizations

To publish an application instance to organizations:

1. In the Application Instance details page, click the **Organizations** tab. A list of organizations to which the open application instance is published is displayed.

For each organization, the **include sub-orgs** option is displayed in the Hierarchy Aware column. Select this option to make the open application instance available to the organization and its suborganizations. Deselect this option to make the open application instance available to the organization only.
2. From the Actions menu, click **Assign**. Alternatively, click **Assign** on the toolbar. The Select Organizations dialog box is displayed.
3. Search for the organizations to which you want to publish to the open application instance.

Note: If you are using Oracle Identity System Administration in French on Google Chrome web browser, the right arrow may be missing or truncated in the search panel of the Select Organizations dialog box. To fix this issue, verify the display language setting in Chrome and change it to French if necessary.

4. Click **Add Selected**. The selected organizations are added to the Selected Organizations table.

If you want to select all organizations, then click **Add All**.

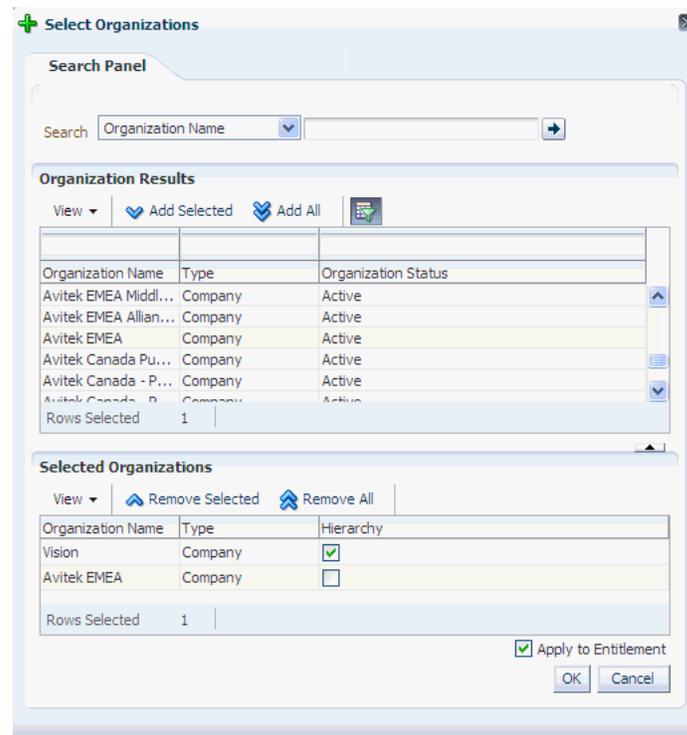
5. For each organization added to the Selected Organizations table, a checkbox is displayed in the Hierarchy column. Select the **Hierarchy** option to publish the open application instance to the suborganizations of the selected organization.

To publish the open application instance to the selected organizations only, leave the **Hierarchy** option deselected.

6. Select the **Apply to Entitlement** option to publish the open application instance to the selected organizations with the entitlements associated with the application instance. Otherwise, leave this option deselected.

Figure 9–3 shows the Select Organizations dialog box with the Hierarchy and Apply to Entitlement options:

Figure 9–3 The Select Organizations Dialog Box



7. Click **OK**. The application instance is published to the selected organizations.

The **include sub-orgs** option is displayed for the organizations for which you selected the **Hierarchy** option in the Select Organizations dialog box.

9.2.3.2.2 Revoking Organizations From an Application Instance

To revoke an organization from an application instance:

1. In the Organizations tab, select an organization that you want to revoke from the open application instance.
2. From the Action menu, select **Revoke**. Alternatively, click **Revoke** on the toolbar. A confirmation box is displayed with the selected organization.
3. Click **Yes** to confirm. The organization is revoked from the application instance.

9.2.3.3 Managing Entitlements Associated With Application Instances

To modify entitlements associated with an application instance:

1. In the Application Instance details page, click the **Entitlements** tab. A list of entitlements associated with the open application instance is displayed.
2. Select the entitlement that you want to modify.
3. From the Actions menu, select **Edit**. Alternatively, click **Edit** on the toolbar. The details of the selected entitlement is displayed in a page.
4. Change the attributes of the attributes, and click **Save**. The entitlement modifications are saved.

9.2.4 Deleting Application Instances

An application instance can be deleted in any one of the following ways:

- Deleting the application instance from the Application Instances section of the Oracle Identity System Administration.
- Deleting the IT resource, which is a constituent of the application instance.

When you delete an application instance by using any one these methods, the application instance is not hard-deleted from Oracle Identity Manager. The application instance is soft-deleted. This is because accounts provisioned as a result of the application instance might exist in the target system. Therefore, after deleting an application instance, you must run a scheduled job to achieve the following:

- Unpublish the application instance from the entity publication
- Unpublish the associated entitlements from the entity publication
- Revoke, or hard-delete, or mark as deleted all the accounts for the application instance

To delete an application instance:

1. In Oracle Identity System Administration, under Configuration, click Application Instances. The Application Instances page is displayed with a list of application instances that are published to your organization.
2. Search and select the application instance that you want to delete.
3. From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar. A message box is displayed asking for confirmation.
4. Click **Delete** to confirm. The application instance is soft-deleted in Oracle Identity Manager.

You can also delete an application instance by deleting the IT resource of the application instance. For information about deleting IT resources, see "Managing IT Resources" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

5. Run the **Application Instance Post Delete Processing Job** scheduled job. This scheduled job can be run in any one of the following modes:
- **Revoke:** This mode is used when the application instance is deleted, but the provisioned accounts in the target system still exist. Using the Revoke mode deletes the accounts from the target system.

Note: Do not use the Revoke mode with disconnected application instances.

- **Delete:** This mode is used when the target system no longer exists, and there are no traces of the accounts in Oracle Identity Manager. Using the Delete mode hard-deletes the accounts from all provisioning tasks and targets, and subsequently from Oracle Identity Manager. If this mode is used when the accounts are assigned in Oracle Identity Manager, then the accounts are listed as deprovisioned under the users they are assigned to.
- **Decommission:** This mode is used when the target system no longer exists and the provisioned accounts cannot be revoked from the target system. Using the Decommission mode changes the account status to Revoke without keeping the accounts in Oracle Identity Manager in provisioned state.

For information about scheduled jobs, see "[Managing the Scheduler](#)" on page 15-1.

Note: The Application Instance Post Delete Processing Job scheduled job can be run after deleting each application instance.

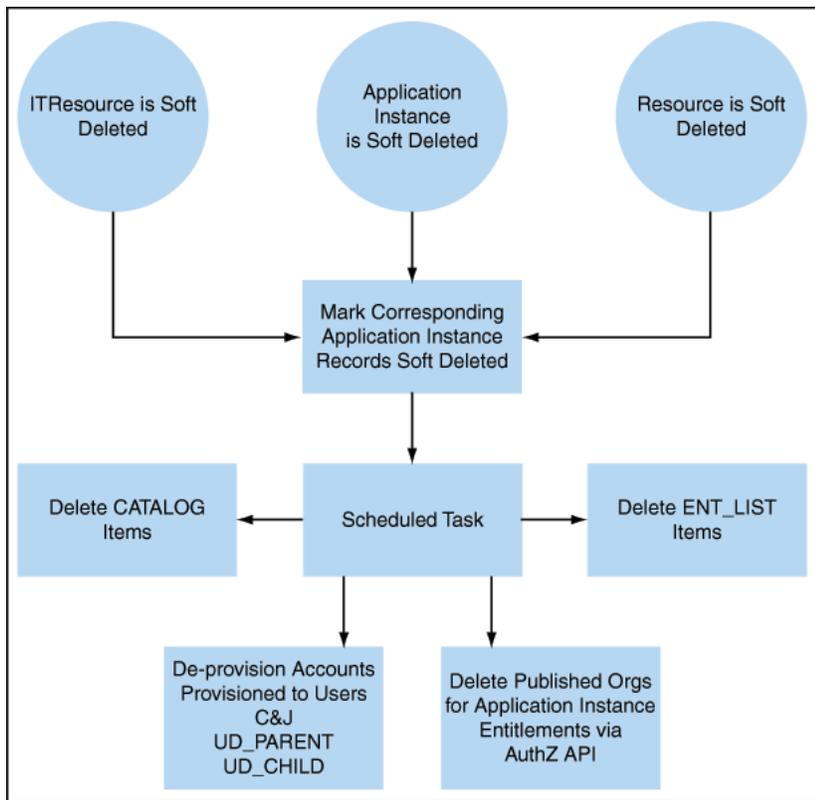
6. Run the **Catalog Synchronization Job** scheduled job. This scheduled job identifies the soft-deleted application instances, and removes them from the catalog.

Note:

- The Catalog Synchronization Job scheduled job run is independent of the Application Instance Post Delete Processing Job run. This means that the Catalog Synchronization Job scheduled job removes the soft-deleted application instances from the catalog even if Application Instance Post Delete Processing Job is not run after soft-deleting the application instances.
 - Catalog Synchronization Job should be run preferably in Incremental mode so that changes, such as add, update, and delete, in base entity application instance and entitlements are synced to catalog DB.
-

[Figure 9-4](#) shows the flow and changes that will be made upon Application Instance soft-deletion.

Figure 9–4 Application Instance Soft Deletion Flow



9.2.5 Creating and Modifying Forms

In the Application Instances section of Oracle Identity System Administration, you can create and modify forms associated with the resource objects, and subsequently with the application instances.

See Also:

- See "Managing Sandboxes" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for information about sandbox
- See [Chapter 7, "Managing Forms"](#) for information about creating forms
- See [Chapter 8, "Configuring Custom Attributes"](#) for information about configuring custom attributes

This section describes the following topics:

- [Creating Forms Associated With Application Instances](#)
- [Modifying Forms Associated With Application Instances](#)
- [Localizing Application Instance Form](#)

9.2.5.1 Creating Forms Associated With Application Instances

To create a form associated with an application instance:

Note: You cannot create forms directly. Before creating forms, you must create a sandbox and activate it. See "Managing Sandboxes" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for information about creating and activating a sandbox.

1. Open the Create Application Instance page or the Attributes tab of the Application Instance details page.
2. Adjacent to the Forms field, click **Create**. The Create Form page is displayed.
3. In the Name field, verify that the name of the resource object with which the form is associated is displayed. To change the resource object name, click the search icon next to the Name field, and search and select a name from the Search and Select: Name dialog box.
4. In the Form Name field, enter a form name.
5. In the Available form fields section, a list of form field names along with description and Display Name are displayed. These fields are available for the form you are creating. For each available form field, select one or more of the following options:
 - **Bulk Update:** Selecting this option makes the form field available for updating the entities in bulk.
 - **Encrypted:** Selecting this option displays the value of the form field in encrypted format.
6. Click **Create**. A message is displayed stating that the form is created.
7. In the Create Application Instance page or the Attributes tab of the Application Instance details page, click **Refresh** adjacent to the Form field. The newly created form is available for selection in the Form list.

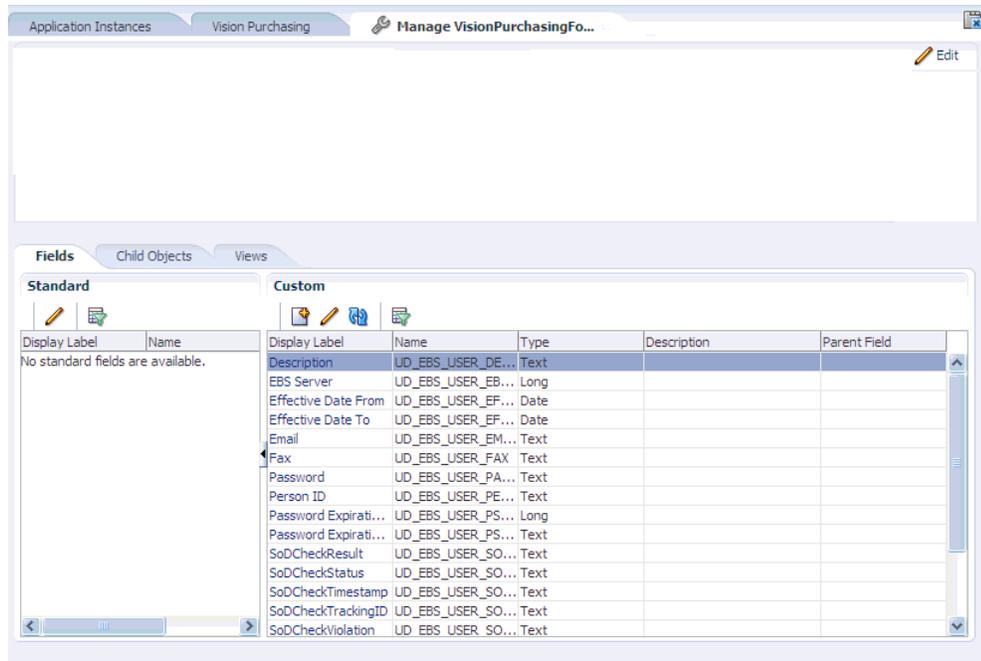
9.2.5.2 Modifying Forms Associated With Application Instances

Note: You cannot modify forms directly. Before creating forms, you must create a sandbox and activate it. See "Managing Sandboxes" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for information about modifying and activating a sandbox.

To modify a form associated with an application instance:

1. Open the Create Application Instance page or the Attributes tab of the Application Instance details page.
2. From the Form list, select the form you want to modify.
3. Click **Edit** to right of the Form field. The Manage Form page is displayed, as shown in [Figure 9-5](#):

Figure 9–5 The Manage Form Page



For detailed information about modifying forms, see "Developing Process Forms" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

For information about creating and editing custom fields, see "[Configuring Custom Attributes](#)" on page 8-1.

9.2.5.3 Localizing Application Instance Form

To localize the application instance form:

1. Create an application instance of connector with a form attached to it.
2. Login to Oracle Enterprise Manager.
3. Go to **Application Deployments, oracle.iam.console.identity.sysadmin.ear, MDS Configuration**.
4. Click **Export** and save the archive to the host.
5. Unzip the archive, and open the `SAVE_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf` file in a text editor.

Note: This file may not exist in MDS. If it does not exist, then create a new one, but the path must be the same.

6. Edit the BizEditorBundle.xlf file in the following way:
 - a. Search and replace the following:

```
<file source-language="en"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

With the following for Japanese language:

```
<file source-language="en" target-language="ja"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

- b. Search for the application instance code. This procedure shows a sample edit for JDE application instance. The original code is:

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_JDE_LANGUAGE__c_description']}">
<source>Language</source>
</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.JDEArj.entity.JDEArjEO.UD_J
DE_LANGUAGE__c_LABEL">
<source>Language</source>
</target>
</trans-unit>
```

- c. Open the resource file from the connector package, for example `JDEdwards_ja.properties`, and get the value of the attribute from the file, for example, `global.udf.UD_JDE_LANGUAGE=\u8A00\u8A9E`.
- d. Replace the original code shown in step 6b with the following:

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_JDE_LANGUAGE__c_description']}">
<source>Language</source>
<target>\u8A00\u8A9E</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.JDEArj.entity.JDEArjEO.UD_J
DE_LANGUAGE__c_LABEL">
<source>Language</source>
<target>\u8A00\u8A9E</target>
</trans-unit>
```

- e. Repeat steps 6a through 6d for all attributes of the process form.
- f. Save the file as `BizEditorBundle_ja.xlf`.
7. Repackage the ZIP file and import it to MDS.

See Also: "Deploying and Undeploying Customizations" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*, for more information about exporting and importing metadata files

8. Logout or Oracle Identity Manager and login again.

9.3 Configuring Application Instances

You can configure application instances by using Oracle Identity System Administration. This includes:

- [Section 9.3.1, "Configuring Provisioning for Connected Application Instances"](#)
- [Section 9.3.2, "Configuring a Resource Object"](#)

- [Section 9.3.3, "Configuring IT Resource"](#)
- [Section 9.3.4, "Configuring Password Policies for Application Instances"](#)

9.3.1 Configuring Provisioning for Connected Application Instances

To configure the provisioning for connected (AD User) application instances:

1. Go to Oracle Identity System Administration.
2. Under Configuration, click **Application Instances**.
3. Select the connected application instance, for example ActiveDirectoryApplicationInstance (AD User).
4. Enter the required fields and click **Apply**.

Figure 9–6 Connected Application Instance



9.3.2 Configuring a Resource Object

For information about configuring a resource object, see "Resource Objects Form" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

9.3.3 Configuring IT Resource

For information about configuring an IT resource, see "Creating IT Resources" and "Managing IT Resources" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

An application instance can be configured for only one IT resource. If the process form requires value of two or more IT resources for provisioning an account, then it cannot be configured directly from the UI. To configure two or more IT resources for provisioning an account:

1. Identify the main IT resource for the account and configure the application instance with that.

2. Use entity adapter to populate the value for other required IT resources. For example, the Microsoft Exchange connector 9.1.1.7 requires an IT resource value of AD IT resource and Exchange IT resource to provision Exchange account. Here are the steps to make it work in R2
 - a. Create an application instance with Exchange IT resource, and choose AD application instance as parent application because it is a dependent resource for Exchange.
 - b. Configure an entity adapter to pass the value of the AD IT resource to the process form. To do so:
 - i.) Keep a track of the dependent IT resource name, such as Exchange, and independent IT resource name, such as AD. This can be in the code, or externalized in a lookup and then initialized in the code.
 - ii.) Create an entity adapter that takes long as a parameter. This is the parent IT resource key that will be populated.
 - iii.) In the adapter code, find the parent IT resource name and do a reverse lookup on the child IT resource name by using the map mentioned in step i.
 - iv.) From the child IT resource name, get the child IT resource key as a long and return it. The entity adapter return value gets set on the child IT resource field on the process form.

9.3.4 Configuring Password Policies for Application Instances

Perform the following steps to configure the password policy for application instances:

1. Go to Oracle Identity System Administration.
2. Under Policies, click **Password Policy**.
3. Set the required field to set a new rule for the password.

shows the Policy Rules fields and Custom Policy fields that you can configure.

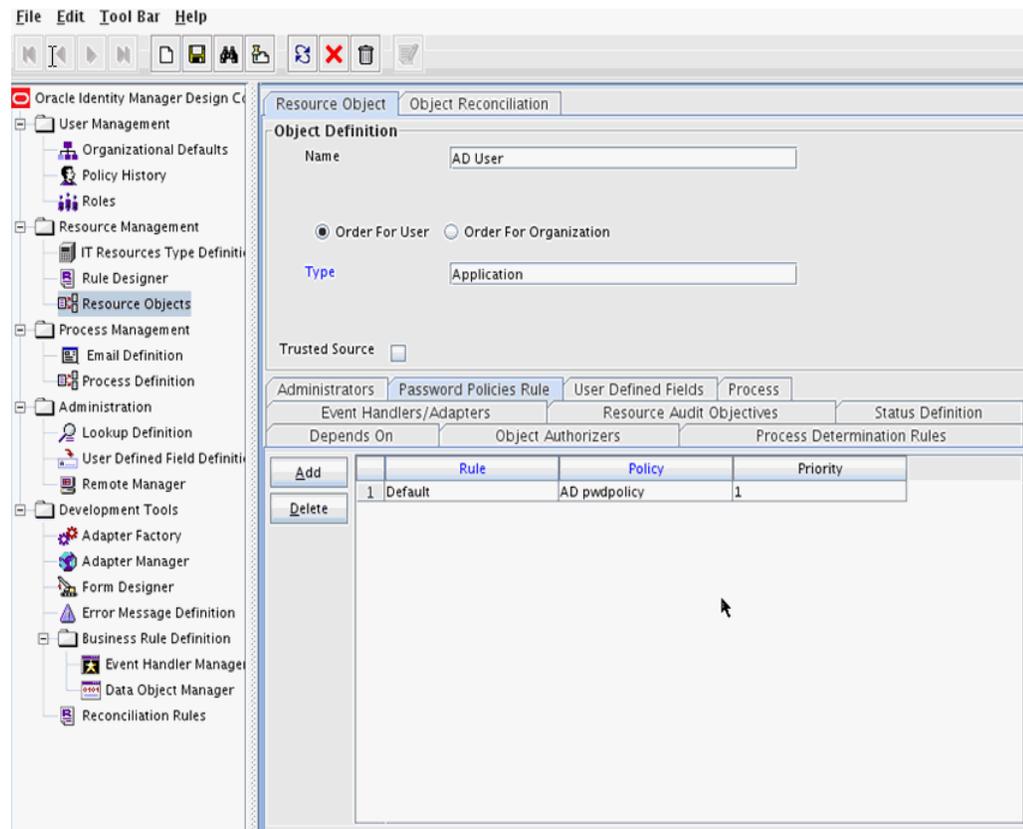
Figure 9–7 Password Policy for Application Instance

The screenshot displays the Oracle Identity System Administration interface for configuring a password policy. The main content area shows the following fields and sections:

- Policy Name:** AD pwdpolicy
- Description:** Password policy for Active Directory Application Instance
- Policy Rules:**
 - Minimum Length: 8
 - Disable First Passwords: 3
 - Minimum Password Age (Days):
 - Expires After (Days):
 - Warn After (Days):
- Complex Password:**
 - 1. The password is at least six characters long.
 - 2. The password contains characters from at least three of following five categories:
 - a. English Uppercase Characters (A-Z)
 - b. English Lowercase Characters (a-z)
 - c. Base 10 Digits (0-9)
 - d. Non-alphanumeric (for example: !, \$, # or *)
 - e. Unicode Characters
 - 3. The password does not contain any of user ID, first name, or last name when their length is larger than 2.
- Custom Policy:**
 - Maximum Length:
 - Maximum Repeated Characters:
 - Minimum Numeric Characters:
 - Minimum Alphanumeric Characters:
 - Minimum Unique Characters:
 - Minimum Alphabet Characters:
 - Minimum Uppercase Characters:
 - Minimum Lowercase Characters:
 - Characters Required:
 - Characters Allowed:
 - Characters Not Allowed:
 - Substrings Not Allowed:
 - Special Characters: Min: Max:
 - Unicode Characters: Min: Max:
 - Start with Alphabet:
 - Disallow First Name:
 - Disallow User ID:
 - Disallow Last Name:
- Password Dictionary Details:**
 - Password File:
 - File Delimiter:

4. After you set the password policy for an Application Instance, you need to attach the new policy to the connected (AD User) application instance. To do so:
 - a. Go to Design Console.
 - b. Under Resource Management, click **Resource Objects**.
 - c. Click on Password Policies Rule tab.
 - d. Select the new password policy (AD pwdpolicy) that you created to attach it to the connected application instance.
 - e. Click **Add**.

Figure 9–8 Attach Password Policy to Application Instance



9.4 Developing Entitlements

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 a 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.

In Oracle Identity Manager, there is one process form for each account (resource) provisioned to an OIM User. Entitlement data is stored in child process forms of the process form. In the example described earlier, the process form for Richard’s account on the target system has a child process form that holds Inventory Manager role data.

Attributes that constitute entitlement data stored on a child process form may vary from one target system to another. In addition, different types of entitlements, such as

roles and responsibilities, may have different attributes. For example, Target System A contains the following role data attributes:

- Role Name
- Role Description
- Start Date
- End Date

The same target system can have a different set of attributes for responsibility data:

- Responsibility ID
- Date Assigned
- Proxy User
- Escalation User

You can mark or highlight the attribute that uniquely identifies an entitlement on a target system. For the sample role and responsibility data attributes listed earlier, the Role Name and Responsibility ID attributes uniquely identify the role and responsibility entitlements on Target System A. By marking attributes that uniquely identify entitlements, you enable the capture of entitlement data that can be used by other identity management solutions and also displayed in reports.

Note: If you are using the SAP User Management connector release 9.x with this release of Oracle Identity Manager, then perform the following steps for the Roles and Profiles entitlements to work correctly:

1. In the Role Child Form, from the Role System Name field, remove the Entitlement and Required properties.
 2. In the Profiles Child Form, from the Profile System Name field, remove the Entitlement and Required properties.
-
-

This section discusses the following sections:

- [Available Entitlements and Assigned Entitlements](#)
- [Entitlement Data Capture Process](#)
- [Marking Entitlement Attributes on Child Process Forms](#)
- [Duplicate Validation for Entitlements or Child Data](#)
- [Configuring Scheduled Tasks for Working with Entitlement Data](#)
- [Deleting Entitlement](#)
- [Refreshing the Entitlement List Post Delete for New Entries](#)
- [Disabling the Capture of Modifications to Assigned Entitlements](#)
- [Entitlement-Related Reports](#)

9.4.1 Available Entitlements and Assigned Entitlements

A target system can have a set of entitlements defined and ready for assignment to accounts (users) on the target system. When you integrate this target system with Oracle Identity Manager, you can import (synchronize) entitlement data from the target system into the LKV table on Oracle Identity Manager.

Note: If you use a predefined connector to integrate the target system, then you can use scheduled tasks to fetch entitlement data into this table.

The schedule job, Entitlement List will synchronize the entitlements from LKV to ENT_LIST. This job will also kick off Catalog Synchronization job to synchronize the entitlements to Catalog. An entitlement is available when it can be found in Catalog. See [Section 17.3.2.3, "Ongoing Synchronization"](#) for more information about configuring Catalog Synchronization.

During a provisioning operation, you request the entitlement through the Catalog. You can also populate the entitlement data along with the parent data as request data set when submitting a request for an application instance.

In this guide, entitlements assigned to accounts are called assigned entitlements. Data about assigned entitlements is stored in child process form tables.

9.4.2 Entitlement Data Capture Process

After you mark the entitlement attribute in each child process form, the following processes take place:

- [Capture of Data About Available Entitlements](#)
- [Capture of Data About Assigned Entitlements](#)

9.4.2.1 Capture of Data About Available Entitlements

The following steps describe how data about available entitlements is captured:

Note:

- You must mark the entitlement attribute in each child process form to enable the process described in these steps. The procedure is described later in this chapter.
 - Make sure that the parent form has the latest child form version. It does not automatically happen when you create, edit, and activate the child parent without doing the same with the parent form.
-
-

1. Data about available entitlements is stored in the LKV table through synchronization with the target system.
2. You schedule and run the Entitlement List scheduled task.
3. The schedule task identifies the entitlement through the entitlement property in process form.
4. The scheduled task copies data about available entitlements from the LKV table to the ENT_LIST table.

9.4.2.2 Capture of Data About Assigned Entitlements

This section describes how data about assigned entitlements is captured. When the entitlement attribute is marked in a child process form, a trigger is created on the corresponding UD table. The same holds true when a form with entitlement attribute marked is imported via connector installation.

Note: You must mark the entitlement attribute in each child process form UD_ table to enable the process described in these steps. The procedure is described later in this chapter.

Entitlement assignment is mostly performed in real time via triggers.

The trigger:

1. Copies assigned entitlements from UD tables to ent_assign table when the entitlement is inserted to the UD tables.
2. Moves assigned entitlements from ent_assign to ent_assign_list when the entitlement is removed from UD tables.
3. Copies newly assigned entitlement from UD tables to ent_assign table when the entitlement is updated in UD tables and moves the old assignment to ent_assign_list table.

In case entitlement does not get assigned properly via trigger, then you can use the Entitlement Assignments scheduled task to do a full synchronization.

For example, if an Account Reconciliation scheduled task runs and brings in new entitlement assignments from the target, but the entitlement definitions do not exist in ENT_LIST, then the trigger-based mechanism will not work. In this condition, you need to ignore such entries in the trigger, and handle them via the scheduled task. This is applicable after the entitlement is reconciled from the target.

9.4.3 Marking Entitlement Attributes on Child Process Forms

You must mark the entitlement attribute in the child process form UD_ table for resources for which you want to capture entitlement data. Suppose there are 15 target systems in your operating environment. If you want to capture entitlement data from 12 of 15 resources, then you must mark the entitlement attribute in those 12 resources.

Apply the following guidelines while performing the procedure described in this section:

- On a child process form, only one attribute holding entitlement data can be marked.
- The attribute that you mark must be of the LookupField type and its property must be one of the following:
 - Lookup code
 - Lookup query

The Lookup query must satisfy the following conditions:

- * The query uses the LKU and LKV tables
- * The Lookup code in the query is from the LKU table
- * The LKV_ENCODED column value is used for saving
- * The LKV_DECODED column value is used for display purposes

To mark a field as an entitlement in a child process form:

1. Log in to the Design Console.
2. Expand **Development Tools**, and then double-click **Form Designer**.
3. Search for and open the child form on which you want to mark an entitlement.

For example, you might want to mark an entitlement on the UD_ADUSRC child form.

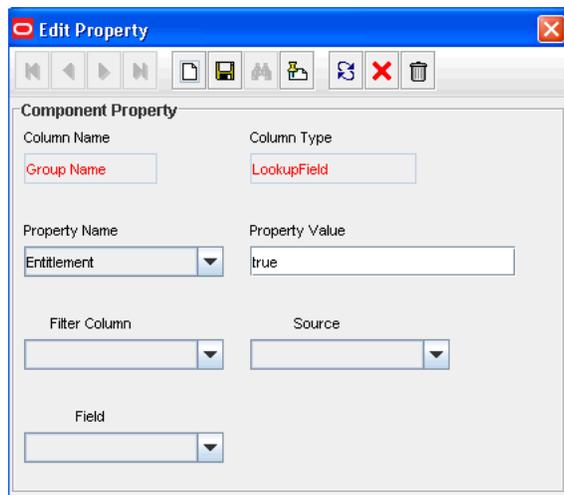
4. Click **Create New Version**.
5. Enter a label for the new version, click the Save icon, and then close the dialog box.
6. From the **Current Version** list, select the version that you create.
7. On the Properties tab, select the field that you want to mark as an entitlement and then click **Add Property**.
8. From the Property Name list in the Add Property dialog box, select **Entitlement**.

Note: You can set Entitlement as the property of a field only if the column type is set to LookupField and the property name is set to Lookup Code.

9. In the **Property Value** field, enter `true`.

You need not specify values for any of the other fields in the dialog box.

The following screenshot shows the Edit Property dialog box for the lookup field:



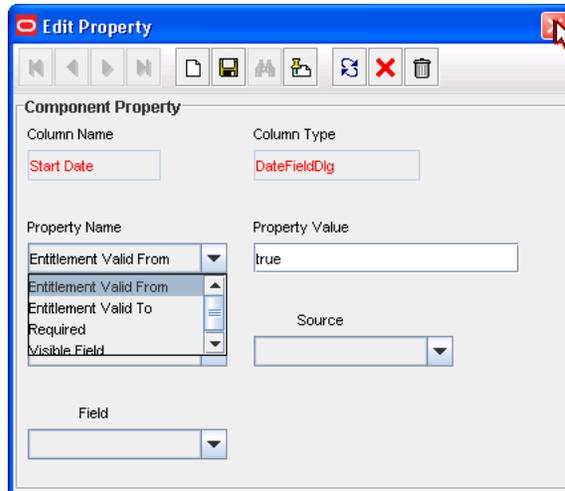
10. Click the Save icon and then close the dialog box.
11. If you want to enable the capture of Start Date and End Date values for the entitlement, then:

Note: You can enable the capture of the Start Date and End Date values only if the column type for both fields is DateFieldDlg.

- a. On the Properties tab, select the **Start Date** field and then click **Add Property**.
- b. From the Property Name list in the Add Property dialog box, select **Entitlement Valid From**.
- c. In the Property Value field, enter `true`.
- d. Click the Save icon and then close the dialog box.
- e. On the Properties tab, select the **End Date** field and then click **Add Property**.

- f. From the Property Name list in the Add Property dialog box, select **Entitlement Valid To**.
- g. In the Property Value field, enter `true`.

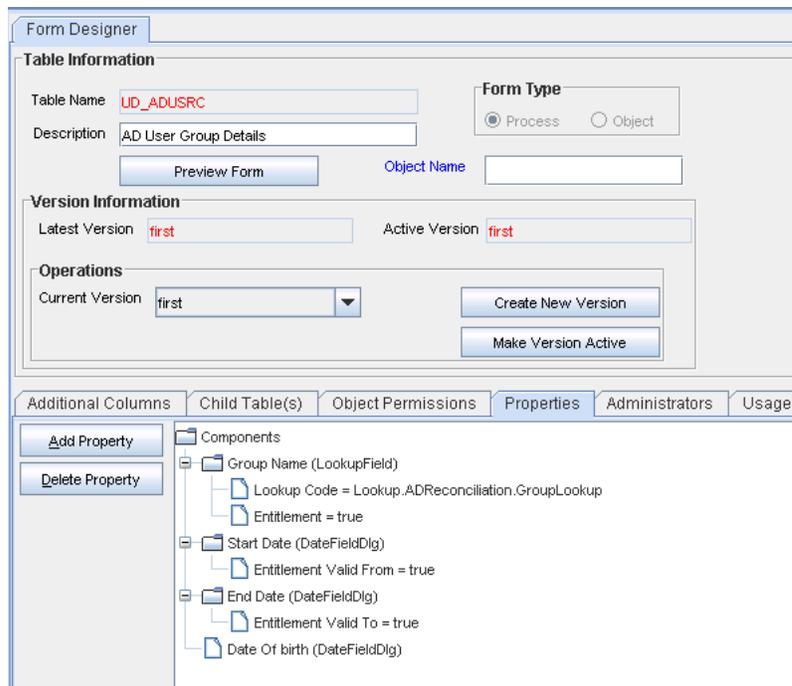
The following screenshot shows the Edit Property dialog box for the Start Date field:



- h. Click the Save icon, and then close the dialog box.

12. Click the Save icon to save the changes made to the child process form.

The following screenshot shows the Properties tab of the child process form:



Note: Marking Start Date and End Date are optional.

13. Click **Make Version Active**.

Note: Make sure that the parent form has the latest child form version. It does not automatically happen when you create, edit, and activate the child parent without doing the same with the parent form.

9.4.4 Duplicate Validation for Entitlements or Child Data

Oracle Identity Manager validates duplicate entitlement or child data based on the following attributes, which ever is set:

- Key attribute
- Entitlement attribute

The configuration of the above mentioned attributes are checked prior to validating duplicates in the child data. [Table 9–2](#) summarizes the possible valid and invalid configurations.

Table 9–2 Possible Scenarios and Duplicate Validation Basis

Entitlement Attribute	Key Attribute for Reconciliation Field Mapping	Configuration Validation	
		Connected Application Instance	Disconnected Application Instance
Not defined	Not defined	Valid	Valid
<p>Note: In this scenario, the user is at a risk of adding duplicate entitlements or child data as the configurations are not defined properly. A warning message is logged on the server asking the user to define entitlement attribute and matching reconciliation field mapping.</p>			
Defined.	Not defined	Invalid	Valid
<p>One attribute, say UD_CHILD1_ENT1 has Entitlement=true</p> <p>Note: Entitlement attribute does not have a matching key attribute defined in reconciliation field mapping.</p>			
Not defined	Defined.	Valid	Valid
<p>One attribute, say UD_CHILD1_ENT1 is set as the key attribute in recon field mapping.</p>			

Table 9–2 (Cont.) Possible Scenarios and Duplicate Validation Basis

Entitlement Attribute	Key Attribute for Reconciliation Field Mapping	Configuration Validation	
		Connected Application Instance	Disconnected Application Instance
Defined. One attribute, say UD_CHILD1_ENT1 has Entitlement=true	Defined. One attribute, say UD_CHILD1_ENT1 is set as the key attribute in recon field mapping.	Valid	Valid
Defined. One attribute, say UD_CHILD1_ENT1 has Entitlement=true Note: Entitlement attribute is a subset of the reconciliation field mapping key attributes.	Defined. Two or more attributes, say UD_CHILD1_ENT1 and UD_CHILD1_ENT2 are defined as key attributes in recon field mapping for child table UD_CHILD1.	Valid	Valid
Defined. One attribute, say UD_CHILD1_ENT1 has Entitlement=true Note: Entitlement attribute does not have a matching key attribute defined in reconciliation field mapping.	Defined. One or more attributes, say UD_CHILD1_ENT2 and UD_CHILD1_ENT3 are defined as key attributes in recon field mapping	Invalid	Invalid

Oracle recommends configuring both the entitlement attribute and the matching key attribute for the child data in reconciliation field mappings to enable effective validation.

Once a valid configuration is detected, duplicates are validated based on the operation as listed in [Table 9–3](#).

Table 9–3 Duplicate Validation Based on Operation

Operation	Duplicate Validation Description
Adding entitlement(s)	The attribute for which "Entitlement=true" property is defined.
Adding child data	The attribute that is the key attribute in the reconciliation field mappings.

Note: Oracle recommends configuring both the entitlement attribute and the key attribute for the child data in reconciliation field mappings to enable effective duplicate entitlement or child data validation.

9.4.5 Configuring Scheduled Tasks for Working with Entitlement Data

You configure the following scheduled tasks for working with entitlement data:

- [Entitlement List](#)
- [Entitlement Assignments](#)

9.4.5.1 Entitlement List

The Entitlement List scheduled task identifies the entitlement attribute from the child process form table and then copies entitlement data from the LKV table into the ENT_LIST table. A record created in the ENT_LIST table corresponds to an entitlement defined on a particular target system.

You must set a schedule for this task depending on how frequently new entitlements are defined on the target systems in your operating environment. In addition, you must run this scheduled task when new target systems are integrated with Oracle Identity Manager. In other words, you must run this task each time you mark a new entitlement. After the connector scheduled tasks fetch lookup field data from the target system into the LKV table, you can run the Entitlement List scheduled task to copy that entitlement data into the ENT_LIST table.

This scheduled task also handles updates to or deletion of entitlements from the target system. For example, if the Senior Accounts Analyst role is removed from the target system, then the connector scheduled task removes the entry for that role from the LKV table. When the Entitlement List scheduled task is run, it marks the row containing the role in the ENT_LIST table as a deleted row.

9.4.5.2 Entitlement Assignments

The Entitlement Assignments scheduled task is used for copying data about assigned entitlements into the ENT_ASSIGN table, in case when triggers fail to synchronization entitlement from UD table to ENT_ASSIGN. This task identifies the entitlement attribute from the child process form table, and then copies data about assigned entitlements from the child process form table into the ENT_ASSIGN table. A record created in the ENT_ASSIGN table corresponds to an entitlement assigned to a particular user on a particular target system.

In addition, it creates INSERT, UPDATE, and DELETE triggers on the child process form tables from which it copies entitlement data. See "[Capture of Data About Assigned Entitlements](#)" on page 9-20 for information about the function of these triggers.

You can use the RECORDS_TO_PROCESS_IN_BATCH attribute of this scheduled task to specify the number of records in each batch. The default batch size is 5000.

9.4.6 Deleting Entitlement

Entitlements can get deleted in any one of the following ways:

- Deleting the Entitlement in the target, followed by synchronizing it via lookup reconciliation and further by the Entitlement List schedule job.
- Direct deletion of the Entitlement from Entitlement List via APIs.
- Deleting via corresponding application instance.

In all the ways of deleting, the Entitlement will be marked as soft-deleted, that is, the "valid" flag on the Entitlement will be updated to mark it as soft-deleted.

In all the cases of deleting, you need to perform the following post-processing.

- Unpublish the entitlement from the organization to which it is published
- Update the Modify_date on the Entitlement in Entitlement List to the current date
- Purge the instances of the Entitlement in the child table and Entitlement Assign
- Remove the Entitlements that are picked up by Catalog harvesting, that are marked as soft-deleted, and all request profiles.

Note:

- In-flight requests that have references to soft-deleted Entitlements will fail.
 - Access Policies having deleted Entitlements should be manually updated to remove the same.
-
-

To perform post-processing of Entitlement soft-deletion in the provisioning component:

1. Run the EntitlementPostDeleteProcessing scheduled job.

This task will take the following inputs:

- Application Instance Name/ALL
- Mode: Revoke/Delete

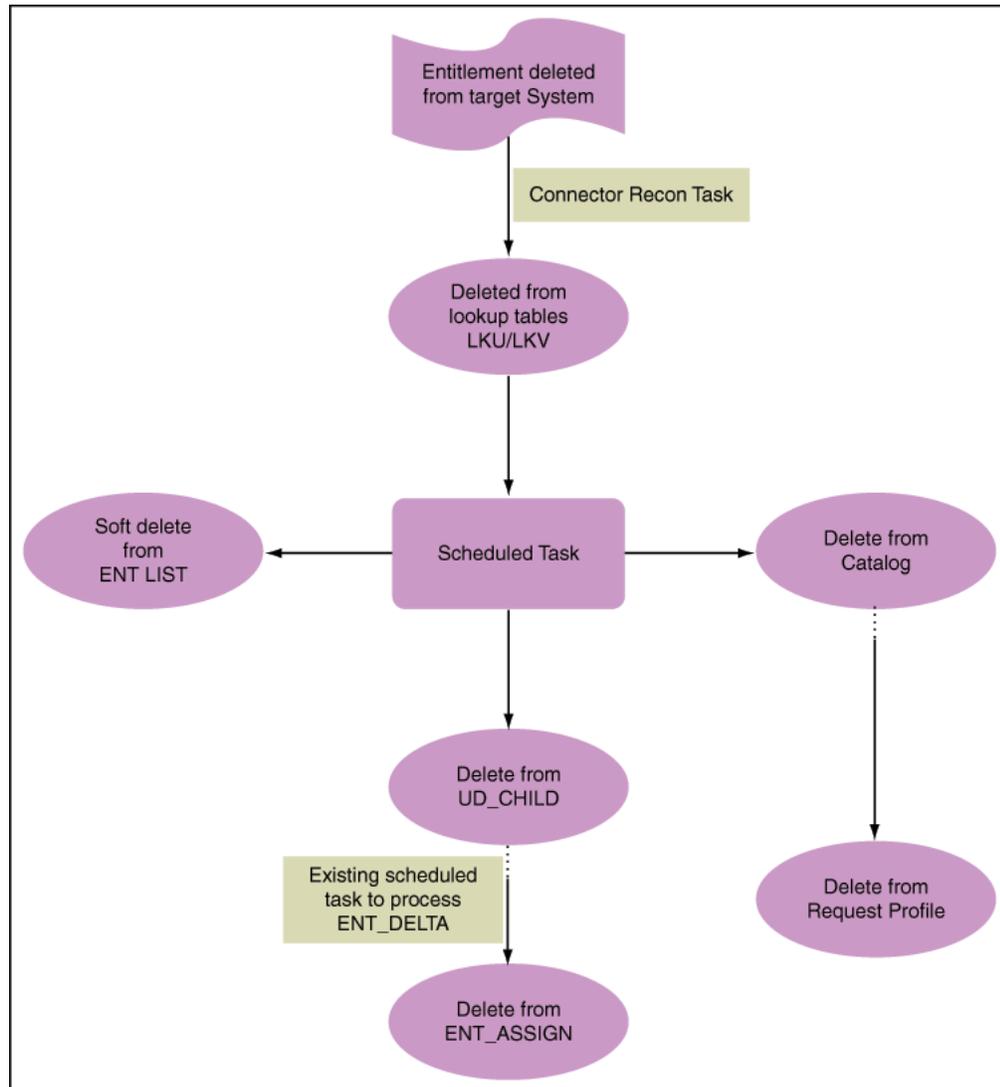
2. The task will perform the following functionality:

- a. Revoke mode: The scheduled task will revoke the entitlement-grant for all the accounts in Oracle Identity Manager, which have that specific entitlement granted.
- b. Delete mode: The schedules task will simply hard-delete the entitlements from OIM database in the UD_CHILD table.
- c. In both the above cases, the Entitlement grant entry will be removed from ENT_ASSIGN.

3. Run the Entitlement List scheduled task. This is an existing scheduled task that will go to all the resources that have an entitlement field, get the corresponding lookup definition and populate ENT_LIST with the values from the lookup definition, setting the correct SVR_KEY in the process.

Figure 9–9 shows the flow and changes that will be made upon Entitlement soft-deletion.

Figure 9–9 Entitlement Soft-Deletion Flow



9.4.7 Refreshing the Entitlement List Post Delete for New Entries

When an entry with the same encoded value is deleted and added consecutively in a lookup code, you need to perform the following steps to synchronize the data to the entitlement list:

1. Login to Oracle Identity System Administration.
2. Run the Entitlement List job to soft delete the existing entry.
3. Run the EntitlementPostDeleteProcessing job with Delete mode to clean up soft deleted items.
4. Run Entitlement List job again to add the new entry.

9.4.8 Disabling the Capture of Modifications to Assigned Entitlements

You can manually disable incremental synchronization of assigned entitlement data in the ENT_ASSIGN table. In other words, you can disable the capture of modifications

to assigned entitlements. To achieve this, you create and run an SQL script to drop the following triggers created on the child process form tables:

Note: These triggers are created by the Entitlement Assignments scheduled task.

- The OIU_UDPATE trigger created on the OIU table
- The *TABLE_NAME_ENT_TRG* triggers created on the UD_ tables:

After you run the script, modifications to assigned entitlements are not copied into the staging table.

The following is a sample SQL script to drop the triggers on the child process form tables:

```
create or replace
TRIGGER UD_LDAP_GRP_ENT_TRG
AFTER INSERT
OR DELETE
OR UPDATE OF UD_LDAP_GRP_GROUP_NAME
ON UD_LDAP_GRP
FOR EACH ROW
BEGIN
CASE
WHEN INSERTING THEN
OIM_SP_MANAGEENTITLEMENT ('UD_LDAP_GRP', :NEW.UD_LDAP_GRP_GROUP_NAME, NULL,
:NEW.UD_LDAP_GRP_KEY, :NEW.ORD_KEY, NULL, NULL, NULL,
NULL, NULL, 'INSERT' );
WHEN UPDATING THEN
IF :NEW.UD_LDAP_GRP_GROUP_NAME != :OLD.UD_LDAP_GRP_GROUP_NAME
THEN
OIM_SP_MANAGEENTITLEMENT ('UD_LDAP_GRP', :NEW.UD_LDAP_GRP_GROUP_NAME,
:OLD.UD_LDAP_GRP_GROUP_NAME, :NEW.UD_LDAP_GRP_KEY, :NEW.ORD_KEY, NULL,
NULL, NULL,
NULL, NULL, 'UPDATE' );
END IF;
WHEN DELETING THEN
OIM_SP_MANAGEENTITLEMENT ('UD_LDAP_GRP', :OLD.UD_LDAP_GRP_GROUP_NAME,
NULL, NULL, :OLD.ORD_KEY, NULL, NULL, NULL,
NULL, NULL, 'DELETE' );
END CASE;
END;
```

9.4.9 Entitlement-Related Reports

The following predefined reports provide data about assigned entitlements:

Note:

You must be a member of the ADMINISTRATORS group to be able to view these reports.

Duplicate assignments of the same entitlement to a particular user are suppressed in the reports because they are not copied to the ENT_ tables. For example, if user John Doe has been assigned the Sales Superintendent role twice on a target system, then the reports show only one instance of this entitlement.

- [Entitlement Access List](#)
- [Entitlement Access List History](#)
- [User Resource Entitlement](#)
- [User Resource Entitlement History](#)

9.4.9.1 Entitlement Access List

The Entitlement Access List report lists users who are currently assigned the entitlements that you specify while generating the report. The report provides basic information about the entitlements and the list of users to whom the entitlements are assigned.

9.4.9.2 Entitlement Access List History

The Entitlement Access List History report lists users who had been assigned the entitlements that you specify while generating the report. The report provides basic information about the entitlements and the list of users to whom the entitlements were assigned.

9.4.9.3 User Resource Entitlement

The User Resource Entitlement report lists the current entitlements of users whom you specify while generating the report. The report displays basic user information and entitlement details.

9.4.9.4 User Resource Entitlement History

The User Resource Entitlement History report lists details of past entitlements assigned to users whom you specify while generating the report. The report displays basic user information and entitlement details.

Managing Disconnected Resources

Disconnected resources are targets for which there is no connector. Therefore, the provisioning fulfillment for disconnected resources is not automated, but manual. In earlier releases of Oracle Identity Manager, disconnected provisioning is not supported as a first class use case, it is supported by using manual tasks in the provisioning process. This approach has a number of limitations, which are taken care in Disconnected Resources model. In Oracle Identity Manager 11g Release 2 (11.1.2.1.0), disconnected resources are an enhanced configuration for manual provisioning that leverage SOA integration to provide higher flexibility and configurability of the manual provisioning workflow.

Some examples of disconnected resources include a Badge, Laptop, Pager, or any such item wherein the fulfillment is manual.

This chapter enlists the following topics:

- [Section 10.1, "Disconnected Resources Architecture"](#)
- [Section 10.2, "Managing Disconnected Application Instance"](#)
- [Section 10.3, "Provisioning Operations on a Disconnected Application Instance"](#)
- [Section 10.4, "Managing Entitlement for Disconnected Resource"](#)
- [Section 10.5, "Status Changes in Manual Process Task Action"](#)
- [Section 10.6, "Customizing Provisioning SOA Composite"](#)
- [Section 10.7, "Troubleshooting Disconnected Resources"](#)

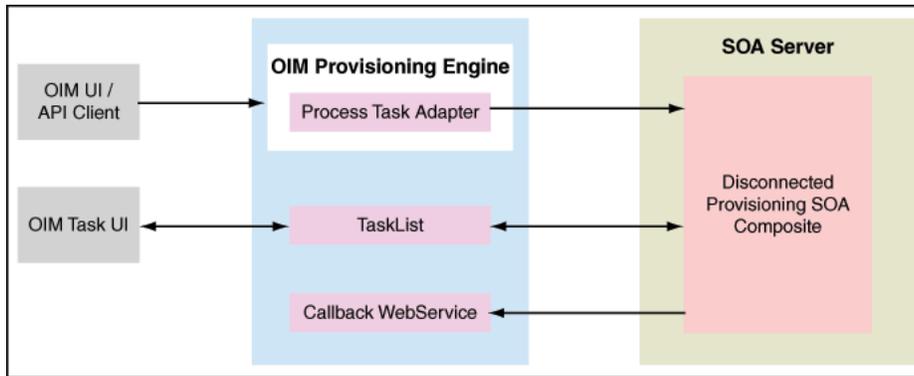
10.1 Disconnected Resources Architecture

The Disconnected Resource feature makes use of the existing Oracle Identity Manager provisioning engine artifacts such as the Provisioning Process, Process Task, Adapters and so on while providing BPEL Integration in a seamless and configurable manner.

When a Disconnected Application Instance is created from the UI, it automatically seeds a number of backend configuration artifacts, including a resource object (of type Disconnected), a provisioning process with tasks for the basic provisioning operations, an IT resource, and a process form with the minimal fields (which can be further customized).

[Figure 10-1](#) illustrates the provisioning process architecture for disconnected resources.

Figure 10–1 Disconnected Resource Architecture



When a disconnected application instance is provisioned to a user (via request or otherwise), the specific workflow in the provisioning process is triggered. This fires the corresponding process task and executes the manual provisioning adapter that invokes the out of the box disconnected provisioning SOA composite. A SOA manual task is assigned to System Administrator by default. When the assignee acts on the manual task, the provisioningcallback webservice is invoked with the assignee specified response and it then completes or aborts the provisioning operation and updates the account appropriately.

Table 10–1 displays the attributes for manual provisioning SOA composite payload that is available in the composite.

Table 10–1 Manual Provisioning SOA Composite Payload Attributes

Attribute	Description
Account ID	Account ID (oiu_key) for the account under consideration
AppInstance Name	Disconnected Application Instance Display Name
Resource Object Name	Disconnected Resource Object Name
ITResource Name	Disconnected ITResource Name
Beneficiary Login	Login of the account beneficiary
Entity Key	Application Instance Key in case of Provision, Revoke, Disable, and Enable account operations.
Entity Type	Type is set to ApplicationInstance, in case of Provision, Revoke, Disable, and Enable account operations.
Beneficiary First Name	First name of the account beneficiary
Beneficiary Last Name	Last name of the account beneficiary
Descriptive Field	Account descriptive field for the account under consideration
URL	Oracle Identity Manager callback URL for the webservice.
Request Key	Request Key if operation is through request.
Requester Login	Login of the requester if operation is through request.

10.2 Managing Disconnected Application Instance

Managing disconnected application instance includes the following tasks:

- [Section 10.2.1, "Creating a Disconnected Application Instance"](#)

- [Section 10.2.2, "Creating a Disconnected Application Instance for an Existing Disconnected Resource"](#)

10.2.1 Creating a Disconnected Application Instance

Note: Before creating the application instance, you must create a new sandbox and publish it after creating the application instance. See "Managing Sandboxes" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for information about creating and publishing a sandbox.

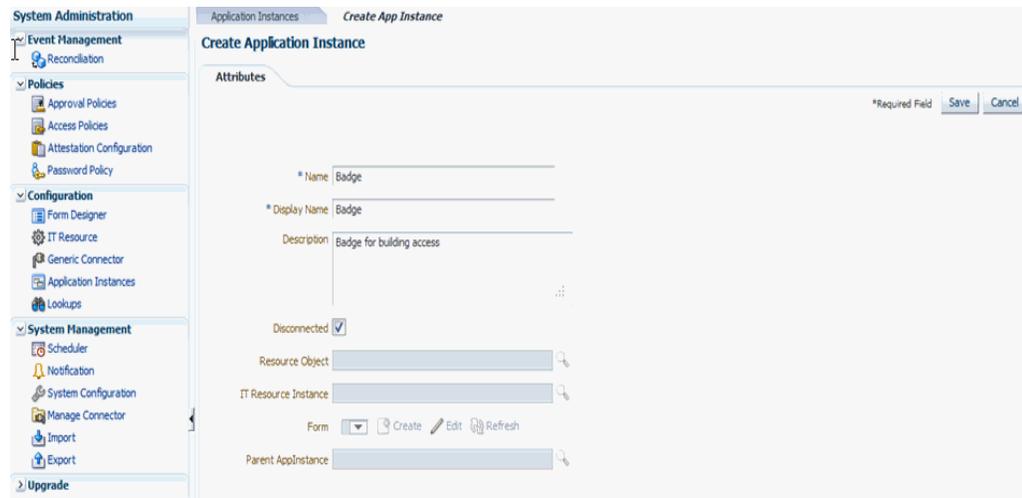
To create disconnected application instance:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **Application Instances**. The Application Instances page is displayed.
3. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Application Instance page is displayed.
4. In the respective attribute fields, enter the values as shown in the following table:

Attribute	Value
Name	Enter the name of the application instance. This is a required field.
Display Name	Enter the display name of the application instance. This is a required field.
Description	Specify a description of the application instance.
Disconnected	Select the checkbox. This is the flag to indicate whether the application instance is not connected. Note: This is a UI only flag and is not persisted in the backend. Checking this flag will disable Resource Object and ITResource Instance fields, as these will be automatically created in the back end.

Figure 10–2 shows the attributes for Create Application Instance attributes:

Figure 10–2 Create Application Instance Attributes



5. Click **Save**. The application instance is created, and the details of the application instance is displayed.
6. The UI form for the disconnected resource is automatically created and set, click **Apply**.
7. In addition to the application instance, in the back end, the following provisioning artifacts are automatically created:
 - Resource object of type Disconnected
 - ITresource type definition with the following parameters:
 - Configuration Lookup
 - Connector Server Name
 - Identity Gateway Name

Note: IT resource type definition parameters are for future use and the values for the same need not be set.

- IT resource of type definition
- Parent process form with the following fields:
 - Account ID
 - Password
 - Account login
 - IT resource
- Process definition with workflows for the following operations:
 - Provision Account
 - Enable Account
 - Disable Account
 - Revoke Account
 - Modify Account Attributes

- Adapters
 - Manual Provisioning
 - Manual Entitlement Provisioning
- 8. From the System Administration UI, search for schedule job called "Catalog Synchronization Job" and execute it.

10.2.2 Creating a Disconnected Application Instance for an Existing Disconnected Resource

To create a disconnected application instance for an existing disconnected resource, see [Section 9.2.1, "Creating Application Instances"](#).

Note: You must not select the **Disconnected** option, as this will create artifacts including the resource object and IT resource in the backend.

10.3 Provisioning Operations on a Disconnected Application Instance

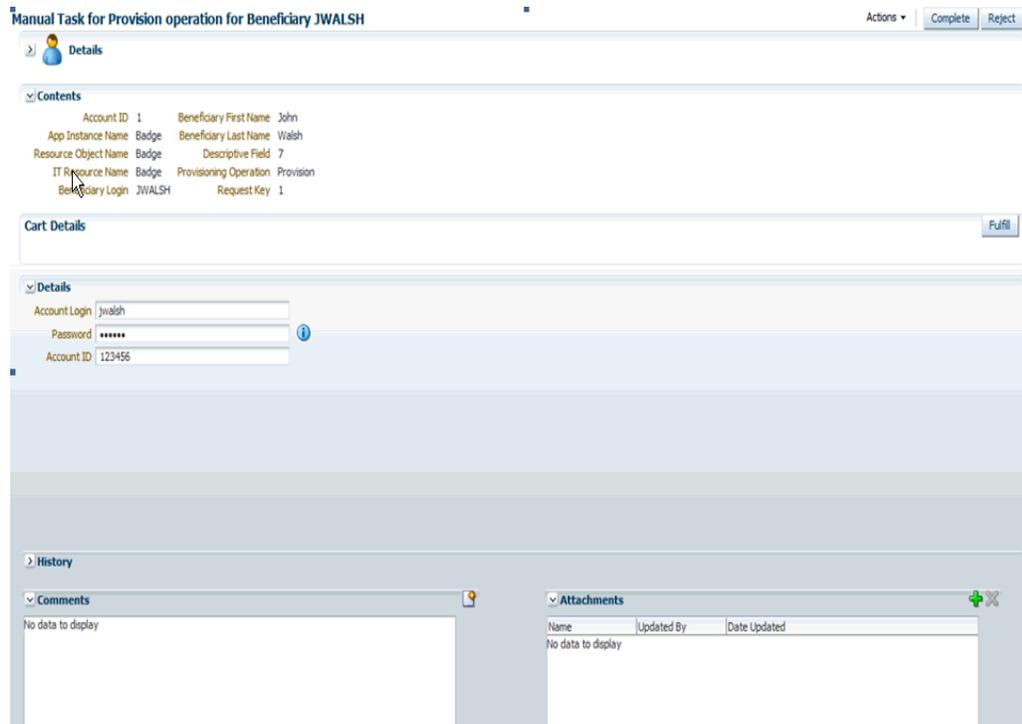
When provisioning process is triggered for Enable, Disable, Revoke, or Provision operations, the corresponding process task is inserted which runs the Manual Provisioning adapter. This adapter invokes the out of the box provisioning SOA composite. A SOA Human Task is assigned to the System Administrator by default.

The System Administrator from the pending approvals page can:

- Check the task details
- Check the account details
- Change process form data in OIM by changing data and clicking the Fulfill button
- Perform the operation manually in the target
- Act on the pending task by clicking Complete or Reject.

[Figure 10–3](#) displays the field options for provisioning operations for beneficiary.

Figure 10–3 Provision Operation for Disconnected Resources



When the assignee acts on the pending manual tasks, the provisioning callback webservice is invoked which continues with the Oracle Identity Manager operation and updates the account appropriately. See [Section 10.5, "Status Changes in Manual Process Task Action"](#) for details on changes to account status based on assignee action.

10.3.1 Process Form Updates

When a process form field of a disconnected resource is updated, the "<FORM_NAME> Updated" process task will be inserted into the provisioning process. This would generate a manual SOA human task, so that the assignee can manually update the changes in the corresponding target.

Note: The "<FORM_NAME> Updated" task will be inserted irrespective of whether updates are to a single process form field or multiple process form field. This behavior is different from that of a connected resource. In addition, note that the individual process form field update tasks need not be configured for a disconnected resource.

10.4 Managing Entitlement for Disconnected Resource

Managing entitlement for disconnected resource includes the following tasks:

- [Section 10.4.1, "Configuring Entitlement Grant"](#)
- [Section 10.4.2, "Configuring for Entitlement Revoke"](#)

10.4.1 Configuring Entitlement Grant

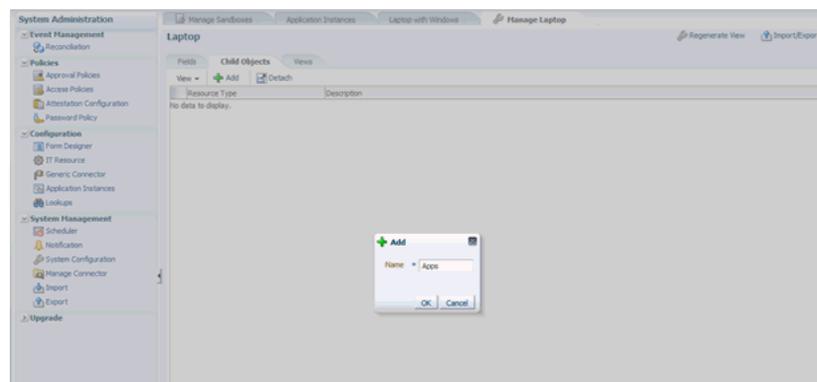
Configuring Entitlement Grant for disconnected resource involves configuring the following:

- Section 10.4.1.1, "Creating a Child Form and Configuring Entitlement Lookup via Form Designer"
- Section 10.4.1.2, "Configuring the Process Task that Invokes the SOA Composite"

10.4.1.1 Creating a Child Form and Configuring Entitlement Lookup via Form Designer

To create a child form and configure the lookup definition for entitlements:

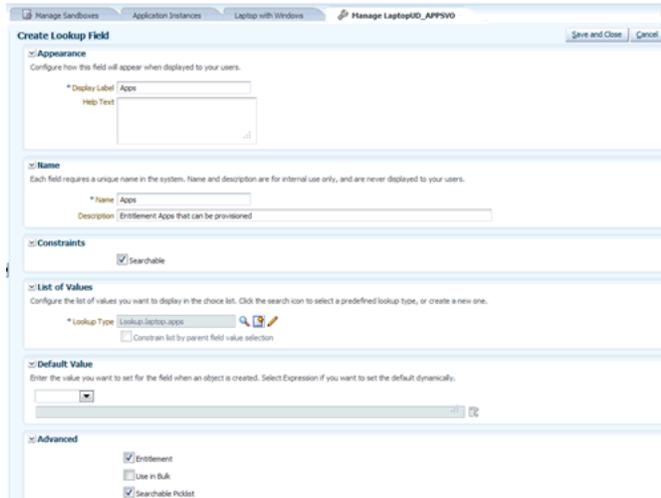
1. Once the disconnected application instance is created, the IT Resource Instance field will be populated by the name of the IT Resource instance created. Note down the IT resource instance name (this step is referring to Create Application Instance page).
2. Using SQL Plus, open a connection to Oracle Identity Manager database and run the following query:
 - a. Select svr_key, svr_name from svr where svr_name=<IT_RESOURCE_NAME>
 - b. Use the IT resource name from Step 1 as the svr_name. Note down the svr_key that this query returns.
3. Go to Oracle Identity System Administration. Under Configuration, click **Form Designer** and perform the following steps:
 - a. Select Type as Resource.
 - b. Click on the Resource Type and search for the Disconnected Resource.
 - c. From the search result, click on the disconnected application instance form name.
4. Go to Child Objects tab and click **Add** to add a child form.
5. In the Name field, provide a name to the child table and click **OK**.



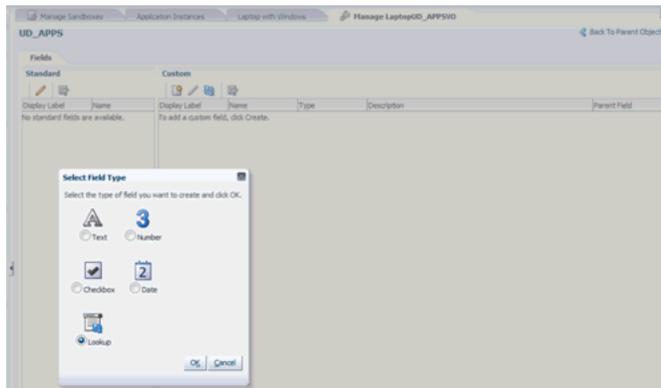
6. Click the UD_<CHILD_TABLE_NAME> link to open it for editing.
7. Provide the following values for the entitlement field:
 - a. In the Display Label field, enter a display name.
 - b. In the Name field, enter a name for the lookup.
8. Select the following check boxes:
 - Searchable
 - Entitlement

- Searchable Picklist

Note: It is mandatory that you must select Searchable, Entitlement, and Searchable Picklist check boxes to create an entitlement field on the child form.



9. Create a new custom field of Lookup Type and click **OK**.

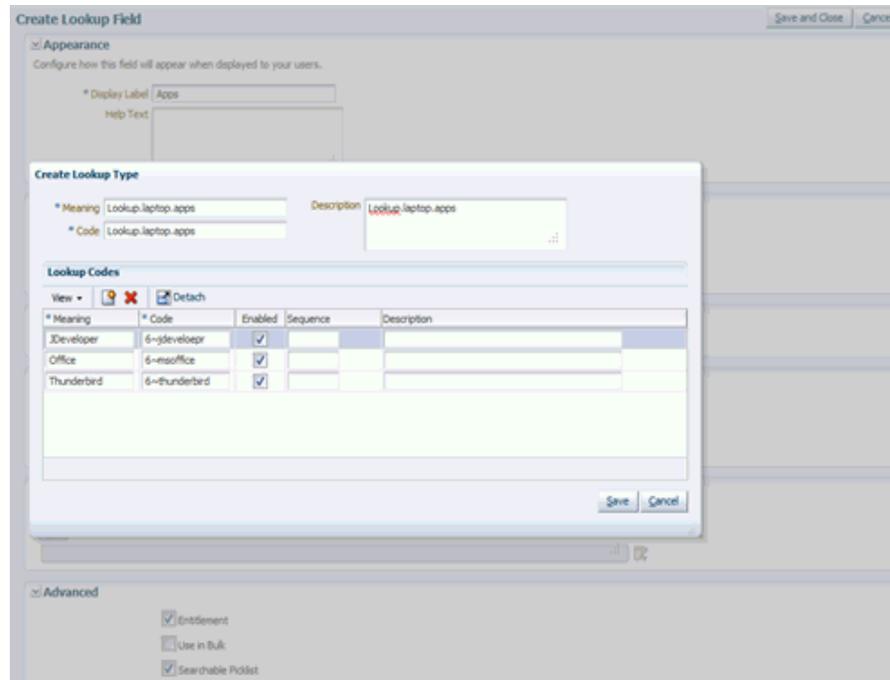


10. In the List of Values section, click the create a new lookup type icon and provide values for Meaning (for example, Lookup.Laptop.apps), Code (for example, Lookup.Laptop.apps) and description as follows:

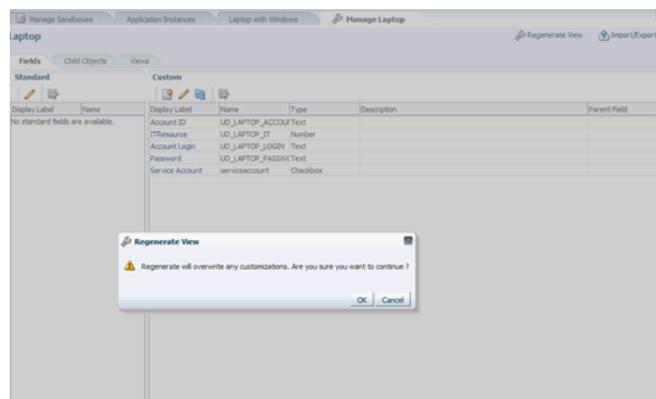
a. Click new to add entitlement values to add Lookup Codes. The value in the Code and Meaning columns should have the following format:

Code	Meaning
<svr_key>~<ENTIT LEMENT_NAME>	<ENTITLEMENT_D ESCRPTION>

b. Click **Save and Close**.



11. Click **Back to Parent Object** to return to the parent form.
12. Click **Regenerate View** to regenerate UI artifacts and dataset, and confirm by clicking **OK**.



13. Go back to Oracle Identity System Administration, System Management, Scheduler.
14. Search for a scheduled job called Entitlement List and execute it.
15. After the scheduled job execution completes, search for another schedule job called Catalog Synchronization Job and execute it.

10.4.1.2 Configuring the Process Task that Invokes the SOA Composite

To configure the process task that invokes the SOA composite:

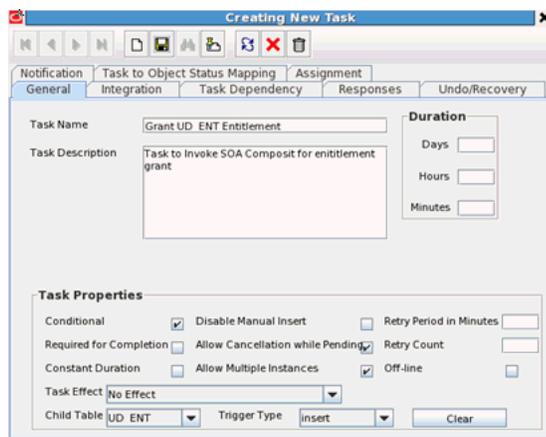
1. From the Design Console, navigate to the Process Definition form of the disconnected resource.
2. Click **Add Task** to add a new process task with the name for example, Grant UD_ENT Entitlement.

Note: You must make sure:

1. that the following flags are set:
 - Conditional
 - Allow Multiple Instances
2. to deselect the "Required for Completion" flag.

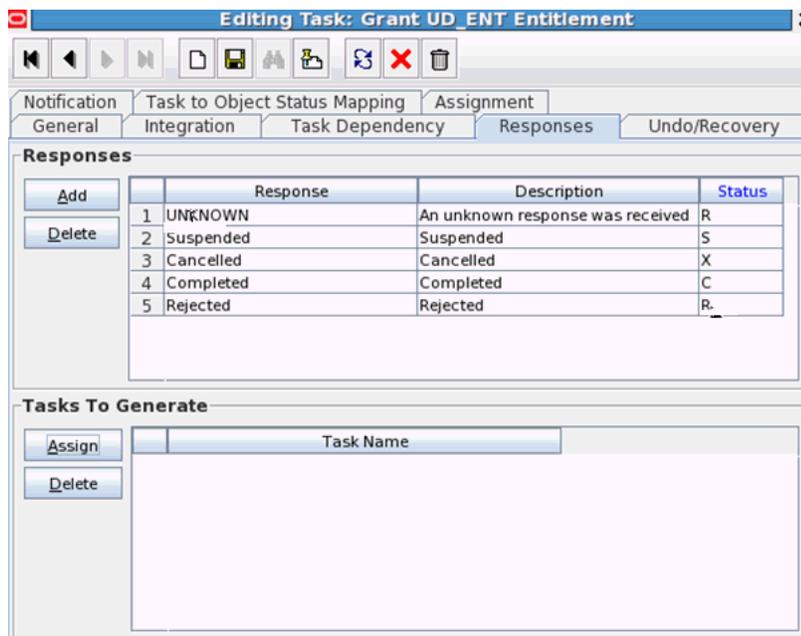
3. Select the child table, for example, UD_ENT from the combo box and set Trigger Type as **Insert**.
4. Save the task. [Figure 10-4](#) displays the process task fields.

Figure 10-4 Create Process Task



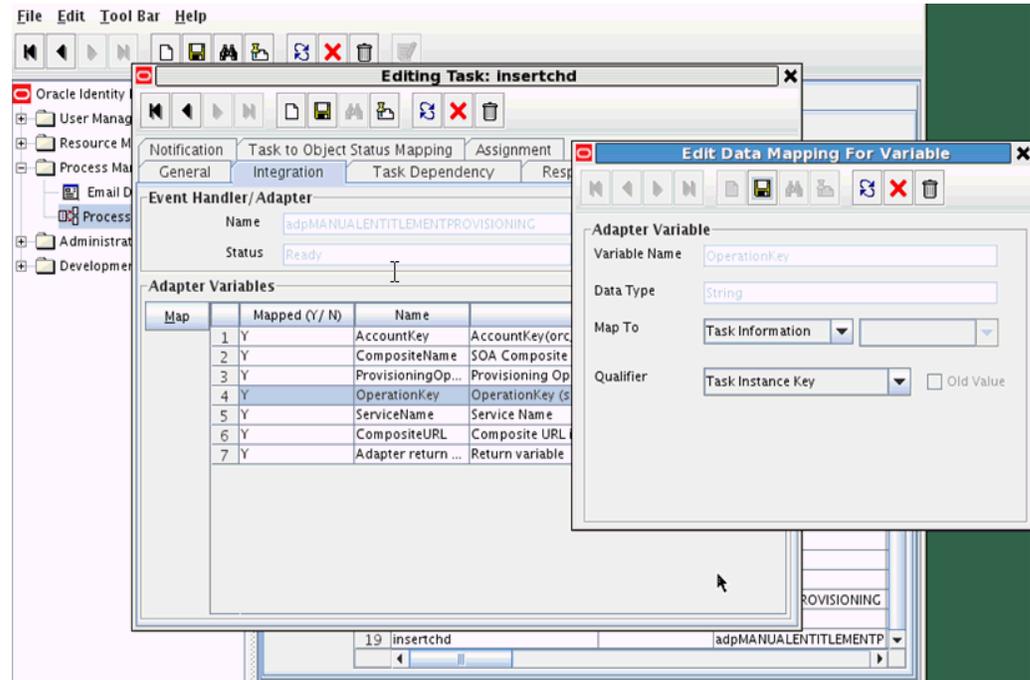
5. Navigate to the Responses tab for the same task, and add Response, Description, and Status as shown in [Figure 10-5](#).

Figure 10-5 Edit Entitlement



6. Navigate to the Integration tab for the same task.
7. Click **Add** and select the Adapters radio button.
8. Select the `adpMANUALENTITLEMENTPROVISIONING` adapter. The adapter has seven variables. [Figure 10–5](#) shows a sample adapter variable mapping.

Figure 10–6 Sample Adapter Variable Mapping



9. Configure the adapter variable mappings to Literal Strings as shown in [Table 10–2](#).

Note: While performing this step, you must ensure that there are no trailing spaces.

Table 10–2 Adapter Variable Mappings for Entitlement Grant

Variable Name	Map To
AccountKey	Process Data, Process Instance
CompositeName	default/DisconnectedProvisioning!1.0
ProvisioningOperation	Grant Entitlement
OperationKey	Task Information, Task Instance Key
Service Name	manualprovisioningprocess_client
CompositeURL	http://xmlns.oracle.com/DefaultProvisioningComposite/DisconnectedProvisioning/ManualProvisioningProcess
Adapter Return Value	Response Code

Once the above configuration is done, a disconnected resource entitlement can be requested for a user with the account. This will insert the process task created in Step 4. A SOA Human Task will be assigned to the System Administrator for

granting the entitlement in the target manually. When the assignee acts on the pending human task, the provisioning call back webservice is invoked which completes or aborts the Oracle Identity Manager Operation. See [Section 10.5, "Status Changes in Manual Process Task Action"](#) for more information about changes to status based on assignee action.

10.4.2 Configuring for Entitlement Revoke

To configure entitlement revoke:

1. Go to Design Console, navigate to the Process Definition form of the disconnected resource, and click **Add Task**.
2. Add a new process task with name, ManualRevokeEntitlementStart.

Note: You must make sure:

1. that the following flags are set:
 - Conditional
 - Allow Multiple Instances
 2. to deselect the "Required for Completion" flag.
-
-

3. Navigate to the Responses tab for the same task, and add the following responses and statuses:

Response	Description	Status
Completed	Completed	C
Rejected	Rejected	R

4. Navigate to the Integration tab for the same task.
5. Click **Add** and select the Adapters radio button.
6. Select the adpMANUALENTITLEMENTPROVISIONING adapter. The adapter has seven variables.
7. Click **Save** to save the process task and close.
8. Configure the adapter variable mappings to Literal Strings as shown in [Table 10-3](#).

Note: You must make sure that there are no trailing spaces.

Table 10-3 Adapter Variable Mappings for Entitlement Revoke

Variable Name	Map To
AccountKey	Process Data, Process Instance
CompositeName	default/DisconnectedProvisioning!1.0
ProvisioningOperation	Revoke Entitlement
OperationKey	Task Information, Task Instance Key
Service Name	manualprovisioningprocess_client

Table 10–3 (Cont.) Adapter Variable Mappings for Entitlement Revoke

Variable Name	Map To
CompositeURL	http://xmlns.oracle.com/DefaultProvisioningComposite/DisconnectedProvisioning/ManualProvisioningProcess
Adapter Return Value	Response Code

Note: While performing this step, you must ensure that there are no trailing spaces.

10.5 Status Changes in Manual Process Task Action

Table 10–4 provides details about status changes based on manual task action:

Table 10–4 Manual Process Task Action Statuses

Provisioning Operation	Manual Task Action	Provisioning Action
Provision	Complete	Account status will be set to Provisioned.
Provision	Reject	Account status will not be updated.
Disable	Complete	Account status will be set to Disabled.
Disable	Reject	Account status will not be updated.
Enable	Complete	Account status will be set to Enabled.
Enable	Reject	Account status will not be updated.
Revoke	Complete	Account status will be set to Revoked.
Revoke	Reject	Account status will not be updated.
Update	Complete	No Operation
Update	Reject	No Operation
Grant Entitlement	Complete	Completes the child table insert trigger process task and sets entitlement status to Provisioned.
Grant Entitlement	Reject	Cancels the child table insert trigger process task, which deletes the child table entry.
Revoke Entitlement	Complete	Deletes the child table entry from Oracle Identity Manager.
Revoke Entitlement	Reject	No Operation

10.6 Customizing Provisioning SOA Composite

Provisioning SOA composite includes the following customizations:

- [Section 10.6.1, "Customizing Human Task Assignment via SOA Composer"](#)
- [Section 10.6.2, "Customizing by Modifying the Out of the Box Composite"](#)

10.6.1 Customizing Human Task Assignment via SOA Composer

The manual disconnected provisioning SOA composite, has a default rule, ManualProvisioningRule, which assigns the human task to the System Administrator.

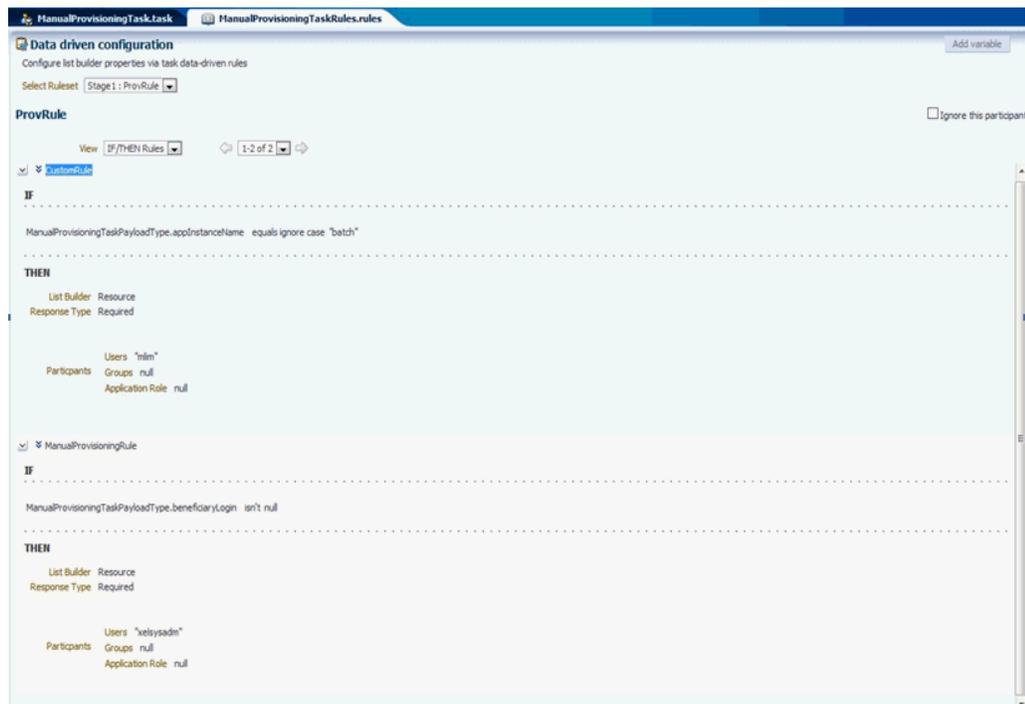
A custom rule with higher priority, based on the payload, for example Application Instance Name, can be created from the SOA Composer UI, based on which the manual task assignment can be customized.

To add a custom rule:

1. Log in to the SOA Composer UI and click **Open Task** and select `DisconnectedProvisioning_rev1.0` composite.
2. From the `ManualProvisioningTaskRules.rules` tab, click **Edit** to add a custom rule.
3. Add Rule by providing the rule name and the conditional assignment rule.
4. Using the Up arrow, move the custom rule above the `ManualProvisioningRule`.
5. Save and commit changes. [Figure 10-7](#) displays the manual provisioning rule that is added.

See Also: SOA Composer documentation for more information about creating rules

Figure 10-7 Add Manual Provisioning Rule



10.6.2 Customizing by Modifying the Out of the Box Composite

To modify the out of the box Disconnected Provisioning composite:

1. Copy the composite from `OIM_HOME/workflows/composites/DisconnectedProvisioning.zip` to a local JDeveloper working location. Unzip it in the same directory to create the `DisconnectedProvisioning` directory.
2. Open the composite in JDeveloper in Default Role.

Note: You must install the version of JDeveloper that is compatible with the Oracle Identity Manager deployment. In addition, install any patches for JDeveloper so that JDeveloper works correctly with the SOA composites.

3. As part of customization do not alter the following:
 - Payload attributes defined in `DisconnectedProvisioning\xsd\ManualProvisioningTaskPayload.xsd`
 - `ProvisioningCallbackService` partnerlink and mappings
4. Double-click **composite.xml** to open the composite and modify as per your requirements.
5. Deploy the SOA composite from Jdeveloper to Oracle SOA server. Make sure that you do not update the Revision ID and select the Overwrite any existing composites with the same revision ID option.

10.7 Troubleshooting Disconnected Resources

Table 10-5 displays the common problems that you may encounter while performing provisioning and other tasks for disconnected resources.

Table 10-5 Troubleshooting Disconnected Resources

Problem	Solution
Upon provisioning disconnected application instance, manual task is not assigned to assignee.	Perform the following steps: <ol style="list-style-type: none"> 1. Make sure that the SOA server is running. 2. Check Open tasks page for rejected process tasks, and check the error information in the task, if it exists. 3. Check Oracle Identity Manager logs to check if adapter is running. 4. Check the adapter mappings in the process task to make sure that there are no typos.
Upon manual task completion, account status is not modified.	Perform the following steps: <ol style="list-style-type: none"> 1. Make sure that the provisioning callback webservice, Provcallback is deployed. 2. Test the Webservice from the application server console.
Upon submitting catalog request for Revoke Entitlement operation, the following error is thrown: JBO-29115 Unable to construct the error message due to error:java.lang.IllegalArgumentException: can't parse argument number	Make sure that the process task with name "ManualRevokeEntitlementStart" is configured correctly as per steps mentioned in Section 10.4.2, "Configuring for Entitlement Revoke" .

Managing Lookups

This chapter describes how to manage lookups in Oracle Identity Manager by using the Form Designer in the Oracle Identity System Administration.

The Form Designer in the Oracle Identity System Administration enables you to perform the following:

- [Searching a Lookup Type](#)
- [Creating a Lookup Type](#)
- [Modifying a Lookup Type](#)

11.1 Searching a Lookup Type

To search for a lookup type:

1. Login to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **Lookups**. The Search and Select: Lookup Type window 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 Meaning field, enter the humanly readable description of the lookup value you want to search.

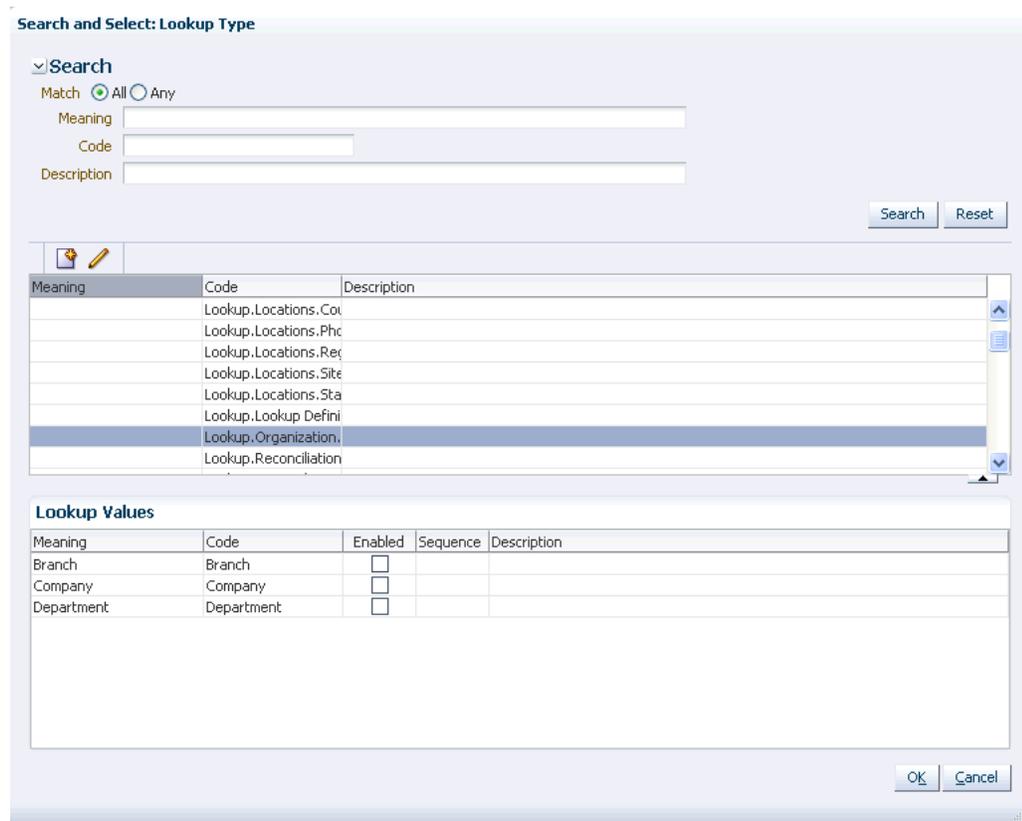
Note: Meaning is the decoded value, and Code is the encoded value. The value in the Meaning field is a humanly readable description of the field. The value in the Code field is the actual code value that is used for provisioning. For example, decoded value can be a LDAP group name, and encoded value is the LDAP group GUID.

5. In the Code value, enter the Code value of the lookup type that you want to search.

Note: To specify the search criteria, you can use the percent (%) wildcard character.

6. In the Description field, you can enter a description of the lookup type.
7. Click **Search**. The lookup types that match your search criteria are displayed in a tabular format.
8. Select a row in the search results table. The details of the selected lookup type is displayed in the Lookup Values section, as shown in [Figure 11-1](#):

Figure 11-1 The Search and Select: Lookup Type Window



9. The lookup values are enabled by default. You can deselect the checkboxes in the Enabled column for each lookup value to disable the lookup value.
10. When finished, click **OK**.

11.2 Creating a Lookup Type

To create a lookup type:

1. Open the Search and Select: Lookup Type window.
2. Click the Create Lookup Type icon on the toolbar. The Create Lookup Type dialog box is displayed, as shown in [Figure 11-2](#):

Figure 11–2 The Create Lookup Type Dialog Box

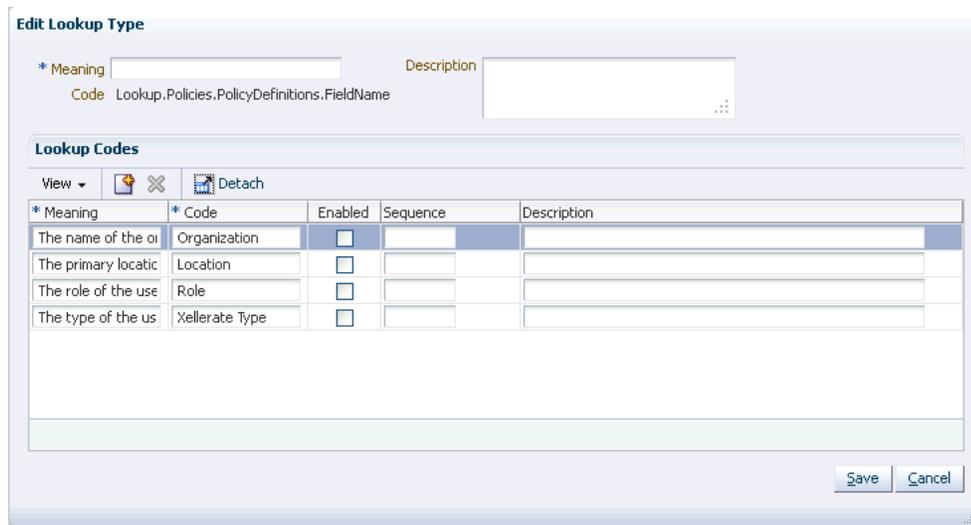
3. Enter values in the Meaning and Code fields. These are mandatory fields. For a description of the Meaning and Code fields, see step 4 in "[Searching a Lookup Type](#)" on page 11-1.
4. In the Description field, optionally enter a description of the lookup type.
5. Create one or more lookup codes for the lookup type. To do so:
 - a. In the Lookup Codes section, click the Create Lookup Code icon. A row is added to the Lookup Codes section in which you can specify values for the attributes of the lookup code.
 - b. Enter values for the Meaning, Code, and Description attributes.
 - c. Select the checkbox in the Enabled column if you want to enable the lookup code.
 - d. In the Sequence field, enter a number to specify a sequence for the lookup code. A lower number indicates higher priority. For example, 1 indicates highest priority.
 - e. Repeat steps a to d to create as many lookup codes you want. To remove a lookup code, you can select the row for the code, and click the Remove Lookup Code icon.
6. Click **Save**. The lookup type is created.

11.3 Modifying a Lookup Type

To modify a lookup type:

1. Open the Search and Select: Lookup Type window.
2. Click the Edit Lookup Type icon on the toolbar. The Edit Lookup Type dialog box is displayed, as shown in [Figure 11–3](#):

Figure 11-3 The Edit Lookup Type Dialog Box



3. To modify the values of the Meaning and Description attributes, specify values in the respective fields. The Code field is a read-only field.
4. To modify lookup codes, select a row for the lookup code, and change the attribute values.
5. Add or remove lookup values by clicking the Create Lookup Code and Remove Lookup Code icons respectively. For more information, see step 5 of "[Creating a Lookup Type](#)" on page 11-2.

Note: The Remove Lookup Code icon is enabled when you are adding or creating new lookup codes before you save the page. This icon is disabled when you save the page.

6. Click **Save**. The Lookup Type is modified.

Note: PurgeCache utility must be run after updating lookup definition, without which you must re-save lookup UDF in a sandbox before the new lookup values can be used.

See *Oracle Fusion Middleware Performance and Tuning Guide* for information about purging the cache.

Managing Connector Lifecycle

Oracle Identity Manager offers various solutions for integration with different kinds of IT-based resources in an organization. Oracle Identity Manager connectors are the recommended solution for integration between Oracle Identity Manager and resources that store and use user data. A connector enables exchange of user data between Oracle Identity Manager and a specific resource or target system.

Oracle Identity Manager server uses connectors to perform operations on target systems. Oracle provides connectors for common enterprise resources. You can develop custom connectors for your own resources.

A connector consists of the following artifacts:

- Binaries (JAR and DLL files) that contain the connector code
- XML file(s) consisting of data of Objects defined in Oracle Identity Manager, such as an IT resource, resource object, provisioning process and process tasks, process form and child forms, adapters and adapter tasks, lookup definitions, reconciliation rules, and scheduled tasks
- Integration libraries that enable adapters to perform actions on the target system

For some target systems, third-party integration libraries might be required to enable communication or specific functionality with the target systems.

See Also: *Oracle Identity Manager Connector Concepts* for detailed conceptual information about connectors and connector objects

This chapter provides information about Connector Lifecycle Management (LCM) features. It is divided into the following sections:

- [Lifecycle of a Connector](#)
- [Connector Lifecycle and Change Management Terminology](#)
- [Viewing Connector Details](#)
- [Installing Connectors](#)
- [Defining Connectors](#)
- [Cloning Connectors](#)
- [Exporting Connector Object Definitions in Connector XML Format](#)
- [Upgrading Connectors](#)
- [Uninstalling Connectors](#)

- [Troubleshooting Connector Management Issues](#)

12.1 Lifecycle of a Connector

The following are stages in the lifecycle of a connector:

Deployment

A connector can be installed by clicking the **Manage Connector** menu on the Advanced Administration section of the Oracle Identity System Administration.

To complete the deployment procedure, you might also need to copy connector files and external code files to destination directories on Oracle Identity Manager and target system host computers. Some connectors require a Remote Manager, which is usually installed on the target system host computer. Some other connectors, specifically the identity connectors, require the local and remote connector server.

Oracle Identity Manager 11.1.1.5.x provide Connector LCM as a new feature to manage connectors and uses Connector Installer (CI) for installing connector.

Installing a connector using Connector Installer is not the same as doing it using Deployment Manager. Although the Deployment Manager offers an alternative approach to import definitions of the objects that constitute a connector, the connector imported using Connector LCM can be managed better as Connector LCM offers a more broader and richer feature than Deployment Manager. Therefore, the Install Connectors feature is the recommended approach for Oracle Identity Manager 11g based connector installation and/or management.

See Also:

- Oracle Identity Manager Connector documentation for information about copying connector files and external code files to destination directories on Oracle Identity Manager and target system host computers. Connector documentation is available on the Oracle Web site at the following URL:

http://download.oracle.com/docs/cd/E22999_01/index.htm

- "Identity Connector Framework" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about the Identity Connector Framework and how to use it to create an identity connector.

Customization

After deployment, you might customize a connector to meet business requirements that are not addressed by the default configuration of the connector. For example, you might add new attributes for reconciliation and provisioning with the target system. An enhancement of this type requires changes to be made in multiple connector objects, such as Resource Object, Process Definition, and Process Form. See Connector Documentation for detailed information about changes required in connector objects.

Cloning

You might have more than one installation of a target system. If you have a target system with multiple instances, and data is either same or shared or replicated, such as in Microsoft Exchange or Active Directory connectors, then you do not need to clone

the connector. You need to create multiple IT resources for the instances. The target works as a single resource object.

If you have a target system with different installations or schema or data, such as a LDAP server for internal users and another LDAP server for external, contractors, and consumers, then you need to clone the connector. The connectors will work as two separate targets.

There might be a scenario where the connector attributes are different. Then instead of creating a new connector, the existing connector can be cloned by using the XML of the original connector. The **Clone Connectors feature** of the Advanced Administration enables you to automatically generate copies of a set of connector objects.

Upgrade

To make use of new features introduced in later releases of a connector, you might upgrade a connector by applying patch sets released by Oracle. Typically, upgrading to a new release of a connector involves processes that range from simple changes (such as a JAR file upgrade) to changes that affect most of the adapter tasks that were shipped as part of the connector. You can use the **Upgrade Connectors feature** to upgrade a connector.

Note: Upgrading connectors preserve the existing customizations in a connector.

Uninstalling

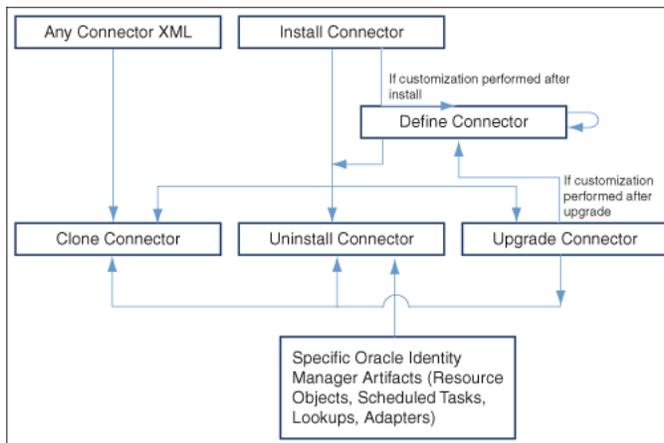
Note: Uninstalling a connector is performed in the development environment and not in production environment.

If you stop using a connector, then this action is also provided to additional environments, such as System Integration Testing, User Acceptance Testing, and Staging, where that connector is also stopped.

The need to keep a clean development environment that does not have any unnecessary Oracle Identity Manager objects, you would like to uninstall a particular connector version that you no longer need to use. The **Uninstall Connectors utility** enables you to uninstall connectors as well as individual connector objects.

Note: You must have the System Administrator role to perform connector lifecycle management tasks, such as installing connectors including importing connector XML files by using the Deployment Manager, and cloning, defining, upgrading, and uninstalling connectors.

Figure 12-1 depicts the connector lifecycle:

Figure 12–1 Connector Lifecycle

12.2 Connector Lifecycle and Change Management Terminology

The following terms have been introduced in this chapter:

- **Oracle-released connector** refers to a connector released by Oracle.
- **Custom release** or **custom connector** refers to connectors that you develop as well as Oracle-released connectors that you customize or reconfigure in any way.
- **Source release** or **source connector** refers to the existing release of the connector that you want to upgrade to a different (that is, new) release. For example, if you want to upgrade the SAP User Management connector from release 9.1.2 to release 9.1.2.1, then release 9.1.2 is the source release.
- **Target release** or **target connector** is the release to which you want to upgrade the source release. In the preceding example, SAP User Management release 9.1.2.1 is the target release.

Note: Some of the preceding terms can be combined to provide a shortened description of the type of connector that is under discussion. For example, a **custom source release** is a connector that you had created, customized, or reconfigured and now want to upgrade to a target release.

- A **configuration XML file** contains information that is used during connector installation by the Install Connectors feature. For a connector released by Oracle, the configuration XML file is included in the deployment package. For a custom-developed connector, you might want to develop the individual connector objects on the staging (test) server and then deploy the connector on the production server. In this case, you can create a configuration XML file for the connector if you want to install the connector on the production server by using the Install Connectors feature.

See Also: ["Installing Connectors"](#) on page 12-6 for information about the Install Connectors feature.

- A **connector XML file** contains definitions of the individual objects that constitute a connector. When the XML file is imported into Oracle Identity Manager through the Deployment Manager, these objects definitions are used to create the connector

objects in the Oracle Identity Manager database. The manner in which the XML file is imported into Oracle Identity Manager depends on the type of connector:

- For an Oracle-released connector that is compatible with the Install Connectors feature, the connector XML file is automatically imported when you use the Install Connectors feature. This feature implicitly calls the Deployment Manager to import the connector XML file.
- For an Oracle-released connector that is not compatible with the Install Connectors feature, you use the Deployment Manager to import the XML file.
- For a custom connector, you can use the Deployment Manager to first export definitions of objects that you had created on the staging server. The output of this process is the connector XML file. You can then import the file into the production server. Alternatively, if you create a complete deployment package (including the configuration XML file) for the connector, then you can use the Install Connectors feature to install the connector. This feature implicitly calls the Deployment Manager to import the file.

See Also: ["Exporting Connector Object Definitions in Connector XML Format"](#) on page 12-35 for information about exporting connector object definitions by using the Deployment Manager

12.3 Viewing Connector Details

To view the details of a connector:

Note: In this release of Oracle Identity Manager, the connector lifecycle management functionality have been introduced such as defining, cloning, upgrading, and uninstalling connectors. For all these features, complete connector DM-XML is required in the database, and this is the source for all the connector lifecycle management activities.

When Oracle Identity Manager is upgraded from earlier releases, such as Release 9.1.x or 11g Release 1 (11.1.1.5), to 11g Release 2 (11.1.2.1.0), you must define the connector so that all the lifecycle management operations on the connector are possible to perform. Without defining the connector, it is not possible to search for the installed connector, upgrade the installed connector, clone the connector, and uninstall the connector. See ["Defining Connectors"](#) on page 12-13 for information about defining connectors.

