

Oracle® Role Manager

Integration Guide

Release 10g (10.1.4.2)

E14611-07

March 2010

Oracle Role Manager Integration Guide Release 10g (10.1.4.2)

E14611-07

Copyright © 2010, Oracle and/or its affiliates. All rights reserved.

Primary Author: Carla Fabrizio

Contributing Author: Prakash Hulikere

Contributors: Vijay Appadorai, Shilpa BR, Miles Chaston, Ashish Chugh, April Escamilla, Bennett Falk, Stephen Grenholm, Ajay Gopal, Ashish Gupta, Sujata Jakate, Parvinder Kaur, Madhup Kumar, Gopal Kumarappan, Avinash Mittal, Jitendra Maheshwari, Subrahmanya Nayak, Parthiban Palani, Devender Sharma, Utkarsh Singh

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

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

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

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

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

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

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

Contents

| | |
|--|------|
| Preface | xiii |
| Audience..... | xiii |
| Documentation Accessibility | xiii |
| Related Documents | xiv |
| Conventions | xiv |
| | |
| 1 Introducing the Oracle Role Manager Integration Library | |
| 1.1 About the Oracle Role Manager Integration Library | 1-1 |
| 1.2 Important Considerations..... | 1-3 |
| 1.3 Architecture | 1-4 |
| | |
| 2 Installing the Oracle Role Manager Integration Library | |
| 2.1 Verifying Requirements..... | 2-1 |
| 2.2 Before You Start..... | 2-2 |
| 2.3 Overview of Installation and Deployment steps..... | 2-2 |
| 2.4 Distributing the Oracle Role Manager Integration Library Software | 2-3 |
| 2.5 Configuring the Commons Logging Level | 2-4 |
| 2.6 The Integration Library Files and Directories..... | 2-4 |
| 2.7 Determining the Release Number of the Integration Library | 2-9 |
| | |
| 3 Upgrading the Oracle Role Manager Integration Library | |
| 3.1 Before You Start..... | 3-1 |
| 3.2 Upgrading the Oracle Role Manager Integration Library Software and Configuration.. | 3-2 |
| 3.3 Resetting the oimSystem System User Privileges | 3-3 |
| 3.4 Running the User Groups Cleanup Task | 3-5 |
| | |
| 4 Automated Configuration for Oracle WebLogic Server | |
| 4.1 Overview | 4-1 |
| 4.1.1 Oracle Identity Manager Setup Script | 4-1 |
| 4.1.2 Oracle Role Manager Setup Script | 4-2 |
| 4.2 Prerequisites | 4-2 |
| 4.2.1 Oracle Identity Manager Prerequisites..... | 4-2 |
| 4.2.2 Oracle Role Manager Prerequisites..... | 4-3 |

| | | |
|-------|--|------|
| 4.2.3 | Configuring Signed Messages (Encryption) | 4-3 |
| 4.3 | Running the Configuration Script for Oracle Identity Manager..... | 4-3 |
| 4.4 | Running the Configuration Script for Oracle Role Manager..... | 4-5 |
| 4.5 | Required Manual Configuration | 4-8 |
| 4.5.1 | Configuring the IT Resource | 4-8 |
| 4.5.2 | Modifying the oimORMUser ID..... | 4-8 |
| 4.5.3 | Resetting the System User Passwords | 4-8 |
| 4.5.4 | Configuring the JMS Connection Factory for XA on the Oracle Role Manager Server | 4-10 |
| 4.5.5 | Configuring the JMS Connection Factory for XA on the Oracle Identity Manager Server | 4-10 |
| 4.5.6 | Disabling Authentication on the Oracle Role Manager Node | 4-10 |
| 4.5.7 | Configuring the Role Grant