1. Login to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Manage Connector**.
3. In the **Connector Name** field, enter the name of the connector and then click **Search**.
4. The search results show the details of the connector.

If you do not know the full name of the connector, then you can perform a wildcard search for a connector. For example, if you want to display details of the Microsoft Active Directory connector installed in your operating environment, then you can use "Direct" as the search string.

If you want to display details of all installed connectors, then leave the Connector Name field blank and click Search.

Figure 12–2 shows the search results table.

Figure 12–2 Search Results Table Showing Details of Connectors

The screenshot shows the 'Connector Management' interface. At the top, there are buttons for 'Define', 'Install', and 'Clone'. Below that is a search bar with a 'Search' button and a 'Clear' button. The search results are displayed in a table with the following data:

Connector Name	Connector Version	Status	Installation Date	Export	Export Silent	Upgrade XML	Upgrade	Clone
IBM Lotus Notes Domino	9.0.4.12.0	Active	February 2, 2011 5:08:50 AM	[Export Icon]	[Export Silent Icon]	[Upgrade XML Icon]	[Upgrade Icon]	[Clone Icon]
Oracle Internet Directory	9.0.4.5	Active	February 2, 2011 5:06:19 AM	[Export Icon]	[Export Silent Icon]	[Upgrade XML Icon]	[Upgrade Icon]	[Clone Icon]
ActiveDirectory	9.1.1.4	Active	February 1, 2011 10:09:57 PM	[Export Icon]	[Export Silent Icon]	[Upgrade XML Icon]	[Upgrade Icon]	[Clone Icon]

The search results table displays the connector name, release number, status, and the date and time at which the connector was installed. The remaining columns of the table provide icons that you can use to begin any of the lifecycle management operations on a connector.

12.4 Installing Connectors

The following sections describe this feature and the procedure to use it:

Note: To determine whether you can install an Oracle-released connector by using the Install Connectors feature, see the connector guide.

- [Overview of the Connector Deployment Process](#)
- [Creating the User Account for Installing Connectors](#)
- [Installing a Connector](#)

12.4.1 Overview of the Connector Deployment Process

To install a connector, you perform some or all of the following tasks:

1. Verify the installation requirements.
2. Configure the target system.
3. Copy the connector files and external code files to directories on the Oracle Identity Manager server.

4. Configure Oracle Identity Manager.
5. Import the connector XML files.
6. Configure reconciliation.
7. Configure provisioning.
8. Configure Secure Sockets Layer (SSL).

Of these tasks, the Install Connectors feature automatically performs the following:

Note: You manually perform the remaining tasks. Connector documentation provides instructions.

- Copying the connector files and external code files to directories on the Oracle Identity Manager server
- Importing the connector XML files
- Compiling adapters (which is part of the procedure to configure provisioning)

At the end of a successful installation, an entry is created in a table in the Oracle Identity Manager database that stores data about installed connectors. "[Defining Connectors](#)" on page 12-13 describes the data that is stored in the database.

12.4.2 Creating the User Account for Installing Connectors

Users belonging to the SYSTEM ADMINISTRATORS group of Oracle Identity Manager can install connectors. Alternatively, members of a group to which you assign the required menu items and permissions can install connectors.

See Also: The "Creating and Managing User Groups" section in the connector guide for information about creating groups and assigning menu items and permissions to them.

The required permissions are the following:

- Form Designer (Allow Insert, Write Access, Delete Access)
- Structure Utility.Additional Column (Allow Insert, Write Access, Delete Access)
- Meta-Table Hierarchy (Allow Insert, Write Access, Delete Access)
- User Should belong to SYSTEM ADMINISTRATORS group.

The required menu item is Deployment Management Install Connector.

To install a connector, if you want to use a user account that does not belong to the SYSTEM ADMINISTRATORS group, then you must apply these permissions and menu item to one of the groups to which the user account belongs.

12.4.3 Installing a Connector

Note:

- From this release onward, re-installing a connector is not supported. You cannot install a connector version which had already been installed in Oracle Identity Manager. However, if the installation process is not successful, Oracle Identity Manager allows you to reinstall the connector.
 - Before installing a connector, create a backup of your environment. This is because, if the installation fails, then the connector cannot be uninstalled. There is no solution for reverting the environment to the previous state or finalizing the connector install.
-
-

To install a connector:

1. Log in to Oracle Identity System Administration by using the user account described in ["Creating the User Account for Installing Connectors"](#) on page 12-7.
2. In the left pane, under System Management, click **Manage Connector**.
3. Click **Install** in the top-right corner of the page.
4. From the **Connector List** list, select the connector that you want to install. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

OIM_HOME/server/ConnectorDefaultDirectory

If you have copied the installation files into a different directory, then:

- a. In the **Alternative Directory** field, enter the full path and name of that directory.
- b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
- c. From the **Connector List** list, select the connector that you want to install.

[Figure 12-3](#) shows the Select Connector to Install page of the Install Connector wizard:

Figure 12–3 The Select Connector to Install Page

The screenshot shows a web-based wizard titled "Install Connector" with a progress indicator showing step 1 of 2. The main heading is "Step 1: Select Connector to Install". Below this, there is a brief instruction: "Select the connector that you want to install, and then click Load. You can specify an alternative directory location for the connector media, and then click Refresh." A note indicates that an asterisk (*) denotes a required field. The "Connector List" is a dropdown menu with a "Select" button to its right. The dropdown menu is open, showing the following options: "Select", "Select", "Oracle Internet Directory 9.0.4.5", "ActiveDirectory 9.1.1.4", "ActiveDirectory 9.1.1.5", and "IBM Lotus Notes Domino 9.0.4.12.0". To the right of the dropdown are "Load" and "Refresh" buttons. Below the dropdown is an "Alternative Directory" text input field. At the bottom of the form are "Cancel" and "Continue >>" buttons.

5. Click **Load**.

The following information is displayed:

- Connector installation history

The connector installation history is information about previously installed releases of the same connector.

- Connector dependency details

There are some connectors that require the installation of some other connectors before you can start using them. For example, before you use the Novell GroupWise connector, you must install the Novell eDirectory connector. Novell eDirectory is called the **dependency connector** for Novell GroupWise.

The connector dependency details include the list of connectors that must be installed before you can install and use the selected connector. These details also include information about any dependency connectors that are already installed, and whether or not any of the installed dependency connectors must be upgraded. However, after showing the dependency information, the Install Connector wizard allows you to install the connector.

You must ensure that the correct versions of dependency connectors are installed after you complete the current installation.

Figure 12–4 shows the page with connector history details and connector dependency details:

Figure 12–4 Connector History and Dependency

Install Connector 1 2

Step 1: Select Connector to Install

Select the connector that you want to install, and then click Load. You can specify an alternative directory location for the connector media, and then click Refresh.

* Indicates required field

Connector List * Oracle Internet Directory 9.0.4.5 Load

Alternative Directory Refresh

Connector History Details

The Oracle Internet Directory 9.0.4.5 connector has no history of prior installations.

Connector Dependency Details

The Oracle Internet Directory 9.0.4.5 connector has no dependencies on other connectors.

Cancel Continue >>

6. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

- a. Configuration of connector libraries
- b. Import of the connector XML files (by using the Deployment Manager)
- c. Compilation of adapters

Figure 12–5 shows the Connector Installation page of the Install Connector wizard:

Figure 12–5 The Connector Installation Page

Install Connector 1 2

Step 2: Connector Installation

Oracle Internet Directory 9.0.4.5 Installation Status : **Successful**

- ✓ Configuration of Connector Libraries
- ✓ Import of Connector XML Files (Using Deployment Manager)
- ✓ Compilation of Adapter Definitions

Perform the following steps before you start using this connector.

1. Ensure that the [Prerequisites](#) are addressed.
2. Go to Advanced >> Configuration >> [Create IT Resource](#) and create an IT resource for this connector.
3. Go to Advanced >> System Management >> Search Scheduled Job and configure the following scheduled Jobs that are already created for this connector.

Exit

On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

- Fix the cause of the error, and then retry installation by clicking **Retry**.

- Cancel the installation and begin again from step 1 of the installation procedure.

One of the reasons for installation failure could be a mismatch between information about files and directory paths in the configuration XML file and the actual files and directory paths. If this happens, then an error message is displayed.

For example, suppose the actual name of the JAR file for reconciliation is `recon.jar`. If the name is provided as `recon1.jar` in the configuration XML file, then an error message is displayed.

If such an error message is displayed, then perform *one* of the following steps:

- Make the change in the configuration XML file, and then retry installation from the Step 1: Select Connector to Install page onward.

In the example described earlier, change the name of the JAR file to `recon.jar` in the configuration XML file, and then retry installation from the Step 1: Select Connector to Install page onward.

- Make the change in the actual name or path of the file or directory, and then use the Retry option.

In the example described earlier, change the name of the JAR file to `recon1.jar` and then click the **Retry** button.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:
 - a. Ensuring that the prerequisites for using the connector are addressed

Note: There are no prerequisites for some connectors.

- b. Creating an IT resource for the connector

Most of the connectors are shipped with a default IT resource. You can use either the default IT resource or create a new one. To create a new IT resource, go to System Administration, under Configuration, click **IT Resource**. The Manage IT Resource page opens. On this page, click **Create IT Resource**.

- c. Configuring the scheduled tasks that are created when you installed the connector.

To configure scheduled task, go to System Administration, under System Management, click **Scheduler** and search for required scheduled job.

12.4.4 Post Installation Steps

To perform post installation configuration:

1. Create or update IT resource with appropriate values using steps defined in 7-b.
2. Creating a Sandbox. To do so:

See Also: "Managing Sandboxes" section in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for complete information on Sandboxes

- a. Navigate to System Administration and on the top right hand corner, click **Sandboxes**.
 - b. In the Manage Sandboxes tab, click **Create Sandbox**.
 - c. In the Create Sandbox dialog box, enter a sandbox name and description, click **Save and Close**. Click **Ok** in the confirmation dialog box.
 - d. Select the newly created (Active) Sandbox.
3. Creating a new UI form. To do so:
- See Also:** see [Chapter 7, "Managing Forms."](#) for complete information about forms.
- a. In the System Administration page, under Configuration, click **Form Designer**.
 - b. Under Search Results, click **Create**.
 - c. Select the resource type for which form needs to be created.
 - d. Enter a form name and click **Create**.
4. Creating an Application Instance. To do so:
- See Also:** see [Chapter 9, "Managing Application Instances."](#) for complete information about Application Instances.
- a. In the System Administration page, under Configuration, click **Application Instances**.
 - b. Under Search Results, click **Create**.
 - c. Enter appropriate values for fields displayed on the Attributes form and click **Save**.
 - d. In the Form dropdown, select the newly created form and click **Apply**.
 - e. Publish the application instance. See [Section 9.2.3.2, "Managing Organizations Associated With Application Instances."](#) for more information about publishing an application instance for a particular organization.
5. Publish the Sandbox:
- a. In the Manage Sandboxes tab, which is open, select the sandbox.
 - b. Click **Publish Sandbox**.
 - c. Click **Yes** in the confirmation dialog box.
6. Entitlement Harvesting and Catalog Sync:
- a. In the System Administration page, under System Management, click **Scheduler**.
 - b. Run connector lookup reconciliation scheduled jobs.
 - c. Run Entitlement List scheduled job.
 - d. Run Catalog Synchronization Job scheduled job.

12.5 Defining Connectors

Connector LCM operations such as Upgrade, Clone, and Uninstall needs a source for each connector where all the connector objects reside. The Connector Install stores the Deployment Manager (DM) XML in Oracle Identity Manager database.

Typically, you will install the shipped connector and then perform one or both of the following operations:

- Customize the connector by, for example, add/ modify existing object definitions, add additional adapters
- (Re) Configure the connector by, for example, changing attribute names and key fields

The DM XML in Oracle Identity Manager database, which will be the reference for all Connector LCM operations need to be updated for customization changes. Oracle Identity Manager provides **Define** feature to update the DM XML stored in Oracle Identity Manager database with customization changes. Define feature is similar to Export where user need to add all the connector objects related to a specific connector. The end result of defining a connector is an XML file, which will be updated in Oracle Identity Manager database.

At this point, the customized or re-configured connector is not the same as the Oracle-released connector. The connector XML file for the Oracle-released connector might not be valid for the customized or re-configured connector.

In the Advanced Administration page of the Oracle Identity System Administration, you can **define** a customized or re-configured connector. Defining a connector is equivalent to registering the connector with Oracle Identity Manager.

Note: You must add only those Oracle Identity Manager artifacts that are specific to the connector and do not add default objects or any other connector objects that are shared across connectors. The defined XML is the source for life cycle operations such as upgrade, clone, and uninstall. If an object is used in define and is shared across connectors or a default Oracle Identity Manager object, then there will be un-intended behavior. For example, a Lookup Definition which is there by default in Oracle Identity Manager is added as a part of define, then clone operation will create another copy of the object, which is not required. The uninstall will delete this default object from Oracle Identity Manager as it is defined specific to a connector. Such incorrect definition will have impact on Oracle Identity Manager functionality. Therefore, you must be careful while adding an object while defining a connector.

When you define a connector, a record representing the connector is created in the Oracle Identity Manager database. If this record already exists, then it updates:

- The name of the connector. For example, `Microsoft Active Directory`.
- The release number of the connector. For example, `9.1.1`.
- The connector XML definitions.

Note:

- You can define the connector XML definitions in the form of an XML file. See the "Exporting Connector Object Definitions in Connector XML Format" section of the connector guide for more information. You can then use this connector XML file to build the installation package for installing the connector on a different Oracle Identity Manager installation.
 - Oracle recommends defining a connector immediately after customizing the connector or updating the DM XML file with the customization changes.
-

A connector is automatically defined when you install it using the Install Connectors feature or when you upgrade it using the Upgrade Connectors feature. Therefore, if you install a connector and want to clone it without customizing the connector, then there is no need to define the connector.

You must manually define a connector, otherwise newer version (which basically pertains to entry in CIH table) of connector may not be reflected even though import of new XML was successfully completed. Perform this procedure only if:

- You import the connector by using the Deployment Manager.
- You customize or reconfigure the connector.

Note: You can continue to use a connector without defining it after you customize or reconfigure a connector or after you upgrade Oracle Identity Manager. However, if you want to upgrade, clone, or uninstall the connector, then you must first define it.

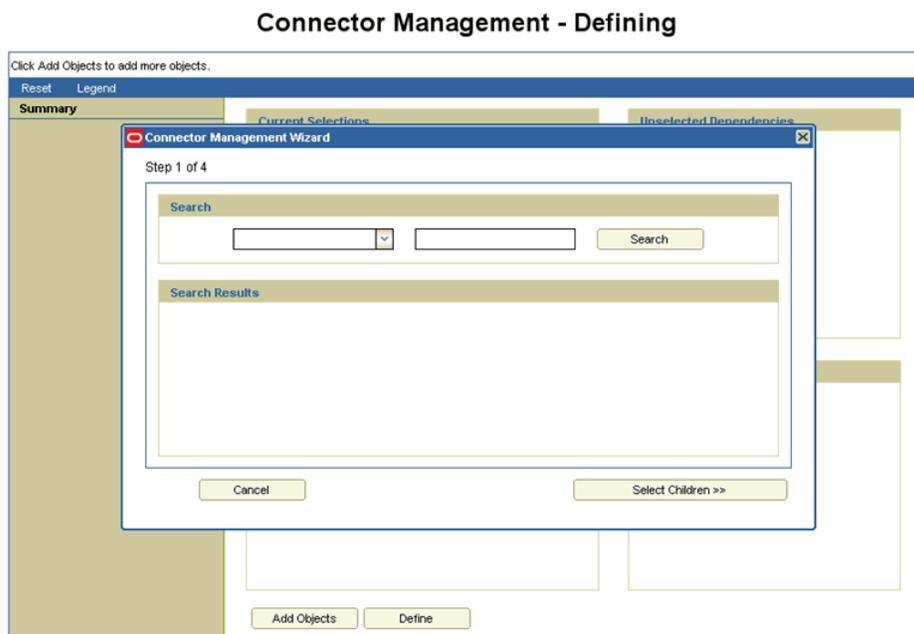
- You upgrade Oracle Identity Manager.
- It is a custom connector that you develop.

To define a connector:

Note: To determine whether you can define a particular release of a connector by using the Oracle Identity System Administration, see the documentation for that release of the connector.

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Manage Connector**.
3. On the Connector Management window, click **Define**. The Connector Management Wizard is displayed, as shown in [Figure 12-6](#):

Figure 12–6 Connector Management Wizard for Defining Connectors



4. On the first page of the wizard, select either **Resource** or **Process** from the Search list. In the adjoining field, you can enter a search string and the asterisk (*) as a wildcard character to refine your search for resource objects or process definitions belonging to the connector. Then, click **Search**.

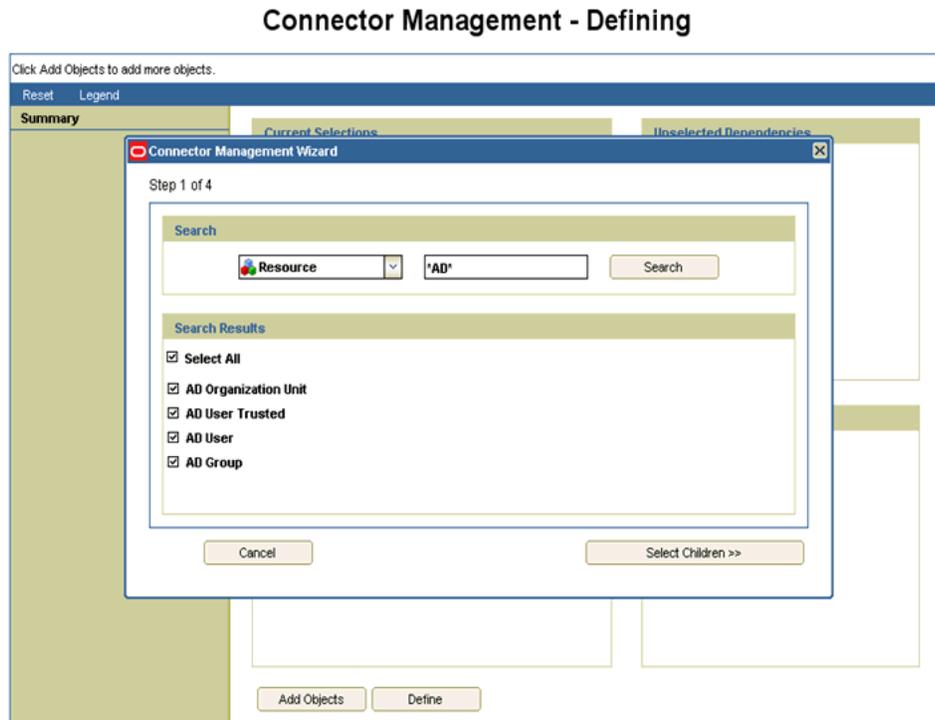
Most of the objects that constitute a connector are linked to the resource objects and process definition of the connector. By selecting the resource objects or process definition, you automatically select the objects linked with them. Some of the connector objects, for example, scheduled task, do not have dependency with the resource object. Ensure that you search all the attributes and add them while defining.

When you click Search, the list of resource objects or process definitions that meet the specified search criteria are displayed.

5. Select the check boxes for the resource objects or process definitions that are part of the connector.

Figure 12–7 shows step 1 of the Connector Management Wizard with search results for connector objects:

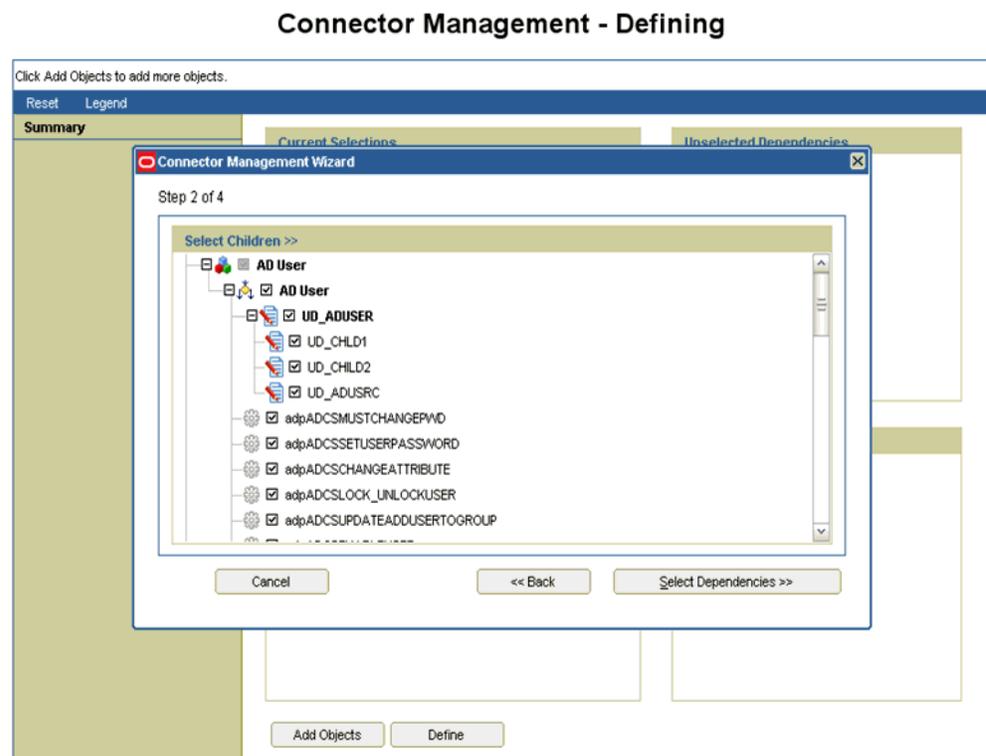
Figure 12–7 Step 1 of the Connector Management Wizard



6. Click **Select Children**.
7. From the list of connector objects displayed, ensure that all the objects belonging to the connector are selected. Then, click **Select Dependencies**.

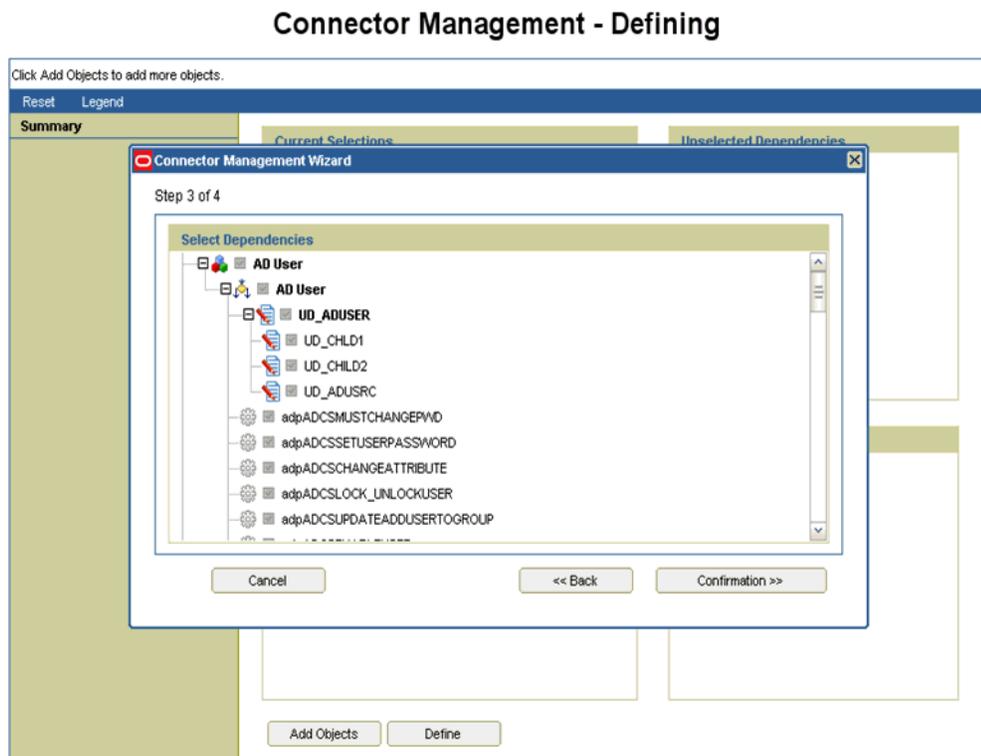
Note: For an Oracle-released connector, the adapters that are part of the connector are listed in the connector guide. Select the check boxes for those adapters.

Figure 12–8 shows step 2 of the Connector Management Wizard:

Figure 12–8 Step 2 of the Connector Management Wizard

8. After you review the list of objects that you have selected, click **Confirmation**. [Figure 12–9](#) shows step 3 of the Connector Management Wizard with the list of selected connector objects:

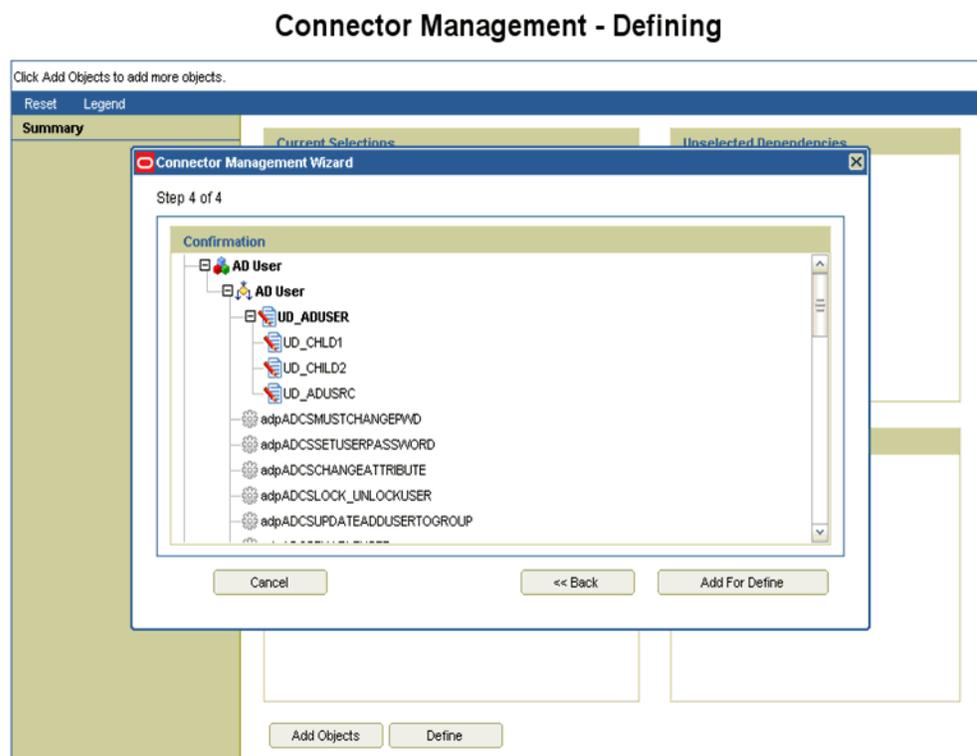
Figure 12–9 Step 3 of the Connector Management Wizard



9. Click **Add For Define**.

Figure 12–10 shows step 4 of the Connector Management Wizard:

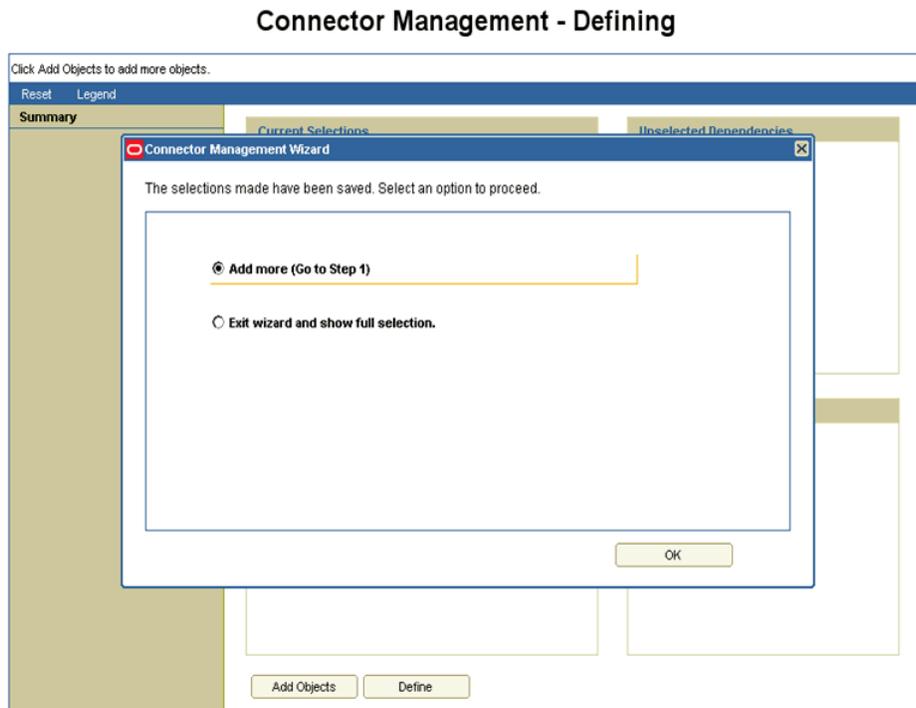
Figure 12–10 Step 4 of the Connector Management Wizard



10. To proceed, select any one of the following options, and click OK:

- **Add more (Go to Step 1):** Select this option if you want to go to step 1 of the Connector Management Wizard and select more connector objects.
- **Exit wizard and show full selection:** Select this option if you want to exit the Connector Management Wizard and display the complete list of selected connector objects.

Figure 12–11 shows the page with the options to add more connector objects or to exit the wizard:

Figure 12–11 Options to Select More Objects or Exit

11. On the page that is displayed, only objects shown in the Current Selections list are included in the connector definition. You can drag objects across lists. For example, you can drag an adapter from the Current Selections list to the Unselected Children list. After you make the required changes, click **Define**.

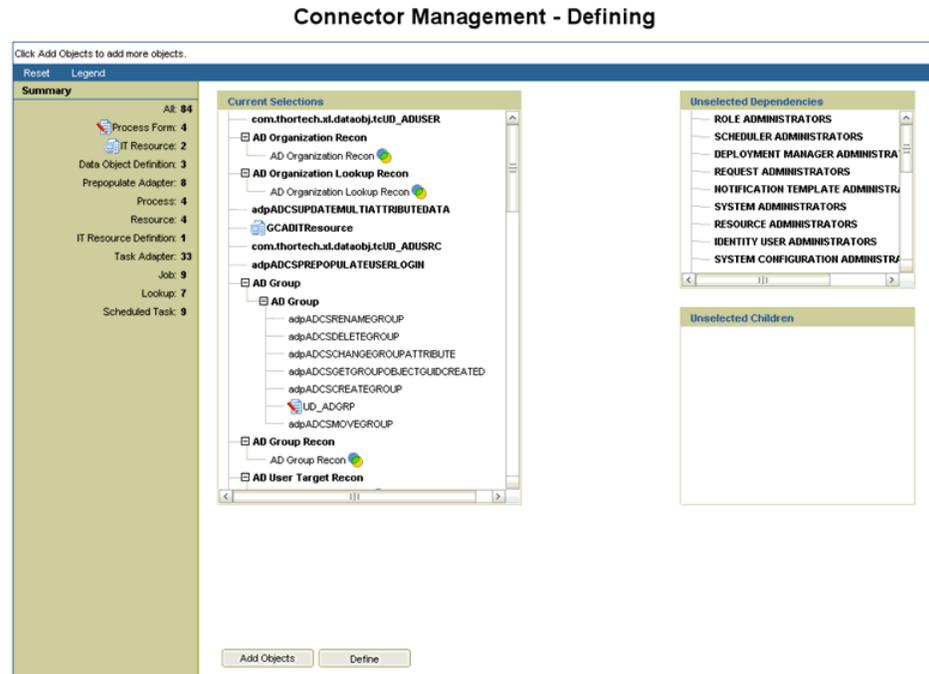
Note: Make sure that you have added all the Oracle Identity Manager connector objects specific to defining connector. If you do not have a specific connector object while defining the connector, then upgrade, clone, or uninstall may not handle the undefined object.

The following are Oracle Identity Manager artifacts that are generally associated with almost all the connectors:

- Resource objects
 - Event handlers
 - Process forms
 - IT resources
 - Data object definitions
 - Prepopulate adapters
 - Processes
 - IT resource type definitions
 - Task adapters
 - Lookups
 - Scheduled tasks
-

Figure 12–12 shows the page with the complete list of selected connector objects that are to be included in the connector definition and the unselected connector dependencies:

Figure 12–12 Selected Connector Objects

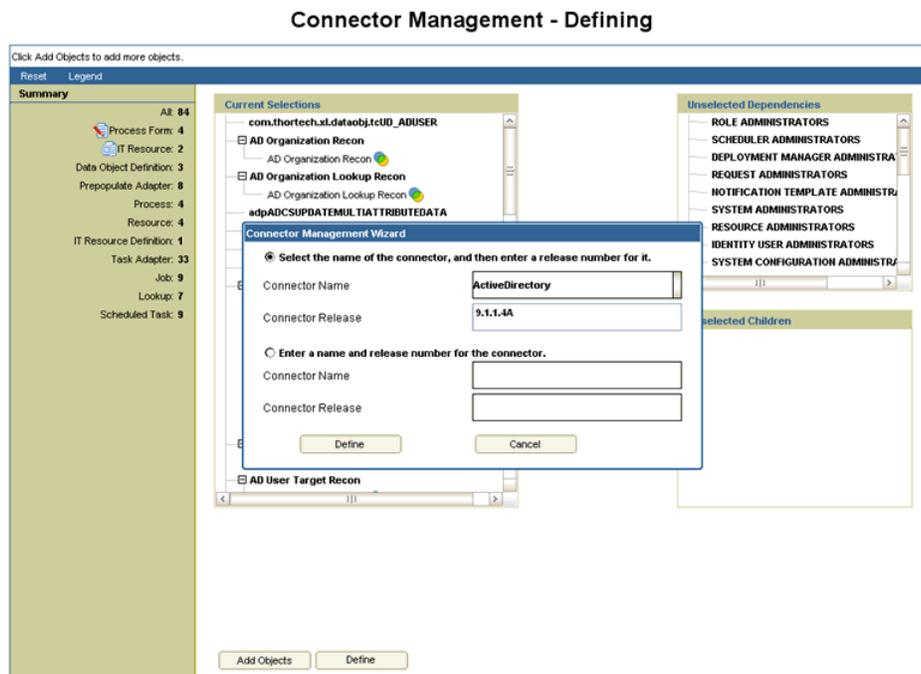


12. In the dialog box that is displayed, select one of the following options:

- **Select the name of the connector, and then enter a release number for it:** Select this option if an earlier release of this connector already exists on this Oracle Identity Manager installation. In addition, select a connector name and enter a release number.
- **Enter a name and release number of the connector:** Select this option if an earlier release of this connector does not exist on this Oracle Identity Manager installation. In addition, enter a connector name and release number.

Figure 12–13 shows the dialog box to specify the connector name and release number:

Figure 12–13 Connector Name and Release Number



13. Click **Define**.

14. At the end of the process, a message stating that the operation was successful is displayed. Click **Close**.

12.6 Cloning Connectors

Note: In this guide, the term **Clone Connectors feature** refers to the set of Oracle Identity Self Service pages that you can use to clone connectors.

This section describes the procedure to create a copy of a connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

Note: Oracle Identity Manager offers a different feature for using a single connector to integrate:

- Multiple installations of a particular target system with Oracle Identity Manager
- A target system that stores data about multiple user types (for example, employee and contractor) and requires Oracle Identity Manager to provide a different resource object for each user type

See the connector guide for information about how to use access policies to create resource objects for different user types on a particular target system.

This section contains the following topics:

- [Guidelines for Cloning a Connector](#)
- [Cloning a Connector](#)
- [Postcloning Steps](#)

12.6.1 Guidelines for Cloning a Connector

Apply the following guidelines while using the Clone Connectors feature:

- The Clone Connectors feature does not support request dataset cloning. This is because request dataset definitions are not usually included in the connector XML file. Cloned copy of the connector is needed when there is a change in attributes of the same target but for different instances. If attributes are different, then the same request dataset cannot be used.
- A connector must be compatible with the Clone Connectors feature before you can use the utility to create a clone of the connector. For an Oracle-released connector, see the connector guide for information about whether or not the connector is supported by the Clone Connectors feature.
- Validation performed on the names of connector objects does not cover the names of objects that belong to other connectors. However, when you import the connector XML file that is created by the Clone Connectors feature, the Deployment Manager throws an error when it encounters duplicate object names. This is illustrated by the following example:

AD_USER is the name of a resource object belonging to the Microsoft Active Directory connector. Suppose My_RO is the name of an existing resource object defined in the Oracle Identity Manager database. If the new name that you specify for the AD_USER resource object is My_RO, then the Clone Connectors feature does not display an error message stating that a resource object with the specified name already exists.

12.6.2 Cloning a Connector

Cloning a connector involves performing a two-step procedure:

- [Step 1: Create the connector XML file for the cloned connector](#)
- [Step 2: Install the clone connector](#)

Step 1: Create the connector XML file for the cloned connector

To create the connector XML file for the cloned connector:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Manage Connector**.
3. The next step depends on the source XML that you want to use to create the clone:
 - If you want to use a connector XML file as the source, then:
 - a. Click **Clone** in the upper-right corner.
 - b. On the Step 1: XML Selection from File System page, use the Browse option to navigate to and select the connector XML file.

[Figure 12–14](#) shows the XML Selection from File System page of the Connector Management - Cloning wizard:

Figure 12–14 The XML Selection from File System Page

The screenshot shows a web-based wizard interface titled "Connector Management - Cloning". At the top right, there is a progress indicator with 12 numbered steps, where step 1 is highlighted. Below the title, the current step is "Step 1: Select Connector XML for the Cloning Operation". The main content area contains the instruction: "Provide the path to the connector XML file that you want to use for the cloning operation." Below this, there is a note: "* Indicates Required Field". The form includes a text input field labeled "Connector XML File for Cloning" with a "Browse..." button to its right. At the bottom left of the form, there are two buttons: "Cancel" and "Continue >>".

- c. Click **Continue**.
- If you want to use the connector XML that was stored in the database when the connector was defined, then:
 - a. Use the Search feature to search for the connector. [Figure 12–15](#) shows the page to search for the connector:

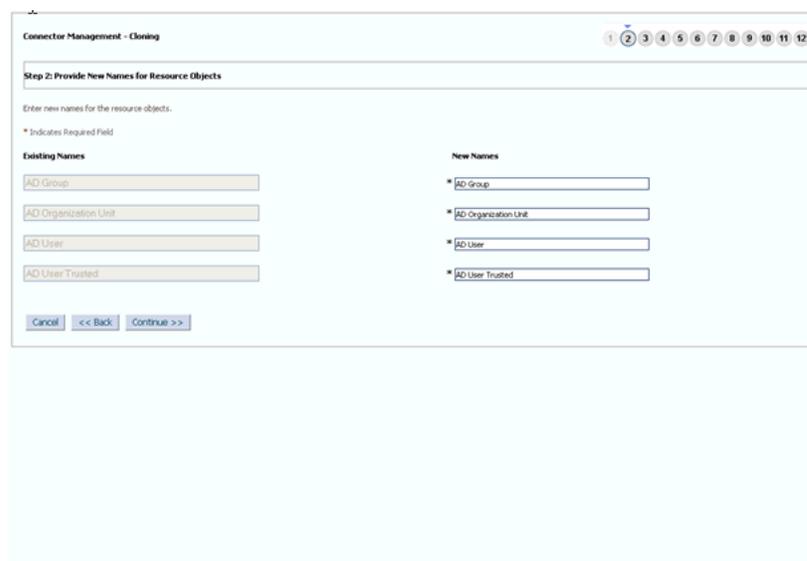
Figure 12–15 Searching the Connector

- b. In the search results that are displayed, click the Clone icon in the row for the connector that you want to clone.
4. On the Step 2: Provide New Names for ROs page, enter new names for the resource objects of the clone.

If the connector has multiple resource objects, then the new name that you specify for each resource object must be different from the names of all the existing resource objects of that connector.

Click **Continue** after you specify new names for all the resource objects.

[Figure 12–16](#) shows the Provide New Names for Resource Objects page of the Connector Management - Cloning wizard:

Figure 12–16 The Provide New Names for Resource Objects Page

5. On the Step 3: Provide New Names for Process Definitions page, enter new names for the process definitions of the clone.

If the connector has multiple process definitions, then the new name that you specify for each process definition must be different from the names of all the existing process definitions of that connector.

Click **Continue** after you specify new names for all the process definitions.

[Figure 12–17](#) shows the Provide New Names for Process Definitions page of the Connector Management - Cloning wizard:

Figure 12–17 The Provide New Names for Process Definitions Page

- On the Step 4: Provide New Names for Process Forms page, enter new names for the process forms of the clone.

If the connector has multiple process forms, then the new name that you specify for each process form must be different from the names of all the existing process forms of that connector.

Click **Continue** after you specify new names for all the process forms.

Figure 12–18 shows the Provide New Names for Process Forms page of the Connector Management - Cloning wizard:

Figure 12–18 The Provide New Names for Process Forms Page

- On the Step 5: Provide New Names for IT Resource Type Definitions page, enter new names for the IT resource type definitions of the clone.

If the connector has multiple IT resource type definitions, then the new name that you specify for each IT resource type definition must be different from the names of all the existing IT resource type definitions of that connector.

Click **Continue** after you specify new names for all the IT resource type definitions.

[Figure 12–19](#) shows the Provide New Names for IT Resource Type Definitions page of the Connector Management - Cloning wizard:

Figure 12–19 The Provide New Names for IT Resource Type Definitions Page

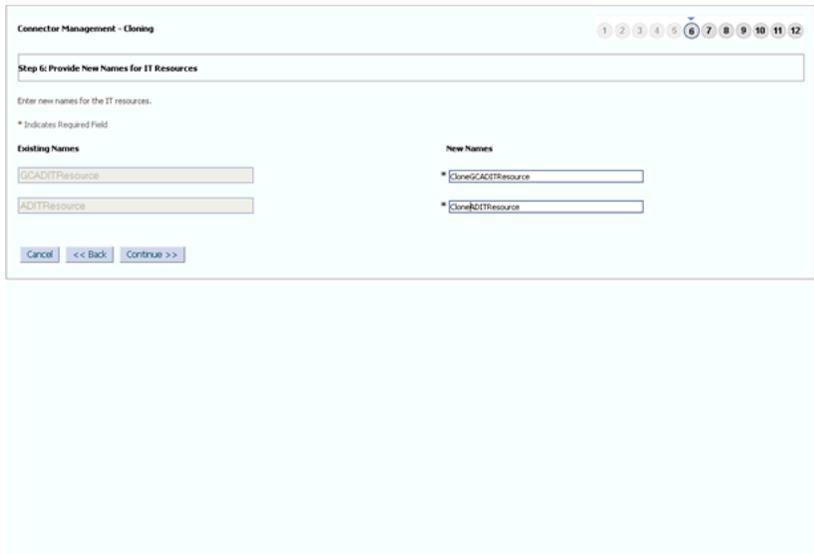
8. On the Step 6: Provide New Names for IT Resources page, enter new names for the IT resources of the clone.

If the connector has multiple IT resources, then the new name that you specify for each IT resource must be different from the names of all the existing IT resources of that connector.

Click **Continue** after you specify new names for all the IT resources.

[Figure 12–20](#) shows the Provide New Names for IT Resource Type Definitions page of the Connector Management - Cloning wizard:

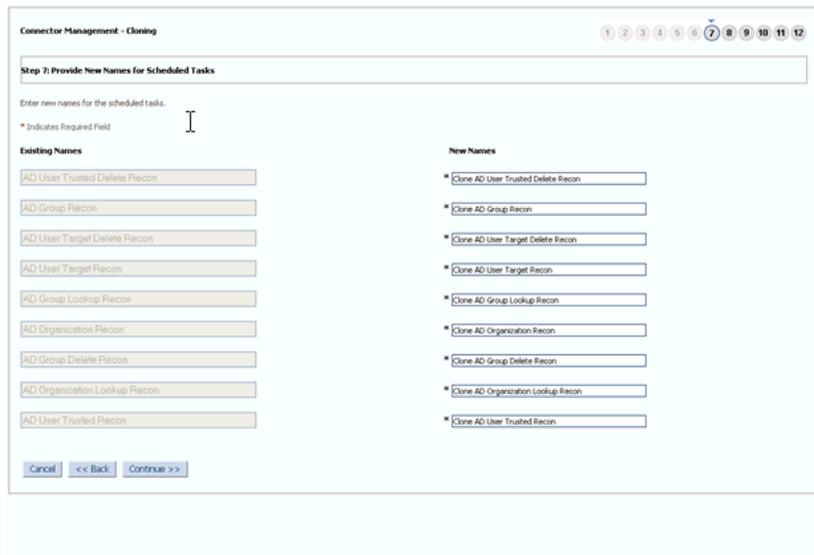
Figure 12–20 The Provide New Names for IT Resources Page



9. On the Step 7: Provide New Names for Scheduled Tasks page, enter new names for the scheduled tasks of the clone.
 Enter new names for the scheduled tasks. However, you cannot use the same set of scheduled tasks for the clone and the original connector.
 Click **Continue**.

Figure 12–21 shows the Provide New Names for Scheduled Tasks page of the Connector Management - Cloning wizard:

Figure 12–21 The Provide New Names for Scheduled Tasks Page



10. On the Step 8: Provide New Names for Lookup Type Definitions page, enter new names for the lookup definitions of the clone.
 Click **Continue**.

Figure 12–22 shows the Provide New Names for Lookup Type Definitions page of the Connector Management - Cloning wizard:

Figure 12–22 The Provide New Names for Lookup Type Definitions Page

Connector Management - Cloning

1 2 3 4 5 6 7 8 9 10 11 12

Step 8: Provide New Names for Lookup Type Definitions

Enter new names for the lookup definitions.

* Indicates Required Field

Existing Names	New Names
Lookup.AD.Group.Type	* Lookup.CloneAD.Group.Type
Lookup.AD.FieldsForValidation	* Lookup.CloneAD.FieldsForValidation
ADMap.ADAM.Group	* ADMap.CloneADAM.Group
Lookup.ADRReconciliation.TransformationMap	* Lookup.CloneADRReconciliation.TransformationMap
ADMap.AD.RemoteScriptLookup	* ADMap.CloneAD.RemoteScriptLookup
Lookup.AD.BLOBAttribute.Values	* Lookup.CloneAD.BLOBAttribute.Values
Lookup.ADAMReconciliation.FieldMap	* Lookup.CloneADAMReconciliation.FieldMap
ADMap.ADAM	* ADMap.CloneADAM
ADMap.FIM	* ADMap.CloneFIM
Lookup.AD.Constants	* Lookup.CloneAD.Constants
Lookup.ADRReconciliation.Organization	* Lookup.CloneADRReconciliation.Organization
Lookup.AD.Country	* Lookup.CloneAD.Country
ADMap.AD.Group	* ADMap.CloneAD.Group
ADMap.AD.RemoteScriptLookup	* ADMap.CloneAD.RemoteScriptLookup
Lookup.AD.BLOBAttribute.Values	* Lookup.CloneAD.BLOBAttribute.Values
Lookup.ADAMReconciliation.FieldMap	* Lookup.CloneADAMReconciliation.FieldMap
ADMap.ADAM	* ADMap.CloneADAM
ADMap.FIM	* ADMap.CloneFIM
Lookup.AD.Constants	* Lookup.CloneAD.Constants
Lookup.ADRReconciliation.Organization	* Lookup.CloneADRReconciliation.Organization
Lookup.AD.Country	* Lookup.CloneAD.Country
ADMap.AD.Group	* ADMap.CloneAD.Group
Lookup.ADRReconciliation.FieldMap	* Lookup.CloneADRReconciliation.FieldMap
Lookup.AD.GroupChildData	* Lookup.CloneAD.GroupChildData
Lookup.ADRReconciliation.GroupLookup	* Lookup.CloneADRReconciliation.GroupLookup
ADMap.AD	* ADMap.CloneAD
Lookup.AD.Domains	* Lookup.CloneAD.Domains
Lookup.AD.GroupReconciliation.FieldMap	* Lookup.CloneAD.GroupReconciliation.FieldMap
Lookup.ADAMGroupReconciliation.FieldMap	* Lookup.CloneADAMGroupReconciliation.FieldMap
Lookup.AD.Configuration	* Lookup.CloneAD.Configuration

Cancel << Back Continue >>

11. On the Step 9: Provide a Prefix for Adapters page, enter the string that will be set as the prefix for the copies of the adapters. Then, click **Continue**.

You must ensure that the prefix that you specify does not cause the full name of any adapter to exceed 80 characters. The Clone Connectors feature cannot check if this limit is exceeded. However, when you import the connector XML file created for the clone, the Deployment Manager throws an error. Remember that the Deployment Manager is called even when you build a deployment package for the clone and use the Install Connectors feature to install the clone.

You can use the Design Console to determine the character length of the longest adapter name.

Figure 12–23 shows the Provide a Prefix for Adapters page of the Connector Management - Cloning wizard:

Figure 12–23 The Provide a Prefix for Adapters Page

Connector Management - Cloning

Step 9: Provide a Prefix for Adapter Names

Enter the string to be prefixed to all adapter names.

* Indicates Required Field

* clon

Cancel << Back Continue >>

- On the Step 10: Provide New Names for Reconciliation Rules page, enter new names for the reconciliation rules of the clone.

Figure 12–24 shows the Provide New Names for Reconciliation Rules page of the Connector Management - Cloning wizard:

Figure 12–24 The Provide New Names for Reconciliation Rules Page

Connector Management - Cloning

Step 10: Provide New Names for Reconciliation Rules

Enter new names for the reconciliation rules.

* Indicates Required Field

Existing Names	New Names
AD Group Piecon	* AD Group Reconst
Target Resource Piecon Rule	* Target Resource Reconst
Trusted Source Piecon Rule	* Trusted Source Reconst

Cancel << Back Continue >>

- On the Step 11: Object Names Summary page, review the names that you have set for the connector objects of the clone and then click **Continue**.

[Figure 12-25](#) shows the Object Names Summary page of the Connector Management - Cloning wizard:

Figure 12-25 *The Object Names Summary Page*

Connector Management - Cloning 1 2 3 4 5 6 7 8 9 10 **11** 12

Step 11: Object Names Summary

Review the new object names, and then click Confirm to proceed with the cloning operation.

Resource Objects mapping summary.

Existing Object Names	New Object Names
AD Group	Clone AD Group
AD Organization Unit	Clone AD Organization Unit
AD User	Clone AD User
AD User Trusted	Clone AD User Trusted

Process Definition mapping summary.

Existing Object Names	New Object Names
AD Organization Unit	Clone AD Organization Unit
AD User	Clone AD User
AD Group	Clone AD Group
AD User Trusted	Clone AD User Trusted

Process Form mapping summary.

Existing Object Names	New Object Names
LD_ADUSER	LD_ADUSERA
LD_OU	LD_OUB
LD_ADUSRCD	LD_ADUSRCD
LD_ADGRP	LD_ADGRPE

IT Resource type definition mapping summary.

Existing Object Names	New Object Names
AD Server	Clone AD Server

IT Resource mapping summary.

Existing Object Names	New Object Names
GCADITResource	CloneGCADITResource
ADITResource	CloneADITResource

Scheduled tasks mapping summary.

Existing Object Names	New Object Names
AD User Trusted Delete Recon	Clone AD User Trusted Delete Recon
AD Group Recon	Clone AD Group Recon
AD User Target Delete Recon	Clone AD User Target Delete Recon
AD User Target Recon	Clone AD User Target Recon
AD Group Lookup Recon	Clone AD Group Lookup Recon
AD Organization Recon	Clone AD Organization Recon
AD Group Delete Recon	Clone AD Group Delete Recon
AD Organization Lookup Recon	Clone AD Organization Lookup Recon
AD User Trusted Recon	Clone AD User Trusted Recon

Lookup definitions mapping summary.

Existing Object Names	New Object Names
Lookup.AD_Group Type	Lookup.CloneAD_Group Type
Lookup.AD.FieldsForValidation	Lookup.CloneAD.FieldsForValidation
AtMap.ADAMGroup	AtMap.CloneADAMGroup
Lookup.ADRconciliation.TransformationMap	Lookup.CloneADReconciliation.TransformationMap
AtMap.AD.RemoteScriptLookup	AtMap.CloneAD.RemoteScriptLookup
Lookup.AD.BLOBAttribute.Values	Lookup.CloneAD.BLOBAttribute.Values
Lookup.ADAMReconciliation.FieldMap	Lookup.Clone.ADAMReconciliation.FieldMap
AtMap.ADAM	AtMap.CloneADAM
Atmap.RM	Atmap.CloneRM
Lookup.AD.Constants	Lookup.CloneAD.Constants
Lookup.ADRconciliation.Organization	Lookup.CloneADReconciliation.Organization
Lookup.AD.Country	Lookup.CloneAD.Country
AtMap.ADGroup	AtMap.CloneADGroup
Lookup.ADRconciliation.FieldMap	Lookup.CloneADReconciliation.FieldMap
lookup.AD.GroupChildData	lookup.CloneAD.GroupChildData
Lookup.ADRconciliation.GroupLookup	Lookup.CloneADReconciliation.GroupLookup
AtMap.AD	AtMap.CloneAD
Lookup.AD.Domains	Lookup.CloneAD.Domains
Lookup.ADGroupReconciliation.FieldMap	Lookup.CloneADGroupReconciliation.FieldMap
Lookup.ADAMGroupReconciliation.FieldMap	Lookup.CloneADAMGroupReconciliation.FieldMap
Lookup.AD.Configuration	Lookup.CloneAD.Configuration

Adapter names mapping summary.

Existing Object Names	New Object Names
ADCS Update Multi Attribute Data	ClonADCS Update Multi Attribute Data
ADCS Prepopulate User Last Name	ClonADCS Prepopulate User Last Name
ADCS Execute Remote Script	ClonADCS Execute Remote Script
ADCS Change Org Name	ClonADCS Change Org Name
ADCS Prepopulate User Password	ClonADCS Prepopulate User Password
ADCS Prepopulate User Middle Name	ClonADCS Prepopulate User Middle Name
ADCS Rename Group	ClonADCS Rename Group
ADCS Must Change PWD	ClonADCS Must Change PWD
ADCS Lock_Unlock User	ClonADCS Lock_Unlock User
ADCS Remove User From Group	ClonADCS Remove User From Group
ADCS Add User To Group	ClonADCS Add User To Group
ADCS Prepopulate UserPrincipalName	ClonADCS Prepopulate UserPrincipalName
ADCS Rename User Account	ClonADCS Rename User Account
ADCS Get Group ObjectGUID Created	ClonADCS Get Group ObjectGUID Created
ADCS Prepopulate AD Group Name	ClonADCS Prepopulate AD Group Name
ADCS Remove Multi Attribute Data	ClonADCS Remove Multi Attribute Data
ADCS Get USNChanged	ClonADCS Get USNChanged
ADCS Pwd Never Expires	ClonADCS Pwd Never Expires
ADCS Set User Password	ClonADCS Set User Password
ADCS Get USNCreated	ClonADCS Get USNCreated
ADCS Update Redirect Mail ID	ClonADCS Update Redirect Mail ID
ADCS Check Process Parent Org	ClonADCS Check Process Parent Org
ADCS Add Multi Attribute Data	ClonADCS Add Multi Attribute Data
ADCS Create Group	ClonADCS Create Group
ADCS Set Account Exp Date	ClonADCS Set Account Exp Date
ADCS Disable User	ClonADCS Disable User
ADCS Move User	ClonADCS Move User
ADCS Create OU	ClonADCS Create OU
ADCS Change Attribute	ClonADCS Change Attribute
ADCS Delete OU	ClonADCS Delete OU
ADCS Create User	ClonADCS Create User
ADCS Prepopulate User Full Name	ClonADCS Prepopulate User Full Name
ADCS Prepopulate User First Name	ClonADCS Prepopulate User First Name
ADCS Delete User	ClonADCS Delete User
ADCS Update Add User to Group	ClonADCS Update Add User to Group
ADCS Move Group	ClonADCS Move Group
ADCS Move OU	ClonADCS Move OU
ADCS Prepopulate User Login	ClonADCS Prepopulate User Login
ADCS Delete Group	ClonADCS Delete Group
ADCS Change Group Attribute	ClonADCS Change Group Attribute
ADCS Enable User	ClonADCS Enable User

Reconciliation rules mapping summary.

Existing Object Names	New Object Names
AD Group Recon	AD_Group Recon1
Target Resource Recon Rule	Target Resource Recon Rule1
Trusted Source Recon Rule	Trusted Source Recon Rule 1

Cancel << Back Confirm

14. On the Step 12: Object Clone Generation page, click **Generate XML**.

Figure 12–26 shows the Object Clone Generation page of the Connector Management - Cloning wizard:

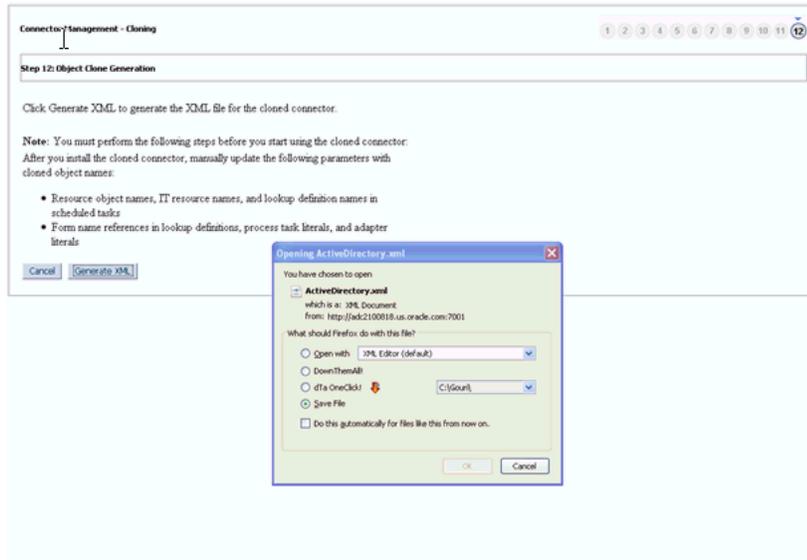
Figure 12–26 The Object Clone Generation Page



15. In the File Download dialog box, use the Save option to save the connector XML file of the clone to a location of your choice.

Figure 12–27 shows the File Download dialog box:

Figure 12–27 The File Download Dialog Box



Step 2: Install the clone connector

You can install the clone connector by using one of the following approaches:

Note: You can install the clone connector on either the same or a different Oracle Identity Manager installation.

- Use the Deployment Manager to import the connector XML file. If you use Deployment Manager import to install the connector, then you need to define the cloned connector. This will enlist the cloned connector in the list of connectors in Connector Management Search. If the connector is imported in different Oracle Identity Manager environment where the original connector does not exist, then you need to upload the related Jar files of the connector using JarUpload utility and adapters need to be compiled after all connector jars have been uploaded.
- Create a deployment package for the cloned connector, and then install it using the Install Connectors feature. For a sample, see the contents of the deployment package for any Oracle-released connector.

12.6.3 Postcloning Steps

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- **Lookup Definition:** If the lookup definition contains the old lookup definition details, then it must be modified to provide the new cloned lookup definition names. If the encode and decode values are referring the base connector attribute references, then these must be replaced with new cloned attributes.
- **Scheduled Task:** The base connector resource object name in the scheduled task must be replaced with the cloned resource object name. If the scheduled task parameter has any data referring to the base connector artifacts or attributes, then these must be replaced with the new cloned connector artifacts or attributes.

12.7 Exporting Connector Object Definitions in Connector XML Format

As mentioned earlier, the Oracle Identity Manager database stores the definitions of all connector objects. You can export these definitions to create a connector XML file for a particular connector. By using the Deployment Manager, you can import the connector XML file to create the connector object definitions in another Oracle Identity Manager installation.

Alternatively, you can use the connector XML file as one of the components of a deployment package that you create for the connector. This deployment package can then be installed using the Install Connectors feature. For a sample, see the contents of the deployment package for any Oracle-released connector. Another important component of a deployment package is the configuration XML file, which is used by the Install Connectors feature. You must manually create the configuration XML file.

See Also : Connector guide for information about the contents of the configuration XML file

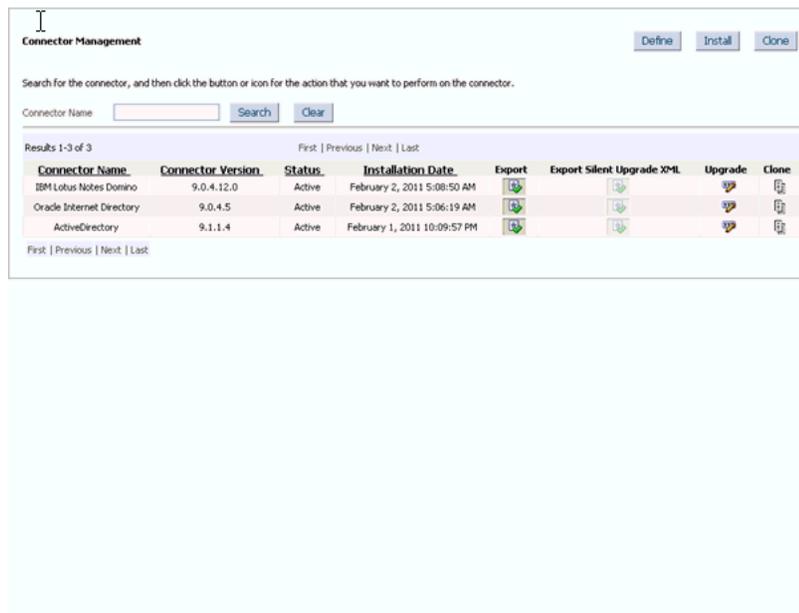
To export connector object definitions in connector XML format:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Manage Connector**.

3. You can use one of the following options to export the connector XML file:
 - If you want the XML file to include definitions of only specific connector objects, then use the Export button to open the Deployment Manager. See the "Using the Deployment Manager" chapter in the connector guide for detailed information about using this feature to select connector objects whose definitions you want to include in the connector XML file.
 - If you want to create the connector XML file out of the connector XML stored in the database when the connector was defined, then:
 - a. In the Connector Management page, use the Search feature to display the connector for which you want to create the connector XML file.
 - b. Use the Export icon displayed in the connector row to export the connector XML file from the entry created in the database when defining the connector.

Figure 12–28 shows the Connector Management page:

Figure 12–28 The Connector Management Page



12.8 Upgrading Connectors

Connector Upgrade utility is responsible for upgrading the OIM artifacts from source version to the target version, by retaining the customer customization done on the source connector. Connector upgrade does not handle connector library upgrade/update. User need to manually upgrade the libraries involved in connector.

The following are sample scenarios that describe a need for upgrading a connector:

- Reconfiguring or customizing an existing connector

After you install a connector, you might customize or reconfigure it according to your requirements. For example, you might add new attributes for reconciliation and provisioning and modify the scheduled tasks for reconciliation or lookup field synchronization. Ideally, you would make these changes to the connector on a staging server. You would then want to upgrade the connector deployed on your

production server to the version that you create by making changes on the staging server.

- **Upgrading a customer-developed connector**

You might have developed your own connector. When an Oracle-released upgrade is available for your connector, you might want to upgrade from your connector to the Oracle-released connector. For example, suppose you have developed and are using a connector for IBM Lotus Notes and Domino. When Oracle ships a new release of Oracle Identity Manager Connector for IBM Lotus Notes and Domino, you might want to use some of the features included in the new release. You can use the Upgrade Connectors feature to upgrade from your connector to the Oracle-released connector.

- **Upgrading an Oracle-released connector**

Oracle ships connector upgrades. An upgrade includes enhancements and fixes that you might need. For example, if you are currently using SAP User Management release 9.1.2, then you might want to upgrade to release 9.1.2.3 of the same connector when that release is available.

In scenarios such as these, you can use the Upgrade Connectors feature to upgrade the connector.

Upgrading connectors can be done by two ways:

- Silent mode upgrade: Used in staging and production environments
- Wizard mode upgrade: Used in development environment

In this guide, Wizard upgrade, which is performed using Oracle Identity System Administration pages is described.

This section is divided into the following topics:

- [Upgrade Use Cases Supported by the Connector Upgrade Feature](#)
- [Summary of the Upgrade Procedure](#)
- [Procedure to Upgrade a Connector](#)

12.8.1 Upgrade Use Cases Supported by the Connector Upgrade Feature

The following types of source connectors are supported by the Upgrade Connectors feature:

- Customer-developed connectors
- Oracle-released connectors that are not supported by the Install Connectors feature
- Oracle-released connectors that are supported by the Install Connectors feature
- Oracle-released connectors that are supported by the Install Connectors feature and have been customized
- Cloned connectors

The upgrade process does not cover the following objects:

- E-mail definitions
- Password policies
- Error message definitions
- Business rule definitions

- Object forms
- Access policies

Note:

- Connector lifecycle management does not support the upgrade of a trusted connector if the source connector uses the Xellerate User resource object for trusted source configuration. Therefore, you must manually upgrade the connector. Contact Oracle Support for more information.
 - Connector lifecycle management does not support the upgrade of a connector from the target mode (source version) to the trusted mode (target version). Similarly, upgrading from trusted mode to the target mode is also not supported.
-
-

Use Case 1: Custom-Developed Source Connector

A custom-developed source connector must meet the following requirements so that it is compatible with the Upgrade Connectors feature:

- The connector must be defined in Oracle Identity Manager. See "[Defining Connectors](#)" on page 12-13 if you want to manually define the connector.
- The connector must have a configuration XML file. See the connector guide for information about configuration XML files.

The following are sample events that can take place before you upgrade a custom-developed source connector:

- You develop the connector and its configuration XML file.
- Create a deployment package that is compatible with the Connector Installation feature. When you use this feature to deploy the connector on the production server, the connector is automatically defined at the end of the installation process.
- You use the connector for reconciliation and provisioning. Target system resources are allocated (through reconciliation and provisioning) for OIM Users.
- You modify the connector on the staging server, redefine it, and then regenerate the connector XML file.

Use Case 2: Oracle-released connector that is not supported by the Install Connectors feature

A connector that is not supported by the Install Connectors feature connector must meet the following requirements so that it is compatible with the Upgrade Connectors feature:

- The connector must be defined in Oracle Identity Manager. See "[Defining Connectors](#)" on page 12-13 if you want to manually define the connector.
- The connector must have a configuration XML file. See the connector guide for information about configuration XML files.

Sample events and the upgrade procedure for this use case are the same as those for Use Case 1.

Use Case 3: Oracle-released connector that is installed using the Install Connectors feature

A connector that is installed using the Install Connectors feature meets the requirements specified for Use Cases 1 and 2.

Use Case 4: Oracle-released connector that has been installed and then customized

A connector that is supported by the Install Connectors feature meets the requirements specified for Use Cases 1 and 2. However, customizations are overwritten during the upgrade process. For example, if you have added an attribute in a scheduled task and also modified the JAR file for reconciliation, then this customization would be lost after the upgrade. To work around this issue:

1. Keep a record of customizations that you implement on a connector.
2. After you upgrade the connector, reapply the customizations.

Use Case 5: Cloned connector

A connector that is installed using the Clone Connectors feature meets the requirements specified for Use Cases 1 and 2.

After the upgrade operation, you can use each clone to manage resource data that was collected through the clone before the upgrade.

12.8.2 Connector Object Changes Supported by the Upgrade Connectors Feature

Before you upgrade a connector, you might have reconfigured or customized the connector by making changes in individual connector objects. The upgrade process itself changes individual connector objects. The following sections list connector object changes supported by the Upgrade Connectors feature. These changes may have been performed manually (that is, at any time before the Upgrade Connectors feature is used) or may be performed by the Upgrade Connectors feature itself.

- [Resource Object Changes](#)
- [Process Definition Changes](#)
- [Process Form Changes](#)
- [Lookup Definition Changes](#)
- [Adapter Changes](#)
- [Rule Changes](#)
- [IT Resource Type Changes](#)
- [IT Resource Changes](#)
- [Scheduled Task Changes](#)

12.8.2.1 Resource Object Changes

The Upgrade Connectors feature can run on a resource object on which any combination of the following changes have been made. In addition, an upgrade operation might involve any combination of the following changes to a resource object.

- Status definitions can be added or deleted.
- Administrators can be assigned or deleted.

- Password policies can be added or deleted.
- User-defined fields (UDFs) can be added or deleted.
- Dependencies with other resource objects can be assigned or deleted.
- Object authorizers can be assigned or deleted. In addition, the priority number assigned to the authorizers can be modified.
- Process determination rules can be assigned or deleted.
- Event-handler adapters can be assigned or deleted.
- Resource object fields that are not present in the connector XML of the target connector are marked as obsolete.
- Customizations performed on the resource object are not retained.

After the upgrade, the new name of the resource object is the one specified in the connector XML of the target connector.

12.8.2.2 Process Definition Changes

The Upgrade Connectors feature can run on a process definition on which any combination of the following changes have been made. In addition, an upgrade operation might involve any combination of the following changes to a process definition.

- The existing process definition can be replaced by a new process definition.
- The existing provisioning definition can be renamed.
- Existing reconciliation field mappings can be retained without change or modified.
- New process tasks can be added.
- Custom process tasks can be retained without a change.
- Default process tasks can be retained, but you need to confirm that there are no changes in the default process task in the new version. Refer to the connector guide for more information.
- Any combination of the following changes can be made to an existing process task:
 - The name and properties of the task can be modified.
 - An attached event handler-adapter can be modified.
 - Preceding and dependent tasks can be added, modified, or deleted.
 - New response codes can be added.
 - Existing response codes can be modified or deleted.
 - New tasks can be generated.
 - Undo tasks and recovery tasks can be modified.
 - Task-to-object status mapping can be modified.
 - Assignment rules can be modified.
- Existing process tasks can be deleted.

After the upgrade, the new name of the process definition is the one specified in the connector XML of the target connector.

12.8.2.3 Resource Object Changes

To update the resource bundles:

1. If there are any customization on the resource bundles such as adding new entries to the connector resource bundles, the changes need to be applied on the resource bundles present in the "resources" folder of the connector distribution bundle. The existing resource bundles present in Oracle Identity Manager database can be downloaded using the DownloadResourceBundles utility available under *OIM_HOME/server/bin*.
2. Use DownloadResourceBundles utility (available under *OIM_HOME/server/bin*) to delete all the resource bundles specific to the connector from Oracle Identity Manager database.
3. Use UploadResourceBundles utility (available under *OIM_HOME/server/bin*) to upload all the resource bundles specific to the connector to Oracle Identity Manager database.

12.8.2.4 Process Form Changes

The Upgrade Connectors feature can run on a process form on which any combination of the following changes have been performed. In addition, an upgrade operation might involve any combination of the following changes to a process form.

Note:

- An upgrade operation works on only the active version of the process form. No changes are made to earlier versions.
 - The existing process form cannot be renamed.
-
-
- Columns can be added, modified, or deleted.
 - Child forms can be added, modified, or deleted.
 - Pre-populate adapters can be added.
 - The name, mappings, order, and rule of existing pre-populate adapters can be modified.
 - The user can manually add the customizations to the active version if they wish to add certain fields to the new version that were present in the existing form.
 - If the form attribute is retained and the corresponding connector objects, for example Lookup Definition and IT Resource Type Definition are removed to which this attribute has references, then you need to modify the form attribute properties by pointing it to the correct connector object.

After the upgrade, the name of the process form is the version number of the upgraded connector.

12.8.2.5 Lookup Definition Changes

The Upgrade Connectors feature can run on a lookup definition on which any combination of the following changes have been made. In addition, an upgrade operation might involve any combination of the following changes to a lookup definition.

- Lookup definitions can be added.

Note: Existing lookup definitions are not deleted during an upgrade operation.

- Existing lookup definitions can be retained or modified. During an upgrade operation, new entries in an existing lookup definition are appended after the existing entries.

12.8.2.6 Adapter Changes

The Upgrade Connectors feature can run on an adapter on which any combination of the following changes have been made. In addition, an upgrade operation might involve any combination of the following changes to an adapter.

Note: Existing adapters are not deleted during an upgrade operation.

- New adapters can be added.
- The custom adapters are retained as part of upgrade. If there are any customization on the default adapters, these changes need to be applied after upgrade as all the default adapters will be overwritten.
- After applying the customization on the default adapters (if there are any), the corresponding mapping for these adapters in Process Task, form field, and data object manager need to be verified for mapping.

12.8.2.7 Rule Changes

The Upgrade Connectors feature can run on a rule on which any combination of the following changes have been made. In addition, an upgrade operation might involve any combination of the following changes to a rule.

- New rules can be added.
- If there are any customizations in default Rules, these customizations need to be applied after the upgrade as all default Rules will be overwritten.

12.8.2.8 IT Resource Type Changes

The Upgrade Connectors feature can run on an IT resource type on which any combination of the following changes have been made. In addition, an upgrade operation might involve any combination of the following changes to an IT resource type.

- The existing IT resource type can be replaced by a new IT resource type.
- In an existing IT resource type, new parameters can be added and existing parameters can have their default values and types modified or deleted.
- All custom parameters are displayed while mapping IT Resource Type definitions. You can retain the custom parameters.

12.8.2.9 IT Resource Changes

The Upgrade Connectors feature can run on an IT resource on which any combination of the following changes have been made. In addition, an upgrade operation might involve any combination of the following changes to an IT resource.

- The parameter retained for IT Resource Type definition will be available for all the IT Resource instances of this type. If an existing parameter in IT Resource Type definition is not retained, then this parameter will not be available in all the IT Resource instances of this type.
- In an existing IT resource, new parameters can be added and existing parameters can have their default values and types modified or deleted.

After the upgrade, the new name of the IT Resource Type definition is the one specified in the connector XML of the target connector.

12.8.2.10 Scheduled Task Changes

The Upgrade Connectors feature can run on a scheduled task that has been retained or existing scheduled tasks have been replaced by new scheduled tasks.

12.8.3 What Happens When You Upgrade a Connector

See [Upgrade Use Cases Supported by the Connector Upgrade Feature](#) for information about the changes that can be put into effect when you upgrade a connector.

Note: After upgrading the Active Directory connector to Release 11.1.1.6.0, the connector does not work when a run is initiated from the browser of a remote machine. Connector Upgrade is working from the browser of the server on which Oracle Identity Manager is deployed.

In addition, the following events are part of the outcome of an upgrade operation:

- While performing the upgrade procedure, you are prompted to map new connector objects with existing objects. For example, you are prompted to map each resource object in the target connector with a resource object in the source connector. If the object names are same in both source and target, then for the new object, the corresponding old object need to be mapped. If there are changes in the object names in source and target, then you need to map the object properly by referring the source and target connector release documents. It is your responsibility map the source and target objects properly. If the objects are not mapped properly, then the source object will be corrupted by the upgrade process. Therefore, it is mandatory that you must know about all the source and the target connector objects.

12.8.4 Summary of the Upgrade Procedure

The following is a summary of the procedure to upgrade a connector:

Note: The procedure explained in this chapter is based on the best practice in which you first perform the upgrade in a test development environment. All functional use cases need to be tested before applying the upgrade in production server. Wizard mode upgrade should not be used in production, only silent mode need to be used in production server.

1. Read through the upgrade procedure.

This will let you make an estimate of the time for which the connector and, therefore, the target system might be unavailable to Oracle Identity Manager users. You can also determine if you have the Oracle Identity Manager expertise required to complete all the upgrade and post-upgrade steps.

2. Make a note of associations between objects of the source connector and other Oracle Identity Manager objects. For example, make a note of associations between resource objects and access policies.

3. If required, create the connector XML file for a clone of the source connector.

If the object names in the target connector are different from object names in the source connector, then it is recommended that you first create the connector XML file for the clone connector. ["Step 1: Create the connector XML file for the cloned connector"](#) on page 12-24 describes the procedure. While performing the procedure, specify object names that are the same as object names in the target connector. This will help avoid the need for renaming connector objects after you upgrade the connector.

4. Upgrading the source connector to target connector on staging server.

The XML file contains details of changes to be made to the connector objects of the source connector so that they are converted into the connector objects of the target connector. These changes are applied automatically during the upgrade process.

To upgrade the source connector:

- a. Back up the Oracle Identity Manager database on the production server.
 - b. Perform the steps described in ["Preupgrade Procedure"](#) on page 12-45
 - c. Perform the steps described in ["Silent Mode Upgrade in Staging and Production Environment"](#) on page 12-57 The resulting transformed XML can be generated and used in production server.
5. Use the silent delta XML for connector upgrade.

To use the delta XML file:

- a. Restore the production database on the staging server.
 - b. Perform the steps described in ["Preupgrade Procedure"](#) on page 12-45
 - c. Perform the steps described in ["Silent Mode Upgrade in Staging and Production Environment"](#) on page 12-57
 - d. Perform the steps described in ["Postupgrade Procedure"](#) on page 12-60
6. Verify that the source connector on the production server is the same as the source connector on the staging server. If there are differences in the source connector on the staging server and the production server, then the delta XML file is not correctly imported on the production server.
 7. Import the delta XML file on the production server.

After you verify that the upgraded target connector is working as expected on the staging server, perform the following steps:

- a. Perform the steps described in ["Preupgrade Procedure"](#) on page 12-45
- b. Perform the steps described in ["Silent Mode Upgrade in Staging and Production Environment"](#) on page 12-57
- c. Perform the steps described in ["Postupgrade Procedure"](#) on page 12-60

12.8.5 Procedure to Upgrade a Connector

The following sections discuss the procedure to upgrade a connector:

- ["Preupgrade Procedure"](#) on page 12-45
- ["Upgrade Procedure"](#) on page 12-45
- ["Postupgrade Procedure"](#) on page 12-60

12.8.5.1 Preupgrade Procedure

Before you begin the upgrade procedure, ensure that the following prerequisites are addressed:

- Read through the upgrade procedure documented in this chapter.
- Note down customizations made in the connector objects on source connector.
- Call a Java API to handle workflows that are in progress. See Step 3 of [Section 12.8.5.2, "Upgrade Procedure"](#) for information about pending workflows. You need to make sure that there are no requests in pending state for the resource objects that are part of this connector. You also need to complete all the requests before going for connector upgrade. Requests can be closed if they are in a closable state. All the requests associated with the connector resource objects should in one of the following states before starting the upgrade process.
 - Request Completed
 - Request Closed
 - Request Withdrawn
 - Request Failed
 - Template Approval Rejected
 - Request Approval Rejected
 - Operation Approval Rejected
- If required, create the connector XML file for a clone of the source connector.
- Disable all the scheduled tasks.
- Make sure that the connector is defined if there are any customizations done after installing the connector. See ["Defining Connectors"](#) on page 12-13 for information about defining connectors.

12.8.5.2 Upgrade Procedure

Upgrading connectors is a two-stage procedure:

- [Wizard Mode Upgrade in Staging Environment](#)
- [Silent Mode Upgrade in Staging and Production Environment](#)

Wizard Mode Upgrade in Staging Environment

Note: You need to perform preupgrade and post upgrade steps while performing wizard mode upgrade.

To perform the wizard mode upgrade on the staging server:

1. Create a backup of the Oracle Identity Manager database.

2. Create Oracle Identity Manager metadata (MDS) backup. See "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about exporting and importing Oracle Identity Manager metadata to and from MDS.
3. Run the connector preupgrade utility.

A validation script is provided with Oracle Identity Manager. This script performs the following functions:

- Determines whether the connector that you want to upgrade has been defined in Oracle Identity Manager

In other words, the script checks whether the connector XML stored in the database when the connector was installed/defined is consistent with the connector object definitions in the database. Apart from checking the consistency of the connector XML, it also checks whether the Connector XML is present in Oracle Identity Manager Database or not. If it is not present, then it displays the corresponding message to define the connector before proceeding with upgrade. Refer the "[Defining Connectors](#)" on page 12-13 to perform the procedure to define a connector.

- Identifies the Oracle Identity Manager scheduled tasks that are currently running.

You must disable all scheduled tasks that belong to the source connector before you proceed with the upgrade procedure. In addition, it is recommended to disable all other scheduled tasks before proceeding with the upgrade procedure.

- Identifies the Attestation tasks associated with the resource object of the connector.

You must complete all the attestation tasks that belong to the source connector before you proceed with the upgrade procedure.

- Identifies all the pending requests associated with the resource objects of the connectors.

You must either close or complete all the pending requests that belong to the source connector before you proceed with the upgrade procedure.

To run the validation script:

- a. Ensure that Oracle Identity Manager is running.
- b. In a command window, change to the *OIM_HOME/server/bin* directory.
- c. Run the script as follows:

Note: Set *APP_SERVER*, *OIM_ORACLE_HOME*, *JAVA_HOME*, *MW_HOME*, *WL_HOME*, and *DOMAIN_HOME* before running the scripts.

For Unix:

```
sh ConnectorPreUpgradeUtil.sh
```

For Windows:

```
ConnectorPreUpgradeUtil.bat
```

You will be prompted to provide the following details:

- Enter Oracle Identity Manager administrator's username: Enter the Oracle Identity Manger administrator's username.
- Enter Oracle Identity Manager administrator's password: Enter the Oracle Identity Manger administrator's password.
- Enter t3 Oracle Identity Manager Server URL: Enter the Oracle Identity Manger server URL. For example, t3://hostname:hostport.
- Enter OIM Database username: Enter the Oracle Identity Manager Database's username.
- Enter OIM Database Password: Enter the password of the Oracle Identity Manager Database.
- Enter the JDBC URL for the OIM Database: Enter the JDBC URL of the Oracle Identity Manager Database. For Example:

```
jdbc:oracle:thin:@HOST_NAME:DB_PORT:iam/ORACLE_SID
```

After the successful login, you will be prompted to provide the following details:

- Enter the connector name: Enter the connector name to be validated before upgrade.
- Enter the connector version: Enter the connector version to be validated before upgrade.

On successfully connecting to the Oracle Identity Manager database, a message is displayed.

The output generated by the script is displayed in the command window and is also recorded in the *OIM_HOME/server/bin/validateUtil.log* file.

The action that you must take depends on the message generated by the script:

- If the message states that the connector XML in the database is not consistent with the connector objects defined in the database, then perform the procedure described in the "[Defining Connectors](#)" on page 12-13 of the connector guide.
- If the message states that the "connector XML does not exists in Oracle Identity Manager database. Define a connector before upgrade.", then perform the procedure described in the "[Defining Connectors](#)" on page 12-13 section of the connector guide before proceeding with upgrade
- If the message contains the names of the scheduled tasks that are currently running, then you must disable all scheduled tasks. To disable a scheduled task, in the Advanced Administration, click **System Management**, search for scheduled jobs, and click the specific scheduled job, and then click **Stop**.
- If the message contains the names of the Attestation Processes of which some attestation tasks associated with the resource object of the connector is pending, then you must complete all the attestation tasks belonging to the connector that you are upgrading before proceeding with the upgrade process.
- If the message contains the names of the pending requests associated with the resource object of the connector, then you must either close or complete all the pending requests belonging to the connector that you are upgrading before proceeding with the upgrade process.

4. Copy the JARs and the resource bundles to the specified directories.

If the target release also contains new or updated JARs and resource bundles, then download the version of the jar to Oracle Identity Manager, check the version of the jar which is shipped with Oracle Identity Manager, compare these files and copy the JARs manually to their destination directories. For an Oracle-shipped connector, details of the destination directories are given in the connector guide. See the [Connector Code Files Changes](#) section for more information.

5. Use the Upgrade Connectors feature.
 - a. Log in to the Oracle Identity System Administration.
 - b. In the left pane, under System Management, click **Manage Connector**.
 - c. Use the Search feature to search for the source connector that you want to upgrade. In the table of search results, click the Upgrade icon for the source connector.
 - d. On the Step 1: On the Upgrade page, select Connector XML for the Wizard Mode XML File field. Use the Browse option to navigate to the target version of the connector XML to which you want to upgrade. You can also enter the full path of the target connector XML file. Make sure that you select the correct target connector XML. Upgrade feature does not validate the XML for target version or for any other connector object details. Leave Silent Mode XML File field empty.

For example, if a user is upgrading the Active Directory connector from source version 9.1.1.7 to target version 11.1.1.5.0, user needs to select Active Directory 11.1.1.5.0 connector config XML (which is under xml folder) for Wizard mode upgrade XML field.

Note: There will be only one XML file for both trusted source reconciliation and target resource reconciliation for all the ICF based connectors. If you have more than one XML file, that is one for trusted source reconciliation and another for target resource reconciliation, you need to select the XML file for target resource reconciliation. Refer the connector guide (CI-XML) for the XML file name.

[Figure 12–29](#) shows the Select Connector XML to Upgrade page of the Connector Management - Upgrading wizard:

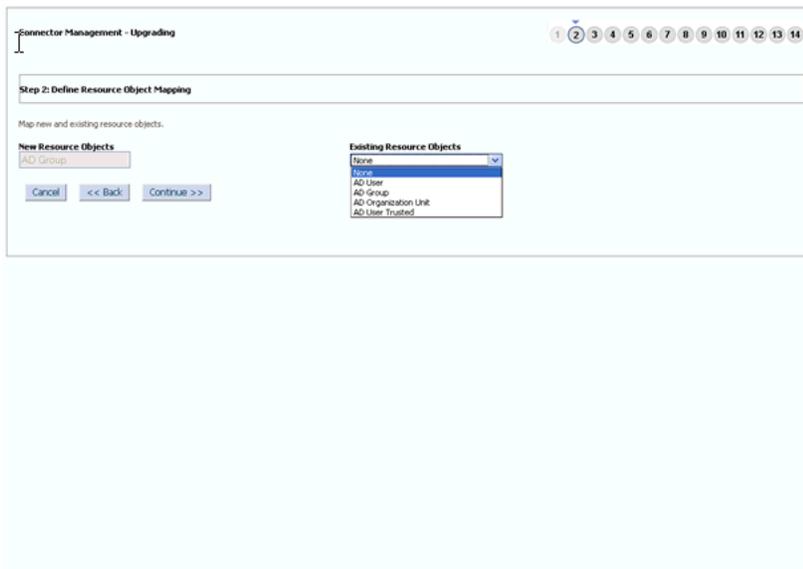
Figure 12–29 The Select Connector XML to Upgrade Page

- e. Click **Continue**.
- f. On the Step 2: Resource Object Mapping page, apply the following guidelines to map each new resource object with an existing resource object. Click Continue after you create each mapping.
 - The New Resource Object field shows the name of a resource object in the target release. From the Existing Resource Object list, select the resource object in the source release to which you want to map the resource object in the target release. There might be a change in resource object names. It is your responsibility to map the resource object properly.
 - If there are new resource objects that do not have a corresponding resource object in the source release, then select None from the Existing Resource Object list. This will happen only when the target connector versions add new resource objects that are not there in the source version.

Note: If you are upgrading from an Oracle-released source connector to an Oracle-released target connector, then see the connector guide for information about the mappings that you must create.

Figure 12–30 shows the Resource Object Mapping page of the Connector Management - Upgrading wizard:

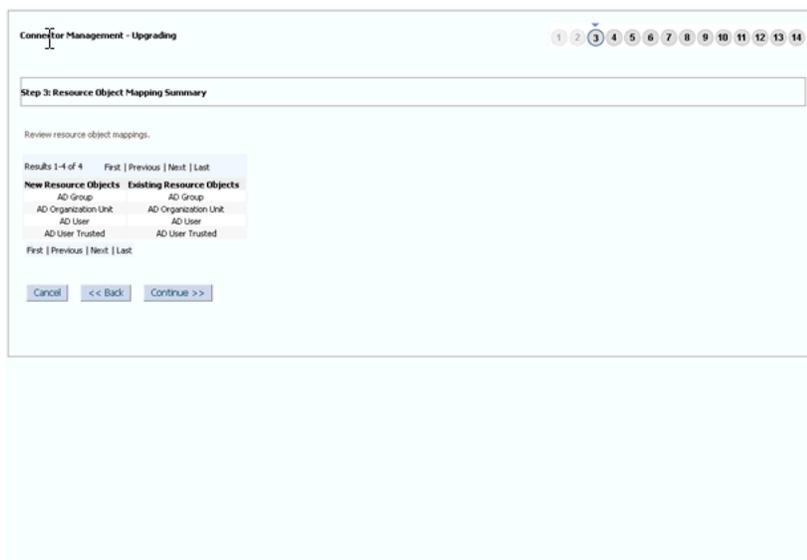
Figure 12–30 The Resource Object Mapping Page



- g. On the Step 3: Define Resource Scope page, a summary of the resource object mappings that you create is displayed. If there are resource objects in the source release that do not have corresponding resource objects in the target release, then they are displayed in the second table on this page. If you want to delete these resource objects, then select their check boxes. If a resource object is selected for deletion, then the resource will not be deleted from Oracle Identity Manager database. It just updates the OBJ_IS_SOFT_DELETE flag for the corresponding Resource Object to "1". The resource will be still available for all provisioning and reconciliation. This flag will be used in future.

Figure 12–31 shows the Define Resource Scope page of the Connector Management - Upgrading wizard:

Figure 12–31 The Define Resource Scope Page



- h. Click **Continue**.

- i. On the Step 4: Define Process Definition Mapping page, map each new process definition with an existing process definition. Follow the guidelines given in Step f for mapping resource objects. Click Continue after you create each process definition mapping. If there are changes in the process definition names in source and target, it is your responsibility to map them properly. After selecting the corresponding source process definition for a specified target process definition, the page displays the list of process tasks available in the source process definition. You can retain the process tasks from the Source process definition. If there are any custom process tasks added to the source process definition, they can be retained. If there are any customization on the default process task, then before retaining such tasks you need to make sure there are no changes for this process task in the new connector release version by refereeing the connector guide. If a specific default process task is selected to retain, you might lose the changes (if there are any) for this process task in the new connector release. If the process tasks are part of the source connector and are not required in the target connector, then such process tasks must not be retained. It is recommended only to retain tasks that are added by user as part of customization of the source connector.

Figure 12–32 shows the Define Process Definition Mapping page of the Connector Management - Upgrading wizard:

Figure 12–32 The Define Process Definition Mapping Page

The screenshot shows the 'Step 4: Define Process Definition Mappings' page. At the top, there are navigation buttons (1-14) and a title bar 'Connector Management - Upgrading'. Below the title, there are two dropdown menus for 'New Process Definitions' and 'Existing Process Definitions', both set to 'AD User'. A note states: 'Select the process tasks that must be retained from the existing process definition. The process tasks listed below only exists in the old process definition. Notes: If you have customized a shipped process task, then consider whether you would like to retain your customization.' Below this is a table with the following data:

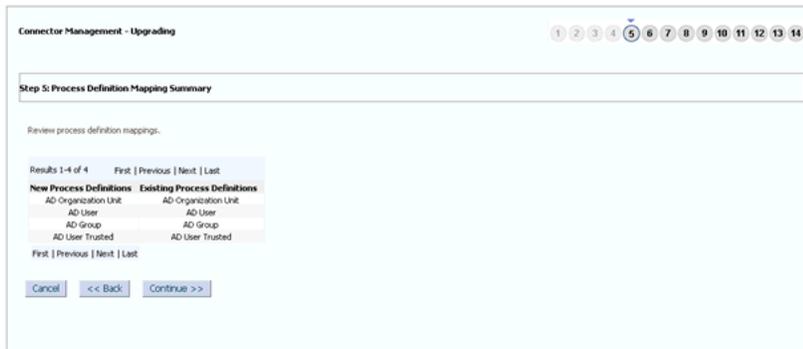
Process Task	Retain
Telephone Number Updated	<input type="checkbox"/>
Department Updated	<input type="checkbox"/>
Office Updated	<input type="checkbox"/>
Custom Process Task1	<input checked="" type="checkbox"/>
User Principal Name Updated	<input type="checkbox"/>
Title Updated	<input type="checkbox"/>
Mobile Updated	<input type="checkbox"/>
Update Add User To Group	<input type="checkbox"/>
Street Updated	<input type="checkbox"/>
State Updated	<input type="checkbox"/>

At the bottom of the table is a 'Retain' button. Below the table are navigation buttons: 'First | Previous | Next | Last', 'Cancel', '<< Back', and 'Continue >>'.

- j. On the Step 5: Process Definition Mapping Summary page, a summary of the process definition mappings that you create is displayed. Click Continue to proceed.

Figure 12–33 shows the Process Definition Mapping Summary page of the Connector Management - Upgrading wizard:

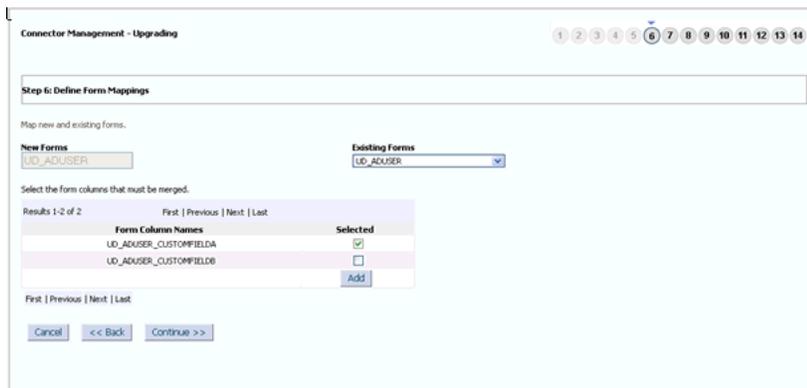
Figure 12–33 The Process Definition Mapping Summary Page



- k. On the Step 6: Define Form Mappings page, map each new form with an existing form. Follow the guidelines given in Step f for mappings resource objects. In addition, apply the following guideline and then click Continue after you create a mapping for each form. When a source process form is selected for each target, the page displays list of process form fields from the source process form attributes, which are not available in the target process form. These attributes either added to the source process as a part of customization or these were default attributes part of the source process form which may not be required for the target. You can select the attributes which are added as a part of customization, but need to verify if a default attribute is required in the target before retaining it.

Figure 12–34 shows the Define Form Mappings page of the Connector Management - Upgrading wizard:

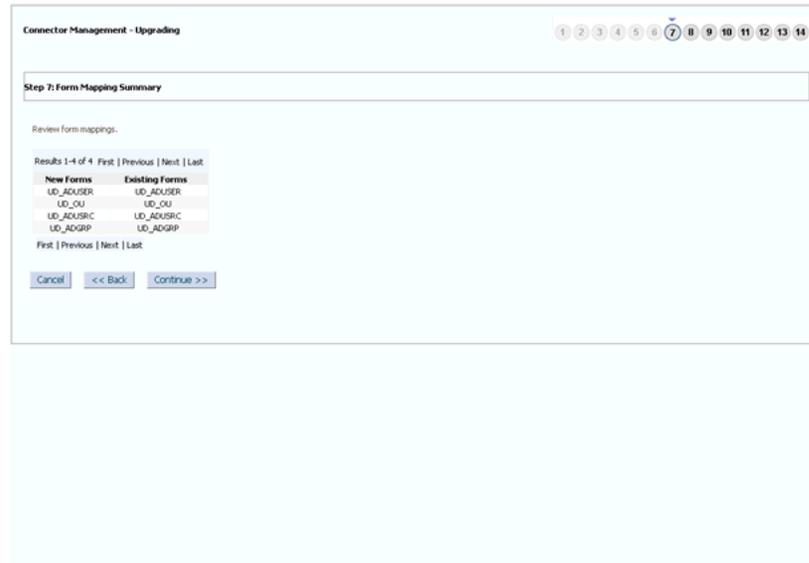
Figure 12–34 The Define Form Mappings Page



- I. On the Step 7: Form Mapping Summary page, a summary of the form mappings that you create is displayed. Click Continue to proceed.

Figure 12–35 shows the Form Mapping Summary page of the Connector Management - Upgrading wizard:

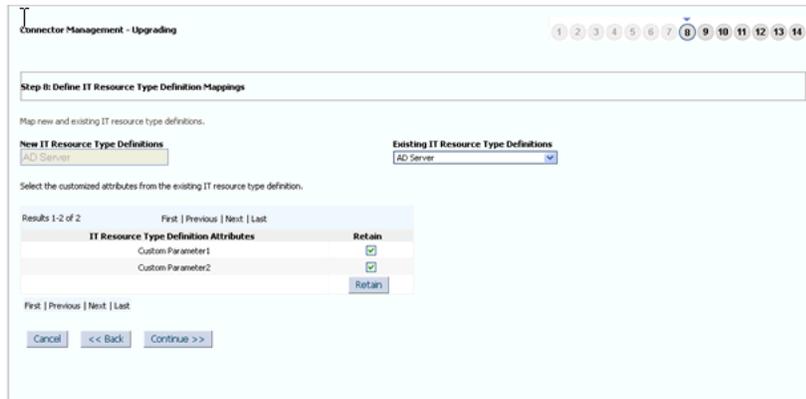
Figure 12–35 The Form Mapping Summary Page



- m. On the Step 8: Define IT Resource Type Definition Mappings page, map each new IT resource definition with an existing IT resource definition. Follow the guidelines given in Step f for mappings resource objects. Click Continue after you create a mapping for each IT resource definition. If there are changes in the names of the IT resource type definition, then it is your responsibility to map them properly. Refer the connector guide to check the change in default IT resource type definition names. When a target IT resource type definition is mapped with corresponding source IT resource type definition, the page displays list of IT resource type definition parameters, which are part of source definition but not available in target definition. These are either added as a part of customization or they were part of source definition. If these parameters are added as part of customization, then you need to retain them.

Figure 12–36 shows the Define IT Resource Type Definition Mappings page of the Connector Management - Upgrading wizard:

Figure 12–36 The Define IT Resource Type Definition Mappings Page



- n. On the Step 9: IT Resource Type Definition Mapping Summary page, a summary of the IT resource type definition mappings that you create is displayed. Click Continue to proceed.

Figure 12–37 shows the IT Resource Type Definition Mapping Summary page of the Connector Management - Upgrading wizard:

Figure 12–37 The IT Resource Type Definition Mapping Summary Page



- o. On the Step 12: Preupgrade Steps page, enter a new release number for the connector in the Connector Version field. Click Continue to proceed. The upgrade process does not validate the version provided with the connector release version. You need to provide correct version here by referring the connector guide.

Figure 12–38 shows the Preupgrade Steps page of the Connector Management - Upgrading wizard:

Figure 12–38 The Preupgrade Steps Page

Connector Management - Upgrading

Step 12: Preupgrade Steps

* Indicates required field
Enter the release number of the connector.

Connector Name: ActiveDirectory
Connector Release: * 9.1.1.5.0

Note:
Before you proceed, ensure that the following prerequisites are addressed:

- Create a backup of the Oracle Identity Manager database.
- Ensure that there are no pending JMS messages to be processed.
- Ensure that there are no pending tasks to be performed.
- Copy the required connector and third-party JARs and resource bundles into the specified Oracle Identity Manager directories.

Cancel << Back Continue >>

- p. On the Step 13: Select Connector Objects to Be Upgraded page.

Figure 12–39 shows the Select Connector Objects to Be Upgraded page of the Connector Management - Upgrading wizard:

Figure 12–39 The Select Connector Objects to Be Upgraded Page

Connector Management - Upgrading

Step 13: Select Connector Objects to Be Upgraded

Summary: All 185
Resource: 5
IT Resource Definition: 1
Task Adapter: 33
Process Form: 4
User XML: 1
IT Resource: 2
Job: 9
Data Object Definition: 5
Prepopulate Adapter: 8
Process: 6
Lookup: 21
Scheduled Task: 9
User Metadata: 1

Current Selections

- Lookup:ADGroupReconciliationFieldMap
- adpADCSPREPOPULATEUSERBYRSNAME
- adpADCSPREPOPULATEUSERLOGIN
- com.thortech.util.adobj.totID_ADUSER
- AD Organization Unit
- AD Organization Unit
- adpADCMOVEOU
- adpADCSOHCOPROCESSPARENTORG
- adpADCSOHCOPROCESSORNAME
- LD_OU
- adpADCSGETUSNOCHANGED
- adpADCSDELETEOU
- adpADCSGETUSNOCREATED
- adpADCSCREATEOU
- com.thortech.util.adobj.totID_ADGRP
- AD User
- AD User
- LD_ADUSER
- LD_ADUSRC
- adpADCMUSTCHANGEPWD
- adpADCSSETUSERPASSWORD

Objects Removed From Import

Deleted Objects

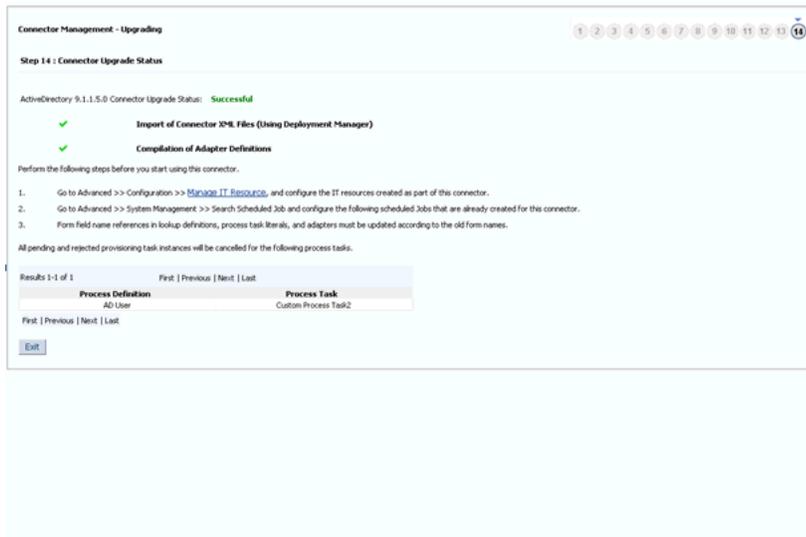
Exit Upgrade

Note: If the Connector Management - Upgrading wizard is opened by using Microsoft Internet Explorer, then all the fields and buttons on the Step 13: Select Connector Objects to Be Upgraded page might not be visible. There is no scroll bar available in the page. Therefore, maximize the window to display all the controls in the page.

- q. After you review the information on the Connector Upgrade Status page, click **Upgrade** to start the upgrade process.

Figure 12–40 shows the Connector Upgrade Status page of the Connector Management - Upgrading wizard:

Figure 12–40 The Connector Upgrade Status Page



Note down the process definition names and the corresponding process task names. These process tasks are not going to be used by Oracle Identity Manager anymore. Therefore, all their pending and rejected instances need to be canceled.

Use `cancelProcessTask` utility available in `OIM_HOME/server/bin`. The utility takes the process definition name and the process task name as input. You need to run the utility for each process task.

The Upgrade Connectors feature processes connector object mappings in the following manner:

- If a new connector object is mapped to None, then the new connector object is inserted in the database.
 - A new resource object, process definition, or form replaces the old resource object, process definition, or form to which it is mapped.
 - The new names of the process form are converted into the old process form names.
 - If an old and a new lookup definition have the same name, then their contents are merged.
 - When the Upgrade Connectors feature tries to delete an object, which is not going to be used by upgraded version of connector, an exception is thrown if the instances of the object exists in Oracle Identity Manager database. Such an object is renamed and soft deleted so that it will not be used anymore by Oracle Identity Manager.
6. Perform the following steps:
 - a. Change form names and form field column name references in the following objects:

Note: For an Oracle-released connector, see the connector guide for information about the changes to be made.

- Lookup definitions
 - Process task literals
 - Adapter literals
- b. All the default adapters are overwritten. Therefore, if customer has done any customization, the changes need to be applied after connector upgrade.
 - c. After the upgrade, contents of existing and new lookup definitions are merged. In these lookup definitions, you must manually delete entries that are not required.
7. Use the FVC Utility to update existing user data created through the connector.
See "Using the Form Version Control Utility" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about using the FVC Utility.
 8. Verify that all use cases specific to the target are working fine including provisioning and reconciliation.
 9. Generate the XML file. This XML file contains details of the object definition changes from the source release to the target release.

To generate this file:

- a. Log in to the Oracle Identity System Administration.
- b. In the left pane, under System Management, click **Manage Connector**.
- c. Use the Search feature to search for the connector.
- d. In the search results table, click the Export Silent Upgrade XML icon for the connector.
- e. Specify the location where you want the file to be saved.

Note: If the upgrade fails, then perform the following steps:

1. Look at the exception and take suitable action.
 2. Restore the Oracle Identity Manager database and MDS.
 3. Proceed for the upgrade.
-
-

Silent Mode Upgrade in Staging and Production Environment

Note: You need to perform preupgrade and post upgrade steps while performing wizard mode upgrade.

Caution: Before you import the XML file, verify that the source connector on the production server is the same as the source connector on the staging server. If there are differences in the source connector on the staging server and the production server, then the XML file is not correctly imported on the production server.

To perform the silent mode upgrade on the production server:

1. Copy the XML file to the host computer of the Oracle Identity Manager installation on which you want to import the file. Alternatively, copy the XML file to a shared folder on another computer that can be accessed from the Oracle Identity Manager host computer.
2. Log in to the Oracle Identity System Administration.
3. In the left pane, under System Management, click **Manage Connector**.
4. Use the Search feature to search for the source connector that you want to upgrade.
5. In the table of search results, click the Upgrade icon for the source connector.
6. On the Step 1: Select Connector XML to Upgrade page of the utility, enter the full path and name of the connector XML file for the source release in the Silent mode upgrade XML field. You can use the Browse option to navigate to the XML file.

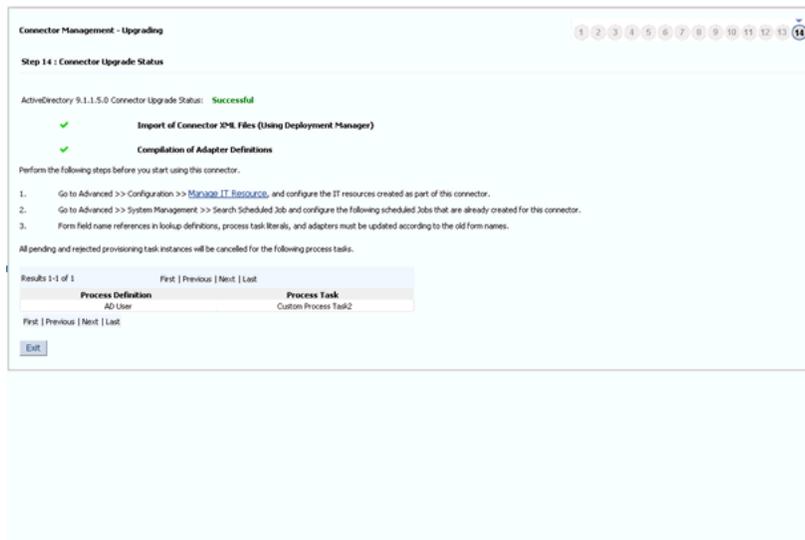
Note: There will be only one XML file for both trusted source reconciliation and target resource reconciliation for all the ICF based connectors. If you have more than one XML file, that is one for trusted source reconciliation and another for target resource reconciliation, you need to select the XML file for target resource reconciliation. Refer the connector guide (CI-XML) for the XML file name.

Figure 12–41 shows the Select Connector XML to Upgrade page of the Connector Management - Upgrading wizard:

Figure 12–41 The Select Connector XML to Upgrade Page

7. Click **Continue**.
8. On the Step 12: Preupgrade Steps page, click **Continue** to proceed.

Figure 12–42 shows the Preupgrade Steps page of the Connector Management - Upgrading wizard:

Figure 12–44 The Connector Upgrade Status Page

12.8.5.3 Postupgrade Procedure

The following sections describe procedures that you must perform after the upgrade operation:

- [Connector Code Files Changes](#)
- [Running the PurgeCache Utility](#)
- [Running cancelProcessTask Utility](#)
- [Running the FVC Utility](#)
- [Updating Access Policies](#)
- [Updating Approval Policies](#)
- [Configuring the IT Resource](#)
- [Configuring the Scheduled Tasks](#)
- [Other Postupgrade Steps](#)

Connector Code Files Changes

During an upgrade operation, you need copy connector code files, which include JAR files and scripts to the specified directories. To do so:

1. Manually upload all the connector specific jars (excluding common library files Common.jar, FAMILYCommon.jar, and icf-Common.jar) present in the "lib" folder of the connector distribution bundle using UpdateJars utility (available under OIM_HOME/server/bin) to Oracle Identity Manager database. Before running the UpdateJars utility, set *APP_SERVER*, *OIM_ORACLE_HOME*, *JAVA_HOME*, *MW_HOME*, *WL_HOME*, and *DOMAIN_HOME*.
2. Download common library (Common.jar, FAMILYCommon.jar and icf-Common.jar) from Oracle Identity Manager database using DownloadJar utility (available under OIM_HOME/server/bin).
3. Extract MANIFEST.MF from the downloaded libraries. Compare this version of MANIFEST.MF with the version in MANIFEST.MF of the common libraries that is available as part of ICF based distribution bundle. If the distributed library version

is higher than the one downloaded from Oracle Identity Manager database, then use the UploadJar utility (available under `OIM_HOME/server/bin`) to upload the common libraries to Oracle Identity Manager database.

Running the PurgeCache Utility

When the upgrade is performed, there might be stale data in the cache, which is required to be purged. The PurgeCache utility purges the cache. See *Oracle Fusion Middleware Performance and Tuning Guide* for information about purging the cache.

Note: Before running this utility, set `APP_SERVER`, `OIM_ORACLE_HOME`, `JAVA_HOME`, `MW_HOME`, `WL_HOME`, and `DOMAIN_HOME`.

Running cancelProcessTask Utility

This utility is used for canceling the pending and rejected instances of a process task. If a process task of a process definition, which is there in the source connector and is not required in the target, then the process task will be soft deleted in the upgrade process. Oracle Identity Manager will not use such soft deleted task as part of provisioning work flow after upgrade. All the instances of such deleted process task, which are in pending and rejected status need to be canceled.

The utility is available in `OIM_HOME/server/bin`. This utility will take the process task name and the corresponding process definition name as input.

Note: Before running this utility, set `APP_SERVER`, `OIM_ORACLE_HOME`, `JAVA_HOME`, `MW_HOME`, `WL_HOME`, and `DOMAIN_HOME`.

Running the FVC Utility

Connector upgrade process creates the new process form versions. The account data created using the source connector will have an association with the source connector process form version. Therefore, after the upgrade, you need to run the FVC utility to update the new process form version which is created in upgrade process. Apart from this, FVC provides the feature to copy the old form field data to the new form fields. You can use the FVC Utility to copy process form data from the source release to the process form of the target release. You can also specify changes to be made to the resource data so that it is consistent with changes made in the process form of the target release. See *Oracle Identity Manager Tools Reference* for information about using this utility.

Updating Access Policies

In Oracle Identity Manager, an access policy is associated with a resource object. While creating an access policy, user would have provided the data for the process form attributes. As the part of connector upgrade, if there are changes in the form attributes, then you need to edit the access policy to check the data for the existing and the new fields. For example, if the connector upgrade adds a new process form attribute, you can provide the data for the new attribute by editing the access policy.

Updating Approval Policies

In Oracle Identity Manager, an approval policy is associated with a resource object. While creating a policy, user would have provided the data for the process form attributes. As the part of connector upgrade, If there are any change in the resource

object names, then the user need to verify all the Approval Policies associated with the resources to modify the resource name to the new resource name.

Configuring the IT Resource

Verify that the IT resource instances have proper values after upgrade.

Configuring the Scheduled Tasks

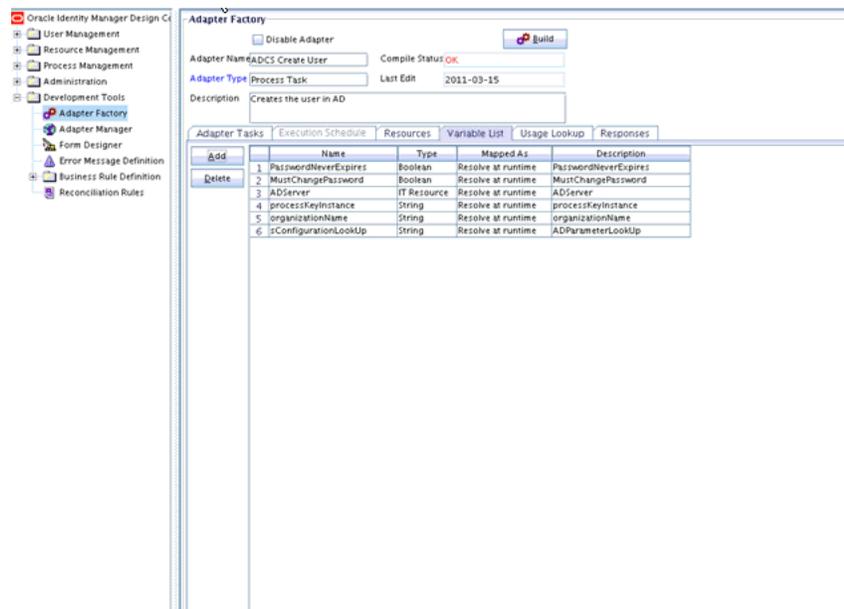
Set values for attributes of the scheduled tasks of the target release. For an Oracle-released target connector, see the connector guide for information about the scheduled task attributes.

Update Adapters for Changes in IT Resource Type Definition Parameter

If there are changes in the IT Resource Type Definition Parameter names, you need to update the custom adapters for the parameter changes. To do so:

1. Log in to Design Console.
2. Open the custom adapter using the adapter factory.
3. Go to the variable list and check if there are any variables of type IT Resource, as shown in [Figure 12–45](#):

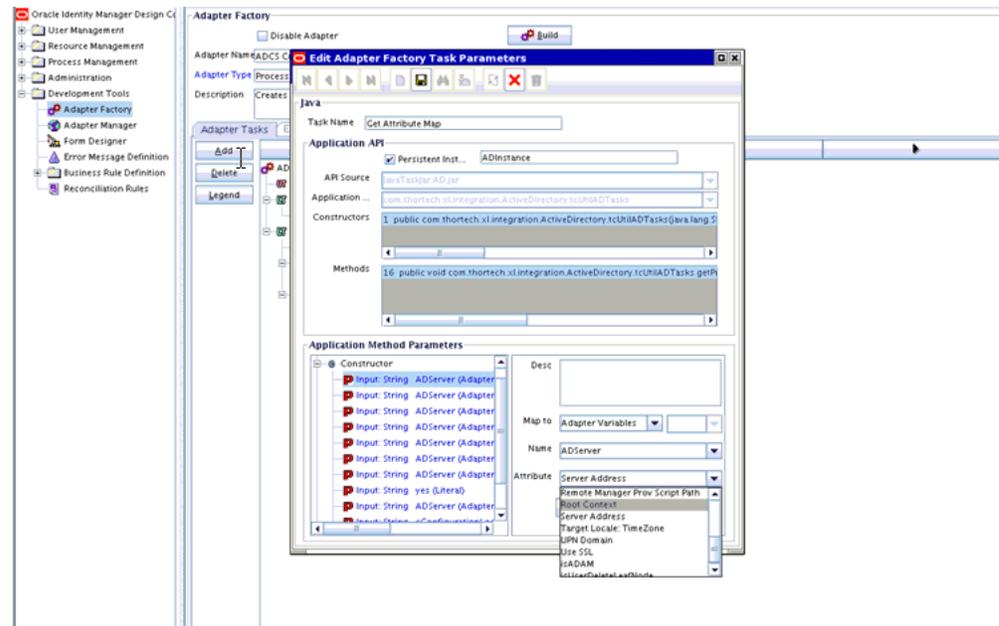
Figure 12–45 The Variable List Tab of the Adapter Factory Form



4. If there is a variable of IT Resource, then go to the task details and change the mapping of the IT Resource parameter mapping to the new target field (if the parameter is changed/ deleted).

[Figure 12–46](#) shows the Edit Adapter Factory Task Parameters dialog box that enables you to change the mapping of the IT Resource parameter mapping to the new target field:

Figure 12–46 The Edit Adapter Factory Task Parameters Dialog Box



5. If the adapter is mapped to the IT Resource Type Definition parameter, then you need to verify if the mapped parameter is not deleted. If the parameter is deleted, then you need to remap it to the correct parameter.

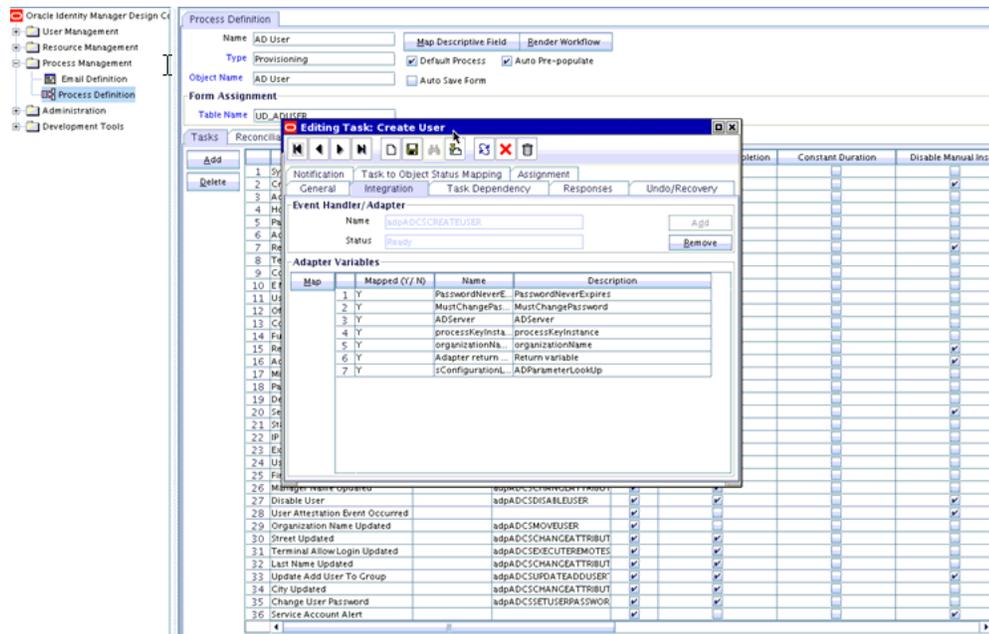
To verify the adapter mappings:

- a. Verify the mapping for process task adapter as follows:

- i) Log in to Design Console.
- ii) Go to Process Definition.

- iii) Click the task, and then click the **Integration** tab, as shown in [Figure 12–47](#):

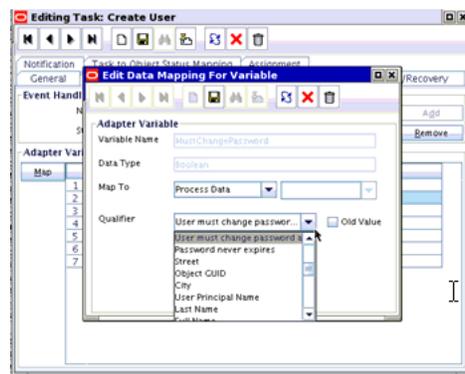
Figure 12-47 The Integration Tab of the Editing Task Dialog Box



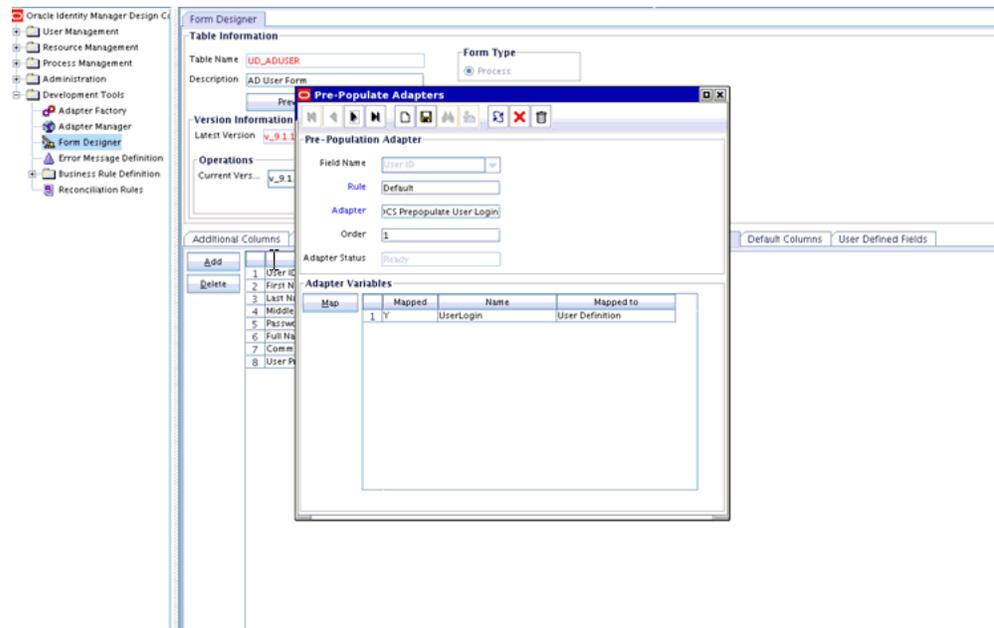
iv) Check if the adapter variable is mapped to the deleted/modified form attribute. If yes, remap such attributes to adapter variables. Repeat this step for all process tasks of all process definitions of the connector.

Figure 12-48 shows the Editing Data Mapping for Variable dialog box that enables you to view and edit the adapter variable mapping to the form attribute:

Figure 12-48 The Editing Data Mapping for Variable Dialog Box



- b. Prepopulate adapter mappings as follows:
 - i) Log in to Design Console.
 - ii) Go to Form Designer, Pre-Populate Adapters, as shown in Figure 12-49:

Figure 12–49 The Pre-Populate Adapters Dialog Box

iii) Click **Map** to map adapter variable and check if any of the fields are mapped to the process data attributes. If it is mapped, then verify the process form attribute is not deleted as part of upgrade. If the process form attributes are deleted, then remap them to the correct form attribute data.

Figure 12–50 shows the Map Adapter Variable dialog box:

Figure 12–50 The Map Adapter Variable Dialog Box

Note: Repeat the procedure for all the prepopulated fields of all the process forms of the connector. If there are any entity adapter, then check the adapter variables mapping for these adapters in Data Object Manager.

Other Postupgrade Steps

Perform the following postupgrade steps:

1. Change form names and form field column name references in the following objects:

Note: For an Oracle-released connector, see the connector guide for information about the changes to be made.

- Lookup definitions
 - Process task literals
 - Adapter literals
2. Verify all the reconciliation fields on the resource object and corresponding reconciliation form field mapping on the process definition. Delete old default reconciliation fields, if there are any, which have mapping to the process form fields that are not retained as part of upgrade.
 3. Verify that upgrade process has retained all customizations, for example, customizations on Resource Object, Process definition, and Process Form.
 4. After the upgrade, contents of existing and new lookup definitions are merged. In these lookup definitions, you must manually delete entries that are not required.
 5. Run the Lookup reconciliation again. The old lookup reconciliation data will be available in the Lookups after upgrade. Re-running the Lookups is required if there is a change in the format for the lookup values. Refer the specific connector guide for more details about lookup reconciliation.
 6. Recalculate statistics and re-create indexes and other database objects that are removed or made invalid by the upgrade process. For more information, see Oracle Identity Manager Database guide.
 7. Check adapters status related to the connectors. If the adapters are not compiled, then you must compile them.
 8. Verify that the custom parameters are available after upgrade. Custom Scheduled Task parameters are retained as part of upgrade process. Modify the scheduled task to add the parameter if it is not available after upgrade.
 9. If there are any change in Resource object names the user need to verify all the Approval Policies associated with the Resources to modify the Resource name to the new Resource name.
 10. Verify if there are any changes in the new request dataset shipped with the connector. If yes, then delete the existing request dataset for the resource from MDS. Modify the new request dataset for any customization and import the new dataset to MDS. See "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about importing and exporting data to and from MDS.

12.8.6 Procedure to Upgrade a 9.x Connector Version to an ICF Based Connector

ICF based Connector provides LCM as a new feature that uses Connector Installer to import the connector, where as 9.x connector uses Deployment Manager to import definitions of the objects that constitute a connector. Since LCM offers a more broader and richer feature in installing and/or managing a connector than Deployment Manager, it is recommended to use only Connector installer for Oracle Identity Manager 11g connectors installation and/or management.

To upgrade a 9x connector version to a ICF based connector:

1. Delete all the existing jar files such as Javataasks, ScheduleTask, and ThirdParty jars related to the 9x connector except for the Common.jar file.
2. Download Common.jar and extract its MANIFEST.MF. Compare this version of MANIFEST.MF with the version in MANIFEST.MF of the Common.jar that is available as part of ICF based connectors distribution bundle. Retain/Upload

(using UploadJars utility) Common.jar in Oracle Identity Manager database that has higher version.

3. Manually upload all the jars present in the "lib" folder of the ICF based connector distribution bundle using the UploadJars utility in Oracle Identity Manager database (available under *OIM_HOME*/server/bin).
4. Explode the connector bundle (with naming convention "org.identityconnectors.*") in some temporary folder. Make a folder named "lib" in the same temporary folder and copy all the third party libraries to that folder.
5. Retain MANIFEST.MF from the above exploded bundle.
6. Repackage the connector with the same name and with the same MANIFEST.MF that was being retained. Now, the repackaged connector bundle will also be having third party libraries.
7. Upload the repackaged connector in Oracle Identity Manager database with jar type as "ICFBundle".
8. Delete the temporary folder created in Step 4.
9. Upgrade the connector by following the upgrade process
10. Purge cache or restart the server.

12.9 Uninstalling Connectors

WARNING: This utility is specifically created for use in development environments. It should not be used in a production environment, because the utility deletes data from the Oracle Identity Manager database directly and is therefore meant to be used only in development/staging environments.

Connector uninstall utility deletes the data related to the connector chosen for uninstall from Oracle Identity Manager Database. It deletes all the account related data associated with resource objects of the connector.

This utility does not delete:

- The actual user account from the target system
- Identities from Oracle Identity Manager although the users are brought from trusted source to Oracle Identity Manager through trusted reconciliation
- Audit data
- Archival data

Connector uninstall utility does not validate and notify the user if there is any object dependency present. For example, while uninstalling a Microsoft Active Directory (AD) connector, it does not validate if a dependent connector, such as Microsoft Exchange connector, already exists or not. Before uninstalling a connector, you must check if there are any other connectors dependent on the connector. If there are any, then the connector must not be uninstalled because this will affect the functionality of the dependent connectors. You must uninstall all the dependent connectors before uninstalling the base connector.

This section discusses the following topics:

- [Use Cases Supported by the Uninstall Connectors Utility](#)

- [Overview of the Connector Uninstall Process](#)
- [Setting Up the Uninstall Connector Utility](#)
- [Uninstalling Connectors and Removing Connector Objects](#)

12.9.1 Use Cases Supported by the Uninstall Connectors Utility

The following use cases are supported by the Uninstall Connectors utility:

- A target system that has been decommissioned, and you want to uninstall the connector that was used to link that target system with Oracle Identity Manager.
- Instead of directly upgrading to the latest release of a connector, you want to uninstall the earlier release and then perform a fresh installation of the latest release.
- You want to remove an individual connector object from the Oracle Identity Manager database. For example, you had created a resource object in Oracle Identity Manager to represent the Intern user type defined in your target system. This user type has been removed from the target system, and you now want to remove the resource object from Oracle Identity Manager.

The Uninstall Connectors utility supports independent deletion of following connector artifacts:

- Adapters
- Lookup definitions
- Resource objects
- Scheduled tasks

12.9.2 Overview of the Connector Uninstall Process

When you run the Uninstall Connectors utility, the utility performs the following steps before deleting the resource objects of the connector:

1. Checks if there are any access policies associated with the resource objects of the connector. If there are any access policies present, then the utility displays the list of access policies associated with the resource object and prompts you to modify the access policy and terminates with no data deletion. The access policy should be modified to remove the resource object from it. If the access policy is associated with only one resource object, then you need to create a dummy resource object, assign it to the access policy and then proceed with the removal of resource object from the access policy.
2. Closes all requests associated with the resource objects.
3. Displays list of request templates that are used while creating requests that are associated with the resource objects. The request templates are generic in nature, therefore the utility does not delete request templates. It prompts a message recommending you to delete/modify these templates as the resource objects would be deleted from Oracle Identity Manager. If the request template is associated with the resource object, then the request template needs to be modified to remove the resource name. If the request template is created for this resource object only, then you can delete the request template.
4. Displays the list of attestation processes which are associated with the resource objects. Attestation processes are generic in nature, therefore the utility does not delete attestation processes from Oracle Identity Manager. It prompts you to

modify these processes as the resource objects would be deleted from Oracle Identity Manager.

5. Deletes only the operational level approval policies, which are associated with the resource object. The utility does not delete or modify request level approval policies and other operational level approval policies that are not associated with the resource object.

The following objects that constitute the connector are dropped from the Oracle Identity Manager database.

1. Resource object and objects related to the resource object.
 - a. Entitlement assignment, entitlement assignment history, and entitlement data
 - b. Tasks and task history associated with any provisioning process linked to the resource object
 - c. Process forms associated with the resource object
 - d. Process instance and object instances associated with the resource object
 - e. Reconciliation events and data associated with the resource object
 - f. Attestation event data for the resource object
 - g. Requests and request data associated with the resource object
 - h. E-mail definitions for the resource object
 - i. Entitlements associated with the resource object
 - j. Regular rules associated with the resource object
 - k. Reconciliation owner matching rules for the resource object
 - l. Reconciliation action rules for the resource object
 - m. Status codes corresponding to this resource object
 - n. Reconciliation process mappings for the resource object
 - o. Reconciliation object fields for the resource object
 - p. Request dataset to process form mappings for the resource object.
 - q. Object dependency tables for parent and child forms for the resource object
 - r. Resource object for organization
 - s. Process determination rules associated with the resource object
 - t. Password policy rules associated with the resource object
 - u. IT resource instances that are associated with IT resource types defined on forms that are linked to provisioning processes. If there is any default IT resource instance, they will not be deleted, for example, IT resource instance of Remote Manager
 - v. Process instances and resource object instances
 - w. Tasks associated with the provisioning processes
 - x. The actual object and process, parent and child tables associated with the resource object.
2. Scheduled tasks and scheduled jobs
3. Adapters/Event Handlers

4. Lookup definitions

12.9.3 Setting Up the Uninstall Connector Utility

To set up the Uninstall Connector utility:

- Files that constitute the Uninstall Connector utility are viable in *OIM_HOME/server/bin* directory. These files are as follows:
 - ConnectorUninstall.properties
 - uninstallConnector.bat
 - uninstallConnector.sh

12.9.4 Uninstalling Connectors and Removing Connector Objects

Depending on your requirements, you can use the Uninstall Connectors utility to perform any of the following tasks:

- [Uninstalling a Connector](#)
- [Removing Adapters, Lookup Definitions, Resource Objects, and Scheduled Tasks](#)

The following section provides detailed instructions on using the ConnectorUninstall script to delete connector objects from the Oracle Identity Manager database. Each of the earlier sections provides a link to this section.

- [Running the Script to Uninstall Connectors and Connector Objects](#)

12.9.4.1 Uninstalling a Connector

Caution: It is strongly recommended that Oracle Identity Manager is idle and it is not available for any operations. You must ensure that:

- There are no operations on Oracle Identity Manager while using uninstalling connector or connector objects
 - All scheduled tasks are disabled and there are no asynchronous messages pending for processing such as audit messages, offline provisioning messages, offline task messages, requests scheduled for future and so on.
-
-

You can use the ConnectorUninstall script to uninstall a connector. When you run the script, all objects that form part of the connector and all the resource data that was collected through the connector are deleted from the database.

Note: Before running the uninstall utility:

- You cannot use uninstall utility on production database.
 - You cannot delete data that are already archived.
 - You must ensure that you have the latest Oracle Identity Manager schema and MDS backup, which will help to restore if uninstall utility does not complete successfully.
 - You must ensure that your UNDO tablespace is sized properly. This is required if your development/test environment has significant amount of data to be deleted.
-
-

As mentioned earlier in this guide, when a connector is defined, an entry is created for the connector in the Oracle Identity Manager database. This entry also includes the contents of the connector XML. When you choose to uninstall a connector, the utility identifies the connectors objects to be dropped by parsing the connector XML contents.

Warning:

- Connector uninstall collects all the objects information from the connector XML, which is created while installing or defining a connector. If an additional object, which is not related to this connector is added while defining the connector, uninstall would delete that too. For example, while defining AD connector, if user adds a system lookup or lookup related to other connector, uninstall would delete that lookup.
 - Ensure that only the connector specific objects are added while defining a connector.
-
-

See "[Running the Script to Uninstall Connectors and Connector Objects](#)" on page 12-71 for the procedure.

12.9.4.2 Removing Adapters, Lookup Definitions, Resource Objects, and Scheduled Tasks

Caution: It is strongly recommended that Oracle Identity Manager is idle and it is not available for any operations. You must ensure that:

- there are no operations on Oracle Identity Manager while using uninstalling connector or connector objects
 - all scheduled tasks are disabled and there are no asynchronous messages pending for processing such as audit messages, offline provisioning messages, offline task messages, requests scheduled for future and so on.
-
-

You can use the ConnectorUninstall script to remove an adapter, lookup definition, resource object, or scheduled task. Only the object that you specify is removed from Oracle Identity Manager.

12.9.4.3 Running the Script to Uninstall Connectors and Connector Objects

Running the script to uninstall connectors and connector objects includes the following procedures:

- [Preuninstall](#)
- [Uninstall](#)
- [Postuninstall](#)

12.9.4.3.1 Preuninstall

Note: Before executing the uninstall, you must ensure that all scheduled tasks are disabled.

Before Uninstalling the connector, you must:

1. Create a backup of Oracle Identity Manager database so that if something goes wrong during uninstalling, then the data can be restored. See Oracle Identity Manager Database documentation for details about creating database backup.
2. Create Oracle Identity Manager metadata (MDS) backup.
3. Ensure that there are no operations on Oracle Identity Manager until the Uninstall utility is completed. Oracle Identity Manager and SOA servers should be up and running.
4. Ensure that all the JMS messages are processed.

12.9.4.3.2 Uninstall To run the ConnectorUninstall script for uninstalling the connector:

1. Set values in the properties file used by the script.

Note: If you provide ConnectorName and Release along with ObjectType and ObjectValues, then deletion of ObjectValues will be performed by the utility and the Connector information will be skipped.

The ConnectorUninstall.properties file is a viable in *OIM_HOME/server/bin*. This file contains information that is used by the script for deleting connector objects.

Open the properties file in a text editor, and then set values for the following properties:

- DatabaseURL: Enter the JDBC URL for the Oracle Identity Manager database in the following format:

```
jdbc:oracle:thin:@HOST_NAME:DATABASE_PORT:DATABASE_NAME/ORACLE_SID
```

For example: jdbc:oracle:thin:@localhost:1521:orcl

- DBUserName: Enter the user name of an Oracle Identity Manager database.
- DBType: Specifies the type of database.
- LogLevel: Enter one of the following as the log level: DEBUG, WARN, INFO, or ERROR.
- Location: Enter the directory location where you want to have all the log files generated by the Uninstall utility.

If the Uninstall utility completes successfully, then the ConnectorUninstall.log file, along with <ResourceObject>.log files are generated.

If the Uninstall utility fails, then the ConnectorUninstall.log file along with the ConnectorUninstall_Error.log file are generated.

Note: If the uninstall utility fails with errors, then check the ConnectorUninstall.log and ConnectorUninstall_Error.log and take suitable action. Then, run the uninstall utility again.

For example, if the Uninstall utility of ActiveDirectory Connector succeeds, then the following logs will be generated:

- ConnectorUninstall.log
- AD User.log
- AD Group.log
- AD Organization Unit.log
- AD User Trusted.log

If the Uninstall utility of ActiveDirectory Connector Fails, then the following logs will be generated:

- ConnectorUninstall.log
 - ConnectorUninstall_Error.log
- ConnectorName: The value that you set for this property depends on your requirement. If you want to delete a specific connector, then enter the name of the connector. The name that you enter must be the same as the name shown in the search results displayed through the Manage Connector feature. For example, enter *Active Directory* if you want to delete the Microsoft Active Directory connector.
 - Release: The value that you set for this property depends on your requirement. If you want to delete a specific connector, then enter the release number of the connector. The release number that you enter must be the same as the release number shown in the search results displayed through the Manage Connector feature. For example, enter *9.1.0.1* if you want to delete the Microsoft Active Directory 9.1.0.1 connector.
 - ObjectType: The value that you set for this property depends on your requirement:
 - If you want to uninstall a connector, then ensure that the ObjectType property is not assigned a value.
 - If you want to delete adapters, lookup definitions, resource objects, or scheduled task, then enter *Adapter*, *Lookup*, *ResourceObject*, or *ScheduledTask* respectively.

Example: *ResourceObject*
 - ObjectValues: Enter a semicolon-separated list of object values.

Example: *AD User; AD Group*
2. In a command window, change to the *OIM_HOME/server/bin* directory and then run the script, *sh uninstallConnector.sh* (or bat file).

Note: Before running this utility, set *APP_SERVER*, *OIM_ORACLE_HOME*, *JAVA_HOME*, *MW_HOME*, *WL_HOME*, and *DOMAIN_HOME*.

While the script runs, logs will be generated at the location provided.

After you run the utility, you will be prompted to enter following information:

- a. Oracle Identity Manager Database Password
- b. Oracle Identity Manager Administrator Name
- c. Oracle Identity Manager Administrator Password

- d. Oracle Identity Manager Server t3 URL
- e. Confirmation for the deletion of the connector/object(s)

12.9.4.3.3 Postuninstall After uninstalling the connector, you must perform the following steps:

1. Use DeleteJars utility for deleting the jars associated with the connector from Oracle Identity Manager database.
2. Use DeleteResourceBundles utility for deleting all resources that are associated with the connector from Oracle Identity Manager database.
3. Revisit the log, look for the following information and perform the steps mentioned for each of it:
 - a. The list of request templates: Delete/modify these templates as the resource objects, which used these templates are now deleted.
 - b. The list of attestation processes: Delete/modify these attestation process as the resource objects, which used these attestation processes are now deleted.
 - c. Modify request and approval policies manually to delete the resource object names that are cleaned by the uninstall utility.
 - d. As the part of connector uninstall, the approval processes (Approval workflow/SOA composites) are not deleted. If the approval processes are generic, then you need to modify them if they have association with the deleted resource objects.
4. Recalculate statistics and re-create indexes and other database objects that are removed by the connector uninstall utility. For more information, see "Performance Tuning and Best Practices".
5. Restart Oracle Identity Manager, or use PurgeCache utility to purge the Cache.
See Oracle Fusion Middleware Performance and Tuning Guide for information about purging the cache.

12.10 Troubleshooting Connector Management Issues

Problem

Using Oracle Identity Manager 11g Release 2 (11.1.2.1.0), you can configure a cloned Active Directory (AD) Release 9.x connector for target AD and run an AD trusted source reconciliation to create users in Oracle Identity Manager. After the user is created in Oracle Identity Manager, when you run the target resource reconciliation for AD, the user details are linked in the Accounts tab. However the Detail Information tab displays a blank page. When you check the Application Instances section in Oracle Identity System Administration and search and open the relevant application instance, no form is found associated with the application instance.

Solution

Create a new set of forms for each application instance.

Managing Reconciliation

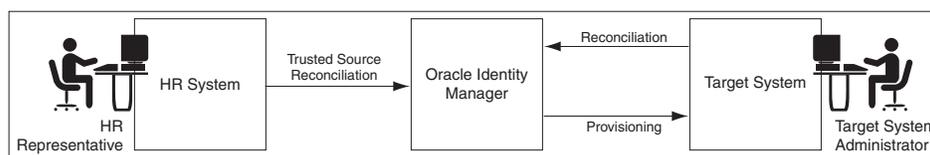
Reconciliation is the process by which operations, such as user creation, modification, or deletion, started on the target system are communicated to Oracle Identity Manager. The reconciliation process compares the entries in Oracle Identity Manager repository and the target system repository, determines the difference between the two repositories, and applies the latest changes to Oracle Identity Manager repository.

Reconciliation of roles, role memberships, and role hierarchy changes are handled as separate reconciliation events. Ideally role events must be submitted first and then only the membership events in order to avoid race conditions. For race conditions, the automatic retry logic allows the reconciliation engine to handle it.

See Also: "Handling of Race Conditions" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about race conditions

Figure 13–1 shows that provisioning and reconciliation involve synchronization from Oracle Identity Manager to the target system or from the target system to Oracle Identity Manager. Provisioning and reconciliation enable the provisioning system to build the managed identities in the target system as well as replicate the managed identities as they already exist in the target system.

Figure 13–1 Provisioning and Reconciliation



In Figure 13–1, a user is created by the HR representative when a new employee joins. The user is reconciled to Oracle Identity Manager by trusted source reconciliation. When the user is created in Oracle Identity Manager, the account for the user is provisioned in the target system. In the target system, the target system administrator can make changes in the account, which must be reconciled to Oracle Identity Manager.

In terms of data flow, provisioning provides the outward flow from the provisioning system by using a push model, in which the provisioning system indicates the changes to be made to the target system. Reconciliation provides the inward flow into the provisioning system by using either a push or a pull model, by which the provisioning system finds out about any activity on the target system.

The reconciliation process involves generation of events to be applied to Oracle Identity Manager. These events reflect atomic changes in the target system, and contain the data that has changed, the type of change, along with other information. The reconciliation events that are generated consequently because of changes occurring in the target system are managed by using the Event Management section in Oracle Identity System Administration, which addresses these event management needs. See "[Managing Reconciliation Events](#)" on page 13-10 for information about managing reconciliation events by using Oracle Identity System Administration.

This section consists of the following topics:

- [Types of Reconciliation](#)
- [Managing Reconciliation Events](#)

See Also: "Customizing Reconciliation" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about reconciliation features and architecture

13.1 Types of Reconciliation

Reconciliation can be of different types, as shown in [Table 13-1](#):

Table 13-1 *Types of Reconciliation*

Classification Criteria	Reconciliation Type
Object being reconciled	Based on identity being reconciled, such as user, account, role, organization, or relationship that includes role hierarchy and role membership
Mode of reconciliation	Changelog Regular
Approach used for reconciliation	Incremental reconciliation Full reconciliation

This section describes the following topics:

- [Reconciliation Based on the Object Being Reconciled](#)
- [Mode of Reconciliation](#)
- [Approach Used for Reconciliation](#)

13.1.1 Reconciliation Based on the Object Being Reconciled

Reconciliation depends on the entity object that is being reconciled. The following entities in Oracle Identity Manager are reconciled:

- **User:** A user is an identity that exists within and is managed through Oracle Identity Manager.
- **Account:** An account is granted to a user to give the user the ability to log in to Oracle Identity Manager and access Oracle Identity Manager features. At the minimum, these features involve self-service and request. An account can be granted additional privileges including the ability to define workflows and the delegated administration of various entities, such as users, organizations, and roles.

- **Organization:** An organization entity represents a logical container of entities, such as users and other organizations, that exists in Oracle Identity Manager.
- **Role:** A role is a logical grouping 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.
- **Role hierarchy:** Role hierarchy is the inheritance of the parent role to child roles. The parent role has the same permissions and privileges on the members as the inherited roles.
- **Role membership:** Role membership means that the members of the inheritor role inherit from the inherited role. See "Managing Roles" in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about membership and permission inheritance.

This section discusses the following topics:

- [Trusted Source Reconciliation](#)
- [Account Reconciliation](#)
- [Reconciliation Process Flow](#)

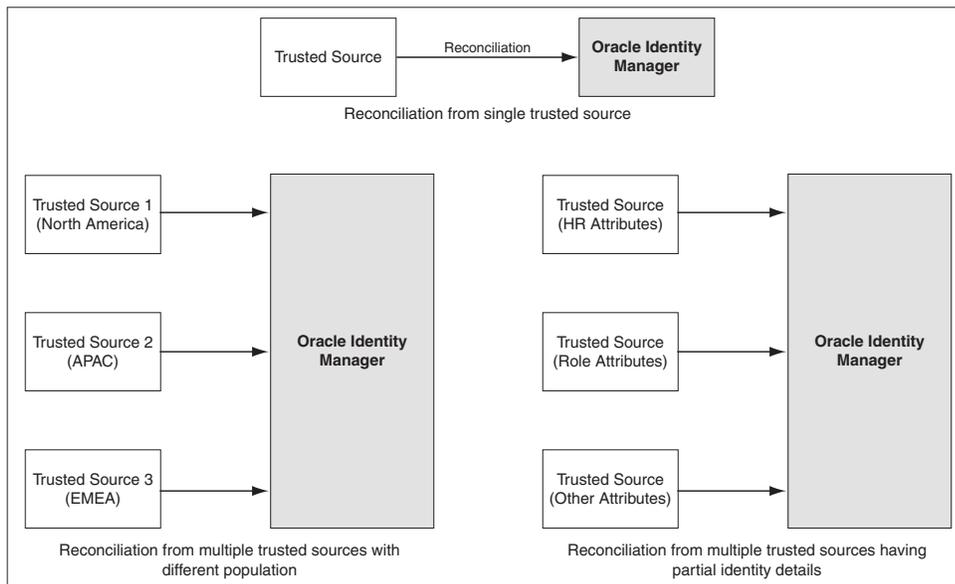
13.1.1.1 Trusted Source Reconciliation

If data is reconciled from a system that drives the *creation* of users, roles, role memberships, or role hierarchies in Oracle Identity Manager repository, then that reconciliation mode is called identity reconciliation, or authoritative source reconciliation, or trusted source reconciliation. The system that is being reconciled from is referred to as the authoritative source for the enterprise identities, and may be an HR system or a corporate directory.

Note: If the user login is not passed for trusted reconciliation, then the login handler generates the user login. The password is generated in postprocessing event handler, and notification is sent for the same. See "Customizing Reconciliation Operations" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about event handlers.

As shown in [Figure 13–2](#), the authoritative sources of identity may be more than one. The different authoritative sources may be the source of reconciliation for different categories of user identities or may be the source of reconciliation for different sets of attributes. The various events generated by the reconciliation engine are add, modify, and delete.

Figure 13–2 Trusted Source Reconciliation from Single and Multiple Authoritative Sources



In [Figure 13–2](#), trusted source reconciliation from a single authoritative source and multiple authoritative sources are shown. Creation of user entities can be reconciled from multiple authoritative sources. In addition, different attributes can be reconciled from different multiple authoritative sources. For example, the user ID and e-mail ID can be provided by an authoritative source and role attributes can be provided by another authoritative source.

Trusted source reconciliation must be followed by account reconciliation when the target system is the source for identities as well as accounts. For instance, if Active Directory is the corporate LDAP repository in which user information is stored, then the user information is reconciled from the Active Directory target system. Subsequently, the Active Directory accounts are reconciled into Oracle Identity Manager by using a different connector. Identity reconciliation occurs only from trusted sources, by using connectors specific to those trusted sources.

Note: A reconciliation connector is a component developed to reconcile identities or accounts from a specific target system. Typically, a reconciliation connector is configured to be run as a scheduled task. However, there are push-based connectors, such as the PeopleSoft HR connector, for which there is no scheduled task to trigger the reconciliation.

13.1.1.2 Account Reconciliation

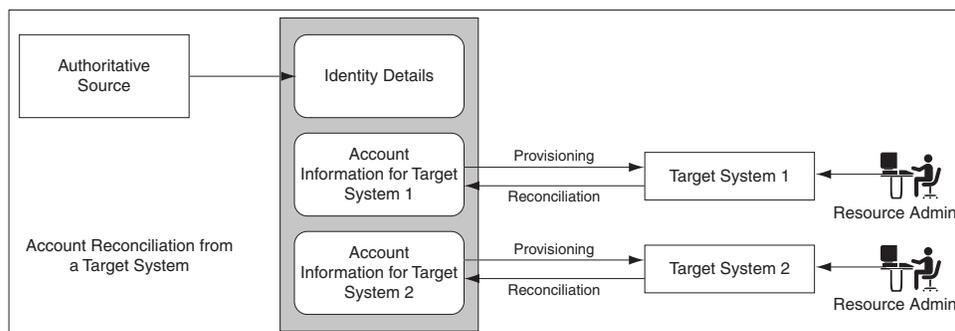
If the target system identities are accounts that get reconciled to Oracle Identity Manager, then that is target resource reconciliation or account reconciliation. This type of reconciliation is to reconcile a specific resource object that represents the target system being managed. There is always a corresponding provisioning flow for it. The identity retrieved from the target system maps to a resource object instance that has been provisioned to a user or organization.

Account reconciliation takes place in the following scenarios:

Scenario I

Identity gets created in Oracle Identity Manager from an authoritative source. The identities are provisioned with resources on the target system. Any change on the target system is reconciled with Oracle Identity Manager. [Figure 13-3](#) shows account reconciliation from a target system:

Figure 13-3 Account Reconciliation From a Target System



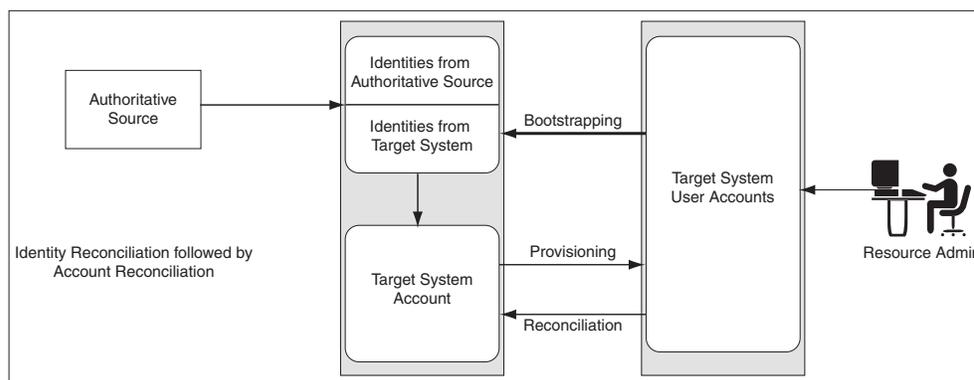
Scenario II

In this scenario, the target system initially plays the role of an authoritative source. Later it plays the role of a regular provisioning target. Following are the sequence of steps:

1. Identities are created in Oracle Identity Manager based on the target system entity details. Corresponding accounts are also created for these entities.
2. The entities are updated as provisioned entities in the target system.
3. The resource administrator at the target system makes changes to the accounts.
4. The changes made on the target system are reconciled with Oracle Identity Manager.

[Figure 13-4](#) shows identity reconciliation followed by account reconciliation:

Figure 13-4 Identity and Account Reconciliation

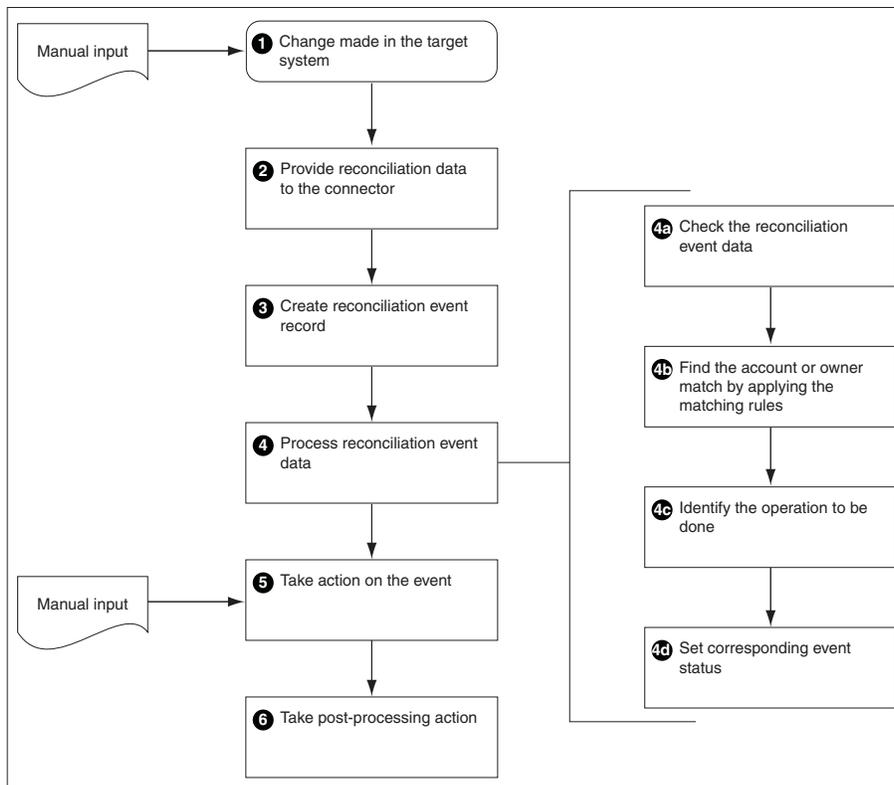


Note: When the value of the `XL.UserProfileAuditDataCollection` property is set to an audit data collection level, then the account reconciliation performs the matching in the database layer at a batch-level and performs the event action by using the provisioning APIs. This in turn triggers the audit event handlers for account reconciliation. By default, the value of this property is set to Resource Form. See "Administering System Properties" for information about system properties in Oracle Identity Manager in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

13.1.1.3 Reconciliation Process Flow

The reconciliation process flow is shown in [Figure 13-5](#):

Figure 13-5 Reconciliation Process Flow



Reconciliation process involves the following steps:

1. **Changes in the target system:** The various activities that can happen in the target system are creation, modification, or deletion of user, account, role, role membership, or role hierarchy.

Note: If you create an entity on an external system and then modify it a short time later, reconciliation processes the create entity step, but the modify entity step fails with the Creation Failed event status. This is because reconciliation cannot process a create and a modify action for the same entity in the same batch process.

However, the entity modification action can be resubmitted for reconciliation at a later time by one of the following built-in mechanisms:

- The "Automated Retry of Failed Async Task" scheduled task will run to re-process the failed events without any manual intervention. See "Automated Retry Error Handling Mechanism" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for details.
- The failed event will be re-processed if the "Manual Retry Error Handling Mechanism" is triggered. See "Manual Retry Error Handling Mechanism" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for details.

Reconciliation failure messages that are caused by processing conflicts within the same batch process should be regarded as transitory failures only.

2. **Providing reconciliation data:** When the creation, modification, or deletion event occurs, data about that event is sent to the reconciliation service by using reconciliation APIs.

Note: Reconciliation service refers to the collection of reconciliation engine, reconciliation APIs, and the associated metadata and schema.

3. **Creation of reconciliation event record:** When the data for a reconciliation event is provided to reconciliation service, a record of that event is stored in Oracle Identity Manager repository.
4. **Processing of the reconciliation event data:** The data received is then evaluated to determine the actual operation to be performed in Oracle Identity Manager based on the changes in the target system. The evaluation involves application of a specific set of rules that help in:
 - a. Identifying whether the data is for an account or for an identity that Oracle Identity Manager already has a record of
 - b. Identifying the owner of the account or identity that the data represents
 - c. Defining the context-sensitive action to be taken
 - d. Setting the status of the event at the end of evaluation and the action that the reconciliation engine must take
5. **Taking action on the event:** Based on the evaluation result of processing the reconciliation event data, the intended action is taken. The various actions can be:

Note: The actions on the event can be manually performed through the UI, or they can be automatic actions.

- Creating a new account and associating with proper owner identity
- Updating the matched account
- Deleting the matched account
- Creating a new user in Oracle Identity Manager
- Modifying an existing user in Oracle Identity Manager
- Deleting an existing user
- Enabling and disabling account status by updating the status attribute
- Enabling or disabling user
- Creating, updating, or deleting role
- Creating or deleting role membership
- Creating or deleting role hierarchy

See Also: "Reconciliation Engine" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about role membership and role hierarchy

6. **Follow up actions triggered by the reconciliation event:** After the action is taken, follow up tasks can be started based on the reconciliation event. An example of follow up tasks or post-processing task is creating a request to provision a resource, such as a laptop computer, after a user creation event.

13.1.2 Mode of Reconciliation

The mode of reconciliation is either pull or push that depends on the connector used. Most connectors, such as Active Directory, use the pull model. For the pull model, a pull reconciliation task is scheduled in the IAM Scheduler. The task runs at recurring intervals.

See Also: "[Managing the Scheduler](#)" on page 15-1 for information about the IAM Scheduler

Typically, the pull-based reconciliation connectors submit the reconciliation events within a scheduled task. Every time the scheduled task runs, a new reconciliation run is triggered and the reconciliation events are created in batches. When the batch size is met, the batch is submitted for processing. At the end of the scheduled task, an end of job listener is triggered, which submits all the batches whose size is not met.

Other reconciliation connectors, such as the PeopleSoft connector, use a push model. The connector comprises of an HTTP listener that detects any asynchronous messages issued by PeopleSoft. On receiving a message, the listener submits reconciliation events by calling the reconciliation API. The events are processed by the reconciliation engine in batches when the batch size is met. For batches where batch size is not met, a scheduled task runs periodically and submits the batches for reconciliation processing.

Pull or push model is used based on the nature of the target system and how the changes can be detected in the target system. But irrespective of the push or pull model being used, reconciliation is performed by using a scheduled task that runs in the IAM Scheduler.

Note: You can also create the reconciliation events directly by using the reconciliation APIs.

Changelog reconciliation is the default reconciliation mode. In this mode, only changed attributes are reconciled. Unspecified fields are ignored. You typically use the Changelog reconciliation mode when a connector is aware of the list of changed attributes. Along with the changed attributes, Oracle Identity Manager needs a list of required fields for matching. The Changelog reconciliation mode was supported in previous Oracle Identity Manager releases, so all connectors work in this mode.

Regular reconciliation is a new reconciliation mode, introduced in this release, where the reconciliation engine completely replaces the existing snapshot of the entity. You typically use this reconciliation mode when the connector cannot determine which attributes have changed, and therefore, sends an entire snapshot of the entity. For new connectors, you can specify this mode when performing a full reconciliation. Using regular reconciliation mode results in better performance because the events are processed faster.

Note: The mode of reconciliation depends on the connector implementation. For information about connector implementation, see "Connector for Reconciliation" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Table 13–2 lists the differences between regular and changelog reconciliation modes:

Table 13–2 Regular and Changelog Reconciliation Modes

Regular	Changelog
Must pass a full set of mapped attributes	Must pass a subset of mapped attributes that are required by the specific profile and used by matching a rule
Performs better in batch processing mode (no difference in performance while in single event processing mode)	
Creates and updates all fields	Creates and updates only specified fields, and all other fields remain unchanged

See Also: "Changing the Profile Mode" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about changing the reconciliation mode

13.1.3 Approach Used for Reconciliation

When you run reconciliation for the first time on a target system, all users and accounts on the target system are reconciled into Oracle Identity Manager by default. This is called full reconciliation. To perform full reconciliation, the connector sends the reconciliation events for each entity in the target system. The reconciliation engine processes the events as create or update events depending on whether or not the entity already exists in Oracle Identity Manager. The connector also identifies all the deleted entries and sends the deletion events to Oracle Identity Manager.

At the end of full reconciliation, the connector typically sets the last execution time parameter to the time when the reconciliation run ends. For the next reconciliation run,

only the entity records that have been added, modified, or deleted after the first reconciliation run ended are fetched for reconciliation. This is called incremental reconciliation.

You can manually switch from incremental reconciliation to full reconciliation by setting the value of the timestamp IT resource parameter to 0.

13.2 Managing Reconciliation Events

The reconciliation process involves generation of events to be applied to Oracle Identity Manager. These events reflect atomic changes in the target system, and contain the data that has changed, the type of change, along with other information. The reconciliation events that are generated as a result of changes occurring in the target system must be managed in such a way that they meet various business requirements. The Event Management section in the Oracle Identity Manager Advanced Administration addresses these event management requirements.

You can manage reconciliation events by using the Event Management section, which lets you query the events stored in various ways and display all event data. The events are always displayed in the same form, which is on the Event Details page. You can run custom queries for the events through the Advanced Search feature. It also allows you to perform any necessary action to resolve event issues.

Events are generated by reconciliation runs. These reconciliation runs are scheduled to run by using the Oracle Identity Manager Scheduler.

See Also: ["Managing the Scheduler"](#) on page 15-1" for detailed information about the scheduler

You can perform the following event management tasks by using the Event Management section of Oracle Identity Manager Advanced Administration:

- [Searching Events](#)
- [Displaying Event Details](#)
- [Determining Event Actions](#)
- [Re-evaluating Events](#)
- [Closing Events](#)
- [Linking Reconciliation Events](#)

13.2.1 Searching Events

You can display a summary of reconciliation events by performing the following types of search:

- [Performing a Simple Search for Events](#)
- [Performing an Advanced Search for Events](#)

13.2.1.1 Performing a Simple Search for Events

To perform a simple search for events:

1. Login to Oracle Identity System Administration.
2. In the left pane, under Event Management, click **Reconciliation**. The Advanced Administration is displayed with the Reconciliation section in the Event Management tab active.

3. In the left pane, enter a search criterion in the Search field. You can include wildcard characters (*) in your search criterion.

The simple search takes one argument. The text arguments are searched in the following event fields:

- Event ID
- Profile Name
- Key Fields

Note: In simple search, you cannot perform the search by event dates.

4. Click the icon next to the Search field. The events that match your search criterion is displayed in the search results table.

The search fetches all rows for which the aforementioned attributes contains the string specified in the Search field. The search result displays the Event ID, Profile Name, and Key Fields columns. The Event ID column displays the event ID. The IDs are sorted as integers, not strings. The Profile Name column displays the name of the reconciliation profile. Key field is an attribute that uniquely identifies a row of data. In reconciliation, some attributes are flagged as Key in the profile. These fields are displayed in the Key Fields column.

Note: Simple Search is paginated, meaning it only displays search results 64 rows at a time. This is to improve performance. Scrolling down past the 64th row in the UI triggers another page fetched from the database and so on for every 64 rows beyond that.

13.2.1.2 Performing an Advanced Search for Events

The advanced search takes multiple arguments and lets you fine-tune the list of events. To perform an advanced search for events:

1. In the left pane of the Reconciliation section, click **Advanced Search**. The Search: Events page is displayed.
2. 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.
3. In the Event ID field, enter the event ID that you want to search. You can use wildcard characters (*) in your search criteria. Select a search condition in the list adjacent to the Event ID field.
4. Specify search arguments in the other fields displayed in the Search: Events page. [Table 13-3](#) lists the fields in the Search: events page.

Table 13–3 Advanced Search Fields

Field	Description
Event Id	The event ID. The IDs are sorted as integers, not strings.
Resource Name	The name of the resource object representing the target system the event originates from.
Current Status	A string representing the current state of the event.
Type	The type of operation performed by the event: regular (add or modify) or delete.
Profile Name	The name of the reconciliation profile this event pertains to. See Also: "Reconciliation Profile" in the <i>Oracle Fusion Middleware User's Guide for Oracle Identity Manager</i> for information about reconciliation profile
Entity	The type of Oracle Identity Manager entity this event pertains to. Can be either user, account, role, role grant, or role hierarchy.
Start Date	Oldest event creation date to search for.
End Date	Most recent event creation date to search for.
Linked User Login	A string representing the login ID of the user linked to the event.
Key Fields	The fields flagged as key fields in the reconciliation profile that uniquely identifies rows of data.

5. Click **Search**. The search results are displayed, which consists of the Event ID, Resource Name, Entity, Event Status, Type, Profile Name, Job ID, Key Fields, and Date columns.

From the search results, you can perform event bulk actions, such as close and re-evaluate, and also display the details of any specific event.

If you want to search for events with LDAP profile, use the following LDAP profiles in your search:

Object	Profile
User	LDAPUser
Role	LDAPRole
Role Membership	LDAPRoleMembership
Role Hierarchy	LDAPRoleHierarchy

13.2.2 Displaying Event Details

To display the details pertaining to an event:

- In the left pane of the Oracle Identity Manager Advanced Administration, from the list of events, select an event whose details you want to display.
- From the advanced search result table, click an event in the Event ID column.
- From the Actions list, select **Lookup**. The Event Details page is displayed. The fields in the Event Details page change dynamically based on the event type and event status. Alternatively, you can select an event from the Event Summary on the right pane, and click the magnifying glass icon for lookup to open the Event Details page.

The data in the Event Details page is displayed in the following sections:

- **Event:** This section displays the information about the event, such as event ID, whether the event type is User or Account, the time when the event was created, the reconciliation run ID, resource name, the profile name, and the key field values. Reconciliation can use several key fields, and the key field values are shown separated by commas.
- **Linked To:** This section shows that the event is linked to a user or account. It displays the user or account ID to which the event is linked, the account description (if any), and the type of linking, such as rule-based linking or manual linking. Rule-based linking means that the reconciliation engine has performed the linking. Manual linking means that the administrator performs the linking manually.
- **Notes:** The reconciliation engine adds notes where appropriate. For example, when there is a 'Data Validation Fail', the engine adds a note explaining the reason. This is a read-only field and is blank if no notes are attached to the event.
- **Reconciliation Data:** This table displays the reconciliation event data. This shows the attribute name, attribute value, and Oracle Identity Manager mapped field. It also shows the child data of the event, if any. The reconciliation data displays the last name, first name, hiring date, user ID, and the IT resource name.

If there are attributes with multi-language support, then these attribute values are also displayed in a separate table similar to child data.
- **Matched Accounts:** This table displays the accounts that are matched. The columns in the Matched Accounts table are listed in [Table 13-4](#):

Table 13-4 Columns in the Matched Accounts Table

Column	Description
Account ID	The account ID of the matched account
Orc Key	An internal key that is stored in the ORC table. This key indicated if the event is matched to a user or an account.
Descriptor Field	A description that is associated to the account
Login ID	The user login ID corresponding to the user ID displayed for user events.
Account Owner Name	A string comprising of the first name and last name and the login ID of the user who owns the account. The event pertains to this account.
Account Owner Type	The type of account owner, such as user.

- **Matched Users:** This table shows the user matches found by the reconciliation engine. For a multiple match, the linked user is not shown in this table.
- **History:** This table shows the operations that took place for this event from event creation and data validation to account matching and whether the update was successful. The columns in the History table are listed in [Table 13-5](#):

Table 13-5 Columns in the History Table

Column	Description
Status	Event status at the given date and time.
Action	Action performed on the event at the given date and time.
Action Performed by User	The ID and login ID of the user who performed the cited action. The engine uses the Default IAM Admin id: xelsysadm, ID = 1.

Table 13–5 (Cont.) Columns in the History Table

Column	Description
Date and Time	Date and time of the cited action.
Notes	Any notes attached to the event at the specified date and time.

Note: Oracle Identity Manager does not support translation of the reconciliation field names.

13.2.3 Determining Event Actions

The list of actions allowed for an event depends on the status, type, and operation of the event. [Table 13–6](#) lists the possible actions for each type and status of events.

Table 13–6 Actions for Event Status and Types

Event Status	Event Type	Possible Actions
No matches found	User	Close event
		Re-apply reconciliation rules
	Account	Create entity
		Ad-hoc linking
Users matched	User	Close event
		Re-apply reconciliation rules
		Linking
	Account	Close event
		Re-apply reconciliation rules
		Linking
Accounts matched	Account	Close event
		Re-apply reconciliation rules
		Linking
Event Received	Any	Close event

The possible actions are described in the subsequent sections.

13.2.4 Re-evaluating Events

Re-evaluating an event means reapplying the reconciliation rules on the event. Reconciliation rule refers to the matching rule used to identify the owner of an event. For instance, if you change the reconciliation rules by using Oracle Identity Manager Design Console, then you can re-evaluate the rules in the Event Management section of the Oracle Identity Manager Advanced Administration.

To re-evaluate an event:

1. From the list of events, select an event. You can select multiple event rows by pressing the Ctrl key if you want to re-evaluate multiple events at a time.

2. From the Actions list, select **Re-Evaluate Event**. The Re-Evaluate Event dialog box is displayed with the event IDs that you have selected.
3. Click **Perform**. A confirmation message is displayed stating that the reconciliation rules are successfully reapplied for the event. If the selected action fails for any event, a generic message is displayed that shows the event IDs for which bulk processing has failed. The events can then be processed one at a time.

Note:

- The preprocess validation lists the events that are valid and those that are invalid for re-evaluation. If you click Perform, then only the valid events are re-evaluated.
 - All event actions are tracked in the Event History table.
-
-

13.2.5 Closing Events

This action closes or discards the selected events, and the events are removed from any further processing queues. To close an event:

1. From the list of events, select an event.
2. From the Actions list, select **Close Event**. You can select multiple event rows by pressing the Ctrl key if you want to close multiple events at a time. The Close Event dialog box is displayed.

Note: If closing an event is not a valid option, then an error message is displayed in the Close Event dialog box.

3. In the Justification box, enter a reason to close the event.
4. Click **Perform**. A confirmation message is displayed stating that the event is closed. If the selected action fails for any event, a generic message is displayed that shows the event IDs for which bulk processing has failed. The events can then be processed one at a time.

Note:

- All event actions are tracked in the Event History table.
 - The close event operation needs a justification to be entered. Therefore, when multiple events are closed at a time by performing bulk action, all the closed events will have the same justification.
-
-

13.2.6 Linking Reconciliation Events

Oracle Identity Manager allows you to perform the following operations for linking reconciliation events:

- [Ad Hoc Linking](#)
- [Manual Linking](#)
- [Linking Orphan Accounts](#)

13.2.6.1 Ad Hoc Linking

Ad hoc linking allows you to link an event to any user or role in Oracle Identity Manager. Even if the reconciliation engine finds user matches for the events, you can use ad hoc linking to ignore those matches and select a different user. This allows you to handle exceptions resulting from error matches because the reconciliation matching rules may not work correctly all the time.

This action lets you link an event to any entity other than the already matched entities. In other words, instead of selecting a row from the Matched Users table, you can select another user to link with the event.

To create an ad hoc link for an event:

1. In the Event Details page, from the Actions list, select **Ad Hoc Link**. The Ad Hoc Link dialog box is displayed.
2. Perform a user search by specifying a search criterion.
3. Select a user from the search result, and click **Perform**. A confirmation message is displayed that states that the ad hoc linking with the event is successful.

13.2.6.2 Manual Linking

When a reconciliation event has multiple matches, each match is displayed on the Matched Accounts (for account entity) or Matched Users (for user entity) tab of the Event Details page. You can manually select any match out of all the matches found by the reconciliation engine. To perform manual linking:

Note: In manual linking, you select a match from a list of matches found by the reconciliation engine instead of selecting from a list of all Oracle Identity Manager users.

1. In the Event Details page, select a row from the table that lists all the matches found by the reconciliation engine.
2. Click **Link**. A message is displayed asking for confirmation.
3. Click OK to confirm.

13.2.6.3 Linking Orphan Accounts

Orphan accounts refer to accounts in the target system for which there is no corresponding user that exists in Oracle Identity Manager.

You can resolve events for orphan accounts for which the events either have no user match in Oracle Identity Manager, or several users are found for the match. You can therefore perform any one of the following:

- Re-create the user in Oracle Identity Manager
- Trigger a provisioning process to delete the user or account from the target system
- Perform ad hoc or manual linking

The Event Management section allows you to resolve orphan accounts by selecting the correct user for the match in the following scenarios:

- [For an Event With Multiple Matches](#)
- [For an Event With No Matches](#)

13.2.6.3.1 For an Event With Multiple Matches When several users are matched to the event data by the reconciliation engine, you must select the right user by using ad hoc or manual linking.

For information about ad hoc linking, see "[Ad Hoc Linking](#)" on page 13-16.

For information about manual linking, see "[Manual Linking](#)" on page 13-16.

13.2.6.3.2 For an Event With No Matches When no matches are found for an event, you can either trigger an entity creation, or select an Oracle Identity Manager entity to link to the event. For information about how to select and Oracle Identity Manager entity to link to an event, see "[Ad Hoc Linking](#)" on page 13-16.

Part VI

Managing Infrastructure Services

This part describes infrastructure services in Oracle Identity Manager.

It contains the following chapters:

- [Chapter 14, "Managing Notification Service"](#)
- [Chapter 15, "Managing the Scheduler"](#)
- [Chapter 16, "Managing System Properties"](#)

Managing Notification Service

Information about events occurring in Oracle Identity Manager are required to be sent to various users, such as requesters, beneficiaries, or administrators. This information about events is sent by using the notification service in the form of notification e-mail messages. The notification service allows you to perform all notification-related operations in Oracle Identity Manager.

An event is an operation that occurs in Oracle Identity Manager, such as user creation, request initiation, or any custom event created by the user. The events are generated as part of business operations or via generation of errors. Event definition is the metadata that describes the event. To define metadata for events, it is important to identify all event types supported by a functional component. For example, as a part of the scheduler component, metadata can be defined for scheduled job execution failed and shutting down of the scheduler. Every time a job fails or the scheduler is shut down, the events are raised and notifications associated with that event are sent.

The data available in the event is used to create the content of the notification. The different parameters defined for an event help the system to select the appropriate notification template. The different parameters that are defined for an event help the system decide which event variables can be made available at template design time.

A notification template is used to send notifications. These templates contain variables that refer to available data to provide more context to the notifications. The channel through which a notification is sent is known as the notification provider. Examples of such channels are e-mail, Instant Messaging (IM), Short Message Service (SMS), and voice. To use these notification providers, Oracle Identity Manager uses Oracle User Messaging Service (UMS).

At the backend, the notification engine is responsible for generating the notification, and utilizing the notification provider to send the notification.

The notification templates and notification providers are described in the following sections:

- [Managing Notification Providers](#)
- [Managing Notification Templates](#)
- [Configuring Default Email Provider](#)
- [Configuring SOA Email Notification](#)
- [Disabling Email Notification](#)
- [Testing Notification Configuration](#)

14.1 Managing Notification Providers

Managing notification providers is described in the following sections:

- [Using UMS for Notification](#)
- [Using SMTP for Notification](#)
- [Using SOA Composite for Notification](#)
- [Configuring Custom Notification Provider](#)
- [Disabling and Enabling Notification Providers](#)

14.1.1 Using UMS for Notification

UMS offers various capabilities for sending notifications. These capabilities are used by Oracle Identity Manager notification engine to achieve the following:

- **Support for a variety of messaging channels:** Messages can be sent and received through e-mail, IM, SMS, and voice. Oracle Identity Manager 11g Release 2 (11.1.2.1.0) supports sending notification messages only via e-mail.
- **Robust message delivery:** UMS keeps track of delivery status information provided by messaging gateways, and makes this information available to applications so that they can respond to a failed delivery.

This section contains the following topics:

- [Enabling Oracle Identity Manager to Use UMS for Notification](#)
- [Applying OWSM Policy to the UMS Web Service](#)

14.1.1.1 Enabling Oracle Identity Manager to Use UMS for Notification

To enable Oracle Identity Manager to use UMS for notification:

1. Configure UMS properties by using the `UMSEmailNotificationProviderMBean` MBean. To do so:
 - a. Log in to Oracle Enterprise Manager.
 - b. Click **Application Deployments**.
 - c. Right-click **OIMAppMetadata(11.1.2.0.0)(oim_server_name)**, and select **System MBean Browser**.
 - d. In the System MBean Browser, navigate to **Application Defined MBeans, oracle.iam, Server: oim_server_name, Application: oim, IAMAppRuntimeMBean**, and select **UMSEmailNotificationProviderMBean**.
 - e. In the Attributes tab, enter the following information:
 - * **Policies:** The Messaging UMS web service is used for integration between Oracle Identity Manager and UMS. This Web Service can be secured via Oracle Web Services Manager (OWSM) policy. If OWSM policy is attached to the Messaging web service at server level, then provide the name of the corresponding client side policy. Otherwise, leave the field blank. For example, if `oracle/wss11_username_token_with_message_protection_service_policy` is applied at the server level, then provide the corresponding client policy name here, such as `oracle/wss11_username_token_with_message_protection_client_policy`.

- * **WSUrl:** This is the URL of the UMS Web service to be started. By default, it contains the URL of the Messaging UMS web service used for integration between Oracle Identity Manager and UMS.

You can use any other SOA server, for example:

`http://SOA_HOST:SOA_PORT/ucs/messaging/webservice`

Here, replace *SOA_HOST* with the host name of the SOA server and *SOA_PORT* with the port number to connect to the SOA server.

- * **CSFKey:** This is the UMS e-mail notification provider credential store (CSF) key name. The key name is populated by default. This key is in the `oracle.wsm.security` map.

f. Click **Apply**.

2. If Oracle Identity Manager and UMS server are in different domains, then you must import the UMS public key into Oracle Identity Manager domain's keystore, and must import Oracle Identity Manager domain's public key into the UMS keystore.

See Also: "Configuring Oracle User Messaging Service" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite* for details about UMS Web service security

3. Configure the mail server. UMS uses the local LINUX mail server by default, and no configuration change is required in UMS for configuring this mail server. However, to use any other Simple Mail Transfer Protocol (SMTP) server:

- a. In Oracle Enterprise Manager, expand **User Messaging Service**, and select **usermessagingdriver-email** (*soa_server_name*).
- b. From the User Messaging Email Driver list, select **Email Driver Properties**.
- c. In the Driver-Specific Configuration section, populate the following mandatory fields:

- * **OutgoingMailServer:** The name of the SMTP server, for example, `stbeehive.oracle.com`.
- * **OutgoingMailServerPort:** The port number of the SMTP server, for example, `465`.
- * **OutgoingMailServerSecurity:** The security setting used by the SMTP server. Possible values can be `None`, `TLS`, or `SSL`.
- * **OutgoingUsername:** Any valid username similar to your mail client configuration, such as in the `firstname.lastname@xyz.com`.
- * **OutgoingPassword:** The password used for SMTP authentication. This consists of the following fields:

Type of Password: Select **Indirect Password, Create New User**.

Indirect Username/Key: Enter a unique string, for example, `OIMEmail-Config`. This masks the password and does not expose it in clear text in the configuration file.

Password: Enter a valid password for this account.

d. Click **Apply**.

4. If mail server security is SSL, then you must remove DemoTrust store references from the SOA environment. To do so:

- a. In a text editor, open the `DOMAIN_HOME/bin/setDomainEnv.sh` file. Open `setDomainEnv.bat` file for Microsoft Windows.

- b. Remove the following line:

```
-Djavax.net.ssl.trustStore=${WL_HOME}/server/lib/DemoTrust.jks from
EXTRA_JAVA_PROPERTIES
```

- c. Save and close the file.

- d. In a text editor, open the `DOMAIN_HOME/bin/startManagedWeblogic.sh` file. For Microsoft Windows, open the `startManagedWeblogic.bat` file.

- e. Remove the following `weblogic.security.SSL.trustedCAKeyStore` property set in `JAVA_OPTIONS` from this file:

```
JAVA_OPTIONS="-Dweblogic.security.SSL.trustedCAKeyStore="{MW_HOME}/server/s
erver/lib/cacerts" ${JAVA_OPTIONS}"
```

- f. Save and close the file.

- g. Restart the Admin and Managed servers.

Note: For more details on configuring UMS to connect to a mail server with SSL, see "Configuring Oracle User Messaging Service" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite*.

5. Edit the username and password in the CSF key. To do so:

- a. In Oracle Enterprise Manager, expand **WebLogic Domain**.

- b. Right-click the base domain, and select **Security, Credentials**. The Credentials page is displayed.

- c. In the Credential column, expand the **oracle.wsm.security** map.

- d. Select the record for the **Notification.Provider.Key** credential key.

- e. On the toolbar, click **Edit**. The Edit Key dialog box is displayed.

- f. Edit the values in the User Name and Password fields, and click **OK**.

14.1.1.2 Applying OWSM Policy to the UMS Web Service

Server-side OWSM policy can be applied to the UMS Web service to protect any other Web service that uses EM. The corresponding client side policy, username, and password must be provided in the provider XML or via MBean.

To attach server-side policy to the UMS Web Service:

1. In Oracle Enterprise Manager, expand **User Messaging Service**, and click **usermessagingserver (soa_server)**.
2. From the User Messaging Service list, select **Web Services**.
3. In the Web Service Details section, click the **Web Service Endpoints** tab.
4. In the Endpoint Name column, click **Messaging**.
5. Click the **OWSM Policies** tab.

6. Under Directly Attached Policies, click **Attach/Detach**. A list of available policies and the options to attach and detach policies are displayed.
7. Select a policy from the available policies list, and click **Attach**. The selected policy is added to the Directly Attached Policies list.

The policy you select is for securing the Messaging UMS web service.

8. To validate the applied policy combination, refresh the page. A message is displayed stating that the validation is successful.
9. Click **OK**.

To provide the corresponding client-side policy to the in the provider XML, edit the following properties in the UMS XML Bean in Oracle Identity Manager:

To provide the corresponding client-side policy to the UMSEmailProviderMBean, provide the name of the client-side policy in the UMSEmailNotificationProviderMBean MBean. To do so:

1. Login to Oracle Enterprise Manager.
2. Go to **Application Deployments**. Right-click **OIMAppMetadata(11.1.2.0.0)(oim_server1)**, and select **System MBean Browser**.
3. Go to **Application Defined MBeans, oracle.iam, Server: oim_server1, Application: oim, IAMAppRuntimeMBean, UMSEmailNotificationProviderMBean**.
4. Provide the client-side policy name in the policies properties shown in this MBean.

[Table 14–1](#) lists the properties of the UMSEmailProviderMBean.

Table 14–1 *UMSEmailProviderMBean Properties*

Property	Description
enabled	A notification provider is used to send the notification e-mail if value for this property is true.
type	In this release of Oracle Identity Manager, this value is EMAIL only, and the property is not used.
itrName	Various configuration values required to send the e-mail via UMS, can be either provided in XML properties or IT resource. If configuration values are to be read from IT resource, then provide the name of the IT resource here. If the IT resource name is present, than the IT resource configuration settings are used. If IT resource name is incorrect or invalid, or the values given in the IT resource instance are invalid, then an error is generated and email is not sent. Note: Using the IT resource is not a recommended channel to configure UMS in Oracle Identity Manager. This is because there is no mechanism to validate the values provided in the XML or IT resource before sending the e-mail to the server.
ws_url	The URL of UMS Web service to be invoked. Any SOA server can be used, in the following format: http://SOA_HOST/SOA_PORT/ucs/messaging/webservice

Table 14–1 (Cont.) UMSEmailProviderMBean Properties

Property	Description
CSFKey	This is the default notification key under oracle.wsm.security map. This key contains username and password required for OWSM policy. The default and recommended username/password in this key is the WebLogic administrator username and password. This can be changed to any valid username/password on the server side, which is SOA. See step 5 in "Enabling Oracle Identity Manager to Use UMS for Notification" on page 14-2 for information about editing the default values in CSF key by using Oracle Enterprise Manager.
policies	If OWSM policy is attached to the given Web service at server level, then provide the name of the corresponding client side policy here. Otherwise, leave this field blank. For example, if oracle/wss11_username_token_with_message_protection_service_policy is applied at server level, then provide the corresponding client policy name here, such as oracle/wss11_username_token_with_message_protection_client_policy.
keystoreAlias	The keystore alias for the target service. For details about the keystore alias, see "Client Aliases" in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite</i> .
sender	A valid username of any OIM User. The e-mail ID of this user is used to send the e-mail.

14.1.2 Using SMTP for Notification

By default, the SMTP Email Notification Provider is disabled. This is enabled by setting the value of the enabled attribute to true. To configure SMTP Email Notification Provider properties by using the EmailNotificationProviderMBean MBean:

1. Login to Oracle Enterprise Manager.
2. Click **Application Deployments**.
3. Right-click **OIMAppMetadata(11.1.2.0.0)(oim_server1)**, and select **System MBean Browser**. The System MBean Browser is displayed.
4. Navigate to **Application Defined MBeans, oracle.iam, Server: oim_server1, Application: oim, IAMAppRuntimeMBean, EmailNotificationProviderMBean**. All the attributes of the EmailNotificationProviderMBean MBean is displayed in the Attributes tab.

The Bean of Default SMTP Email notification provider is as follows:

```
<bean id="EmailServiceProvider"
class="oracle.iam.notification.provider.EmailServiceProvider"
lazy-init="true">
<property name="enabled" value="false" />
<property name="type" value="EMAIL" />
<property name="isAuth" value="false"/>
<property name="itrName" value="" />
<!-- Use any existing credential Map e.g. oracle.wsm.security or oim-->
<property name="CSFMap" value="oracle.wsm.security" />
<!-- Either create a new key in above given Map or use existing one e.g.
Notification.Provider.Key -->

<property name="CSFKey" value="" />
<property name="connectionTimeout" value="60000" />
```

```
<property name="mailServerName" value="" />
<property name="sender" value="xelsysadm" />
</bean>
```

Table 14–2 describes the properties of Default SMTP Email notification provider.

Table 14–2 Default SMTP Email Notification Provider Properties

Property	Description
enabled	This property derives the status of the notification provider. If the value of this property is false, then the provider is inactive. To activate the provider, change the value to true.
type	This property determines the type of the notification provider. Oracle Identity Manager supports only Email type.
isAuth	If the value of this flag is false, then authentication is not required at mail server. As a result, you do not need to provide the CSFKey and CSFMap values. But this depends on the mail server in use. Most of the mail servers support this flag. If any mail server does not support this flag, then authentication credentials must be provided in CSFKey and corresponding CSFMap.
itrName	If you want to provide connectivity information via IT resource instance of type Mail Server, then provide the name of IT resource instance here. This is not a recommended option.
CSFMap	This property determines the name of the existing CSF Map, for example oim and oracle.wsm.security.
CSFKey	This property takes the name of the key that contains the authentication credentials, which are username and password. This key must exist under the map name. By default, one key with name Notification.Provider.Key is available under oracle.wsm.security map. This key is used for UMS Email notification provider, and default username and password is weblogic/weblogic1. If UMS email provider is disabled, then use the same map and key to provide the username and password required at mail server for authentication. Otherwise, create a new key under any of the default maps, and provide the name of map and key in these properties. Adding a CSF key is described later in this section.
connectionTimeout	This is in milliseconds. This is required for setting a maximum time for connection establishment.
mailServername	This is the name of mail server.
sender	This is the sender used in Oracle Identity Manager for sending the emails.

To add a CSF key:

1. Login to Oracle Enterprise Manager.
2. Expand **WebLogic Domain**.
3. Right-click **base_domain**, and select **Security, Credentials**.
4. Expand **oracle.wsm.security**, and then click **Create Key**.
5. Create a key of type password. Provide the key name, description, username, and password. Click **OK**.

14.1.3 Using SOA Composite for Notification

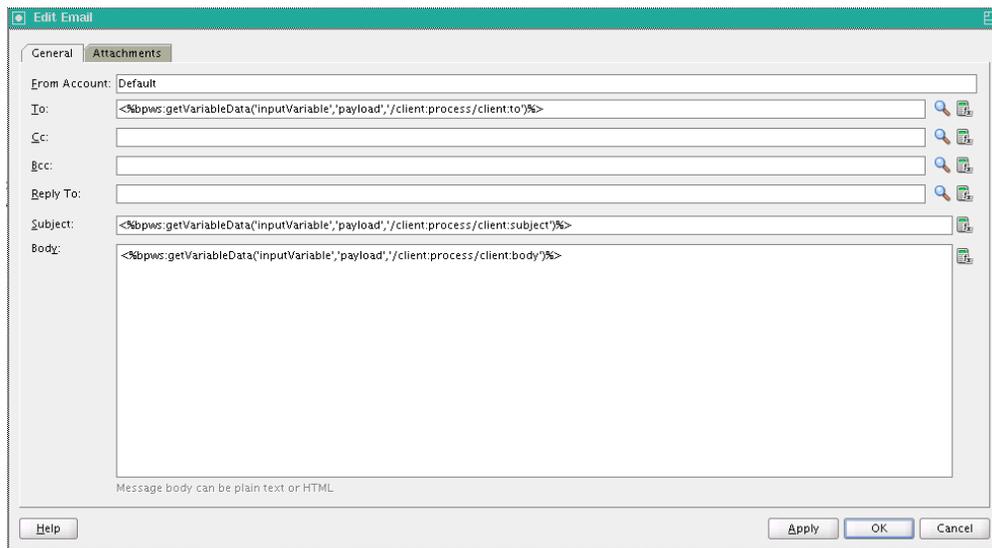
By default, the SOA Email Notification Provider is disabled. You can enable this notification provider by changing the value of the enabled property to true.

To use SOA composite in Oracle Identity Manager for notification:

1. Create a SOA composite with notification activity. For details, see "Using the Notification Service" in the *Oracle Fusion Middleware Developer's Guide for Oracle SOA Suite*.

Figure 14–1 shows the sample mapping of the composite payload via Expression Builder.

Figure 14–1 Sample Mapping of Composite Payload



2. Manually deploy the SOA composite on the SOA server. To do so:
 - a. Create an application connection. To do so:
 - i. Open the SOA composite in JDeveloper.
 - ii. Create a new Application Server Connection by right-clicking the project and selecting **New, Connections, Application Server Connection**.
 - iii. Name the connection as `SOA_server`, and click **Next**.
 - iv. Select WebLogic 10.3 as the Connection Type.
 - v. Enter the authentication information. The typical values are:

Username: weblogic

Password: weblogic1
 - vi. On the Connection screen, enter the hostname, port, and SSL port for the SOA Admin server or Admin server, and enter the name of the WebLogic domain.
 - vii. Click **Next**.
 - viii. On the Test screen, click **Test Connection**. Verify that the success message is displayed.
 - b. Deploy the project. To do so:

- i. Right-click the project, select **deploy**, select the project name. Select the **to** option to create the application connection, which is SOA_server. Verify that the build successful message is stored in the log.
 - ii. Enter the default revision, and click **OK**. Verify that the Deployment Finished message is stored in the deployment log.
3. Using Enterprise Manager, navigate to **soa-infra, (Menu), Workflow Notification Properties**, and set the Notification Mode to ALL.
 4. Configure the SOA Email Notification Provider properties by using the SOAEmailNotificationProviderMBean MBean. To do so:
 - a. Log in to Oracle Enterprise Manager.
 - b. Expand **Application Deployments**. Right-click **OIMAppMetadata(11.1.2.0.0)(oim_server1)**, and select **System MBean Browser**.
 - c. Navigate to **Application Defined MBeans, oracle.iam, Server: oim_server1, Application: oim, IAMAppRuntimeMBean, SOAEmailNotificationProviderMBean**.
 5. Change the value of the enabled property from false to true in the SOAEmailNotificationProviderMBean. Figure 14–2 shows the properties of the Bean of SOA Email notification provider.

Figure 14–2 SOAEmailNotificationProviderMBean Properties

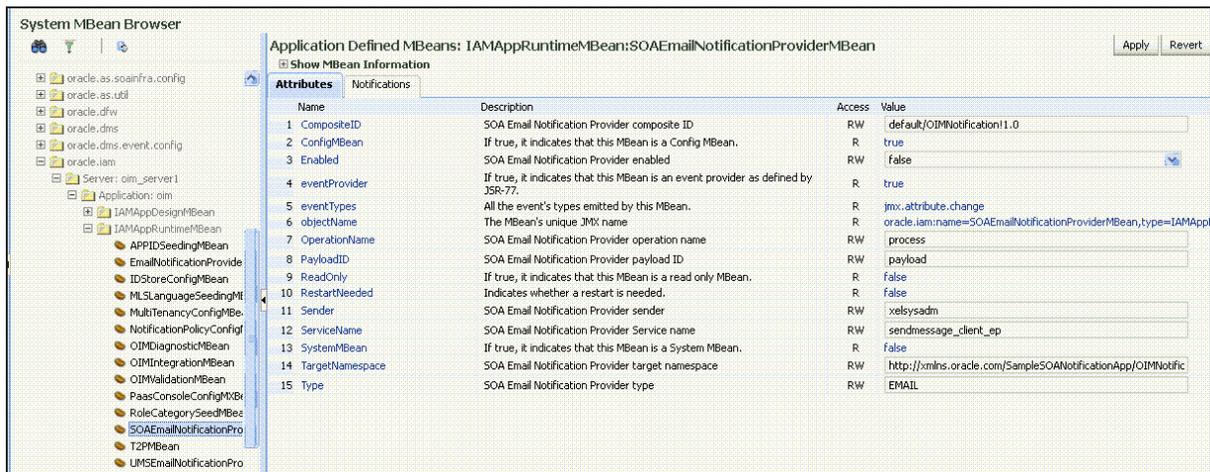


Table 14–3 lists some of the properties of the SOA Email Notification Provider.

Table 14–3 SOA Email Notification Provider Properties

Property	Description
enabled	This property derives the status of the notification provider. If the value of this property is false, then the provider is inactive. To activate the provider, change the value to true.
type	This property determines the type of the notification provider. Oracle Identity Manager supports only Email type.
compositeID	This represents the name of the SOA composite. Name includes pkg/Name!version.
serviceName	This is the name given to the service in the SOA composite.

Table 14–3 (Cont.) SOA Email Notification Provider Properties

Property	Description
operationName	This is the name given to the process in the SOA composite.
payloadID	This is the name given to the payload in the SOA composite.
targetNamespace	This is the name of the targetNamespace given in various XMLs generated while creating the SOA composite.
sender	This is the sender used in Oracle Identity Manager for sending the emails.

6. Configure the user messaging drivers, if required. If you do not specify values for the user messaging drivers, then the local Linux mail server is used by default. To use any other mail server:
 - a. Log in to Oracle Enterprise Manager.
 - b. Navigate to **User Messaging Service, usermessagingdriver-email (soa_server1), Email Driver Properties** in Driver-Specific Configuration.
 - c. Configure the following mandatory values:
 - **OutgoingMailServer:** Name of the SMTP server, for example, stbeehive.oracle.com.
 - **OutgoingMailServerPort:** Port of the SMTP server, for example, 465.
 - **OutgoingMailServerSecurity:** The security setting used by the SMTP server. Possible values can be None, TLS, or SSL.
 - **OutgoingUsername:** Any valid username, similar to firstname.lastname@abc.com.
 - **OutgoingPassword:** Select **Indirect Password, Create New User**. Provide a unique string for Indirect Username/Key, for example, OIMEmailConfig. This will mask the password and not expose it in clear text in the config file. Provide a valid password for this account.

See Also: "Configuring the Email Driver" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management* for more information about configuring user messaging drivers
7. After successful deployment of the SOA composite, trigger the notify API from any client, for example, the reset password event.

14.1.4 Configuring Custom Notification Provider

You can configure and use a custom notification provider, other than the default notification providers, for sending notifications.

To configure a custom notification provider:

1. Implement a custom Notification Provider class extending the `oracle.iam.notification.provider.NotificationProviderBase` base class.
2. Create a JAR file containing the class, and upload the file by using the UploadJAR utility. For information about using the UploadJAR utility, see "Upload JAR and Resource Bundle Utilities" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

3. Create an XML file similar to the following:

```
<beans xmlns="http://www.springframework.org/schema/beans" \\\
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" \\\
xmlns:util="http://www.springframework.org/schema/util" \\\
xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.spri
ngframework.org/schema/beans/spring-beans-2.0.xsd
http://www.springframework.org /schema/util
http://www.springframework.org/schema/util/spring-util-2.0.xsd" def
ault-lazy-init="true">
<bean id="<customProvider>" class="<oracle.i
am.notification.provider.CustomProvider>" lazy-init="true">
<!--Mandatory Attributes-->
<property name="enabled" value="<true>" />
<property name="type" value="EMAIL" />
<!--Optional Attributes-->
<property name="sender" value="SYSTEM_ADMINISTRATOR_USERNAME" />
</bean>
</beans>
```

When the value of the enabled property name is true, then this custom provider is used for sending notifications.

4. Import the XML file to MDS by using Oracle Enterprise Manager. For information about exporting and importing metadata files to and from MDS, see "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

14.1.5 Disabling and Enabling Notification Providers

The notification providers, such as UMS notification provider or EmailNotificationProvider, can be disabled or enabled by using the Enterprise Manager console. For example, to disable UMS notification provider:

1. Login to Enterprise Manager.
2. Go to **Application Deployments**.
3. Right-click **OIMAppMetadata(11.1.2.0.0)(oim_server1)**, and select **System MBean Browser**. The System MBean Browser pane is displayed.
4. Go to **Application Defined MBeans, oracle.iam, Server: oim_server1, Application: oim, IAMAppRuntimeMBean**.
5. Select **UMSEmailNotificationProviderMBean**.
6. In the Attributes tab, from the Value list corresponding to the Enabled attribute, select **false** to disable UMS notification provider. To enable UMS notification provider, select **true**.

14.2 Managing Notification Templates

Oracle Identity Manager provides a set of default notification templates, as shown in [Table 14-4](#).

Table 14-4 Default Notification Templates

Notification Template	Description
Add Proxy Notification	Template to send notification after a proxy has been added for a user

Table 14–4 (Cont.) Default Notification Templates

Notification Template	Description
Bulk Request Creation	Template to send notification during a bulk request creation
Create User Self Service Notification	Template to send notification after a new user is created
End Date	Template to send notification to the manager when end date of the reportee expires
Forgotten Username Notification	Template to send notification after user submits the Forgotten Username form
Generated Password Notification	Template to send notification after a password is generated by Oracle Identity Manager
Pass Bulk Upload Success	Template to send notification on completion of user upload
Password Expired Notification	Template to send notification after password has expired
Password Warning Notification	Template to send notification before password expires
Request Creation	Template to send notification during a request creation
Request Identity Creation	Template to send notification during a Create User request
Request Status Change	Template to send notification during a request status change
Reset Password	Template to send notification after password has been reset
User Deleted	Template to send notification to the manager when the user account of the reportee is deleted as a result of expired end date

Notification templates are described in the following sections:

- [Creating a Notification Template](#)
- [Searching for a Notification Template](#)
- [Modifying a Notification Template](#)
- [Deleting a Notification Template](#)
- [Adding and Removing Locales from a Notification Template](#)
- [Configuring Notification for a Proxy](#)

14.2.1 Creating a Notification Template

Note: Corresponding to each event that happens, you have to configure an XML file. The XML file defines the behavior of each event. You must first configure the XML for an event. After this is done, you can create a notification template for that event.

For information about creating the event XML file, see "Defining Event Metadata" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

To create a notification template:

1. Log in to Oracle Identity System Administration.

2. In the left pane, under System Management, click **Notification**. The Notification page is displayed.
3. From the Actions menu, select **Create**. The Create Template page is displayed.
4. In the Template Information section, enter values for the following fields:
 - **Template Name:** Enter the template name in this field.
 - **Description Text:** Enter a brief description of the template in this field.

Note: The Description Text field cannot be translated and is available only in English.

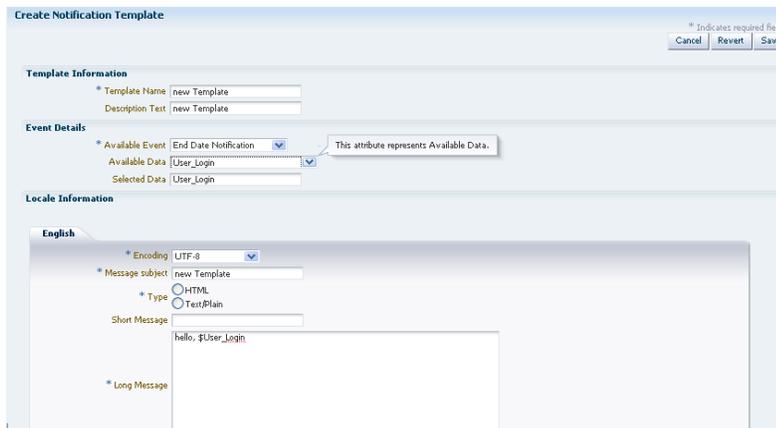
5. In the Event Details section, from the Available Event list, select the event for which the notification template is to be created from a list of available events. Depending on your selection, other fields are displayed in the Event Details section.
6. Under the Locale Information section, enter values in the following fields:

Note: The Default Locale information is stored in the PTY table and is fetched from there.

- To specify a form of encoding, select either UTF-8 or ASCII.
 - In the **Message Subject** field, enter a subject for the notification.
 - From the **Type** options, select the data type in which you want to send the message. You can choose between HTML and Text/Plain.
 - In the **Short Message** field, enter a short version of the message.
 - In the **Long Message** field, enter the message that will be sent as the notification. See step 7.
7. To use the token for available data in the messages that will be sent as notification:
 - a. Select the attribute from the list. This attribute will be displayed in the Selected Data field.
 - b. Copy the attribute and add it in the message text by placing it inside `{}`. For example, if selected data is `FA_Territory`, then include it in the text as `{FA_Territory}`.

Figure 14–3 shows the Create Notification Template page with sample values:

Figure 14–3 The Create Notification Template Page



8. After you have entered the required values in all the fields, click **Save**.
9. A message is displayed confirming the creation of the notification template. Click **OK**.

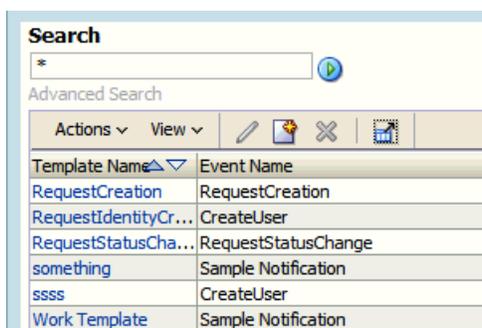
14.2.2 Searching for a Notification Template

You can perform a simple search or an advanced search for a notification template by using Advanced Administration.

To perform a simple search for a notification template:

1. In Oracle Identity System Administration, under System Management, click **Notification**. Advanced Administration is displayed with the Notification tab enabled.
2. Click the icon next to the **Search** field. All the existing notification templates are displayed on the left pane, as shown in [Figure 14–4](#):

Figure 14–4 Notification Search Result



3. Select the template that you want to view. The details of the selected notification template are displayed on the right pane.

To perform an advanced search for a notification template:

1. In the left pane of the Advanced Administration, click **Advanced Search**. The Advanced Search page is displayed.
2. Select one of the following matching options:

- **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful based on Search field with any input from the user. Search field with no input from the user is not considered.
 - **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. Specify the search criteria in the Template Name, Event Name, and Subject Details fields. You can remove any of these fields that you do not want to include in the search by clicking the icon next to it. You can add a field that you want to include in the search by clicking **Add Fields**, and then selecting the field name from the list.
 4. Click **Search**. The search results table is displayed with details about template names, event names, and subject details.

14.2.3 Modifying a Notification Template

To modify a notification template:

1. In Identity System Administration, under System Management, click **Notification**.
2. Search for the notification template that you want to modify.
3. Select the template that you want to modify. The details of a notification template is displayed, as shown in [Figure 14-5](#).

Figure 14-5 Notification Template Modification

The screenshot shows a web application window titled "Notification Template Details: Generated Password Notification". The window has a "Welcome" tab and a "Notification Template Details: Generated Password Notification" tab. In the top right corner, there are buttons for "Cancel", "Revert", and "Save", along with a note: "* Indicates required fields." The form is organized into three main sections:

- Template Information:** Contains "Template Name" (Generated Password Notification) and "Description Text" (To be sent after password has been).
- Event Details:** Contains "* Available Event" (Generated Password).
- Locale Information:** Features a tabbed interface with tabs for Spanish, Norwegian, Dutch, Hungarian, Hebrew, English, and German. Under the "Spanish" tab, there are three fields:
 - * Encoding: UTF-8
 - * Message subject: Información de Nueva Cuenta
 - * Type: HTML (selected with a radio button), Text/Plain

4. Change the values that you want to and click **Save**.
5. A message is displayed confirming the modification of the notification template. Click **OK**.

14.2.4 Deleting a Notification Template

To delete a notification template:

1. In the Identity System Administration, under System Management, click **Notification**.
2. Search for the notification template that you want to delete.
3. Select the template that you want to delete.
4. From the Actions menu, click **Delete**. A message is displayed prompting you to confirm the delete the operation. Click **OK**. A message is displayed confirming the delete operation.

14.2.5 Adding and Removing Locales from a Notification Template

To add locales to a notification template:

1. In the Identity System Administration, under System Management, click **Notification**.
2. Search for the template that you want to add a locale to.
3. From the Actions menu, select **Add Locale**. The Add Locale page is displayed.
4. In the Locale Name field, click the icon next to the Locale Name field to select a locale from a list. After selecting the locale, and click **Confirm**.
5. Click **Next**. The Locale Information page is displayed and the locale that you added is displayed as a tab in the page.
6. In the Locale Information section, specify values for all the fields as mentioned in step 6 of "[Creating a Notification Template](#)" on page 14-12, and then click **Save**. The locale is added to the template.

Note: Notification can be sent in all the locales that are added to the notification template. A user receives notification in the same locale specified in the user preferences. If a locale is not specified in the user preferences, then the notification is sent in the default locale. The default locale is to be specified in the PTY table in Oracle Identity Manager database at the time of installation.

To remove locales from a notification template:

1. Search for the notification template from which you want to remove a locale. Select the template from the search results table.
2. From the Actions menu, click **Remove Locale**. The Remove Locale page is displayed.
3. Click the icon next to the Locale Name field to select a locale from a list . You can remove a locale from a template only if that template contains multiple locales. You cannot remove a locale if it is the only one associated with the template. Click **Save**.
4. A message is displayed confirming the removal of the locale. Click **OK**.

Note: You must not remove default locale to ensure that a notification is sent every time when there is no user preferred locale is set or when notification template does not contain a locale template matching to user preferred locale.

14.2.6 Configuring Notification for a Proxy

Use the following steps to configure notification for a proxy:

1. Configure a new Email IT resource.
2. Create a new user. (For example, create a user Jane Doe.)
3. Create a second user. (For example, create a user John Doe.)
4. Assign the Jane Doe user as a manager for John Doe.
5. Specify your email ID for John Doe, which enables you to receive notifications in your inbox.
6. Log in as Jane Doe and navigate to the Oracle Identity Self Service.
7. Under My Profile, select **My Information**. The My Information page is displayed.
8. Expand **Proxies**. In the Proxies section, add John Doe as a proxy for Jane Doe.

Note: If you successfully added the proxy, you (John Doe in this case) will receive an email notification message similar to the following:

"You have been made the proxy for Jane Doe [JANED] from April 9, 2012 12:00:00 AM to April 30, 2010 12:00:00 AM".

14.3 Configuring Default Email Provider

Oracle Identity Manager sends email notifications during some operations, such as create user and password reset. There are two type of email providers, the default and UMS providers. This section describes how to configure default email provider for sending email notifications.

To configure default email provider:

1. Verify the Email Provider Configuration in Oracle Enterprise Manager. Modify the configuration as required.
2. Login to Oracle Identity System Administration, and set the value of the Email Server system property to point to the IT resource with name Email Server. For information about this system property, see "[Managing System Properties](#)" on page 16-1.
3. Verify that the Email Server IT resource exists. This IT resource must have Mail Server as the IT resource type, and it must have a server name, for example localhost. If this IT resource is not present for mail server, then create the IT resource. For information about creating IT resources, see "Creating IT Resources" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

14.4 Configuring SOA Email Notification

This section contains the following topics:

- [Configuring Actionable Email Notification on SOA](#)
- [Troubleshooting SOA Email Notification](#)

14.4.1 Configuring Actionable Email Notification on SOA

To configure email notifications on SOA:

1. Before performing the steps to configure email notifications in SOA, ensure the following:
 - Make sure that the user to whom task is assigned has a valid email account set in Oracle Identity Manager.
 - If you want email notifications to be actionable, such as allowing approving or rejecting requests from the email, then ensure that you have configured human task to send actions in the notification. You can verify this by using SOA Composer. To do so:
 - a. Login to SOA Composer by using weblogic user by using the following URL:
`http://SOA_HOST:SOA_PORT/soa/composer`
 - b. Go to **Open Menu, Open Tasks**.
 - c. In the Notification Settings dialog box, select the human task for which you want to verify the settings.
 - d. Verify that the **Make notification actionable** option is selected.
2. Login to Oracle Enterprise Manager as weblogic user.
3. Go to SOA. Right-click **soa-infra** (*soa_server_name*), and select **SOA Administration, Workflow notification properties**.
4. From the Notification Mode list, select **Email**.
5. Enter values for the following:
 - **Email : From Address:** Email account from which notification will be sent to approvers
 - **Email : Actionable Address:** Email account that will receive approve/reject response sent by approvers via email
 - **Email : Reply To Address:** Optional email address to which the reply will be sent, for example, no.reply@yourdomain.com
6. Click **Apply**.
7. Go to User Messaging Service. Right-click **usermessagingdriver-email** (*soa_server_name*), and select **Email driver properties**.
8. In the Driver-Specific Configuration section, configure the following minimum attributes for email notifications to work correctly:
 - **MailAccessProtocol:** Select IMAP or POP3
 - **OutgoingMailServer:** Name of the SMTP server, for example, myhost.mycompany.com
 - **OutgoingMailServerPort:** Port of the SMTP server, for example, 465
 - **OutgoingDefaultFromAddress:** Same as OutgoingMailServer
 - **OutgoingPassword:** You can provide the password in clear text stored in driverconfig.xml, or store password in CSF by using indirect option.
 - **IncomingMailServer:** The hostname of the incoming mail server. Required only if receiving emails is supported on the driver instance.
 - **IncomingMailIDs:** The email addresses corresponding to the user names. Each email address is separated by a comma and must reside in the same

position in the list as their corresponding user name appears on the usernames list. Required only if receiving emails is supported on the driver instance.

- **IncomingUserPasswords:** You can provide password in clear text stored in driverconfig.xml, or store password in CSF using indirect option.
- **Debug (Optional):** Setting this to true logs all email activity on SOA server console but not SOA log files. Set this to true until you are sure that notifications are working correctly.

See Also: "Configuring Human Workflow Service Components and Engines" and "Configuring Oracle User Messaging Service" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite* for detailed information about driver-specific configuration and Human workflow service components

9. Restart SOA Managed Server.
10. Generate the human task by raising a request.
11. Use your email client to check mails in user's email account.

14.4.2 Troubleshooting SOA Email Notification

Consider the following to troubleshoot issues encountered with SOA email notification:

- Enable the Debug option in the driver-specific configuration if you are facing issues with sending or receiving notifications. If you modify the email driver properties, then restart SOA server.
- Send test notifications. To do so:
 - a. Login to Oracle Enterprise Manager.
 - b. Go to SOA. Right-click **soa-infra** (*soa_server_name*), and select **Service Engines, Human Workflow, Notification Management, Send Test Notification**.
- Verify that email server and accounts are working. Try sending/receiving emails using your email client.
- Check the SOA server log. Usually, the issue is with user messaging service configuration. If you have enabled the debug option, then SOA server log provides debugging information.
- Sometimes if email is not being sent to a particular email account (because of incorrect configuration), then SOA server marks it as bad address. You must manually remove such bad address. To do so:
 - a. Login to Oracle Enterprise Manager.
 - b. Go to SOA. Right-click **soa-infra** (*soa_server_name*), **Service Engines, Human Workflow, Notification Management, View Bad Address, Remove the Bad Address**.

14.5 Disabling Email Notification

Notifications are sent in the following scenarios by event handlers when users are created through UI or through SPML:

See Also: "Developing Event Handlers" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about event handlers

- A user is created with manual password as a result of SelfServiceNotificationHandler. To disable sending email notification, remove the SelfServiceNotificationHandler section in the /metadata/iam-features-selfservice/event-definition/EventHandlers.xml in MDS.
- System Administrator creates user with autogenerated password as a result of PasswordNotificationHandler. To disable sending email notification, remove the PasswordNotificationHandler section in the /metadata/iam-features-passwordmgmt/event-definition/EventHandlers.xml file in MDS.
- System Administrator changes password manually. The notification can be disabled through UI based on the email checkbox selected on the UI.
- System Administrator changes password with autogenerated password (reset password) as a result of ResetPasswordActionHandler. This is not a postprocess event handler that can be disabled.

To disable email notifications:

1. Export the /metadata/iam-features-selfservice/event-definition/EventHandlers.xml file from MDS by using Oracle Enterprise Manager. See "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Note: Save a local copy of the EventHandlers.xml for future reference.

2. Remove the following from the EventHandlers.xml file:

```
<postprocess-handler
class="oracle.iam.selfservice.uself.uselfmgmt.impl.handlers.create.SelfServiceN
otificationHandler"
entity-type="User"
operation="CREATE"
name="SelfServiceNotificationHandler"
order="1160"
stage="postprocess"
sync="TRUE">
</postprocess-handler>
```

3. Export the /metadata/iam-features-passwordmgmt/event-definition/EventHandlers.xml file from MDS by using Oracle Enterprise Manager.

4. Remove the following from the EventHandlers.xml file:

```
<postprocess-handler
class="oracle.iam.passwordmgmt.eventhandlers.PasswordNotificationHandler"
entity-type="User" operation="CREATE" name="PasswordNotificationHandler"
order="1180" stage="postprocess" sync="TRUE">
</postprocess-handler>
```

5. Import the files to MDS by following the instructions in "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
6. Export the files again to verify that the edits have been correctly uploaded to MDS.
7. Login to Oracle Identity System Administration, and set the Should send notifications in recon or not system property to FALSE. For information about this system property, see "Managing System Properties".

14.6 Testing Notification Configuration

This section describes the following notification configuration tests:

- [Testing UMS Email Notification](#)
- [Testing SMTP Connectivity](#)

14.6.1 Testing UMS Email Notification

You can use the run.sh script to send notification through UMS. If the script is successful in sending notification through UMS, then the configuration is correct.

To test UMS email notification:

1. Copy the run.sh script and ClientNotificationTest.class file in the same directory in the host on which UMS notification has been configured.

2. Edit the run.sh script with following values:

```
APPSERVER_TYPE=wls
```

```
JAVA_HOME=VALID_JAVA_HOME
```

```
OIM_HOME=OIM_HOME
```

```
OIM_ORACLE_HOME=VALID_OIM_ORACLE_HOME
```

3. Run the run.sh script by using the following command:

```
sh run.sh OIM_HOST OIM_PORT SYS_ADMINISTRATOR_PASSWORD
VALID_OIM_USER_WITH_VALID_EMAIL_ID
```

In this command syntax:

- OIM_HOST is the host on which Oracle Identity Manager is deployed.
- OIM_PORT is the Oracle Identity Manager port.
- SYS_ADMIN_PASSWORD is the System Administration password.
- VALID_OIM_USER_WITH_VALID_EMAIL_ID is a valid user in Oracle Identity Manager with a valid email ID to which the mail will be sent.

The following is an example of the run.sh command:

```
sh run.sh myhost.mycompany.com 8003 adminuser Welcome1 testuser
```

Note: It might take some time for the mail to be sent to the user's email id.

14.6.2 Testing SMTP Connectivity

To check the SMTP connectivity from a host, you can telnet from the host and send a test mail, as shown:

```
>> [aime@slcaa403 config]$ telnet internal-mail-router.mycompany.com 25
>> Trying 192.0.2.20...
>> Connected to internal-mail-router.oracle.com (192.0.2.1).
>> Escape character is '^]'.
>> 220-myhost.mycompany.com ESMTP Oracle Corporation - Unauthorized Use Prohibited
>> 220 Ready at Wed, 11 Jan 2012 09:30:44 GMT
>> MAIL From:<john.doe@mycompany.com>
>> 503 5.0.0 Polite people say HELLO first
>> Hello mycompany.com
>> 250 myhost.mycompany.com Hello anotherhost.mycompany.com [192.0.2.21],
pleased to meet you
>> MAIL From:<john.doe@mycompany.com>
>> 250 2.1.0 <john.doe@mycompany.com>... Sender ok
>> RCPT To:<john.doe@mycompany.com>
>> 250 2.1.5 <john.doe@mycompany.com>... Recipient ok
>> DATA
>> 354 Enter mail, end with "." on a line by itself
>> Testing internal mail router.
>> .
>> 250 2.0.0 q0B9Ui4h013576 Message accepted for delivery
>>
```

Managing the Scheduler

In Oracle Identity Manager, it is often required to run jobs at specified times on a regular basis to manage various activities. Scheduler enables you to schedule jobs that automatically run predefined scheduled tasks at the specified time. This is illustrated by the following example:

To meet the security policies of an organization, employees may be required to change their product application password every 60 days. For this purpose, the system administrator has to ensure that an email is sent to all employees whose passwords for the respective product applications have expired. One approach would be to identify the set of users whose passwords have expired and send email to each employee manually. Alternatively, the system administrator can use a service, such as scheduler. In Oracle Identity Manager, there is a predefined scheduled task called Password Warning Task. The system administrator can use this scheduled task to create a scheduled job with the intended schedule.

See Also: [Table 15-2, "Predefined Scheduled Tasks"](#) for information about the Password Warning Task scheduled task

Scheduler also enables you to create your own scheduled tasks that can be run by a job at a set time.

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. 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.

This chapter discusses the following topics:

- [Configuring the oim-config.xml File](#)
- [Starting and Stopping the Scheduler](#)
- [Disabling and Enabling the Scheduler on a Node in Cluster Setup](#)
- [Scheduled Tasks](#)
- [Jobs](#)

15.1 Configuring the oim-config.xml File

After you install Oracle Identity Manager, you can configure the scheduler settings by editing the child elements of the Scheduler element in the oim-config.xml file located in the following location in Meta Data Store (MDS):

db/oim-config.xml

See Also: "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about importing and exporting data to and from MDS

Table 15–1 lists the default elements that you can configure within the Scheduler element in the oim-config.xml file.

Note: You can add new configurable child elements. For the information about new child elements, refer to the following URL:

<http://www.quartz-scheduler.org/>

Table 15–1 Child Elements of the Scheduler Element

Element Within Scheduler Element	Description
DSJndiURL	This element is used for configuring transactional data source in the application server, which is used by Quartz to establish the connection. Default value: jdbc/operationsDB
nonTxnDSJndiURL	This element is used for configuring non-transactional data source in the application server, which is used by Quartz to establish the connection. Default value: jdbc/oimJMSStoreDS
Clustered	Enter true if Oracle Identity Manager has been installed in a clustered environment. Otherwise, enter false. Default value: true NOTE: In a clustered environment, the clocks on all nodes of the cluster must be synchronized.
implementationClass	Enter the name of the Java class that implements scheduler. Default value: oracle.iam.scheduler.impl.quartz.QuartzSchedulerImpl
instanceID	Enter a unique string value in this element. This value represents a string that uniquely identifies an Oracle Identity Manager scheduler instance. NOTE: In a clustered environment, each node of the cluster must have a unique InstanceId. This can be achieved by entering a value of AUTO in the instanceId element.
startOnDeploy	Enter false if you do not want scheduler service to start automatically when Oracle Identity Manager is started. Otherwise, enter true. Default value: true
threadPoolSize	Enter an integer value in this element. This value represents the number of threads that must be used for running jobs. Default Value: 10

15.2 Starting and Stopping the Scheduler

The Scheduler Status page is an authenticated UI page that displays the current status of the scheduler. At any given instance, the scheduler can be in one of the following statuses:

- Started

If the scheduler is in the started status, then jobs can be scheduled and jobs that have already been scheduled will continue to run at the scheduled time.

- Stopped

If the scheduler is in the stopped status, then all jobs are stopped. When the scheduler gets the stopped status while jobs are running, the currently running jobs are stopped. In addition, the jobs that are scheduled to run does not run, but are submitted for run according to the schedule. When the Scheduler Service is up in the future, all submitted jobs are run.

The Scheduler Status page also displays a detailed error message in the Last Error field, if any.

You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

By default, the scheduler is in the started status after you install Oracle Identity Manager. However, if you want to stop scheduler for any reason and then restart it, then you must follow the procedure discussed in this section.

To start or stop the scheduler:

Note:

- You need to have Scheduler Admin role to start or stop the scheduler.
 - In a clustered environment, you must perform this procedure on each node of the cluster.
-
-

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

`http://OIM_HOST:OIM_PORT/SchedulerService-web/status`

In this URL, *OIM_HOST* represents the name of the computer hosting the Oracle Identity Manager server, and *OIM_PORT* refers to the port on which Oracle Identity Manager server is listening.

2. Enter the User ID and password, and then click **Submit**.

The Scheduler Status page is displayed.

Note: You may be automatically logged in to the scheduler service if you are working in a single sign-on environment.

3. Depending on the type of action that you want to perform, click one of the following:

- **START:** Click this button to start the scheduler.
- **STOP:** Click this button to stop the scheduler. This stops the scheduler and further execution of triggers, but it does not stop or abort any jobs that are

already executing. When the Scheduler Service is started again, jobs will then be executed at their appropriate times based on when they are scheduled.

- **REINIT:** Click this button to reinitialize the scheduler.

15.2.1 Controlling Scheduler Start or Stop in a Clustered Environment

The scheduler.disabled system property is required if you want to control scheduler start or stop on a clustered setup. The scheduler.disabled system property must be set to true if you do not want to start the scheduler service on that node of the cluster.

This section contains the following topics:

- [Adding the Server Side Property for Oracle Identity Manager](#)
- [Restarting Oracle Identity Manager Managed Servers from the Node Manager](#)
- [Modifying the Server Side Property for Oracle Identity Manager](#)

15.2.1.1 Adding the Server Side Property for Oracle Identity Manager

To add the scheduler.disabled server-level property:

1. Log in to the WebLogic Administrative Console.
2. On the left panel, select **Environment, Servers**.
3. Click the name of the managed server where you want to add the scheduler.disabled=false property.
4. Select **Lock and Edit**.
5. Select **Configuration, Server Start**.
6. In the Arguments box, add the scheduler.disabled=false property, and click **Save**.
7. Click **Activate Change**.

Restart the managed server using node manager so that the newly added property is picked up. Restarting from the Command-Line Interface does not work.

15.2.1.2 Restarting Oracle Identity Manager Managed Servers from the Node Manager

To restart Oracle Identity Manager Managed Servers from the Node Manager:

1. Start the Administration server. To do so:
 - a. From your current working directory, go to the `MW_HOME/user_projects/domains/base_domain/` directory.
 - b. Run the following command:
For UNIX:

```
startWebLogic.sh
```


For Windows:

```
startWebLogic.cmd
```
2. Start the Node Manager. To do so:
 - a. From your current working directory, go to the `MW_HOME/wlserver_10.3/server/bin/` directory.
 - b. Run the following command:

For UNIX:

```
startNodeManager.sh
```

For Windows:

```
startNodeManager.cmd
```

3. Log in to the WebLogic Administrative Console.
4. On the left panel, select **Environment, Servers**.
5. Select Control from the right panel.
6. Select the option where the property is added, and click **Start**.

15.2.1.3 Modifying the Server Side Property for Oracle Identity Manager

To modify the scheduler.disabled system property:

1. Log in to the WebLogic Administrative Console by using the WebLogic administrator credentials.
2. Under Domain Structure, select **Environment, Servers**. The Summary of Servers page is displayed.
3. Click the Oracle Identity Manager server name, for example, oim_server1. The settings for oim_server1 is displayed.
4. Click **Configuration, Server Start**.
5. In the Arguments box, change the existing property scheduler.disabled = false/true.
6. Click **Save**.
7. Click **Activate Changes**.
8. Restart the Oracle Identity Manager Managed Server.

Note: After modifying the scheduler.disabled system property, you must start the Managed Server by using the Node Manager.

15.3 Disabling and Enabling the Scheduler on a Node in Cluster Setup

Disabling and enabling the scheduler on a node in cluster setup involves the following:

- [Adding the Server-Level Property](#)
- [Restarting the Managed Server from the Node Manger](#)

15.3.1 Adding the Server-Level Property

To add the server-level property to disable/enable the scheduler on a node in cluster setup:

1. Log in to the WebLogic Administrative Console.
2. In left pane, click **Environment, Servers**.
3. Click the name of the managed server in which you want to add the scheduler.disabled=true property.

4. Click **Lock and Edit** in the left tab.
5. Click **Configuration, Server start** tab in the right pane.
6. In the Argument Text box, add scheduler.disabled=true, and save.
7. Click **Activate Change** in the left pane.
8. To ensure that this property is picked, restart the managed server via the node manager. Restarting from script does not work.

15.3.2 Restarting the Managed Server from the Node Manger

To restart the managed server from the node manager:

1. Start the Admin Sever by running the following script:

```
MW_HOME/user_projects/domains/base_domain/startWebLogic.sh
```

2. Start the Node Manager by running the following script:

```
MW_HOME/wlserver_10.3/server/bin/startNodeManager.sh
```

3. Login to the WebLogic Administrative Console.
4. In left pane, click **Environment, Servers**.
5. Click the **Control** tab in the right pane.
6. Select the checkbox against the managed server in which the property has been added, and then click the **start** button.

After restarting the managed server, scheduler will not start because the value of the scheduler.disabled property is set to true. To verify this, navigate to the following URL and log in:

<http://HOST:PORT/SchedulerService-web>

15.4 Scheduled Tasks

In Oracle Identity Manager, metadata is predefined for the default scheduled tasks. New tasks can be added by the user with new metadata, or the existing tasks can be updated to add or update the parameters or other configuration details.

For example, you can configure a reconciliation run using a scheduled task that checks for new information on target systems periodically and replicates the same in Oracle Identity Manager. Each scheduled task contains the following metadata information:

- Name of the scheduled task
- Name of the Java class that runs the scheduled task
- Description
- Retry
- (Optional) Parameters that the scheduled task accepts. Each parameter contains the following additional information:
 - Name
 - Data Type
 - Required/ Optional
 - Help Text

- Encryption

This section discusses the following topics:

- [Predefined Scheduled Tasks](#)
- [LDAP Scheduled Tasks](#)
- [Creating Custom Scheduled Tasks](#)

15.4.1 Predefined Scheduled Tasks

This release of Oracle Identity Manager provides a set of predefined scheduled tasks that you can use while creating or working with jobs. [Table 15-2](#) lists the predefined scheduled tasks.

Table 15-2 Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Password Expiration Task	This scheduled task sends e-mail to users whose password expiration date had passed at the time when the task was run and then updates the USR_PWD_EXPIRED flag on the user profile.	Email Definition Name: Name of the email definition created in the Design Console for sending password expired notification to the user. The default value is "Password Expired".	Yes
Password Warning Task	This scheduled task sends e-mail to users whose password warning date had passed at the time when the task was run and then updates the USR_PWD_WARNED flag on the user profile.	Email Definition Name: Name of the email definition created in the Design Console for sending password expiration warning notification to the user. The default value is "Password Expiration Warning".	No
User Operations	This scheduled task performs the operation specified by the UserOperation attribute on the user account specified by the UserLogin attribute.	<ul style="list-style-type: none"> ■ UserLogin: User ID of the user account ■ UserOperation: Operation that you want to perform on the user account. The value of this attribute can be ENABLE, DISABLE, or DELETE. 	No
Attestation Grace Period Expiry Checker	This scheduled task delegates the attestation process after the grace period expires.	None	Yes
Task Escalation	This scheduled task escalates pending tasks whose escalation time had elapsed at the time when the scheduled task was run.	None	Yes
Task Timed Retry	This scheduled task creates a retry task for rejected tasks whose retry time has elapsed and whose retry count was greater than zero.	None	Yes
Set User Deprovisioned Date	A deprovisioning date is defined when a user account is created. For users whose deprovisioning date had passed at the time when this scheduled task was run, the task sets the deprovisioned date as the current date.	None	Yes

Table 15–2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Disable/Delete User After End Date	An end date is defined when a user account is created. This scheduled task disables user accounts for which the end date had passed the current date at the time when the task is run. Note: Oracle recommendation is to run this scheduled task every 30 minutes or 1 hour.	None	Yes
Set User Provisioned Date	This scheduled task sets the provisioned date to the current date for users for whom all of the following conditions are true: <ul style="list-style-type: none"> ■ The provisioning date is in the past. ■ The deprovisioned date has not been set. ■ The deprovisioning date has not been reached or is NULL. 	None	Yes
Enable User After Start Date	A start date is set when a user account is created. This scheduled task enables user accounts for which the start date has passed, and the user status is Disabled Until Start Date. These users are enabled thorough this scheduled task, thereby making the users ACTIVE.	None	Yes
Remove Open Tasks	This scheduled task removes information about open tasks from the table that serves as the source for the list displayed in Oracle Identity System Administration.	Day Limit Number of days for which information about an open task should be retained in the table before the information is deleted By default, this attribute is not specified and disabled. You must enable and configure the time.	No
Issue Audit Messages Task	This scheduled task fetches audit message details from the aud_jms table and sends a single JMS message for a particular identifier and auditor entry in the aud_jms table. An MDB processes the corresponding audit message.	Max Records: Use this attribute to specify the maximum number of audit messages to be processed for a specified scheduled task run. The default value of this attribute is 400.	Yes
Initiate Attestation Processes	This scheduled task initiates a call to the Attestation Engine to run attestation processes that are scheduled to run at a time that has passed.	None	Yes
Request Execution Scheduled Task	This is a periodic scheduled task searches for requests with status "Request Awaiting Completion" and moves requests forward to the next stage "Operation Initiated" if the effective date set during the request submission is prior or equal to the current date.	Job Periodic Settings: Use this attribute to specify the time interval for the scheduled task to be run. The default value is 6 hours.	Yes

Table 15–2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Automated Retry of Failed Async Task	This scheduled task retries Async Tasks (JMS Messages) that have failed. If the execution of the task succeeds, it is removed from the list of failed tasks. If it fails, the retry count is incremented. The maximum number of times a Failed Task is retried is determined by the 'maxRetries' defined for that task in async-messaging.xml.	None	Yes
Evaluate User Policies	This scheduled task evaluates the access policies.	<p>Number of Threads: Use this attribute to specify the total number of threads that will process re-evaluation. The default value is 20.</p> <p>Batch Size: Use this attribute to fetch number of records from the database to be processed in one iteration. The default value is 500.</p> <p>Time Limit in mins: Use this attribute to specify time in minutes, after which the schedule task will stop.</p> <p>By default, this attribute is not specified and disabled. You must enable and configure the time.</p>	Yes
Automatically Unlock User	This scheduled task automatically unlocks an user after the specified number of days.	None	Yes
Delayed Delete User	<p>This scheduled task automatically deletes the user whose delete date is set as today. The scheduled task reads the XL.UserDeleteDelayPeriod system property, which indicates the number of days for which user will be in a Disable state when the user is deleted. This scheduled task finds all such users for whom this period has been reached and marks those users as deleted.</p> <p>Note: See "System Properties in Oracle Identity Manager" on page 16-1 for information about the XL.UserDeleteDelayPeriod system property.</p> <p>In Oracle Identity Manager 11g Release 1 (11.1.1.5), this scheduled task is not active by default. In Oracle Identity Manager 11g Release 1 (11.1.1.3), this scheduled task is active by default. However, the state of this scheduled task does not change if Oracle Identity Manager is upgraded from Release 1 (11.1.1.3) to Release 1 (11.1.1.5).</p> <p>Note: Oracle recommendation is to run this scheduled task frequently, such as every 1 hour.</p>	None	No

Table 15–2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Entitlement Assignments	This scheduled task populates Entitlement Assignment schema from child process form table whose field, Entitlement is marked as true.	RECORDS_TO_PROCESS_IN_BATCH: Number of records to process in a batch.	No
Entitlement List	This scheduled task populates Entitlement schema from lookup table whose child process form field, Entitlement is marked as true.	None	No
Get SOD Check Results Approval	This scheduled task gets back the result of SoD Evaluation from the SoD Server, for example, OAACG, SAP, and GRC for all requests waiting for SoD Check results. It reflects the SoDCheckResult and violation in appropriate dataset attributes. It will pick up all requests that are in "SoD check result pending" state and mark them as "SoD check completed".	None	No
Get SOD Check Results Provisioning	This scheduled task gets back the result of SoD Evaluation from the SoD Server, for example, OAACG, SAP, and GRC for all pending SoDCheck provisioning tasks. It reflects the SoDCheckResult and violation in appropriate process form attributes.	None	No
Non Scheduled Batch Recon	This scheduled task tries to process all the events created by non scheduled task based connectors such as PeopleSoft. Such connector created events are in either Event Received State or Data Received State, they only get processed if the batch size specified by the set of events is reached or via this scheduled task. This task executes as per settings to pick up all the unprocessed non scheduled task based events and submits them to the reconciliation engine for processing.	None	No
Orchestration Process Cleanup Task	This scheduled task deletes all completed parent orchestration processes.	Batch Size: Use this attribute to specify the number of completed orchestration processes to be deleted in each iteration. Delete Just One Batch: Use this attribute to specify the value <i>true</i> or <i>false</i> . Only a single batch is deleted if the value is true. All the completed events are deleted batch at a time in a loop if the value is false.	Yes
Refresh Materialized View	The materialized view is used to generate reports related to reconciliation. This view needs to be updated periodically (at a specified interval, for instance, once a day). Therefore, this scheduled task was created to update the view on a periodic basis.	None	No

Table 15–2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Resubmit Uninitiated Approval SODChecks	This scheduled task tries to initiate SoD Check for pending requests, which have SoDCheckStatus as "SoD check not initiated" or "SoD check completed with error". The pending requests are the ones for which SoD initiation failed in first try and are pending for some level of approval.	None	No
Resubmit Uninitiated Provisioning SODChecks	This scheduled task tries to initiate SoD Check by submitting a JMS message for all pending SoDCheck provisioning tasks. The SoD Check initiation may have failed because of SoD server being down at the time of entitlement add/update via direct provisioning.	None	No
Reconciliation Retry Scheduled Task	This scheduled task processes the failed reconciliation event for the users whose status is set as Failed.	None	Yes
Run Future Dated Reconciliation Events	This scheduled task processes the current dated reconciliation event for the users whose status is set as Deferred.	None	No
Job History Archival	This scheduled task is designed to archive/purge entries for Job History.	<p>Archival Date: Use this attribute to specify date till which the records need to be archived/purged.</p> <p>Batch Size: Use this attribute to specify the size of a batch in which the records must be processed.</p> <p>Operation Type: Use this attribute to specify the operation type. This attribute can have two possible values, Archive and Purge.</p> <p>The default value is Archive.</p>	No

Table 15–2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Bulk Load Post Process	This scheduled task starts post processing jobs for the Bulk Load Utility.	<ul style="list-style-type: none"> <li data-bbox="854 289 1209 447">■ Batch Size for Processing Records: User records are processed in batches. This attribute specifies the size of the batch and must have a value. The default is 500. <li data-bbox="854 464 1209 674">■ Generate Password: This attribute specifies whether a password will be automatically generated when users are created with the Bulk Load Utility. It must have a value of Yes or No; the default is Yes. <li data-bbox="854 690 1209 974">■ Ldap Sync: This attribute specifies whether users created in Oracle Identity Manager using the Bulk Load Utility will also be created in the LDAP repository in an LDAP enabled environment. This attribute must have a value of Yes or No; the default is No. <li data-bbox="854 991 1209 1180">■ Notification: This attribute specifies whether users created using the Bulk Load Utility will be notified with an email. It must have a value of Yes or No; the default is Yes. <li data-bbox="854 1197 1209 1455">■ Process User Ids: This attribute specifies the range of user keys (in the Oracle Identity Manager Database) that need to be processed. The keys are associated with the users created using the Bulk Load Utility. It defines a range from start (From:) to finish (To:). 	No
Bulk Load Archival Job	This scheduled task cleans up the processed entries in the Oracle Identity Manager Database staging tables used during bulk load post processing.	<ul style="list-style-type: none"> <li data-bbox="854 1472 1209 1640">■ Archival Date: This attribute specifies the date up to which the records will be purged. It must have a value. The format is ddMMyyyy or MMM dd, yyyy. <li data-bbox="854 1656 1209 1797">■ Batch Size: Database records are cleaned up in batches. This attribute specifies the size of the batch and must have a value. The default is 1000. 	No

Table 15–2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Retry Failed Orchestrations	This scheduled task retries all failed orchestrations based on the attribute values provided. If there is no parameter value defined, no orchestration will be retried.	<ul style="list-style-type: none"> ■ Orchestration ID: This attribute takes a comma separated list of Orchestration Ids to be retried. ■ Entity Type: Orchestrations submitted for the given Entity will be retried. ■ Operation: Orchestrations submitted for given Operation will be retried. ■ Stage: Orchestrations on the given stage will be retried. ■ From Date: Orchestrations submitted after the given date will be retried. The format is ddMMyyyy or MMM dd, yyyy. ■ To Date: Orchestrations submitted before given date will be retried. The format is ddMMyyyy or MMM dd, yyyy. 	No
DataCollection Scheduled Task	This scheduled task is used to populate data from Oracle Identity Manager operational tables to the staging tables in an offline manner. The scheduled task is set to run manually, and is triggered when Oracle Identity Analytics (OIA) invokes the DataCollectionOperationsIntf->startDataCollection API. See " Oracle Identity Analytics " on page 32-2 for information about integration between Oracle Identity Manager and OIA.	None	Yes
Application Instance Post Delete Processing Job	This scheduled task is used to revoke, delete, or decommission application instances that have been soft-deleted. It can be run in the following modes: <ul style="list-style-type: none"> ■ Revoke: Deletes the provisioned accounts from the target system after the application instances has been deleted ■ Delete: Hard-deletes the accounts from all provisioning tasks and targets, and subsequently from Oracle Identity Manager ■ Decommission: Changes the account status to Revoke without keeping the accounts in Oracle Identity Manager in provisioned state 	None	Yes
Catalog Synchronization Job	This scheduled task is used to identify the soft-deleted application instances, and remove them from the catalog.	None	Yes

Table 15–2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Retry Reconciliation Batch Job	This scheduled task is used to re-process batches with the 'Ready for Processing' status.	Batch ID: This is the comma-separated ID of the batches to be retried.	No
Entitlement Post Delete Processing Job	This scheduled task is used for post-processing of entitlement soft deletion in the provisioning component.	None	Yes
Update Accounts with App Instance Job	<p>This scheduled task is used to ensure that application instance keys are populated for all entries in the OIU table.</p> <p>In some instances, the application instance might not be available when the account is provisioned. This is possible when:</p> <ul style="list-style-type: none"> ■ Oracle Identity Manager is upgraded, when <code>app_instance_key</code> is to be populated for all the existing entries in the OIU table. ■ Accounts are brought in via reconciliation, but the application instances are not available when the accounts are reconciled. The application instances are created after the reconciliation. ■ Accounts are provisioned via access policies, but the application instances are not available when the accounts are provisioned. The application instances are created after the provisioning. <p>The Update Accounts with App Instance Job scheduled task checks all the entries in the OIU table corresponding to the resource objects that have a null <code>app_instance_key</code>. It attempts to determine the application instance key based on the <code>obj_key</code> and the IT Resource instance value in the process form. If the scheduled task finds an application instance corresponding to the <code>obj_key</code> and IT resource instance value, then it updates the <code>app_instance_key</code> in the OIU table.</p>	None	Yes

Table 15–2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Entitlement Post Delete Processing Job	<p>This scheduled task is used to revoke or delete entitlements that have been soft-deleted. It can be run in the following modes:</p> <ul style="list-style-type: none"> ■ Revoke: Revokes the entitlement-grant for all the accounts in Oracle Identity Manager, which have that specific entitlement granted. ■ Delete: Hard-deletes the entitlements from the UD_CHILD table. <p>Irrespective of the mode, the entitlement grant entry is removed from the ENT_ASSIGN table.</p>	None	Yes
Risk Aggregation Job	<p>This scheduled task is used for calculating the risk summary value for users, roles, and accounts based on their item-risk and risk-factor levels as defined in the system</p> <p>Note: See "Understanding Risk Aggregation and Risk Summaries" for more information.</p>	<ul style="list-style-type: none"> ■ Number of Concurrent Threads: Use this attribute to specify the number of threads that process risk aggregation. ■ User Batch Size: Use this attribute to specify the number of users that must be processed in each thread. 	No
Certification Event Trigger Job	<p>This scheduled task is responsible for running event listeners against the set of user modification events that have occurred in the system. All event listeners will be executed by default if none are listed in the Event Listener Name List parameter.</p> <p>See Section 6.8, "Configuring Event Listeners and Certification Event Trigger Jobs" for more information.</p>	Event Listener Name List: This is a comma-separated list of event listeners to be evaluated. If no value is specified for this attribute, then all event listeners will be evaluated.	No

15.4.2 LDAP Scheduled Tasks

This release of Oracle Identity Manager provides a set of LDAP scheduled tasks that you can use while creating or working with jobs. These schedule tasks are created only when Oracle Identity Manager is configured with LDAP synchronization. [Table 15–3](#) lists the LDAP scheduled jobs.

See Also: "Configuring the Integration with LDAP" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about configuring the integration between Oracle Identity Manager and LDAP

Table 15–3 LDAP Scheduled Jobs

Scheduled Jobs	Description	User-Configurable Attributes	Enabled By Default
LDAP User Create and Update Reconciliation	<p>This scheduled job reconciles user updates based on the change log from LDAP.</p> <p>The LDAP User Create and Update Reconciliation scheduled job cannot reconcile the User Defined Fields (UDFs). To enable this scheduled job to reconcile UDFs, export the /db/LDAPUser and /db/RA_LDAPUSER.xml files from MDS, make required configuration changes in the files, and import them back to MDS. See "Migrating User Modifiable Metadata Files" in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i> for information about importing and exporting MDS files.</p> <p>Note: While modifying the files, you must not specify any spaces when providing attribute names in the profile.</p>	<p>Last Change Number: Use this attribute to update the last change number of scheduled jobs with last changelog number value of Oracle Internet Directory.</p> <p>Batch Size: Use this attribute to fetch number of entries from the directory in each query.</p> <p>OIM User Type: Use this attribute to specify the user type, for example, End-User or End-User Administrator.</p> <p>OIM User Organization Name: Use this attribute to specify Oracle Identity Manager organization in which reconciled users will be created.</p> <p>OIM Employee Type: Use this attribute to specify the value of employee type for users that are created through reconciliation.</p>	No
LDAP User Delete Reconciliation	<p>This scheduled job reconciles user deletes based on the change log from LDAP.</p>	<p>Last Change Number: Use this attribute to specify the last changelog identifier processed by this job.</p> <p>Batch Size: Use this attribute to fetch number of entries from the directory in each query.</p>	No
LDAP Role Create and Update Reconciliation	<p>This schedule job reconciles role creates or updates based on the change log from LDAP.</p>	<p>Last Change Number: Use this attribute to specify the last changelog identifier processed by this job.</p> <p>Batch Size: Use this attribute to fetch number of entries from the directory in each query.</p>	No
LDAP Role Delete Reconciliation	<p>This schedule job reconciles role deletes based on the change log from LDAP.</p>	<p>Last Change Number: Use this attribute to specify the last changelog identifier processed by this job.</p> <p>Batch Size: Use this attribute to fetch number of entries from the directory in each query.</p>	No
LDAP Role Membership Reconciliation	<p>This schedule job reconciles role membership based on the change log from LDAP.</p>	<p>Last Change Number: Use this attribute to specify the last changelog identifier processed by this job.</p> <p>Batch Size: Use this attribute to fetch number of entries from the directory in each query.</p>	No

Table 15–3 (Cont.) LDAP Scheduled Jobs

Scheduled Jobs	Description	User-Configurable Attributes	Enabled By Default
LDAP Role Hierarchy Reconciliation	This schedule job reconciles role hierarchy based on the change log from LDAP.	Batch Size: Use this attribute to fetch number of entries from the directory in each query. Last Change Number: Use this attribute to specify the last changelog identifier processed by this job.	No
LDAP User Create and Update Full Reconciliation	This schedule job reconciles user creates or updates from LDAP, which includes all users under the search base that is defined in the Directory Server IT resource.	Batch Size: Use this attribute to fetch number of entries from the directory in each query. OIM Use Type: User this attribute to specify the user type, for example, End-User or End-User Administrator. OIM User Organization Name: Use this attribute to specify Oracle Identity Manager organization in which reconciled users will be created. OIM Employee Type: Use this attribute to specify the value of employee type for users that are created through reconciliation.	Yes
LDAP User Delete Full Reconciliation	This schedule job reconciles user deletes from LDAP. It detects the deleted users by comparing the users that exist in Oracle Identity Manager and LDAP.	Batch Size: Use this attribute to fetch number of entries from the directory in each query.	Yes
LDAP Role Create and Update Full Reconciliation	This schedule job reconciles role creates or updates from LDAP, which includes all roles under the search base that is defined in the Directory Server IT resource.	Batch Size: Use this attribute to fetch number of entries from the directory in each query.	Yes
LDAP Role Delete Full Reconciliation	This schedule job reconciles role deletes from LDAP. It detects the deleted roles by comparing the roles that exist in Oracle Identity Manager and LDAP.	Batch Size: Use this attribute to fetch number of entries from the directory in each query.	Yes
LDAP Role Membership Full Reconciliation	This schedule job reconciles role membership from LDAP. It detects the addition or deletion of role membership by comparing the entries existing in Oracle Identity Manager and LDAP.	Batch Size: Use this attribute to fetch number of entries from the directory in each query.	Yes

Table 15-3 (Cont.) LDAP Scheduled Jobs

Scheduled Jobs	Description	User-Configurable Attributes	Enabled By Default
LDAP Role Hierarchy Full Reconciliation	This schedule job reconciles role hierarchy from LDAP. It detects the addition or deletion of role hierarchy by comparing the entries existing in Oracle Identity Manager and LDAP.	Batch Size: Use this attribute to fetch number of entries from the directory in each query.	Yes
Fusion Applications Role Category Seeding	This schedule job will query the LDAP system for all roles and find out their Role Category. If there are new role category in LDAP that are not in Oracle Identity Manager, it creates a new role category in Oracle Identity Manager.	Start Change Log Number: Use this attribute to specify last changelog identifier processed by this job or starting identifier for next run.	Yes

Table 15–3 (Cont.) LDAP Scheduled Jobs

Scheduled Jobs	Description	User-Configurable Attributes	Enabled By Default
LDAP Consolidated Full Reconciliation	<p>This scheduled job runs the following jobs in order:</p> <ol style="list-style-type: none"> 1. LDAP User Create and Update Full Reconciliation 2. LDAP Role Create and Update Full Reconciliation 3. LDAP Role Membership Full Reconciliation 4. LDAP Role Hierarchy Full Reconciliation <p>By default, these jobs are selected in the Job Details page and are automatically triggered when you click Run.</p> <p>The delete full reconciliation jobs, LDAP User Delete Full Reconciliation and LDAP Role Delete Full Reconciliation are not run automatically by this consolidated job.</p> <p>The LDAP Consolidated Full Reconciliation scheduled job consolidates these jobs into a single job and provides all the common parameters in the consolidated job. In addition, this scheduled job provides separate reconciliation parameters to support full reconciliation from specific nodes in LDAP, and a search base for reconciliation.</p> <p>Note: See "Consolidated LDAP Sync Full Reconciliation" in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i> for information about the Reconciliation Search Base, Reconciliation Role Search Filter, and Reconciliation User Search Filter parameters.</p>	<p>Batch Size: Use this attribute to fetch number of entries from the directory in each query.</p> <p>OIM Employee Type: Use this attribute to specify the type of employee, such as full-time employee, intern, contractor, part-time employee, consultant, or temporary.</p> <p>OIM User Organization Name: Use this attribute to specify the organization name of the user.</p> <p>OIM User Type: Use this attribute to specify the type of user, such as End-User or End-User Administrator.</p> <p>Reconciliation Role Search Filter: Use this attribute to specify the search filter for full reconciliation of roles.</p> <p>Reconciliation Search Base: Use this attribute to specify the search base for the full reconciliation of users or roles.</p> <p>Reconciliation User Search Filter: Use this attribute to specify the search filter for full reconciliation of users.</p> <p>Use the following attributes to specify whether or not you want to run the scheduled jobs of the same names as a part of the LDAP Consolidated Full Reconciliation job run:</p> <ul style="list-style-type: none"> ■ Run Role Create and Update Full Reconciliation ■ Run Role Delete Full Reconciliation ■ Run Role Hierarchy Full Reconciliation ■ Run Role Membership Full Reconciliation ■ Run User Create and Update Full Reconciliation ■ Run User Delete Full Reconciliation 	Yes

Note: Granular or node-specific reconciliation is possible by running all the LDAP Consolidated Full Reconciliation jobs. This is achieved by specifying values for the Reconciliation Search Base parameter.

15.4.2.1 Using Attribute-Level Filtering for Running LDAP Sync Incremental Reconciliation Jobs

Changelog query returns incremental changes of user/role account or entries in LDAP server to Oracle Identity Manager database during changelog reconciliation when LDAP Sync incremental reconciliation jobs are run. You might not want to return changes to the database for some entries in LDAP based on a rule or filter during the changelog reconciliation when LDAPSsync incremental reconciliation jobs are run. To do this, you can use the `includeEntriesFilter` filter tag or filter parameter in the `LDAPUser.xml` file to filter out the unwanted entries and bring in only the required entries based on the rule before sending the data for reconciliation, so that those entries would not be in the database. In other words, you can use attribute-level filtering for changelog reconciliation.

See Also:

- ["Mode of Reconciliation"](#) on page 13-8 for information about changelog reconciliation
- "Enabling Postinstallation LDAP Synchronization" in the Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite for information about the `LDAPUser.xml` file, which is a metadata file used for configuring reconciliation profile

The usage of the `includeEntriesFilter` tag is shown in the following example:

```
<parameter name="includeEntriesFilter">
  <value>employeeNumber=123456</value>
</parameter>
```

The `<value>` tag contains the `employeeNumber` LDAP attribute and the corresponding value. This filters out all the changelog entries or user entries from the LDAP server that match the criteria `employeeNumber=123456`, and sends them to the reconciliation engine for the users to be reconciled into Oracle Identity Manager database. Other changelog entries that do not match the filter are stopped from being reconciled into Oracle Identity Manager database.

The following are sample usages of the `includeEntriesFilter` filter parameter:

- `(!(LDAP_attribute=VAL1) (LDAP_attribute=VAL2) (LDAP_attribute=VAL3) ...)`
- If the values are variables, then the filter must be:
`ObjectClass=*`
- `LDAP_attribute_name=SOME_VARIABLE_VALUE`

This means that different users have different attribute values.

Note: Make sure that the LDAP attributes used in the filter value are indexed.

15.4.3 Creating Custom Scheduled Tasks

Oracle Identity Manager provides you with the capability of creating your own scheduled tasks. You can create scheduled tasks according to your requirements if you choose not to use any of the predefined scheduled tasks listed in [Table 15-2](#).

See Also: "Developing Scheduled Tasks" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about creating a scheduled task

To create a custom scheduled task:

1. Create the scheduled task XML file and seed it in MetaData Store (MDS).
2. Develop the schedule task class and package it in a Jar.
3. Upload the Jar by:
 - [Using Plug-ins](#)
 - [Using Database](#)

Using Plug-ins

You can upload the jar using the Plug-in Framework provided by Oracle Identity Manager.

To upload the jar using plug-ins:

1. Create the plugin.xml file.
2. Create the directory structure (plugin.zip) for the scheduled task.
3. Place the ZIP file in the file store (the *OIM_HOME*/plugins/ directory) or database store.

Using Database

You can upload the jar in the database (DB) of Oracle Identity Manager.

To upload the jar using DB:

Upload the jar in DB using UploadJar utility. You can run this utility from the following location:

```
$OIM_HOME/bin/
```

See Also: "Upload Jar Utility" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about running the UploadJar utility

15.5 Jobs

As discussed in one of the earlier chapters, a job is a task that can be scheduled to run at the specified interval. A job run is a specific execution of a job. Each job run includes information such as the start time, stop time, job status, exceptions and status of the execution.

This section discusses the following topics:

- [Creating Jobs](#)
- [Searching Jobs](#)
- [Viewing Jobs](#)
- [Modifying Jobs](#)
- [Disabling and Enabling Jobs](#)
- [Deleting Jobs](#)

15.5.1 Creating Jobs

Note: The procedure described in this section assumes that the XML file for the scheduled task, which contains the job description is available in the *OIM_HOME*/metadata/file directory.

To create a job:

1. Log in to Oracle Identity System Administration with the appropriate credentials.
2. In the left pane, under System Management, click **Scheduler**. The Advanced Administration is displayed with the Scheduler section in the System Management tab active.
3. On the left pane, from the **Actions** menu, select **Create**. Alternatively, you can click the icon with the plus (+) sign beside the View list.
4. On the Create Job page, enter values in the following fields under the Job Information section:
 - **Job Name:** Enter a name for the job.
 - **Task:** Specify the name of the scheduled task that runs the job. Alternatively you can search and specify a scheduled task.

To search and specify a scheduled task:

- a. Click the magnifying glass icon next to this field.
 - b. In the Search and Select : Scheduled Task dialog box, specify a search criterion for the scheduled task and click the icon next to Search field.

A list of all scheduled tasks that meet the search criterion is displayed.
 - c. From this list, select the scheduled task that runs the job being created, and then click **Confirm**.
- **Start Date:** Specify the date and time on which you want the job to run. To do this, select the date and time along with timezone from the date editor and click **Ok**. By default, the timezone is "(UTC-08:00) US Pacific Time".
 - **Retries:** Retry count is used to manage the job in case of failure. A job cannot execute more than its retry count if it fails consecutively. The job is disabled if it fails consecutively till its retry count is exhausted. The job must be enabled from the UI for further execution.
 - **Schedule Type:** Depending on the frequency at which you want the job to run, select one of the following schedule types:
 - **Periodic:** Select this option if you want the job to be run at a time that you specify, on a repeating basis. If you select this option, then you must enter an integer value in the Run every field under the Job Periodic Settings section and select one of the following values:
 - mins
 - hrs
 - days
 - **Cron:** Select this option if you want the job to be run at a particular interval on a recurring basis. For example, you can create a job that must

run at 8:00 A.M. every Monday through Friday or at 1:30 A.M. every last Friday of the month.

The recurrence of the job must be specified in the Cron Settings section. In the Recurring Interval field, you can select any of the following values:

- Daily
- Weekly
- Monthly on given dates
- Monthly on given weekdays
- Yearly

After selecting a value, you can enter an integer value in the Days between runs field.

- **Single:** Select this option if the job is to be run only once at the specified start date and time.
- **No pre-defined schedule:** This option specifies that no schedule is attached to the job you are creating, and therefore, it is not triggered automatically. As a result, the only option to trigger the job is by clicking **Save and Run Now**.

Note: For all the schedule types, if you want the job to be saved run immediately, then click **Save and Run Now**.

A message confirming that the job has been successfully created and triggered is displayed.

15.5.2 Searching Jobs

You can perform the following search operations to search for jobs in the Oracle Identity Administration:

- [Performing a Simple Search for Jobs](#)
- [Performing an Advanced Search for Jobs](#)

15.5.2.1 Performing a Simple Search for Jobs

To perform a simple search for jobs:

1. In the Welcome page of the Advanced Administration, under System Management, click **Search Scheduled Jobs**. Alternatively, you can click the **System Management** tab, and then click **Scheduler**.
2. On the left pane, in the **Search** field, specify the search criterion for the job that you want to locate. You can also include wildcard characters in the search criteria.
3. Click the icon next to the Search field. A list of all jobs that meet the search criterion is displayed.

The search results are displayed in a tabular format with the following columns:

- **Job Name:** This column displays the name of the job. If you want to view the details of the job, then click its name in the column.
- **Status:** This column displays the status of the Job. A job can be in any one of the following statuses:

- **RUNNING:** The job is currently running.
- **STOPPED:** The job is currently not running. However, the job will run again at the date and time specified in the Next Scheduled Run field.
- **INTERRUPT:** The job is interrupted while running. This status may appear if admin server go down in between while job is running.
- **FAILED:** The Job was failed to execute due to some reasons.

15.5.2.2 Performing an Advanced Search for Jobs

To perform an advanced search for scheduler:

1. On the left pane of the Scheduler section, click **Advanced Search**. The Advanced Search: Scheduled Jobs page is displayed.
2. 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.
3. In the Job Name field, enter the job name that you want to search. You can use wildcard characters in your search criteria. Select a search condition in the list adjacent to the Job Name field. The search conditions include Not Contains, Not Begins With, Not Equals, Equals, Ends With, Not Ends With, Contains, and Begins With.
4. For the Status field, select a search condition. Then select a status: **All**, **Running**, or **Stopped**.
5. In the Task Name field, enter the task name. You can use wildcard characters in your search criteria. Select a search condition in the list adjacent to the Task Name field.
6. Click **Search**. The list of jobs that match your search criteria are displayed in the search results table.

Table 15–4 lists the columns of the search results table:

Table 15–4 Fields in the Search Results Table

Field	Description
Job Name	The name of the scheduled job
Task	The task associated with the job
Status	The status of the job, RUNNING, STOPPED, FAILED, or INTERRUPT
Schedule	The schedule or the time for the job to run
Last Run	The time when the job ran for the last time
Enable	The job is enabled or disabled

15.5.3 Viewing Jobs

To view the details of a job:

1. Search for the job whose details you want to view. See "[Searching Jobs](#)" on page 15-23 for information about how to search a job.
2. Click the job whose details you want to view in the Job Name column of the search results table.

The Job Details page is divided into the following sections:

- Job Information: This section displays the fields that provide information about the job. For example, Job Name, Task, Retries, and Start Date fields. If you want to modify the details of the job, then make the relevant change and click **Apply**. See "[Modifying Jobs](#)" on page 15-26 for more information about modifying jobs.
- Job Status: This section displays details of the status of the job in the following fields:
 - Current Status: This field displays the status of the job.
 - Last Run Start: This field displays the date and time of when the job started to run last.
 - Last Run End: This field displays the most recent date and time of when the job stopped running
 - Next Scheduled Run: This field specifies that no schedule is attached to the job you are creating and therefore the job is not triggered automatically. The only option to trigger the job in this case is performing "Run Now" .

Note: No value is displayed in this field if the Schedule Type is No pre-defined schedule.

- Parameters: The parameter values specified are used at run-time while the job is being executed. The values need not be provided at the runtime, they can be there for each job and are used when the job is executed.
- Job History: This section displays a list of all job runs for the job in a table. Each row of the table displays the following information about the job:
 - Start Time: This column displays the date and time at which the job run started its run.
 - End Time: This column displays the time at which the job run ended its run.
 - Job Status: This column displays the status of the job.
 - Execution Status: This column displays the job execution status.

You can reorder the display of columns in the table under the History section:

- a. From the View list, select **Reorder Columns**.
- b. In the Reorder Columns dialog box, select the column name that you want to move.
- c. Depending on the order in which you want to columns to appears, click the up or down arrows.

To add or remove the columns displayed in the table under the History section:

- a. From the View list, select **Columns**.
- b. Depending on your requirement, select one of the following:
 - Show All

- Start Time
- End Time
- Job Status
- Execution Status

c. Repeat Steps a and b for each column that you want to add or remove.

After viewing the details of the job, you can either modify, run, or stop the job. In addition, you can also enable or disable the job. Job Detail screen can be refreshed.

After you view the details of the job on the Job Details page, you can perform one of the following:

- If you want to modify the details of the job, then make the relevant change and click **Apply**. See "[Modifying Jobs](#)" on page 15-26 for more information about modifying jobs.
- If you want to run the job, then click **Run Now**.
- If the Disable button is enable, then it means that the job is currently enabled and you can disable the job by clicking **Disable**.
- If the Enable button is enable, then it means that the job is currently disabled and you and enable the job by clicking **Enable**.
- If you want to refresh a job detail screen, then click **Refresh**.
- If the Stop button is displayed, then it means that the job is currently running and you can stop the job by clicking **Stop**.

15.5.4 Modifying Jobs

To modify a job:

1. Search and view the details of the job that you want to modify. See "[Viewing Jobs](#)" on page 15-24 for information about viewing job details.

Note: If you want to run the job, then click the job name in the first column of the search results table and then click **Run Now**. After you click **Run Now**, you need not perform the rest of the steps in this procedure. However, if you want to modify the job and then run it, then perform the next step and click **Run Now**.

2. On the Job Details page, you can modify all the details of the job, except for the Job Name and Task fields under the Job information section and the fields under the Job Status section. See Step 4 of "[Creating Jobs](#)" on page 15-22 for details about the fields that you want to modify.
3. Click **Apply** to commit the changes made on the Job Details page to the database.
A message confirming that the job has been successfully modified is displayed.

15.5.5 Disabling and Enabling Jobs

In addition to creating and modifying jobs, you can disable a job that is currently enabled, and enable a job that has been disabled earlier. On the Job Details page:

- If the Enabled button is enable, then it means that the job is currently disabled and you can enable it by clicking **Enable**. A job that has been enabled will run only when one of the following is true on the Job Details page:
 - The date and time displayed in the **Start Date** field matches the current date and time.
 - The date and time displayed in the **Next Scheduled Run** field matches the current date and time.
- If the Disabled button is enable, then it means that the job is currently enabled and you can disable the job by clicking **Disable**. A job that has been disabled will not run even when the date and time on which the job has been scheduled to run matches the current date and time.

To enable or disable a job:

1. Search for the job that you want to enable or disable by performing the procedure described in "[Searching Jobs](#)" on page 15-23.
2. On the left pane, in the search results table, right click on the job name and select **Enable** or **Disable**. Depending on whether you click **Enable** or **Disable**, a message indicating that the job has either been successfully enabled or disabled is displayed.
3. Click **OK** to close the dialog box.

15.5.6 Starting and Stopping Jobs

In addition to scheduling jobs to run automatically at the specified time, you can manually start or stop a job at any given time. For example, you create and schedule a job that runs every Friday. However, if you want to run the job on any day other than Friday, then you must run the job manually.

To start or stop a job:

1. Search for the job that you want to start or stop by performing the procedure described in "[Searching Jobs](#)" on page 15-23.
2. On the left pane, in the search results table, click the job name of the job that you want to start or stop.

Note: By default, the status of all jobs is STOPPED unless a job is running.

3. If you want to start a job, then from the Actions list, click **Run Now**.
A dialog box prompting you to confirm if you want to run the job is displayed.
4. If you want to stop a job, then from the Action list, click **Stop**.
A dialog box prompting you to confirm if you want to stop the job is displayed.
5. Click **OK**.

15.5.7 Deleting Jobs

To delete a job:

1. Search for the job that you want to delete by performing the procedure described in "[Searching Jobs](#)" on page 15-23.

2. On the left pane, in the search results table, click the job name of the job that you want to delete.
3. From the Actions list, click **Delete**. Alternatively, you can click the Delete icon next to the icon with the plus (+) sign.

A dialog box prompting you to confirm if you want to delete the job is displayed.

4. Click **OK**. A message indicating that the job has been deleted successfully is displayed.

Managing System Properties

The system configuration service enables you to manage system properties used by Oracle Identity Manager. This service allows you to create, modify, delete, or search existing system properties depending on their roles.

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 Administration and Oracle Identity Manager Self Service by using system properties. For example, you can define the number of consecutive attempts the user can make to login to Oracle Identity Manager unsuccessfully before Oracle Identity Manager locks the user account. In other words, a system property is an entity by which you can control the configuration of Oracle Identity Manager.

This chapter discusses the following topics:

- [System Properties in Oracle Identity Manager](#)
- [Creating and Managing System Properties](#)

16.1 System Properties in Oracle Identity Manager

[Table 16–1](#) lists and describes the default system properties in Oracle Identity Manager.

Table 16–1 Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Access Policy Revoke If No Longer Applies Enhancement Note: This property is not used in Oracle Identity Manager Release 2 (11.1.2), but has been retained only for backward compatibility.	Determines if the Revoke if no longer applies flag in access policy is applicable. If the value is true, then this flag is applicable to child table data (entitlements) along with parent data. The user can determine if child data must be removed or retained when access policy no longer applies to user based on this flag. If the value if false, then child table data (entitlements) are always removed after access policy is no longer applied.	XL.AccessPolicyRevokeIfNoLonger AppliesEnhancement	FALSE
Allows access policy based provisioning of multiple instances of a resource	Determines if multiple instances of a resource can be provisioned to multiple target resources. When the value is false, provisioning multiple instances of resource object via access policy is not allowed. When the value is true, provisioning multiple instances of resource object via access policy is allowed.	XL.AllowAPBasedMultipleAccount Provisioning	false
Are challenge questions disabled in OIM	Determines if challenge questions are enabled or disabled when a user logs in to Oracle Identity Manager for the first time. When value is False, challenge questions are enabled. When value is True, challenge questions are disabled. This property is primarily used in the context of Oracle Adaptive Access Manager (OAAM) configuration. When the value is TRUE, the challenge questions are handled by OAAM.	OIM.DisableChallengeQuestions	FALSE
Catalog search MAX result size. Default value is -1 which means return all	When the data is huge in the request catalog and you encounter any issue with the performance of the catalog, you can change the value of this system property and provide some reasonable values, such as 500. As a result, catalog search will not return more than the specified value. If the value is -1, then no result size limit is applied on the catalog search result.	XL.CatalogSearchResultCap	-1

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
CommonName generation plugin	Determines the common name generation plugin to generate common name.	XL.DefaultCommonNamePolicyImpl	oracle.iam.Idapsync.impl.plugins.FirstNameLastNamePolicy
Compiler Path for Connectors	Specifies the Java home depending on the application server. Note: If the path of the JDK directory is not included in the System Path variable, then you must set the path of the JDK directory in the XL.CompilerPath system property. If this is not done, then an error is encountered during the adapter compilation stage of the process performed when you import an XML file by using the Deployment Manager.	XL.CompilerPath	
Notify other recipients with the password reset email if email of user is null	Specifies whether the manager of the user whose password is being reset must be notified of this password reset, if the email ID of the user is null.	XL.NotifyPasswordGenerationToOther	false
Data Collection Session ID	Specifies the session ID of the current Oracle Identity Analytics (OIA) Data collection session.	XL.DataCollectionSessionID	dummy
Data Collection Status	Specifies the status of the current OIA data collection session.	XL.DataCollectionStatus	FAILED
Default Date Format	When creating reconciliation events by calling the APIs and date format is not passed as one of the arguments to the API, Oracle Identity Manager assumes that all the date field values are specified in Default Date Format.	XL.DefaultDateFormat	yyyy/mm/dd hh:mm:ss z
Default Policy for common name generation	Determines the common name generation policy to be picked while generation of common name.	XL.DefaultCommonNamePolicyImpl	oracle.iam.identity.usermgmt.impl.plugins.FirstNameLastNamePolicy
Default policy for username generation	Determines the username policy to use when generating a username.	XL.DefaultUserNamePolicyImpl	oracle.iam.identity.usermgmt.impl.plugins.DefaultComboPolicy
Default user name domain	This property is used by the DefaultComboPolicy to generate a user name in e-mail format.	XL.UserNameDomain	oracle.com

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Direct Provisioning vs. Request for Access Policy Conflicts	<p>By default, the value of this property is TRUE. If a user has multiple access policies and these policies provision a particular resource multiple times, and at least one policy specifies that the resource can be provisioned directly, then the resource is provisioned without creating a request.</p> <p>Setting this property to FALSE specifies that conflicts are resolved by creating a request for the resource, which are not provisioned directly. If there are no conflicts, then resources are provisioned based on what is defined in the access policy.</p>	XL.DirectProvision	TRUE
Display Certification or Attestation	<p>This property is used to show/hide the certification and/or attestation features. Possible values are:</p> <ul style="list-style-type: none"> ▪ both: This value specifies that all the attestation and identity certification navigation menus and pages are displayed in Oracle Identity Self Service and Oracle Identity System Administration. ▪ attestation: This is the default value. This value specifies that only attestation feature can be used, and all identity certification navigation menus and pages are hidden in Oracle Identity Self Service and Oracle Identity System Administration. ▪ certification: This value specifies that only identity certification feature can be used, and all attestation navigation menus and pages are hidden in Oracle Identity Self Service and Oracle Identity System Administration. <p>Note: After setting the value of this system property, you must restart Oracle Identity Manager.</p>	OIM.ShowCertificationOrAttestation	attestation
Does user have to provide challenge information during registration	If the value is TRUE, then users will have to provide challenge information during registration.	PCQ.PROVIDE_DURING_SELFREG	TRUE

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Duplicate challenge responses allowed	This property is used to indicate whether or not duplicate challenge responses are allowed.	XL.IsDupResponsesAllowed	FALSE
Email Server	Name of the e-mail server. Note: After modifying the Email Server system property value, you must restart the server for the change to take effect.	XL.MailServer	Email Server
Email Validation Pattern	This property contains the regular expression used to validate the email ID of a user.	XL.EmailValidationPattern	[A-Za-z0-9\._\#\!\\$\&\'*\ \/\=\?^\^\\{\}\ \~\ \% \+ \-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}
Enable 9.x permission checking when searching organizations	This property controls the display of organizations in the organization search performed by the user. When XL.EnableOrgPermissionCheck = false, all the organizations are displayed when the user searches for organizations. When XL.EnableOrgPermissionCheck = true or the property is removed, only the organizations assigned to the user performing the search are displayed.	XL.EnableOrgPermissionCheck	TRUE
Enable Exception Reports	This property is used to enable the exception reporting feature. Exception reporting is enabled only if the value is set to TRUE.	XL.EnableExceptionReports	FALSE
Enable disabled resource instances when a user is enabled	If the value is TRUE, then the disabled resource instances are enabled when a user is enabled.	XL.EnableDisabledResources	TRUE
Enables retrying failed callbacks feature	This property enables Oracle Identity Manager to retry failed callback notifications at regular interval. All failed callback notifications are retried in their order of origin. The feature is disabled if the value is set to false. Changing the value to true, enables retry failed callback notifications. Note: If you change the value of this system property, then you must restart Oracle Identity Manager.	OIM.RetryFailedCallbacks	false

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Evaluate LDAP Container Rules for Entity Modification	<p>If the property value is TRUE, then the LDAP container rules defined in LDAPContainerRules.xml are evaluated for entity modification. However, if none of the rules match, then the default container is not returned. The original parent container of the entity is returned, which means that there is no change in the entity DN. For more information, see "Configuring LDAP Container Rules" in <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i>.</p> <p>If the property value is FALSE, then the LDAP container rules defined in LDAPContainerRules.xml are not evaluated. The entity DN does not change.</p> <p>Note: This property only applies to a modification scenario and not to the entity creation scenario.</p>	LDAPEvaluateContainerRulesForModify	FALSE
FA Administrators Role Name IN LDAP	<p>Name of this role, usually "Administrators", stored in the top of the user container in LDAP. This is the user who can login and manage SOA tasks lists.</p> <p>Note: This property is not used in Oracle Identity Manager.</p>	FA.AdministratorsRole	Administrators
FA cookie-http-only flag turned on	This property is seeded using the RoleCategorySeedMXBeanImpl MBean by FA provisioning system.	FA.CookieHTTPOnly	false

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Flag for new permissioning model	<p>This system property determines the data object permission model for inserting, updating, and deleting records in the Oracle Identity Manager database. Before inserting, updating, and deleting records into a database table, Oracle Identity Manager checks the roles assigned to the user who wants to insert, update, or delete records. The roles have data objects assigned to them along with details of permissions to insert, update, or delete a record.</p> <p>For a user to insert, update, or delete records into the table, the user must have permissions for all the roles assigned to him on that data object. If the user does not have insert, update, or delete permission on any one role, then the user is not allowed to insert, update, or delete records in the table corresponding to the data object. This applies when the value of this property is set to <code>FALSE</code>.</p> <p>When the value is set to <code>TRUE</code>, the user must have insert, update, and delete permissions for any one of the roles assigned to the user on a particular data object. If any one permission is available to the user for a role, then the user can insert, update, or delete records in the table corresponding to the data object.</p>	XL.NewPermissionModel	False
Force Password Change at First Login	This system property is not used in Oracle Identity Manager 11g Release 2 (11.1.2.1.0). Setting this property has no effect.	XL.ForcePasswordChangeAtFirstLogin	<p>TRUE or FALSE</p> <p>The default value for this property is <code>FALSE</code> if the user is created by self registration and <code>TRUE</code> if the user is created by any other method.</p>
Force to set questions at startup	<p>When the user logs into the Oracle Identity Self Service or Oracle Identity System Administration for the first time, the user must set the default questions for resetting the password.</p> <p>Note: After modifying the value of this property, you must restart Oracle Identity Manager server for the changes to take effect.</p>	PCQ.FORCE_SET_QUES	False

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
GTC Auto Import	<p>Based on the value of this property, the DM xml that is generated while GTC creation can be saved to a directory.</p> <p>The default value of this property is true.</p> <p>When the value of this property is set to "False", then while creating GTC, the DM xml (the xml that GTC creates and imports using Deployment Manager internally while GTC creation) created by the GTC framework is stored in the following directory:</p> <p><i>OIM_HOME/GTC/XMLOutput</i></p> <p>The naming convention followed for the DM xml is:</p> <p><i>GTCNAME_CURRENTDATE_TIMESTAMP</i> created using date format "yyyy-MM-dd-HH-mm-ss".xml</p> <p>For example:</p> <p>TRUSTEDCSV_2009-02-05-22-41-11.xml</p>	XL.GTCAutoImport	true
Homepage for Self Service console	<p>This property is used to set the page to be displayed after a user logs in to Oracle Identity Manager Self Service.</p> <p>You can set one of the following as the value of this property:</p> <ul style="list-style-type: none"> ▪ my_access: Displays the My Access page ▪ my_info: Displays the My Information page ▪ home: Displays the Home page ▪ catalog_home: Displays the Catalog page ▪ none: Displays no page <p>Note: After modifying the value of this property, you must restart Oracle Identity Manager server for the changes to take effect.</p>	OIM.IdentityHomepage	none
Indicates if referential integrity is enabled in target LDAP directory	<p>The value of this property is TRUE if referential integrity in target LDAP directory is turned on.</p> <p>The value of this property is FALSE if referential integrity in target LDAP directory is turned off.</p>	XL.IsReferentialIntegrityEnabledIn LDAP	FALSE

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Is Self-Registration Allowed	If the value is TRUE, then the users are allowed to self-register.	XL.SelfRegistrationAllowed	TRUE
Is disabled manager allowed	Specifies whether a user in the disabled state can be set as a manager for another user.	AllowDisabledManagers	FALSE
LDAP Reservation Plugin	This property determines the LDAP reservation plugin implementation to be picked up for reservation of user attributes.	XL.LDAPReservationPluginImpl	oracle.iam.identity.usermgmt.impl.plugins.reservation.ReservationInOID
Level of Role Auditing	This property controls the amount of audit data collected when an operation is performed on a role, such as creation or modification. The supported levels are: <ul style="list-style-type: none"> ■ None: No audit data is collected. ■ Role: Creation, modification, and deletion of role is audited. ■ Role Hierarchy: Changes made to the role inheritance is audited. 	XL.RoleAuditLevel	None
Maximum Number of Login Attempts	Determines how many consecutive times the user can attempt to login to Oracle Identity Manager unsuccessfully before Oracle Identity Manager locks the user account. <p>Note: If the user account is locked, then it can be unlocked by any one of the following ways:</p> <ul style="list-style-type: none"> ■ Resetting the password by using Forgot Password ■ Unlocking the user by the delegated administrator ■ Automatic unlocking after the expiry of the lock period, which is done using the Automatically Unlock User scheduled task that runs daily 	XL.MaxLoginAttempts	10
Maximum Number of Password Reset Attempts	Determines how many consecutive times the user can attempt to reset the password unsuccessfully before Oracle Identity Manager locks the user account. <p>Important: When the user account is locked, the user cannot unlock it. If this occurs, then contact the system administrator.</p>	XL.MaxPasswordResetAttempts	3

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Minimum length of challenge response	This property is used to set the minimum length of answers to challenge questions.	XL.ResponseMinLength	0
Number of Correct Answers	This value represents how many questions the user must answer correctly to reset user password.	PCQ.NO_OF_CORRECT_ANSWERS	3
Number of Questions	Sets the number of questions that must be completed by a user who is using the Web Application to reset the user's password.	PCQ.NO_OF_QUES	3 Note: The value set for PCQ.NO_OF_QUES must not be less than the value set for PCQ.NO_OF_CORRECT_ANSWERS.
Number of records to be executed in a batch during Catalog Enrichment	This property determines how many records must be processed in a batch by the catalog job during catalog enrichment.	XL.CatalogEnrichmentBatchSize	500
OIA integration status	Specifies whether OIA is integrated with Oracle Identity Manager. Set the value of this property to <code>TRUE</code> before you add role memberships in Oracle Identity Manager. If you set the value of this property to <code>FALSE</code> , incremental role memberships into OIA will not work. Note: You must do a full import of role memberships at least once after this property is enabled.	OIM.IsOIAIntegrationEnabled	FALSE
Old Password Validator	The property specifies the name of the plugin class to be used for verifying old passwords.	OIM.OldPasswordValidator	oracle.iam.identity.usermgmt.impl.ContainerLoginPasswordVerifier
Organization Delete/Disable Action	If this property is set to <code>TRUE</code> , then users can disable/delete the organization even if the organization contains users and suborganizations. If this property is <code>FALSE</code> , then users cannot disable/delete the organization if the organization contains users and suborganizations. The default value is <code>FALSE</code> .	ORG.DisableDeleteActionEnabled	FALSE

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Pending Cancelled Tasks	If this property is set to TRUE and tasks are configured to allow cancellation while they are pending, then these tasks are moved to Pending Cancelled (PX) status if the corresponding process instance is cancelled. If the property is set to FALSE, then tasks are moved to Cancelled (X) status when corresponding process instance is cancelled. Note that process instances are called by Oracle Identity Manager when the corresponding resource instances are revoked.	XL.PendingCancelled	true
Period to Delay User Delete	This property is used to specify the time period before deleting a user. When this property is set and a user is deleted, the user's state is changed to disabled and "automatically delete on date" is set to current date plus the delay period.	XL.UserDeleteDelayPeriod	0
Property dictates whether database name will be displayed	If the value is TRUE, then the database name is displayed on the Design Console.	XL.TOOLBAR_DBNAME_DISPLAY	TRUE
Proxy User Email Notification	The corresponding PTY_VALUE is the e-mail definition name that is sent when a proxy user is created. User gets a notification e-mail when the user is made the proxy for some other user.	XL.ProxyNotificationTemplate	Notify Proxy User
Recon Batch Size	This property is used to specify the batch size for reconciliation. You can specify 0 as the value for this to indicate that the reconciliation will not be performed in batches. Note: If a profile-level batch size is provided, then it overrides the system batch size setting mentioned in the system properties.	OIM.ReconBatchSize	500 Note: When using trusted source reconciliation from Oracle Directory Server Enterprise Edition (ODSEE), the value of this property must not be 0. When the value is 0, users are not created in Oracle Identity Manager.
Record Read Limit	Sets the maximum number of records that can be displayed in a query result set in the Oracle Identity System Administration.	XL.READ_LIMIT	500

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Request Notification Level	<p>This property indicates whether or not notification is sent to the requester and beneficiary when a request is created or the request status is changed.</p> <p>When the value of this property is 0, then the notification feature is disabled. When the value is 1, then the notification feature is enabled.</p>	RequestNotificationLevel	0
Reset with generated password	<p>If a user's password is to be reset, then this property determines how the password is to be reset by the delegated administrator.</p> <p>If this property is set to true, then the password is always automatically generated. If set to false, then an additional option of setting the password manually is provided.</p>	XL.ResetWithGeneratedPwd	TRUE
Retry Count for recon event	<p>This property determines the reconciliation retry count. The retry count value is picked up from the value of this property.</p> <p>If you specify a value that is greater than 0, then auto retry is configured. If you specify 0 as the value of this property, then auto retry is not configured.</p>	Recon.RetryCount	5

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Role SoD Check Topology Name	<p>This property is used to define the topology name which informs SIL (SoD Invocation Library) the SoD Engine to be used for performing SoD checks. The topology name is defined in the SILConfig.xml file and is a combination of an identity management system, target system and an SoD Engine.</p> <p>Role SoD Check based on SIL is supported only if you are using OIA as the SoD engine. The default topology name set in the SILConfig.xml file if you are using OIA is <code>sodoia</code>.</p> <p>If you set the value of this property to <code>sodoia</code>, then any request raised for roles will go through SoD Check with OIA. An SoD Check is performed only when a request for roles is raised and not in case of direct assignment.</p> <p>If you want to use a topology name other than the default, then it must be defined in the SILConfig.xml file and registered with SIL. For details on registering new topology name with SIL, see "Using Segregation of Duties (SoD)" in <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i>.</p> <p>Note: This property is used only for non-FA role SoD check.</p>	RoleSoDCheckTopologyName	
Search Stop Count	<p>This property determines the maximum number of records that are displayed in the advanced search result. If the search criteria specified returns more number of records than that value of this property, then the number of records displayed is limited to this value. In addition, a warning is displayed stating that the results exceed maximum counts and you must refine your search with additional attributes.</p>	XL.IDADMIN_STOP_COUNT	300
Segregation of Duties (SOD) Check Required	<p>This property indicates whether or not Segregation of Duties (SoD) check is required.</p>	XL.SoDCheckRequired	FALSE

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Send email notification based on user locale	This property determines whether an email notification is sent based on the receiver's (user/manager/assignee/requestor) locale when the value is set to true. If the value is set to false, then the notification is in English irrespective of the receiver's locale.	XL.SendEmailNotificationBasedOn UserLocale	false
Should send notifications in recon or not	Determines if notification is sent to the user when the user login and password are generated in postprocess event handler for user creation via trusted source reconciliation. If the value is set to true, then notification is sent when user login and password are generated in postprocess event handler for user creation via trusted source reconciliation. If the value is set to false, then notification is not sent when user login and password are generated in postprocess event handler for user creation via trusted source reconciliation.	Recon.SEND_NOTIFICATION	true
Show left navigation taskflow panel in Self Service console?	This property is used to specify whether the left pane, which is the primary navigation tool, must be displayed when a user is logged in to Oracle Identity Manager Self Service. Set the value of this property to true to display the left pane. Otherwise, set the value of the property to false. Note: <ul style="list-style-type: none"> ■ If you set the value of this property to false, then you must set the value of the Show toolbar navigation in Self Service console? property to true. ■ After modifying the value of this property, you must restart Oracle Identity Manager server for the changes to take effect. 	OIM.IdentityShowLeftNav	true

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Show toolbar navigation in Self Service console?	<p>This property is used to specify whether the links (in the upper-right-hand corner of the page) such as Accessibility, Help, and so on must be displayed to a user logged in to Oracle Identity Self Service.</p> <p>Set the value of this property to <code>true</code> to display the links. Otherwise, set the value of the property to <code>false</code>.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ If you set the value of this property to <code>false</code>, then you must set the value of the Show left navigation taskflow panel in Self Service console? property to <code>true</code>. ▪ After modifying the value of this property, you must restart Oracle Identity Manager server for the changes to take effect. 	OIM.IdentityShowToolbar	false
Skin Family for OIM UI	The ADF skin family for Oracle Identity Manager UI that the application uses at runtime.	OIM.SkinFamily	fusionFX
Skin Version for OIM UI	<p>The skin version, if any, for the skin family being used for Oracle Identity Manager UI.</p> <p>If the skin has a version, then set <code>trinidad-config.xml</code> <code>SKIN-VERSION</code> to be the skin version of your skin. Otherwise, set the default value for this property if you want to select the skin marked to be the default for that skin family.</p>	OIM.SkinVersion	default

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Specifies the LDAP container mapper plug-in to be used	<p>When Oracle Identity Manager is installed with LDAP synchronization enabled, this plug-in determines in which container users and roles are to be created. Value of this system property indicates the default Oracle Identity Manager plug-in name used for computing the container values. If the default plug-in does not meet the requirement, then you can define your own plug-in to determine the container and specify the name of the plug-in in this system property.</p> <p>Note: For information about this plug-in, see "Developing LDAP Container Rules" in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i>.</p>	LDAPContainerMapperPlugin	oracle.iam.Idapsync.impl.DefaultLDAPContainerMapper
URL for challenge questions modification	<p>When a user is locked, an automatic unlock occurs after a prescribed time period. This property defines that time period in seconds. Therefore, for example, if a user account is locked and the value of this property is 86400 seconds (one day), then the account is automatically unlocked after one day.</p> <p>The value of this property is the URL within OAAM that handles the challenge questions. For example:</p> <p><code>http://OAAM_HOST:OAAM_PORT/OAAM_SERVER/userPreferences.do?showView=registerQuestions</code></p>	OIM.ChallengeQuestionsModificationURL	NONE
URL for change password	<p>This property is used in combination with the property OIM.DisableChallengeQuestions. The value of this property is the URL within OAAM that handles the change password functionality. For example:</p> <p><code>http://OAAM_HOST:OAAM_PORT/OAAM_SERVER/userPreferences.do?showView=changePassword</code></p>	OIM.ChangePasswordURL	NONE

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Unlock Account Automatically After Time Period	<p>This property is used to automatically unlock user accounts after the specified time period.</p> <p>The default value is zero days. This means that user will not be automatically unlocked. To unlock users based on this system property, specify the value as a non-zero positive integer.</p>	XL.UnlockAfter	0 days
Use Row Restriction	<p>Note: This property is for internal use by Oracle Identity Manager. You must not use this property.</p>	XL.UseRowRestriction	FALSE
Use of Default Questions	<p>For customers who have customized their UI to allow end-users to set their own challenge questions, this property determines whether the user must select challenge questions from a predefined list in the Web Application, or if users are required to provide their own questions.</p> <p>Note: Functionality that allows end-users to set their own challenge questions is not supported in the standard out-of-the-box user interface.</p>	PCQ.USE_DEF_QUESTIONS	TRUE
Use semicolon as delimiter in API parameters	<p>This property is used to specify whether or not semicolon should be used as a delimiter to the API input parameter values. Some APIs accepted string input values that are separated by semicolon. This has been changed to use a vertical bar " " instead. To keep backward compatibility, this new property can be used to go back to using semicolons. The default value is FALSE signifying the usage of " ". When set to TRUE, the input for those APIs are accepted with semicolon as separator.</p>	XL.UseSemiColonAsDelimiter	FALSE
User Attribute Reservation Enabled	<p>This property is used to enable user attribute reservation.</p>	XL.IsUsrAttribReservEnabled	TRUE

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
User Id reuse property.Requires dropping the index present on USR_LOGIN column	<p>Determines whether a deleted user account can be reused. To reuse a deleted user account, assign this property a value of TRUE and drop the unique index for the USR_LOGIN column in the USR table and create a nonunique index. To prevent a user account from being reused, assign this property a value of FALSE.</p> <p>Note: It is imperative to de-provision all accounts associated with a deleted user, because if you create a new user with the same user name as that of the deleted user by setting the XL.UserIDReuse property to true, then the new user might get access to offline accounts of the deleted user that was not deleted as part of the de-provisioning process.</p>	XL.UserIDReuse	FALSE
User Language	The user.language value is configured during installation for Locale handling at server side.	user.language	en
User Region	The user.region value is configured during installation for Locale handling at server side.	user.region	US
User Variant	The user.variant value is configured during installation for locale handling at server side.	user.variant	

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
User profile audit data collection level	<p>This property controls the user profile data that is collected for audit purpose when an operation is performed on the user, such as creation, modification, or deletion of a user, role grants or revokes, and resource provisioning or deprovisioning. Depending upon the property value, such as Resource Form or None, the data is populated in the UPA table.</p> <p>The audit levels are specified as values of this property. The supported levels are:</p> <ul style="list-style-type: none"> ▪ Process Task: Audits the entire user profile snapshot together with the resource lifecycle process. ▪ Resource Form: Audits user record, role membership, resource provisioned, and any form data associated to the resource. ▪ Resource: Audits the user record, role membership, and resource provisioning. ▪ Membership: Only audits the user record and role membership. ▪ Core: Only audits the user record. ▪ None: No audit is stored. 	XL.UserProfileAuditDataCollection	Resource Form

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Xellerate User resource provision mode	<p>This property determines whether provisioning of the Xellerate User resource to the user's organization occurs in the database layer through stored procedure, or in the Java layer via Event Handlers.</p> <p>Note: See <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i> for information about Event Handlers.</p> <p>This property has the following allowed values:</p> <ul style="list-style-type: none"> ▪ DB: Provisioning of the Xellerate User resource to the user's organization occurs in the database layer through stored procedure. This in turn does not trigger any further process. Therefore, custom tasks associated with the Xellerate User provisioning process that is associated with the Xellerate User resource does take place. ▪ Java: Provisioning of the Xellerate User resource to the user's organization occurs in the database layer via Event Handlers. Custom tasks associated with the Xellerate User provisioning process that is associated with the Xellerate User resource takes place. This is applicable to the upgrade scenario, where you have your own tasks associated with provisioning processes in earlier releases of Oracle Identity Manager, and you want them to run even after 11g upgrade. In such scenario, set the value of this property value to JAVA. 	XLUserResource.ProvisionMode	DB

Table 16–1 (Cont.) Default System Properties in Oracle Identity Manager

Property Name	Description	Keyword	Default Value
Whether or not email should be validated for uniqueness	<p>This property is available in an Oracle Identity Manager 11g Release 2 (11.1.2.1.0) deployment that has been upgraded from an earlier release of Oracle Identity Manager.</p> <p>If the value of this property is FALSE, then Email Uniqueness check is not performed by Oracle Identity Manager.</p> <p>If the value if TRUE, then Email Uniqueness check is performed by Oracle Identity Manager.</p> <p>Note: If this property is not present, then Email Uniqueness check is performed by Oracle Identity Manager.</p>	OIM.EmailUniqueCheck	TRUE

Oracle Identity Manager provides a set of system properties that are not present in the PTY table by default. You can add these system properties to the PTY table by using the Oracle Identity System Administration, and then use the properties to change some of the default settings in Oracle Identity Manager. For example, if you want to configure the number of times Oracle Identity Manager retries to get a connection when the JDBC connection fails, then you can configure the JDBC Connection Retry Attempts system property.

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information about GTC

[Table 16–2](#) lists the system properties you can add to the PTY table:

Table 16–2 Nondefault System Properties

Property Name	Description	Keyword	Sample Value
OIM Database Query Retry Attempts	<p>Number of times SQL queries to be retried for handling Oracle RAC failures.</p> <p>In the absence of this property in the PTY table, SQL queries for handling Oracle RAC failures are retried three times by default.</p>	OIM.DBQueryRetryAttempts	5
OIM Database Query Retry Interval	<p>Time in seconds after which each SQL retry takes place for Oracle RAC failures.</p> <p>In the absence of the property in the PTY table, SQL query occurs after every 7 seconds by default.</p>	OIM.DBQueryRetryInterval	10 seconds
JDBC Connection Retry Attempts	<p>Number of times Oracle Identity Manager retries to get a connection when the JDBC connection fails.</p> <p>In the absence of this property in the PTY table, the JDBC connection is retried three times by default.</p>	OIM.JDBCConnectionRetryAttempts	5 When the value is 0, it means no retry.
JDBC Connection Retry Interval	<p>Time in seconds between each JDBC connection retry.</p> <p>In the absence of this property in the PTY table, each JDBC connection retry occurs at an interval of 7 seconds.</p>	OIM.JDBCConnectionRetryInterval	10 seconds
Default Tenant GUID	<p>In non-MT mode of Oracle Identity Manager, this property is to be set with a value that works as a tenant GUID for applications that expect a value for the tenant GUID.</p> <p>In MT mode, this property is not required. This is because the tenant GUID is part of the user attributes.</p>	OIM.DefaultTenantGUID	201
Allowed Back URLs	<p>This property is required if you want to setup any non-OIM/OAM URLs to be a valid backURL on the Track Self Registration Request page. Oracle Identity Manager validates the back URLs and redirect URLs against a list of URLs provided by this system property. The value of this property is a comma-separated list of URLs that Oracle Identity Manager allows for redirection.</p>	XL.AllowedBackURLs	http://OIM_HOST:OIM_PORT/

16.2 Creating and Managing System Properties

This section discusses the following topics:

- [Creating System Properties](#)
- [Purging Cache](#)
- [Searching for System Properties](#)
- [Modifying System Properties](#)
- [Deleting System Properties](#)

16.2.1 Creating System Properties

Oracle Identity Manager provides you with the capability of creating your own system properties. You can create system properties according to your requirements if you choose not to use any of the predefined system properties listed in "[System Properties in Oracle Identity Manager](#)" on page 16-1.

You can create a system property by using the Create System Property page in Oracle Identity Manager Administration. You can open this page only if you are authorized to create system properties.

While creating a system property, you specify values for the Property Name, Keyword, and Value fields. These values are saved in the PTY table of the Oracle Identity Manager database.

To create a system property:

1. Login to Oracle Identity System Administration.
2. In the left pane, under System Management, click **System Configuration**. The Advanced Administration is displayed with the System Configuration section in the System Management tab is active.
3. On the left pane, from the Actions menu, select **Create**. Alternatively, you can click the create icon on the toolbar. The Create System Property page is displayed, as shown in [Figure 16-1](#):

Figure 16-1 Create System Property Page

The screenshot shows a web browser window titled "Create System Property". The page has a header with "Welcome" and "Create System Property". Below the header, there are three buttons: "Cancel", "Reset", and "Perform". A legend indicates that an asterisk (*) denotes a required field. The form contains three input fields: "* Property Name", "* Keyword", and "* Value". At the bottom right, there are three buttons: "Cancel", "Reset", and "Perform".

4. On the Create System Property form, enter details of the system property. [Table 16-3](#) describes the fields of this form.

Table 16–3 Fields of the Create System Property Form

Field	Description
Property Name	Enter a name of the system property.
Keyword	Enter a unique ID for the system property. You can enter the keyword in any format. Note: The property name can be translated to various locales, but the keyword cannot be translated.
Value	Enter a value for the system property, for example, 4.

Note: Any special character (.) is not allowed in the beginning or end of Keyword fields while creating or updating a system property. In case of Value fields, special characters are allowed in the beginning or in the end.

- Click **Perform** to create the system property. A message confirming that the system property has been created is displayed. For the new system property that is created, by default, the data level is set to 2 and login_required is set to true.

After the system property is created, you can use SQL to set the values for the following system property fields that are automatically added to the system property recorded in the PTY table of the database:

- Data Level:** Every system property has a data level associated with it. The data level field determines the kind of operations that can be performed on a system property. Data levels are a means of specifying the operations that can be performed on a system property. For example, a data level value of 1 for a system property indicates that the system property can neither be modified nor deleted. The default value of this field is 2.

The data level field cannot be modified by using the UI. It can only be modified by using a SQL script. [Table 16–3](#) lists and describes the various data levels associated with a system property.

Table 16–4 Data Levels Associated with a System Property

Data Level	Description
0	Indicates that the system property can be modified or deleted
1	Indicates that the system property cannot be modified or deleted
2	Indicates that the system property can only be modified
3	Indicates that a system property can only be deleted

- Log In Required:** This field specifies whether or not a login is required to access the system property. The default value of this field is 1, which means that a login is required to access the system property. You can change the value of this field to 0 by using a SQL script.
- LKU_KEY:** This field determines the set of values that can be specified in the Value field of a system property. The default value of this field for a newly created system property is null.

Oracle Identity Manager represents sets using two tables, the LKU and LKV tables. The LKU table holds keys that identify each set. The LKV table defines

the members of each set, in which each row in the LKV table uses one column to identify the set (a LKU_KEY column in the LKU table), and another column to declare a value that will be a member of that set.

LKU_KEY is a column in the LKU table of the Oracle Identity Manager database. For a system property with non-null value in the LKU_KEY column, you can insert the values in this column from a predefined set of values that are in the LKV table. This is done by using a SQL script to include any valid LKU_KEY column value from the LKU table to associate multiple values with the system property. See step 7 for more details.

6. If you want to modify the data level of the system property, then run the following SQL statement:

```
UPDATE PTY SET PTY_DATA_LEVEL=DATA_LEVEL_VALUE WHERE
PTY_KEYWORD = SYSTEM_PROPERTY_KEYWORD;
```

In this SQL statement:

- *DATA_LEVEL_VALUE* is any value listed in the Data level column of [Table 16-4](#).
- *SYSTEM_PROPERTY_KEYWORD* is the unique ID for the system property that you entered in the Keyword field in Step 4.

Note: Any special character (.) is not allowed in the beginning or end of Keyword fields while creating or updating a system property. In case of Value fields, special characters are allowed in the beginning or in the end.

7. If you want to modify the value of the Log In Required field, then run the following command:

```
UPDATE PTY SET PTY_LOGINREQUIRED=LOGIN_REQUIRED_VALUE
WHERE PTY_KEYWORD = SYSTEM_PROPERTY_KEYWORD;
```

In this command:

- *LOGIN_REQUIRED_VALUE* can take a value of either 0 or 1.
If a login is required for accessing the system property, then enter 1. Otherwise, enter 0.
- *SYSTEM_PROPERTY_KEYWORD* is the unique ID for the system property that you entered in the Keyword field in Step 4.

8. If you want to define the set of values that can be specified in the Value field of a system property, then run the following commands:

- a. Run the following command to insert a row into the LKU table:

```
INSERT INTO LKU (LKU_KEY, LKU_LOOKUP_KEY, LKU_TYPE, LKU_GROUP,
LKU_REQUIRED, LKU_TYPE_STRING_KEY, LKU_FIELD, LKU_DATA_LEVEL, LKU_CREATE,
LKU_CREATEBY, LKU_UPDATE, LKU_UPDATEBY, LKU_NOTE, LKU_ROWVER) VALUES
(LKU_KEY_VALUE, LKU_LOOKUP_KEY_VALUE, ...);
```

For example, if you want to update a set of values for the Title field, then run the following INSERT statement:

```
INSERT INTO LKU (LKU_KEY, LKU_LOOKUP_KEY, LKU_TYPE, LKU_GROUP,
LKU_REQUIRED, LKU_TYPE_STRING_KEY, LKU_FIELD, LKU_DATA_LEVEL, LKU_CREATE,
LKU_CREATEBY, LKU_UPDATE, LKU_UPDATEBY, LKU_NOTE, LKU_ROWVER) VALUES (201,
```

Title, ...);

Here, *LKU_KEY_VALUE* is 201 that uniquely identifies the record in the LKU table, and *LKU_LOOKUP_KEY_VALUE* is Title.

Note: You must insert a record in the LKU table before inserting any record in the LKV table because the value of *LKU_KEY* is used in the LKV insert statement.

- b. Run the following command to insert a row into the LKV table:

```
INSERT INTO LKV (LKV_KEY, LKU_KEY, LKV_ENCODED, LKV_DECODED, LKV_LANGUAGE,
LKV_COUNTRY, LKV_VARIANT, LKV_DISABLED, LKV_DATA_LEVEL, LKV_CREATE,
LKV_CREATEBY, LKV_UPDATE, LKV_UPDATEBY, LKV_NOTE, LKV_ROWVER) VALUES
(LKV_KEY_VALUE, LKU_KEY_VALUE, LKV_ENCODED_VALUE, LKV_DECODED_VALUE, ...);
```

For example, to define the set of values for the Title field as Mr, Ms, and Dr, run the following INSERT statements:

```
INSERT INTO LKV (LKV_KEY, LKU_KEY, LKV_ENCODED, LKV_DECODED, LKV_LANGUAGE,
LKV_COUNTRY, LKV_VARIANT, LKV_DISABLED, LKV_DATA_LEVEL, LKV_CREATE,
LKV_CREATEBY, LKV_UPDATE, LKV_UPDATEBY, LKV_NOTE, LKV_ROWVER) VALUES (1001,
201, 'Ms', 'Miss', ...);
```

```
INSERT INTO LKV (LKV_KEY, LKU_KEY, LKV_ENCODED, LKV_DECODED, LKV_LANGUAGE,
LKV_COUNTRY, LKV_VARIANT, LKV_DISABLED, LKV_DATA_LEVEL, LKV_CREATE,
LKV_CREATEBY, LKV_UPDATE, LKV_UPDATEBY, LKV_NOTE, LKV_ROWVER) VALUES (1002,
201, 'Mr', 'Mister', ...);
```

```
INSERT INTO LKV (LKV_KEY, LKU_KEY, LKV_ENCODED, LKV_DECODED, LKV_LANGUAGE,
LKV_COUNTRY, LKV_VARIANT, LKV_DISABLED, LKV_DATA_LEVEL, LKV_CREATE,
LKV_CREATEBY, LKV_UPDATE, LKV_UPDATEBY, LKV_NOTE, LKV_ROWVER) VALUES (1003,
201, 'Dr', 'Doctor', ...);
```

In this example:

- *LKV_KEY_VALUE* is 1001, 1002, and 1003 respectively that uniquely identifies the records in the LKV table
- *LKV_ENCODED_VALUE* is Ms, Mr, and Dr respectively
- *LKV_DECODED_VALUE* is Miss, Mister, and Doctor respectively

See Also: "Configuring Custom Attributes" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information about the LKU and LKV tables

- c. Run the following command to update the value of the *LKU_KEY* column in the PTY table:

```
UPDATE PTY SET LKU_KEY=LKU_KEY_COLUMN_IN_THE_LKV_TABLE
WHERE PTY_KEYWORD = SYSTEM_PROPERTY_KEYWORD;
```

In this command:

- *LKU_KEY_COLUMN_IN_THE_LKV_TABLE* is the value of the *LKU_KEY* column in the LKV table.
- *SYSTEM_PROPERTY_KEYWORD* is the unique ID for the system property that you entered in the Keyword field in Step 4.

Note: If you want to view the changes in Oracle Identity Manager Advanced Administration, then you must run purge cache immediately after modifying a system property by using Microsoft SQL.

16.2.2 Purging Cache

Whenever you make any change to a system property by using any method other than from the Advanced Administration, you must run purge cache to get the changes reflected in Oracle Identity Manager:

To clear the server cache:

1. Depending on the operating system being used, navigate to the following directory:
 - For Microsoft Windows:
`OIM_HOME\server\bin\`
 - For UNIX:
`OIM_HOME/server/bin/`
2. Run one of the following commands:
 - For Microsoft Windows:
`PurgeCache.bat CATEGORY_NAME`
 - For UNIX:
`PurgeCache.sh CATEGORY_NAME`

The `CATEGORY_NAME` name argument represents the Oracle Identity Manager category name that is to be purged, for example, `FormDefinition`. To purge all the categories, pass a value of "All" to the `PurgeCache` utility. It is recommended to clear all the categories.

16.2.3 Searching for System Properties

Oracle Identity Manager Advanced Administration allows you to perform the following types of search operations for system properties:

- [Performing a Simple Search](#)
- [Performing an Advanced Search](#)

16.2.3.1 Performing a Simple Search

To perform a simple search for system properties:

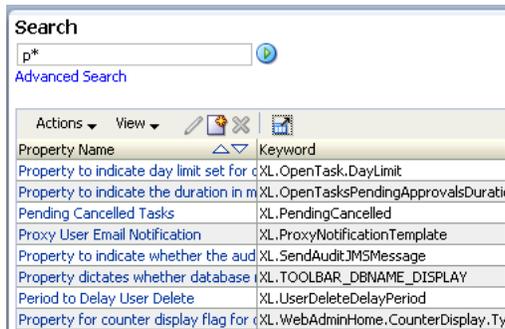
1. In the Welcome page of the Advanced Administration, under System Management, click **System Configuration**. Alternatively, you can click the **System Management** tab, and then click **System Configuration**.
2. In the left pane, enter a search criterion in the Search field for the system property that you want to search. You can include wildcard characters (*) in your search criterion.

If you enter * in the Search field, then all the system properties are displayed. You can filter your search by combining characters with the wildcard characters. For

example, to search all system properties starting with p, you can enter p* in the Search field.

3. Click the icon next to the Search field. A list of all system properties that meet the search criterion is displayed, as shown in [Figure 16–2](#).

Figure 16–2 List of System Properties



The search results table displays the system property names and keywords. You can click a property name to open the details for the system property.

16.2.3.2 Performing an Advanced Search

To perform an advanced search for system properties:

1. In the left pane of the System Configuration section, click **Advanced Search**. The Properties: Advanced Search page is displayed.
2. In the list adjacent to the Property Name field, select a search condition.
3. In the Property Name field, enter a search criterion for the system property that you want to search. You can include wildcard characters (*) in your search criterion. Select the search conditions in the list adjacent to the fields. The search conditions include Not Contains, Not Begins With, Not Equals, Equals, Ends With, Not Ends With, Contains, and Begins With.
4. Click **Search**. The system properties that match the search criterion are displayed in the search results table, as shown in [Figure 16–3](#):

Figure 16–3 Advanced Search Result

Key	Property Name	Keyword	Value	Allowed Values	Date Level
61	Specifies the LDAP container mapping	LDAP.ContainerMapping	oracle.iam.ldapsync.ii		2
77	Account Post-Process	OIM.ReconAccountProc	0		2
76	Recon Batch Size	OIM.ReconBatchSize	500		2
23	Organization Delete/Disable	ORG.DisableDeleteAction	FALSE		2
19	Organization Self-Service	ORG.SELF_SERVICE	FALSE		2
13	Force to set question	PCQ.FORCE_SET_Q	TRUE		2
36	Number of Correct Answers	PCQ.NO_OF_CORRECT	10		2
11	Number of Questions	PCQ.NO_OF_QUESTIONS	3		2
40	Does user have to provide duration	PCQ.PROVIDE_DURATION	TRUE		2
12	Use of Default Questions	PCQ.USE_DEF_QUESTIONS	TRUE		2
44	Compiler Path for Core	XL.CompilerPath			2
75	Is Configured in SSI	XL.ConfiguredInSSIM	FALSE		2

The search result displays key, property name, keyword, value, allowed value, and date level for each system property.

16.2.4 Modifying System Properties

A modify operation lets you modify an existing system property by using the System Property Detail page. If any system property is tagged with a set of allowed values, then you must specify a value from that set only.

Note: While modifying a system property that has multiple values attached to it, a message is displayed if the modified value is not part of the values defined in the LKU and LKV tables. For information about associating multiple values to a system property, see step 7 of ["Creating System Properties"](#) on page 16-23.

You cannot modify the Property Name and Keyword fields of a system property created in a non-English locale. As a workaround, delete the existing system property and create a new one with the desired values.

In an English locale, non-ASCII characters are allowed in a system property name. When you modify the name of a system property to include non-ASCII characters, you must ensure the following if you want the changes to be translated into other languages:

As the translation bundles (.properties file) are not automatically updated, you must update the .properties file corresponding to the language into which you want the name to be translated. The value of the Property Name field of a system property is the translation key for all translation bundles. If the system property name contains a space, then you must replace the space with the tilde (~) character. This is illustrated by the following example:

Suppose you change the name of a system property to "Direct Provisioning vs Request for Access Policy Conflicts" in an English locale. Now suppose you want this to be translated to Italian. The given key and translation value in the translation bundle for Italian is as follows:

```
Direct-Provisioning-vs-Request-for-Access-Policy-Conflicts = Provisioning diretto rispetto a richiesta di conflitti dei criteri di accesso
```

Change the above entry to:

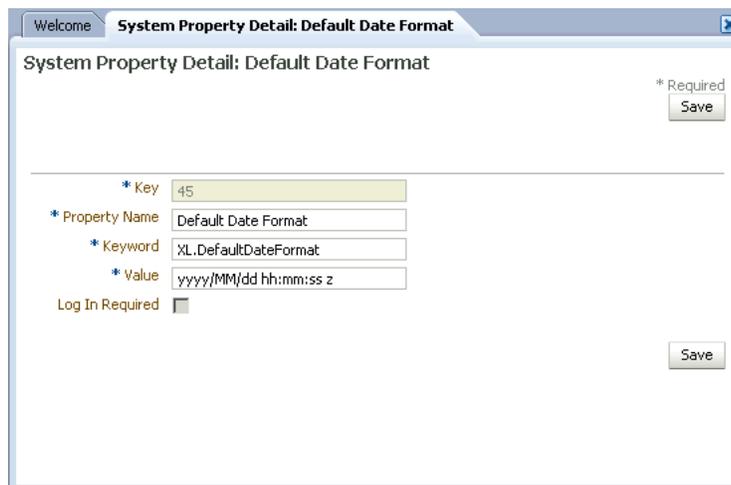
```
Konflikt-zwischen-direktem-Provisioning-und-Anforderung-von-Zugriffs-Policy-XL = Provisioning diretto rispetto a richiesta di conflitti dei criteri di accesso
```

To modify a system property:

1. Search for the system property that you want to modify.
2. In the Property Name column of the search results table, click the system property that you want to modify.

The System Property Details page is displayed, as shown in [Table 16-4](#).

Figure 16-4 System Property Detail Page



3. If you want to modify the Property Name, keyword, and the Value fields, then perform Step 4 of "[Creating System Properties](#)" on page 16-23.
4. If you want to modify the Log In Required field, then perform Step 7 of "[Creating System Properties](#)" on page 16-23.
5. If you want to modify the Allowed Values column, then perform Step 8 of "[Creating System Properties](#)" on page 16-23.
6. If you want to modify the data level associated with a system property, then perform Step 6 of "[Creating System Properties](#)" on page 16-23.
7. Click **Save** to save the changes made.

A message confirming that the system property has been modified is displayed.

16.2.5 Deleting System Properties

To delete a system property:

Note: You can delete a system property only if the data level of that system property is set to either 0 or 3. While deleting a system property, a message is displayed if the data level associated with the system property is not appropriate. For a description of the data levels, see [Table 16-4, "Data Levels Associated with a System Property"](#).

1. In the Advanced Administration, click the **System Management** tab and then click **System Configuration**.
2. On the left pane, search for the system property that you want to delete.
3. In the Property Name column of the search results table, select the system property that you want to delete.
4. From the Actions menu, select **Delete**. A message is displayed asking for confirmation. Click **OK**.
5. A message is displayed confirming that the system property has been deleted. Click **OK**.

Part VII

Requests

This part describes the administration of request catalog and request service.

Part I contains the following chapter:

- [Chapter 17, "Managing the Access Request Catalog"](#)

Managing the Access Request Catalog

This chapter provides an introduction to the Access Request Catalog and describes the key features, benefits and use cases of the Access Request Catalog. It contains the following sections:

- [Section 17.1, "Access Request Catalog"](#)
- [Section 17.2, "About the Access Request Catalog"](#)
- [Section 17.3, "Administering the Access Request Catalog"](#)
- [Section 17.4, "Managing the Lifecycle of the Catalog"](#)
- [Section 17.5, "Troubleshooting"](#)

The Access Request Catalog provides a simple, intuitive, web-based user interface that allows business users to request access to roles, application instance, and additional access (also known as entitlements) within applications.

The Access Request Catalog allows a business to categorize and publish roles, application instance, and entitlements to the Catalog and provide additional business context using extensible metadata. Users use familiar request access for themselves using an intuitive "Catalog search" and "Shopping Cart" user experience.

17.1 Access Request Catalog

This section provides an introduction to the Access Request Catalog. It contains the following sections:

- [Section 17.1.1, "Access Request Challenges"](#)
- [Section 17.1.3, "Catalog Use cases"](#)
- [Section 17.1.2, "Concepts"](#)

17.1.1 Access Request Challenges

Enterprises have tried to simplify and streamline the process of managing the identity lifecycle and access privileges of end users as part of improving operational efficiency and reducing IT costs. To meet these goals, businesses have tried to implement various solutions to allow end users to manage their own identity and access. However, they have faced several challenges in doing so:

- End-users had to be trained to understand IT concepts and terminology and use IT processes to request access.

- The training cycle had to be repeated as new employees joined, lowering productivity, and increasing IT costs.
- End-users had to get IT assistance when their requests were not fulfilled in a timely manner and did not have visibility into the status of their request.
- Typically, additional access within an application had to be granted by IT or by Application administrators.
- This limited business users' view of available access and limited their productivity, while forcing them to rely on IT.

The Access Request Catalog addresses these challenges by providing an easy to use web interface where users can search and browse various types of access and select the ones they need to perform their job duties. It provides the following benefits:

- The end user does not need to know technical jargon or follow IT processes to request access. The Catalog uses well-known and familiar search and shopping cart patterns to guide the user through the access request process.
- The end-user does not need to know specific application instance, role or entitlement names. The Catalog provides an extensible metadata model and provides tagging capabilities. This allow business users to specify alternate terms to be used to search for the specific access. End users can search the Catalog using combinations of keywords and wildcards to search for the access they need.

17.1.2 Concepts

The following discussion introduces key access request catalog concepts

- **Catalog**
Catalog (aka Request Catalog) offers a consistent and intuitive request experience for customers to request Roles, Entitlements and Application Instances 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 item (Roles, Entitlements or Application Instances) that can be requested by a user, either for themselves or on behalf of other users.
- **Category**
A Catalog Item 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 System Administrators can edit a Catalog Item and provide a value for the category.

Note: You cannot leave Category field blank for a catalog item. Therefore, you must ensure that a value is present for the category.

- **Application Instance**
An Application Instance represents an account on particular target. When users request an application instance, they are requesting an account in a particular target. Application Instances can be connected, if fulfillment is automated via a Connector, or disconnected, if fulfillment is manual. Application Instances can have entitlements associated with them.
- **Enterprise Roles**

Enterprise Roles are defined by customers. Enterprise Roles have policies associated with them. Users can request enterprise roles via the Catalog. When a role is granted, application instances or entitlements are provisioned to the user.

- Entitlement

Entitlements are privileges in an application that govern what a user of the application can do.

- Catalog User-defined field

Catalog User-defined fields are additional attributes that are added by customers to the Catalog entity

- Catalog Item Metadata

Catalog Item Metadata refers to the values for the Catalog Item attributes. Metadata can be managed on a per-item basis by the Catalog System Administrator or can be populated in bulk.

- Tags

Tags are search keywords. When users search the Access Request Catalog, the search is performed against the tags. Tags are of three types

- Auto-generated: The Catalog synchronization process auto-tags the Catalog Item using the Item Type, Item Name and Item Display Name
- User-defined: User-defined Tags are additional keywords entered by the Catalog System Administrator
- Arbitrary tags: While defining a metadata if user has marked that metadata as searchable, then that will also be part of tags.

- Catalog System Administrator

The Catalog System Administrator is a global security role. The Catalog can be managed by members of this role only.

- Shopping Cart

The Shopping Cart refers to the collection of Catalog Items that are being requested. A user can have only one cart active at any given time and the cart can contain roles, application instances, entitlements, or any combination of the three.

- Catalog synchronization

Catalog synchronization refers to the process of loading roles, application instances, and entitlements into the Catalog.

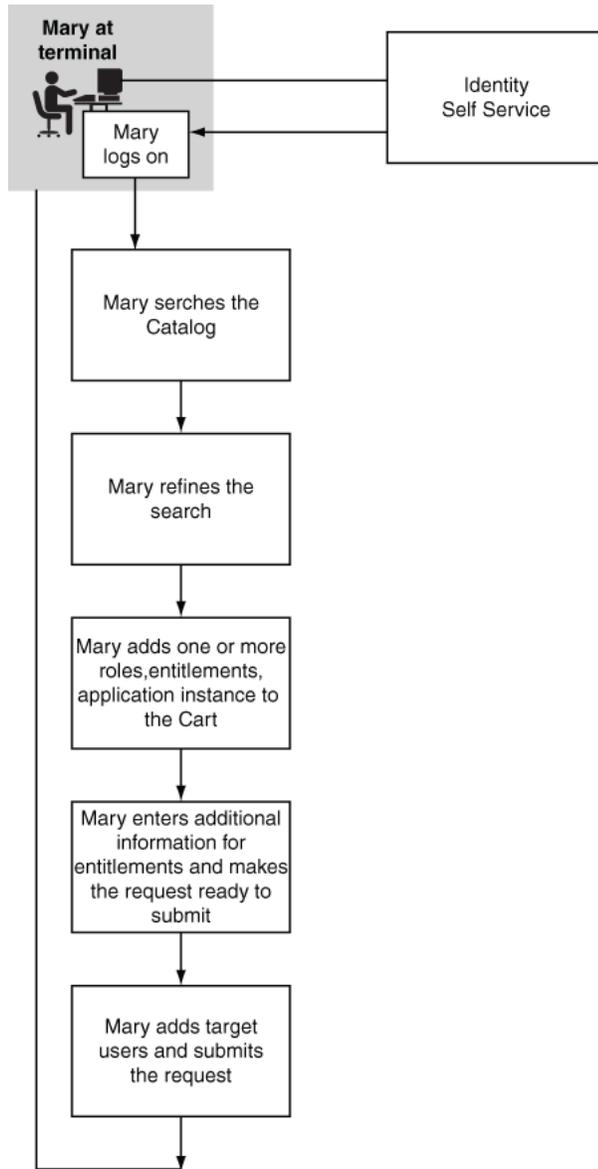
17.1.3 Catalog Use cases

Use cases in this section explain how the access request catalog make it easy for end users to request roles, application instance, and entitlements required to perform their duties.

Requesting access

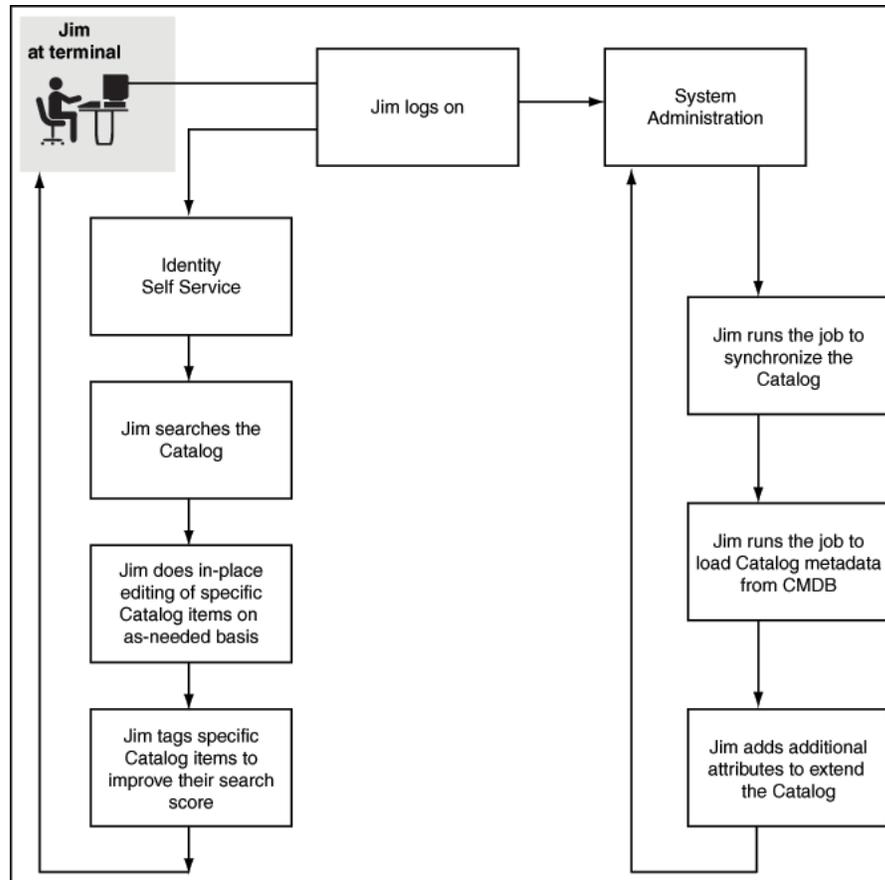
Mary, a Manager in MyCorp, would like to request access to MyCorp Trading application for herself and her directs. To do this, she searches the Catalog using the keyword trading. The catalog returns all items that match Mary's keywords and that she is allowed to request. Mary filters the search results by selecting Application from the list of categories. The Catalog returns a reduced set of search results. Mary adds

the MyCorp Trading application to the cart and checks out. She adds herself and her directs to the request and submits the request.



Administering the Catalog

Jim, a Catalog System Administrator, would like to onboard new application instance and their entitlements, add additional attributes and improve the searchability of the catalog items. He runs the Catalog Synchronization job to harvest the new application instance and their entitlements. Next, he extends the Catalog metadata by adding additional attributes and identifies certain attributes as searchable. Next, he loads the catalog with metadata and tags for the new attributes. For certain Catalog items, he searches the Catalog and edits the Catalog item in place.



These use cases are typical examples of using the Access Request Catalog to make applications and entitlements in the applications and roles visible in the Catalog and allowing users to request access to them via simple web-based interface.

17.2 About the Access Request Catalog

This section covers the features and benefits of the Access Request Catalog and its architecture. It contains the following topics

- [Section 17.2.1, "Features and Benefits"](#)
- [Section 17.2.2, "Architecture"](#)

17.2.1 Features and Benefits

The Access Request Catalog is a searchable, categorized collection of entities that are requestable in Oracle Identity Manager. Any authenticated user can access the Catalog and search the Catalog using one or more keywords and search operators, add one or more Catalog items into a shopping cart and submit a request for themselves and others.

Key features of the access request catalog include:

- Extensible Catalog schema that allows administrators to add additional attributes and specify how the attribute is rendered using a simple browser-based UI
- Automated harvesting of roles, applications, and entitlements

- Automated loading of Catalog metadata using a CSV file
- Powerful search using keywords with support for complex search operators
- Flexible categorization model that allows the Catalog to be organized based on customer choice
- Catalog search results secured based on viewer privileges of the requester
- Catalog item data available via a web service for use in workflows

17.2.2 Architecture

Figure 17–1 High-Level Catalog Architecture

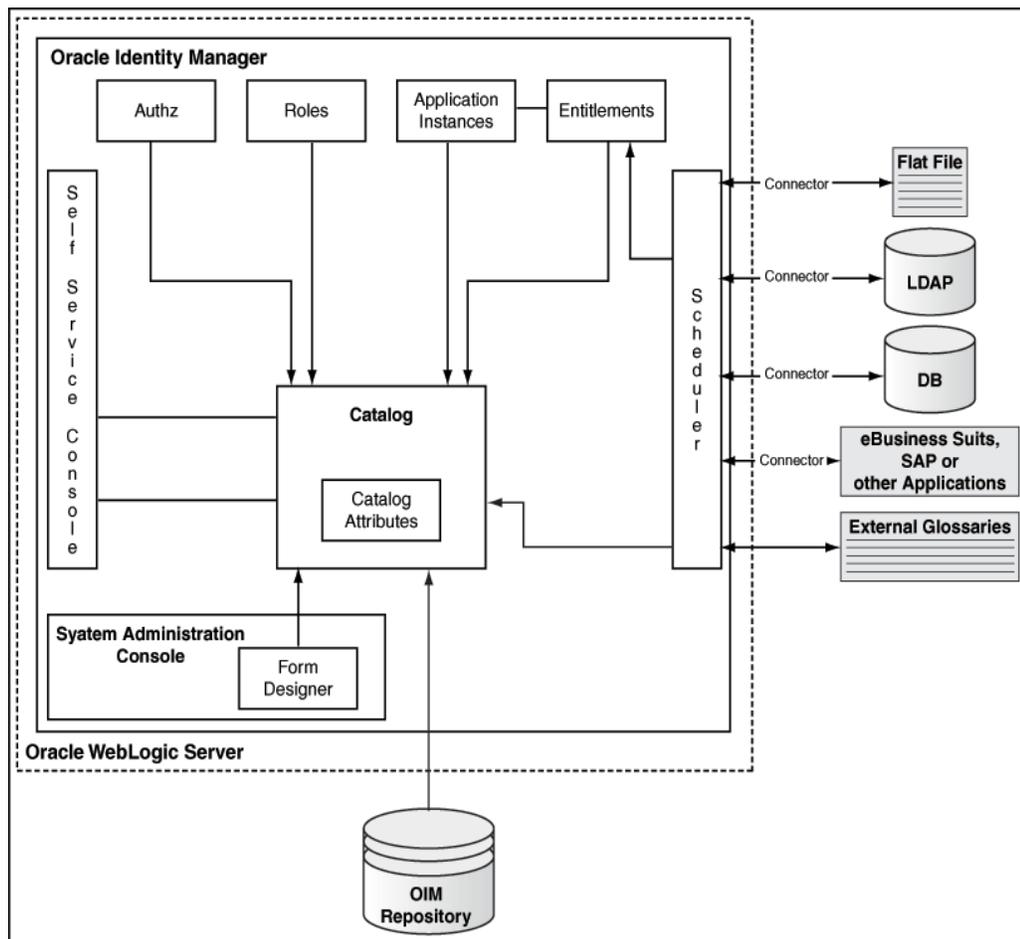


Figure 17–1 shows the components of the Access Request Catalog and its relationship with other components of Oracle Identity Manager. The Access Request Catalog consists of the following components:

1. Catalog Tables
2. Catalog Loaders
3. Catalog Metadata
4. Catalog User Interface in the Identity Self Service Console

17.3 Administering the Access Request Catalog

This section describes the basic administration of the Access Request Catalog. It consists of the following topics

- [Section 17.3.1, "Pre-requisites"](#)
- [Section 17.3.2, "Common Tasks"](#)
- [Section 17.3.3, "Database Best Practices for Access Request Catalog"](#)

17.3.1 Pre-requisites

The Access Request Catalog is used by end-users to request access to roles and entitlements to help them perform their duties. As a result, it is very important that the Catalog be current, have a rich metadata and be organized so that users can find the right access. To ensure this, you need to have a plan to manage the Access Request Catalog. The ensuring sections give the steps that you should follow to administer the Catalog. Before implementing those steps, there are certain pre-requisites. These include

- [Section 17.3.1.1, "Setting up the Catalog System Administrator"](#)
- [Section 17.3.1.2, "Defining the Catalog Metadata"](#)

17.3.1.1 Setting up the Catalog System Administrator

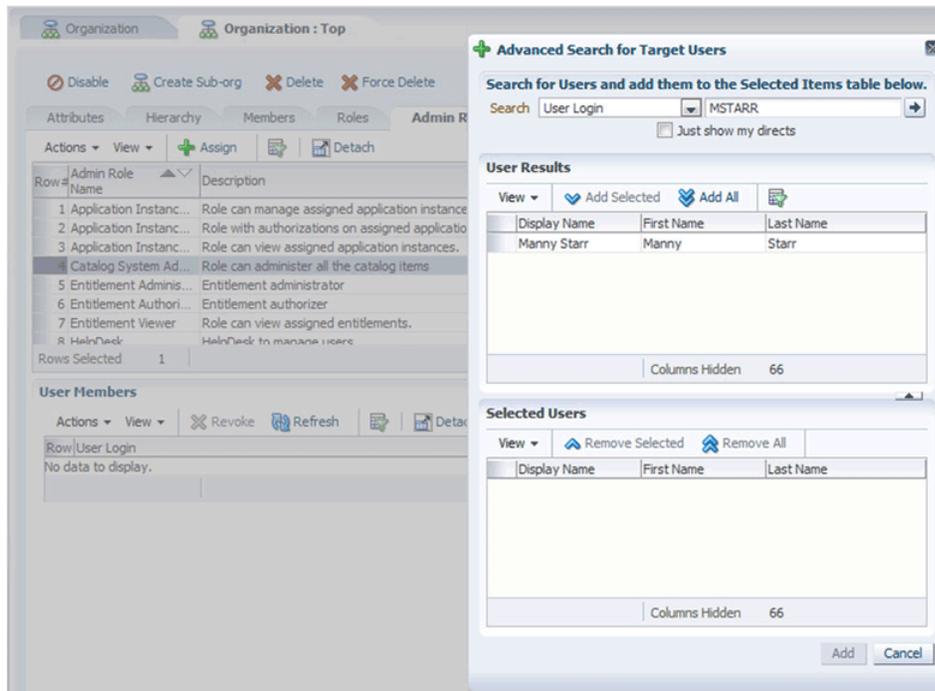
The Catalog System Administrator is an admin role, similar to the System Administrator and System Configurator role. In Oracle Identity Manager 11g Release 2 (11.1.2.1.0), a member of this role (and those of the System Administrators role) can perform the following actions:

- Load the Catalog
- Manage Catalog Items
- Manage Request Profiles

This role is a global role and not scoped by organization.

To grant the Catalog System Administrator:

1. Log in to the Oracle Identity System Administration Console.
2. Click **Organizations**.
3. Search and open the Top organization.
4. Click the **Admin Roles** tab.
5. Select the **Catalog System Administrators** admin role and click **Assign** in the toolbar.
6. Search and select the users that you want to assign, and click **Add Selected**.



7. Click **Add** to add the users.

The new members of the Catalog System Administrator role can login to the Self Service Console and start managing the Catalog.

17.3.1.2 Defining the Catalog Metadata

A rich catalog metadata is important to for the following reasons:

- End-users are only interested in getting access to what they need to perform their job duties. When they search and browse the Catalog, the information presented to them must relate to the business. If the Catalog is sparse (minimal attributes), users will not know which access to pick. If the Catalog is rich but technical, users will get confused and will choose not to use the Catalog.
- Requesters and Approvers need as much contextual information as possible to help them submit a request or approver one. When approvers review a request, the Catalog item detail helps them understand what is being requested, why and the impact of approving the request.
- Approval workflows use routing rules to correctly determine approvers. These rules need access to additional context about the requested item to do approver resolution. If the Catalog information is sparse, the routing rules will not have enough data available to determine the correct approvers.

To meet these challenges, the Catalog must contain additional metadata that can help place the access, that is the Catalog item, in the correct business context.

To add one or more attributes to the Catalog:

1. Log in to the Oracle Identity System Administration Console.
2. Click **Sandboxes, Create Sandbox**.



3. Click **Save and Close** to create and activate the sandbox.



4. Ensure that you are in the correct and activated sandbox session.
5. Click **Form Designer**.
6. Select **Catalog** from the Type drop-down list.
7. Click **Search**
8. Select the **Catalog** entity and click **Open**
9. Click **Custom New Attribute** to add an attribute.

See Also: See "Developing Process Forms" for more information on the Form Designer and its capabilities and "Managing Sandboxes" for more information on the Sandbox and its capabilities

10. Select from one of the pre-defined attribute types and click **OK**.
11. Provide the necessary information and click **Save and Close**.

Note: When you create a field (UDF) using form designer for an entity, you can specify the length of the field. During that time, you must ensure that you have chosen a significant value. Similarly, when you create a form for an existing process form make sure that fields in the process form have significant size to accommodate the necessary value size.

12. Add additional attributes as required.
13. You have completed the first step in extending the Catalog.
14. If you do not want to modify the Catalog search results or Catalog Item details UI, then you can have your changes reviewed and after approval of the changes, click **Publish** to publish the sandbox.
15. If you want to modify the Catalog search results and Catalog Item details UI, then proceed further.

16. Logout and login to the Identity Console as a member of the System Administrator role.
17. Click **Sandboxes** and select the same sandbox that you used to extend the Catalog.
18. Click **Activate** to activate the sandbox.
19. Publish the Sandbox by selecting the sandbox and clicking **Publish Sandbox**

17.3.2 Common Tasks

This section describes the common tasks to be performed by the Catalog System Administrator. It consists of the following tasks:

- [Section 17.3.2.1, "Onboard Applications and Roles"](#)
- [Section 17.3.2.2, "Bootstrapping the Catalog"](#)
- [Section 17.3.2.3, "Ongoing Synchronization"](#)
- [Section 17.3.2.4, "Enrich the Catalog"](#)
- [Section 17.3.2.5, "Managing Catalog Items"](#)

17.3.2.1 Onboard Applications and Roles

The Access Request Catalog must be populated with enterprise roles, application instances and entitlements so that users can search and request for access. You must develop a process by which enterprise roles, application instances and entitlements can be on-boarded to the Catalog with minimal administrator intervention. This section covers the various steps involved in on-boarding roles, application instances and entitlements into the Catalog.

17.3.2.1.1 Prepare an Onboarding checklist Use the following onboarding checklist items to develop a high-level process for onboarding roles, application instances and entitlements into the Access Request Catalog. Later, you can follow individual checklists for roles, application instances, and entitlements.

- Identify Catalog System Administrators
- Identify and extended Catalog attributes
- Customize Catalog search results UI
- Customize Catalog Item Details UI
- Identify navigational categories
- Identify Owners, Certifiers, Approvers for roles and applications
- Identify sources of truth for Catalog Item metadata/glossary
- Develop procedures to generate and load Catalog item metadata/glossary
- Develop glossary of tags and a process to maintain tags

17.3.2.1.2 Onboarding Roles There are no onboarding steps for enterprise roles. Roles, belonging to a role category other than OIM Roles are published directly to the Catalog when they are created.

When user edits the role and changes its category from OIM Role to any other category, then the Catalog Synchronization scheduled job must be run to have the role searchable in the catalog.

17.3.2.1.3 Onboarding Application Instances Application Instances require additional configuration before they can be requested by end users. Use the following checklist items to make sure that you have performed the configuration required to onboard application instances:

- Ensure that the Connector is installed (for new targets)
- If you are upgrading Oracle Identity Manager from Release 9.1.x or 11g Release 1 to 11g Release 2 (11.1.2.1.0), see "Upgrading Oracle Identity Manager 11g Release (11.1.1.5.0) Environments" of the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for information about mandatory post-upgrade steps
- Verify that the process forms have an IT resource field
- Verify that you have defined the form field properties correctly
- Verify that you have created the application instances with suitable display names and descriptions
- Verify that you have created the forms required for account requests
- Verify that you have published the application instances to the relevant organizations
- For disconnected applications, verify that you have created the application instances. See [Section 10.2.1, "Creating a Disconnected Application Instance"](#) for detailed description of the steps

After verifying the steps in the check list, follow the instructions below to onboard application instances.

See Also: [Section 9.2, "Managing Application Instances"](#) for more information on managing Application Instances

Steps to onboard Application Instances

1. Login to the **System Administration** Console as a member of the System Administrator role
2. Click **Scheduler**
3. Search for the **Catalog Synchronization** job
4. Check the **Process Application Instances** parameter
5. Set the parameter **Mode** to Incremental

17.3.2.1.4 Onboarding Entitlements Use the following checklist items to make sure that you have performed the configuration required to onboard entitlements.

Note: Job entitlement list loader should be executed before executing catalog synchronization job.

- Ensure that the Connector is installed (for new targets)
- If you are upgrading Oracle Identity Manager from Release 9.1.x or 11g Release 1 to 11g Release 2 (11.1.2.1.0), see "Upgrading Oracle Identity Manager 11g Release (11.1.1.5.0) Environments" of the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for information about mandatory post-upgrade steps

- Verify that the process forms have an IT resource field
- Verify that you have defined the form field properties correctly
- Verify that you have correctly associated the parent and child forms
- Verify that you have run the common lookup reconciliation job for ICF-based targets
- Verify that you have run the connector-specific lookup reconciliation jobs for non-ICF connectors
- Verify that you have created application instances correctly, corresponding to the resource object and IT resource instance specified in the Lookup Reconciliation job
- Verify that you have published entitlements to relevant organizations
- Verify that you have run the entitlement list loader job, so that data can be populated in ent_list table

After verifying the steps in the check list, follow the instructions below to onboard entitlements

Steps to onboard Entitlements

1. Log in to the **Oracle Identity System Administration** Console as a member of the System Administrator role.
2. Click **Scheduler**.
3. Search for the **Catalog Synchronization** job.
4. Check the **Process Entitlements** parameter.
5. Set the parameter Mode to **Incremental**.

Note:

- If its a first time harvesting, then you should set the parameter to **Full**.
 - If the parameter mode is Incremental, then only those entities will be picked by scheduled task for processing, whose create date is greater than update date for creation, and update date is greater than update date value.
-
-

17.3.2.2 Bootstrapping the Catalog

Bootstrapping refers to the process of populating the Catalog for the first time. After Bootstrapping large number of any entity, you can gather statistics on base tables. This section refers to bootstrapping the Catalog after you have installed Oracle Identity Manager 11g Release 2 (11.1.2.1.0). If you are upgrading from Oracle Identity Manager 9.1.x or 11g Release 1, then see Chapter, "Upgrading Oracle Identity Manager 11g Release (11.1.1.5.0) Environments" of the Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management.

Pre-requisites

- You have extended the Catalog using the Form Designer by following the steps given in [Section 17.3.1.2, "Defining the Catalog Metadata"](#)
- You have carried out the necessary UI customization steps required when a user-defined field is added to the Catalog.

17.3.2.2.1 Bootstrapping the Catalog with Roles There are two ways to bootstrap the Catalog with Roles.

- Bootstrapping the Catalog with Roles when you are not using Oracle Identity Analytics customer

In Oracle Identity Manager 11g R2, roles are published immediately to the Catalog when they are created and assigned a role category other than the OIM Roles category. If you have made changes to the role categories or need to synchronize the enterprise roles with the Catalog, follow the steps given below

To bootstrap the catalog with roles:

1. Login to the **Oracle Identity System Administration** Console as a member of the System Administrator role.
2. Click **Scheduler**.
3. Search for the **Catalog Synchronization** job.
4. Check the **Process Roles** parameter.
5. Set the parameter Mode to **Full**.

Note: If you are running the job for the first time and the **Mode** is set to **Full**, then you must not provide any value in the Update Date parameter.

6. Click **Run Now** to run the job immediately or provide a date and time to run the job later.
- Bootstrapping the Catalog with Roles when you are using Oracle Identity Analytics for managing the lifecycle of enterprise roles

17.3.2.2.2 Bootstrapping the Catalog with Application Instances Bootstrapping the Catalog with Application Instances requires additional steps to be carried out. Use the checklist given in [Section 17.3.2.1.3, "Onboarding Application Instances"](#) to ensure that you have completed the pre-requisites.

Once you have completed the pre-requisites, follow the steps given below to onboard application instances:

1. Login to the **Oracle Identity System Administration** Console as a member of the System Administrator role.
2. Click **Scheduler**.
3. Search for the **Catalog Synchronization** job.
4. Check the **Process Application Instances** parameter.
5. Set the parameter Mode to **Full**.

Note: If you are running the job for the first time and the **Mode** is set to **Full**, then you must not provide any value in the Update Date parameter.

6. Click **Run Now** to run the job immediately or provide a date and time to run the job later.

17.3.2.2.3 Bootstrapping the Catalog with Entitlements Bootstrapping the Catalog with Entitlements requires additional steps to be carried out. Use the checklist given in [Section 17.3.2.1.4, "Onboarding Entitlements"](#) to ensure that you have completed the pre-requisites.

Once you have completed the pre-requisites, follow the steps given below to onboard entitlements.

1. Login to the **Oracle Identity System Administration** Console as a member of the System Administrator role.
2. Click **Scheduler**.
3. Search for the **Catalog Synchronization** job.
4. Check the **Process Entitlements** parameter.
5. Set the parameter Mode to **Full**.

Note: If you are running the job for the first time and the **Mode** is set to **Full**, then you must not provide any value in the Update Date parameter.

6. Click **Run Now** to run the job immediately or provide a date and time to run the job later.

17.3.2.3 Ongoing Synchronization

To automate the process of onboarding roles, application instances, and entitlements, you can configure the Catalog Synchronization job in the following manner.

1. Login to the **Oracle Identity System Administration** Console as a member of the System Administrator role.
2. Click **Scheduler**.
3. Search for the **Catalog Synchronization** job.
4. Check the **Process Roles, Process Application Instances, and Process Entitlements** parameters.
5. Set the parameter **Mode** to Incremental.
6. Provide a date and time to run the job later.
7. Set the Job frequency to run every five minutes.

17.3.2.4 Enrich the Catalog

Enriching the Catalog refers to the process of populating the Access Request Catalog with data so that the information is available for end-users to see. The additional data helps end-users understand the business context associated with the Catalog Item. The additional data is also available as part of the approval workflow, allowing the workflow to make intelligent routing decisions based on the data about the Catalog Item.

There are two ways to enrich the Catalog:

- [Section 17.3.2.4.1, "Editing a Catalog Item Online"](#)
- [Section 17.3.2.4.2, "Enriching the Catalog in bulk from external sources"](#)

Pre-requisites

- You have extended the Catalog using the Form Designer by following the steps given in [Section 17.3.1.2, "Defining the Catalog Metadata"](#).
- You have added UI customizations required when a user-defined field is added to the Catalog. See [Chapter 8, "Configuring Custom Attributes"](#) for information about adding user-defined fields and customizing the UI to display the user-defined field in the UI.
- You have created a Catalog System Administrator role and assigned users as given in [Section 17.3.1.1, "Setting up the Catalog System Administrator"](#)

17.3.2.4.1 Editing a Catalog Item Online To edit a Catalog Item online, using the Oracle Identity Manager Self Service Console:

Note: Name, Display Name, and Description cannot be edited on the catalog screen. These are base level attributes and you cannot edit from Catalog UI.

1. Log in to the Oracle Identity Manager Self Service Console as a member of the Catalog System Administrator role.
2. Click **Catalog** to access the Catalog.
3. Enter one or more keywords and click **Search**.
4. Use the Refine Search to find the Catalog Item(s) to be edited.
5. Select the Catalog Item to be edited.
6. In the Detailed Information section, edit the Catalog Item and click **Apply**. Verify the confirmation message.

17.3.2.4.2 Enriching the Catalog in bulk from external sources While Catalog System Administrators can make use of the robust Catalog Item editing capabilities in the Oracle Identity Manager Self Service Console, there are scenarios where the data needs to be loaded in bulk from external sources.

Examples of bulk updates:

- MyCorp wants to provide users with asset information from their IT CMDB system or from their Corporate Asset Management system. The information cannot be entered manually since the CMDB or AMS system gets updated on a regular basis. In such a scenario, MyCorp needs a way to update the Catalog in bulk.
- MyCorp was using a home grown access request application prior to implementing Oracle Identity Manager 11g R2. This application contains the glossary and other relevant information about the roles, application instances and entitlements. As part of migrating to Oracle Identity Manager 11g R2, MyCorp Catalog System Administrators would like to move the Catalog Item information from the legacy system.

17.3.2.4.3 Loading data from an external source

Follow the steps given below to load data from an external source into the Catalog:

1. Export the data to be loaded into a comma-separated values format file.
2. Ensure that the first line of the file contains the Catalog attribute names.

3. Move the file to a file system that is accessible from the server on which is Oracle Identity Manager is deployed.
4. Login to the **Oracle Identity System Administration** Console as a member of the System Administrator or System Configurator role.
5. Click **Scheduler**.
6. Search for the **Catalog Synchronization** Job.
7. Provide the full path to the file in the parameter **File Path**.
8. Set the value of the parameter Mode to **Metadata**. [Table 17-1](#) provides sample parameter details.

Table 17-1 Catalog Metadata Loader Sample

Parameter	Value
ENTITY_TYPE	Role
ENTITY_KEY	12
ENTITY_NAME	test
IS_REQUESTABLE	1
USER_DEFINED_TAGS	UDTags
CATEGORY	mycategory
AUDIT_OBJECTIVE	AO111
APPROVER_USER	1
APPROVER_ROLE	1
FULFILLMENT_USER	1
FULFILLMENT_ROLE	1
CERTIFIER_USER	1
CERTIFIER_ROLE	1
ITEM_RISK	1
CERTIFIABLE	1
STUDF	1

9. Click **Run Now** to run the job immediately or select a data and click **Apply** to run the job later.

17.3.2.5 Managing Catalog Items

This section contains the following topics

- [Deleting a Catalog Items of Type Roles](#)
- [Deleting Catalog Items of Type Application Instances](#)
- [Deleting Catalog Items of type Entitlements](#)

17.3.2.5.1 Deleting a Catalog Items of Type Roles

To delete role Catalog Items:

1. Login to the Oracle Identity Self Service.
2. Search for the role to be deleted and delete the role.

3. The associated Catalog Item will be marked as soft-deleted and will not appear in the Catalog.
4. For deleting large number of roles, use the APIs to delete the role. It is not recommended to use database techniques to delete roles.

17.3.2.5.2 Deleting Catalog Items of Type Application Instances Application Instances, in almost all use cases, represent a target system (sometimes known as an endpoint) and an account in a target system. When you delete an Application Instance, you are essentially decommissioning the target system from Oracle Identity Manager. Depending upon the scale of your deployment and the number of accounts provisioned to the target system, deleting an Application Instance can have a significant impact to the end users and their access.

To delete application instance Catalog Items:

1. Login to Oracle Identity System Administration.
2. Click **Application Instances**.
3. Search for application instances.
4. Select one or more application instances. Delete and confirm.
5. Click **Scheduler**.
6. Search for the Catalog Synchronization Job.
7. Set the Mode to Incremental.
8. Click **Run Now** to run the job immediately or set it up to run at a particular time.

17.3.2.5.3 Deleting Catalog Items of type Entitlements To delete entitlement Catalog Items:

1. To delete Entitlements, login to the Oracle Identity System Administration Console.
2. Click **Lookups**.
3. In the Code column, enter the name of the Lookup Definition that contains the entitlement. Refer to the Connector documentation to find out the name of the Lookup Definition.
4. Delete one or more entitlement values.
5. Click **Scheduler**.
6. Search for the **Entitlement List Load** job.
7. Click **Run now**.
8. Search for the Catalog Synchronization Job.
9. Set the Mode to **Incremental**.
10. Click **Run Now** to run the job immediately or set it up to run at a particular time.

17.3.3 Database Best Practices for Access Request Catalog

Access Request Catalog uses "Oracle Text" option in Oracle database for text search capabilities. Oracle Text is a fast and accurate full-text retrieval technology integrated with Oracle Database.

The CATALOG table which contains catalog items is indexed using CONTEXT index type of Oracle Text. Although Oracle Text index operates like a regular database index,

the architecture and processing behind Text index highlights the importance of best practices when creating the Text index and also the on-going maintenance.

Following sections are aimed at providing more information in this regard for Oracle Identity Manager administrators and database administrators.

- [Section 17.3.3.1, "One-Time Optimizations for Oracle Text Index"](#)
- [Section 17.3.3.2, "Text Index Optimization"](#)

17.3.3.1 One-Time Optimizations for Oracle Text Index

When you install Oracle Identity Manager, the Text index for Access Request Catalog is created with possible optimizations. However, Oracle Text has some more optimizations that are better applied based on the characteristics of the deployment. Following are the optimizations that you should consider applying for improving Access Request Catalog search performance. It is important to note that Access Request Catalog is not usable when applying these and these are recommended to be done during a scheduled maintenance window.

Note: Catalog Synchronization job and Access Request Catalog should be down when these one-time optimizations are applied.

Storage of Text Index

Oracle Text index is stored in relational tables (DR\$) which are presently resides in the default tablespace of OIM schema. It is recommended to separate them out to their own tablespace. You can use the following commands to do that. You are recommended to be familiar with these steps and also make changes where needed.

1. Login to SYS schema and create a new tablespace to hold the text index internal tables. You can use the following sample command for it. Replace DATA_DIR with the directory in which you want to store the data file and adjust the size and other parameters as necessary for your environment.

```
CREATE TABLESPACE catalog_text_ind_tables
  DATAFILE 'DATA_DIR/catalog_text_ind_tables_01.dbf' SIZE 2048M REUSE
  EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
```

2. Connect to the database using OIM schema.
3. Create a storage preference using the commands below. Oracle recommends you to be familiar with BASIC_STORAGE clause of Oracle Text and add more storage clauses if required. You can find more info on BASIC_STORAGE in Oracle Text Reference document.

```
Begin
Ctx_Ddl.Create_Preference('cat_storage', 'BASIC_STORAGE');
End;
/

Begin
ctx_ddl.set_attribute('cat_storage', 'I_TABLE_CLAUSE', 'tablespace
catalog_text_ind_tables storage (initial 5M next 5M)');
End;
/

Begin
ctx_ddl.set_attribute('cat_storage', 'K_TABLE_CLAUSE', 'tablespace
catalog_text_ind_tables storage (initial 5M next 5M)');
```

```

End;
/

Begin
ctx_ddl.set_attribute('cat_storage', 'R_TABLE_CLAUSE','tablespace
catalog_text_ind_tables storage (initial 1M) lob (data) store as (cache)');
End;
/

Begin
ctx_ddl.set_attribute('cat_storage', 'N_TABLE_CLAUSE','tablespace
catalog_text_ind_tables storage (initial 1M)');
End;
/

Begin
ctx_ddl.set_attribute('cat_storage', 'I_INDEX_CLAUSE','tablespace
catalog_text_ind_tables storage (initial 1M) compress 2');
End;
/

```

4. Apply the new storage preference using the following command. Make sure the Text index status is valid after this step.

```
ALTER INDEX CAT_TAGS rebuild parameters ('replace storage cat_storage');
```

5. Verify that the above tables are moved to the new tablespace by querying USER_SEGMENTS table.

KEEP Pool Settings for Text Index:

Oracle recommends put all the tables that make up the Text index in database KEEP pool to improve the performance of Access Request Catalog search. You must size the KEEP pool (DB_KEEP_CACHE_SIZE) correctly so that these Text index tables and other OIM objects are retained in KEEP pool. To do so:

1. Connect to the database using OIM schema.
2. Compute the size of the text index using the following query and use that to set/adjust DB_KEEP_CACHE_SIZE accordingly.

```
SELECT ctx_report.index_size('CAT_TAGS') FROM dual;
```

3. Run the following commands as OIM schema user to put the tables in KEEP pool.

```
ALTER INDEX DR$CAT_TAGS$X STORAGE (buffer_pool keep);
ALTER TABLE DR$CAT_TAGS$R STORAGE (buffer_pool keep);
ALTER TABLE DR$CAT_TAGS$R STORAGE (buffer_pool keep) MODIFY lob (data) (STORAGE
(buffer_pool keep));
ALTER TABLE DR$CAT_TAGS$K STORAGE (buffer_pool keep);
ALTER TABLE DR$CAT_TAGS$I STORAGE (buffer_pool keep);
```

17.3.3.2 Text Index Optimization

The Text index could become fragmented due to on-going "Catalog Synchronization" Optimizing the text index on regular basis removes the old data and minimizes the fragmentations, which can improve the search performance of Access Request Catalog. To perform this, Oracle Identity Manager has introduced the following Oracle Database scheduler jobs:

- FAST_OPTIMIZE_CAT_TAGS

- REBUILD_OPTIMIZE_CAT_TAGS

These jobs reside in OIM database schema and they are disabled by default. Oracle strongly recommends you to view these jobs, make schedule changes if needed and enable them. When changing the schedule, make sure the new schedule is set on the same line as the default schedule.

FAST_OPTIMIZE_CAT_TAGS meant to be running on frequent basis. By default, it is scheduled to run once a day at 1 AM. REBUILD_OPTIMIZE_CAT_TAGS does a full optimization and rebuilds the Text index. REBUILD_OPTIMIZE_CAT_TAGS is not meant to be running frequent basis. By default, REBUILD_OPTIMIZE_CAT_TAGS is scheduled to run every Sunday at 2 AM. Note that optimization may take a long time if your Text index is big.

Perform the following steps to change the schedule and/or enable these jobs.

1. Make sure the default schedule (daily 1 AM for FAST and every Sunday 2 AM for REBUILD) is acceptable to your environment. If not, change the schedule. If you are not sure, you can keep the default schedule and change later when needed.
2. Enable the jobs using the following commands:

```
BEGIN
DBMS_SCHEDULER.ENABLE ('FAST_OPTIMIZE_CAT_TAGS');
END;
/

BEGIN
DBMS_SCHEDULER.run_job ('REBUILD_OPTIMIZE_CAT_TAGS');
END;
/
```

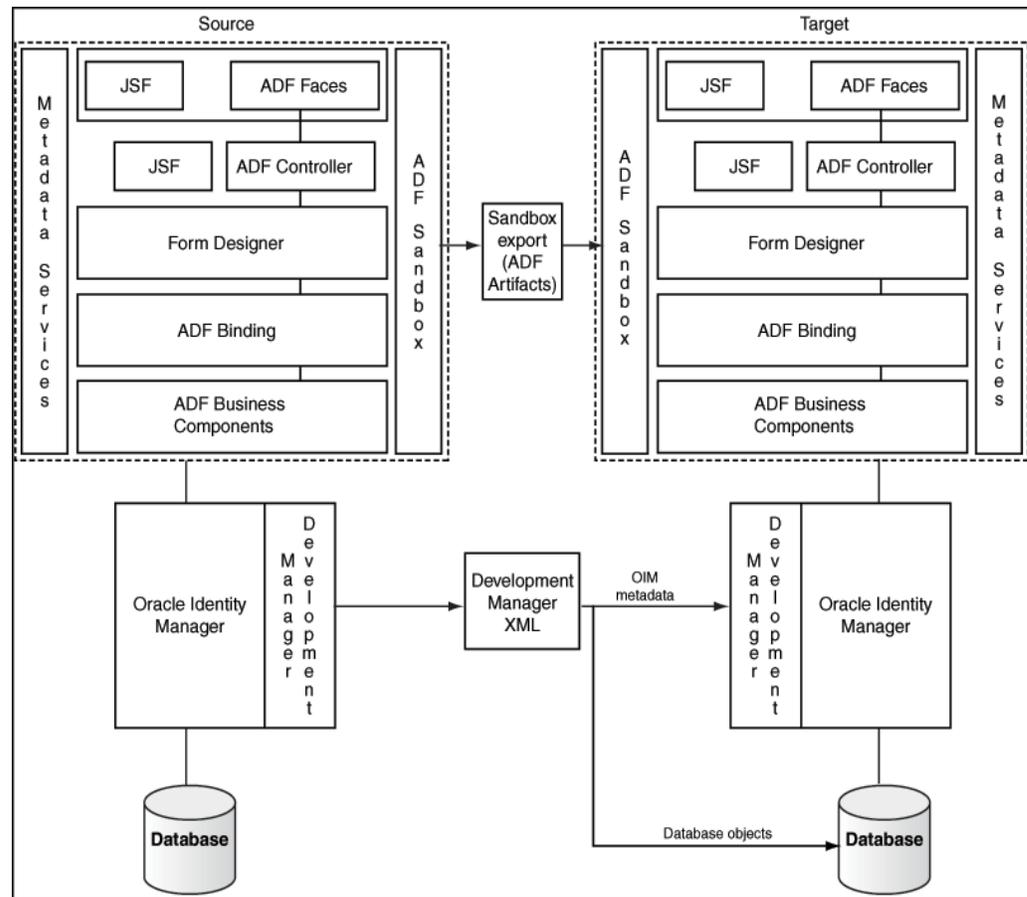
Note: The Text index optimization can be done when the server is up and search of Access Request Catalog takes place.

17.4 Managing the Lifecycle of the Catalog

This section describes how to move Catalog customizations from a test environment to a production environment. You can extend the Catalog, customize the Catalog UI, and develop and test the customizations in a test environment, and then eventually roll out the customizations to your production environment.

This section includes the following topics

- [Section 17.4.1, "Overview of Catalog Customization"](#)
- [Section 17.4.2, "Test to Production procedures for Catalog customizations"](#)
- [Section 17.4.3, "Limitations of the Test to Production procedures"](#)

Figure 17–2 Test to Production Process for Catalog

17.4.1 Overview of Catalog Customization

While the Access Request Catalog in Oracle Identity Manager 11g R2 provides robust and rich out of the box functionality, there may be scenarios where you need to extend the Catalog and customize it to meet your business needs.

The following scenarios illustrate common scenarios where the Catalog may require customization.

- MyCorp would like to add additional attributes such as Cost to Line of Business, License required, to give the requester an idea about the cost that would be incurred by the Line Of Business, when the requested item was granted. To support this scenario, the Catalog System Administrator extends the Catalog and adds two additional attributes, Cost to Line of Business, a numeric attribute, and License required, a Boolean attribute. Next, the administrator customizes the Catalog search results and Catalog item details page.
- MyCorp would like to show the Risk associated with an entitlement as part of Catalog search results. To support this scenario, the Catalog System Administrator customizes the Catalog search results and adds the item risk as an image widget.

These customizations will be implemented by System Integrators or the customer's own IT staff and need to be moved to Test and to Production.

Figure 17–1 shows the high-level process of moving customizations from Test to Production for the Catalog. Catalog customizations have three components:

1. ADF customizations

ADF customizations include Catalog UI customizations including search results, item details, cart details and Catalog attributes added or modified using the Form Designer. These customizations should be done within a Sandbox session. For more information on Sandboxes, please refer to [Section 17.4.2, "Test to Production procedures for Catalog customizations"](#)

2. Oracle Identity Manager metadata customizations

When you add new attributes to the Catalog entity or modify an existing attribute and change its properties, additional metadata is generated in Oracle Identity Manager. For example, if a new attribute, Secondary Approver, is added to the Catalog entity using the Form Designer, Oracle Identity Manager adds a database column corresponding to the attribute. If the attribute is searchable, Oracle Identity Manager stores additional metadata. These customizations should be moved from Test to Production using the Deployment Manager.

3. Data Migration

The Catalog needs to be populated with relevant information, after adding/ modifying attributes in the Catalog to make the Catalog business-friendly and provide enough information so that users can use the Catalog effectively. Once this additional information, also referred to as the Glossary, has been reviewed and approved, it needs to be moved to Production.

17.4.2 Test to Production procedures for Catalog customizations

This section describes the steps to perform for moving the Catalog definition from Test to Production. It consists of the following steps:

- [Section 17.4.2.1, "Exporting using the Sandbox and Deployment Manager"](#)
- [Section 17.4.2.2, "Importing Using the Deployment Manager and Sandbox"](#)

Depending upon the type of customization done, you may need either one or both the steps. Use [Table 17-2](#) to make a determination of which steps to carry out.

Table 17-2 Catalog Customization Steps

Customization	Sandbox required	Deployment Manager required
Adding/ Modifying a seeded Catalog attribute	Yes	Yes
Adding/ Modifying a Catalog UDF	Yes	Yes
Customizing Catalog UI	Yes	No
Populating Catalog	No	No

See Also:

- "Migrating Configurations and Customizations" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Deployment Manager
- "Managing Sandboxes" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about sandboxes
- "Handling Concurrency Conflicts" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about handling concurrency conflicts when multiple users customize an application by using sandboxes and troubleshooting concurrency issues

17.4.2.1 Exporting using the Sandbox and Deployment Manager**To Export Using Sandbox**

To move the ADF customizations from Test to Production, follow the steps given below

1. Login to the Oracle Identity System Administration Console as a member of the System Administrator role.

Note: In scenarios where you need to switch between the Self Service (or Identity) and System Administration consoles and the Oracle Identity Manager 11g R2 deployment is not protected by Single Sign On, you must log out of one console before logging in into another.

2. Click **Sandbox** and select the Sandbox to be exported.
3. Click **Export Sandbox**. A sandbox can be exported as a file for transporting, sharing, and other usages where packaging it as a file is required.
4. Specify a file location for the zip file created.

To Export Using Deployment Manager

Note: Make sure that you do not have any popup blockers enabled in your browser and that you have a supported Java Runtime Environment (JRE) installed in the browser. This is because the Deployment Manager uses a popup window and it requires JRE to be installed in the browser.

To export the Oracle Identity Manager metadata from Test to Production, follow the steps given below

1. Login to the Oracle Identity System Administration Console as a member of the System Administrator or System Configurator role.
2. Click **Export**.
3. Select **Catalog Metadata** as the object to be exported.
4. Enter * in the search field and click **Search**.

5. Follow the steps to generate the Deployment Manager XML.

Note: Perform the following optional steps as a best practice:

- Backup/Check-in the sandbox zip file and the Deployment Manager XML as a single file into a source code control system like Subversion, SourceSafe, and so on.
 - Repeat the steps above in the target (Production) environment and backup the Catalog entity and the Catalog UI.
-
-

17.4.2.2 Importing Using the Deployment Manager and Sandbox

Importing the customizations should be done in the reverse order. This is required since the ADF customizations expect the Oracle Identity Manager metadata to be present, when the ADF customizations are imported.

To Import Using Deployment Manager

To import the Oracle Identity Manager metadata from Test to Production:

1. Login to the Oracle Identity System Administration Console as a member of the System Administrator or System Configurator role.
2. Click **Import**.
3. In the File browser popup, select the **Deployment Manager XML** file to be imported.
4. Follow the wizard steps to import the XML.

To import using the Sandbox

To move the ADF customizations from Test to Production:

1. Login to the Identity or Oracle Identity System Administration Console as a member of the System Administrator role.

Note: In scenarios where you need to switch between the Self Service (or Identity) and System Administration consoles and the Oracle Identity Manager 11g R2 deployment is not protected by Single Sign on, you must log out of one console before logging in into another.

2. Click **Sandbox** and then click **Import Sandbox**.
3. In the dialog, select the file to be imported.
4. Click **Import**.
5. In the Sandbox Manager, select the sandbox and click **Publish Sandbox**.
6. Logout and log back in to view and verify the changes.

17.4.3 Limitations of the Test to Production procedures

There are some limitations in the Test to Production process for the Catalog, including the following:

- All ADF customizations must be done within a single sandbox session. While you can have multiple sandboxes, only one sandbox can be active at a time and as a result, changes in the System Administration Console i.e. Catalog entity extension

and those done in the Identity Console, that is, Catalog UI customization, must be done in the same sandbox.

- Changes done outside a sandbox or done either before creating and activating a sandbox or after, are not visible in the sandbox.
- Once you publish a sandbox, you cannot export it or revert it. As a result, you must export the sandbox while it is still activated and not published and also ensure that you back your customizations before you import and publish a sandbox.
- Deployment Manager imports are committed immediately. There is no rollback capability in the Deployment Manager.

17.5 Troubleshooting

This section describes the troubleshooting procedures to be followed while resolving issues with the Access Request Catalog. It contains the following topics

- [Section 17.5.1, "Catalog synchronization issues"](#)
- [Section 17.5.2, "Catalog security issues"](#)
- [Section 17.5.3, "Catalog Search Issues"](#)

17.5.1 Catalog synchronization issues

Catalog synchronization issues occur when roles, application instances and entitlements are not visible in the Access Request Catalog. Use the flow charts given below to troubleshoot synchronization issues for each of three Catalog item types that can be requested.

Note: Harvesting job picks up the data for harvesting on the basis of the Update date parameter. If the update is blank, then all the records are fetched for processing.

However, if the user has specified some date in the Update date parameter, only that data is processed which is created or updated after the given date.

- Troubleshooting synchronizing Roles with the Catalog

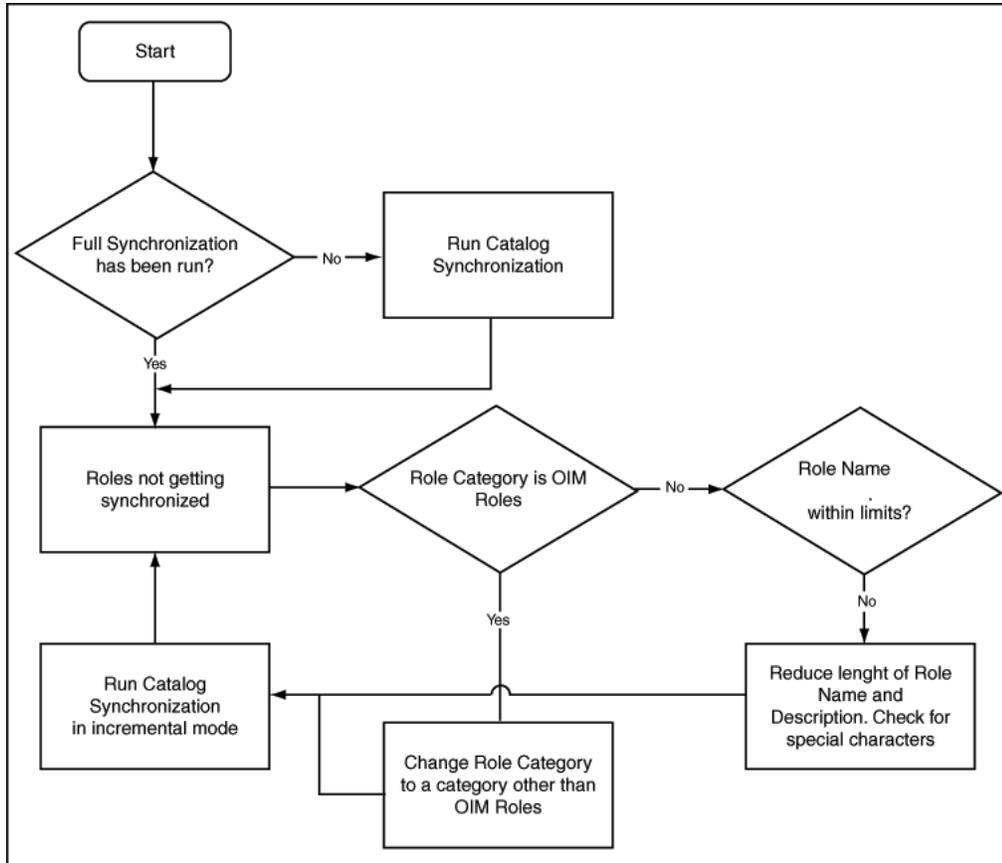
The synchronization of Roles with the Catalog is real-time in nature. When a role is created, it is published to the Catalog immediately as long as it does not belong to the OIM Roles category.

Note: The OIM Roles role category is meant for OIM usage only. Customers should not use this category for their enterprise Roles.

In a new Oracle Identity Manager 11g R2 installation, enterprise roles created by customers will be available in the Catalog and the visibility will be based on the organization scoping. In an upgraded environment, customers will have to run the Catalog Synchronization job in a bootstrap mode to publish the existing roles to the Catalog. New roles, created after upgrade, will be available in the Catalog immediately.

Figure 17-3 shows a diagnostic flowchart that customers can use to troubleshoot scenarios where the roles created in Oracle Identity Manager are not visible in the Catalog.

Figure 17-3 Catalog Synchronization Diagnostic Flowchart



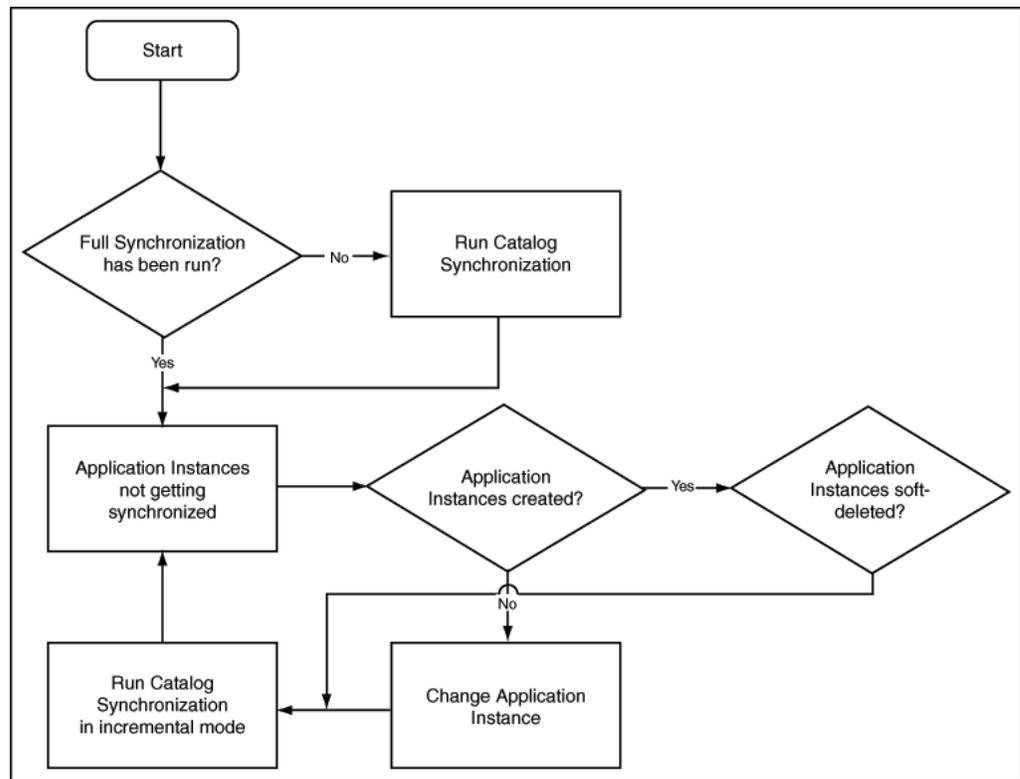
This diagram illustrates the diagnostic flow chart details.

- Troubleshooting synchronizing Application Instances with the Catalog

The synchronization of Application Instances with the Catalog is controlled by the Catalog Synchronization job. Application Instances require more configuration (than enterprise roles) and hence are not synchronized immediately with the Catalog.

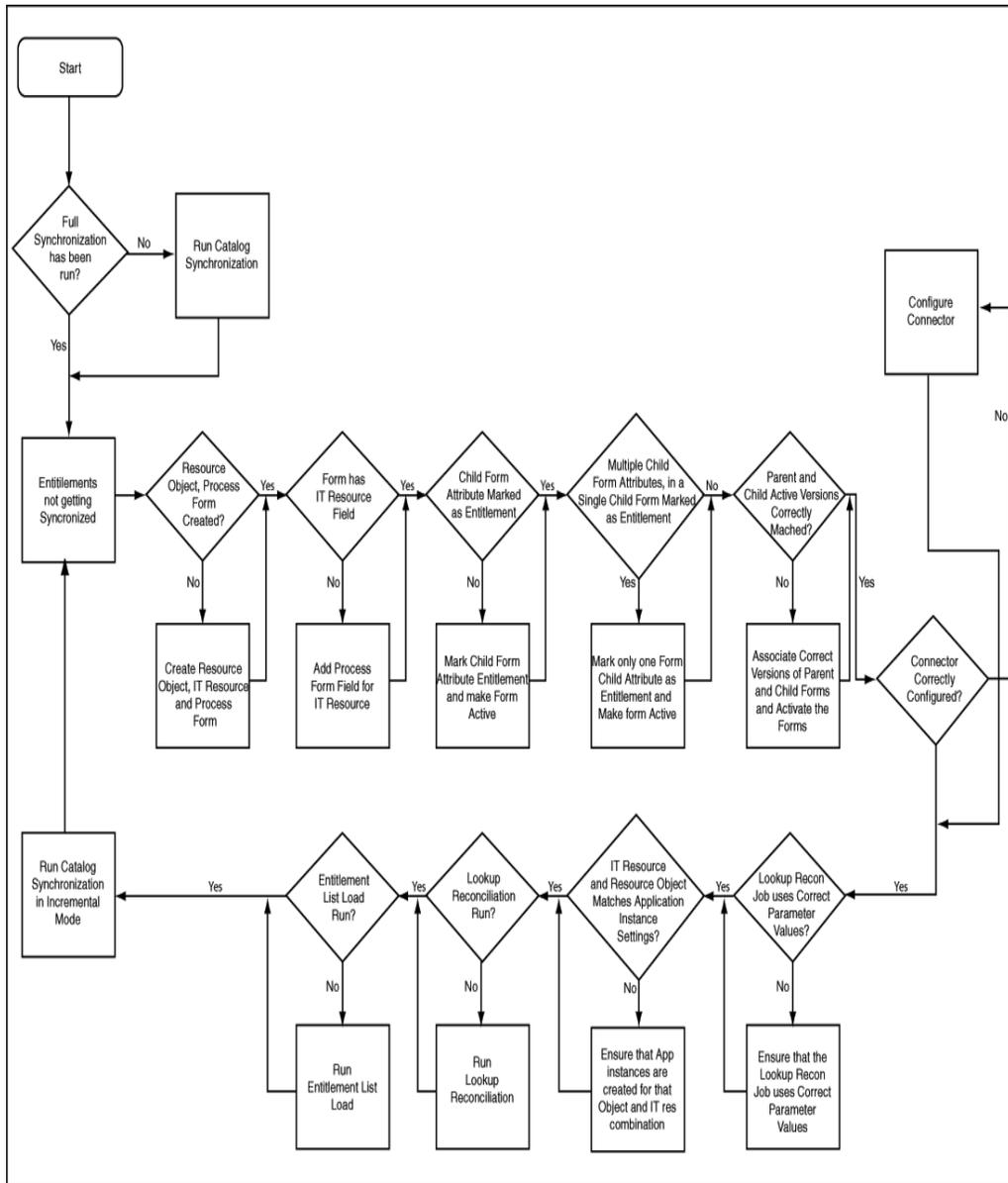
Figure 17-4 shows a diagnostic flowchart to be followed when troubleshooting issues related to synchronizing application instances with the Catalog.

Figure 17-4 *Trouble Shooting Synchronization Application Instances Flowchart*



- Troubleshooting synchronizing Entitlements with the Catalog

Figure 17-5 Troubleshooting Synchronizing Entitlements Flowchart



17.5.2 Catalog security issues

Catalog security is driven by two factors:

- The security model that uses Organization-based scoping for users, roles, application instances and entitlements. This security model controls what items a requester can see in the Catalog search results and the users who can be added as target users.
- The security model that is not scoped by organization and is used for global Admin Roles such as Catalog System Administrator.

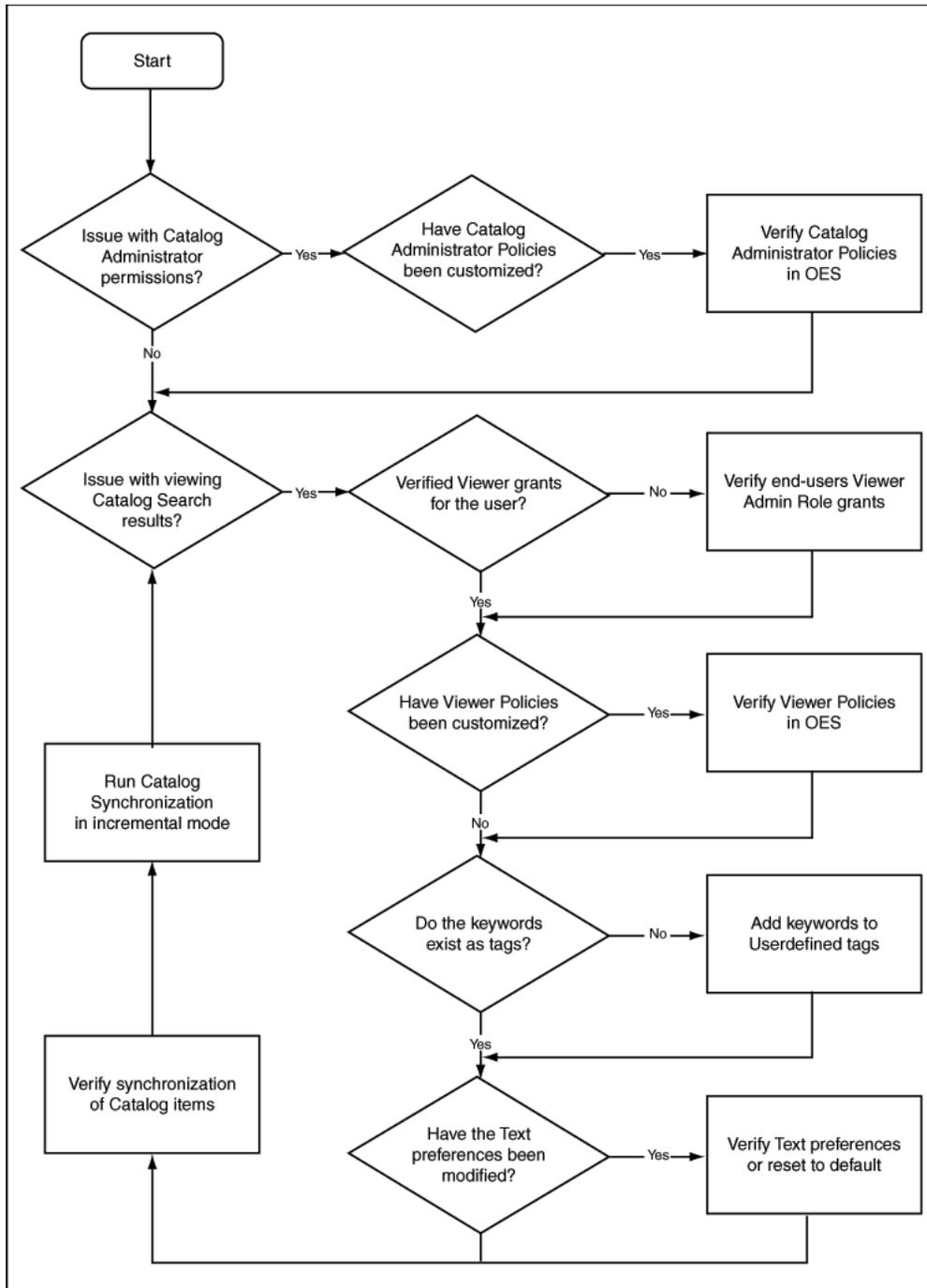
Typical issues with Catalog security are:

- Requesters cannot see the Catalog item even though they have entered the correct search keyword.

- Requesters are not able to add target users to the request
- Requesters are not able to provide additional information for application instance requests
- Requesters cannot see Catalog Item details such as Approver User, Approver Role, Fulfillment User, and Fulfillment Role.
- Catalog System Administrators do not see the Catalog Item in an edit mode and are not able to edit the Catalog Item
- Catalog System Administrators are not able to create Request Profiles

[Figure 17-6](#) shows a diagnostic flow chart to be followed to troubleshoot issues with Catalog security.

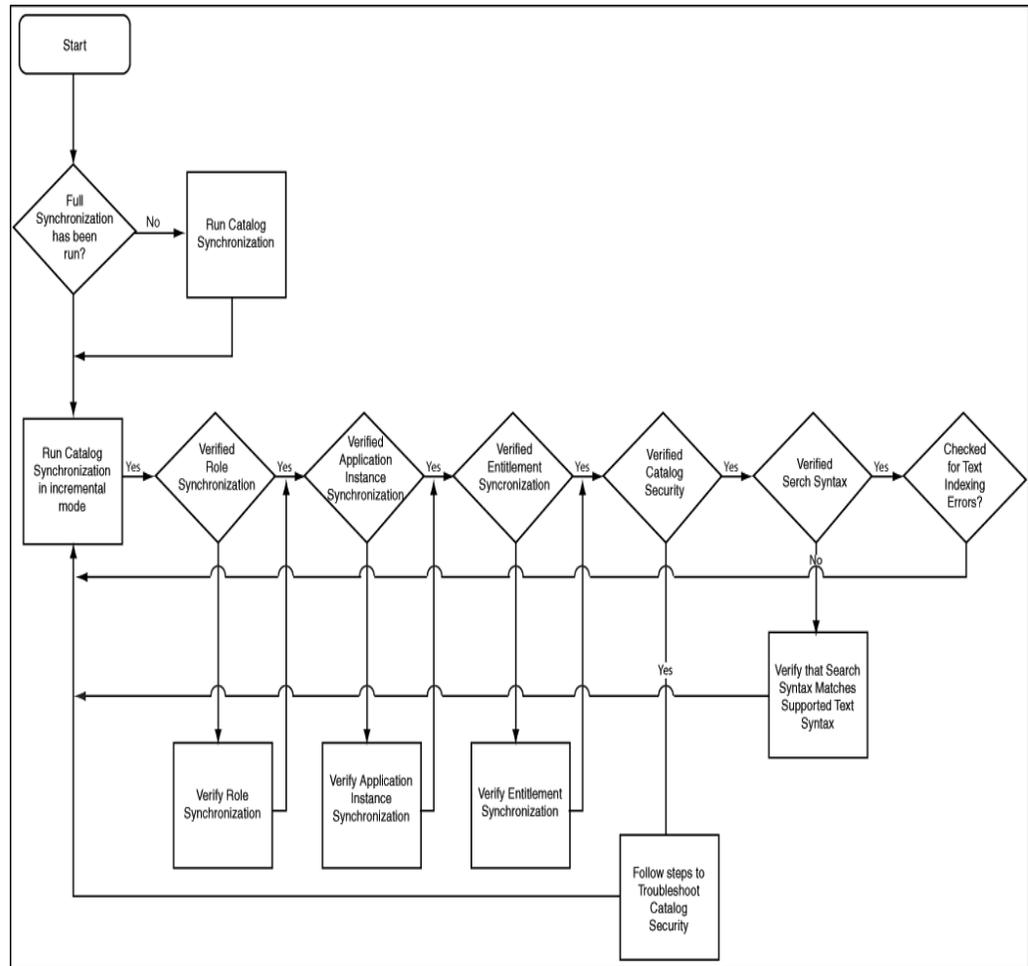
Figure 17-6 Diagnostic Flowchart With Security Issues



17.5.3 Catalog Search Issues

Figure 17-7 shows a diagnostic flow chart to be followed to troubleshoot issues with Catalog search.

Figure 17-7 Catalog Search



Part VIII

Auditing and Reporting

This part describes auditing and reporting features of Oracle Identity Manager.

It contains the following chapters:

- [Chapter 18, "Configuring Auditing"](#)
- [Chapter 19, "Using Reporting Features"](#)
- [Chapter 20, "Using the Archival Utilities"](#)

Configuring Auditing

Oracle Identity Manager provides a powerful audit engine to collect extensive data for audit and compliance purposes. You can use the audit functionality together to capture, archive, and view entity and transactional data for compliance monitoring and IT-centric processes and forensic auditing. Therefore, with the audit and compliance modules, Oracle Identity Manager provides profile auditing, reporting, and attestation features. You can capture, transport, store, retrieve, and remove historical data over its life cycle. Security is maintained at every stage of the data life cycle. For information about attestation processes, see "[Managing Attestation Processes](#)" on page 5-1.

This chapter consists of the following topics:

- [Overview](#)
- [User Profile Auditing](#)
- [Role Profile Auditing](#)
- [Enabling and Disabling Auditing](#)

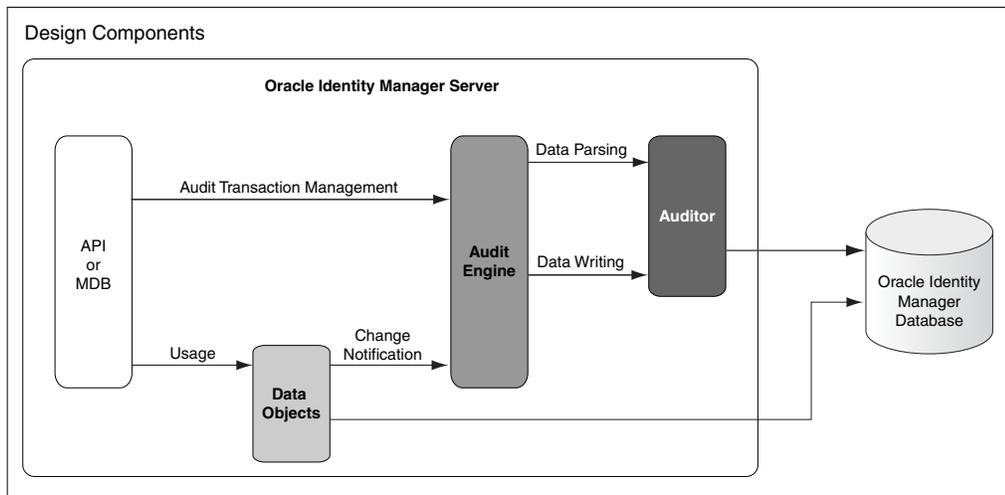
18.1 Overview

This section provides an overview of auditing in the following sections:

- [Auditing Design Components](#)
- [Profile Auditing](#)
- [Standard and Customized Reports](#)

18.1.1 Auditing Design Components

[Figure 18-1](#) shows the design components for Oracle Identity Manager auditing process.

Figure 18–1 Design Components of the Auditing Process

Any action that a user performs in Oracle Identity Manager translates into an Application Programming Interface (API) call or into a Message Driven Bean (MDB) picking up a message to process an action.

One action can cause multiple changes. All changes are combined into an audit transaction. Each API method that can modify data objects calls the `startTransaction` method in the audit engine at the beginning of the API call and the `endTransaction` method at the end of the API call. This defines boundaries for the audit transaction. The audit engine generates a transaction ID to identify the changes made in the transaction.

18.1.2 Profile Auditing

Oracle Identity Manager provides auditing and historical archiving of profile information. It takes a snapshot of a profile, stores the snapshot in an audit table in the database, and updates the snapshot each time the profile data changes. In the context of profile auditing, the term snapshot means a copy taken of the entire profile data at any instant when the data is modified.

18.1.3 Standard and Customized Reports

The BI Publisher provides standard reports for viewing archived data. You can also create customized reports.

For information about reporting, refer to the following:

- ["Using Reporting Features"](#) on page 19-1
- ["Configuring Reports"](#) in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about reporting

18.2 User Profile Auditing

User profile audits cover changes to user profile attributes, user membership, resource provisioning, access policies, and resource forms.

This section discusses the following topics:

- [Data Collected for Audits](#)

- [Post-Processor Used for User Profile Auditing](#)
- [Tables Used for User Profile Auditing](#)
- [Archival](#)

18.2.1 Data Collected for Audits

By default, user profile auditing is enabled and the auditing level is set to Resource Form when you install Oracle Identity Manager. This auditing level specifies the minimum level required for attestation of form data.

You configure the audit level in the System Configuration part of the Advanced Administration by using the `XL.UserProfileAuditDataCollection` system property.

See Also:

- "Audit Levels" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information about audit levels
- "[System Properties in Oracle Identity Manager](#)" on page 16-1 for information about the `XL.UserProfileAuditDataCollection` system property

This section discusses the following topics:

- [Capture of User Profile Audit Data](#)
- [Storage of Snapshots](#)
- [Trigger for Taking Snapshots](#)

18.2.1.1 Capture of User Profile Audit Data

Each time a user profile changes, Oracle Identity Manager takes a snapshot of the user profile and stores the snapshot in an audit table in the database.

A snapshot is also generated when there is a change in a user profile that must be audited, even if an initial snapshot is missing. The current snapshot is treated as the initial snapshot.

The following are the components of a user profile and the tables that store these components:

- **User Record:** Contains the USR table, including all User Defined Fields (UDFs).
The USR table stores user attributes. When you create a user, Oracle Identity Manager adds an entry to this table.
- **User Role Membership:** Contains the RUL, UGP, and USG tables, as listed in [Table 18-1](#).

Table 18-1 *User Group Membership Tables*

Table Name	Description
RUL	Stores rule definitions.
UGP	Defines roles (or groups) in the system.

Table 18–1 (Cont.) User Group Membership Tables

Table Name	Description
USG	Defines which users are in which groups and lists priorities for the users in a specific group. Oracle Identity Manager might use these priorities when making task assignments for a group. For example, a process task might be assigned to the user having highest priority. In addition, if a role/group is granted through a rule, then it lists the specific rule.

- **User Policy Profile:** Contains the following tables:
 - **UPD:** Stores User Policy Profile data. This is a policy-centric view of the resources that are provisioned to a user.
 - **UPP:** Stores User Policy Profile-related details. This is a user-centric view of all the applicable policies for a user, and the resources they allow/deny.

Note: When you change a role name by using Oracle Identity Self Service, the User Profile Audit (UPA) tables in the database are not updated with the change until the next snapshot of the user.

- **User Resource Profile:** This component can be divided into the following subcomponents:
 - **User Resource Instance:** Contains the OBI, OBJ, and OIU tables, as listed in [Table 18–2](#).

Table 18–2 User Resource Instance Tables

Table Name	Description
OBI	Stores resource (object) instance information. Oracle Identity Manager creates a resource instance every time a resource is provisioned. This instance stores all generic information related to that provisioned instance, including a request key (if the resource has been provisioned through a request), the corresponding process instance, and the instance status.
OBJ	Represents the resource object data, including details about the resource, such as resource name, whether or not auto-save and auto-prepopulate are set, and whether or not the resource object allows multiple instances.
OIU	Associates applicable user information to the resource object instance when provisioning takes place. In addition, it stores policy-related information for the specific resource instance.

- **Resource Lifecycle (Provisioning) Process:** Contains the MIL, ORC, OSI, PKG, SCH, and TOS tables, as listed in [Table 18–3](#).

Table 18–3 Resource Lifecycle Process Tables

Table Name	Description
MIL	Defines the process task definitions. Each entry corresponds to a process task. A process definition (PKG table) comprises of multiple tasks, which are a part of the various workflows in the definition.

Table 18–3 (Cont.) Resource Lifecycle Process Tables

Table Name	Description
ORC	Stores process instance information when provisioning takes place. When provisioning starts, Oracle Identity Manager generates an associated process (or workflow) instance that stores process-related information specific to the provisioning instance.
OSI	Stores information about tasks created for process instance.
PKG	Defines processes or workflows in Oracle Identity Manager, including process details such as process name, process type, descriptive field mapping, and associated resources and process forms.
SCH	Stores information related to running of a specific task instance such as the task status, status bucket, and timing of when the adapter run started or ended.
TOS	Stores atomic process information.

- **Resource State (Process) Form:** This information is stored in the UD parent and child tables. The UD_* tables are user-defined field tables that store the account state.

18.2.1.2 Storage of Snapshots

When Oracle Identity Manager takes a snapshot of a user profile, it stores the snapshot in the UPA table. The structure of the UPA table is described in [Table 18–4](#).

Table 18–4 Definition of the UPA Table

Column	Data Type	Description
UPA_KEY	NUMBER (19,0)	Key for the audit record
USR_KEY	NUMBER (19,0)	Key for the user whose snapshot is recorded in this entry
EFF_FROM_DATE	TIMESTAMP (6)	Date and time at which the snapshot entry became effective
EFF_TO_DATE	TIMESTAMP (6)	Date and time at which the snapshot entry was no longer effective In other words, this is the date and time at which the next snapshot entry was created. For the entry representing the latest user profile, the To Date column value is set to NULL.
SRC	VARCHAR2 (4000)	User ID of the user responsible for the change, and the API used to carry out the change
SNAPSHOT	CLOB	XML representation of the snapshot
DELTAS	CLOB	XML representation of old and new values corresponding to a change made to the snapshot
SIGNATURE	CLOB	Can be used to store a digital signature for the snapshot (for nonrepudiation purposes)

Note: The initial audit snapshots for default users in Oracle Identity Manager is not UTF-8 encoded. However, auditing of subsequent modifications to these users have UTF-8 encoded snapshots.

18.2.1.3 Trigger for Taking Snapshots

When any data element in a user profile changes, Oracle Identity Manager creates a snapshot.

The following events trigger the creation of a user profile snapshot:

- Modification of any kind to the user record (for example, through reconciliation and direct provisioning)
- Role membership change for the user
- Changes in the policies that apply to the user
- Provisioning a resource to the user
- Deprovisioning of a resource for the user
- Any provisioning-related event for a provisioned resource:
 - Resource status change
 - Addition of provisioning tasks to the provisioning process
 - Updates to provisioning tasks in the provisioning process, for example, status changes, escalations, and so on
 - Creation of or updates to Process Form data

18.2.2 Post-Processor Used for User Profile Auditing

The user profile auditor has an internal post-processor that normalizes the snapshot XML into the reporting tables: UPA_USR, UPA_FIELDS, UPA_GRP_MEMBERSHIP, UPA_RESOURCE, UPA_UD_FORMS, and UPA_UD_FORMFIELDS. These tables are used by the reporting module to generate the appropriate reports.

18.2.3 Tables Used for User Profile Auditing

Table 18–5 lists the tables in the database that User profile audits use:

Note: For more information about the User Profile Audits tables, such as column names and how to use them, refer to the schema documentation provided with Oracle Identity Manager.

Table 18–5 User Profile Audit Tables

Table Name	Description
AUD	Stores detailed information about all of the Auditors (for example, the User Profile Auditor) supported by Oracle Identity Manager. Currently, only the UserProfileAudit entry is available.
AUD_JMS	Staging table that stores information about changes made as a part of any business transaction. This is an intermediate table to temporarily store data changelog data before the audit engine consumes it. When Audit messages are successfully processed, corresponding records are deleted from the table. Note: This table is not intended for end users and must not be used directly.
UPA	Main auditing table for storing all snapshots and changes made to the user profiles.

Table 18–5 (Cont.) User Profile Audit Tables

Table Name	Description
UPA_FIELDS	Stores user profile audit history changes in denormalized (vertical) format.
UPA_GRP_MEMBERSHIP	Stores groups membership history in denormalized format.
UPA_RESOURCE	Stores user profile resource history in denormalized format.
UPA_USR	Stores user profile history in denormalized format.
UPA_UD_FORMS	Together with the UPA_UD_FORMFIELDS table, contains information about changes to the user's account profile (process form). This table keeps track of the changes to the various forms, such as parent or child forms, which are being changed in any transaction. The changes to the account or entitlement attributes are stored in the UPA_UD_FORMFIELDS table.
UPA_UD_FORMFIELDS	Stores the names of account or entitlement profile fields that are modified. This table also keeps track of the old and new values of the modified fields.

Note:

- The UPA_UD_FORMS and UPA_UD_FORMFIELDS tables together store the audit trail of changes to the user's account profile in a de-normalized format. These tables can be used in various audit-related reports.
- The UPA_UD_FORMS and UPA_UD_FORMFIELDS tables will be populated only if the XL.EnableExceptionReports system property is set to TRUE. For more information about this property, see "System Properties in Oracle Identity Manager" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

18.2.4 Archival

User Profile audit data growth is based on the setting of the audit levels, and the growth can be significant in most of the deployments.

There is also a requirement to clean or archive the old user profile audit data to accommodate future growth.

You can use Audit Archival and Purge Utility to meet these requirements. See ["Using the Audit Archival and Purge Utility"](#) on page 20-14 for detailed information about this utility.

18.3 Role Profile Auditing

Role profile audits cover changes to role profile attributes, role administrators, and direct subroles.

This section discusses the following topic:

- [Data Collected for Audits](#)

18.3.1 Data Collected for Audits

Role profile auditing is determined by the value of the Level of Role Auditing system property with keyword XL.RoleAuditLevel. This property controls the amount of

audit data collected when an operation is performed on a role, such as creation or modification. The supported levels are:

- **None:** No audit data is collected. This is the default value.
- **Role:** Creation, modification, and deletion of role is audited.
- **Role Hierarchy:** Changes made to the role inheritance is audited.

This section discusses the following topics:

- [Capture and Archiving of Role Profile Audit Data](#)
- [Storage of Snapshots](#)
- [Trigger for Taking Snapshots](#)

18.3.1.1 Capture and Archiving of Role Profile Audit Data

Each time a role profile changes, Oracle Identity Manager takes a snapshot of the role profile and stores the snapshot in an audit table in the database.

Oracle Identity Manager generates a snapshot when an audit is created for a role, even if an initial snapshot is missing. The current snapshot is treated as the initial snapshot.

The following are the components of a role profile and the tables that constitute these components:

- User role record: UGP table, including all UDFs for roles
- Subrole information: GPG table

18.3.1.2 Storage of Snapshots

When Oracle Identity Manager takes a snapshot of a role profile, it stores the snapshot in a GPA table. The structure of this table is as described in [Table 18–6](#).

Table 18–6 Definition of the GPA Table

Column	Data Type	Description
GPA_KEY	NUMBER (19,0)	Key for the audit record
UGP_KEY	NUMBER (19,0)	Key for the role whose role snapshot is recorded
EFF_FROM_DATE	TIMESTAMP (6)	Date and time at which the snapshot entry became effective
EFF_TO_DATE	TIMESTAMP (6)	Date and time at which the snapshot entry was no longer effective In other words, this is the date and time at which the next snapshot entry was created. For the entry representing the latest user profile, the To Date column value is set to NULL
SRC	VARCHAR2 (4000)	Source of the entry, User ID of the user responsible for the change, and the API used to carry out the change
SNAPSHOT	CLOB	XML representation of the snapshot
DELTAS	CLOB	XML representation of old and new values corresponding to a change made to the snapshot
SIGNATURE	CLOB	Can be used to store a digital signature for the snapshot (for nonrepudiation purposes)

18.3.1.3 Trigger for Taking Snapshots

When any data element in the role profile snapshot changes, Oracle Identity Manager creates a snapshot.

The creation of role profile snapshots is triggered by events that result in changes in any of the following:

- Role profile data
- Subrole information
- Adding or revoking users or user memberships

18.4 Enabling and Disabling Auditing

This section describes how to enable and disable auditing in Oracle Identity Manager in the following sections:

- [Disabling Auditing](#)
- [Enabling Auditing](#)

18.4.1 Disabling Auditing

To disable auditing in Oracle Identity Manager:

1. Set the values of User profile audit data collection level (XL.UserProfileAuditDataCollection) and Level of Role Auditing (XL.RoleAuditLevel) system properties to None, as described in "[Modifying System Properties](#)" on page 16-29.
2. Disable the Issue Audit Messages Task scheduled job as described in "[Disabling and Enabling Jobs](#)" on page 15-26.

If pending audit changes are required to be recorded in the audit tables, then disable the scheduled task after all the pending audit changes are processed.

18.4.2 Enabling Auditing

To enable auditing in Oracle Identity Manager:

1. Set the values of User profile audit data collection level (XL.UserProfileAuditDataCollection) and Level of Role Auditing (XL.RoleAuditLevel) system properties to one of the levels defined in "Audit Levels" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
See "[Managing System Properties](#)" on page 16-1 for information about modifying the values of system properties.
2. Enable the Issue Audit Messages Task scheduled job as described in "[Disabling and Enabling Jobs](#)" on page 15-26.
3. Generate snapshots by running the GenerateSnapshot script as described in "Generating an Audit Snapshot" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

The following is the command-line usage of the GenerateSnapshot script:

```
./GenerateSnapshot.sh -username OIM_ADMIN_USERNAME -numOfThreads 8 -serverURL
t3://WLS_SERVER:PORT -ctxFactory weblogic.jndi.WLInitialContextFactory
[-inputFile fileWithUserKeys]
```

Here:

- `OIM_ADMIN_USERNAME` is the Oracle Identity Manager administrator username.

- *WLS_SERVER* is the Oracle WebLogic Server name.
- *PORT* is the port number of the WebLogic Server.

Using Reporting Features

This chapter includes the following sections:

- [Reporting Features](#)
- [Starting Oracle Identity Manager Reports](#)
- [Running Oracle Identity Manager Reports](#)
- [Supported Output Formats](#)
- [Reports for Oracle Identity Manager](#)
- [Exception Reports](#)
- [Creating Reports Using Third-Party Software](#)
- [Required Scheduled Tasks for BI Publisher Reports](#)

Note:

- Oracle Identity Manager Reports enables you to use Oracle BI Publisher as the reporting solution for Oracle Identity Management products.
 - Oracle Identity Manager Reports are classified based on the functional areas. For instance, Access Policy Reports, Attestation, Request and Approval Reports, Password Policy Reports and so on. It is no longer named Operational and Historical.
 - Oracle Identity Manager Reports provides a restricted-use license for Oracle BI Publisher and easy-to-use reporting packages for multiple Oracle Identity Management products.
 - For large-scale deployments, especially those taking advantage of the extensive auditing capabilities of Oracle Identity Manager, it is highly recommended that you deploy a dedicated enterprise-class reporting solution. A solution based on tools such as Oracle Business Intelligence Enterprise Edition can provide the flexibility, automation, and performance required for a large-scale organizations.
-
-

19.1 Reporting Features

The following are Oracle Identity Manager reporting features:

- Select and view reports from a predefined list in the BI Publisher.

- Filter report information.
- View reports on-screen in the desired format.
- Provide interactive reports.

19.2 Starting Oracle Identity Manager Reports

Start BI Publisher server explicitly as managed server from the WebLogic Administrative Console.

To start BI Publisher:

1. Navigate to **Start, Oracle BI Publisher Desktop, Oracle - BIPHome10134**, and then click **Start BI Publisher**.

The Oracle BI Publisher Home page appears.

2. Enter the user name and password.
3. Click **Sign In**.

19.3 Running Oracle Identity Manager Reports

To run a report:

Note: BI Publisher cannot be accessed through Oracle Identity Manager UI. You must open BI publisher explicitly to access the Oracle Identity Manager 11g reports.

1. Start Oracle Identity Manager Reports. See [Section 19.2, "Starting Oracle Identity Manager Reports"](#) for more information.
2. Click the **more...** link under **Shared Folders**.
3. Do one of the following to access the reports.
 - Click **Oracle Identity Manager Reports**.
 - Click the **more...** link under **Oracle Identity Manager Reports**.

The resulting page displays Oracle Identity Manager Reports classified according to their functional areas.

4. To view a report:
 - a. Select the report by clicking its name.
 - b. Click **View**.

The Report Input Parameters page is displayed. This page displays the input parameters that must be provided to run a report. The report input parameters act as a filter criterion.

In some cases, at least one or more parameter fields are required fields. Some reports do not require any input parameter. If this is not the case, then you must populate at least one of the fields to run a report.

Note: If you leave the input parameter field blank, and then click **View**, all the information associated with the report is displayed.

5. Enter the information required to identify what information the report contains.
6. Click **View** to run the report.
The report is displayed.

19.4 Supported Output Formats

BI Publisher supports multiple report output formats. All reports are generated in a native XML format which can be transformed into different other output formats. The following formats are supported:

- HTML
- PDF
- RTF
- MHTML

19.5 Reports for Oracle Identity Manager

All the reports containing Date type input parameters, have the following default date range in the date type input parameters:

Date Range is : Sysdate-30 To Sysdate.

If you want to run the reports for different date range, then please change the date type input parameters with your date ranges.

Oracle Identity Manager Reports are now classified based on the functional areas. For instance, Access Policy Reports, Attestation, Request and Approval Reports, Password Policy Reports, and so on. It is no longer named Operational and Historical.

Oracle Identity Manager Reports are classified into the following categories based on their functional areas:

- [Access Policy Reports](#)
- [Attestation, Request, and Approval Reports](#)
- [Role and Organization Reports](#)
- [Password Reports](#)
- [Resource and Entitlement Reports](#)
- [User Reports](#)
- [Certification Reports](#)
- [Exception Reports](#)
- [Best Practices for Running Oracle Identity Manager Reports](#)

19.5.1 Access Policy Reports

Oracle Identity Manager BI Publisher Reports provides the following access policy reports for Oracle Identity Manager:

- [Access Policy Details](#)
- [Access Policy List by Role](#)

19.5.1.1 Access Policy Details

It provides administrators or auditors the ability to view a current snapshot of all the policies defined in Oracle Identity Manager system, along with key information about each policy, and the number of instances in which each policy has been activated.

Input Parameters

The following table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Access Policy Name	Name of the Access Policy

Fields

The following table lists the fields of the report:

Report Field	Description
Description	Description of the policy
Approval Required	Approval required for the policy
Creation Date	Date when the policy is created
Retrofit Access Policy	Retrofit of the access policy
Created By	Name of the person who created the policy
Priority	Priority of the policy

Columns

The following table lists the columns of the report:

Report Column	Description
Resource Name	Name of the resource

19.5.1.2 Access Policy List by Role

It lists all policies defined in Oracle Identity Manager system by role. This report can be used for operational and compliance purposes.

Input Parameters

The following table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Role Name	Name of the role

Fields

The following table lists the fields of the report:

Report Field	Description
Description	Description of the policy
Approval Required	Approval required for the policy
Creation Date	Date when the policy is created
Retrofit Access Policy	Retrofit of the access policy
Created By	Name of the person who created the policy
Priority	Priority of the policy

Columns

The following table lists the columns of the report:

Report Column	Description
Role Name	Name of the role

19.5.2 Attestation, Request, and Approval Reports

Oracle Identity Manager BI Publisher Reports provides the following attestation, request, and approval reports for Oracle Identity Manager:

- [Approval Activity](#)
- [Attestation Process List](#)
- [Attestation Request Details](#)
- [Attestation Requests by Process](#)
- [Attestation Requests by Reviewer](#)
- [Request Details](#)
- [Request Summary](#)
- [Task Assignment History](#)

19.5.2.1 Approval Activity

This report provides the administrators the ability to view the approval activity including requests that are approved, rejected, or pending.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Approver's First Name	First name of the approver

Report Parameter	Description
Approver's Last Name	Last name of the approver
Approver's User ID	User ID of the approver
Organization	Name of the organization

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Approver's First Name	First name of the approver
Approver's Last Name	Last name of the approver
Approver's User ID	User ID of the approver
Organization	Organization of the approver
Approval Accepted	Count of the accepted approval
Approval Rejected	Count of the rejected approval
Approvals Pending	Count of the pending approval
Approval Requests Total	Total number of approval requests

19.5.2.2 Attestation Process List

This report displays details of all the attestation process. The security model is implemented in this report.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Attestation Process Name	Name of the attestation process
Attestation Process Owner	Owner of the attestation process

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Attestation Process Name	Name of the attestation process
Owner User ID	ID of the owner of attestation process
Date of Current Request	Data on which the request was made
Date of Last Completion	Data on which the request was completed
Certified	Attestation process certified
Rejected	Attestation process rejected
Declined	Attestation process declined
Delegated	Attestation process delegated
Total	Sum of certified, rejected, and declined

19.5.2.3 Attestation Request Details

It lists details of selected Oracle Identity Manager attestation requests.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Attestation Process Name	Name of the attestation process
Attestation Request ID	ID of the attestation process
Request Initiation Date Range From	Start date of the attestation request
Request Initiation Date Range To	End date of the attestation request

Fields

The following table lists the fields of the report:

Report Field	Description
Attestation Process Name	Name of the attestation process

Report Field	Description
Attestation Request ID	ID of the attestation request
Request Initiation Date	Date on which the request is initiated
Completion	Date on which the request is completed
Certified	Attestation process certified
Rejected	Attestation process rejected
Delegated	Attestation process delegated
No Action	Number of attestation processes on which no action is taken

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user who initiated the attestation request
Last Name	Last name of the user who initiated the attestation request
User ID	ID of the user who initiated the attestation request
Resource	Name of the resource
Descriptive Data	Date on which the request is completed
Reviewer's First Name	First name of the reviewer
Reviewer's Last Name	Last name of the reviewer
Reviewer's User ID	ID of the reviewer
Action	Action taken by the reviewer

19.5.2.4 Attestation Requests by Process

This report displays details of all the attestation process and the request for each process, where the logged in user is a member of the administrator or the owner role of the attestation process.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Attestation Process Name	Name of the attestation process
Attestation Process Owner	Owner of the attestation process

Fields

The following table lists the fields of the report:

Report Field	Description
Attestation Owner	Name of the attestation process owner
Total Number of Requests	Total number of requests
Last Completion Date	Date by which attestation should be completed
Current Request Initiation Date	Date on which attestation is initiated

Columns

The following table lists the columns of the report:

Report Column	Description
Request ID	ID of the attestation request
Initiation Date	Date on which attestation is initiated
Completion Date	Date by which attestation should be completed
Certified	Attestation process certified
Rejected	Attestation process rejected
Declined	Attestation process declined
Delegated	Attestation process delegated
Total Attested	Sum of certified records, rejected records and declined records

19.5.2.5 Attestation Requests by Reviewer

It displays list of attestation requests by reviewer. The report includes the number of requests associated with each reviewer and information about each request. In addition, it displays the time at which the request is created and completed.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Reviewer First Name	First name of the reviewer
Reviewer Last Name	Last name of the reviewer
Reviewer User ID	User ID of the reviewer

Fields

The following table lists the fields of the report:

Report Field	Description
Reviewer 's First Name	First name of the reviewer
Reviewer 's Last Name	Last name of the reviewer
Reviewer 's User ID	User ID of the reviewer
Total Number of Requests	Count of requests to review

Columns

The following table lists the columns of the report:

Report Column	Description
Request ID	ID of the attestation request
Process Name	Name of the process
Initiation Date	Date on which attestation is initiated
Completion Date	Date by which attestation should be completed
Certified	Attestation process certified
Rejected	Attestation process rejected
Declined	Attestation process declined

Report Column	Description
Delegated	Attestation process delegated
Total Attested	Count of requests to attest

19.5.2.6 Request Details

This report provides administrators the ability to view the details (requestor, current approver and so on) of all requests with the input current status. Additionally, this report displays the details of all users (user name, organization, manager details, user status and so on) that will be provisioned as a result of the request approval. This helps administrators in planning and prioritizing operational activities so that they may expedite the closure of pending requests.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Requestor User First Name	First name of the requestor
Requestor User Last Name	Last name of the requestor
Request User ID	ID of the requestor
Request ID	Request ID
Request Parent ID	Parent ID of the request
Request Status	Status of the request
Request Type	Type of the request
Request Date From	Start date of the request
Request Date To	End date of the request
Beneficiary User First Name	First name of the beneficiary
Beneficiary User Last Name	Last name of the beneficiary
Beneficiary User ID	ID of the beneficiary

Fields

The following table lists the fields of the report:

Report Field	Description
Request ID	Request ID
Request Type	Type of the request
Requester User ID	ID of the requester

Report Field	Description
Request Date	Date on which request is initiated
Approver User ID	ID of the approver
Current Status	Status of the request
Parent Request ID	ID of the parent Requester

Columns

The following table lists the columns of the report, if a beneficiary is present:

Report Column	Description
First Name	First name of the beneficiary
Last Name	Last name of the beneficiary
User ID	ID of the beneficiary
User Type	Type of user
User Status	Status of the beneficiary
Organization	Organization of the beneficiary
Request Value	Request value of the resource

The following table lists the columns of the report, if a beneficiary is not present:

Report Column	Description
Request Name	Name of the request
Request Value	Value of the request

19.5.2.7 Request Summary

This report provides administrators the ability to view the current status of all requests raised in the specified time interval. This helps administrators in planning and prioritizing operational activities so that they may expedite the closure of pending requests.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Request Type	Type of request
Request Date From	Start date of the request

Report Parameter	Description
Request Date To	End date of the request
Organization	Details of the organization

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Request ID	Request ID
Parent Request ID	ID of the parent Requester
Request Type	Type of request
Request Status	Status of request
Requestor User ID	ID of the requestor
Beneficiary User ID	ID of the beneficiary
Request Details	Details of the request
Approver User ID	ID of the approver
Request Date	Date of request

19.5.2.8 Task Assignment History

It lists the history of all task assignments.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
User ID	ID of the beneficiary
Assignee First Name	First name of the assignee
Assignee Last Name	Last name of the assignee
Assignee User ID	ID of the assignee
Assignee Role Name	Role name of the assignee
Assignee User Name	User name of the assignee
Employee Type	Type of employee

19.5.3 Role and Organization Reports

Oracle Identity Manager BI Publisher Reports provides the following role and organization reports for Oracle Identity Manager:

- [Role Membership History](#)
- [Role Membership Profile](#)
- [Role Membership](#)
- [Organization Details](#)
- [User Membership History](#)

19.5.3.1 Role Membership History

This report displays membership history of all the roles. The report will not show indirect memberships.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Role Name	Name of the role
Role Category	Category of the role
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date
Membership Status	Status of membership: Revoked, Active

Report Parameter	Description
Effective From	Role membership effective from date
Effective To	Role membership effective to date

Fields

The following table lists the fields of the report:

Report Field	Description
Created By	Name of the person who created the role
Creation Date	Date on which the role was created

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Type	Type of employee
Employee Status	Status of the employee
Membership Status	Membership date of the user
Effective From	Membership start date of the user
Effective To	Membership end date of the user
Manager's First Name	First name of the manager
Manager's Last Name	Last name of the manager
Manager's User ID	ID of the manager

19.5.3.2 Role Membership Profile

This report shows number of users present for number of roles and the details of users belonging to count number of roles.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Organization	Organization of the user

Fields

The following table lists the fields of the report:

Report Field	Description
Membership in Number of Roles	Number of members in number of roles
Number of Users	Number of users in the role

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor

19.5.3.3 Role Membership

This report displays membership details of all roles.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Role Name	Name of the role
Role Category	Category of the role
Organization	Name of the organization
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date

Fields

The following table lists the fields of the report:

Report Field	Description
Created By	Name of the person who created the user
Creation Date	Date on which the user is created

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of user
Employee Status	Status of the user
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Member Since	Joining date of the user
Manager's First Name	First name of the manager
Manager's Last Name	Last name of the manager
Manager's User ID	ID of the manager

19.5.3.4 Organization Details

It lists the hierarchical organization structure and details about users in the organization.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Organization Name	Name of the organization

Fields

The following table lists the fields of the report:

Report Field	Description
Parent Organization Name	Name of the parent organization

Columns

The following table lists the columns of the report:

Report Column	Description
Role	Name of Administrator User roles
First Name	First name of the user in the organization
Last Name	Last name of the user in the organization
User ID	ID of the user
User Status	Status of the user
User Type	Type of user
Start Date	Joining date of the user
End Date	Leaving date of the user

19.5.3.5 User Membership History

This report lists the logged in users with their membership history.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Last Name	First name of the user
First Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
User First Name	First name of the user
User Last Name	Last name of the user
Organization	Organization of the user
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor

Columns

The following table lists the columns of the report:

Report Column	Description
User Role	Name of the user role
Membership Status	Status of membership
Effective From	Date from which the membership is effective

19.5.4 Password Reports

Oracle Identity Manager BI Publisher Reports provides the following password reports for Oracle Identity Manager:

- [Password Expiration Summary](#)
- [Password Reset Summary](#)
- [Resource Password Expiration](#)

19.5.4.1 Password Expiration Summary

This report shows the list of all active users whose Oracle Identity Manager passwords are about to expire within a specified period.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Last Name	Last name of the user
First Name	First name of the user

Report Parameter	Description
User ID	ID of the user
Organization	Organization of the user
Expiration Date Range From	Start date of the expiration date
Expiration Date Range To	End date of the expiration date

Fields

N/A

Columns

The following table lists the columns of the report:

Report Field	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date
Organization	Organization of the user
Password Expiration Date	Date on which the password expires

19.5.4.2 Password Reset Summary

This report provides the ability to view the aggregated metrics around password change attempts done by users themselves or on behalf of them. The metrics include all password change attempts, successful or failure outcome of password change attempt, users locked due to multiple concurrent unsuccessful password change attempts.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Aggregation Frequency	The frequency of the report generated

Report Parameter	Description
Date Range From	Start date of the report generated
Date Range To	End date of the report generated
Organization	Name of the organization

Fields

The following table lists the fields of the report:

Report Field	Description
Aggregation Frequency	The frequency of the report generated

Columns

The following table lists the columns of the report:

Report Column	Description
Time Period	Date and time of reset attempts performed
Reset Attempts	Number of reset attempts
Failed Reset Attempts	Number of failed reset attempts
Locked Users due to Failed Reset Attempts	Number of users locked due to a failed reset attempt
Resets by non-beneficiary	Number of resets by non-beneficiary

19.5.4.3 Resource Password Expiration

It lists users whose resource passwords will expire in a specified time period.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
User Status	Status of the user
Password Expiration Date From	The password expiry starting date

Report Parameter	Description
Password Expiration Date To	The password expiry ending date

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Field	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
User Status	Status of the user: Active, Disabled, Deleted, Disabled Until Start Date
User Type	Type of the user: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Password Expiration Date	Date on which the password expires

19.5.5 Resource and Entitlement Reports

Oracle Identity Manager BI Publisher Reports provides the following resource and entitlement reports for Oracle Identity Manager:

- [Account Activity In Resource](#)
- [Delegated Admins and Permissions by Resource](#)
- [Delegated Admins by Resource](#)
- [Entitlement Access List](#)
- [Entitlement Access List History](#)
- [Financially Significant Resource Details](#)
- [Resource Access List History](#)
- [Resource Access List](#)
- [Resource Account Summary](#)
- [Resource Activity Summary](#)

- [User Resource Access History](#)
- [User Resource Access](#)
- [User Resource Entitlement](#)
- [User Resource Entitlement History](#)

19.5.5.1 Account Activity In Resource

It lists all account activities in each resource. It also provides information on how each user is associated with a specific activity of that resource.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
Date Range From	Date from which reports are displayed
Date Range To	Date to which reports are displayed

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Name	Name of the resource
Activity Type	The type of activity
Resource Authorizer User Role(s)	Name of the role which authorize the role
Resource Administrator User Role(s)	Name of the role which authorize the resource

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
User Status	Status of the user: Active, Disabled, Deleted, Disabled Until Start Date
Organization	Organization of the user

Report Column	Description
Manager's User ID	ID of the manager
Timestamp	Date when the report is created

19.5.5.2 Delegated Admins and Permissions by Resource

This report displays the list of user roles with write and delete access that are administrators of the resource.

Input Parameters

The table lists the report parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Administrator Role Name	Name of the Administrator role
Administrator Role Information	Information about the Administrator role
Read Access	Indicates whether the resource has read access
Write Access	Indicates whether the resource has write access
Delete Access	Indicates whether the resource has delete access
Authorizer Role	Authorizer role name
Name Priority	Priority of the resource
Created By	Name of the person who created the resource
Creation Date	Resource creation date

19.5.5.3 Delegated Admins by Resource

The report displays the list of user roles that are the administrators or authorizers of the resource and members of those roles.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
Resource Type	Type of resource
Resource Audit Objective	Objective to carry out the audit for the resource

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource
Target	Indicates whether the resource is a target for organization or user
Write Access	Indicates whether the resource has write access
Delete Access	Indicates whether the resource has delete access
Creation By	Resource creation source
Creation Date	Date on which resource is created

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
User Status	Status of the user
Member Since	Joining date of the user
Manager's First Name	First name of the manager
Manager's Last Name	Last name of the manager

Report Column	Description
Manager's User ID	ID of the manager

19.5.5.4 Entitlement Access List

This report provides administrators or auditors the ability to query all existing users, who have a specified entitlement. This report can be used for operational and compliance purposes.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Entitlement Code	Code of the entitlement
Resource Name	Name of the resource
Organization	Organization of the user
Role Name	Name of the role
User Status	Status of the user: Active, Disabled, Deleted, Disabled Until Start Date
User Type	Type of user
Provisioning Date From	Date from which the resource is provisioned to the user
Provisioning Date To	Date to which the resource is provisioned to the user

Fields

The following table lists the fields of the report:

Report Field	Description
Entitlement Code	Code of the entitlement
Entitlement Name	Name of the entitlement
Entitlement status	Status of the entitlement.
Resource Name	Name of the resource
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
User Id	ID of the user
First Name	First name of the user
Last Name	Last name of the user
User Status	User Status
User Type	Type of the user
Organization	Organization of the user
Valid To Date	Entitlement valid from date
Valid From Date	Entitlement valid to date

19.5.5.5 Entitlement Access List History

This report provides administrators or auditors the ability to query all existing users provisioned to a entitlement over its lifecycle. This is a lifetime report showing entire history of resource's access list or entitlements.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Entitlement Code	Code of the entitlement
Resource Name	Name of the resource
Organization	Organization of the user
Role Name	Name of the role
User Status	Status of the user: Active, Disabled, Deleted, Disabled Until Start Date
User Type	Type of user
Effective From Date	Entitlement effective from date
Effective To Date	Entitlement effective to date

Fields

The following table lists the fields of the report:

Report Field	Description
Entitlement Code	Code of the entitlement

Report Field	Description
Entitlement Name	Name of the entitlement
Resource Name	Name of the resource
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
User Id	ID of the user
First Name	First name of the user
Last Name	Last name of the user
User Status	Status of the user
User Type	Type of user
Effective From	Entitlement effective from date
Effective To	Entitlement effective to date

19.5.5.6 Financially Significant Resource Details

This report provides Administrators to get a list of financially significant resources to prioritize various administrative and cleanup activities. It also helps Compliance or Privacy and Security officers assessing effectiveness of preventive and detective controls in financial significant resources and Auditors to understand the IT resources that host financial data.

Input Parameters

The table lists the report parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
User Roles	Lists the resource administrator user roles

19.5.5.7 Resource Access List History

This report provides administrators or auditors the ability to query all existing users provisioned to a resource over its lifecycle. This is a lifetime report showing entire history of resource's access list or entitlements.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
User Status	Status of the user
User Type	Type of the user
Snapshot Date From	Effective start date of resource access to the user
Snapshot Date To	Effective end date of resource access to the user
Changes Date From	Resource changed from date to user
Changes Date To	Resource changed to date to user

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user

Report Column	Description
User ID	ID of the user
Organization	Organization of the user
Resource Descriptive data	Descriptive data to identify the resource
User Status	Status of the user
Resource Status	Status of the resource
Effective From	Effective start date
Effective To	Effective end date

19.5.5.8 Resource Access List

This report provides administrators or auditors the ability to query all existing users provisioned to a specified resource. This report can be used for operational and compliance purposes.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
User Status	Status of the user
User Type	Type of the user
Provisioning Date From	Resource provision start date
Provisioning Date To	Resource provision end date

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Parameter	Description
First Name	First name of the user

Report Parameter	Description
Last Name	Last name of the user
User ID	ID of the user
User Type	Type of the user
User Status	Status of the user
Organization	Organization of the user
Provisioning Date	Date on which the resource is provisioned

19.5.5.9 Resource Account Summary

This report lists the number of users for each status within each resource.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
Resource Type	Type of resource
Account Status	Status of the account

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource
Total Number of Users	Total number of users associated with the account

Columns

The following table lists the columns of the report:

Report Column	Description
Account Status	Status of the account
Number of Users	Number of users with that account status

19.5.5.10 Resource Activity Summary

It lists the history of all provisioning and approval activities for a resource.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
Date Range From	Start date
Date Range To	End date

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
Accounts Provisioned	Number of accounts provisioned
Accounts De-Provisioned	Number of accounts de-provisioned
Approval Requests	Number of approval requests
Approval Accepted	Number of approved requests
Approval Rejected	Number of rejected requests

19.5.5.11 User Resource Access History

This report provides administrators or auditors the ability to view user's resource access history over user's lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a user access profile snapshot report. This is a lifetime report showing entire history of user's entitlements.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Status	Status of the user
Employee Type	Type of employee

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
User First Name	First name of the user
User Last Name	Last name of the user
Manager User ID	ID of the reporting Manager
Manager First Name	First name of the reporting Manager
Manager Last Name	Last name of the reporting Manager
Organization	Organization of the user
Employee Status	Status of employee
Employee Type	Type of employee
Identity Creation Date	User creation date

Columns

The following table lists the columns of the report:

Report Column	Description
Resource Name	Name of the resource
Resource Descriptive Data	Description of the resource
Provisioned Date	Date on which the resource is provisioned
Provisioned By	Name of the person who provisioned the resource
Effective From	Effective start date of resource access to the user
Effective To	Effective end date of resource access to the user

19.5.5.12 User Resource Access

This report provides administrators or auditors the ability to query all existing users provisioned to a specified resource. This report can be used for operational and compliance purposes.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Status of employee
Employee Type	Type of employee

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
User First Name	First name of the user
User Last Name	Last name of the user
Manager User ID	ID of the reporting Manager
Manager First Name	First name of the reporting Manager
Manager Last Name	Last name of the reporting Manager
Organization	Organization of the user
Employee Status	Status of employee
Employee Type	Type of employee
Identity Creation Date	User creation date

Columns

The following table lists the columns of the report:

Report Column	Description
Resource Name	Name of the resource
Resource Descriptive Data	Description of the resource
Resource Status	Status of the resource
Provisioned Date	Date on which the resource is provisioned

19.5.5.13 User Resource Entitlement

This report provides administrators or auditors the ability to query all existing entitlements provisioned to specific users. This report can be used for operational and compliance purposes.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
User ID	ID of the user
First Name	First name of the user
Last Name	Last name of the user
Email	Email of the user
Resource Name	Name of the resource
Organization	Organization of the user
Role Name	Name of the role
User Status	Status of the user
User Type	Type of the user

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
First Name	First name of the user
Middle Name	Middle name of the user
Last Name	Last name of the user
Email	Email of the user
Organization	Organization of the user
User Status	Status of the user
User Type	Type of the user
Manager First Name	First name of the manager
Manager Last Name	Last name of the manager
Start Date	Entitlement of resource start date
End Date	Entitlement of resource end date

Columns

The following table lists the columns of the report:

Report Column	Description
Entitlement Code	Code of the entitlement

Report Column	Description
Entitlement Name	Name of the entitlement
Entitlement Status	Status of the entitlement
Resource	Type of the resource
Provisioning Start	Date from which the resource is provisioned to the user
Valid From Date	Entitlement of resource valid start date

19.5.5.14 User Resource Entitlement History

This report provides administrators or auditors the ability to view user's resource entitlement history over user's lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a user access profile snapshot report. This is a lifetime report showing entire history of user's entitlements.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
User ID	ID of the user
First Name	First name of the user
Last Name	Last name of the user
Email	Email of the user
Resource Name	Name of the resource
Organization	Organization of the user
Role Name	Name of the role
User Status	Status of the user
User Type	Type of the user
Effective From Date	Resource entitlement effective start date
Effective To Date	Resource entitlement effective end date

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
First Name	First name of the user
Last Name	Last name of the user

Report Field	Description
User Status	Status of the user
User Type	Type of the user
Organization	Organization of the user
Email	Email of the user
Start Date	Start date of resource entitlement
End Date	End date of resource entitlement
Identity Creation Date	Date of identity creation
Manager First Name	First name of the manager
Manager Last Name	Last name of the manager

Columns

The following table lists the columns of the report:

Report Column	Description
Entitlement Code	Code of the entitlement
Entitlement Name	Name of the entitlement
Resource	Type of the resource
Effective From Date	Resource entitlement effective start date
Effective To Date	Resource entitlement effective end date

19.5.6 User Reports

Oracle Identity Manager BI Publisher Reports provides the following user reports for Oracle Identity Manager:

- [User Profile History](#)
- [User Summary](#)
- [Users Deleted](#)
- [Users Disabled](#)
- [Users Unlocked](#)

19.5.6.1 User Profile History

This report shows all the users and their details based on the input parameters.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Role Name	Role of the user
Manager User ID	ID of the Manager to whom the user reports
Employee Status	Status of the user
Employee Type	Type of employee
Changes Date Range From	Effective start date of the changes
Changes Date Range To	Effective end date of the changes
Snapshot Date Range From	Effective start date of resource access to the user
Snapshot Date Range To	Effective end date of resource access to the user

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
User First Name	First name of the user
User Last Name	Last name of the user
Manager User ID	ID of the reporting Manager
Manager First Name	First name of the reporting Manager
Manager Last Name	Last name of the reporting Manager
Organization	Organization of the user
Employee Status	Status of employee
Employee Type	Type of employee
Identity Creation Date	User creation date

Columns

The following table lists the columns of the report:

Report Column	Description
Profile Parameter	Name of user profile
Value	Value of user profile
Date Effective From	Effective from date
Time Effective From	Effective from time

19.5.6.2 User Summary

It lists all Oracle Identity Manager users created in a specified time period. In addition, it provides information on whether the users were created manually or through trusted reconciliation.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Status	Status of the user
Employee Type	Type of employee
Creation Date From	Start date of user summary
Creation Date To	End date of user summary

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Status of the user
Employee Type	Type of employee
Manager ID	ID of the Manager to whom the user reports
Source	User creation source

Report Column	Description
Creation Date	Date at which the user is created

19.5.6.3 Users Deleted

This report shows all the deleted users and their details based on input parameters.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Type	Type of employee
Deletion Date From	Start date of summary of deleted users
Deletion Date To	End date of summary of deleted users

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Type	Type of employee
Manager ID	ID of the Manager to whom the user reports
Source	User creation source
Deletion Date	Date at which the user is deleted

19.5.6.4 Users Disabled

This report provides the ability to view the details of users whose accounts are disabled. The account may be disabled for various reasons. For example, rejection in attestation, unsuccessful login or password reset attempts failure and so on.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Type	Type of employee
Disabled Date From	Start date of user disabled
Disabled Date To	End date of user disabled

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Current status of the employee
Employee Type	Type of employee
Manager ID	ID of the Manager to whom the user reports
Source	User creation source
Disabled Date	Date at which the user is disabled

19.5.6.5 Users Unlocked

This report provides the ability to view the details of users whose disabled accounts are unlocked by administrators. Delegated administrators of the organizations to whom the user belongs may enable the accounts.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user

Report Parameter	Description
User ID	ID of the user
Organization	Organization of the user
Employee Type	Type of employee
Unlocked Date From	Start date of user unlocked
Unlocked Date To	End date of user unlocked

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Status of the user
Employee Type	Type of employee
Manager ID	ID of the Manager to whom the user reports
Source	User creation source
Unlocked Date	Date at which the user is unlocked

19.5.7 Certification Reports

Certification reports select data from the certification tables of the Oracle Identity Manager database. For detailed information about certification reports, see "Generating Certification Reports" in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

19.5.8 Exception Reports

In Oracle Identity Manager, **exception** refers to the difference between accounts that a user is entitled to and the accounts that are actually assigned to a user. The user is assigned these accounts as a result of access policies, provisioning of resources, approval requests, and reconciliation events. Any difference of these accounts assigned to a user in the target system and the ones assigned to the user in Oracle Identity Manager comprises an exception.

To populate the data for account audit and reconciliation exceptions report:

1. Set the value of the XL.EnableExceptionReports system property to True. See "Administering System Properties" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for information about system properties.

2. Verify that the Object Initial Reconciliation Date field of the resource object is earlier than the sysdate.

Oracle Identity Manager provides the following exception reports:

- **Rogue Accounts By Resource**

This report returns a list of all the rogue accounts existing in a resource. The following exceptions are reported:

- An account that exists in the target system, but is not provisioned to the corresponding user in Oracle Identity Manager
- An account that exists in the target system, but has been deprovisioned for the corresponding user in Oracle Identity Manager

- **Orphaned Account Summary Report:** An account that exists in the target system, but the corresponding user to whom the account is provisioned has been deleted in Oracle Identity Manager. For the given input resource, it lists the rogue accounts that exist in the target system, but the corresponding users to whom the accounts are provisioned has never existed in Oracle Identity Manager.

- **Fine Grained Entitlement Exceptions By Resource**

This report returns a list of all the accounts in a resource for which the process form data being reconciled is different from the expected values. It means that this report returns any account existing in the target system that is also provisioned to the corresponding user in Oracle Identity Manager, but for which the process data does not match.

Note:

- After completion of initial target reconciliation, all account-related activities performed directly on a target resource are tracked as exception activity. Account-related activities include account creation, account modification, and entitlement assignment/revocation. The exception reports should be used only if the organization policies enforce that all account-related activities in target resources would always be initiated in Oracle Identity Manager. In addition, remember that exception detection and recording are an extension of account data reconciliation and, therefore, may result in a drop in performance during reconciliation.
 - All the exception reports depend on reconciliation data. Therefore, these reports will not display any data if the corresponding reconciliation events are archived.
-
-

This section describes the following exception reports:

- [Fine Grained Entitlement Exceptions By Resource](#)
- [Orphaned Account Summary](#)
- [Rogue Accounts By Resource](#)

19.5.8.1 Fine Grained Entitlement Exceptions By Resource

This report enables administrators, signing officers, internal and external auditors to analyze discrepancies in various process forms and related child tables of various

resources and mitigate material weaknesses in the resources through remediation activities.

Input Parameters

The table lists the report parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Type	Type of the employee such as fulltime, part time
Organization Name	Name of the organization
Role Name	Name of the role

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Name	Name of the resource
User ID	ID of the user

Columns

The following table lists the columns of the report:

Report Column	Description
Form Name	Name of the form
Form Type	Type of the form

Note: Before running this report, you must populate data for account audit and reconciliation exceptions.

To populate the data for account audit and reconciliation exceptions:

1. Set the value of the system property, `XL.EnableExceptionReports`, to True.
2. Provision an user to any target.
3. Modify any of the user's attribute in the target and reconcile the user.
4. Find data in `UPA_UD_FORMFIELDS` and `UPA_UD_FORMS` tables.
5. Go to Oracle Identity Manger server and run `RefreshMaterializedViewScheduler` Task.
6. Log in to BIP and view the report.

19.5.8.2 Orphaned Account Summary

It lists the rogue accounts for the input resource for which a user existed in the target system, but the associated user to whom the account is provisioned never existed in Oracle Identity Manager.

Input Parameters

The table lists the report parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
Reconciliation Date Range From	Start date of reconciliation
Reconciliation Date Range To	End date of reconciliation

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Resource	Name of the resource
Account Information	Information of the orphaned account
Reconciliation Date	Date of reconciliation

19.5.8.3 Rogue Accounts By Resource

This report includes all rogue accounts for the input resource. This report also includes the corresponding attestation data to analyze if the rogue accounts represent outstanding or accepted exceptions in the system. This enables administrators, signing officers, internal and external auditors to identify material weaknesses in the resources and plan their mitigation through remediation activities.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization Name	Organization of the user
User Status	Status of the user
User Type	Type of the user

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
User Status	Status of the user
User Type	Type of the user
Exception Type	Type of exception
Exception Approved in Attestation	Indicates whether the exception is approved or not
Reviewer First Name	First name of the reviewer
Reviewer Last Name	Last name of the reviewer
Reviewer User ID	User ID of the reviewer

19.5.9 Best Practices for Running Oracle Identity Manager Reports

As a best practice, you must consider the following points before running Oracle Identity Manager BI publisher reports:

- Do not run Oracle Identity Manager reports with null value in date range parameters. You must run Oracle Identity Manager reports always with date range values in data range parameters, otherwise report will not display anything.
- Invoke the reports with the set of values as input parameters to provide the selectivity, thus improving the performance.

19.6 Creating Reports Using Third-Party Software

Oracle Identity Manager supports the creation of reports by using third-party tools such as Crystal Reports. You can use a third-party tool to create the reports listed in [Section 19.5, "Reports for Oracle Identity Manager"](#).

Note: To learn how to create reports by using third-party software, see the third-party software documentation.

19.7 Required Scheduled Tasks for BI Publisher Reports

Table 19–1 lists the scheduled tasks required for Oracle Identity Manager BI Publisher reports:

Table 19–1 *Scheduled Tasks for BI Publisher Reports*

Report Name	Scheduled Task Name	Description
Fine Grained Entitlement Exceptions By Resource	RefreshMaterializedView	To refresh the Materialized View used in this report with the latest data
User Profile History	IssueAuditTask	To populate the audit tables with the latest data
User Unlocked	IssueAuditTask	To populate the audit tables with the latest data
User Membership History	IssueAuditTask	To populate the audit tables with the latest data
Role Membership History	IssueAuditTask	To populate the audit tables with the latest data
Resource Access List History	IssueAuditTask	To populate the audit tables with the latest data
User Resource Access History	IssueAuditTask	To populate the audit tables with the latest data
Resource Activity Summary	IssueAuditTask	To populate the audit tables with the latest data
Password Reset Summary	IssueAuditTask	To populate the audit tables with the latest data
Entitlement Reports	Entitlement List	To populate the Entitlement List table with the marked entitlements
	Entitlement Assignment	To populate the Entitlement Assignment tables with the assigned entitlements
	Entitlement Updates	To populate the latest data into the Entitlement Assignment tables, if any entitlement has assigned to any user periodically or later

Using the Archival Utilities

This chapter describes how to use the various archival utilities in the following sections:

- [Using the Reconciliation Archival Utility](#)
- [Using the Task Archival Utility](#)
- [Using the Requests Archival Utility](#)
- [Using the Audit Archival and Purge Utility](#)

Note: You can use the Reconciliation Archival utility, the Task Archival utility, and the Requests Archival utility in both offline and online modes.

20.1 Using the Reconciliation Archival Utility

This section describes how to use the Reconciliation Archival utility. It contains the following topics:

- [Understanding the Reconciliation Archival Utility](#)
- [Prerequisite for Running the Reconciliation Archival Utility](#)
- [Archival Criteria](#)
- [Running the Reconciliation Archival Utility](#)
- [Log File Generated by the Reconciliation Archival Utility](#)

20.1.1 Understanding the Reconciliation Archival Utility

Oracle Identity Manager stores reconciliation data from target systems in Oracle Identity Manager tables called **active reconciliation tables**:

During the reconciliation process, Reconciliation Manager reconciles data in the active reconciliation tables with the Oracle Identity Manager core tables. Because Reconciliation Manager does not remove reconciled data from the active reconciliation tables, they might eventually grow very large, resulting in decreased performance during the reconciliation process. You can use the Reconciliation Archival utility to archive data that has been reconciled with Oracle Identity Manager. The Reconciliation Archival utility stores archived data in the **archive reconciliation tables**, which have the same structure as the active reconciliation tables.

Table 20–1 lists the active reconciliation tables with the corresponding archive reconciliation tables in which data from the active reconciliation tables are archived.

Table 20–1 Active and Archive Reconciliation Tables

Active Reconciliation Tables (Oracle Identity Manager Tables)	Archive Reconciliation Tables
RECON_EVENTS	ARCH_RECON_EVENTS
RECON_JOBS	ARCH_RECON_JOBS
RECON_BATCHES	ARCH_RECON_BATCHES
RECON_EVENT_ASSIGNMENT	ARCH_RECON_EVENT_ASSIGNMENT
RECON_EXCEPTIONS	ARCH_RECON_EXCEPTIONS
RECON_HISTORY	ARCH_RECON_HISTORY
RECON_USER_MATCH	ARCH_RECON_USER_MATCH
RECON_ACCOUNT_MATCH	ARCH_RECON_ACCOUNT_MATCH
RECON_CHILD_MATCH	ARCH_RECON_CHILD_MATCH
RECON_ORG_MATCH	ARCH_RECON_ORG_MATCH
RECON_ROLE_MATCH	ARCH_RECON_ROLE_MATCH
RECON_ROLE_HIERARCHY_MATCH	ARCH_RECON_ROLE_HIER_MATCH
RECON_ROLE_MEMBER_MATCH	ARCH_RECON_ROLE_MEMBER_MATCH
RA_LDAPUSER	ARCH_RA_LDAPUSER
RA_MLS_LDAPUSER	ARCH_RA_MLS_LDAPUSER
RA_LDAPROLE	ARCH_RA_LDAPROLE
RA_MLS_LDAPROLE	ARCH_RA_MLS_LDAPROLE
RA_LDAPROLEMEMBERSHIP	ARCH_RA_LDAPROLEMEMBERSHIP
RA_LDAPROLEHIERARCHY	ARCH_RA_LDAPROLEHIERARCHY
All horizontal tables mentioned under RECON_TABLES	"ARCH_" + substr(HTnames,1,25)

You can use the Reconciliation Archival utility to perform the following tasks:

- Archive all or specific data from the active reconciliation tables to the archive reconciliation tables
- Delete all data from the active reconciliation tables

When you archive data by moving it from the active reconciliation tables to the archive reconciliation tables, you must specify the date in the YYYYMMDD format, such as all records on or before this date will be archived, and a reconciliation event status parameter value, which defines the data that you want to archive. For information about these archiving criteria, refer to ["Archival Criteria"](#) on page 3.

If you choose to archive selective data, then the utility archives reconciliation data based on selected event status that have been created on or before the specified date and event status.

When you archive all data from the active reconciliation tables to the archive reconciliation tables, the Reconciliation Archival utility archives all reconciliation data that have been created on or before the specified date.

The files that constitute the Oracle Database version of the Reconciliation Archival utility are located in the following directory:

```
OIM_ORACLE_HOME/server/db/oim/oracle/Utilities/Recon11gArchival
```

You can run the Reconciliation Archival utility in offline mode with Oracle Identity Manager stopped, or in online mode with Oracle Identity Manager running.

Before running the utility in offline mode, you must stop Oracle Identity Manager.

20.1.2 Prerequisite for Running the Reconciliation Archival Utility

Before running the Reconciliation Archival utility, the OIM_RECON_ARCH tablespace must be created in the database. To do so, you can run the following sample command as a DBA privilege user, for instance SYS or SYSTEM.

```
CREATE TABLESPACE OIM_RECON_ARCH
  LOGGING DATAFILE 'ORADATA/OIM_RECON_ARCH.dbf'
  SIZE 500M REUSE AUTOEXTEND ON NEXT 10M;
```

Note:

- You must replace *ORADATA* in the preceding sample command with the full path to your *ORADATA* directory.
 - You must set *LD_LIBRARY_PATH* to start Oracle utilities such as SQL*Plus in the environment where you want to run Oracle Identity Manager utilities.
 - Data that has been archived from the active reconciliation tables to the archive reconciliation tables will no longer be available through Oracle Identity Manager. To access this data, you must query the archive reconciliation tables in your Oracle Identity Manager database.
-
-

If you are using ASM, Exadata (ASM) or Oracle Managed Files (OMF), then follow the instructions described here.

If you are using ASM, then you can use the name of a diskgroup say *DATA 1* to create the tablespace in the database as follows:

```
CREATE TABLESPACE OIM_RECON_ARCH
  LOGGING DATAFILE '+DATA1'
  SIZE 500M AUTOEXTEND ON NEXT 10M;
```

If you are using Oracle Managed Files, then you can omit the datafile and run the command as follows:

```
CREATE TABLESPACE OIM_RECON_ARCH
  LOGGING DATAFILE
  SIZE 500M AUTOEXTEND ON NEXT 10M;
```

If you want to run the utility in offline mode, then you must stop Oracle Identity Manager before running the utility.

20.1.3 Archival Criteria

To select reconciliation data to archive, provide the following criteria. Data with matching values will be archived.

- Date must be in the format YYYYMMDD. All records on or before this date that match the specified reconciliation event parameter value will be archived.
- Select Closed, Linked, Closed or Linked, or All for the reconciliation event parameter.
 - Closed describes events that have been manually closed in Reconciliation Manager.
 - Linked describes events that were reconciled in Oracle Identity Manager, including the following states:
 - * Creation Succeeded
 - * Update Succeeded
 - * Delete Succeeded
 - * Creation Failed
 - * Update Failed
 - * Delete Failed
 - Closed or Linked
 - Select status for reconciliation events to be archived.
 - * Enter 1 for Closed
 - * Enter 2 for Linked
 - * Enter 3 for Closed and Linked
 - * Enter 4 for Exit

20.1.4 Running the Reconciliation Archival Utility

To run the Reconciliation Archival utility:

1. Ensure that the Oracle Identity Manager database is available and that no reconciliation processes are running.

Note: Oracle recommends that you run the Reconciliation Archival utility during off-peak hours.

2. If you want to run the utility in offline mode, then stop Oracle Identity Manager by following the instructions in the ["Starting and Stopping Servers"](#) chapter.

To run the utility in online mode, ignore this step and proceed to step 3.

3. On Microsoft Windows platforms, you must specify the short date format as M/d/yyyy. In addition, you must specify the time format as H:mm:ss. To customize the date and time formats, use the Regional and Language Options command in Control Panel.

Note:

- When you change the date and time format, the change is applied to all the applications running on the Microsoft Windows platform.
- Minimal validation is done on date before calling the utility, and you can scan logs files for any ORA-18xx errors for invalid date-related errors.

4. On Linux or UNIX platforms, run the following commands to set execution permission for the `oim_recon_archival.sh` file and to ensure that the file is a valid Linux or UNIX text file:

```
chmod 755 path/oim_recon_archival.sh
dos2unix path/oim_recon_archival.sh
```

5. On Linux or UNIX platforms, run the `path/oim_recon_archival.sh` file to run the utility.
On Microsoft Windows platforms, run the `path\oim_recon_archival.bat` file to run the utility.
6. For Oracle Database installations, enter values for the following parameters when prompted:
 - Oracle home directory
 - Oracle Identity Manager database user name and password
7. Enter the reconciliation creation date in the YYYYMMDD format. All records on or before this date with required status value will be archived.
8. When prompted, select a reconciliation event status for the data that you want to archive:
 - Enter 1 for Closed
 - Enter 2 for Linked
 - Enter 3 for Closed or Linked
 - Enter 4 for Exit
9. When prompted to specify the mode of running the utility, enter 1 if you want to run the utility in online mode. Otherwise, enter 2 to run the utility in offline mode.
10. Enter the batch size for processing.

The default batch size is 5000.

Note: Batch size is a value for the number of records to be processed in a single iteration of archival/purge, also as an internal commit at the database level. You must provide the batch size as an input parameter value while starting the operation of Archival Utilities at run time.

This batch size by default is 5000. When purging greater than few hundred thousand `recon_events`, a higher batch size can be opted for. This may need more resources from RDBMS, such as more space from the TEMP and UNDO tablespaces.

The utility archives the reconciliation data and provides an execution summary in a log file.

11. On Microsoft Windows platforms, reset the short date format to the date format for your region or locale after you run the utility. Use the Regional and Language Options command in Control Panel to reset the date format.
12. Because the data from active reconciliation tables are removed, your DBA must analyze the active reconciliation tables and their indexes in order to update the statistics. Perform this step only if you are using Oracle Database as the database for Oracle Identity Manager.

20.1.5 Log File Generated by the Reconciliation Archival Utility

After running the Reconciliation Archival utility, the following log file is generated:

```
./logs/oim_recon_archival_summary_TIMESTAMP.log
```

If running the utility fails, then the log file records the batch number at which the utility fails along with the error messages.

20.2 Using the Task Archival Utility

This section describes how to use the Task Archival utility. It contains the following topics:

- [Understanding the Task Archival Utility](#)
- [Preparing Oracle Database for the Task Archival Utility](#)
- [Running the Task Archival Utility](#)
- [Reviewing the Output Files Generated by the Task Archival Utility](#)

20.2.1 Understanding the Task Archival Utility

In Oracle Identity Manager, a **task** refers to one or more activities that comprise a process, which handles the provisioning of a resource. For example, a process for requesting access to a resource may include multiple provisioning tasks. Oracle Identity Manager stores task data in the following tables, which are called **active task tables**:

- OSI
- OSH
- SCH

By default, Oracle Identity Manager does not remove completed tasks from the active task tables. As the size of the active task tables increases, you might experience a reduction in performance, especially when managing provisioning tasks. After a task executes successfully, you can use the Task Archival utility to archive the task data and remove it from the active task tables. Archiving task data with the Task Archival utility improves performance and ensures that the data is safely stored.

The Task Archival utility stores archived task data in the following **archive task tables**, which have the same structure as the active task tables:

- ARCH_OSI
- ARCH_OSH
- ARCH_SCH

You can use the Task Archival utility to archive the following types of tasks:

- Provisioning tasks for resource instances that have been revoked for disabled or deleted users
- Provisioning tasks for resource instances that have been revoked

When you archive tasks with the Task Archival utility, you can specify the type of archive operation, the user status, the task execution date, and the number of records above which to drop the indexes before archiving. The archive operation represents the type of task data to archive and the user status determines whether to archive data for users who have been deleted, disabled, or both. The task execution date represents the date on which a task is executed and must be in the format YYYYMMDD.

All executed tasks, up to the task execution date you specify, will be archived. To reduce the time that the archiving process takes, the utility drops the indexes on all active task tables when the number of records to be archived is greater than 200000. The indexes are re-created after the archived data is deleted from the active task tables. You can change the value 200000 to your preferred value. You can change the value in the following lines of code in the OIM_TasksArch.bat file or in the OIM_TasksArch.sh file:

In the .bat file, set `INDXRESP=200000`

In the .sh file, `indxopt=200000`

The files that constitute the Oracle Database version of the Task Archival utility are located in the following directory:

`OIM_HOME/db/oim/oracle/Utilities/TaskArchival`

Note: Data that has been archived from the active task tables to the archive task tables will no longer be available through Oracle Identity Manager. To access this data, you must query the archive task tables in your Oracle Identity Manager database.

You can run the Task Archival utility in offline mode with Oracle Identity Manager stopped, or in online mode with Oracle Identity Manager running.

Before running the utility in offline mode, you must stop Oracle Identity Manager.

20.2.2 Preparing Oracle Database for the Task Archival Utility

Before you can use the Task Archival utility with Oracle Database, you must perform the following steps:

1. Start SQL*Plus and connect to Oracle Database as a SYS user.
2. Create a separate tablespace for the archival task tables by entering the following command. Replace `DATA_DIR` with the directory in which you want to store the data file and adjust the size and other parameters as necessary for your environment.

```
CREATE TABLESPACE TasksArch
  DATAFILE 'DATA_DIR\tasksarch_01.dbf' SIZE 1000M REUSE
  EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
```

Note: Oracle recommends that you allocate a large UNDO tablespace when archiving large amounts of data. In addition, turn on parallel execution by configuring the `parallel_max_servers` and `parallel_min_servers` initialization parameters. Parallel execution helps improve the performance of the archival process.

3. Connect to Oracle Database as the Oracle Identity Manager database user.
4. Enter the following command to run the `cr_taskarchival_ddl_table.sql` script, which creates a table named `OIM_TASK_ARCH_DDL`. This table is used by the Task Archival utility.

```
@ path/cr_taskarchival_ddl_table.sql
```

5. Enter the following command to run the `Create_TasksArch_Tables.sql` script, which creates the archive task tables:

```
@ path/Create_TasksArch_Tables.sql
```

6. Enter the following command to run the `OIM_SP_TASKS_ARCHIVAL.sql` script, which creates a stored procedure that the Task Archival utility uses to archive and delete task data:

```
@ path/OIM_SP_TASKS_ARCHIVAL.sql
```

Note: You must set `LD_LIBRARY_PATH` to start Oracle utilities such as `SQL*Plus` in the environment where you want to run Oracle Identity Manager utilities.

20.2.3 Running the Task Archival Utility

Perform the following steps to run the Task Archival utility:

1. Ensure that the Oracle Identity Manager database is available but it is not open to other Oracle Identity Manager transactions.

Note: Oracle recommends that you run the Task Archival utility during off-peak hours.

2. Ensure that you have created a backup of the `OSI`, `SCH`, and `OSH` tables.
3. If you want to run the utility in offline mode, then stop Oracle Identity Manager by following the instructions in the ["Starting and Stopping Servers"](#) chapter.
To run the utility in online mode, ignore this step and proceed to step 4.
4. On Microsoft Windows platforms, you must specify the short date format as `dddd M/d/yyyy`. In addition, you must specify the time format as `H:mm:ss`. To customize the date and time formats, select the `Regional and Language Options` command in the Control Panel.

Note:

- When you change the date and time format, the change is applied to all the applications running on the Microsoft Windows platform
 - Minimal validation is done on date before calling the utility, and you can scan logs files for any ORA-18xx errors for invalid date-related errors
-
-

5. On Linux and UNIX platforms, run the path/OIM_TasksArch.sh file. On Microsoft Windows platforms, run the path\OIM_TasksArch.bat file.
6. For Oracle Database installations, enter values for the following parameters when prompted:
 - Oracle home directory
 - Oracle Identity Manager database name or TNS string if the Oracle Identity Manager database is running on a remote computer
 - Oracle Identity Manager database user name and password
7. When prompted, select one of the following options:
 - Archive all provisioning tasks on resource instances that have been revoked for disabled or deleted users.
 - Archive all provisioning tasks on resource instances that have been revoked.
 - Exit.
8. When prompted to specify the mode of running the utility, enter 1 if you want to run the utility in online mode. Otherwise, enter 2 to run the utility in offline mode.
9. If you chose to archive all provisioning tasks for resource instances that have been revoked for disabled or deleted users, select one of the following options:
 - Users at Deleted status
 - Users at Disabled status
 - Users at Deleted and Disabled status
 - Go back to Main Menu
10. Enter a task execution date in the format YYYYMMDD when prompted. All executed tasks, up to the task execution date you specify, will be archived. To archive all tasks that were executed on or before the current date, press **Enter** without entering a date.
11. Summary information is displayed before the utility starts the archival process. The summary information gives you the total number of tasks to be archived. Read the summary information carefully and make sure your database can support the delete volume listed in the summary.

Enter a value of **y** or **Y** when prompted to archive the tasks. Otherwise, enter a value of **n** or **N** to exit the utility.

Note: You must enter the value of Y or N when prompted. If you press Enter without selecting a value, then the utility again counts the number of tasks to be archived and prompts you without beginning the archive.

12. On Microsoft Windows platforms, reset the short date format to the date format for your region or locale after the Task Archival utility finishes running. Use the Regional and Language Options command in the Control Panel to reset the date format.

Note: You must analyze the active task tables and their indexes for updated statistics, because the data from active task tables is removed. Perform this step only if you are using Oracle Database as the database for Oracle Identity Manager.

20.2.4 Reviewing the Output Files Generated by the Task Archival Utility

Table 20–2 describes the output files that are generated by the Task Archival utility.

Table 20–2 *Output Files Generated by the Task Archival Utility*

File	Description
Err_DB_Conn_timestamp.log	Generated when the utility is unable to connect to the database with the specified credentials
Err_Arch_Tasks_timestamp.log	Generated when the archival or deletion processes fail
Arch_TaskData_timestamp.log	Generated when the archival or deletion processes succeed

Note: These error log files are deleted when you run the utility again.

20.3 Using the Requests Archival Utility

This section describes how to use the Requests Archival utility. It contains the following topics:

- [Understanding the Requests Archival Utility](#)
- [Prerequisites for Running the Requests Archival Utility](#)
- [Input Parameters](#)
- [Running the Requests Archival Utility](#)
- [Log Files Generated by the Utility](#)

20.3.1 Understanding the Requests Archival Utility

By default, Oracle Identity Manager does not remove closed or withdrawn requests from the active request tables. To archive these requests and free up the disk space and thereby enhance database performance, the Requests Archival utility is used. You can archive request data based on request creation date and request status. Archiving

requests based on the request status is optional. By using request status, you can archive:

- Completed requests such as requests with status Withdrawn, Closed, and Completed. This is specified by selecting the **1 for Completed** option.
- Completed and failed requests such as requests with status Withdrawn, Closed, Completed, Failed, and Partially Failed. This is specified by selecting option **2 for Completed and Failed**.
- All requests based on request creation date. This is specified by selecting option **3 for All**.

Table 20–3 lists the names of the tables which are to be archived and the corresponding archival table names.

Table 20–3 Archival Tables

Main Table	Archival Table
REQUEST	ARCH_REQUEST
REQUEST_HISTORY	ARCH_REQUEST_HISTORY
REQUEST_APPROVALS	ARCH_REQUEST_APPROVALS
REQUEST_ENTITIES	ARCH_REQUEST_ENTITIES
REQUEST_ENTITY_DATA	ARCH_REQUEST_ENTITY_DATA
REQUEST_BENEFICIARY	ARCH_REQUEST_BENEFICIARY
REQUEST_BENEFICIARY_ENTITIES	ARCH_REQUEST_BE
REQUEST_BENEFICIARY_ENTITYDATA	ARCH_REQUEST_BED
REQUEST_TEMPLATE_ATTRIBUTES	ARCH_REQUEST_TA
WF_INSTANCE	ARCH_WF_INSTANCE
REQUEST_COMMENTS	ARCH_REQUEST_COMMENTS

The files that constitute the Oracle Database version of the Requests Archival utility are located in the following directory:

`OIM_HOME/db/oim/oracle/Utilities/RequestArchival`

You can run the Requests Archival utility in offline mode with Oracle Identity Manager stopped, or in online mode with Oracle Identity Manager running.

Before running the utility in offline mode, you must stop Oracle Identity Manager.

20.3.2 Prerequisites for Running the Requests Archival Utility

Before running the Requests Archival utility:

Note: You must set `LD_LIBRARY_PATH` to start Oracle utilities such as SQL*Plus in the environment where you want to run Oracle Identity Manager utilities.

- Create the `OIM_REQUEST_ARCH` tablespace. When the Requests Archival utility is run for the first time, a corresponding archival table is created for all the tables that are to be archived. The archival tables are created in a separate tablespace

named OIM_REQUEST_ARCH. This tablespace must be created before running the utility.

- Create the required archival tables for the request tables by running the oim_create_request_arch_tables.sql script. This is the PL/SQL script to create archival tables against all tables that are to be archived.
- If you want to run the utility in offline mode, then you must stop Oracle Identity Manager before running the utility.

20.3.3 Input Parameters

Table 20–4 lists the input parameters used by the Requests Archival utility:

Table 20–4 Input Parameters

Parameter	Description
Oracle Home	The value of <code>ORACLE_HOME</code> environment variable on the system.
Oracle SID	The SID of the Oracle Identity Manager database, which is a TNS name or TNS alias.
OIM DB User	The database login ID of the Oracle Identity Manager database user.
OIM DB Pwd	The password of the Oracle Identity Manager database user.
Request Status	The request status based on the user inputs 1, 2, or 3.
Request Creation Date	The utility archives all requests created on or before this request creation date with the required request status.
Batch Size	The utility processes a group of records or batch as a single transaction. The batch size can influence the performance of the utility. Default value of Batch Size is 2000.
Utility Running Mode	The mode in which you want to run the utility, online or offline. You must enter 1 for online mode, or 2 for offline mode. The utility runs faster when you run it in offline mode than online mode. However, running the utility in offline mode requires downtime. The archival operation can be speeded up by running in offline mode, but Oracle Identity Manager is not usable until the utility completes the archival operation. Therefore, make sure that Oracle Identity Manager is not running before choosing this option.

20.3.4 Running the Requests Archival Utility

To run the Requests Archival utility:

1. Ensure that the Oracle Identity Manager database is available.

Note: It is recommended that you run the Requests Archival utility during off-peak hours.

2. If you want to run the utility in offline mode, then stop Oracle Identity Manager by following the instructions in the "Starting and Stopping Servers" chapter.

To run the utility in online mode, ignore this step and proceed to step 3.

3. On Microsoft Windows platform, you must specify the short date format as `dddd M/d/yyyy`. In addition, you must specify the time format as `H:mm:ss`. To customize the date and time formats, use the Regional and Language Options command in Control Panel.

Note:

- When you change the date and time format, the change is applied to all the applications running on the Microsoft Windows platform.
 - Minimal validation is done on date before calling the utility, and you can scan logs files for any ORA-18xx errors for invalid date-related errors.
-
-

4. On UNIX platform, run the following commands to set execution permission for the `OIM_request_archival.sh` file and to ensure that the file is a valid UNIX text file:

```
chmod 755 path/OIM_request_archival.sh
dos2unix path/OIM_request_archival.sh
```

5. On UNIX platform, run the `path/OIM_request_archival.sh` file. On Microsoft Windows platform, run the `path\OIM_request_archival.bat` file.

The `oim_request_archival` script validates the database input and establishes a connection with the database. It then calls the `oim_request_archival.sql` script, the script is used to compile PL/SQL procedures related to the utility.

6. For Oracle Database installations, enter values for the following parameters when prompted:
 - Oracle home directory.
 - Oracle Identity Manager database name or TNS string if the Oracle Identity Manager database is running on a remote computer. Otherwise, enter ORACLE SID.
 - Oracle Identity Manager database user name and password.
7. When prompted, enter one of the following options:
 - Enter 1 to archive the requests with status Request Withdrawn, Request Closed, or Request Completed, and requests with creation date on or before the request creation date specified by the user in the format `YYYYMMDD`.
 - Enter 2 to archive the requests with status Request Withdrawn, Request Closed, Request Completed, or Request Partially Failed, and requests with creation date on or before the request creation date specified by the user in the format `YYYYMMDD`.
 - Enter 3 to archive all the requests with request creation date on or before the request creation date specified by the user in the format `YYYYMMDD`.
8. When prompted to specify the mode of running the utility, enter 1 if you want to run the utility in online mode. Otherwise, enter 2 to run the utility in offline mode.
9. Specify the batch size, when prompted.

Note: Batch size is a value for the number of records to be processed in a single iteration of archival/purge also an internal commit at the database level. You must provide the batch size as an input parameter value while starting the operation of Archival Utilities at run time.

This batch size by default is 2000. A higher batch size can be opted for, but this might require more resources from the database, such as more space from the TEMP and UNDO tablespaces.

The utility archives the request data and provides an execution summary in a log file.

10. On Microsoft Windows platforms, reset the short date format to the date format for your region or locale after you run the utility. Use the Regional and Language Options command in Control Panel to reset the date format.
11. Because the data from active request tables are removed, your DBA must analyze the active request tables and their indexes in order to update the statistics. Perform this step only if you are using Oracle Database as the database for Oracle Identity Manager.

20.3.5 Log Files Generated by the Utility

All the logs are written to the logs/ directory created in the current folder. [Table 20–5](#) lists the log files generated by the utility.

Table 20–5 *Logs Generated by the DB Archival Utility*

Log File	Description
oim_create_request_arch_tables.log	Created when the utility fails to create the archival tables
oim_request_archival.log	Created when the utility fails to create the procedures required for archival
validate_date.log	Created when the input REQUEST_CREATION_DATE is invalid
oim_request_archival_summary_TIMESTAMP.log	Contains the summary of the run
Err_DB_Conn_TIMESTAMP_ATTEMPTNUMBER.log	Created when the utility is unable to connect to the database with the credentials provided

20.4 Using the Audit Archival and Purge Utility

This section describes how to use the Audit Archival and Purge utility. It contains the following topics:

- [Overview](#)
- [Prerequisites for Using the Utility](#)
- [Preparing the UPA Table for Archival and Purge](#)
- [Archiving or Purging the UPA Table](#)

Note: The partitioning feature of Oracle Database Enterprise Edition is required for implementing audit archival and purge.

20.4.1 Overview

Continuous data generation in the Oracle Identity Manager database schema and the audit data growth results in a gradual increase in the storage consumption of the database server. The audit data is populated in the UPA table. The growth of data in the UPA table can pose disk space and maintenance issues. Therefore, old audit data in the UPA table must be cleaned or archived.

To keep this disk space consumption in control, you can use the Audit Archival and Purge utility. This utility controls the growth of the audit data by purging the data in a logical and consistent manner.

Note:

- The audit archival and purge solution is only applicable to the UPA table. It is not applicable to audit reporting tables, which are tables with the UPA_ prefix.
 - The utility is compatible with Oracle Identity Manager release 9.1.0 and later.
-
-

You must shut down Oracle Identity Manager to fetch the latest data, which is to retrieve EFF_TO_DATE as null records. You can retrieve the remaining data later when Oracle Identity Manager is running with the new partitioned UPA.

Oracle recommends partitioning of the UPA table on the basis of calendar year, which allows you to archive or drop partitions. The advantage of partitioning is that the old partitions can be archived or purged because Oracle Identity Manager does not use old audit data lying in those partitions. Oracle Identity Manager uses the latest audit data and the current calendar year data. Therefore, the UPA table is partitioned based on date range-partitioning approach by calendar year using EFF_TO_DATE column. After partitioning, the latest audit data where EFF_TO_DATE is NULL, can be grouped in one partition, and there will be one partition for each calendar year. Oracle Identity Manager do not read or write into any other partitions except the latest and current year partitions.

For instance, if you are using Oracle Identity Manager audit feature since 2005 and implementing the audit archive and purge solution in calendar year 2011, then you will have seven partitions after this exercise, assuming that you create a partition for each calendar year. In those seven partitions, Oracle Identity Manager will only read or write the following partitions:

- The latest partition
- The partition for the current year, for example 2011

All the previous year partitions can be archived and then purged. If you do not want to archive, then you can purge those old partitions. You can reclaim the space by archiving and purging those old partitions. You must keep the latest and current year partitions untouched for Oracle Identity Manager to continue working.

20.4.2 Prerequisites for Using the Utility

The following prerequisites must be met before or when using the Audit Archival and Purge utility:

- Database partitioning is supported only on Enterprise Edition of Oracle Database. Therefore, to implement the audit archival and purge solution, you must run Enterprise Edition of Oracle Database.

- The UPA table must be range-partitioned. Time interval can be any value as per data distribution. Other modes of partition methods are not supported.
- Make sure that the latest backup of the UPA table is available. Creating a backup of the UPA table is a compulsory prerequisite before applying this solution. It is recommended to try out this solution in the development or staging environment before implementing it on the production database.
- Decide how many previous year's of audit data you require to keep online before implementing this solution. This helps in creating partitions beforehand.
- Each partition should be placed on its own tablespace. Do not share the tablespace between partitions of different year or with some other data.
- During partitioning, the audit data for each calendar year is copied into a table before it is moved into a final destination. You must have provision for disk space to hold the copied data.

20.4.3 Preparing the UPA Table for Archival and Purge

To prepare the UPA table for the audit and purge solution:

1. Make sure that Oracle Identity Manager database has no transaction against it until the UPA table is partitioned.
2. Query the UPA table to get the minimum and maximum calendar year for the audit data. Following queries can help you get the minimum and maximum year. The maximum year should be the current calendar year.

```
SELECT EXTRACT (YEAR FROM MIN (eff_to_date)) min_year,
EXTRACT (YEAR FROM MAX (eff_to_date)) running_year FROM upa;
```

This helps in deciding the partitions for each calendar year starting from minimum year.

3. Make sure that Oracle Identity Manager is not running and is not available for off-line utilities.
4. Create a new partition table.

Assuming 2005 as minimum year and 2011 as running or current calendar year, the following decisions are to be made before creating a newly partition table:

- How many years of old audit data you want to keep? If it is important to keep only three years of audit data, then you have to create newly partitioned table starting from year 2008. The data older than 2008 will get cleaned up when the original UPA table gets dropped.
- After deciding the years of old data to keep, the next question is how and where the old data should be kept? Do you want to keep all the old data partitions in the active UPA table, or create backup of the old partitions and then drop the old partitions? Oracle recommends moving the old partitions into tapes and then purging them from the UPA table. As stated earlier, you must keep the latest and running calendar year partition untouched.

The following sample assumes that you want to keep three years of audit data in UPA table and current calendar year is 2011:

```
SQL> SELECT 'Create Table UPA_PART
(
UPA_KEY NUMBER (19) Not Null,
USR_KEY NUMBER (19) Not Null,
EFF_FROM_DATE TIMESTAMP (6) Not Null,
```

```

EFF_TO_DATE TIMESTAMP (6),
SRC VARCHAR2 (4000),
SNAPSHOT CLOB,
DELTAS CLOB,
SIGNATURE CLOB
)
PARTITION BY RANGE (EFF_TO_DATE)
(PARTITION UPA_2008 VALUES LESS THAN (TO_DATE('01/01/2009', 'DD/MM/YYYY'))
Tablespace upa_2008,
PARTITION UPA_2009 VALUES LESS THAN (TO_DATE('01/01/2010', 'DD/MM/YYYY'))
Tablespace upa_2009,
PARTITION UPA_2010 VALUES LESS THAN (TO_DATE('01/01/2011', 'DD/MM/YYYY'))
Tablespace upa_2010,
PARTITION UPA_2011_PART1 VALUES LESS THAN
(TO_DATE(' ' || TO_CHAR(SYSDATE, 'DD/MM/YYYY HH24:MI:SS') || ' ', 'DD/MM/YYYY
HH24:MI:SS')) TABLESPACE UPA_2011_PART1,
PARTITION UPA_2011_PART2 VALUES LESS THAN
(TO_DATE('01/01/2012', 'DD/MM/YYYY')) TABLESPACE UPA_2011_PART2,
PARTITION UPA_LATEST VALUES LESS THAN (MAXVALUE) TABLESPACE UPA_MAX
)
ENABLE ROW MOVEMENT;' FROM DUAL;

```

5. Create another non-partitioned table with similar structure as the UPA table, by running the following statement:

```

SQL> Create table upa_non_part Tablespace TBS_NAME as select * from upa where
1=2;

```

Here, *TBS_NAME* is the name of the same tablespace as of partition, which is to be exchanged.

This table is temporary in nature. The purpose of this table is to facilitate the loading of audit data to a newly partitioned UPA table.

Note: UPA_NON_PART or temporary non-partitioned table must be created on same tablespace as the partition to be exchanged.

6. Load the latest audit data into the non-partitioned UPA table, as shown:

```

SQL> Insert /*+ parallel */ into upa_non_part select /*+ parallel */ * from
upa where eff_to_date is null;
SQL> COMMIT;

```

Note: Using hint */*+parallel*/* in the INSERT statement is optional and you can use other hints also to improve performance according to the available resources.

7. Swap the data into the partitioned table by using the ALTER TABLE command, as shown:

```

SQL> ALTER TABLE upa_part EXCHANGE PARTITION UPA_LATEST WITH TABLE UPA_NON_PART
WITH VALIDATION UPDATE GLOBAL INDEXES;

```

8. Drop the upa_non_part table, as shown:

```

SQL> DROP TABLE upa_non_part;

```

While exchanging partitions, the data dictionary is updated instead of writing data physically. Therefore, it is necessary to drop and re-create the temporary non-partitioned UPA_NON_PART table in the same tablespace associated to the partition to be exchanged.

9. Rename the original non-partitioned UPA table to UPA_OLD, as shown:

```
SQL> ALTER TABLE upa rename TO upa_old;
```

10. Rename the newly partitioned UPA_PART table to UPA:

```
SQL> RENAME UPA_PART to UPA;
```

11. Manage the constraints for the new UPA table. To do so:

- a. Rename the constraint from old UPA table to some other name, as shown:

```
ALTER TABLE UPA_old RENAME CONSTRAINT PK_UPA TO PK_UPA_old;
ALTER INDEX IDX_UPA_EFF_FROM_DT RENAME TO IDX_UPA_EFF_FROM_DT_old;
ALTER INDEX IDX_UPA_EFF_TO_DT RENAME TO IDX_UPA_EFF_TO_DT_old;
ALTER INDEX IDX_UPA_USR_KEY RENAME TO IDX_UPA_USR_KEY_old;
ALTER INDEX PK_UPA RENAME TO PK_UPA_OLD;
```

- b. Create the necessary indexes and primary key constraint on the newly partitioned UPA table. Make sure to add storage characteristics, such as tablespace and size. To do so, run the following SQL query:

```
SQL>create index IDX_UPA_EFF_FROM_DT on UPA (EFF_FROM_DATE) Local;
SQL>create index IDX_UPA_EFF_TO_DT on UPA (EFF_TO_DATE) Local;
SQL>create index IDX_UPA_USR_KEY on UPA (USR_KEY) Local;
SQL>ALTER TABLE UPA add constraint PK_UPA primary key (UPA_KEY) using
index;
```

Note: The global non-partitioned index is created to support the primary key. Global index becomes unusable every time a partition is touched. You must rebuild the index when required.

12. Run the statistics collection for the UPA table, as shown:

```
SQL>Exec dbms_stats.gather_table_stats(ownname => 'SCHEMA_NAME',tabname =>
'UPA',cascade => TRUE,granularity => 'GLOBAL and PARTITION');
```

Note: Global statistics must be gathered by default. Oracle 11g includes improvements to statistics collection for partitioned objects so untouched partitions are not rescanned. This significantly increases the speed of statistics collection on large tables where some of the partitions contain static data. When a new partition is added to the table, you need to collect statistics only for the new partition. The global statistics is automatically updated by aggregating the new partition synopsis with the existing partitions synopsis.

13. Start Oracle Identity Manager. The database is ready to be opened for transactions. Test and make sure that applications are running as expected.
14. Bring current year data in UPA_2011_PART1 to have all data and maintain consistency for current year. To do so, run the following SQL queries in sequence:

```
SQL> CREATE TABLE upa_non_part Tablespace TBS_NAME AS SELECT * FROM upa WHERE
1=2;
```

Here, *TBS_NAME* is the same tablespace name as of the partition, which is to be exchanged.

```
SQL> Alter Table UPA_NON_PART add constraint PK_UPA_NON_PART primary key
(UPA_KEY) using index;
```

```
.....
.....
SQL> Insert into upa_non_part select * from upa_old where eff_to_date >=
to_date('01/01/2011', 'mm/dd/yyyy');
```

```
.....
.....
SQL> COMMIT;
```

```
.....
.....
```

```
SQL> ALTER TABLE upa_part exchange partition UPA_2011_PART1 WITH table
upa_non_part WITH VALIDATION UPDATE GLOBAL INDEXES;
```

```
.....
.....
SQL> Drop table upa_non_part;
```

- 15.** If required, bring previous year's data into the newly partitioned UPA table. To do so:

- a.** Run the following SQL queries in sequence:

```
SQL> CREATE TABLE upa_non_part Tablespace TBS_NAME AS SELECT * FROM upa
WHERE 1=2;
```

Here, *TBS_NAME* is the same tablespace as of the partition, which is to be exchanged.

```
.....
.....
SQL> Alter Table UPA_NON_PART add constraint PK_UPA_NON_PART primary key
(UPA_KEY) using index;
```

```
.....
.....
SQL> Insert into upa_non_part select * from upa_old where eff_to_date >=
to_date('01/01/YEAR', 'mm/dd/yyyy') and eff_to_date <
to_date('01/01/<YEAR+1>', 'mm/dd/yyyy');
```

Here, *YEAR* is the year for which you want to bring the data into newly partitioned UPA table.

```
.....
.....
SQL>COMMIT;
```

```
.....
.....
SQL> Alter table upa exchange partition UPA_<year> with table upa_non_part
with validation Update global indexes;
```

- b. Rebuild indexes if they are unusable. The Following SQL query shows the indexes that are unusable:

```
SQL> Select index_name, partition_name, tablespace_name, status from
user_ind_partitions;
```

- c. Drop the table upa_non_part, as shown:

```
SQL> Drop table upa_non_part;
```

Note: Repeat step 15 for each old year.

16. All partition operations against UPA table are done and all the data is brought into. Run the statistics collection for the UPA table, as shown:

```
SQL>Exec dbms_stats.gather_table_stats(ownname => '<Schem_name>',tabname =>
'UPA',cascade => TRUE,granularity => 'GLOBAL and PARTITION');
```

17. Drop the UPA_OLD table if it is not required. You can create a backup of this table before dropping.

20.4.4 Archiving or Purging the UPA Table

Archiving and purging the UPA table is described in the following sections:

- [Partitions That Must Not Be Archived or Purged](#)
- [Ongoing Partition Maintenance](#)
- [Archiving or Purging Partitions in the UPA Table](#)

20.4.4.1 Partitions That Must Not Be Archived or Purged

Oracle Identity Manager always requires the latest and the current calendar year audit data. The following are the names of latest and calendar year partitions:

- **UPA_LATEST:** The latest partition
- **UPA_2011_PART1** and **UPA_2011_PART2:** Partitions for the current year if current year is 2011

You must keep these two partitions untouched for Oracle Identity Manager to continue working. These two partitions should never be archived or purged.

20.4.4.2 Ongoing Partition Maintenance

A new partition must be added to the UPA table before the new calendar year arrives. To do so, use the following SQL template:

```
SQL> Alter table UPA split partition UPA_LATEST at
(TO_DATE('01/01/YEAR+1','DD/MM/YYYY')) into (partition UPA_YEAR tablespace
UPA_YEAR,partition UPA_LATEST tablespace UPA_MAX) update global indexes;
```

Here, *YEAR* in the TO_DATE function represents the new calendar year plus one. *YEAR* for partition name and tablespace name represents new upcoming calendar year.

An example of SQL statement for adding new partition for new calendar year 2012 is as follows:

```
SQL> Alter table UPA split partition UPA_LATEST at
```

```
(TO_DATE('01/01/2013','DD/MM/YYYY')) into (partition UPA_2012 tablespace
UPA_2012,partition UPA_LATEST tablespace UPA_MAX) update global indexes;
```

Oracle recommends adding new partition with the given SQL template before the new calendar year arrives. However, if you do not add the same before the arrival of the next calendar year, then the same can be done after the next year has started by using the same SQL command.

20.4.4.3 Archiving or Purging Partitions in the UPA Table

To archive or purge partitions in the UPA table:

1. If you use the attestation feature of Oracle Identity Manager, then make sure that the partition to be archived or purged does not have any active attestation records. You can use the following SQL to verify that.

```
SQL> SELECT COUNT(1) FROM UPA PARTITION(<PARTITION_TO_BE_DROPPED>)
WHERE UPA_KEY IN (select distinct (upa_key) from apt apt, atr atr, atd atd
where apt.atr_key=atr.atr_key and atr.atr_completion_time is NULL and
apt.apt_key = atd.apt_key);
```

This query should return zero records, which means there are no active attestation records. If this returns non-zero value, then it means that there are still active attestations pointing to the partition to be dropped. This is not common, but you must make sure that there are no active attestation records before dropping an old year partition.

2. Make sure that there are no custom reports or queries that needs the data from partition to be dropped.
3. Archive the partition to be dropped to tape or any other media. There are many ways to archive a partition. One of the ways is to use data pump or export utility to archive the partition to be dropped. Choose a way that works best in your environment.
4. Purge the partition. To do so:

```
SQL> Alter table UPA drop partition PARTITION_NAME UPDATE GLOBAL INDEXES;
SQL>Drop tablespace TBS_NAME including contents and datafiles;
```

Here, TBS_NAME is the tablespace associated with the partition to be dropped, and it must not contain any other data.

Note:

- The current year contains two partitions named UPA_2011_PART1 and UPA_2011_PART2. When current year becomes an old year and the data for that is ready to be archived or purged, make sure to archive or purge these two partitions.
 - It is your responsibility to restore the archived data later, if required.
-
-

Part IX

Diagnostics and Troubleshooting

This part describes diagnostics in Oracle Identity Manager and troubleshooting tasks.

It contains the following chapters:

- [Chapter 21, "Configuring Logging"](#)
- [Chapter 22, "Managing Asynchronous Execution"](#)
- [Chapter 23, "Using Enterprise Manager for Managing Oracle Identity Manager Configuration"](#)
- [Chapter 24, "Setting the Language for Users"](#)
- [Chapter 25, "Working with the Diagnostic Dashboard"](#)
- [Chapter 26, "Enabling Diagnostics"](#)
- [Chapter 27, "Handling Errors"](#)

Configuring Logging

Oracle Identity Manager uses two logging services: Oracle Diagnostic Logging (ODL), which is the logging service used by most Oracle Fusion Middleware applications, and Apache log4j.

Oracle Identity Manager logging is primarily done with ODL. Apache log4j is only used with third-party applications, such as Nexaweb for Deployment Manager and Workflow Designer, and OSCache for caching.

This chapter contains the following sections:

- [Logging in Oracle Identity Manager By Using ODL](#)
- [Logging in Oracle Identity Manager By Using log4j](#)
- [Setting Warning State](#)

21.1 Logging in Oracle Identity Manager By Using ODL

Oracle Diagnostic Logging (ODL) is the principal logging service used by Oracle Identity Manager. For ODL logging to work, both loggers and log handlers need to be configured. Loggers send messages to handlers, and handlers accept messages and output them to log files.

Logging configuration is controlled by the logging.xml file described in "[Log Handler and Logger Configuration](#)" on page 21-3. This file can either be edited directly or edited through the Enterprise Manager. On the Enterprise Manager, the logging configuration can be accessed by clicking the OIM server link and by selecting the WebLogic Server drop down from the top, and then clicking on Logs - Log Configuration.

To access the logging configuration on the Enterprise Manager:

1. Click the OIM server link.
2. From the WebLogic Server list, select Logs - Log Configuration. All the packages available for logging are displayed on the log configuration screen.

For any additional packages to be logged that are not available in the Enterprise Manager (such as, for connector packages), follow the instructions to manually edit the logging.xml file. The packages specific to Oracle Identity Manager can be accessed under oracle.iam. The different log levels are available for selection under the Oracle Diagnostic Logging Level column. Select a particular log level, and then click **Apply** for the changes to take effect. In addition, new log handlers can be created and configured by clicking the **Log Files** tab.

Each Oracle Identity Manager module has its own logger that can be configured independently to send different amounts of information to one or more log handlers. [Table 21–2, "Oracle Identity Manager Loggers"](#) lists the more than twenty different Oracle Identity Manager loggers that can be configured to send messages to log handlers.

You can output more or less information to a log by adjusting the level attribute for each logger. To select a logging level, choose from one of five message types (INCIDENT_ERROR, ERROR, WARNING, NOTIFICATION, and TRACE). Each message type can also take a numeric value between 1 (highest severity) and 32 (lowest severity) that you can use to further restrict the volume of messages that a logger will output. Table 1 on page 2 lists the message type and level combinations that are used most often.

Log handlers specify the target where log messages should appear. For example, log handlers can write messages to the console, to various log files, and to additional outputs.

This section contains the following topics:

- [Message Types and Levels](#)
- [Log Handler and Logger Configuration](#)
- [Configuring Log Handlers](#)
- [Configuring Loggers](#)
- [Sample ODL Log Output](#)

21.1.1 Message Types and Levels

ODL recognizes five message types: INCIDENT_ERROR, ERROR, WARNING, NOTIFICATION, and TRACE. Each message type can also take a numeric value between 1 (highest severity) and 32 (lowest severity) that you can use to further restrict message output.

When you specify a message type, ODL returns all messages of that type, as well as the messages that have a higher severity. For example, if you set the message type to WARNING, ODL also returns messages of type INCIDENT_ERROR and ERROR.

Message types and levels are described in greater detail in "Setting the Level of Information Written to Log Files" of the *Oracle Fusion Middleware Administrator's Guide*. [Table 21–1](#) lists the diagnostic message types that you can use most often with Oracle Identity Manager.

Table 21–1 Oracle Identity Manager Diagnostic Message Types

Message Type and Numeric Value	Description
INCIDENT_ERROR:1	A serious problem that may be caused by a bug in the product and that should be reported to Oracle Support. Examples are errors from which you cannot recover.
ERROR:1	A serious problem that requires immediate attention from the administrator and is not caused by a bug in the product. An example is if Oracle Fusion Middleware cannot process a log file, then you can correct the problem by fixing the permissions on the document.

Table 21–1 (Cont.) Oracle Identity Manager Diagnostic Message Types

Message Type and Numeric Value	Description
WARNING:1	A potential problem that should be reviewed by the administrator. Examples are invalid parameter values or a specified file does not exist.
NOTIFICATION:1	A major lifecycle event such as the activation or deactivation of a primary sub-component or feature. This is the default level for NOTIFICATION.
NOTIFICATION:16	A finer level of granularity for reporting normal events.
TRACE:1	Trace or debug information for events that are meaningful to administrators, such as public API entry or exit points.
TRACE:16	Detailed trace or debug information that can help Oracle Support diagnose problems with a particular subsystem.
TRACE:32	Very detailed trace or debug information that can help Oracle Support diagnose problems with a particular subsystem.

21.1.2 Log Handler and Logger Configuration

Both log handlers and loggers can be configured by editing `logging.xml`, which is located in:

`DOMAIN_NAME/config/fmwconfig/servers/SERVER_NAME/logging.xml`

Here, `DOMAIN_NAME` and `SERVER_NAME` are the domain name and server name respectively specified during the installation of Oracle Identity Manager.

The `logging.xml` file has a `<log_handlers>` configuration section, followed by a `<loggers>` configuration section. Each log handler is defined within the `<log_handlers>` section, and each logger is defined within the `<loggers>` section.

The file has the following basic structure:

```
<logging configuration>
  <log_handlers>
    <log_handler name='console-handler' level="NOTIFICATION:16"></log_handler>
    <log_handler name='odl-handler'></log_handler>
    <!--Additional log_handler elements defined here....-->
  </log_handlers>
  <loggers>
    <logger name="example.logger.one" level="NOTIFICATION:16">
      <handler name="console-handler"/>
    </logger>
    <logger name="example.logger.two" />
    <logger name="example.logger.three" />
    <!--Additional logger elements defined here....-->
  </loggers>
</logging_configuration>
```

When configuring a logger to write messages to either the console or a file, make configuration changes to both the logger and the handler. Setting the level attribute for the logger configures the amount of detail (and therefore, the volume of messages) that the logger sends to the handler. Similarly, setting the level attribute for the handler configures the amount of detail that the handler accepts from the logger.

Note: If you are not getting the volume of output that you expect in a log, then verify that the level attribute for both the logger and the log handler are set appropriately. For example, if the logger is set to TRACE and the log handler is set to WARN, then the handler does not generate messages more detailed than WARN.

21.1.3 Configuring Log Handlers

Individual log handlers are configured in the <log_handlers> section of the logging.xml file. Configure the level attribute for the handler to set the amount of detail that the handler will accept from loggers.

To configure the log handler-level attribute:

Note: You must have a basic understanding of XML syntax before you attempt to modify the logging.xml file.

1. Open the `DOMAIN_NAME/config/fmwconfig/servers/SERVER_NAME/logging.xml` file.

2. Change the level attribute as shown in the following examples.

In this example XML code, the level attribute for the console-handler is set to WARNING:32.

```
<log_handler name='console-handler'
class='oracle.core.ojdl.logging.ConsoleHandler'
formatter='oracle.core.ojdl.weblogic.ConsoleFormatter' level='WARNING:32' />
```

For the console-handler to be able to write TRACE level messages to the console, change the level attribute as shown:

```
<log_handler name='console-handler'
class='oracle.core.ojdl.logging.ConsoleHandler'
formatter='oracle.core.ojdl.weblogic.ConsoleFormatter' level='TRACE:1' />
```

3. Save your changes and restart the application server.

21.1.3.1 Log Handler Configuration Tools

Log handlers that write to a file have additional properties that can be configured. For example, this excerpt from logging.xml configures the odl-handler:

```
<log_handler name='odl-handler' class='oracle.core.ojdl.logging.ODLHandlerFactory'
filter='oracle.dfw.incident.IncidentDetectionLogFilter'>
  <property name='path'
value='${domain.home}/servers/${weblogic.Name}/logs/${weblogic.Name}-diagnostic.log' />
  <property name='maxFileSize' value='10485760' />
  <property name='maxLogSize' value='104857600' />
  <property name='encoding' value='UTF-8' />
  <property name='useThreadName' value='true' />
  <property name='supplementalAttributes' value='J2EE_APP.name,J2EE_MODULE.name,
WEBSERVICE.name,WEBSERVICE_PORT.name,composite_instance_id,component_instance_id,
composite_name,component_name' />
</log_handler>
```

To make changes to log handler properties, you can use either the Fusion Middleware Control tool or the WLST command-line tool.

See Also:

- "Configuring Settings for Log Files" in the *Oracle Fusion Middleware Administrator's Guide* for information about both the Fusion Middleware Control tool and the WLST command-line tool
- "Logging Custom WLST Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference* for information about the WLST command-line tool

21.1.4 Configuring Loggers

Individual loggers are configured in the <loggers> section of the logging.xml file. More than twenty different Oracle Identity Manager loggers that can be configured to send messages to log handlers. Oracle Identity Manager loggers are described in Table 2 on page 7.

Setting the level attribute for the logger configures the amount of detail (and, hence, the volume of messages) that the logger sends to its handlers. Nesting one or more <handler> elements inside of <logger> elements assigns handlers to loggers.

The following excerpt shows a logger called OIMCP.PSFTCOMMON. The level attribute is set to WARNING:32 and the logger sends messages to three handlers:

```
<logger name="OIMCP.PSFTCOMMON" level="WARNING:32" useParentHandlers="false">
  <handler name="odl-handler" />
  <handler name="wls-domain" />
  <handler name="console-handler" />
</logger>
```

A logger can inherit a parent logger's settings, including the parent's level setting and other attributes, as well as the parent logger's handlers. To disable inheritance, set the useParentHandlers attribute to false, as shown in the previous excerpt.

At the top of the logger inheritance tree is the root logger. The root logger is the logger with an empty name attribute, as shown in the following example.

```
<loggers>
  <logger name="" level="WARNING:1">
    <handler name="odl-handler" />
    <handler name="wls-domain" />
    <handler name="console-handler" />
  </logger>

  <!-- Additional loggers listed here -->
</loggers>
```

If a logger is configured with only its name attribute, the logger will inherit the rest of its attributes from the root logger, as shown in the following example:

```
<loggers>
  <logger name="oracle.iam.identity.rolemgmt" />
  <!-- Additional loggers listed here -->
</loggers>
```

To configure loggers:

1. Open the `DOMAIN_NAME/config/fmwconfig/servers/SERVER_NAME/logging.xml` file.
2. Locate the logger you want to configure. [Table 21–2](#) lists the Oracle Identity Manager loggers.

Table 21–2 Oracle Identity Manager Loggers

Logger	Description
oracle.iam.request oracle.iam.requestdatasetgeneration oracle.iam.requestactions oracle.iam.platform.workflowservice	Logs events related to request and request dataset management.
oracle.iam.selfservice	Logs events related to authenticated and unauthenticated self-service operations.
oracle.iam.ChangePasswordtaskflow	Logs events for the password change functionality UI.
oracle.iam.forgotpasswordtaskflow	Logs events for the "forgot password" functionality UI.
oracle.iam.identitytaskflow	Logs events for the administrative UI identity operations.
oracle.iam.identity.orgmgmt	Logs events related to the organization manager service operations.
oracle.iam.identity.rolmgmt	Logs events related to the role manager service operations.
oracle.iam.identity.usermgmt	Logs events related to the user manager service operations.
oracle.iam.identity.scheduledtasks	Logs events related to scheduled tasks in the identity feature.
oracle.iam.platform.utils	Logs events related to utilities provided by the platform (mainly used by other features). Includes utilities for message resources handling, logging handling, internationalization, caching, and so on.
oracle.iam.platformservice	Logs events related to utilities that are mainly executed from the client side. For example, the plug-in registration utility, the purge cache utility, and so on. Some server-side utilities, such as the date-time utility and the exception handling utility, also use this logger.
oracle.iam.platform.canonic	Logs events related to the platform UI framework.
oracle.iam.consoles.faces oracle.iam.consoles.common	Logs messages generated from the UI framework.
oracle.iam.platform.kernel	Logs events related to the kernel. This includes the logging generated during the handling of orchestrations by the platform. The event handlers executed in the orchestrations within each feature use that feature's respective logger.
oracle.iam.platform.context	Logs events related to the context management feature.

Table 21–2 (Cont.) Oracle Identity Manager Loggers

Logger	Description
oracle.iam.platform.entitymgr	Logs events related to the entity manager feature. This feature provides generic handling of different types of entities, such as users, roles, and so on, and appropriate routing to the respective operations on them.
oracle.iam.scheduler oracle.iam.platform.scheduler Xellerate.Scheduler Xellerate.Scheduler.Task	Logs events related to the scheduler. Note that certain scheduled tasks may also use other loggers.
oracle.iam.reconciliation	Logs events related to the reconciliation feature.
oracle.iam.accesspolicy	Logs events related to the access policy feature.
oracle.iam.autoroles	Logs events related to the auto role membership assignment feature.
oracle.iam.callbacks	Logs events related to the callbacks feature.
oracle.iam.configservice	Logs events related to the Configuration service APIs that are used for configuration of entity attributes.
oracle.iam.ldap-sync	Logs events related to the Oracle Identity Manager and LDAP synchronization feature.
oracle.iam.notification	Logs events related to e-mail templates and the notifications handling feature.
oracle.iam.passwdmgt	Logs events related to the password management feature.
oracle.iam.platform.pluginframework	Logs events from the plug-in framework feature that handles the management of plug-ins.
oracle.iam.platform.async	Logs events from platform that handles asynchronous operations.
oracle.iam.spmlws oracle.iam.wsschema	Logs events related to web services used for Fusion applications that generate requests for different operations.
oracle.iam.diagnostic	Logs messages from the diagnostic service APIs used to run diagnostic checks.
oracle.iam.oimdataprovers	Logs events related to the Oracle Identity Manager data providers. The Oracle Identity Manager data providers provide code to update and fetch data from the Oracle Identity Manager database.
Xellerate.Database	Logs database operations.
Xellerate.PreparedStatement	Same as Xellerate.Database, but logs only PreparedStatement details.
Xellerate.Performance	Logs database performance, such as time to execute a statement (query), or time to iterate through a result set to get data/metadata.

Table 21–2 (Cont.) Oracle Identity Manager Loggers

Logger	Description
oracle.iam.platform.auth	Logs events for the authentication handling feature.
oracle.iam.platform.authz oracle.iam.authzpolicydefn	Logs events for the feature that handles authorization policies.
oracle.iam.sod Xellerate.SoD	Logs events related to SoD (Segregation of Duties).
oracle.jps	Logger for the embedded Oracle Entitlements Server MicroSM engine. Note that the log file is created in the <i>OIM_ORACLE_HOME</i> folder named as Managed Server name-microsm.log (for example, OIMServer1-microsm.log).
Xellerate.Entitlement	Provides logging for entitlement operations used for provisioning entitlements.
oracle.iam.conf	Logs events related to the system configuration services feature that includes handling system properties.
oracle.iam.transUI	Logs events related to the transitional UI feature that handles initiation of legacy APIs from the 11g code. This includes operations such as initiation of provisioning during user creation, and so on.
Xellerate.AccountManagement	Provides logging in legacy user operations APIs.
Xellerate.Server	Provides logging in data objects.
Xellerate.ResourceManagement Xellerate.ObjectManagement	Provides logging for resource object operations.
Xellerate.Workflow	Provides logging for provisioning process operations.
Xellerate.WebApp	Provides logging for the transitional UI operations.
Xellerate.Adapters	Provides logging for the adapter factory.
Xellerate.JavaClient	Provides logging for client-side data objects.
Xellerate.Policies	Provides logging for data objects related to access policies.
Xellerate.Rules	Provides logging for data objects related to rules.
Xellerate.APIs	Provides logging for legacy public APIs.
Xellerate.JMS	Provides logging for JMS operations where messages are produced.
Xellerate.RemoteManager	Provides logging in remote manager.

Table 21–2 (Cont.) Oracle Identity Manager Loggers

Logger	Description	
Xellerate.Auditor	Provides logging in audit framework.	
Xellerate.Attestation	Provides logging in the attestation UI and operations.	
Xellerate.GC.Startup	Provides logging for the Generic Technology Connector (GTC).	
Xellerate.GC.ProviderRegistration		
Xellerate.GC.ImageGeneration		
Xellerate.GC.FrameworkProvisioning		
Xellerate.GC.Provider.ProvisioningFormat		
Xellerate.GC.Provider.ProvisioningTransport		
Xellerate.GC.FrameworkReconciliation		
Xellerate.GC.Provider.ReconciliationFormat		
Xellerate.GC.Provider.Validation		
Xellerate.GC.Provider.Transformation		
Xellerate.GC.Model		
Xellerate.GC.Server		
oracle.iam.connectors.icfcommon		Provides logging for connector framework.

3. Define the level attribute for the <logger> element. See the example at the beginning of this section.
4. Add one or more <handler> elements to the <logger> element.
5. When you are finished editing both the <loggers> and <log_handlers> sections of logging.xml, save the file.
6. Restart the application server for the changes to take effect.

21.1.5 Sample ODL Log Output

The following ODL log excerpt illustrates the kind of output you can expect.

```
<Jun 15, 2010 2:01:20 AM IST> <Error> <oracle.iam.platform.authz.impl>
<IAM-1010032>
<No OES Policy found for the given Action.>
<Jun 15, 2010 2:02:02 AM IST> <Warning> <oracle.iam.platform.canonic.agentry>
<IAM-0091108> <readme.txt is not a valid connector resource file.>
<Jun 15, 2010 2:02:52 AM IST> <Error> <oracle.iam.configservice.impl>
<IAM-3020003> <The attribute User Type does not exist!>
```

For information about managing and interpreting log output, see "Managing Log Files and Diagnostic Data" in the *Oracle Fusion Middleware Administrator's Guide*.

21.2 Logging in Oracle Identity Manager By Using log4j

Apache log4j is used with third-party applications, such as Nexaweb for Deployment Manager and Workflow Designer, and OSCache for caching.

The location of the log4j configuration file is:

`OIM_HOME/config/log.properties`

Logging in Oracle Identity Manager by using log4j is described in the following sections:

- [Log Levels](#)
- [Loggers](#)
- [Configuring and Enabling Logging](#)

21.2.1 Log Levels

Table 21–3 lists the log levels for log4j:

Table 21–3 Log Levels for log4j

Log Level	Description
DEBUG	The DEBUG level designates fine-grained informational events that are useful to debug an application.
INFO	The INFO level designates informational messages that highlight the progress of the application at coarse-grained level.
WARN	The WARN level designates potentially harmful situations.
ERROR	The ERROR level designates error events that might allow the application to continue running.
ALL	The ALL level has the lowest possible rank and is intended to turn on all logging.
OFF	The OFF level has the highest possible rank and is intended to turn off logging.

21.2.2 Loggers

The loggers for the third-party applications used are:

- `com.nexaweb.server` for Nexaweb
- `com.opensymphony.oscache` for OSCache

21.2.3 Configuring and Enabling Logging

Any of the log levels can be used for the third-party applications as follows:

```
log4j.logger.com.nexaweb.server=WARN
log4j.logger.com.opensymphony.oscache=ERROR
```

21.3 Setting Warning State

To set the Oracle Identity Manager server warning state:

1. Set the re-delivery limit on all OIM JMS queues to 1. To do so:
 - a. Login to the WebLogic Administration Console as the administrative user.
 - b. Click **JMS Modules** on the Home page.
 - c. Click **OIMJMSModule**.
 - d. Click **Lock & Edit**.

- e. For each of the queues, click the queue, and then click the **Delivery Failure** tab. Change the Redelivery Limit value from -1 to 1, and then click **Save**.
 - f. Make sure you have performed steps 1.d and 1.e for all the queues under OIMJMSModule.
 - g. Release the configuration and restart Oracle Identity Manager.
This re-delivery is not applicable for existing messages. When the server is restarted, wait for all the good messages to be processed. After that, all the bad messages must be purged.
2. To purge all bad messages:
 - a. Login to the WebLogic Administration Console as the administrative user.
 - b. Click **JMS Servers** on the home page.
 - c. Navigate to **OIMJMSServer, Monitoring, Active Destinations**.
 - d. Select the queues that contain messages. Click **Consumption, Pause**.
 - e. Delete the messages, as described in the following URL:
http://docs.oracle.com/cd/E12840_01/wls/docs103/ConsoleHelp/taskhelp/jms_modules/queues/ManageQueues.html
 - f. After messages are deleted, resume the consumption that has been paused in step 2.d.
 3. Restart Oracle Identity Manager.

Managing Asynchronous Execution

This chapter describes the AsyncService provided by the Oracle Identity and Access Management (IAM) platform and contains the following topics:

- [Section 22.1, "Overview of AsyncService"](#)
- [Section 22.2, "Async Routing and Configuration"](#)
- [Section 22.3, "Troubleshooting Failed Async Tasks"](#)
- [Section 22.4, "Working with the Diagnostic Dashboard UI"](#)

22.1 Overview of AsyncService

The AsyncService is one of the services provided by the IAM platform to run tasks asynchronously. Tasks are executed asynchronously to improve performance and throughput.

Some Identity Management operations take a long time to complete. So, it makes sense to split these operations into two parts, a short synchronous interaction followed by a long asynchronous process. The user is provided a response at the end of the synchronous interaction, and the remaining operation is performed asynchronously.

The AsyncService allows the Oracle Identity Manager component to submit tasks for asynchronous execution. The caller then performs other tasks. It is the responsibility of the AsyncService to execute this task whenever the computing resources are available.

22.2 Async Routing and Configuration

The AsyncService uses a configuration file, *async-messaging.xml*, to route and configure Async tasks. This configuration file is stored in the MetaData Store (MDS) schema in Oracle Identity Manager database. The MDS path of the file is `/file/async-messaging.xml`.

[Example 22–1](#) shows a snippet of the configuration file.

Example 22–1 Sample Configuration File

```
<tns:async-config>
<task-config>
<class>oracle.iam.reconciliation.impl.ActionTask</class>
<destination>queue/oimReconQueue</destination>
</task-config>
<task-config>
<class>com.thortech.xl.schedule.jms.messageType.AttestationTaskMessage</class>
```

```

<destination>queue/oimAttestationQueue</destination>
<priority>NORMAL</priority>
<maxRetries>2</maxRetries>
</task-config>
<task-config>
<class>com.thortech.xl.schedule.jms.messageType.AttestationRequestMessage</class>
<destination>queue/oimAttestationQueue</destination>
<priority>HIGH</priority>
</task-config>
<default-config>
<destination>queue/oimDefaultQueue</destination>
<maxRetries>3</maxRetries>
</default-config>
</tns:async-config>

```

To modify the configuration file, import it from MDS, make changes in the file, and then export the modified file to MDS. For more information about importing and exporting MDS files, see "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

22.2.1 Configuration Parameters

The System Administrators can configure the following parameters in the configuration file for Async tasks:

- **Destination:** You can assign high-volume tasks to their own dedicated queues. For instance, in [Example 22-1](#), all the Async tasks are assigned to the same destination queue `attestationQueue`. You can decide where to send each message by creating separate destination queues for each Async task.

Note: You must ensure that the queue exists in the Application Server before assigning a task to it. For information about creating queues, see *Oracle Fusion Middleware Configuring and Managing JMS for Oracle WebLogic Server*.

- **Priority:** You can set a priority when multiple types of Async tasks are assigned to the same destination queue. Its value can be one of the following:
 - NORMAL
 - HIGH
 - LOW
- **Max Retries:** Async task execution error recovery is handled in two ways, automated and manual. The automated retry mechanism uses a scheduled task to retry all failed tasks at specific intervals. Max Retries parameter allows the System Administrator to specify the maximum number of times a task can be retried in the event of an execution failure. See "[Troubleshooting Failed Async Tasks](#)" on page 22-2 for detailed information about error handling and recovery mechanisms.

22.3 Troubleshooting Failed Async Tasks

Errors may occur during execution of tasks or messages. The Async task execution error recovery is a combination of automated retries and manual intervention. If a task encounters an error during task execution, then it is added to a `FailedTasks` table and the System Administrator is notified. See "[Automated Retry Error Handling](#)"

[Mechanism](#)" on page 22-3 and "[Manual Retry Error Handling Mechanism](#)" on page 22-3 for detailed information about error handling mechanisms.

22.3.1 Automated Retry Error Handling Mechanism

A scheduled task is provided to automate retries of failed tasks at periodic intervals. The maximum number of times a task is retried by the scheduled task can be configured by using the `max-retries` property of the async task, as shown in [Example 22-2](#).

Example 22-2 Configuring Max Retries

```
<async-task>
  <class>oracle.iam.reconciliation.impl.ActionTask</class>
  <destination>reconQueue</destination>
  <max-retries>2</max-retries>
</async-task>
```

22.3.2 Manual Retry Error Handling Mechanism

The System Administrator can use the Oracle Identity Manager Diagnostic Dashboard User Interface (UI) to view the failed tasks and retry a task after taking the appropriate remedial action. See "[Working with the Diagnostic Dashboard UI](#)" on page 22-3 for more information on Oracle Identity Manager Diagnostic Dashboard UI.

22.4 Working with the Diagnostic Dashboard UI

The Diagnostic Dashboard provides a UI for the System Administrator to view and retry failed Async tasks. This section contains the following topics:

- [Starting the Diagnostic Dashboard UI](#)
- [Viewing Failed Async Tasks](#)
- [Retrying Failed Async Tasks](#)
- [Resubmitting Failed Async Tasks](#)
- [Purging Failed Async Tasks](#)

See Also: [Chapter 25, "Working with the Diagnostic Dashboard"](#) for information about installing and enabling the Diagnostic Dashboard

22.4.1 Starting the Diagnostic Dashboard UI

To start the Diagnostic Dashboard UI:

1. Access the Diagnostic Dashboard home page by using the following URL:
`http://host:port/XIMDD`
2. Click the **Manage Failed Tasks** link on the left menu pane.
3. Enter the user name and password. The Manage Failed Tasks page is displayed.

Note: You need System Administrator privileges to access the Diagnostic Dashboard UI.

22.4.2 Viewing Failed Async Tasks

The System Administrator can view the details of each failed task, for instance the cause for the task to fail and the remedial action to be undertaken.

The user can view the details of the failed tasks by either providing the filter criteria or by clicking the **Search** button.

22.4.2.1 To view failed async tasks

1. Log in to the Diagnostic Dashboard main page. See "[Starting the Diagnostic Dashboard UI](#)" on page 22-3 for more information.
2. Perform one of the following to view a list of failed tasks.
 - Click **Search** to view a list of all the failed tasks.
 - Search for the failed task based on the following filter criteria.
 - **Task Name:** Type the name of the failed task.
 - **Category:** Type the category of the failed task.
 - **Between:** Specify the date range.
 - Select the **Exclude if retries are remaining** option if you do not want to view the tasks for which automated retries are still pending.

Click **Search** after providing the filter criteria. The list of failed async tasks are displayed, as shown in [Figure 22-1](#):

Figure 22-1 Failed Async Tasks

Task Name

Category

Between And

Exclude if retries are remaining

Results

Identifier	Task Name	Category	Last Execution Time	Action
222	oracle.iam.test.async.SampleTask	Category2	Tue Dec 02 02:36:04 PST 2008	Retry

3. Click the Identifier link to view detailed information about the failed task. In this scenario, click [222](#). The following information is displayed:
 - Task Name
 - Instance ID
 - Category
 - Last Execution Time
 - Cause
 - Action
 - Stack Trace

22.4.3 Retrying Failed Async Tasks

The System Administrator can retry a specific failed task directly from the Diagnostic Dashboard UI and then view the results of the retry.

22.4.3.1 To retry failed Async task

1. Search for the failed task that you want to retry. See "[To view failed async tasks](#)" on page 22-4 for more information.
2. Click the **Retry** link. The retry status for the task is displayed. The following details are provided.
 - Retry Status
 - Task Summary
 - Stack Trace
 - Cause
 - Resolution

22.4.4 Resubmitting Failed Async Tasks

All the failed tasks are resubmitted to the Async queue. These are later executed asynchronously.

To resubmit failed tasks, click **ResubmitAll**.

22.4.5 Purging Failed Async Tasks

There are situations when there are numerous failed Async tasks. The System Administrator might feel that there is no use retrying these tasks. In such a scenario, the failed tasks can be purged. The action purge removes all the failed Async tasks from the database. In other words, there no more tasks to retry.

22.4.5.1 To purge failed Async tasks

1. Search for the failed task that you want to retry. See "[To view failed async tasks](#)" on page 22-4 for more information.
2. Click **PurgeAll**.

Using Enterprise Manager for Managing Oracle Identity Manager Configuration

Oracle Identity Manager stores the configuration files in MDS. Most of the configurations are exposed as MBeans. Therefore, you can control the configuration values by using Enterprise Manager. In some instances, might have to export the complete files to file system, make the necessary changes, and then import the files back into the repository, as described in the following sections:

- [Using MBeans for Configuration Changes](#)
- [Exporting and Importing Configuration Files](#)

23.1 Using MBeans for Configuration Changes

To change configuration settings by using Mbeans:

1. When the administrative server and at least one Oracle Identity Manager managed server is running, login to Oracle Enterprise Manager Fusion Middleware Control by using the URL in the following format:

`http://ADMINISTRATION_SERVER:PORT/em`

2. Navigate to Identity and Access, **oim**. Right-click and navigate to **System MBean Browser**.
3. Under Application Defined MBeans, navigate to **oracle.iam, Application:oim, XMLConfig, Config**.

All the configuration files are in this location.

23.2 Exporting and Importing Configuration Files

To export or import configuration files:

1. When the administrative server and at least one Oracle Identity Manager managed server is running, login to Oracle Enterprise Manager Fusion Middleware Control by using the URL in the following format:

`http://ADMINISTRATION_SERVER:PORT/em`

2. Navigate to Identity and Access, **oim**. Right-click and navigate to **System MBean Browser**.
3. Under Application Defined MBeans, navigate to **oracle.mds.lcm, Server:oim_server1, Application:oim, MDSAppRuntime**.

4. To export the configuration files:
 - a. Click the **Operations** tab, and then click **exportMetaData**.
 - b. In the toLocation field, enter /tmp or the name of another directory.
 - c. Select createSubDir as **false**.
 - d. In the docs field, enter the complete file location as the Element.
 - e. Also select **false** for excludeAllCust, excludeBaseDocs, and excludeExtendedMetadata. Then, click **Invoke**.

This exports the file specified in the docs field to the directory specified in the toLocation field.
5. To import the configuration files:
 - a. Click **importMetaData**.
 - b. In the fromLocation field, enter /tmp or the name of the directory in which you have the configuration files.
 - c. Select createSubDir as **false**.
 - d. In the docs field, enter the complete file location as the Element. For example, /db/oim-config.xml.
 - e. Also select **false** for excludeAllCust, excludeBaseDocs, and excludeExtendedMetadata. Then, click **Invoke**.

This imports the file specified in the docs field to MDS in the toLocation field.

Setting the Language for Users

In Oracle Identity Manager 11g Release 2 (11.1.2.1.0), the language preference of the user for the UI is not set according to the locale specified by the user in the Preferences section of the Self Service. However, this locale preference is used to determine the language of notification messages.

The logic to determine the UI locale gives precedence to other ways a locale can be specified, such as through Fusion Apps or Oracle Access Manager (OAM) login page, before using the browser locale.

The `oracle.fusion.appsMode` system property is used internally and is automatically set when the environment is with fusion Apps. Based on this property's value, the appropriate attribute within a cookie called `ORA_FUSION_PREFS` (set and used internally), is used to determine the locale.

To determine the UI locale for a user, the following logic is used internally:

1. Check if the `oracle.fusion.appsMode` system property is available.
2. If the `oracle.fusion.appsMode` system property is not available or the value is set to false, then `preferredLanguage` attribute is checked. The value of this attribute is the UI locale for the user. The `preferredLanguage` attribute is checked inside the `ORA_FUSION_PREFS` cookie.
3. If the `oracle.fusion.appsMode` system property is available and the value is set to true, then the `locale` attribute is checked inside the `ORA_FUSION_PREFS` cookie. The value of this attribute is the UI locale for the user.

Note: The `ORA_FUSION_PREFS` cookie is internal to Oracle Identity Manager.

4. If the `ORA_FUSION_PREFS` cookie is not present, then check the browser language setting. The UI locale for the user is same as the browser language setting.

Note: If none of the above can provide a locale value, then check the server setting.

Working with the Diagnostic Dashboard

This chapter describes the Diagnostic Dashboard utility shipped with Oracle Identity Manager and contains the following topics:

- [Section 25.1, "Overview of the Diagnostic Dashboard"](#)
- [Section 25.2, "Installing the Diagnostic Dashboard"](#)
- [Section 25.3, "Starting the Diagnostic Dashboard"](#)
- [Section 25.4, "Using the Diagnostic Dashboard"](#)
- [Section 25.5, "Running Tests By Using the Diagnostic Dashboard"](#)

25.1 Overview of the Diagnostic Dashboard

The Oracle Identity Manager Diagnostic Dashboard is a standalone Web application that runs on your application server. You use this diagnostic tool to validate preinstallation and postinstallation requirements for Oracle Identity Manager.

You must have the appropriate system administrator permissions for your Application Server and Oracle Identity Manager environments to use this tool. You need DBA-level permissions to execute some database-related tests.

Note: The Diagnostic Dashboard and Oracle Identity Manager must be installed on the same application server.

25.2 Installing the Diagnostic Dashboard

The Diagnostic Dashboard utility is distributed on the installation CD-ROM with the Oracle Identity Manager Installer. It is available as a EAR file in the `Diagnostic Dashboard` directory on the CD-ROM.

25.2.1 Installing the Diagnostic Dashboard on Oracle WebLogic Server

This section discusses the steps you need to perform to install the Diagnostic Dashboard on Oracle WebLogic Server.

To install the Diagnostic Dashboard on Oracle WebLogic Server:

1. Log in to Oracle WebLogic Administration Console.
2. In the left navigation pane, click **Deployments**. It lists all the applications deployed on the server.

3. Click **Install**.
4. Navigate to the location for deploying the EAR file. Typically, the EAR file is located in the following directory:


```
OIM_ORACLE_HOME/server/webapp/optional/
```
5. Select **XIMDD.ear** from the **Current Location** panel.
6. Click **Next** on the **Choose targeting style** page.
7. Select **OimServer** (Oracle Identity Manager Server) from the **Available targets for XIMDD** panel, and click **Next**.
8. Click **Finish**. The following message appears:

All changes have been activated. No restarts are necessary.
The deployment has been successfully installed.

You can access the Diagnostic Dashboard from the following location:

```
http://OIM_server_host_ip:port/XIMDD
```

25.3 Starting the Diagnostic Dashboard

After the Diagnostic Dashboard is deployed, you can access it by using a URL of the following format:

```
http://OIM_HOST:OIM_PORT/XIMDD
```

Log into Diagnostic Dashboard with administrator privileges. Click the **Diagnostic Dashboard** link on the left menu pane to display the Diagnostic Dashboard main page.

The Diagnostic Dashboard utility indicates on which application server the tool is deployed.

25.4 Using the Diagnostic Dashboard

The Diagnostic Dashboard main page includes the sections listed in the following table:

Section	Description
Application Server	Displays the name of the application server
Oracle Identity Manager Installation	Displays installation details such as product version, build number, host, and location of the product
Test Details	Displays the test name and its description
Test Parameters	Displays the parameters required for testing

To run a test:

1. Select the test by selecting the option on the Diagnostic Dashboard main page.
2. Enter the required parameters.
3. Click **Verify** to see the result.

The Diagnostic Dashboard Test Result page is displayed with the status information listed in the following table.

Test Result	Description
Result Summary	Shows all the selected tests with icons (pass or fail) indicating the result. The test name is a Web link that allows the user to jump to the result details directly.
Test Name	Displays the name of the test
Description	Displays the description of the test
Input Parameters	Displays the parameters of the test
Result	Displays the outcome of the test
Details	Displays details about the outcome of the test

4. Click **Diagnostic Dashboard** on the left menu pane or **Return to Diagnostic Dashboard** to return to the previous test page.

25.5 Running Tests By Using the Diagnostic Dashboard

The following tests are available for different application servers.

- [Oracle Database Prerequisites Check](#)
- [Database Connectivity Check](#)
- [Account Lock Status](#)
- [Data Encryption Key Verification](#)
- [Scheduler Service Status](#)
- [Remote Manager Status](#)
- [JMS Messaging Verification](#)
- [Target System SSL Trust Verification](#)
- [Java VM System Properties Report](#)
- [Oracle Identity Manager Libraries and Extensions Version Report](#)
- [Oracle Identity Manager Libraries and Extensions Manifest Report](#)
- [Test Basic Connectivity](#)
- [Test Provisioning](#)
- [Test Reconciliation](#)
- [SOA-Oracle Identity Manager Configuration Check](#)
- [Request Diagnostic Information](#)
- [Orchestration Status](#)
- [Retry Failed Orchestration](#)
- [SPML Web Service](#)
- [Test OWSM Setup](#)
- [Test SPML to Oracle Identity Manager Request Invocation](#)
- [SPML Attributes to Oracle Identity Manager Attributes](#)
- [Username Test](#)
- [Diagnose Creation of User and Role in Oracle Identity Manager and LDAP](#)

- [Diagnose LDAP Reserve Container](#)
- [Validate Recon Profile](#)
- [Notification Configuration Test](#)
- [Diagnose LDAP Connection](#)
- [Diagnose OIM Callback Webservice](#)

25.5.1 Oracle Database Prerequisites Check

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
Database Server	Enter the location of the database server.
Port	Enter the port number.
Database Name	Enter the database name (SID).
Oracle Identity Manager Database User Name	Enter the Oracle Identity Manager database user name.
System User Name	Enter the system user name.
System User Password	Enter system user password.

Description: Checks if the specified Oracle Database instance meets the prerequisites for Oracle Identity Manager installation. This test requires SYSTEM permissions.

Result: It displays the following information:

- Necessary permissions for user
- XA support enabled
- JVM enabled
- Oracle version Information

25.5.2 Database Connectivity Check

Prerequisite: None

Description: Run this test to verify whether or not Oracle Identity Manager is able to connect to the database. This test verifies the direct database connection and the J2EE data sources (XA).

Result: It displays the following information:

- Direct database connectivity
- XA execution

25.5.3 Account Lock Status

Prerequisite: The following is the prerequisite for verifying this test:

Prerequisite	Description
User Login	Enter the user name.

Description: Oracle Identity Manager locks an account when there are successive multiple invalid login attempts. This test checks whether or not a specified account is locked.

Result: Checks for locked or unlocked accounts in the database.

25.5.4 Data Encryption Key Verification

Prerequisite: None

Description: The data encryption key in an Oracle Identity Manager installation should be the same as the one used to encrypt the data in the Oracle Identity Manager database. This may not be the case when an Oracle Identity Manager installation is pointed to a database schema created for a different Oracle Identity Manager installation. This can also happen when a database dump from one Oracle Identity Manager installation is imported for a different Oracle Identity Manager installation without copying the corresponding key.

Result: Checks if the database key is present in the Oracle Identity Manager configuration directory.

25.5.5 Scheduler Service Status

Prerequisite: None

Description: Checks the status of the Oracle Identity Manager Scheduler Service running on the server.

Result: Displays the status of the scheduler service.

25.5.6 Remote Manager Status

Prerequisite: None

Description: Reports the status of the Remote Managers that this Oracle Identity Manager installation is set to work with.

Result: Displays the status of the Remote Manager.

25.5.7 JMS Messaging Verification

Prerequisite: None

Description: The purpose of this test is to verify that Oracle Identity Manager will be able to submit a JMS message and process it.

Result: Displays if Oracle Identity Manager is able to submit and process a JMS message.

25.5.8 Target System SSL Trust Verification

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
Target System	Enter the host name.
Port	Enter the port number.
Certificate Store Location	Enter the location for storage.
Certificate Store Password	Enter the password for storage.

Description: Oracle Identity Manager must be set up to trust the target system certificates if the connectivity is over Secure Sockets Layer (SSL). Enter the host name and the port where a target system is listening for SSL connections.

Result: It displays the following information:

- Valid and invalid host and port address
- Trusted certificates

25.5.9 Java VM System Properties Report

Prerequisite: None

Description: Displays all the Java VM system properties.

Result: Displays all the Java VM system properties.

25.5.10 Oracle Identity Manager Libraries and Extensions Version Report

Prerequisite: None

Description: Reports all the versions of the Oracle Identity Manager libraries and extensions.

Result: Displays the versions of the Oracle Identity Manager libraries and extensions.

25.5.11 Oracle Identity Manager Libraries and Extensions Manifest Report

Prerequisite: None

Description: Reports the manifest information of the Oracle Identity Manager libraries and extensions.

Result: Displays the manifest information of the Oracle Identity Manager libraries and extensions.

25.5.12 Test Basic Connectivity

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
IT Resource Type Name	Enter the IT resource type.
IT Resource Instance Name	Enter the IT resource name.

Description: Tests the connection to the target system by using the IT resource for the target system.

Note: If the specified IT resource type was created when you deployed a predefined connector, then see the Oracle Identity Manager Connector Pack release notes and documentation to determine whether or not this test can be applied for the release of the connector that you deployed.

Result: Displays the results of the connectivity test. If the test fails, then the cause of the error is also displayed.

25.5.13 Test Provisioning

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
IT Resource Type Name	Enter the IT resource type.
IT Resource Instance Name	Enter the IT resource name.

Description: Performs a basic Create User operation on the target system.

Note: If the specified IT resource type was created when you deployed a predefined connector, then see the Oracle Identity Manager Connector Pack release notes and documentation to determine whether or not this test can be applied for the release of the connector that you deployed.

Result: Displays the results of the provisioning test. Test data created on the target system during the test is deleted at the end of the test.

25.5.14 Test Reconciliation

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
IT Resource Type Name	Enter the IT resource type.
IT Resource Instance Name	Enter the IT resource name.

Description: Performs a basic reconciliation operation on the target system.

Note: If the specified IT resource type was created when you deployed a predefined connector, then see the Oracle Identity Manager Connector Pack release notes and documentation to determine whether or not this test can be applied for the release of the connector that you deployed.

Result: Displays the results of the reconciliation test. Test data reconciled into Oracle Identity Manager during the test is deleted at the end of the test.

25.5.15 SOA-Oracle Identity Manager Configuration Check

Prerequisite: None

Description: Checks whether the details provided for SOA-wiring are valid or not.

Result: Displays the status for the following tests:

1. Validation for SOA connection with Oracle Identity Manager and authentication of user in SOA
2. Authentication and search of Oracle Identity Manager DB user

25.5.16 Request Diagnostic Information

Prerequisite: The following is the prerequisite for running this test:

Prerequisite	Description
Request ID	Enter the ID of the request for which diagnostic information is required

Description: Provides the orchestration ID and the composite details for the given request ID.

Result: Displays the following information:

1. Orchestration process ID associated with the given request ID.
2. Composite details of the request along with details of approval and process task.

25.5.17 Orchestration Status

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
Process Id	Enter the Id of the orchestration process.

Description: Provides the status of the orchestration process in the Oracle Identity Manager Kernel. It also provides details and status about all the event handlers involved in that process.

Result: Displays the status of the orchestration process as Failed, Completed, or Active.

Figure 25–1 displays the status of the orchestration process, including the events completed and still pending.

Figure 25–1 Sample Output for Orchestration Status Test

Test Name: Orchestration Status

Description: Get the status of the orchestration process, including the events completed and still pending.

Input Parameters:

Process Id: 3

Result: Passed

Details:

Process Details							
Id	Stage	Status	ChangeType	ParentId	Child Count	Retry Count	
3	PREPROCESS	ACTIVE	null	0	0	0	

List Of Events With ProcessId: 3

Id	Name	Stage	Status	Sync	Result
26	CreateUser/ValidationHandler	VALIDATE	COMPLETED	false	null
17	UserPassword/ValidationHandler	VALIDATE	COMPLETED	false	null
22	CreateUser/PreProcessHandler	PREPROCESS	COMPLETED	true	null
8	PostSubmissionDataActions	PREPROCESS	COMPLETED	true	null
15	GetCurrentUser	PREPROCESS	COMPLETED	true	null
21	UpdateUserPasswordFields	PREPROCESS	COMPLETED	true	null
7	Approval/Initiation	PREPROCESS	PENDING	false	null
14	PostApprovalActions	PREPROCESS	NOTSTARTED	false	null
20	CustomPreProcessHandler	PREPROCESS	NOTSTARTED	true	null
6	CreateUser/ActionHandler	ACTION	NOTSTARTED	true	null
13	User/AuditHandler	AUDIT	NOTSTARTED	true	null
19	CreateUser/PostProcessHandler	POSTPROCESS	NOTSTARTED	true	null
27	SelfService/NotificationHandler	POSTPROCESS	NOTSTARTED	true	null
12	Password/NotificationHandler	POSTPROCESS	NOTSTARTED	true	null
18	Password/History/PostProcessHandler	POSTPROCESS	NOTSTARTED	true	null
24	PostProcessing/Initiation	POSTPROCESS	NOTSTARTED	true	null
10	Role/Change/Calculator	POSTPROCESS	NOTSTARTED	true	null
23	Policy/Evaluator	POSTPROCESS	NOTSTARTED	true	null
9	CustomPostProcessHandler	POSTPROCESS	NOTSTARTED	true	null
16	SelfService/PostHandler	POSTPROCESS	NOTSTARTED	true	null
25	Request/Completed	POSTPROCESS	NOTSTARTED	true	null
11	CreateUser/FinalizationHandler	FINALIZATION	NOTSTARTED	false	null

[Back To Top](#)

25.5.18 Retry Failed Orchestration

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
Process Id	Enter the Id of the orchestration process.

Description: Obtains the response that indicates how to handle the failure for the given orchestration process.

Result: Displays the orchestration process in failed state and continues to retry based on the response.

25.5.19 SPML Web Service

Prerequisite: None

Description: Verifies that SPML WSDL is accessible and the Web service is up and running.

Result: Displays the contents of SPML WSDL file.

25.5.20 Test OWSM Setup

Prerequisite: The following are the prerequisites for running this test:

Prerequisites	Description
SPML User Name	Enter user name to be used to run SPML request.
SPML User Password	Enter user password.

Description: Verifies OWSM setup by submitting a request with OWSM header information. This also ensures a valid response is returned by submitting a request with OWSM header set.

Result: Displays the targets supported by the SPML web-service.

25.5.21 Test SPML to Oracle Identity Manager Request Invocation

Prerequisite: The following are the prerequisites for running this test:

Prerequisites	Description
SPML User Name	Enter user name to be used to run SPML request.
SPML User Password	Enter user password.

Description: SPML WS to Oracle Identity Manager is a signature-based login, This test ensures if this is working, by simulating a Oracle Identity Manager request.

Result: Displays whether signature-based login is working fine.

25.5.22 SPML Attributes to Oracle Identity Manager Attributes

Prerequisite: None

Description: Lists all the mapping of SPML attributes to Oracle Identity Manager attributes which helps the administrator to check if the set up is correct.

Result: Displays a table showing the SPML to Oracle Identity Manager attributes mappings:

SPML Attribute Name	Oracle Identity Manager Attribute Name
Number Format	Number Format
localityName	Locality Name
countryName	Country
manager	User Manager
facsimileTelephoneNumber	Fax
generationQualifier	Generation Qualifier
street	Street
state	State
surname	Last Name
Embedded Help	Embedded Help
Territory	FA Territory
organizationUnit	LDAP Organization Unit
givenName	First Name

25.5.23 Username Test

Prerequisite: None

Description: Lists the existing username generation policy defined in Oracle Identity Manager

Result: Displays the policy name.

25.5.24 Diagnose Creation of User and Role in Oracle Identity Manager and LDAP

Prerequisite: The following are the prerequisites for running this test:

Prerequisites	Description
SPML User Name	Enter user name to be used to run SPML request.
SPML User Password	Enter user password.

Description: Verifies the user creation and role creation are working fine in LDAP and Oracle Identity Manager individually.

Result: Displays the status specifying whether user and role creation was successful in Oracle Identity Manager and LDAP.

25.5.25 Diagnose LDAP Reserve Container

Prerequisite: None

Description: Oracle Identity Manager configuration file has the tree structure of reserve container. This test validates that the reserve container was created during the setup.

Result: Displays whether reserve container is created properly.

25.5.26 Validate Recon Profile

Prerequisite: Profile Name

Description: Validates the reconciliation profile XML file.

Result: Displays the profile XML data along with validation status and validation exception, if validation fails.

25.5.27 Notification Configuration Test

Prerequisite: Ensure that the user ID provided is valid in Oracle Identity Manager, and the user has a valid email ID.

Description: Tests the Oracle Identity Manager Notification Service running on this server.

Result: Displays the status of each notification provider, such as UMSEmailServiceProvide, SOAEmailServiceProvider, and EmailServiceProvider.

25.5.28 Diagnose LDAP Connection

Prerequisite: None

Description: Verifies if Oracle Identity Manager is able to connect to the LDAP server.

Result: Displays whether connection to LDAP is working properly.

25.5.29 Diagnose OIM Callback Webservice

Prerequisite: None

Description: Verifies that Oracle Identity Manager Callback WSDL is accessible.

Result: Displays the contents of Oracle Identity Manager Callback WSDL file.

Enabling Diagnostics

The IdM Diagnostic tool is a standalone diagnostic tool that is intended to accomplish the following:

- Identify problems in Identity Management deployments
- Suggest fixes to resolve application problems
- Run diagnostic tests and collect detailed diagnostic reports
- Assist Oracle Support and development teams conduct analysis and troubleshoot application problems

This chapter provides the details on enabling diagnostics in Oracle Identity Manager for dynamic configuration-related test cases. Dynamic configuration relates to changes made to the configurations at run time and are not easily detected through the static configuration diagnostic tests when there is an issue. In addition, the dynamic issues are encountered while Oracle Identity Manager is running.

Enabling diagnostics in Oracle Identity Manager and test cases related to dynamic configuration are described in the following sections:

- [Enabling Diagnostics in Oracle Identity Manager](#)
- [Troubleshooting Dynamic Configuration-Related Problems](#)

26.1 Enabling Diagnostics in Oracle Identity Manager

You can enable diagnostics in Oracle Identity Manager at run time. To do so:

1. Log in to Oracle Identity System Administration, and go to System Configuration.
2. Create a system property with the following details:
 - **Property Name:** OIM Diagnostic Enabled
 - **Keyword:** OIM.DiagnosticEnabled
 - **Value:** True

You must set the OIM Diagnostic Enabled system property to enable Oracle Identity Manager diagnostics for debugging purpose. To enable diagnostics, set the value of this property to TRUE. If the value is set to FALSE or the property is missing, then diagnostics is disabled. See "[Creating and Managing System Properties](#)" on page 16-22 for information about creating system properties.

3. Add a logger for the diagnostic-related logging. To do so:

- a. In the `DOMAIN_NAME/config/fmwconfig/servers/SERVER_NAME/logging.xml` file for the application server, add a new log handler, as shown:

Note: Here, `DOMAIN_NAME` and `SERVER_NAME` are the domain name and server name respectively specified during the installation of Oracle Identity Manager.

```
<log_handler name='ldap-diagnostic-handler'
class='oracle.core.ojdl.logging.ODLHandlerFactory' level='TRACE:16'>
<property name='logreader:' value='off' />
<property name='path'
value='${domain.home}/servers/${weblogic.Name}/logs/ldapsync-diagnostic.log' />
<property name='format' value='ODL-Text' />
<property name='useThreadName' value='false' />
<property name='locale' value='en' />
<property name='maxFileSize' value='5242880' />
<property name='maxLogSize' value='52428800' />
<property name='encoding' value='UTF-8' />
</log_handler>
```

Note:

- You can change the value of the path property to a different location.
 - See ["Log Handler and Logger Configuration"](#) on page 21-3 and ["Configuring Log Handlers"](#) on page 21-4 for detailed information about configuring loggers.
-

- b. Add a new logger as shown:

Note: Make sure that the value of the handler name attribute is same as in step 3a.

```
<logger name='oracle.iam.ldapsync.diagnostic.logger' level='TRACE:16'
useParentHandlers='false'>
<handler name="ldap-diagnostic-handler" />
</logger>
```

- c. Save the logging.xml file.

Note: Restarting Oracle Identity Manager is not required for the new logger to take effect.

26.2 Troubleshooting Dynamic Configuration-Related Problems

This section describes the following dynamic configuration-related problems and troubleshooting steps:

- [Roles in Oracle Identity Manager and Identity Store in Inconsistent State](#)

- [Postenablement of the oamEnabled Flag Causes Issues](#)
- [Run-time Evaluation of LDAP Containers Defined in LDAPContainerRules.xml](#)

26.2.1 Roles in Oracle Identity Manager and Identity Store in Inconsistent State

Roles in Oracle Identity Manager database and the identity store, such as Oracle Internet Directory (OID), Microsoft Active Directory (AD), and Oracle Directory Server Enterprise Edition (ODSSE), can be in inconsistent state causing unexpected behavior.

As part of the provisioning process, some data, such as roles, are populated into the backend directory server, such as OID. These roles are reconciled into Oracle Identity Manager via a scheduled job so that Oracle Identity Manager and OID are in sync with respect to the roles. There can be various sets of operations that lead Oracle Identity Manager to be in an inconsistent state, as described in [Table 26-1](#).

Table 26–1 Troubleshooting Inconsistent Roles

Problem	Solution
<p>The following operations are performed:</p> <ol style="list-style-type: none"> 1. Roles are seeded into backend identity store as part of running provisioning, bulk load utility, or LDAP Data Interchange Format (LDIF) files. 2. The scheduled task is run and the roles are reconciled into Oracle Identity Manager based on the changelog entries. The roles in Oracle Identity Manager and backend identity store are in sync. 3. In Oracle Identity Manager, some of the roles are assigned to some users. This creates a referential integrity between users and the roles. 4. The seeded roles are deleted from the backend identity store either manually via Oracle Directory Services Manager (ODSM), LDAP browser, or LDIF file. 5. At the next run of the scheduled task, the delete reconciliation event is triggered and the corresponding roles must be deleted from Oracle Identity Manager. 6. The delete reconciliation event fails in Oracle Identity Manager because the roles have dependency, and therefore, are not deleted from Oracle Identity Manager. 7. New roles are seeded in the backend. The new roles are created under a different container. Therefore, the roles have a different DN and GUID. 8. Assuming that the rules specified in the LDAPContainerRules are in place, the new roles with different DNs and GUIDs are reconciled into Oracle Identity Manager under different namespace. As a result, there are two roles with same display names, but under different namespace and different GUIDs. Therefore, Oracle Identity Manager and backend identity store are in inconsistent state. 9. When an attempt is made to assign a role that is not present in the backend identity store to a user, an error occurs stating that the role does not exist in the backend identity store. 	<p>To fix the issue, perform the following steps:</p> <ol style="list-style-type: none"> 1. Identify the root cause of the error, which might involve running some subtests. 2. Analyze the data in the diagnostic logs. 3. Perform any suggested action in the diagnostic logs. 4. Identify the inconsistent data for the current operation and all the related inconsistent data if there are more roles that are not in sync.
<p>The following operations are performed:</p> <ol style="list-style-type: none"> 1. Roles are seeded into backend identity store as part of running provisioning, bulk load utility, or LDIF files. 2. The scheduled task is run and the roles are reconciled into Oracle Identity Manager based on the changelog entries. The roles in Oracle Identity Manager and backend identity store are in sync. 3. The backend identity store administrator changes the remote base in the Oracle Virtual Directory (OVD) configuration to a different container. Because of the change in the OVD configuration, there is a possibility that another role with same name but a different DN and GUID exists under the new container. 4. LDAPContainerRules is also modified to add a new namespace for the new role DNs. 5. After reconciliation, roles with the same name but different DNs or GUIDs are brought into Oracle Identity Manager. This leads to an inconsistent state in Oracle Identity Manager because the original roles cannot be mapped back into the identity store due to remote base change. 	<p>To fix the issue, perform the following steps:</p> <ol style="list-style-type: none"> 1. Identify the root cause of the error, which might involve running some subtests. 2. Analyze the data in the diagnostic logs. 3. Perform any suggested action in the diagnostic logs. 4. Identify the inconsistent data for the current operation and all the related inconsistent data if there are more roles that are not in sync.

26.2.2 Postenablement of the oamEnabled Flag Causes Issues

When the oamEnabled flag in OVD configuration is set after user provisioning is done, the provisioned users do not get the reset password page.

After Oracle Identity Manager and Oracle Access Manager (OAM) is configured, the OVD adapters must be configured with the oamEnabled flag to true. The OVD adapters rely on this flag to set the appropriate Oblix attributes. Failure to do so causes the Password Reset page not being displayed as expected for the first time. This occurs because of the missing ObPasswordChangeFlag attribute in the provisioned user entry. This situation arises when the following steps are performed:

1. Users are provisioned to Oracle Identity Manager and also created in the backend identity store, such as OID, via LDAP synchronization.
2. A user tries to access a protected resource for the first time with the temporary password assigned.

The user is to be redirected to Oracle Identity Manager Reset Password page by OAM based on the oamEnabled flag. Because the flag is not set, the user is instead allowed access to the protected resource.

3. OVD administrator sets the oamEnabled flag for the OVD adapter to true.
4. A user tries to reset the password via the self service page. An error similar to the following is displayed:

```
LDAP: error code 65 - Failed to find orclpwdexpirationdate in mandatory or optional attribute list.
```

To troubleshoot this issue, perform the following steps:

1. Make sure that all the Oblix-related classes are loaded in the backend identity store.
2. Add the required objectclasses and attributes to the existing user entries.

26.2.3 Run-time Evaluation of LDAP Containers Defined in LDAPContainerRules.xml

When LDAP synchronization is enabled in Oracle Identity Manager, the LDAP container in which the entries (user and role) are created is determined based on the rules defined in LDAPContainerRules.xml. The following types of container evaluations are defined in LDAPContainerRules.xml:

See Also: "Configuring LDAP Container Rules" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about LDAP container rules

- **Static:** Static containers are predetermined and do not go through parameter substitution, such as:

```
"<container>cn=Groups,dc=us,dc=mydomain,dc=com</container>"
```

- **Dynamic:** Dynamic containers cannot be predetermined and are evaluated at runtime after the parameter substitution, such as:

```
<container>cn=FusionGroups,cn=$Role
Description$,dc=us,dc=mydomain,dc=com</container>
```

For dynamic containers, when the value of "\$Role Description" is substituted determines the container for entry creation. In addition, there can be one or more such rule elements defined with each having a different expression or container element. If

the parameter passed satisfies the expression for a given rule, then the corresponding container is evaluated at runtime after parameter value substitution. Therefore, it is not possible to determine a priority for the container DN. This often leads to difficulty in analyzing the issue when an entity creation (user/role) fails because of nonexistence of evaluated container value. The diagnostics when enabled, provides run-time container evaluation, and additionally lists the possible container values based on RDN for a given rule. For instance, consider the following rule defined in LDAPContainerRules.xml:

```
<rule>
<expression>Role Description=*</expression>
<container>cn=FusionGroups,cn=$Role
Description$,dc=us,dc=mydomain,dc=com</container>
<description>$Role Description$</description>
</rule>
```

Because the <expression> element contains "Role Description=*", the value of "cn=\$Role Description\$" in the <container> element is evaluated to a parameter passed as Role Description during role creation.

If a role being created has the Role Description as `Temporary Admin`, then it matches the "Role Description=*" expression, and the value of the container is "cn=FusionGroups,cn=Temporary Admin,dc=us,dc=mydomain,dc=com".

If the "cn=FusionGroups,cn=Temporary Admin,dc=us,dc=mydomain,dc=com" container does not exist in the backend directory server, for example OID, then the diagnostics logs this information in the configured log file. In addition, the diagnostics performs a search on RDN, which is "cn=FusionGroups", for all the possible LDAP containers in the configured backend directory server and logs it. This assists in inspecting the possible containers.

Handling Errors

You may encounter the following error message due to slow database connection:

```
<Error> <oracle.iam.oimdataproviders.impl>  
<BEA-000000> <java.sql.SQLException: Internal error: Cannot obtain  
XAConnection weblogic.common.resourcepool.ResourceDisabledException: Pool  
oimOperationsDB is Suspended, cannot allocate resources to applications..  
oracle.iam.platform.entitymgr.vo.ConnectivityException:
```

If you come across such error messages, perform the following steps:

1. Open the *DOMAIN_HOME*\bin\setSOADomainEnv.cmd file.
2. Uncomment the following lines:

```
EXTRA_JAVA_PROPERTIES="{EXTRA_JAVA_PROPERTIES}  
-Dweblogic.resourcepool.max_test_wait_secs=30"  
export EXTRA_JAVA_PROPERTIES
```
3. Save your changes and restart the Oracle Identity Manager managed Oracle WebLogic Server.

Part X

Additional Components

This part describes a number of additional features for Oracle Identity Manager administrators.

It contains the following chapters:

- [Chapter 28, "Installing and Configuring a Remote Manager"](#)
- [Chapter 29, "Using the Form Version Control Utility"](#)
- [Chapter 30, "Starting and Stopping Servers"](#)
- [Chapter 31, "Enabling Secure Cookies"](#)
- [Chapter 32, "Integrating with Other Oracle Components"](#)
- [Chapter 33, "Handling Lifecycle Management Changes"](#)
- [Chapter 34, "Managing Identity and Resource Information"](#)
- [Chapter 35, "Securing a Deployment"](#)

Installing and Configuring a Remote Manager

This chapter describes how to configure the remote manager in the following topics:

- [Overview of the Remote Manager Configuration](#)
- [Configuring the Remote Manager](#)
- [Stopping and Starting the Remote Manager](#)
- [Troubleshooting Remote Manager](#)

28.1 Overview of the Remote Manager Configuration

While performing provisioning or reconciliation actions, Oracle Identity Manager must communicate with the target to perform the business operations. To do so, Oracle Identity Manager uses the target APIs to directly communicate with the target during provisioning and reconciliation. However, Oracle Identity Manager cannot directly communicate with the target in some instances, such as:

- The target is behind a firewall, and the target communication port is not exposed.
- The target does not provide APIs that can be invoked over the network.
- The target APIs cannot be invoked over a secure connection.

In these instances, instead of directly communicating with the target system, Oracle Identity Manager must use an Oracle Identity Manager component that acts like a proxy. This component is known as remote manager.

The remote manager is used for:

- Invoking non-removable target APIs through Oracle Identity Manager
- Invoking target APIs that do not support SSL over secure channel

28.2 Configuring the Remote Manager

Remote manager configuration consists of the following steps:

1. Install the remote manager. See *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* for information about installing the remote manager.
2. Establish trust relationship with remote manager and Oracle Identity Manager. See "[Adding the Trust Relation](#)" on page 28-2 and "[Configuring the Remote Manager by Using Your Own Certificate](#)" on page 28-3 for details.

3. Test the remote manager. See "[Testing the Remote Manager Connection](#)" on page 28-5 for details.

This section contains the following topics:

- [Adding the Trust Relation](#)
- [Configuring the Remote Manager by Using Your Own Certificate](#)
- [Testing the Remote Manager Connection](#)
- [Updating the xlconfig.xml File to Change the Port for Remote Manager](#)

28.2.1 Adding the Trust Relation

The remote manager and Oracle Identity Manager communicate by using SSL. You must enable a trust relationship between Oracle Identity Manager and the remote manager.

Oracle Identity Manager must trust the remote manager certificate. To achieve this, you must import the remote manager certificate into the Oracle Identity Manager keystore and set it up as a trusted certificate.

If required, you can also enable client-side authentication in which the remote manager trusts the server certificate. For client-side authentication, import the certificate for Oracle Identity Manager into the remote manager keystore and set it up as a trusted certificate.

You might have to manually edit the configuration file (xlconfig.xml) associated with Oracle Identity Manager and the remote manager.

Perform the following steps to ensure that the trust relation between the application server and the remote manager is established through the certificate. The keytool utility is used to import/export the certificates.

1. Using a command prompt, navigate to the `$XLREMOTE_HOME` directory and use the keytool utility to list the certificate fingerprints.
2. Enter the following command:

```
$JAVA_HOME/jre/bin/keytool -list -keystore ./config/default-keystore.jks
```

Note: The Oracle Identity Manager keystore is called default-keystore.jks. In Oracle Identity Manager, it is located in the `$DOMAIN_HOME/config/fmwconfig/` directory.

For the remote manager, the keystore is located in the `$XLREMOTE_HOME/config/` directory. The keystore name is default-keystore.jks.

On running the keytool command shown in this step, you will be prompted to enter the default password for the keystore. When you enter the keystore password, the entries in the keystore along with their certificate fingerprints (MD5 hashes) are displayed, as follows:

```
Enter the default password for xellerate keystore: KEYSTORE_PASSWORD
Your keystore contains 1 entry
xell, Jan 7, 2005, keyEntry,
Certificate fingerprint (MD5):
B0:F2:33:C8:69:E4:25:A3:CB:59:E8:51:27:EE:5C:52
```

The certificate fingerprint is marked in bold. This is used to uniquely identify the certificate in the keystore.

3. To establish a trust relationship between Oracle Identity Manager and the remote manager:
 - a. Copy the remote manager certificate to the server computer. Export the remote manager certificate from `$XLREMOTE_HOME/remote_manager/config/default-keystore.jks`, store in the `rmcert.cer` file, and copy it to the server computer.

To export the certificate by using the `keytool` utility, use the following command:

```
$JAVA_HOME\jre\bin\keytool -export -alias xeltrusted -keystore
$XLREMOTE_HOME/remote_manager/config/default-keystore.jks -storepass
KEYSTORE_PASSWORD
```

The output is:

```
Certificate stored in file <rmcer.cer>
```

- b. Open a command prompt on the server computer.
 - c. To import the certificate by using the `keytool` utility, use the following command:

```
$JAVA_HOME\jre\bin\keytool -import -alias rm_trusted_cert -file
RM_CERT_LOCATION\xlserver.cert -trustcacerts -keystore
$DOMAIN_HOME\config\fmwconfig\default-keystore.jks -storepass
KEYSTORE_PASSWORD
```

`$JAVA_HOME` is the location of the Java directory for the application server, the value of `alias` is the name for the certificate in the store, and `RM_CERT_LOCATION` is the location in which you copied the certificate.

- d. Enter **Y** at the prompt to trust the certificate.
 - e. On to the remote manager computer, in a text editor, open the `$XLREMOTE_HOME/xlremote/config/xlconfig.xml` file.
 - f. Locate the `<KeyManagerFactory>` property. If you are using the IBM JRE, then set the value to `IBMX509`. For example:

```
<KeyManagerFactory>IBMX509</KeyManagerFactory>
```

For all other JREs, set the value to `SUNX509`. For example:

```
<KeyManagerFactory>SUNX509</KeyManagerFactory>
```

- g. Save the file.

Note: The server certificate in `OIM_HOME` is also named `xlserver.cert`. Ensure that you do not overwrite that certificate.

- h. Restart Oracle Identity Manager.

28.2.2 Configuring the Remote Manager by Using Your Own Certificate

When the remote manager is installed, the installer generates a keypair and certificate with some default parameters, such as key password, certificate expiration time, and CN. However, you might need to change some of the parameters because of business

security requirements. As a result, you need to generate and use a keypair and certificate, instead of the default certificates that are installed.

To configure the remote manager by using your own certificate on the remote manager server:

Note: Perform the procedure given in this section only if you want to use your own certificate instead of the default Oracle Identity Manager certificates. Otherwise, skip this section.

1. Generate a new custom keystore and certificate. To do so, use the keytool utility, as shown in the following example:

```
keytool-genkeypair -keystore test.jks -alias rmcert -storepass welcome1 -keyalg
DSA -keysize 1024 -dname "CN=TestUser, OU=fmw, O=Oracle, C=US" -keypass
PASSWORD -validity 3650
```

Note the password that you use for the new keystore.

2. Copy the new keystore to the `$XLREMOTE_HOME/config/` directory.
3. In a text editor, open the `$REMOTE_MANAGER/config/xlconfig.xml` file.
4. Locate the `<RMSecurity>` tag and change the value in the `<Location>` and `<Password>` tags as follows:

- If you are using the IBM JRE, then change the values to:

```
<KeyStore>
<Location>new_keystore_name</Location>
<Password encrypted="false">new_keystore_pwd</Password>
<Type>JKS</Type>
<Provider>com.ibm.crypto.provider.IBMJCE</Provider>
</KeyStore>
```

- For all other JREs, change the values to:

```
<KeyStore>
<Location>new_keystore_name</Location>
<Password encrypted="false">new_keystore_pwd</Password>
<Type>JKS</Type>
<Provider>sun.security.provider.Sun</Provider>
</KeyStore>
```

5. Restart the remote manager server, and reopen the `xlconfig.xml` file to ensure that the password for the new keystore is encrypted.

To configure the remote manager by using your own certificate on Oracle Identity Manager:

1. Export the certificate from the newly created keystore on the remote manager computer, as shown in the following example:

```
keytool-export -keystore test.jks -storepass welcome1 -alias rmcert -file
test.cer
```

2. Copy the new certificate file to the `$DOMAIN_HOME/config/fmwconfig/` directory.
3. Import certificate into default-keystore.jks, as shown in the following example:

```
keytool-import -keystore test.jks -storepass welcome1 -alias test_alias -file
```

```
test.cer -trustcacerts
```

4. Check if the connection between remote manager and Oracle Identity Manager is established, as described in "[Testing the Remote Manager Connection](#)" on page 28-5.

28.2.3 Testing the Remote Manager Connection

To see Remote Manager Connection, you must first create a connection. To do so:

1. Login to Oracle Identity System Administration as the System Administrator.
2. Under Configuration, click **IT Resource**.
3. Under Resource Management, click **Create IT Resource**.
4. Enter IT Resource Name and IT Resource Type as Remote Manager. Click **Continue**.
5. Enter the service name as `RManager`. This is the remote manager service name used during the Remote Manager installation.
6. Enter the URL in the format `rmi://REMOTE_MANAGER_HOST:PORT`, for example, `rmi://rmhost.mycompany.com:1234`.
7. Continue with the wizard with default values, and click **Finish**.

After the connection is created, you can log into the Design Console to test the connection.

To test if the connection between remote manager and Oracle Identity Manager is established:

1. Login to the Design Console.
2. Open the Remote Manager form. This form displays the following:
 - The names and IP addresses of the remote managers that communicate with Oracle Identity Manager
 - Whether or not the remote managers are running
 - Whether or not the remote managers represent IT resources that Oracle Identity Manager can use

See Also: "Remote Manager Form" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about the Remote Manager form

3. Verify if the check boxes in the Running and IT Resource columns are selected for the remote manager service that you configured. This ensures that the remote manager is running and it represents an IT resource that Oracle Identity Manager can use.

In addition, Remote Manager connection status can be checked by using the Diagnostic Dashboard. See "[Remote Manager Status](#)" on page 25-5 for more information.

28.2.4 Updating the xlconfig.xml File to Change the Port for Remote Manager

Changing the port for the remote manager is not required at the time of configuring the remote manager. This is required if you need to change ports while using the product.

To update the `xlconfig.xml` file and start the remote manager on a new port as opposed to what was set during installation:

1. In a text editor, open the `$XLREMOTE_HOME/xlremote/config/xlconfig.xml` file.
2. Edit the following tags and change the port number:
 - `ListenPort` under `RMSecurity` for remote manager SSL Listen port
 - `RMRegistryPort` under `RMSecurity` for RMI Registry
3. Restart the remote manager. See ["Stopping and Starting the Remote Manager"](#) on page 28-6 for details.

28.3 Stopping and Starting the Remote Manager

To stop remote manager, navigate to the console from which the remote manager was started, and press CTRL+C. The remote manager is a command-line application, which will stop on this signal.

To start the remote manager, run the following script:

For UNIX:

```
$XLREMOTE_HOME/xlremote/remotemanager.sh
```

For Microsoft Windows:

```
$XLREMOTE_HOME\xlremote\remotemanager.bat
```

28.4 Troubleshooting Remote Manager

[Table 28–1](#) lists the troubleshooting steps that you can perform if you encounter problems with the remote manager:

Table 28–1 Troubleshooting Remote Manager

Problem	Solution
You encounter certificate trust issues.	Ensure that the remote manager certificate is trusted on the Oracle Identity Manager side.
	Ensure that the remote manager certificate has not expired.
	Ensure that the remote manager port is correctly configured on the Oracle Identity Manager host. In other words, ensure that the port configured on the Oracle Identity Manager host must be the same port in the remote manager configuration.
	Ensure that the remote manager configuration, such as keystore location, alias, password, and key password, in the <code>xlconfig.xml</code> file and Oracle Identity Manager host configuration in the <code>oim-config.xml</code> file are correct.
	Ensure that the correct server certificate is trusted on the remote manager if <code>client-auth</code> is set.

Table 28–1 (Cont.) Troubleshooting Remote Manager

Problem	Solution
<p>After ensuring all the conditions to resolve certificate trust issues, failure occurs while communicating between the remote manager and Oracle Identity Manager.</p>	<p>Restart Oracle Identity Manager and remote manager by passing the following flag:</p> <pre data-bbox="716 327 1052 352">-Djavax.net.debug={all ssl}</pre> <p>This flag, when turned on stores all the information related to the SSL/TLS handshake in the logs. Here, all turns on all debugging, and ssl turns on SSL debugging.</p> <p>Note: Use this flag only for debugging purpose. When turned on, it dumps a huge amount of information in the logs.</p>
<p>The remote manager connection fails.</p>	<p>Ensure that there is no firewall between Oracle Identity Manager and remote manager that is blocking tcp traffic on the specific port. To do this, telnet from the Oracle Identity Manager host to the remote manager host on the remote manager port.</p>
<p>Provisioning through the remote manager fails.</p>	<p>Ensure that the adapter JAR files (which are usually located in the <code>\$OIM_HOME/JavaTasks/</code> directory or in the database) are copied on the remote manager host in the <code>JavaTasks/</code> directory.</p> <p>Ensure that the remote manager-based adapters have a Remote Task to invoke target APIs, as opposed to regular adapters, which can just use Java Task to do the same.</p> <p>Ensure that the remote manager-based connectors:</p> <ul style="list-style-type: none"> - Define a remote manager IT resource. - Set the remote manager IT resource on the remote manager field on the regular IT resource, which contains the connectivity information of the target

Using the Form Version Control Utility

Process forms and child forms are used to hold account data of OIM Users. You can upgrade a form by adding, modifying, or removing fields on the form. For example, as part of an upgrade operation, you might add the Hire Date field and remove the Country of Origin field from a form. In addition, fields might be moved from the parent form to the child form. The Oracle Identity Manager Form Version Control (FVC) Utility facilitates the management of form data changes after a form upgrade operation.

The FVC Utility is a command-line utility that works directly on the Oracle Identity Manager database. When you install the Oracle Identity Manager Design Console, the utility is present in the *OIM_DC_HOME* directory. You use a properties file to specify the form data updates that the utility must perform.

The utility supports field mapping and data updates on a provisioning process form and its associated child forms.

Note: The FVC Utility *cannot* perform the following functions:

- Manage data updates on object forms
- Move rows across forms

In addition, you *need not* run the FVC Utility if there are no form-related changes from one release to the next release.

This chapter contains the following sections:

- [Use Cases Supported by the FVC Utility](#)
- [Use Cases That Are Not Supported by the FVC Utility](#)
- [Summary of the Form Version Control Process](#)
- [Components of the FVC Utility](#)
- [Using the FVC Utility](#)
- [Troubleshooting](#)

29.1 Use Cases Supported by the FVC Utility

In a single run, the FVC Utility can be used to manage form data updates corresponding to the following form changes:

See Also: ["Summary of the Form Version Control Process"](#) on page 29-2 provides information about the validation performed by the utility before it starts processing form data.

- A field on the parent form is renamed.
- A field on the child form is renamed.
- A field is moved from the parent form to a child form.
- A field is moved from the parent form to a parent form.
- A field is moved from a child form to the parent form. This scenario is supported only if the child form contains a single record.
- A field is moved from a child form to another child form of the same parent form. This scenario is supported only if the source child form contains a single record.
- A field is moved from one child form to another child form of the same parent form. This scenario is supported only if the child form contains a single record.
- A field is moved from a child form to the parent form and also the data type of the moved field is changed from Lookup Field or Combo Box type to Check Box type in parent form.
- In any of the above use cases, the data type of the field in parent form is changed from Lookup Field or Combo Box type to Check Box type.
- In any of the above use cases, the case of a field name is changed. For example, the field name is changed from `MyField` to `myfield`.
- The data type of a field is changed from Lookup Field or Combo Box type to Check Box type, without any other change being made to the form.
- For a particular OIM User, the utility proceeds with updating account data only if the status of the user's record in the `USR` table is not `Deleted`.

For an OIM User whose status in the `USR` table is not `Deleted`, the utility updates account data in a `UD_` table only if the status of the account is not `Revoked`.

29.2 Use Cases That Are Not Supported by the FVC Utility

The FVC Utility cannot be used to update form data in the following scenarios:

- Fields are modified across multiple process (parent) forms.
- A field is mapped to multiple fields on the same form.
- A field is mapped to multiple fields on different child forms.
- The data type of a field is changed from any type *other than* the Lookup Field or Combo Box type.
- The data type of a field is changed from Lookup Field or Combo Box type to any type *other than* a Check Box type.
- Multiple fields are combined into a single field.

29.3 Summary of the Form Version Control Process

The following steps take place during each run of the FVC Utility:

1. The properties file holds information about the data conversion actions to be performed by the FVC Utility. The utility reads the contents of this properties file.

2. The utility checks the object status of the record in the USR table. The next step depends on the status of the record:
 - If the user's record is in the Deleted state, then the utility moves on to the next user's record.
 - If the user's record is *not* in the Deleted state, then the utility checks the status of the account records in the connector-specific (UD_) tables for that user. For each account record, the next step depends on the status of the account record:
 - If the account record is in the Revoked state, then the utility moves on to the next account record for that user.
 - If the account record is *not* in the Revoked state, then the utility performs the updates specified in the properties file.
3. For a particular account record, the utility first updates the version of the record and then updates the data as specified in the properties file.

Note: If an error is encountered, then an error message is displayed in the command window. After you fix the cause of the error and rerun the utility, records that have been updated before the error was encountered are not processed again.

29.4 Components of the FVC Utility

The following are components of the FVC Utility:

Note: When you install the Design Console, these files are copied into the *OIM_DC_HOME* directory.

- Properties file: You use a file with the ".properties" extension to provide details of the process form, child forms, and resource object on which you want to run the utility. The fvc.properties file is provided as a sample. If a new properties file is used, then the name of the file must be changed in fvcutil.sh or fvcutil.cmd.
- xIFvcUtil.jar: This JAR file contains the utility classes required to run the FVC Utility.
- fvcutil.sh and fvcutil.cmd: You use this script to run the utility.

29.5 Using the FVC Utility

The following sections describe the procedure to use the FVC Utility:

- [Preparing the Properties File](#)
- [Addressing Prerequisites for Using the FVC Utility](#)
- [Running the Utility](#)

29.5.1 Preparing the Properties File

As mentioned earlier in this chapter, you use a properties file to define the data conversion actions that you want the FVC Utility to perform. Whether you must create or update the properties file depends on the upgrade scenario:

- If you are upgrading from a predefined release to a predefined release of a connector, then look for a properties file in the connector deployment package.
- If you are upgrading from a custom release *or* upgrading to a custom release, then you must add the required entries in the properties file.
- If you are upgrading from a custom release to a predefined release of a connector, then see if the connector guide provides information about changes to the process form and child forms of the connector. You can use this information to determine the entries that you must add in the properties file.

The following are sample entries for the properties file:

```
ResourceObject;OID User
FormName;UD_OID_USR
FromVersion;8
ToVersion;9
Parent;UD_OID_USR_DEFTVAL;ABC
Child;UD_OID_GRP_NORMALFIELD;XYZ;Update
ParentChild;UD_OID_USR_FNAME;UD_OID_GRP_NORMALFIELD
ChildChild;UD_OID_GRP_GROUP_NAME;UD_OID_GRP_NORMALFIELD
ChildParent;UD_OID_GRP_NORMALFIELD;UD_OID_USR_LNAME
ParentParent;UD_OID_USR_FNAME;UD_OID_USR_LOGIN;
ParentParentLookupOrComboToCheckBox;UD_OID_USR_PREF_LANG;UD_OID_USR_CHKBOXTTEST
ChildParentLookupOrComboToCheckBox;UD_OID_GRP_GROUP_NAME;UD_OID_USR_CHKBOXTTEST
ChildDiffChild;UD_OID_GRP_NORMALFIELD;UD_OID_ROLE_DIFFFIELD
```

Apply the following guidelines while adding or modifying entries in the properties file:

Note: See the sample entries listed earlier to get a better understanding of the guidelines.

- In the properties file, each line consists of the use case name, followed by old field name and the new field name. Each of these are separated by semicolon.

For Example consider following entry in properties file:

```
ParentChild;UD_OID_USR_FNAME;UD_OID_GRP_NORMALFIELD
```

ParentChild: represents that the fields of the parent have been renamed/moved to be in the new child form

UD_OID_USR_FNAME: represents the old field name in parent form

UD_OID_GRP_NORMALFIELD: represents the new name of the field to be upgraded in the new form.

Note: There can be spaces in the value as long as a space does not appear immediately after the semicolon.

- You must include the following lines in the properties file:

Note: The location and order of these 4 lines in the properties file does not matter.

– ResourceObject;*RESOURCE_OBJECT_NAME*

In this line, replace *RESOURCE_OBJECT_NAME* with the name of the resource object.

Sample line:

```
ResourceObject;OID User
```

- FormName; *FORM_NAME*

In this line, replace *FORM_NAME* with the name of the process (parent) form.

Sample line:

```
FormName;UD_OID_USR
```

- FromVersion; *CURRENT_VERSION_OF_FORM*

In this line, replace *CURRENT_VERSION_OF_FORM* with the current version of the form.

Note: When you run the FVC Utility, only records whose version is the same as *CURRENT_VERSION_OF_FORM* are updated by the utility.

Sample line:

```
FromVersion;8
```

- ToVersion; *NEW_VERSION_OF_FORM*

In this line, replace *NEW_VERSION_OF_FORM* with the new version of the form.

Note: If you want to update form data on a form whose version has not changed, then set *NEW_VERSION_OF_FORM* to the same value as *CURRENT_VERSION_OF_FORM*.

Sample line:

```
ToVersion;9
```

- You can include any combination of the following lines in the properties file:

- Parent; *FIELD_NAME*; *DEFAULT_FIELD_VALUE*; Update

For all records on the parent form, the utility updates the value of the *FIELD_NAME* field with *DEFAULT_FIELD_VALUE*.

Note: If a mandatory (required) field has been added on the parent form, then you must include this line in the properties file for the mandatory field.

Sample line:

```
Parent;UD_OID_USR_DEFTVAL;MyString;Update
```

- Child; *FIELD_NAME*; *DEFAULT_FIELD_VALUE*; Update

For all records on the child form, the utility updates the value of the *FIELD_NAME* field to *DEFAULT_FIELD_VALUE*.

Note: If a mandatory (required) field has been added on the child form, then you must include this line in the properties file.

Sample line:

```
Child;UD_OID_GRP_NORMALFIELD;XYZ;Update
```

- ParentParent; *OLD_FIELD_NAME*; *NEW_FIELD_NAME*

On the parent form, the utility moves data from the *OLD_FIELD_NAME* field to the *NEW_FIELD_NAME* field.

Sample line:

```
ParentParent;UD_OID_USR_FNAME;UD_OID_USR_DEFTVAL;
```

- ParentParentLookupOrComboToCheckBox; *OLD_FIELD_NAME*; *NEW_FIELD_NAME*;

On the parent form, for a Lookup Field or Combo Box type field that has been changed to a Check Box type field and also renamed, the utility sets the check box for each record to the selected state if the field value is True (case insensitive). For all other values, the utility sets the check box to the deselected state.

Sample value:

```
ParentParentLookupOrComboToCheckBox;UD_OID_USR_PREF_LANG;UD_OID_USR_CHKBOXTST
```

- ChildChild; *OLD_FIELD_NAME*; *NEW_FIELD_NAME*

On the child form, the utility copies data from the *OLD_FIELD_NAME* field of the earlier version to the *NEW_FIELD_NAME* field of the new version.

Sample line:

```
ChildChild;UD_OID_GRP_GROUP_NAME;UD_OID_GRP_NORMALFIELD
```

- ParentChild; *OLD_FIELD_NAME*; *NEW_FIELD_NAME*

The *OLD_FIELD_NAME* field was moved from the parent form to the child form and renamed to *NEW_FIELD_NAME*. The utility moves data from the *OLD_FIELD_NAME* field to the *NEW_FIELD_NAME* field.

Sample line:

```
ParentChild;UD_OID_USR_FNAME;UD_OID_GRP_NORMALFIELD
```

- ChildParent; *OLD_FIELD_NAME*; *NEW_FIELD_NAME*

The *OLD_FIELD_NAME* field was moved from the child form to the parent form and renamed to *NEW_FIELD_NAME*. The utility moves data from the *OLD_FIELD_NAME* field to the *NEW_FIELD_NAME* field.

Sample line:

```
ChildParent;UD_OID_GRP_NORMALFIELD;UD_OID_USR_DEFTVAL
```

- ChildParentLookupOrComboToCheckBox; *OLD_FIELD_NAME*; *NEW_FIELD_NAME*

From a child form, a Lookup Field or Combo Box type field (*OLD_FIELD_NAME*) has been changed to a Check Box type field and moved to the parent form. On the parent form, the utility sets the check box for each record to the selected state if the field value is True (case sensitive). For all other values, the utility sets the check box to the deselected state.

Sample line:

```
ChildParentLookupOrComboToCheckBox;UD_OID_GRP_GROUP_NAME;UD_OID_USR
_CHKBOXTEST
```

– ChildDiffChild;*OLD_FIELD_NAME*;*NEW_FIELD_NAME*

The utility moves data from the *OLD_FIELD_NAME* field on the source child form to the *NEW_FIELD_NAME* field on the target child form.

Note: This update is carried out only if the source child form contains a single row. A scenario in which the source child form contains more than one row is not supported.

Sample line:

```
ChildDiffChild;UD_OID_GRP_NORMALFIELD;UD_OID_ROLE_DIFFFIELD
```

29.5.2 Addressing Prerequisites for Using the FVC Utility

Before you run the utility:

1. Set the Java home directory path in the FVC Utility script as follows:
 - a. Depending on the operating system and application server that you are using, open one of the following files in a text editor:

```
fvcutil.sh
```

```
fvcutil.cmd
```

- b. Search for `set JAVA_HOME`.
- c. Set the Java home directory path as shown in the following example:

```
set JAVA_HOME=C:\Java\
```

- d. Set the following if you are running the FVC Utility on Microsoft Windows and Oracle WebLogic Application Server:

```
set APPSERVER_TYPE=wls
```

- e. Save and close the file.

2. Verify that the version of the process (parent) form on which you want to run the utility is the Active version.

To check if the version of a form is the Active version:

- a. Log in to the Design Console
 - b. Expand the **Development Tools** folder, and then double-click **Form Designer**.
 - c. Search for and open the form.
 - d. Active Version field of the form displays the active version of the form.
3. The utility cannot update a form field if the field is associated with error-handling adapters. If any field is associated with error-handling adapters, then dissociate the adapters as follows:

Note: After you run the utility, you can again set up the association between the field and its error-handling adapters. The procedure is described later in this chapter.

- a. Log in to the Design Console
- b. Expand the **Process Management** folder, and then double-click **Process Definition**.
- c. Search for and open the process definition of the connector.
- d. Make a note of the name of the task that updates the field.
- e. Double-click the task. For example, if the userID field has an error-handling adapter, then double-click the **updateUserID** task.
- f. On the Integration tab of the Editing Task dialog box, make a note of the adapter variable names and their descriptions.
- g. Click **Remove**.
- h. To confirm that you want to remove the event-handler adapter, click **OK** in the message that is displayed.
- i. Click **Save**.

29.5.3 Running the Utility

Note: You must execute the FVC utility every time the form version is changed.

Run the following script:

For Unix:

```
sh fvcutil.sh
```

For Windows:

```
fvcutil.bat
```

This will prompt you to enter the following details:

1. Enter Oracle Identity Manager admin username: Enter Oracle Identity Manager administrator username.
2. Enter Oracle Identity Manager admin password: Provide Oracle Identity Manager administrator password.
3. Enter logger level: Enter the logger level. It can be DEBUG, WARN, INFO, or ERROR.
4. Enter logger location: Provide the location and name of the log file that you want the utility to create at the end of each run. For example, <Path name>/FVC.log.

29.6 Troubleshooting

[Table 29–1](#) lists the error messages that you might encounter in the log file and the corresponding actions that you can take to fix the issues:

Table 29–1 Error Messages and Solutions

Error Message	Solution
Could not find objects with name= <i>OBJECT_NAME</i>	Check the name of the resource object provided in the properties file. Ensure that it is spelled correctly.
Could not find form with name= <i>FORM_NAME</i>	Check the name of the form provided in the properties file. Ensure that it is spelled correctly.
Could not find active version of the form.	A newly created form might not have been committed and set to the Active state. Ensure that the form is in the Active state.
ToVersion value and active version of the form do not match.	Ensure that the ToVersion value is the same as the version of the form that is currently active.
Either ToVersion or FromVersion values are not valid versions.	Ensure that the ToVersion and FromVersion values are correct.
<i>FIELD_NAME</i> field does not exist in the Oracle Identity Manager database.	Ensure that the name of the field is spelled correctly.

Starting and Stopping Servers

Most Oracle Identity Manager feature configurations, such as password policy create and update, need the restart of the server for the changes to take effect. This chapter provide procedures to start/stop Oracle WebLogic Servers.

You can perform all start and stop operations for managed WebLogic Servers either from command prompt or from Oracle WebLogic Server Administration Console or Oracle Enterprise Manager Fusion Middleware Control.

The following sections are given only for reference purpose. See Oracle *WebLogic Server Administrator Guide* for detailed information.

Note: Node Manager must be running in order to use the Oracle WebLogic Server Administration Console or Oracle Enterprise Manager Fusion Middleware Control for controlling (start/stop) Oracle Identity Manager WebLogic managed servers and SOA WebLogic managed servers.

- [Configuring the Node Manager](#)
- [Starting the Node Manager](#)
- [Starting or Stopping WebLogic Administration Server](#)
- [Starting or Stopping WebLogic Managed Servers](#)

You can perform all start and stop operations either from command prompt or from Oracle WebLogic Server Administration Console.

Note: Node Manager must be running before you can start and stop administration server, Oracle Identity Manager managed server, and SOA managed server through Oracle WebLogic Server Administration Console.

30.1 Configuring the Node Manager

After installing and configuring Oracle Identity Manager and SOA servers, you must configure node manager for using it with WebLogic Administration Console or Oracle Enterprise Manager Fusion Middleware Control. This configuration is to be done only once.

To configure node manager, you must set `StartScriptEnabled=true` in the `nodemanager.properties` file. To do so, run following script:

For UNIX:

```
MIDDLEWARE_HOME/oracle_common/common/bin/setNMProps.sh
```

For Microsoft Windows:

```
MIDDLEWARE_HOME\oracle_common\common\bin\setNMProps.cmd
```

30.2 Starting the Node Manager

To start the Node Manager:

1. Navigate to `WL_HOME/server/bin`.
2. At the command prompt, enter:

```
./startNodeManager
```

30.3 Starting or Stopping WebLogic Administration Server

To start or stop the WebLogic Administration Server:

1. Navigate to `DOMAIN_HOME/bin`.

Note:

- For Linux Install you have only `./startWebLogic.sh` and you do not have `startWebLogic.cmd` in the bin folder.
 - For Microsoft Windows Install we have both `./startWebLogic.sh` and `startWebLogic.cmd` in the bin folder.
-
-

2. To start the server, enter the following:

For UNIX:

```
./startWebLogic.sh
```

For Microsoft Windows:

```
startWebLogic.cmd
```

To stop the server, enter the following:

For UNIX:

```
./stopWebLogic.sh
```

For Microsoft Windows:

```
stopWebLogic.cmd
```

30.4 Starting or Stopping WebLogic Managed Servers

This section contains the following topics:

- [Starting or Stopping the Managed Servers By Using Command Prompt](#)
- [Starting or Stopping the Managed Server By Using Oracle Enterprise Manager Fusion Middleware Control](#)

- [Starting or Stopping Servers By Using Oracle WebLogic Server Administration Console](#)

Note: You must start the SOA Server before starting Oracle Identity Manager server.

30.4.1 Starting or Stopping the Managed Servers By Using Command Prompt

To start or stop the managed servers using command prompt:

1. Navigate to the *DOMAIN_HOME/bin/* directory.
2. To start the server, enter the following at the command prompt:

For UNIX:

```
./startManagedWebLogic.sh MANAGED_SERVER_NAME ADMIN_SERVER_URL
```

For example:

```
startManagedWebLogic.sh oim_server1
http://mywlsadminhost.mycompany.com:7001

startManagedWebLogic.sh soa_server1
http://mywlsadminhost.mycompany.com:7001
```

For Microsoft Windows:

```
startManagedWebLogic.cmd MANAGED_SERVER_NAME ADMIN_SERVER_URL
```

To stop the server, enter the following at the command prompt:

For UNIX:

```
./stopManagedWebLogic.sh MANAGED_SERVER_NAME ADMIN_SERVER_URL
```

For Microsoft Windows:

```
stopManagedWebLogic.cmd MANAGED_SERVER_NAME ADMIN_SERVER_URL
```

For example:

```
stopManagedWebLogic.cmd oim_server1
http://mywlsadminhost.mycompany.com:7001

stopManagedWebLogic.cmd soa_server1
http://mywlsadminhost.mycompany.com:7001
```

30.4.2 Starting or Stopping the Managed Server By Using Oracle Enterprise Manager Fusion Middleware Control

In order to use the Oracle Enterprise Manager Fusion Middleware Control to control managed servers, Node Manager must be running on the computer.

To start or stop the managed server using Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to the Oracle Enterprise Manager Fusion Middleware Control.
2. Navigate to **Weblogic Domain**, **Domain Name**, *SERVER_NAME*.
3. Right click, and navigate to **Control**.
4. Click **Start Up** to start the server.

Click **Shutdown** to stop the server.

30.4.3 Starting or Stopping Servers By Using Oracle WebLogic Server Administration Console

To start or stop servers by using Oracle WebLogic Administration Console:

1. Log in to the Oracle WebLogic Server Administration Console.
2. On the left pane, under Domain Structure, select **Environment, Servers**.
3. On the right pane, under Summary of Servers, click the **Control** tab.
4. Select the server name.
5. Click **Start** to start the server.

Click **Shutdown** to shutdown the server.

Enabling Secure Cookies

By default, Oracle Identity Manager can be accessed over HTTP but does not work over Secure Socket Layer (SSL). This is because the cookie-secure flag is disabled by default. The cookie-secure flag tells the Web browser to only send the cookie back over an HTTPS connection. This ensures that the cookie is transmitted only on a secure channel. HTTPS must be enabled for the URL exposed by the application.

To enable Oracle Identity Manager to work over SSL, you must enable the cookie-secure flag. To do so:

1. Add the `<cookie-secure>true</cookie-secure>` tag inside the `<session-descriptor>` element to the following files in the Oracle Identity Manager deployment:
 - `OIM_HOME/apps/oim.ear/admin.war/WEB-INF/weblogic.xml`
 - `OIM_HOME/apps/oim.ear/iam-consoles-faces.war/WEB-INF/weblogic.xml`
 - `OIM_HOME/apps/oim.ear/xlWebApp.war/WEB-INF/weblogic.xml`
2. Create a new `weblogic.xml` file for Nexaweb application if it does not exist in its `WEB-INF/` directory.
3. Add the following session descriptor in it:

```
<?xml version='1.0' encoding='UTF-8'?>
<weblogic-web-app
  xmlns="http://xmlns.oracle.com/weblogic/weblogic-web-app/1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.oracle.com/weblogic/weblogic-web-app/1.0
http://xmlns.oracle.com/weblogic/weblogic-web-app/1.0/weblogic-web-app.xsd">

  <session-descriptor>
    <persistent-store-type>replicated_if_clustered</persistent-store-type>
    <cookie-http-only>>false</cookie-http-only>
    <cookie-name>oimjsessionid</cookie-name>
    <cookie-secure>true</cookie-secure>
    <url-rewriting-enabled>>false</url-rewriting-enabled>
  </session-descriptor>

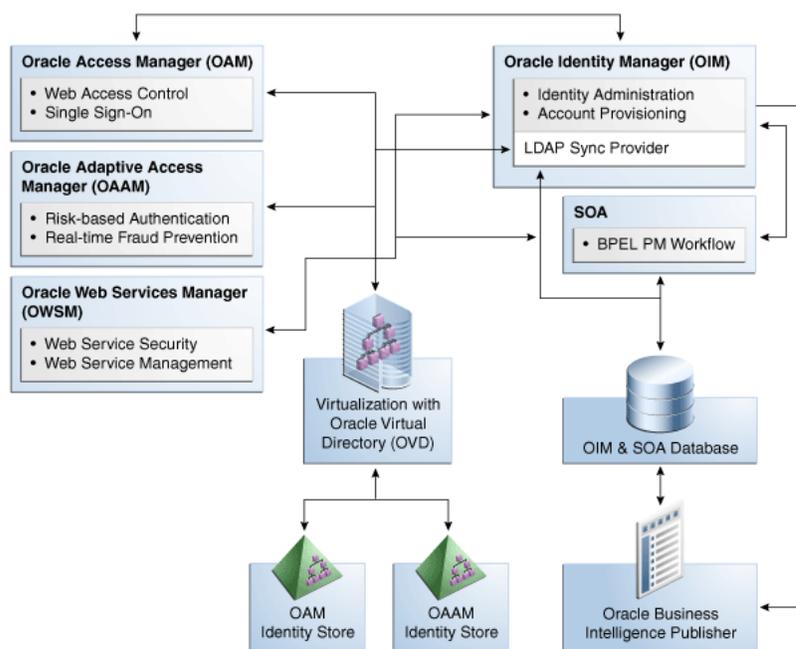
</weblogic-web-app>
```

4. Save `weblogic.xml`.
5. Restart the Oracle Identity Manager Managed Servers.

Integrating with Other Oracle Components

Oracle offers several technologies that compliment and extend the functionality available in Oracle Identity Manager, some of which are described in this chapter. Refer to the "Oracle Fusion Middleware Integration Overview" for complete information about the technologies you can integrate with Oracle Identity Manager. [Figure 32-1](#) shows the integration of Oracle Identity Manager with other Oracle components.

Figure 32-1 *Integration with Other Components*



This chapter discusses the integration of Oracle Identity Manager with the following Oracle components:

- [Oracle Access Manager](#)
- [Oracle Adaptive Access Manager](#)
- [Oracle Identity Analytics](#)
- [Oracle Identity Navigator](#)
- [Oracle Virtual Directory](#)

- [Oracle Service-Oriented Architecture](#)
- [Oracle Business Intelligence Publisher](#)

32.1 Oracle Access Manager

Oracle Access Manager (OAM) protects applications, data, and cloud-based services through a combination of flexible authentication and single sign-on (SSO), identity federation, risk-based authentication, proactive enterprise fraud prevention, and fine-grained authorization.

Web-based SSO provides secure access to multiple applications with one authentication step. When OAM is combined with Oracle Identity Manager, OAM can SSO-enable the Oracle Identity Administration, along with the other Oracle Identity Management components.

Oracle Identity Manager, OAM, and Oracle Adaptive Access Manager (OAAM) share a common set of LDAP attributes, improving efficiency by making it easier to manage workflows and other processes. Integrated password management makes it easy for users to log in to OAM, OAAM, and Oracle Identity Manager, and to manage expired and forgotten passwords.

For integration details, see "Integration Between OIM and OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

32.2 Oracle Adaptive Access Manager

OAAM provides sophisticated multifactor authentication and proactive, real-time fraud prevention functionality for Web-based connections.

Risk-based authentication is one such capability OAAM provides. The OAAM risk-scoring engine combats identity fraud in real-time by evaluating whether a user should be allowed to authenticate based on the type of transaction being attempted and the probability of fraud occurring. Next, the OAAM risk-scoring engine evaluates how a user answers a series of dynamically generated questions that are created based on a combination of public and private data sources. OAAM then generates a fraud score and the user is either allowed to continue with the transaction or is denied access.

When integrated with Oracle Identity Manager, the robust challenge question feature set found in OAAM replaces the more limited set found in Oracle Identity Manager, which handles password validation, storage, and propagation duties.

For information about how password management is achieved when Oracle Identity Manager is integrated with OAM and OAAM, see "Deployment Options for Password Management" in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.

For integration details, see "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager" in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.

32.3 Oracle Identity Analytics

Oracle Identity Analytics (OIA), formerly Sun Role Manager, provides rich identity analytics and dashboards that allow you to monitor, analyze, review, and govern user access in order to mitigate risk, build transparency, and satisfy compliance mandates.

When integrated with Oracle Identity Manager, Oracle Identity Analytics defines the Role-based Access Control (RBAC) framework, the attestation process, and the approach to Segregation of Duties (SoD) policy enforcement, while Oracle Identity Manager serves as the automated provisioning and identity synchronization solution. Rather than assigning individual access entitlements, the RBAC framework allows organizations to assign and unassign roles as a means of controlling user access on various applications.

32.3.1 Integration Configuration in Oracle Identity Analytics

For integration details in Oracle Identity Analytics, see "Integrating With Oracle Identity Manager, Preferred Method" in the *Oracle Fusion Middleware System Integrator's Guide for Oracle Identity Analytics*.

32.3.2 Integration Configuration in Oracle Identity Manager

Oracle Identity Manager is an authoritative source of data for users, accounts, and entitlements. Therefore, in an integrated deployment, OIA needs the following data from Oracle Identity Manager:

- User attributes
- Account attributes, including assigned entitlements
- Entitlements

The requirements for the data synchronization are:

- OIA needs incremental changelog updates for users, accounts, and entitlements from Oracle Identity Manager
- OIA needs, on an ad-hoc basis full set of entities, such as users, accounts, and entitlements, from Oracle Identity Manager on an ad hoc basis

Oracle Identity Manager 11g Release 2 (11.1.2.1.0) allows the data synchronization with the help of:

- APIs to allow OIA to start data collection for a configurable number of entities. In addition, APIs allow OIA to get the status of the data collection.

For information about using Oracle Identity Manager APIs, see *Oracle Fusion Middleware Java API Reference for Oracle Identity Manager* and "Using APIs" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

- Stored procedures that perform the data collection from Oracle Identity Manager transactional tables to the staging tables.

This section describes the data collection process with the help of the following topics:

- [The DataCollectionOperationsIntf API Interface](#)
- [Staging Tables](#)
- [Data Collection Process](#)

32.3.2.1 The DataCollectionOperationsIntf API Interface

The DataCollectionOperationsIntf API interface provides the following APIs:

- **void startDataCollection(String sessionID, Map entities):** This API starts the data collection process for a single session. The parameters are:

- **sessionID:** A unique string identifying the particular session. This string must be the same in repeated invocations of APIs that form the part of a single data collection session.
- **entities:** A Map that contains all the entities and the since dates for which data collection is to be performed. There are two static entities, user and entitlement. The rest can be resource object names in Oracle Identity Manager. If the entity or resource object name cannot be found, it is ignored and no data collection is performed for the same. The values in the Map are java.util.Date objects that represent a timestamp. If this value is NULL, then complete data for that entity is populated. If the data is non-NULL, then data is populated in the staging tables for entities modified after that date.
- **String checkStatus(String sessionID):** This API checks for the status of the specified data collection session. The API returns the following statuses:
 - INITIATED
 - IN PROGRESS
 - COMPLETED
 - FAILED
 - FINALIZED
- **void finalizeSession(String sessionID):** This API finalizes the data collection session by truncating the staging tables and other cleanup activities.

32.3.2.2 Staging Tables

Oracle Identity Manager makes user, account, and entitlement data through certain tables to OIA. These are called staging tables, which can be populated on demand by using the APIs in the DataCollectionOperationsIntf interface. The following staging tables can be populated:

- staging_users_table: Staging table for user profile attributes
- staging_user_extended_props: Staging table for custom user defined fields
- staging_entitlements: Staging table for entitlement information
- staging_accounts: Staging table for account information
- staging_account_attributes: Staging table for account attributes including parent and child form data

32.3.2.3 Data Collection Process

The following is the sequence of steps for the data collection:

1. Invoke startDataCollection() API with the appropriate session ID and entities with since dates. If the since date is NULL, then indicates to Oracle Identity Manager that full data must be populated in the staging tables.
2. Poll Oracle Identity Manager by running the getDataCollectionStatus() API with the same session ID.
3. After the getDataCollectionStatus() API returns COMPLETED status, OIA processes can directly read the data from the staging tables.
4. After data synchronization is complete, run the finalizeDataCollectionSession() API with the same session ID to finalize the data collection session.

5. If there are any errors in the data collection, then Oracle Identity Manager indicates it with a FAILED status. If this happens, then the data collection session must be restarted. You can restart the data collection session by finalizing the current session using `finalizeDataCollectionSession()` API and then running `startDataCollection()` with a new session ID.

32.4 Oracle Identity Navigator

Oracle Identity Navigator (OIN) is a browser-based administrative portal designed to act as a launch pad for Oracle Identity Management components. It does not replace the individual component consoles. Rather, it allows you to access the Oracle Identity Management consoles from one site.

When integrated with Oracle Identity Manager, OIN replaces the Oracle Identity Administration as the primary Oracle Identity Manager user interface.

OIN has a product discovery feature that can be used to discover all active J2EE components in a domain, including the Oracle Identity Administration.

For integration details, see "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

32.5 Oracle Virtual Directory

If you install Oracle Identity Manager with LDAP, you must install Oracle Virtual Directory (OVD). OVD connects to multiple enterprise directories and consolidates the contents of those directories into a unified view. For example, if your enterprise uses Oracle Internet Directory (OID), iPlanet, and Active Directory, OVD can interface with all three directories and create a consolidated view. Oracle Identity Manager can then use a single connector to access the consolidated LDAP data on OVD. The LDAP Sync Provider (also called the LDAP Provider) connects Oracle Identity Manager and OVD.

When integrated with Oracle Identity Manager, OVD provides the following benefits:

- Oracle Identity Manager connector management is simplified - Only a single LDAP connector is needed for multiple directory providers (although, multiple instances may be needed)
- LDAP connector reliability is improved - The same connector is used regardless of the underlying LDAP server. OVD handles the data translation that, in the past, required multiple LDAP connectors for multiple LDAP providers
- The same identity virtualization capability is provided to all Fusion Middleware applications, reducing the overall footprint of components in the Enterprise

For integration details, see the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*, which contains multiple procedures for integrating Oracle Identity Manager and Oracle Virtual Directory in various environments.

Earlier releases of OVD are installed in Blocking IO (BIO) mode. The current release of OVD is installed in Non Blocking IO (NIO) mode by default. However, Oracle Identity Manager is not certified with NIO mode. Therefore, the OVD connection management in Oracle Identity Manager must be modified for working with OVD in NIO mode.

The current release of OVD is also enhanced to include multiple change log support. These enhancements require changes to the OVD Changlog adapter parameters.

See "Creating Adapters in Oracle Virtual Directory" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* for detailed information about creating the OVD adapters for Oracle Identity Manager change log and user management.

32.6 Oracle Service-Oriented Architecture

The Oracle Identity Manager workflow feature utilizes Oracle Service-Oriented Architecture (SOA) back-end services and management capabilities to provide an interactive environment to request, approve, and manage user access. In order to install Oracle Identity Manager, you also must install Oracle SOA.

Oracle Identity Manager makes use of the following SOA Suite components:

- BPEL Process Manager, which provides the end-to-end solution for creating and managing business processes
- Human Workflow, which manages the lifecycle of human tasks, including creation, assignment, deadlines, expiration, and notifications
- Oracle Business Rules, which allows you to define complex business rules to support request assignment, process selection, and approver resolution
- Oracle Web Services Manager, which secures the web service and BPEL processes consumed and invoked by Oracle Identity Manager

For integration details, see "Integration with Oracle SOA Suite" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

32.7 Oracle Business Intelligence Publisher

The Oracle Identity Manager reporting feature utilizes Oracle Business Intelligence Publisher (BI Publisher) to provide high-fidelity reporting capabilities, allowing you to create, deploy, and use complex reports in a multi-channel environment.

For BI Publisher details, see "Using Reporting Features" in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

Handling Lifecycle Management Changes

Because of integrated deployment of Oracle Identity Manager with other applications, such as Oracle Access Manager (OAM), and configuration changes in those applications, various configuration changes might be required in Oracle Identity Manager and Oracle WebLogic Server. These configuration changes are described in the following sections:

- [URL Changes Related to Oracle Identity Manager](#)
- [Password Changes Related to Oracle Identity Manager](#)
- [Configuring SSL for Oracle Identity Manager](#)

33.1 URL Changes Related to Oracle Identity Manager

Oracle Identity Manager uses various hostname and port in its configuration because of the architectural and middleware requirements. This section describes ways to make the corresponding changes in Oracle Identity Manager and Oracle WebLogic configuration for any change in the integrated and dependent applications.

This section contains the following topics:

- [Oracle Identity Manager Host and Port Changes](#)
- [Oracle Identity Manager Database Host and Port Changes](#)
- [Oracle Virtual Directory Host and Port Changes](#)
- [BI Publisher Host and Port Changes](#)
- [SOA Host and Port Changes](#)
- [OAM Host and Port Changes](#)

33.1.1 Oracle Identity Manager Host and Port Changes

This section consists of the following topics:

- [Changing OimFrontEndURL in Oracle Identity Manager Configuration](#)
- [Changing backOfficeURL in Oracle Identity Manager Configuration](#)

Note: When additional Oracle Identity Manager nodes are added or removed, perform the procedures described in these sections to configure Oracle Identity Manager host and port changes.

33.1.1.1 Changing OimFrontEndURL in Oracle Identity Manager Configuration

The OimFrontEndURL is the URL used to access the Oracle Identity Manager UI. This can be a load balancer URL or Web server URL depending on the application server is fronted with load balancer or Web server, or single application server URL. This is used by Oracle Identity Manager in the notification e-mails as well as the callback URL for SOA calls.

The change may be necessary because of change in Web server hostname or port for Oracle Identity Manager deployment in a clustered environment, or WebLogic managed server hostname or port changes for Oracle Identity Manager deployment in a nonclustered environment.

To change the OimFrontEndURL in Oracle Identity Manager configuration:

1. Login to Enterprise Manager by using the following URL when the WebLogic Administrative Server and Oracle Identity Manager managed servers, at least one of the servers in case of a clustered deployment, are running:

`http://ADMIN_SERVER/em`

2. Navigate to **Identity and Access, oim**.
3. Right-click **oim**, and navigate to **System MBean Browser**.
4. Under Application Defined MBeans, navigate to **oracle.iam, Application:oim, XMLConfig, Config, XMLConfig.DiscoveryConfig**, and then **Discovery**.
5. Enter new value for the OimFrontEndURL attribute, and click **Apply** to save the changes. Example values can be:

`http://OIM_SERVER:OIM_PORT`

`https://myoim.mydomain.com`

`https://myoimserver.mydomain.com:14001`

Note: SPML clients store Oracle Identity Manager URL for invoking SPML and sending callback response. Therefore, changes are required corresponding to this. In addition, if Oracle Identity Manager is integrated with OAM, OAAM, or Oracle Identity Navigator (OIN), there may be corresponding changes necessary. For more information, refer to OAM, OAAM, and OIN documentation in the Oracle Technology Network (OTN) Web site.

33.1.1.2 Changing backOfficeURL in Oracle Identity Manager Configuration

Changing backOfficeURL is required only for Oracle Identity Manager deployed in front-office and back-office configuration. This change does not apply for simple clustered or nonclustered deployments. This URL is used internally by Oracle Identity Manager for accessing back-office components from the front-office components. You might change the value of this attribute during the implementation of back-office and front-office configuration, for adding additional servers to back office, and for removing servers from back-office.

To change the value of the backOfficeURL attribute:

1. Login to Enterprise Manager by using the following URL when the WebLogic Administrative Server and Oracle Identity Manager managed servers, at least one of the servers in case of a clustered deployment, are running:

`http://ADMIN_SERVER/em`

2. Navigate to **Identity and Access**, and then **oim**.
3. Right-click **oim**, and navigate to **System MBean Browser**.
4. Under Application Defined MBeans, navigate to **oracle.iam, Application:oim, XMLConfig, Config, XMLConfig.DiscoveryConfig, Discovery**.
5. Enter a new value for the BackOfficeURL attribute, and click **Apply** to save the changes. Example values can be:

t3://mywls1.mydomain.com:8001

t3://mywls1.mydomain.com:8001,mywls2.mydomain.com:9001

Note: The value of the BackOfficeURL attribute must be empty for Oracle Identity Manager nonclustered and clustered deployments.

33.1.2 Oracle Identity Manager Database Host and Port Changes

This section describes the configuration areas where database hostname and port number are used.

After installing Oracle Identity Manager, if there are any changes in the database hostname or port number, then the following changes are required:

Note: Before making changes to the database host and port, shutdown the managed servers hosting Oracle Identity Manager. But you can keep the Oracle WebLogic Administrative Server running.

- **To change datasource oimJMSStoreDS configuration:**
 1. Navigate to **Services, JDBC, Data Sources**, and then **oimJMSStoreDS**.
 2. Click the **Connection Pool** tab.
 3. Modify the values of the **URL** and **Properties** fields to reflect the changes to database host and port.
- **To change datasource oimOperationsDB configuration:**
 1. Navigate to **Services, JDBC, Data Sources**, and then **oimOperationsDB**.
 2. Click the **Connection Pool** tab.
 3. Modify the values of the **URL** and **Properties** fields to reflect the changes to database host and port.
- **To change the datasource related to Oracle Identity Manager Meta Data Store (MDS) configuration:**
 1. Navigate to **Services, JDBC, Data Sources**, and then **mds-oim**.
 2. Click the **Connection Pool** tab.
 3. Modify the values of the **URL** and **Properties** fields to reflect the changes in the database host and port.
- **To change OIMAuthenticationProvider configuration:**
 1. In the WebLogic Administrative console, navigate to **Security Realms, myrealm**, and then **Providers**.
 2. Click **OIMAuthenticationProvider**.

3. Click **Provider Specific**.
4. Modify the value of the DBUrl field to reflect the change in hostname and port.

Note: If Service Oriented Architecture (SOA) and Oracle Web Services Manager (OWSM) undergo configuration changes, then you must make similar changes for datasources related to SOA or OWSM.

After making changes in the datasources, restart the Oracle WebLogic Administrative Server, and start the Oracle Identity Manager managed WebLogic servers.

Note: Whenever Oracle Identity Manager application configuration information is to be changed by using OIM App Config MBeans from the Enterprise Management (EM) console, at least one of the Oracle Identity Manager Managed Servers must be running. Otherwise, you cannot figure out any of the OIM App Config MBeans from the EM console.

- **To change DirectDB configuration:**
 1. Login to Enterprise Manager by using the following URL:
http://ADMIN_SERVER/em
 2. Navigate to **Identity and Access**, and then **oim**.
 3. Right-click **oim**, and navigate to **System MBean Browser** under Application Defined MBeans.
 4. Navigate to **oracle.iam, Application:oim, XMLConfig, Config, XMLConfig,DirectDBConfig**, and then **DirectDB**.
 5. Enter the new value for the URL attribute to reflect the changes to host and port, and then apply the changes.

Note: When Oracle Identity Manager single instance deployment is changed to Oracle Real Application Clusters (Oracle RAC) or Oracle RAC is changed to single instance deployment, change the oimJMSStoreDS, oimOperationsDB, and mds-oim datasources. In addition to the generic changes to make these datasources to multidatasource configuration, change the OIMAuthenticationProvider and domain credential store configurations to reflect the Oracle RAC URL. For information about these generic changes, see *Oracle Fusion Middleware High Availability Guide*.

See "[Oracle Identity Manager Database Host and Port Changes](#)" on page 33-3 for information about changing the port at the database.

33.1.3 Oracle Virtual Directory Host and Port Changes

When LDAP synchronization is enabled, Oracle Identity Manager connects with directory servers through Oracle Virtual Directory (OVD). This connection takes place by using LDAP/LDAPS protocol.

To change OVD host and port:

1. Login to Oracle Identity System Administration.
2. Under Configuration, click **IT Resource**.
3. From the IT Resource Type list, select **Directory Server**, and click **Search**.
4. Edit the Directory Server IT resource. To do so:
 - a. If the value of the Use SSL field is set to `False`, then edit the Server URL field. If the value of the Use SSL field is set to `True`, then edit the Server SSL URL field.
 - b. Click **Update**.

See Also: See "[Updating Oracle Identity Manager for OVD Host/Port](#)" on page 33-30 for information about changing OVD port at OVD/LDAP server.

33.1.4 BI Publisher Host and Port Changes

BI Publisher can be accessed by clicking a simple link from Oracle Identity Manager UI for reporting purposes. This URL is based on the configuration value on Oracle Identity Manager side. If there is host and port changes for BI Publisher, then the following change must be made in Oracle Identity Manager:

1. Login to Enterprise Manager by using the following URL when the WebLogic Administrative Server and Oracle Identity Manager managed servers, at least one of the servers in case of a clustered deployment, are running:
`http://ADMIN_SERVER/em`
2. Navigate to **Identity and Access, oim**.
3. Right-click **oim**, and navigate to **System MBean Browser**.
4. Under Application Defined MBeans, navigate to **oracle.iam, Application:oim, XMLConfig, Config, XMLConfig.DiscoveryConfig, Discovery**.
5. Enter a new value for the BIPublisherURL attribute, and click **Apply** to save the changes.

33.1.5 SOA Host and Port Changes

To change the SOA host and port:

Note: When additional SOA nodes are added or removed, perform this procedure to change the SOA host and port.

1. Login to Enterprise Manager by using the following URL when the WebLogic Administrative Server and Oracle Identity Manager managed servers, at least one of the servers in case of a clustered deployment, are running:
`http://ADMIN_SERVER/em`
2. Navigate to **Identity and Access, oim**.
3. Right-click **oim**, and navigate to **System MBean Browser**.
4. Under Application Defined MBeans, navigate to **oracle.iam, Application:oim, XMLConfig, Config, XMLConfig.SOAConfig, SOAConfig**.

5. Change the value of the Rmiurl attribute, and click **Apply** to save the changes.
The Rmiurl attribute is used for accessing SOA EJBs deployed on SOA managed servers. This is the application server URL. For a clustered deployment of Oracle Identity Manager, it is a comma-separated list of all the SOA managed server URLs. Example values for this attribute can be:
t3://mysoa1.mydomain.com:8001
t3s://mysoaserver1.mydomain.com:8002,mysoa2.mydomain.com:8002
t3://mysoa1.mydomain.com:8001,mysoa2.mydomain.com:8002,mysoa3.mydomain.com:8003
6. Change the value of the Soapurl attribute, and click **Apply** to save the changes.
The Soapurl attribute is used for accessing SOA Web services deployed on SOA managed servers. This is the Web server and load balancer URL for a SOA cluster front-ended with Web server and load balancer. It can be application server URL for a single SOA server.
The example values for this attribute can be:
http://myoimsoa.mydomain.com
https://mysoaserver.mydomain.com:8002
7. Change the SOA JNDIProvider host and port. To do so:
 - a. Login to WebLogic Administration Console.
 - b. In the Domain Structure section, navigate to *OIM_DOMAIN*, **Services**, **Foreign JNDI Providers**.
 - c. Click **ForeignJNDIProvider-SOA**.
 - d. In the Configuration tab, verify that the **General** subtab is active.
 - e. Change the value of Provider URL to the Rmiurl provided in Step 5.

33.1.6 OAM Host and Port Changes

To change the OAM host and port:

1. Login to Enterprise Manager by using the following URL when the WebLogic Administrative Server and Oracle Identity Manager managed servers, at least one of the servers for a clustered deployment, are running:
http://ADMIN_SERVER/em
2. Navigate to **Identity and Access**, and then to **oim**.
3. Right-click **oim**, and navigate to **System MBean Browser**.
4. Under Application Defined MBeans, navigate to **oracle.iam**, **Application:oim**, **XMLConfig**, **Config**, **XMLConfig.SSOConfig**, and then **SSOConfig**.
5. Change the values of the AccessServerHost and AccessServerPort attributes and other attributes as required, and click **Apply** to save the changes.

33.2 Password Changes Related to Oracle Identity Manager

Various passwords are used for Oracle Identity Manger configuration because of the architectural and middleware requirements. This section describes the default passwords and ways to make the changes to the password in Oracle Identity Manger

and Oracle WebLogic configuration for any change in the dependent or integrated products.

This section consists of the following topics:

- [Changing Oracle WebLogic Administrator Password](#)
- [Changing Oracle Identity Manager Administrator Password](#)
- [Changing Oracle Identity Manager Administrator Database Password](#)
- [Changing Oracle Identity Manager Database Password](#)
- [Changing Oracle Identity Manager Passwords in the Credential Store Framework](#)
- [Changing OVD Password](#)
- [Changing Oracle Identity Manager Administrator Password in LDAP](#)
- [Unlocking Oracle Identity Manager Administrator Password in LDAP](#)

33.2.1 Changing Oracle WebLogic Administrator Password

To change Oracle WebLogic administrator password:

1. Login to WebLogic Administrative console.
2. Navigate to **Security Realms, myrealm, Users and Groups, weblogic, Password**.
3. In the New Password field, enter the new password.
4. In the Confirm New Password field, re-enter the new password.
5. Click **Apply**.

Weblogic credentials must be updated in the following places:

1. Foreign JNDI Provider. To do so:
 - a. Login to WebLogic Administrative Console.
 - b. In the Domain Structure section, navigate to **OIM_DOMAIN, Services, Foreign JNDI Providers**.
 - c. Click **ForeignJNDIProvider-SOA**.
 - d. In the Configuration tab, verify that the General subtab is active.
 - e. Provide weblogic user's new password in the password and confirm password fields.
2. SOAAdminPassword in CSF. See "[Changing Oracle Identity Manager Passwords in the Credential Store Framework](#)" on page 33-12 for details.

33.2.2 Changing Oracle Identity Manager Administrator Password

During Oracle Identity Manager installation, the installer prompts for the Oracle Identity Manager administrator password. If required, you can change the administrator password after the installation is complete. To do so, you must login to Oracle Identity Manager Self Service as Oracle Identity Manager administrator. For information about how to change the administrator password, see "Changing Password" in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

When you change the Oracle Identity Manager system administrator password, you must also update the password in the OIMAdmin key under the oracle.wsm.security map in CSF.

Note: If OAM or OAAM is integrated with Oracle Identity Manager, then you must make corresponding changes in those applications. For more information, refer to OAM and OAAM documentation in the Oracle Technology Network (OTN) Web site by using the following URL:

<http://www.oracle.com/technetwork/indexes/documentation/index.html>

33.2.3 Changing Oracle Identity Manager Administrator Database Password

This section describes resetting Oracle Identity Manager password in the following types of deployments:

- Oracle Identity Manager deployment without LDAP synchronization
- Oracle Identity Manager deployment with LDAP synchronization enabled
- Oracle Identity Manager deployment that is integrated with Access Manager (OAM)

Resetting System Administrator password can be performed by using the `oimadminpasswd_wls.sh` utility, which is available in the `OIM_HOME/server/bin/` directory. The steps to run the `oimadminpasswd_wls.sh` utility are the same for both types of deployment: Oracle Identity Manager with LDAP synchronization enabled and without LDAP synchronization enabled.

This section describes resetting Oracle Identity Manager password in the following topics:

- [Resetting System Administrator Database Password in Oracle Identity Manager Deployment](#)
- [Resetting System Administrator Database Password When Oracle Identity Manager Deployment is Integrated With Access Manager](#)

33.2.3.1 Resetting System Administrator Database Password in Oracle Identity Manager Deployment

To reset System Administrator database password:

1. As a prerequisite for running the `oimadminpasswd_wls.sh` utility, open the `OIM_HOME/server/bin/oimadminpasswd_wls.properties` file in a text editor, and set values for the following properties:
 - `JAVA_HOME`: Set this to `jdk6` or later, for example:

```
JAVA_HOME=/opt/softwarewares/shiphome/jdk160_24
```
 - `COMMON_COMPONENTS_HOME`: This is Oracle Middleware common home directory, for example:

```
COMMON_COMPONENTS_HOME=/opt/softwarewares/shiphome/oracle_common
```
 - `OIM_ORACLE_HOME`: This is Oracle Identity Manager Oracle home directory, for example:

```
OIM_ORACLE_HOME=/opt/softwarewares/shiphome/Oracle_IDM1
```
 - `ORACLE_SECURITY_JPS_CONFIG`: Specify the `jps-config-jse.xml` file location present in Oracle Identity Manager Domain, for example:

```
ORACLE_SECURITY_JPS_CONFIG=/opt/software/shiphome/user_projects/domains/base_domain/config/fmwconfig/jps-config-jse.xml
```

- **DOMAIN_HOME:** Specify Oracle Identity Manager Domain Home location of the Weblogic Application Server, for example:

```
DOMAIN_HOME=/opt/software/shiphome/user_projects/domains/base_domain
```

- **DBURL:** Oracle Identity Manager database URL, for example:

```
DBURL=jdbc:oracle:thin:@dbhostname:5521:orclsid
```

- **DBSCHEMAUSER:** Oracle Identity Manager schema username, for example:

```
DBSCHEMAUSER=DEV_OIM
```

- **OIM_OAM_INTG_ENABLED:** Set this to false if Oracle Identity Manager deployment is not integrated with Access Manager, for example:

```
OIM_OAM_INTG_ENABLED=false
```

Note: Other properties, such as LDAPURL, LDAPADMINUSER, and OIM_ADMIN_LDAP_DN can be ignored as they are used only in an integrated setup between Oracle Identity Manager and Access Manager.

2. Go to the `OIM_HOME/server/bin/` directory, and run the following command:

```
sh oimadminpasswd_wls.sh oimadminpasswd_wls.properties
```

The following is a sample output:

```
Enter OIM DB Schema Password :
Enter OIM Administrator xelsysadm new Password:
Re-enter OIM Administrator xelsysadm new Password:
WARNING: Not able to fetch OIMPlatform instance for the given Platform. Hence defaulting to the OIMWebLogicPlatform
```

```
OIM Admin user xelsysadm password reset successfully in OIMDB
```

Note: The warning messages that are displayed while running the `oimadminpasswd_wls.sh` script can be ignored.

33.2.3.2 Resetting System Administrator Database Password When Oracle Identity Manager Deployment is Integrated With Access Manager

If Oracle Identity Manager is integrated with OAM, then LDAP directory, such as Oracle Internet Directory, is used for all authentication purposes. Therefore, Oracle Identity Manager Administrator `xelsysadm` password is reset in LDAP. Although the `xelsysadm` password present in Oracle Identity Manager database is not used in this topology, it is also reset along with LDAP directory to ensure that the passwords in both repositories are in sync.

To reset System Administrator database password when Oracle Identity Manager Deployment is Integrated With Access Manager:

1. As a prerequisite for running the `oimadminpasswd_wls.sh` utility, open the `OIM_HOME/server/bin/oimadminpasswd_wls.properties` file in a text editor, and set values for the following properties:
 - **JAVA_HOME:** Set this to jdk6 or later, for example:
`JAVA_HOME=/opt/softwarewares/shiphome/jdk160_24`
 - **COMMON_COMPONENTS_HOME:** This is Oracle Middleware common home directory, for example:
`COMMON_COMPONENTS_HOME=/opt/softwarewares/shiphome/oracle_common`
 - **OIM_ORACLE_HOME:** This is Oracle Identity Manager Oracle home directory, for example:
`OIM_ORACLE_HOME=/opt/softwarewares/shiphome/Oracle_IDM1`
 - **ORACLE_SECURITY_JPS_CONFIG:** Specify the `jps-config-jse.xml` file location present in Oracle Identity Manager Domain, for example:
`ORACLE_SECURITY_JPS_CONFIG=/opt/softwarewares/shiphome/user_projects/domains/base_domain/config/fmwconfig/jps-config-jse.xml`
 - **DOMAIN_HOME:** Specify Oracle Identity Manager Domain Home location of the Weblogic Application Server, for example:
`DOMAIN_HOME=/opt/softwarewares/shiphome/user_projects/domains/base_domain`
 - **DBURL:** Oracle Identity Manager database URL, for example:
`DBURL=jdbc:oracle:thin:@dbhostname:5521:orclsid`
 - **DBSCHEMAUSER:** Oracle Identity Manager schema username, for example:
`DBSCHEMAUSER=DEV_OIM`
 - **OIM_OAM_INTG_ENABLED:** Set this to true if Oracle Identity Manager deployment is integrated with Access Manager, for example:
`OIM_OAM_INTG_ENABLED=true`
 - **LDAPURL:** LDAP directory URL. Non-SSL port must be specified, for example:
`LDAPURL=ldap://LDAP_HOSTNAME:3060)`
 - **LDAPADMINUSER :** LDAP directory admin username, for example:
`LDAPADMINUSER=cn=orcladmin`
 - **OIM_ADMIN_LDAP_DN:** Oracle Identity Manager Administrator `xelsysadm` complete DN in the LDAP directory, for example:
`OIM_ADMIN_LDAP_DN=cn=xelsysadm,cn=Users,dc=us,dc=mydomain,dc=com`
2. Go to the `OIM_HOME/server/bin/` directory, and run the following command:
`sh oimadminpasswd_wls.sh oimadminpasswd_wls.properties`

The following is a sample output:

```
Enter OIM DB Schema Password :
Enter OIM Administrator xelsysadm new Password:
Re-enter OIM Administrator xelsysadm new Password:
```

WARNING: Not able to fetch OIMPlatform instance for the given Platform. Hence defaulting to the OIMWebLogicPlatform

OIM Admin user xelsysadm password reset successfully in OIMDB
 OIM Admin user cn=xelsysadm,cn=Users,dc=...,dc=...,dc=... password reset successfully in LDAP

Note: The warning messages that are displayed while running the oimadminpasswd_wls.sh script can be ignored.

33.2.4 Changing Oracle Identity Manager Database Password

Oracle Identity Manager uses two database schemas for storing Oracle Identity Manager operational and configuration data. It uses Oracle Identity Manager MDS schema for storing configuration-related information and Oracle Identity Manager schema for storing other information. Any change in the schema password requires changes on Oracle Identity Manager configuration.

Changing Oracle Identity Manager database password involves the following:

Note: Before changing the database password, shutdown the managed servers that host Oracle Identity Manager. However, you can keep the Oracle WebLogic Administrative Server running.

- **To change datasource oimJMSSStoreDS configuration:**
 1. Navigate to **Services, JDBC, Data Sources, oimJMSSStoreDS**.
 2. Click the **Connection Pool** tab.
 3. In the Password and Confirm password fields, enter the new Oracle Identity Manager database schema password.
 4. Click **Save** to save the changes.
- **To change datasource oimOperationsDB configuration:**
 1. Navigate to **Services, JDBC, Data Sources, oimJMSSStoreDS**.
 2. Click the **Connection Pool** tab.
 3. In the Password and Confirm password fields, enter the new Oracle Identity Manager database schema password.
 4. Click **Save** to save the changes.
- **To change datasource related to Oracle Identity Manager MDS configuration:**
 1. Navigate to **Services, JDBC, Data Sources, mds-oim**.
 2. Click the **Connection Pool** tab.
 3. In the Password and Confirm password fields, enter the new Oracle Identity Manager MDS database schema password.
 4. Click **Save** to save the changes.

Note:

- For Oracle Identity Manager deployments with Oracle Real Application Clusters (Oracle RAC) configuration, you might have to make changes in all the datasources under the respective multi-datasource configurations.
 - You might have to make similar changes for datasources related to SOA or OWSM, if required.
-
-

- **To change OIMAuthenticationProvider configuration:**
 1. In the WebLogic Administrative console, navigate to **Security Realms**, **myrealm**, and then **Providers**.
 2. Click **OIMAuthenticationProvider**.
 3. Click **Provider Specific**.
 4. In the DBPassword field, enter the new Oracle Identity Manager database schema password.
 5. Click **Save** to save the changes.
- **To change domain credential store configuration:**
 1. Login to Enterprise Manager by using the following URL:
`http://ADMIN_SERVER/em`
 2. Navigate to **Weblogic Domain**, and then *DOMAIN_NAME*.
 3. Right-click *DOMAIN_NAME*, and select **Security, Credentials**, and then **oim**.
 4. Select **OIMSchemaPassword**, and click **Edit**.
 5. In the Password field, enter the new password, and click **OK**.

After changing the Oracle Identity Manager database password, restart the WebLogic Administrative Server. Start the Oracle Identity manager managed WebLogic Servers as well.

33.2.5 Changing Oracle Identity Manager Passwords in the Credential Store Framework

Oracle Identity Manager installer stores several passwords during the install process. Various values are stored in Credential Store Framework (CSF) as key and value.

[Table 33–1](#) lists the keys and the corresponding values:

Table 33–1 CSF Keys

Key	Description
DataBaseKey	The password for the key used to encrypt database. The password is the user input value in the installer for the Oracle Identity Manager keystore.
.xldatabasekey	The password for keystore that stores the database encryption key. The password is the user input value in the installer for the Oracle Identity Manager keystore.
xell	The password for key 'xell', which is used for securing communication between Oracle Identity Manager components. Default password generated by Oracle Identity Manager installer is xellerate.

Table 33–1 (Cont.) CSF Keys

Key	Description
default_keystore.jks	The password for the default_keystore.jks JKS keystore in the <i>DOMAIN_HOME</i> /config/fmwconfig/ directory. The password is the user input value in the installer for the Oracle Identity Manager keystore.
SOAAdminPassword	The password is user input value in the installer for SOA Administrator Password field.
OIMSchemaPassword	The password for connecting to Oracle Identity Manager database schema. Password is user input value in the installer for OIM Database Schema Password field.
JMSKey	The password is the user input value in the installer for the Oracle Identity Manager keystore.

To change the values of the CSF keys:

1. Login to Oracle Enterprise Manager by navigating to the following URL:
`http://ADMIN_SERVER/em`
2. Navigate to **Weblogic Domain**, *DOMAIN_NAME*.
3. Right-click *DOMAIN_NAME*, and select **Security, Credentials**, and then **oim**.
4. Select the key that you want to modify.

33.2.6 Changing OVD Password

To change the OVD password:

1. Login to Oracle Identity Manager Administration.
2. Click **Advanced**.
3. Under Configuration, click **Manage IT Resource**.
4. From the IT Resource Type list, select **Directory Server**.
5. Click **Search**.
6. Edit the Directory Server IT resource. To do so, in the Admin Password field, enter the new OVD password, and click **Update**.

33.2.7 Changing Oracle Identity Manager Administrator Password in LDAP

To change Oracle Identity Manager System Administrator password in LDAP:

1. Look up the dn for the user from LDAP, as shown:

```
$ORACLE_HOME/bin/ldapsearch -D cn=orcladmin -w fusionapps1 -h localhost -p 6501
-b dc=com "cn=SYS_ADMIN" orclaccountlocked dn
```

Here, *SYS_ADMIN* is the System Administrator user login.

2. Create a file similar to the following:

```
$ more /tmp/resetpassword_SYS_ADMIN
```

```
dn: cn=SYS_ADMIN,cn=Users,dc=us,dc=mydomain,dc=com
changetype: modify
replace: userPassword
userPassword: NEW_PASSWORD
```

Here, *NEW_PASSWORD* is the password that you want in clear text.

3. Change the password, as shown:

```
$ORACLE_HOME/bin/ldapmodify -D cn=orcladmin -w fusionapps1 -h localhost -p 6501
-f /tmp/ resetpassword _SYS_ADMIN
```

4. Verify that the user password is changed, as shown:

```
$ORACLE_HOME/bin/ldapbind -D cn=SYS_ADMIN,cn=Users,dc=us,dc=mydomain,dc=com -w
NEW_PASSWORD -h localhost -p 6501
```

33.2.8 Unlocking Oracle Identity Manager Administrator Password in LDAP

To unlock Oracle Identity Manager System Administrator password in LDAP:

1. Look up the dn for the user from LDAP, as shown:

```
$ORACLE_HOME/bin/ldapsearch -D cn=orcladmin -w fusionapps1 -h localhost -p 6501
-b dc=com "cn=SYS_ADMIN" orclaccountlocked dn
```

If *orclaccountlocked* has a value of 1, then it means that the user is locked.

2. Create a file similar to the following:

```
$ more /tmp/unlock_SYS_ADMIN
```

```
dn: cn=SYS_ADMIN,cn=Users,dc=us,dc=mydomain,dc=com
changetype: modify
replace: orclaccountlocked
orclaccountlocked: 0
```

3. Unlock the user, as shown:

```
$ORACLE_HOME/bin/ldapmodify -D cn=orcladmin -w fusionapps1 -h localhost -p 6501
-f /tmp/unlock_SYS_ADMIN
```

4. Verify that the user is unlocked, as shown:

```
$ORACLE_HOME/bin/ldapsearch -D cn=orcladmin -w fusionapps1 -h localhost -p 6501
-b dc=com "cn=SYS_ADMIN" orclaccountlocked dn
```

The value of *orclaccountlocked* must be 0.

33.3 Configuring SSL for Oracle Identity Manager

This section describes the procedure for generating keys, signing and exporting certificates, setting up SSL Configuration for Oracle Identity Manager and for the components with which Oracle Identity Manager interacts, and establish secure communication between them. It includes the following topics:

- [Generating Keys](#)
- [Signing the Certificates](#)
- [Exporting the Certificate](#)
- [Importing the Certificate](#)
- [Enabling SSL for Oracle Identity Manager and SOA Servers](#)
- [Enabling SSL for Oracle Identity Manager DB](#)

- [Enabling SSL for LDAP Synchronization](#)

Note: Sections "[Generating Keys](#)" on page 33-15 through "[Importing the Certificate](#)" on page 33-16 provide example commands that will be used later in the document. These are for reference and not part of the mandatory steps of configuration.

33.3.1 Generating Keys

You can generate private and public certificate pairs by using the keytool command.

The following command creates an identity keystore (support.jks):

```
$JAVA_HOME/jre/bin/keytool -genkey
-alias support
-keyalg RSA
-keysize 1024
-dname "CN=localhost, OU=Identity, O=Oracle Corporation,C=US"
-keypass KEYSTORE_PASSWORD
-keystore support.jks
-storepass weblogic1
```

Note: Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool argument.

33.3.2 Signing the Certificates

Use the following keytool command to sign the certificates that you created:

```
$JAVA_HOME/jre/bin/keytool -selfcert -alias support
-sialg MD5withRSA -validity 2000 -keypass weblogic1
-keystore support.jks
-storepass KEYSTORE_PASSWORD
```

Note: Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool argument.

33.3.3 Exporting the Certificate

Use the following keytool command to export the certificate from the identity keystore to a file, for example, supportcert.pem:

```
$JAVA_HOME/jre/bin/keytool -export -alias support
-file supportcert.pem
-keypass weblogic1
-keystore support.jks
-storepass KEYSTORE_PASSWORD
```

Note: Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool argument.

33.3.4 Importing the Certificate

Use the following keytool command to import the certificate from a file, such as `wlservercert.pem`, to the identity keystore:

```
$JAVA_HOME/jre/bin/keytool -import -alias serverwl -trustcacerts -file
D:\bea\user_projects\domains\mydomain\wlservercert.pem
-keystore CLIENT_TRUST_STORE -storepass CLIENT_TRUST_STORE_PASSWORD
```

Note: Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool argument.

33.3.5 Enabling SSL for Oracle Identity Manager and SOA Servers

You need to perform the following configurations in Oracle Identity Manager and SOA servers to enable SSL:

- [Enabling SSL for Oracle Identity Manager By Using Default Setting](#)
- [Enabling SSL for Oracle Identity Manager By Using Custom Keystore](#)
- [Changing OimFrontEndURL to Use SSL Port](#)
- [Changing backOfficeURL to Use SSL Port](#)
- [Changing SOA Server URL to Use SSL Port](#)
- [Configuring SSL for Design Console](#)
- [Configuring SSL for Oracle Identity Manager Utilities](#)
- [Configuring SSL for SPML/Callback Domain](#)
- [Connecting Oracle Identity Manager With SOA](#)

33.3.5.1 Enabling SSL for Oracle Identity Manager

Enabling SSL for Oracle Identity Manager is described in the following sections:

- [Enabling SSL for Oracle Identity Manager By Using Default Setting](#)
- [Enabling SSL for Oracle Identity Manager By Using Custom Keystore](#)

33.3.5.1.1 Enabling SSL for Oracle Identity Manager By Using Default Setting

To enable SSL for Oracle Identity Manager and SOA servers by using default setting:

1. Log in to WebLogic Server Administrative console and go to Servers, OIM_SERVER1, General. Under the general section, you can enable ssl port to any value and activate it.
2. The server will start listening and you can access the URL with HTTPS protocol.
3. Perform the same steps for Admin/SOA Servers as Oracle Identity Manager might need to interact with SSL-enabled SOA Server.

33.3.5.1.2 Enabling SSL for Oracle Identity Manager By Using Custom Keystore

To enable SSL for Oracle Identity Manager by using custom keystore:

Note: See ["Generating Keys"](#) on page 33-15 for information about generating custom keys.

1. In the WebLogic Server Administration Console, click **Environment, Servers, Server_Name (OIM_Server1), Configuration, and then General.**
2. Click **Lock & Edit.**
3. Select SSL listen port enabled. The default port is 14001.
4. Select the Keystores tab.
5. From the Keystore list, select **Custom Identity, Java Standard Trust.**
6. In the Custom Identity Keystore field, enter the absolute path of custom identity keystore filename. For example:

DOMAIN_HOME/config/fmwconfig/support.jks

Note: The keystore created at *DOMAIN_HOME*/config/fmwconfig/ by Oracle Identity Manager during installation is default-keystore.jks.

7. Specify JKS as the custom identity keystore type.
8. Type the password (weblogic1) into the Custom Identity Keystore Passphrase and the Confirm Custom Identity Keystore Passphrase fields.
9. Click **Save.**
10. Click the **SSL** tab.
11. Type `support` as the private key alias.
12. Type the password (weblogic1) into the Private Key Passphrase and the Confirm Private Key Passphrase fields.
13. Click **Save.**
14. Click **Activate changes.**
15. Restart all servers for these changes to take effect.
16. Import the certificate that you exported in ["Exporting the Certificate"](#) on page 33-15 into the SPML client truststore.

See ["Importing the Certificate"](#) on page 33-16 for information about importing the certificate.

After enabling SSL on Oracle Identity Manager and SOA Servers, perform the following changes for establishing secured communication between them:

- [Changing OimFrontEndURL to Use SSL Port](#)
- [Changing backOfficeURL to Use SSL Port](#)
- [Changing SOA Server URL to Use SSL Port](#)

33.3.5.2 Changing OimFrontEndURL to Use SSL Port

OimFrontEndURL is used to access the oim application UI. This can be a load balancer URL or web server URL (in case application server is fronted with load balancer or web server) or single application server URL. This is generally used by Oracle Identity Manager in the notification emails or to send a call back web service from SOA to Oracle Identity Manager.

To change the OimFrontEndURL to use SSL port:

1. When the WebLogic admin and Oracle Identity Manager managed servers (at least one of the servers in case of cluster) are running, log in to Enterprise Manager (EM).

For example:

`http://<AdminServer>/em`

2. Navigate to Identity and Access, Oracle Identity Manager.
3. Right click and select System MBean Browser.
4. Under Application Defined MBeans, navigate to oracle.iam, Application:oim, XMLConfig, Config, XMLConfig.DiscoveryConfig, Discovery.
5. Enter a new value for the "OimFrontEndURL" attribute and click **Apply** to save the changes.

For example:

`http://myoim.mydomain.com`

`https://myoim.mydomain.com`

`http://myoimserver.mydomain.com:14002`

Note: Fusion Apps or SPML clients store Oracle Identity Manager URL for invoking SPML and also send callback response. Therefore, there will be changes needed corresponding to this. Also, if Oracle Identity Manager is integrated with OAM/OAAM/OIN, there may be corresponding changes necessary. Refer to [Chapter 32, "Integrating with Other Oracle Components"](#) for detailed information about the integration with other components.

33.3.5.3 Changing backOfficeURL to Use SSL Port

backOfficeURL change is required only for Oracle Identity Manager deployed in front-office/back-office configuration. For simple cluster or non-cluster installations the following does not apply. This URL is used internally by Oracle Identity Manager for accessing back-office components from the front-office components. This value needs to be changed initially during the implementation of back-office/front-office configuration, for adding additional servers to back office, and for removing servers from back-office.

To change the backOfficeURL to use SSL port:

1. When the WebLogic admin and Oracle Identity Manager managed servers (at least one of the servers in case of cluster) are running, log in to Enterprise Manager (EM).

For example:

`http://<AdminServer>/em`

2. Navigate to Identity and Access, Oracle Identity Manager.
3. Right click and select System MBean Browser.
4. Under Application Defined MBeans, navigate to oracle.iam, Application:oim, XMLConfig, Config, XMLConfig.DiscoveryConfig, Discovery.
5. Enter a new value for the "backOfficeURL" attribute and click **Apply** to save the changes.

For example:

t3://mywls1.mydomain.com:8001

t3://mywls1.mydomain.com:8001,mywls2.mydomain.com:9001

Note: For simple cluster and non-cluster installations the value must be empty.

33.3.5.4 Changing SOA Server URL to Use SSL Port

To change SOA server URL to use SSL port:

1. When the admin server and Oracle Identity Manager managed servers are running, log in to Enterprise Manager (EM).

For example:

http://ADMINISTRATIVE_SERVER/em

2. Navigate to Identity and Access, Oracle Identity Manager.
3. Right click and select System MBean Browser.
4. Under Application Defined MBeans, navigate to oracle.iam, Application:oim, XMLConfig, Config, XMLConfig.SOAConfig, SOAConfig.
5. Change the values of the Rmiurl attribute.

Note: Rmiurl is used for accessing SOA EJBs deployed on SOA managed servers.

This is the application server URL. For clustered installation, it is a comma separated list of all the SOA managed server URLs.

For example:

t3://mysoa1.mydomain.com:8001

t3s://mysoaserver1.mydomain.com:8002

t3://mysoa1.mydomain.com:8001,mysoa2.mydomain.com:8002,mysoa3.com:8003

6. Change the value of the Soapurl attribute. For example:

http://myoimsoa.mydomain.com

https://mysoa.mydomain.com: 8001

Note: Soapurl is used to access SOA web services deployed on SOA managed servers. This is the web server/load balancer URL, in case of a SOA cluster front ended with web server/load balancer. In case of single SOA server, it can be application server URL.

7. Click **Apply** to save the changes.

33.3.5.5 Configuring SSL for Design Console

To change the Design console to establish secure connection between Oracle Identity Manager and Design console:

1. Generate and make sure that wlfullclient.jar is in the `$OIM_HOME/designconsole/ext/` directory. To do so:

- a. Go to the `WL_HOME/server/lib/` directory.
- b. Run the following command:

```
java -jar wlfullclient.jar
```

- c. Copy wlfullclient.jar from:

```
$WL_HOME/server/lib/
```

To:

```
$OIM_HOME/designconsole/ext/
```

2. Copy webserviceclient+ssl.jar from:

```
$WL_HOME/server/lib
```

to

```
$OIM_HOME/designconsole/ext/
```

3. Copy OIMMiddleware/modules/cryptoj.jar to the `OIM_HOME/designconsole/ext/` directory.

4. Edit the `$DESIGN_CONSOLE_HOME/config/xlconfig.xml` file. Make the following changes:

Change:

```
<Discovery>
  <CoreServer>
    <java.naming.provider.url>t3://HOST_NAME:PORT_NUMBER/oim</java.naming.provider.url>
    <java.naming.factory.initial>weblogic.jndi.WLInitialContextFactory</java.naming.factory.initial>
  </CoreServer>
</Discovery>
```

To:

```
<Discovery>
  <CoreServer>
    <java.naming.provider.url>t3s://HOST_NAME:OIM_SSL_PORT/oim</java.naming.provider.url>
    <java.naming.factory.initial>weblogic.jndi.WLInitialContextFactory</java.naming.factory.initial>
  </CoreServer>
</Discovery>
```

Change:

```
<ApplicationURL>http://HOST_NAME:PORT_NUMBER/xlWebApp/loginWorkflowRenderer.do<
/ApplicationURL>
```

To:

```
<ApplicationURL>https://HOST_NAME:OIM_SSL_PORT/xlWebApp/loginWorkflowRenderer.d
o</ApplicationURL>
```

5. Use the Server trust store in the Design console. To access this:
 - a. Go to WebLogic Server Administrative console, Environment, Servers.
 - b. Click on <OIM_SERVER_NAME> to view details of the Oracle Identity Manger server.
 - c. Click the KeyStores tab and note down the "Trust keystore" location in the "Trust" section.
 - d. If the Design Console is deployed on the Oracle Identity Manager host, then set the TRUSTSTORE_LOCATION environment variable to the location of the "Trust keystore" location noted above. For example:

```
setenv TRUSTSTORE_LOCATION WL_HOME/server/lib/DemoTrust.jks
```

- e. If the Design Console is deployed on a different host than Oracle Identity Manager, then copy the "Trust keystore" to the host on which Design Console is deployed, and set the TRUSTSTORE_LOCATION env variable to the location where "Trust keystore" is copied on the local host. For example:

```
setenv TRUSTSTORE_LOCATION OIM_HOME/designconsole/DemoTrust.jks
```

6. If `$DESIGN_CONSOLE_HOME/config/xl.policy` does not contain the default grant policy for all, then add the following permission for `cryptoj.jar` at the end of the file, as shown:

```
grant codeBase "file:DIRECTORY_PATH_TO_cryptoj.jar" {
    permission java.security.AllPermission;
};
```

Copy `$MW_HOME/modules/cryptoj.jar` to the `$OIM_HOME/designconsole/ext/` directory.

Note: Here, copying `$MW_HOME/modules/cryptoj.jar` to the `$OIM_HOME/designconsole/ext/` directory is a mandatory step. Setting the permission is necessary if `xl.policy` does not contain the default grant policy for all.

33.3.5.6 Configuring SSL for Oracle Identity Manager Utilities

Oracle Identity Manager client utilities include PurgeCache, GenerateSnapshot, UploadJars, and UploadResources.

Set the TRUSTSTORE_LOCATION environment variable to the location of the "Trust keystore" location.

Note: See ["Configuring SSL for Design Console"](#) on page 33-20 for details about setting the TRUSTSTORE_LOCATION environment variable to the location of the 'Trust keystore' location.

For example:

```
setenv TRUSTSTORE_LOCATION WL_HOME/server/lib/DemoTrust.jks
```

33.3.5.7 Configuring SSL for SPML/Callback Domain

To configure SSL for SPML/callback domain:

1. Ensure that Oracle Identity Manager port is SSL enabled with HostName verification set to false.
2. Enable SSL on Fusion Applications including callback domain.

See Also: ["Enabling SSL for Oracle Identity Manager By Using Custom Keystore"](#) on page 33-17 for information about enabling SSL for Oracle Identity Manager by using custom keystore

3. If you are using WebLogic default trust store, you must not change anything other than enabling the SSL mode.
4. If you have certificates other than default, then the trusted certificates should be exchanged between them to establish two-way trust. See ["Signing the Certificates"](#) on page 33-15 and ["Exporting the Certificate"](#) on page 33-15 for information about signing and exporting certificates.

See Also: ["Configuring SSL"](#) in the *Oracle Fusion Middleware Securing Oracle WebLogic Server* for detailed information about configuring SSL for Oracle WebLogic Server

5. If you are using a stand-alone client for sending SPML requests for testing purpose, then you must:
 - a. Add the following system properties to SPML client command to send the request to SSL enabled OIM port.
 - Djavax.net.ssl.trustStore=D:\Oracle\Middleware1\wlserver_10.3\server\lib\DemoTrust.jks

Note: Change the value of the Djavax.net.ssl.trustStore parameter to point to the truststore used to configure SSL.

See ["Configuring SSL for Design Console"](#) on page 33-20 for information about the location of the trust store used in WebLogic to configure SSL.

- -Djava.protocol.handler.pkgs=weblogic.net
- -Dweblogic.security.TrustKeyStore=DemoTrust

- b. Add webserviceclient+ssl.jar to your client classpath.

33.3.5.8 Connecting Oracle Identity Manager With SOA

SOA can connect to Oracle Identity Manager via web services. If web service invocation fails, then SOA cannot connect to Oracle Identity Manager, and as a result, requests can be stuck. For example, after a create user request is approved at request level, the request might be stuck because the corresponding SOA composite is not able to invoke the request web service deployed on Oracle Identity Manager server, which is SSL enabled. To avoid such issues, in `setDomainEnv.sh`, set `JAVA_OPTIONS`. For example:

```
-Djavax.net.ssl.trustStore=WL_HOME/server/lib/DemoTrust.jks
```

33.3.6 Enabling SSL for Oracle Identity Manager DB

You need to perform the following configurations to enable SSL for Oracle Identity Manager DB:

- [Setting Up DB in Server-Authentication SSL Mode](#)
- [Creating KeyStores and Certificates](#)
- [Updating Oracle Identity Manager](#)
- [Updating WebLogic Server](#)

33.3.6.1 Setting Up DB in Server-Authentication SSL Mode

To set up DB in Server-Authentication SSL mode:

1. Stop the DB server and the listener.
2. Configuring the `listener.ora` file as follows:
 - a. Navigate to the path:


```
$DB_ORACLE_HOME/network/admin
```

 directory
 For example:


```
/scratch/user1/production-database/product/11.1.0/db_1/network/admin
```
 - b. Edit the `listener.ora` file to include SSL listening port and Server Wallet Location.

The following is the sample `listener.ora` file:

```
# listener.ora Network Configuration File: DB_HOME/listener.ora
# Generated by Oracle configuration tools.

SSL_CLIENT_AUTHENTICATION = FALSE

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = DB_HOME/server_keystore_ssl.p12)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCPS) (HOST = server1.mycompany.com) (PORT =
2484))
```

```

        )
        (DESCRIPTION =
          (ADDRESS = (PROTOCOL = TCP) (HOST = server1.mycompany.com) (PORT =
1521))
        )
      )

TRACE_LEVEL_LISTENER = SUPPORT

```

3. Configure the sqlnet.ora file as follows:

a. Navigate to the path:

`$DB_ORACLE_HOME/network/admin` directory

For example:

`/scratch/user1/production-database/product/11.1.0/db_1/network/admin`

b. Edit sqlnet.ora file to include:

- TCPS Authentication Services
- SSL_VERSION
- Server Wallet Location
- SSL_CLIENT_AUTHENTICATION type (either true or false)
- SSL_CIPHER_SUITES that can be allowed in the communication (optional)

The following is the sample sqlnet.ora file:

```

# sqlnet.ora Network Configuration File: DB_HOME/sqlnet.ora
# Generated by Oracle configuration tools.

SQLNET.AUTHENTICATION_SERVICES= (BEQ, TCPS)

SSL_VERSION = 3.0

SSL_CLIENT_AUTHENTICATION = FALSE

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = DB_HOME/server_keystore_ssl.p12)
    )
  )

```

4. Configure the tnsnames.ora file as follows:

a. Navigate to the path:

`$DB_ORACLE_HOME/network/admin` directory

For example:

`/scratch/user1/production-database/product/11.1.0/db_1/network/admin`

b. Edit the tnsnames.ora file to include SSL listening port in the description list of the service.

The following is the sample tnsnames.ora file:

```

# tnsnames.ora Network Configuration File: DB_HOME/tnsnames.ora

```

```
# Generated by Oracle configuration tools.

PRODDB =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCPS) (HOST = server1.mycompany.com) (PORT =
2484))
      (CONNECT_DATA =
        (SERVER = DEDICATED)
        (SERVICE_NAME = proddb)
      )
    )
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = server1.mycompany.com) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = proddb)
    )
  )
)
```

5. Start/Stop utilities for DB server.
6. Start the DB server.

33.3.6.2 Creating KeyStores and Certificates

You can create server side and client side KeyStores using the orapki utility. This utility will be shipped as a part of Oracle DB installation.

KeyStores could be of any format such as JKS and PKCS12. The format of keystore changes based on the provider implementation. For example, JKS is the implementation provided by Sun Oracle whereas PKCS12 is implemented by OraclePKIProvider.

Only JKS client KeyStore is used in Oracle Identity Manager for DB server. This is because using non-JKS KeyStores format such as PKCS12 requires significant changes on the installer side at the critical release time. However, Oracle Identity Manager already has a KeyStore named default-KeyStore.jks, which is in JKS format.

The following are the KeyStores that you can create using orapki utility:

- [Creating a Root CA Wallet](#)
- [Creating DB Server Side Wallet](#)
- [Creating Client Side Wallet](#)

Note: Wallets and KeyStores are interchangeably used and they both mean the same. These refer to a repository of public/private keys and self-signed/trusted certificates.

Creating a Root CA Wallet

To create a root certification authority (CA) wallet:

1. Navigate to the following path:

\$DB_ORACLE_HOME/bin directory

2. Create a wallet by using the command:

```
./orapki wallet create -wallet CA_keystore.p12 -pwd KEYSTORE_PASSWORD
```

3. Add a self signed certificate to the CA wallet by using the command:

```
./orapki wallet add -wallet CA_keystore.p12 -dn 'CN=root_test,C=US' -keysize 2048 -self_signed -validity 3650 -pwd KEYSTORE_PASSWORD
```

4. View the wallet using the command:

```
./orapki wallet display -wallet CA_keystore.p12 -pwd KEYSTORE_PASSWORD
```

5. Export the self signed certificate from the CA wallet using the command:

```
./orapki wallet export -wallet CA_keystore.p12 -dn 'CN=root_test,C=US' -cert self_signed_CA.cert -pwd KEYSTORE_PASSWORD
```

Creating DB Server Side Wallet

To create a DB server side wallet:

1. Create a server wallet using the command:

```
./orapki wallet create -wallet server_keystore_ssl.p12 -auto_login -pwd KEYSTORE_PASSWORD
```

2. Add a certificate request to the server wallet using the command:

```
./orapki wallet add -wallet server_keystore_ssl.p12/ -dn 'CN=Customer,OU=Customer,O=Customer,L=City,ST=NY,C=US' -keysize 2048 -pwd KEYSTORE_PASSWORD
```

3. Export the certificate request to a file, which will be used later for getting it signed using the root CA signature:

```
./orapki wallet export -wallet server_keystore_ssl.p12/ -dn 'CN=Customer,OU=Customer,O=Customer,L=City,ST=NY,C=US' -request server_creq.csr -pwd KEYSTORE_PASSWORD
```

4. Get the server wallet's certificate request signed using the CA signature:

```
./orapki cert create -wallet CA_keystore.p12 -request server_creq.csr -cert server_creq_signed.cert -validity 3650 -pwd KEYSTORE_PASSWORD
```

5. View the signed certificate using the command:

```
/orapki cert display -cert server_creq_signed.cert -complete
```

6. Import the trusted certificate in to the server wallet using the command:

```
./orapki wallet add -wallet server_keystore_ssl.p12 -trusted_cert -cert self_signed_CA.cert -pwd KEYSTORE_PASSWORD
```

7. Import this newly created signed certificate (user certificate) to the server wallet using the command:

```
./orapki wallet add -wallet server_keystore_ssl.p12 -user_cert -cert server_creq_signed.cert -pwd KEYSTORE_PASSWORD
```

Creating Client Side Wallet

To create a client side (Oracle Identity Manager server) wallet:

1. Create a client keystore using default-keystore.jks keystore which is populated in the following path:

DOMAIN_HOME/config/fmwconfig

Note: You can also use Oracle PKCS12 wallet as the client keystore.

2. Import the self-signed CA trusted certificate that you have already exported using the server side commands, to the client keystore (default-keystore.jks) by using the command:

```
JAVA_HOME/jre/bin/keytool -import -trustcacerts -alias dbtrusted -noprompt
-keystore default-keystore.jks -file self_signed_CA.cert -storepass xellerate
```

33.3.6.3 Updating Oracle Identity Manager

You need to perform the following steps in Oracle Identity Manager to enable Oracle Identity Manager and Oracle Identity Manager DB in SSL mode for a secure communication:

1. Import the trusted certificate into the default-keystore.jks keystore of Oracle Identity Manager.
2. Log in to Enterprise Manager.
3. Navigate to Identity and Access, OIM.
4. Right click and navigate to System MBean Browser.
5. Under Application Defined MBeans, navigate to oracle.iam, Application:oim, XMLConfig, Config, XMLConfig.DirectDBConfig, and DirectDB.
6. Change the values for attributes "Sslenabled", "Url" and click **Apply**. If SSL mode is enabled for DB, then "Url" should contain TCPS enables and SSL port in it.

For example:

```
url="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=
my.domain.com)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=proddb)))"
```

7. Restart the Oracle Identity Manager server.

33.3.6.4 Updating WebLogic Server

After enabling SSL for Oracle Identity Manager DB, you need to change the following Oracle Identity Manager datasources and authenticators to use DB SSL port:

- [Updating Datasource oimJMSStoreDS Configuration](#)
- [Updating Datasource oimOperationsDB Configuration](#)
- [Updating Datasource Related to Oracle Identity Manager MDS Configuration](#)
- [Updating Oracle Identity Manager Authenticators](#)

Note: Before performing changes to database host/port, you must shutdown the managed servers hosting Oracle Identity Manager application. However, you can keep the WebLogic Admin Server up and running.

Updating Datasource oimJMSStoreDS Configuration

To update the datasource oimJMSStoreDS configuration:

1. Log in to WebLogic Server.
2. Navigate to Services, JDBC, Data Sources, oimJMSStoreDS.
3. Click the **Connection Pool** tab.
4. Change the value of the URL to reflect the changes to SSI DB host/port, similar to the following example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=myhost.mydomain.com)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=myhost1.mydomain.com)))
```

5. Update Properties to add the following SSL-related properties:

```
javax.net.ssl.trustStore=DOMAIN_HOME/default-keystore.jks
javax.net.ssl.trustStoreType=JKS
EncryptionMethod=SSL
oracle.net.ssl_version=3.0
javax.net.ssl.trustStorePassword=PASSWORD
```

Updating Datasource oimOperationsDB Configuration

To update the Change Datasource oimOperationsDB Configuration:

1. Log in to WebLogic Server.
2. Navigate to Services, JDBC, Data Sources, oimJMSStoreDS.
3. Click the **Connection Pool** tab.
4. Change the value of the URL to reflect the changes to SSI DB host/port, similar to the following example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=myhost.mydomain.com)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=myhost1.mydomain.com)))
```

5. Update Properties to add the following SSL-related properties:

```
javax.net.ssl.trustStore=DOMAIN_HOME/default-keystore.jks
javax.net.ssl.trustStoreType=JKS
EncryptionMethod=SSL
oracle.net.ssl_version=3.0
javax.net.ssl.trustStorePassword=PASSWORD
```

Updating Datasource Related to Oracle Identity Manager MDS Configuration

To update datasource related to Oracle Identity Manager MDS configuration:

1. Log in to WebLogic Server.
2. Navigate to Services, JDBC, Data Sources, mds-oim.
3. Click the **Connection Pool** tab.
4. Change the value of the URL to reflect the changes to SSI DB host/port, similar to the following example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=myhost.mydomain.com)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=myhost1.mydomain.com)))
```

5. Update Properties to add the following SSL-related properties:

```
javax.net.ssl.trustStore=DOMAIN_HOME/default-keystore.jks
javax.net.ssl.trustStoreType=JKS
EncryptionMethod=SSL
```

```
oracle.net.ssl_version=3.0  
javax.net.ssl.trustStorePassword=PASSWORD
```

Note: You might have to perform similar updates for SOA/OWSM related datasources if required.

Updating Oracle Identity Manager Authenticators

The existing Oracle Identity Manager authenticators in the WebLogic server are configured against Non-SSL DB details and they do not use datasources for communicating with Oracle Identity Manager DB. In order to use SSL DB details in the authenticators, you must perform the following:

1. Ensure that Datasources are configured to SSL.
2. In WebLogic Administrative console, navigate to Security Realms, myrealm, Providers.
3. Remove OIMAuthenticationProvider.
4. Create an authentication provider of type "OIMAuthenticator" and mark the control flag as SUFFICIENT.
5. Create an authentication provider of type "OIMSignatureAuthenticator" and mark the control flag as SUFFICIENT.
6. Reorder the authenticators as:
 - a. DefaultAuthenticator
 - b. OIMAuthenticator
 - c. OIMSignatureAuthenticator
 - d. Other providers if any
7. Restart all servers.

33.3.7 Enabling SSL for LDAP Synchronization

You need to perform the following configurations to enable Oracle Identity Manager to use SSL enabled Oracle Virtual Directory (OVD):

- [Enabling OVD-OID with SSL](#)
- [Updating Oracle Identity Manager for OVD Host/Port](#)
- [Enabling Managed WebLogic Server with SSL](#)

33.3.7.1 Enabling OVD-OID with SSL

To enable OVD-OID with SSL:

1. Log in to the OVD EM console.
2. Expand **Identity and Access** and navigate to ovd1, Administration, Listeners.
3. Click **Create** and enter all the required fields.

Note: You must select the Listener Type as LDAP.

4. Click **OK**.

5. Select the newly created LDAP listener and click **Edit**.
6. In the Edit Listener - OIM SSL ENDPOINT page, edit the newly created LDAP listener.
7. Click **OK**. The SSL Configuration page opens.
8. Select the **Enable SSL** checkbox.
9. In the Advanced SSL Settings section, for SSL Authentication, select **No Authentication**.
10. Click **OK**.
11. Stop and start the OVD server for the changes to take effect.

Note: You must not use the restart option.

33.3.7.2 Updating Oracle Identity Manager for OVD Host/Port

When LDAPSync is enabled, Oracle Identity Manager connects with directory servers through OVD. It connects using ldap/ldaps protocol.

To change OVD host/port:

1. Log in to Oracle Identity System Administration.
2. Navigate to Advanced and click **Manage IT Resource**.
3. Select IT Resource Type as **Directory Server** and click **Search**.
4. In the IT Resource Directory Server, edit "server URL" to include SSL protocol and SSL port details.
5. Ensure that Use SSL is set to true and click **Update**.

33.3.7.3 Enabling Managed WebLogic Server with SSL

To enable Managed WebLogic Server with SSL:

1. In a text editor, open the startManagedWebLogic.sh file.
2. Change the value of ADMIN_URL to point to a SSL URL, as shown in the following example:

```
ADMIN_URL="https://myhost.mydomain.com:7002"
```

3. Save the startManagedWebLogic.sh file.
4. Start all servers.

Managing Identity and Resource Information

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

- [Overview of User Management](#)
- [Managing Organization Information](#)
- [Viewing Resources Allowed or Disallowed for Users](#)
- [Assigning Role Entitlements](#)

34.1 Overview of User Management

The User Management folder provides tools to create and manage information about a company's organizations, users, roles, and resources.

This folder contains the following forms:

- **Organizational Defaults:** Use this form to view records that reflect the internal structure of your organization and to designate information related to these entities.
- **Policy History:** Use this form to view user records that your employees require.
- **Roles:** Use this form to view records for roles, called user groups in earlier releases of Oracle Identity Manager, to whom you can assign some common functionality.

34.2 Managing Organization Information

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

A suborganization is an organization that is a member of another organization, for example, a department in a company. The organization that the suborganization belongs to is referred to as a parent organization.

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

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

Figure 34–1 shows the Organizational Defaults form.

Figure 34–1 Organizational Default Form

Table 34–1 describes the fields of the Organizational Default form.

Table 34–1 Fields of the Organizational Defaults Form

Field Name	Description
Organization Name	Name of the organization.
Type	The classification type of the organization, for example, Company, Department, Branch.
Status	The current status of the organization (Active, Disabled, or Deleted).
Parent Organization	The organization to which this organization belongs. If a parent organization is displayed in this field, this organization is displayed on the Sub Organizations tab for the parent organization. If this field is empty, this organization is a top-level organization.

34.3 Viewing Resources Allowed or Disallowed for Users

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

There are two types of users in Oracle Identity Manager:

- **End-user administrators:** This user can access Oracle Identity Manager Design Console and the Oracle Identity Self Service. The system administrator sets permissions to enable end-user administrators to access a subset of the forms in Oracle Identity Manager Design Console.
- **End-users:** This user can access only the Oracle Identity Self Service and generally has fewer permissions than end-user administrators. Only resource objects that are defined as self-service on the Objects Allowed tab of the user's organization are available for provisioning requests by using Oracle Identity Self Service.

Table 34–2 shows this form.

Figure 34–2 Policy History Form

Table 34–2 describes the fields of the Policy History form.

Table 34–2 Fields of the Policy History Form

Field Name	Description
User ID	The user's Oracle Identity Manager login ID.
First Name	The user's first name.
Middle Name	The user's middle name.
Last Name	The user's last name.
Email Address	The user's e-mail address.
Start Date	The date on which the user's account will be activated.
Status	The current status of the user (Active, Disabled, or Deleted).
Organization	The organization to which the user belongs.
User Type	The user's classification status. Valid options are End-User and End-User Administrator. Only end-user administrators have access to Oracle Identity Manager Design Console.
Employee Type	The employment status of the user at the parent organization (for example, full-time, part-time, intern, and so on).
Manager ID	The user's manager.
End Date	The date on which the user's account will be deactivated.
Created on	The date and time when the user record was created.

34.3.1 Policy History Tab

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

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

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

- **Resource Policy Summary:** Displays resource objects that are allowed or disallowed based on the user's organization and applicable access policies.

- **Not Allowed by Org:** Displays only resource objects that are disallowed, based on the user's organization.
- **Resources by Policy:** Displays a second box that contains the access policies for the user groups to which the user is a member.

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

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

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

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

To view the tracking system:

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

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

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

34.4 Assigning Role Entitlements

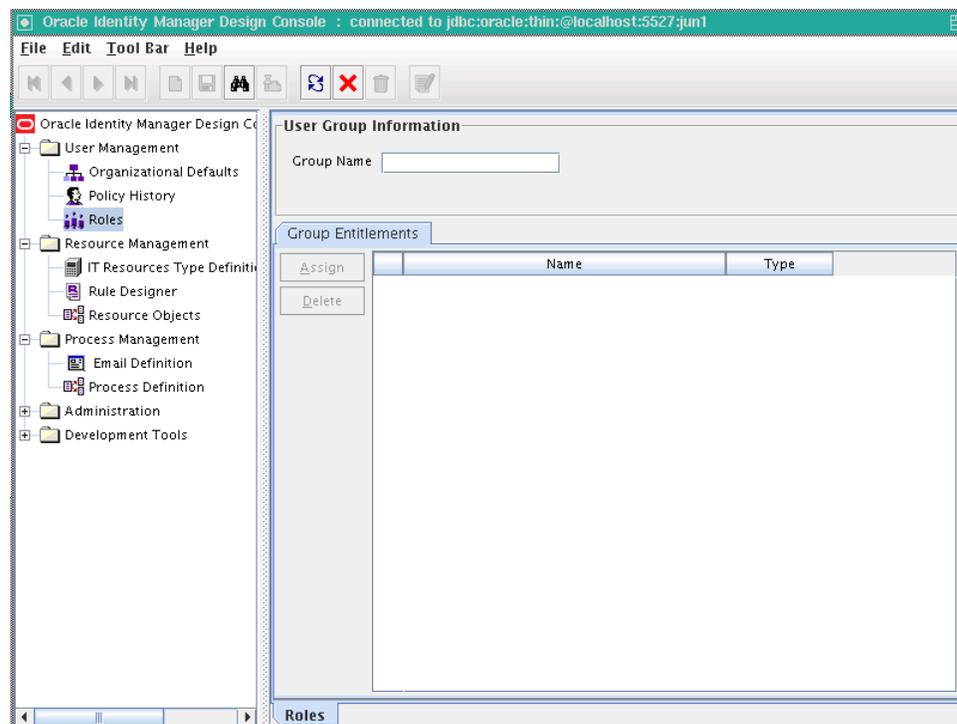
The Group Entitlements form is displayed in the User Management folder. You use it to create and move forms, and to designate the forms and folders that members of a role can access through the Explorer.

To designate forms and folders to roles by using the Group Entitlements form:

1. In the Explorer, double-click **Group Entitlements**.

The User Group Information page is displayed, as shown in [Figure 34-3](#):

Figure 34–3 Roles Form



2. In the **Group Name** field, enter the name of the role.

3. Click **Assign**.

The User Form Assignment lookup table is displayed.

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

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

5. Click **OK**.

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

See Also: "Default Roles" for information about pre-existing roles in Oracle Identity Manager

Securing a Deployment

Securing an Oracle Identity Manager deployment is achieved through authorization and hardening. Authorization controls the access to various components. Hardening secures the components from potential security threats.

Table 35–1 lists the various topics that you can refer for information about securing an Oracle Identity Manager deployment:

Table 35–1 Securing a Deployment

Topic	Topic Type	Information Covered
"Managing the Scheduler" on page 15-1	Hardening	Scheduled tasks and scheduled jobs. Ensure that only required scheduled tasks are enabled.
"System Properties in Oracle Identity Manager" on page 16-1	Hardening	System properties related to system behavior. Ensure that password policies and challenge questions and answers are defined.
"Creating the User Account for Installing Connectors" on page 12-7	Hardening	Specific permissions required to install connectors.
"Enabling Secure Cookies" on page 31-1	Hardening	Enabling Oracle Identity Manager to work over SSL.
"Enabling SSL Between Identity Store Service and the Directory Server" in the <i>Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite</i>	Hardening	Instructions specific to Microsoft Active Directory, iPlanet Directory Server, and Oracle Internet Directory for Identity Store Service
"Configuring LDAP Authentication When LDAP Synchronization is Enabled" in the <i>Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite</i>	Hardening	Enabling LDAP authentication.
"URL Changes Related to Oracle Identity Manager" on page 33-1	Hardening	Steps to make the corresponding changes in Oracle Identity Manager and Oracle WebLogic configuration for any change in the integrated and dependent applications
"Password Changes Related to Oracle Identity Manager" on page 33-6	Hardening	Steps to make the changes to the password in Oracle Identity Manager and Oracle WebLogic configuration for any change in the dependent or integrated products.
"Configuring SSL for Oracle Identity Manager" on page 33-14	Hardening	Securing Oracle Identity Manager by configuring SSL.
"Managing Password Policies" on page 4-1	Hardening	Password policy configuration.
"Adding the Trust Relation" on page 28-2	Hardening	Remote Manager SSL configuration.

Table 35-1 (Cont.) Securing a Deployment

Topic	Topic Type	Information Covered
"Configuring the Remote Manager by Using Your Own Certificate" on page 28-3	Hardening	Remote Manager configuration by using your own certificate instead of the default Oracle Identity Manager certificate.
"Security Architecture" in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i>	Authorization	Authorization and security model in Oracle Identity Manager
"Check Permissions for Roles" in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i>	Authorization	Permissions for role while importing and exporting roles. Check for any errors in setting data object permissions if data object is missing.

See Also: *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* and *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* for information about Oracle Identity Management software integrations and related security aspects

Part XI

Appendixes

This part contains the following appendixes:

- [Appendix A, "Configuring SSO Providers for Oracle Identity Manager"](#)
- [Appendix B, "Localizing Challenge Questions and Responses"](#)

Configuring SSO Providers for Oracle Identity Manager

This appendix contains the configuration steps for enabling Oracle Identity Manager for Single Sign On (SSO). To do so, Oracle Identity Manager is enabled to use third-party SSO providers, such as OpenSSO, IBM Tivoli Access Manager, and CA SiteMinder.

This appendix contains the following sections:

- [Enabling Oracle Identity Manager to Work With OpenSSO](#)
- [Enabling Oracle Identity Manager to Work With IBM Tivoli Access Manager](#)
- [Enabling Oracle Identity Manager to Work With CA SiteMinder](#)
- [Configuring SSO for XIMDD](#)

A.1 Enabling Oracle Identity Manager to Work With OpenSSO

This section contains the following topics:

- [Prerequisites](#)
- [Integrating Oracle Identity Manager with OpenSSO](#)
- [Running Validation Tests to Verify the Configuration](#)

A.1.1 Prerequisites

The prerequisites for integrating Oracle Identity Manager with OpenSSO are:

- Oracle Identity Manager 11g Release 2 (11.1.2.1.0) is installed and running.
- OpenSSO 8.0 is installed and configured
- OpenSSO Enterprise Policy Agent 3.0 for Oracle WebLogic Server/Portal 10 (weblogic_v10_agent_3) is installed.
- It is expected that identity information in Oracle Identity Manager is synchronized with LDAP server configured as user data store in OpenSSO. For example, the LDAP synchronization feature of Oracle Identity Manager can be used for this purpose.

A.1.2 Integrating Oracle Identity Manager with OpenSSO

To integrate Oracle Identity Manager 11g Release 2 (11.1.2.1.0) with OpenSSO 8.0 on Oracle WebLogic Server:

1. Start OpenSSO.
2. Start Oracle Identity Manager.
3. Install OpenSSO policy agent on Admin Server of Oracle Identity Manager domain. To do so:
 - a. Create a J2EE agent profile on OpenSSO. Refer to the policy agent section in OpenSSO documentation for creating the profile.
 - b. Install agent on WebLogic Admin Server. Install the agent by using the agentadmin utility. Refer to the policy agent section in OpenSSO documentation.
4. Install OpenSSO policy agent on Oracle Identity Manager Managed Server of Oracle Identity Manager domain. To do so, install agent on Oracle Identity Manager Managed Server. Refer to the policy agent section of OpenSSO documentation for installing the agent on a managed server. Use the same agent profile that you created in step 3.a.

Note: For a clustered deployment of Oracle Identity Manager, install the policy agent on each Oracle Identity Manager Managed Server.

5. To configure OpenSSO policy agent after installation:

Note: For a clustered deployment of Oracle Identity Manager, OpenSSO policy agent must be configured on each Oracle Identity Manager Managed Server.

- a. Configure WebLogic Server instances with set Agent classpath and JAVA options.
- b. Deploy agent application on Admin and Managed Servers.
- c. Deploy and configure agent authentication provider.
- d. Add WebLogic admin to bypasslist.
- e. Install agent filter to oim web-apps. In this step, add OpenSSO Agent filter to all the Oracle Identity Manager web-apps that support OIM user login. To do so:

Note: The corresponding deployment-descriptors are located at:

IDM_ORACLE_HOME/server/apps/oim.ear/iam-consoles-faces.war/WEB-INF/web.xml

IDM_ORACLE_HOME/server/apps/oracle.iam.console.identity.self-service.ear/oracle.iam.console.identity.self-service.war/WEB-INF/web.xml

IDM_ORACLE_HOME/server/apps/oracle.iam.console.identity.sysadmin.ear/oracle.iam.console.identity.sysadmin.war/WEB-INF/web.xml

- i) Go to the *IDM_ORACLE_HOME*/server/apps/ directory.

ii) Create a backup of the `oim.ear/iam-consoles-faces.war/WEB-INF/web.xml` file, and then edit it to add the filter element as mentioned in OpenSSO documentation. Save the changes.

iii) Create a backup of the `oracle.iam.console.identity.self-service.ear` file, and then extract it in a temporary location. Then extract the `oracle.iam.console.identity.self-service.war` file. Edit `WEB-INF/web.xml` to add the filter element as mentioned in OpenSSO documentation. Repackage `oracle.iam.console.identity.self-service.war` with the modified `web.xml`, and then repackage `oracle.iam.console.identity.self-service.ear` with modified `oracle.iam.console.identity.self-service.war`.

iv) Create a backup of `oracle.iam.console.identity.sysadmin.ear`, and then extract it in a temporary location. Then extract the `oracle.iam.console.identity.sysadmin.war` file. Edit `WEB-INF/web.xml` to add the filter element as mentioned in OpenSSO documentation. Repackage `oracle.iam.console.identity.sysadmin.war` with the modified `web.xml`, and then repackage `oracle.iam.console.identity.sysadmin.ear` with modified `oracle.iam.console.identity.sysadmin.war`.

Note: Ensure that after performing steps iii and iv, the only difference between the modified EAR files and the original EAR files is in the `web.xml` files.

v) Shutdown Oracle Identity Manager instance.

vi) Go to
`OIM_DOMAIN_HOME/servers/OIM_SERVER_INSTANCE/tmp/_WL_user/`
 directory. Go to
`OIM_DOMAIN_HOME\servers\OIM_SERVER_INSTANCE\tmp_WL_user\`
 directory if the setup is on Microsoft Windows.

vii) Delete the directories specific to `oracle.iam.console.identity.self-service.ear` and `oracle.iam.console.identity.sysadmin.ear` UI applications. In a typical Oracle Identity Manager setup, the directories to be deleted are `oracle.iam.console.identity.self-service.ear_V2.0` and `oracle.iam.console.identity.sysadmin.ear_V2.0`.

viii) Restart Oracle Identity Manager Managed Server instance, and then check that the directories are re-created in the directory path mentioned in step vi.

6. Update the agent profile for Oracle Identity Manager Managed Server with Oracle Identity Manager URL information. To do so:

- a. Login to OpenSSO application, and select the Oracle Identity Manager Managed Server agent profile.
- b. Click the **general** tab. Change the Agent filter mode. Remove all existing values. Add new value with empty key and corresponding map value as `J2EE_POLICY`.
- c. Click the **applications** tab. Update the various sections as follows:

– Login Form URI. Add the following:

```
/oim/faces/pages/Login.jspx
/identity/faces/signin
/sysadmin/faces/signin
```

– Login Error URI. Add the following:

```

/identity/faces/signin
/sysadmin/faces/signin
/oim/faces/pages/LoginError.jspx

```

- Not Enforced URI Processing. Add the following:

```

/identity/faces/register
/identity/faces/forgotpassword
/identity/faces/trackregistration
/identity/faces/forgotuserlogin
/identity/faces/accountlocked
/identity/adfAuthentication
/identity/afr/blank.html
/sysadmin/adfAuthentication
/sysadmin/afr/blank.html
/sysadmin/faces/noaccess
/oim/afr/blank.html
/workflowservice/*
/callbackResponseService/*
/spml-xsd/*

```

7. Configure SSO in Oracle Identity Manager. To do so:

- a. Set up WebLogic authenticators. To do so:

i) Add and configure WebLogic authentication provider for LDAP server corresponding to the user data store used by OpenSSO. For example, if OpenSSO uses Sun DSEE, then configure iPlanet authentication provider. Set the control flag as SUFFICIENT.

Note: Ensure that all the Oracle Identity Manager users are synchronized with the LDAP server to which the authenticator points to.

ii) Add and configure Oracle Identity Manager signature authentication provider (OIMSignatureAuthenticator). Set the control flag as SUFFICIENT.

iii) Arrange the authenticator chain in the following order:

- DefaultAuthenticator - SUFFICIENT
- OIMSignatureAuthenticator - SUFFICIENT
- AgentAuthenticator - OPTIONAL
- LDAPAuthenticator - SUFFICIENT
- DefaultIdentityAsserter

- b. Change the Oracle Identity Manager logout to execute OpenSSO logout URL by running the following command:

```

cd <IDM_ORACLE_HOME>/common/bin
./wlst.sh
connect()
addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication",
logouturi="http(s)://openssohost:openssoport/opensso/UI/Logout",
autologinuri="/obrar.cgi")
exit()

```

- c. Set Oracle Identity Manager ssoenabled flag to true. To do so:

- i) Login to Enterprise Manager. Open System Mbean Browser.
 - ii) Open the oracle.iam:Location=oim_server1,name=SSOConfig,type=XMLConfig,SSOConfig,XMLConfig=Config,Application=oim,ApplicationVersion=11.1.1.3.0 mbean.
 - iii) Set the value of ssoEnabled to true.
8. Restart Oracle Identity Manager domain.
 9. Test the configuration by navigating to the following URL:
http://OIM_HOST:OIM_PORT/identity/
 The page is redirected to the OpenSSO login page. Login as valid Oracle Identity Manager user.

A.1.3 Running Validation Tests to Verify the Configuration

Run the following validation steps to verify if the integration between Oracle Identity Manager and OpenSSO is successful:

User Login to Oracle Identity Manager Through SSO

Prerequisite: Create a user, for example ENDUSER001 in Oracle Identity Manager and LDAP.

Step: Try logging in to Oracle Identity Manager through SSO as the user you created, for example ENDUSER001, and check if the login is successful.

Expected output: Login is successful.

Client-Based Login to Oracle Identity Manager

Prerequisite: Make sure that Oracle Identity Manager Design Console is installed and configured.

Step: Try logging in to the Design Console as system administrator with SSO password.

Expected output: Login to the Design Console is successful, assuming that LDAPAuthenticator is configured properly for SSO login.

Signature-Based Authentication

To test signature-based authentication:

1. Try accessing the scheduler service URL. It should be running on Oracle Identity Manager Managed Server port, as shown:

http://OIM_HOST:OIM_PORT/SchedulerService-web

2. Login as system administrator with SSO password.
3. If the login is successful and you can see the following details on the screen, then signature login is successful:

Scheduler Current Status: STARTED

Last Error: NONE

4. Click **Start** on the page if the following is displayed:

Scheduler Current Status: STOPPED

If no errors are displayed on the page, then signature login is successful.

A.2 Enabling Oracle Identity Manager to Work With IBM Tivoli Access Manager

This section contains the following topics:

- [Prerequisites](#)
- [Integrating Oracle Identity Manager with IBM Tivoli Access Manager](#)
- [Running Validation Tests to Validate the Configuration](#)

A.2.1 Prerequisites

The prerequisites for integrating Oracle Identity Manager with OpenSSO are:

- Oracle Identity Manager 11g Release 2 (11.1.2.1.0) is installed.
- IBM Tivoli Access Manager (TAM) for e-business 6.1 is installed.
- IBM Tivoli Access Manager Adapter for Oracle WebLogic Server for TAM 6.1 and Oracle WebLogic Server 10g or 11g are installed.
- The identity information in Oracle Identity Manager is synchronized with identity information in the LDAP registry used by TAM. For example, the LDAP synchronization feature of Oracle Identity Manager can be used for this purpose.
- Form based login is enabled in TAM.

A.2.2 Integrating Oracle Identity Manager with IBM Tivoli Access Manager

To integrate Oracle Identity Manager 11g Release 2 (11.1.2.1.0) with IBM Tivoli Access Manager for e-business 6.1:

1. Start IBM Tivoli Access Manager.
2. Start Oracle Identity Manager.
3. Setup connection between webseal and WebLogic. To do so:
 - a. Create junctions to connect webseal to Oracle Identity Manager WebLogic Server.
 - b. Configure webseal logout and login page.
 - c. Deploy weblogic security providers.

Refer to TAM-weblogic integration documentation provided as part of IBM Tivoli Access Manager Adapter for Oracle WebLogic Server. The additional details are as follows:

- Keep both non-SSL and SSL ports on Oracle Identity Manager into consideration while creating junctions.
- While creating webseal junction(s) for protected resources, make sure to use the "-c iv-user" (insert iv-user HTTP header) option.
- List of resources that needs to be protected/unprotected:

Protect the following resources:

/oim

/xlWebApp

/Nexaweb

/identity

```
/sysadmin
```

Unprotect following uris:

```
/identity/faces/register
```

```
/identity/faces/forgotpassword
```

```
/identity/faces/trackregistration
```

```
/identity/faces/forgotuserlogin
```

```
/identity/faces/accountlocked
```

```
/identity/adfAuthentication
```

```
/identity/afr/blank.html
```

```
/sysadmin/adfAuthentication
```

```
/sysadmin/afr/blank.html
```

```
/sysadmin/faces/noaccess
```

```
/oim/afr/blank.html
```

Unprotect following resources:

```
/workflowservice
```

```
/callbackResponseService
```

```
/spml-xsd
```

- Only configure Tivoli Access Manager Identity assertion provider (AMIdentityAsserterLite). Select the **iv-user** option while configuring it.
- Do not configure Tivoli Access Manager Identity authentication provider.
- Configure WebLogic authentication provider for LDAP server corresponding to the LDAP registry used by TAM. For example, if TAM uses Sun DSEE, then configure iPlanet authentication provider. Set its control flag as SUFFICIENT. Ensure that all users in Oracle Identity Manager are synchronized to this LDAP server. If any Oracle Identity Manager user is not present in the LDAP server, then that user will not be able to login to Oracle Identity Manager.
- Configure Oracle Identity Manager signature authentication provider (OIMSignatureAuthenticationProvider). Provide the Oracle Identity Manager database details while configuring it. You can use the same details as specified in OIMAuthenticationProvider. Set its control flag as SUFFICIENT.
- Arrange the authenticator chain in the following order:
 - TAMIdentityAsserter
 - OIMSignatureAuthenticator - SUFFICIENT
 - LDAPAuthenticator - SUFFICIENT
 - DefaultAuthenticator - SUFFICIENT
 - DefaultIdentityAsserter

4. Change the Oracle Identity Manager logout to execute TAM logout URL by using the following commands:

```
cd <IDM_ORACLE_HOME>/common/bin
```

```
./wlst.sh
connect()
addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication",
logouturi="http(s)://<webseal-host:port>/pkmslogout",
autologinuri="/obrar.cgi")
exit()
```

5. Set OIM ssoenabled flag to true. To do so:
 - a. Login to Enterprise Manager. Open System Mbean Browser.
 - b. Open the oracle.iam:Location=oim_server1,name=SSOConfig,type=XMLConfig,SSOConfig,XMLConfig=Config,Application=oim,ApplicationVersion=11.1.1.3.0 mbean.
 - c. At the value of ssoEnabled to true.
6. Restart Oracle Identity Manager.
7. Test the configuration by navigating to the following URL:

http(s)://WEBSEAL_HOST:WEBSEAL_PORT/identity/faces/home

TAM login page is displayed. Login as valid Oracle Identity Manager user, and the login should be successful.

A.2.3 Running Validation Tests to Validate the Configuration

Run the following validation steps to verify if the integration Oracle Identity Manager and TAM is successful:

User Login to Oracle Identity Manager Through SSO

Prerequisite: Create a user, for example ENDUSER001, in Oracle Identity Manager and LDAP.

Step: Try logging in to Oracle Identity Manager through SSO as the user that you created, for example ENDUSER001, and check if the login is successful.

Expected output: Login should be successful.

Client-Based Single Login to Oracle Identity Manager

Prerequisite: Make sure that Oracle Identity Manager Design Console is installed and configured.

Step: Try logging in to the Design Console as system administrator with SSO password.

Expected output: Login to the Design console must be successful, assuming that LDAPAuthenticator is configured properly for SSO login.

Signature-Based Authentication

To test signature-based authentication:

1. Try accessing the scheduler service URL. It should be running on Oracle Identity Manager Managed Server port, as shown:

http://OIM_HOST:OIM_PORT/SchedulerService-web
2. Login as system administrator by providing SSO password.

3. If the login is successful and you can see the following details on the screen, then signature login is successful:
Scheduler Current Status: STARTED
Last Error: NONE
4. Click **Start** on the page if the following is displayed:
Scheduler Current Status: STOPPED
If there are no errors on the page, then the signature login is successful.

A.3 Enabling Oracle Identity Manager to Work With CA SiteMinder

This section contains the following topics:

- [Prerequisites](#)
- [Integrating Oracle Identity Manager with CA SiteMinder](#)
- [Running Validation Tests to Validate the Configuration](#)

A.3.1 Prerequisites

The prerequisites for integrating Oracle Identity Manager with CA SiteMinder are:

- Oracle Identity Manager is installed.
- Identity information in Oracle Identity Manager is synchronized with identity information in the LDAP registry used by SiteMinder. The LDAP synchronization feature in Oracle Identity Manager can be used for this purpose.

A.3.2 Integrating Oracle Identity Manager with CA SiteMinder

To integrate Oracle Identity Manager with CA SiteMinder:

1. Install SiteMinder WebLogic Agent by referring to SiteMinder installation documentation. Follow install GUI instructions.
2. Edit the setDomainEnv.sh file to set the variables, as shown:

```
ASA_HOME='PATH_TO_SITEMINDER_AGENT_HOME'
export ASA_HOME

SMASA_CLASSPATH="$ASA_HOME/conf:$ASA_HOME/lib/smagentapi.jar:$ASA_HOME/lib/smjava
sdk2.jar:$ASA_HOME/lib/sm_jsafe.jar:$ASA_HOME/lib/smclientclasses.jar:$ASA_HO
ME/lib/sm_jsafeJCE.jar"
export SMASA_CLASSPATH

SM_JAVA_OPTIONS=" -Dmsasa.home=$ASA_HOME"
export SM_JAVA_OPTIONS

CLASSPATH=${SMASA_CLASSPATH}:${CLASSPATH}
export CLASSPATH
```

3. Edit the startWebLogic.sh file to add SM_JAVA_OPTIONS to the JAVA command, as shown:

```
$JAVA_HOME/bin/java ${JAVA_VM} ${MEM_ARGS} -Dweblogic.Name=${SERVER_NAME}
-Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy ${JAVA_OPTIONS}
${SM_JAVA_OPTIONS} ${PROXY_SETTINGS} ${SERVER_CLASS}
```

4. Edit the `ASA_HOME/conf/WebAgent.conf` file to change the value of the `EnableWebAgent` parameter to YES.
5. Restart all Managed and Admin servers.
6. Add/Configure `SiteminderIdentityAsserter` and `SiteminderAuthenticationProvider` in the Weblogic authentication chain. In Identity Asserter common configuration, select `SMSSESSION`.
7. In the Provider Specific subtab, set the "SMIdentity Asserter Config File:" field to `ASA_HOME/conf/WebAgent.conf`.
8. In `SiteminderAuthenticationProvider` 'ProviderSpecific', update "SMAuth Provider Config File:" to `ASA_HOME/conf/WebAgent.conf`.
9. Remove existing `OIMAAuthenticationProvider` from the authentication chain.
10. Add `OIMSignatureAuthenticator` to the authentication chain. Set the control flag to `SUFFICIENT`.
11. Rearrange the authentication chain, as listed in [Table A-1](#):

Table A-1 Authentication Chain

Authentication Provider	Control Flag
<code>SiteminderIdentityAsserter</code>	
<code>DefaultAuthenticator</code>	<code>SUFFICIENT</code>
<code>OIMSignatureAuthenticator</code>	<code>SUFFICIENT</code>
<code>SiteminderAuthenticationProvider</code>	<code>SUFFICIENT</code>
<code>DefaultIdentityAsserter</code>	<code>SUFFICIENT</code>

Note: In the order shown in [Table A-1](#), `OIMAAuthenticationProvider` has been removed. Therefore, all authentication either via browser (`http/https`) or non-`http`, such as Design Console login or `t3/t3s` route, must be handled by Siteminder SSO. Only signature authentication will be handled by Oracle Identity Manager.

12. Restart Admin server and all the Managed Servers in the domain.
13. Configure SSO logout for oim by using the following command:

```
cd <IDM_ORACLE_HOME>/common/bin

./wlst.sh

connect()

addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication",
logouturi="SITEMINDER_LOGOUT_URL", autologinuri="/obrar.cgi")

exit()
```

Note: The `connect()` call will ask for Admin server URL and WebLogic Admin username and password.

14. Set the ssoenabled flag for Oracle Identity Manager to true. To do so:
 - a. Login to Enterprise Manager, and open System MBean Browser.
 - b. Open the oracle.iam:Location=oim_server1,name=SSOConfig,type=XMLConfig,SSOConfig,XMLConfig=Config,Application=oim,ApplicationVersion=11.1.1.3.0 mbean.
 - c. Set the value of ssoEnabled to true.
15. Restart Admin Server and all Managed Servers in the domain.
16. Protect/unprotect the following Oracle Identity Manager resources:
 - Protect following resources:
 - /identity
 - /sysadmin
 - /oim
 - /xlWebApp
 - /Nexaweb
 - Unprotect the following URIs:
 - /identity/faces/register
 - /identity/faces/forgotpassword
 - /identity/faces/trackregistration
 - /identity/faces/forgotuserlogin
 - /identity/faces/accountlocked
 - /identity/adfAuthentication
 - /identity/afr/blank.html
 - /sysadmin/adfAuthentication
 - /sysadmin/afr/blank.html
 - /sysadmin/faces/noaccess
 - /oim/afr/blank.html
 - Unprotect the following resources:
 - /workflowservice
 - /callbackResponseService
 - /spml-xsd
17. To support client-based login to Oracle Identity Manager, the smclientclasses.jar must be added to the client classpath. To set the client classpath:
 - a. Go to the *OIM_ORACLE_HOME*/server/bin/ directory using the cd command.
 - b. Open the setEnv.sh file in VI Editor.
 - c. Add smclientclasses.jar to the CLASSPATH variable at the end. This setting ensures successful client login to Oracle Identity Manager while executing most of the client utilities present in *OIM_ORACLE_HOME*/server/bin.

However, client classpath must be separately set for the Design Console login to work. To do so:

- a. Go to the `OIM_ORACLE_HOME/designconsole` directory.
- b. Open the `classpath.sh` file in VI Editor.
- c. Add `smclientclasses.jar` to the `CLASSPATH` variable at the end.

A.3.3 Running Validation Tests to Validate the Configuration

Run the following validation steps to verify if the integration Oracle Identity Manager and CA SiteMinder is successful:

User Login to Oracle Identity Manager Through SSO

Prerequisite: Create a user, for example `ENDUSER001`, in Oracle Identity Manager and LDAP.

Step: Try logging in to Oracle Identity Manager through SSO as the user that you created, for example `ENDUSER001`, and check if the login is successful.

Expected output: Login should be successful.

Client-Based Login to Oracle Identity Manager

Prerequisite: Make sure that Oracle Identity Manager Design Console is installed and configured.

Step: Try logging in to the Design Console as the system administrator with SSO password.

Expected output: Login to the Design console should be successful, assuming that `SiteminderAuthenticationProvider` is configured properly for SSO login.

Signature-Based Authentication

To test signature-based authentication:

1. Try accessing the scheduler service URL. It should be running on Oracle Identity Manager Managed Server port, as shown:
`http://OIM_HOST:OIM_PORT/SchedulerService-web`
2. Login as system administrator by providing SSO password.
3. If the login is successful and you can see the following details on the screen, then signature login is successful:

Scheduler Current Status: STARTED

Last Error: NONE

4. Click **Start** on the page if the following is displayed:

Scheduler Current Status: STOPPED

If there are no errors on the page, then the signature login is successful.

A.4 Configuring SSO for XIMDD

To configure SSO for XIMDD:

1. Edit the `web.xml` file in XIMDD. To do so:

- a. Locate the XIMDD.ear file on the server. The location is `OIM_ORACLE_HOME/server/webapp/optional/XIMDD.ear`.
 - b. Unjar the XIMDD.ear file at a temporary location. This contains XIMDD.war.
 - c. Untar XIMDD.war, and edit the WEB-INF/web.xml file.
 - d. The login-config section in at the end of the web.xml file. Here, for `<auth-method>`, add CLIENT-CERT in addition to the already present value FORM, as shown:


```
<auth-method>CLIENT-CERT, FORM</auth-method>
```
 - e. Recreate the JAR with the updated web.xml, and pack it in the XIMDD.ear.
2. Deploy the XIMDD.ear. To do so:
 - a. Select the XIMDD.ear from the Deployments screen, and click **Start** to start the application.
 - b. Log in to Oracle WebLogic Administration Console.
 - c. In the left navigation pane, click **Deployments**. It lists all the applications deployed on the server.
 - d. Click **Install**.
 - e. Navigate to the location for deploying the EAR file. Typically, the EAR file is located in the following directory:


```
OIM_ORACLE_HOME/server/webapp/optional/
```
 - f. Select XIMDD.ear from the Current Location panel.
 - g. Click **Next** on the Choose targeting style page.
 - h. Select **OimServer (Oracle Identity Manager Server)** from the Available targets for XIMDD panel, and click **Next**.
 - i. Click **Finish**. The following message appears:

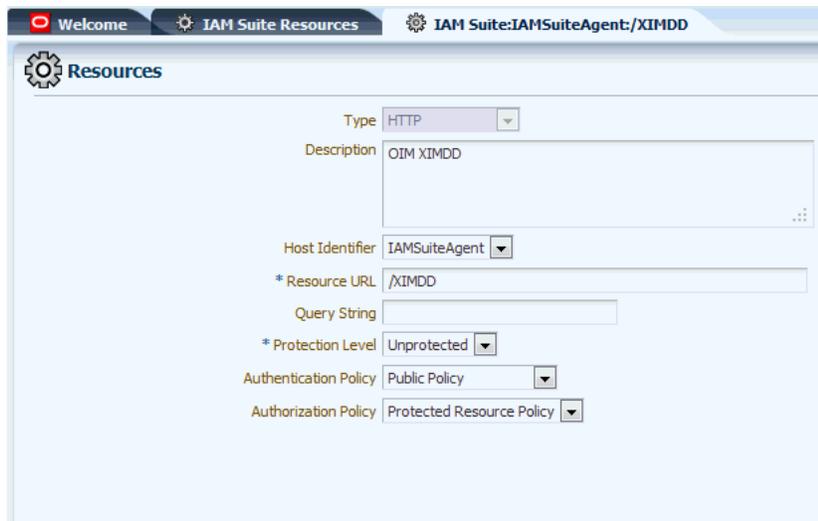

```
All changes have been activated. No restarts are necessary. The deployment has been successfully installed.
```
 - j. Select the XIMDD.ear from the list of applications on the Deployment page. Click **Start** to start the application.
 3. Update the `/u01/ohsauth/ohsauth11g_inst/config/OHS/ohs1/moduleconf/idm.conf` file to add a new section for `/XIMDD`. There are multiple virtual hosts. Add the section for the Admin virtual host, as shown:


```
<Location /XIMDD>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost myhost.mycompany.com
  WebLogicPort 14000

WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>
```
 4. Change the `/XIMDD` to protected resource from `/oamconsole`. To do so:
 - a. Login to the `/oamconsole` as `oamAdminUser`.

- b. Navigate to **Policy Configuration, Application Domains, IAMSuiteAgent, Resources**. Edit the entry for /XIMDD, so that the screen is similar to [Figure A-1](#):

Figure A-1 The Resources Screen



The screenshot shows the 'Resources' configuration page in the IAM Suite. The page has a breadcrumb trail: 'Welcome' > 'IAM Suite Resources' > 'IAM Suite:IAMSuiteAgent:/XIMDD'. The main heading is 'Resources'. The configuration fields are as follows:

- Type: HTTP
- Description: OIM XIMDD
- Host Identifier: IAMSuiteAgent
- * Resource URL: /XIMDD
- Query String: (empty)
- * Protection Level: Unprotected
- Authentication Policy: Public Policy
- Authorization Policy: Protected Resource Policy

- c. From the Protection Level list, select **Protected**, and click **Apply**.
5. Login to /XIMDD. To do so, login to Oracle Identity System Administration as the system administrator. Then, navigate to `http://HOST:PORT/XIMDD`. The Diagnostic Dashboard is displayed after auto login.
6. Run the tests on the Diagnostic Dashboard. For information about the various tests in the Diagnostic Dashboard, see ["Working with the Diagnostic Dashboard"](#) on page 25-1.

Localizing Challenge Questions and Responses

The following default challenge questions are localized automatically in Oracle Identity Manager:

- What is the name of your pet?
- What is the city of your birth?
- What is your favorite color?
- What is your mother's maiden name?

Localized default challenge questions are located in the `CommonModelBundle_LANG.properties` file. Here, *LANG* is the locale code. Depending on the application server on which Oracle Identity Manager is deployed, the `CommonModelBundle_LANG.properties` file is available in one of following locations:

- **For IBM WebSphere Application Server**

To locate the `CommonModelBundle_LANG.properties` file:

1. Navigate to the `OIM_HOME\server\apps\was\lib\oracle.iam.ui.view` directory.
2. Extract the contents of the `adflibCommonModel.jar` file.
3. Navigate to the `oracle/iam/ui/common/model` directory. The `CommonModelBundle_LANG.properties` file is available in this directory.

- **For Oracle WebLogic Application Server**

To locate the `CommonModelBundle_LANG.properties` file:

1. Navigate to the `OIM_HOME/server/apps/oracle.iam.ui.view.war` directory and extract the contents of the WAR file.
2. Navigate to the `WEB-INF/lib` directory and extract the contents of the `adflibCommonModel.jar` file.
3. Navigate to the `oracle/iam/ui/common/model` directory. The `CommonModelBundle_LANG.properties` file is available in this directory.

Note: The CommonModelBundle_LANG.properties file is also available in the `OIM_HOME/server/apps/oracle.iam.ui.model.ear!APP-INF/lib/adflibCommonModel.jar` location. To locate the CommonModelBundle_LANG.properties file, first extract the contents of the EAR file, and then the contents of the CommonModel.jar file.

If you add custom challenge questions to Oracle Identity Manager Design Console for lookup code `Lookup.WebClient.Questions`, then add corresponding properties to the common model bundles to localize the question text in the supported languages. Corresponding translations should be saved to the CommonModelBundle_LANG.properties file.

For example, you might add the new challenge question "What is your favorite sport?". To localize this text, add properties to the property files in the following format:

```
KEY_QUESTION-TEXT?=VALUE
```

Replace any white spaces in the question text with an underscore (`_`). For example, to localize the "What is your favorite sport?" challenge question in French, add the following property to the CommonModelBundle_fr.properties file:

```
KEY_WHAT_IS_YOUR_FAVORITE_SPORT?=Quel est votre sport favori?
```

To modify the text of the default challenge questions, add corresponding properties to the common model bundles (specific to the locale). For example, to modify the text of the "What is your favorite color?" question to use the British spelling (favourite and colour) instead of the American version (favorite and color), modify the following property in the CommonModelBundle_en.properties file:

```
KEY_WHAT_IS_YOUR_FAVORITE_COLOR?=What is your favourite colour?
```

A

- access policies, 3-1
 - creating, 3-7
 - disabling, 3-3
 - evaluating, 3-4
 - features, 3-2
 - managing, 3-10
 - priority, 3-5
 - revoking, 3-3
- access request catalog
 - administering, 17-7
 - bootstrapping, 17-12
 - Catalog System Administrator, 17-7
 - customization, 17-21
 - features, 17-5
 - managing, 17-1
 - security, 17-28
 - troubleshooting, 17-25
- account reconciliation, 13-4
- active reconciliation tables, 20-1
- active task tables, 20-6
- ad-hoc linking, 13-16
- advanced search
 - approval policies, 2-8
 - jobs, 15-24
 - notification templates, 14-14
 - system properties, 16-28
- application instance, 9-1
 - architecture, 9-2
 - attributes, 9-7
 - configuring, 9-15
 - creating, 9-4
 - deleting, 9-10
 - disconnected, 9-4, 10-2
 - entitlements, 9-3
 - forms, 9-12
 - managing, 9-1
 - modifying, 9-7
 - multiple accounts, 9-2
 - searching, 9-5
- approval policies
 - advanced search, 2-8
 - creating, 2-4
 - deleting, 2-9
 - managing, 2-1
 - modify priority, 2-9
 - modifying, 2-8
 - searching, 2-7
 - simple search, 2-7
- approval policy, 2-1
- approvals
 - selection methodologies, 2-2
- archival utilities, 20-1
 - Reconciliation Archival utility, 20-1
 - Requests Archival utility, 20-10
 - Task Archival utility, 20-6
- archive reconciliation tables, 20-1
- archive task tables, 20-6
- asynchronous execution
 - async routing and configuration, 22-1
 - AsynchService, 22-1
- attestation, 5-1
- Attestation Dashboard, 5-19
 - e-mail notifications, 5-21
 - scheduled tasks, 5-21
 - using, 5-19
 - viewing attention request details, 5-20
- attestation processes, 5-13
 - Attestation Dashboard, 5-19
 - Attestation engine, 5-9
 - Attestation Inbox, 5-4
 - attestation requests, 5-4
 - configuration, 5-13
 - creating, 5-14
 - declined attestation entitlements, 5-12
 - defining schedules, 5-2
 - definition, 5-2
 - delegation, 5-4
 - deleting, 5-2, 5-18
 - disabling, 5-2, 5-17
 - editing, 5-17
 - e-mails, 5-10
 - enabling, 5-18
 - lifecycle, 5-5
 - managing, 5-16
 - managing administrators, 5-18
 - notifying delegated reviewers, 5-11
 - notifying reviewers, 5-10
 - process owners, 5-2
 - reviewer setup, 5-2
 - reviewers, 5-12

- running, 5-18
- scheduled tasks, 5-10
- scope, 5-2
- task components, 5-3
- viewing execution history, 5-18
- attestation task
 - creating, 5-5
- attestation task components
 - attestation actions, 5-3
 - attestation data, 5-3
 - attestation date, 5-3
 - reviewers, 5-3
 - task source, 5-3
- attestation tasks
 - actions, 5-7
 - attestation driven workflow capability, 5-10
 - processing submitted tasks, 5-7
 - reviewer response to entitlement, 5-7
 - workflow diagram, 5-6
- audit engine, 18-1
- auditing, 18-1
 - profile auditing, 18-2
 - role profile auditing, 18-7
 - user profile auditing, 18-2
- asynchronous execution
 - configuration parameters, 22-2
 - managing, 22-1

B

- BI Publisher, 19-1, 32-6
 - starting, 19-2

C

- certification, 6-1
 - authorization, 6-3
 - closed-loop remediation, 6-2, 6-24
 - concepts, 6-1
 - configuration, 6-3
 - configuration options, 6-8
 - definition, 6-2, 6-9
 - event listener, 6-3, 6-25, 6-26
 - event trigger jobs, 6-26
 - jobs, 6-2
 - line item, 6-1
 - LOB, 6-1
 - managing, 6-1
 - multi-phased review, 6-31
 - object, 6-2
 - remediation tracking, 6-2, 6-24
 - reports, 6-29
 - risk summaries, 6-19
 - scheduling, 6-19
 - task, 6-1
 - TPAD, 6-31
 - two-phased review, 6-31
- certification authorization, 6-3
- certification configuration options, 6-8
- certification definition, 6-2, 6-9

- certification jobs, 6-2
- certification object, 6-2
- certification reports, 6-29
- certification task, 6-1
- close reconciliation events, 13-15
- closed-loop remediation, 6-2, 6-24
- complex password, 4-5
- configure
 - log handlers, 21-4
 - loggers, 21-5
 - node manager, 30-1
- configuring
 - application instances, 9-15
 - Remote Manager, 28-1
- configuring certification, 6-3
- configuring notification for proxy, 14-17
- connectors
 - cloning, 12-22
 - custom, 12-4
 - defining, 12-13
 - exporting connector object definitions, 12-35
 - installing, 12-6
 - managing lifecycle, 12-1
 - postcloning steps, 12-35
 - uninstalling, 12-67
 - upgrade procedure, 12-45
 - upgrading, 12-36
- create
 - access policies, 3-7
 - approval policies, 2-4
 - notification template, 14-12
 - password policy, 4-2
 - scheduled job, 15-22
 - system properties, 16-23
- creating
 - custom scheduled tasks, 15-20
 - lookup type, 11-2
- custom scheduled tasks, 15-20

D

- data collection, 18-3, 18-7
 - archiving, 18-8
 - capturing, 18-3, 18-8
- default notification templates, 14-11
- default system properties, 16-1
- delete
 - approval policies, 2-9
 - jobs, 15-27
 - notification templates, 14-15
 - system properties, 16-30
- deployment
 - securing, 35-1
- Deployment Manager, 12-13
- Design Console
 - Group Entitlements form, 34-4
 - Organizational Defaults form, 34-1
 - Policy History form, 34-2
 - User Management folder, 34-1
- Diagnostic Dashboard, 22-3, 25-1

- executing tests, 25-3
- installing, 25-1
- purging failed async tasks, 22-5
- resubmitting failed async tasks, 22-5
- retrying failed async tasks, 22-5
- running a test, 25-2
- starting, 22-3, 25-2
- viewing failed async tasks, 22-4

diagnostic message types, 21-2

diagnostics

- enabling, 26-1

disconnected application instance

- managing, 10-2
- provisioning, 10-5

disconnected resources

- architecture, 10-1
- managing, 10-1

display reconciliation event details, 13-12

E

enable

- secure cookies, 31-1
- system logging, 21-1

enable and disable jobs, 15-26

enabling

- diagnostics, 26-1

end-user administrator, 34-2

end-users, 34-2

Enterprise Manager, 23-1

- exporting and importing configuration files, 23-1
- Mbeans, 23-1

entitlements

- available and assigned, 9-19
- child process forms, 9-21
- configuring scheduled tasks, 9-25
- data capture process, 9-20
- developing, 9-18
- reports, 9-29

event listener, 6-3, 6-25, 6-26

event trigger jobs, 6-26

exception, 19-42

exception reports, 19-42

F

form attributes

- hiding, 7-4
- removing, 7-4

Form Designer, 7-1

Form Version Control Utility, 29-1

forms

- creating, 7-1
- Form Designer, 7-1
- managing, 7-1
- modifying, 7-3
- searching, 7-2

FVC utility, 12-61

H

host and port changes

- BI Publisher, 33-5
- OAM, 33-6
- Oracle Identity Manager, 33-1
 - backOfficeURL, 33-2
 - OimFrontEndURL, 33-2
- Oracle Identity Manager database, 33-3
- OVD, 33-4
- SOA, 33-5

I

identity certification, 6-1

- managing, 6-1

IdM Diagnostic tool, 26-1

install

- Diagnostic Dashboard, 25-1

integration

- BI Publisher, 32-6
- OAAM, 32-2
- OAM, 32-2
- OIA, 32-2
- OIN, 32-5
- OVD, 32-5
- SOA, 32-6

J

job, 15-21

- creating, 15-22
- viewing, 15-24

jobs

- advanced search, 15-24
- deleting, 15-27
- enabling and disabling, 15-26
- modifying, 15-26
- simple search, 15-23
- starting and stopping, 15-27

L

LDAP scheduled tasks, 15-15

lifecycle management, 33-1

link orphan accounts, 13-16

link reconciliation events, 13-15

log handlers

- configuring, 21-4

log handlers and loggers, 21-3

log levels, 21-10

log4j, 21-9

- log levels, 21-10

loggers, 21-10

- configuring, 21-5

logging services, 21-1

- ODL, 21-1

logging.xml, 21-4

lookup type

- creating, 11-2
- modifying, 11-3

- searching, 11-1
- lookups
- managing, 11-1

M

- manage
 - access policies, 3-10
 - approval policies, 2-1
 - reconciliation events, 13-10
- managing
 - asynchronous execution, 22-1
- managing identity certification, 6-1
- manually link reconciliation events, 13-16
- mode of reconciliation, 13-8
- modify
 - approval policies, 2-8
 - approval policy priority, 2-9
 - jobs, 15-26
 - notification templates, 14-15
 - system properties, 16-29
- multi-phased review, 6-31

N

- node manager, 30-1
 - configuring, 30-1
 - starting, 30-2
- notification
 - notification template, 14-1
- notification template, 14-1
 - creating, 14-12
- notification templates
 - adding and removing locales, 14-16
 - default, 14-11
 - deleting, 14-15
 - modifying, 14-15
 - purging cache, 16-27
 - searching, 14-14

O

- OAAM, 32-2
- OAM, 32-2
- ODL log output, 21-9
- OIA, 32-2
- oim-config.xml, 15-2
- OIN, 32-5
- Oracle Identity Manager
 - attestation, 5-1
 - reporting, 19-1
- Oracle Identity Manager loggers, 21-6
- Oracle Identity Manager reports, 19-3
- Oracle Identity Manger
 - password changes, 33-6
 - URL changes, 33-1
- OVD, 32-5

P

- password changes

- Oracle Identity Manager, 33-7
- Oracle Identity Manager database, 33-11
- Oracle Identity Manager in CSF, 33-12
- Oracle Identity Manger, 33-6
- Oracle WebLogic administrator, 33-7
- OVD, 33-13
- password policy
 - complex password, 4-5
 - creating, 4-2
 - custom policy, 4-6
 - deleting, 4-9
 - searching, 4-1
 - setting rules, 4-3
- post-processors, 18-6
- predefined scheduled tasks, 15-7
- profile auditing, 18-2
- provisioning
 - disconnected application instance, 10-5
 - multiple account, 3-12
 - multiple instances of the same resource, 3-10
 - multiple resource objects to multiple target systems, 3-12
 - options, 3-3
- provisioning SOA composite
 - customizing, 10-13
- purge cache, 16-27

R

- reconciliation
 - account reconciliation, 13-4
 - approach, 13-9
 - changelog, 13-9
 - event actions, 13-14
 - mode, 13-8
 - process flow, 13-6
 - push or pull model, 13-8
 - regular, 13-9
 - trusted source, 13-3
 - types, 13-2
- Reconciliation Archival utility, 20-1
 - log files, 20-6
- active reconciliation tables, 20-1
- archival criteria, 20-3
- archive reconciliation tables, 20-1
- prerequisites, 20-3
- running, 20-4
- reconciliation events, 13-10
 - ad-hoc linking, 13-16
 - advanced search, 13-11
 - closing, 13-15
 - details, 13-12
 - linking, 13-15
 - linking orphan accounts, 13-16
 - manual linking, 13-16
 - orphan accounts, 13-16
 - re-evaluating, 13-14
 - searching, 13-10
 - simple search, 13-10

- re-evaluate reconciliation events, 13-14
- regular reconciliation, 13-9
- remediation tracking, 6-2, 6-24
- Remote Manager, 28-1
 - configuring, 28-1
 - starting, 28-6
 - stopping, 28-6
 - troubleshooting, 28-6
- reporting, 19-1
 - BI Publisher, 19-1
 - features, 19-1
- reports, 19-3
 - access policy reports, 19-3
 - attestation, request, and approval reports, 19-5
 - Crystal Reports, 19-46
 - exception reports, 19-42
 - password reports, 19-19
 - resource and entitlement reports, 19-22
 - role and organization reports, 19-14
 - running, 19-2
 - user reports, 19-37
- Requests Archival utility, 20-10
 - archival tables, 20-11
 - input parameters, 20-12
 - log files, 20-14
 - preparing, 20-11
 - request status, 20-11
 - running, 20-12
- risk summaries, 6-19
- role profile auditing, 18-7

S

- scheduled job, 15-21
 - advanced search, 15-24
 - simple search, 15-23
- scheduled tasks, 15-6
 - LDAP, 15-15
 - predefined, 15-7
- scheduler
 - child elements, 15-2
 - creating custom scheduled tasks, 15-20
 - job, 15-1, 15-21
 - job run, 15-1
 - LDAP scheduled tasks, 15-15
 - oim-config.xml, 15-2
 - predefined scheduled tasks, 15-7
 - scheduled task, 15-1
 - scheduled tasks, 15-6
 - starting and stopping, 15-3
- scheduling certifications, 6-19
- search
 - approval policies, 2-7
 - jobs, 15-23
 - notification templates, 14-14
 - reconciliation events, 13-10
- searching
 - system properties, 16-27
- searching jobs, 15-23
- secure cookies

- cookie-secure flag, 31-1
 - enabling, 31-1
- simple search
 - approval policies, 2-7
 - jobs, 15-23
 - notification templates, 14-14
 - system properties, 16-27
- snapshot
 - storing, 18-5, 18-8
- SOA, 32-6
- SOA Composer, 10-13
- SOA composite payload, 10-2
- SSL, 31-1
- start and stop
 - jobs, 15-27
- start and stop scheduler, 15-3
- starting and stopping
 - WebLogic Administration Server, 30-2
 - WebLogic Managed Servers, 30-2
- starting and stopping server, 30-1
- synchronize UDFs, 8-25
- system logging
 - configuring log handlers, 21-4
 - configuring loggers, 21-5
 - diagnostic message types, 21-2
 - enabling, 21-1
 - log handlers and loggers, 21-3
 - log levels, 21-10
 - log4j, 21-9
 - loggers, 21-10
 - logging.xml, 21-4
 - ODL log output, 21-9
 - Oracle Identity Manager loggers, 21-6
- system properties, 16-1
 - advanced search, 16-28
 - configuring notification for proxy, 14-17
 - creating, 16-23
 - default, 16-1
 - deleting, 16-30
 - modifying, 16-29
 - searching, 16-27
 - simple search, 16-27

T

- Task Archival utility, 20-6
 - active task tables, 20-6
 - archive task tables, 20-6
 - output files, 20-10
 - preparing Oracle database, 20-7
 - running, 20-8
- TPAD, 6-31
- troubleshooting
 - Access Request Catalog, 17-25
 - disconnected resources, 10-15
 - Remote Manager, 28-6
- trusted source reconciliation, 13-3
- two-phased review, 6-31

U

UDF

- synchronizing, 8-25

URL changes

- Oracle Identity Manger, 33-1

user profile audit tables, 18-6

user profile auditing, 18-2

- data collection, 18-3, 18-7

- post-processors, 18-6

- XL.UserProfileAuditDataCollection, 18-3

user profile audits

- tables used, 18-6

user profile snapshot

- trigger, 18-6, 18-8

users

- language, 24-1

utility

- cancelProcessTask, 12-61

- FVC, 12-61, 29-1

- PurgeCache, 12-61

- uninstall connector, 12-70

V

viewing jobs, 15-24

W

WebLogic Administration Server

- starting and stopping, 30-2

WebLogic Managed Servers

- starting and stopping, 30-2

X

XL.UserProfileAuditDataCollection, 18-3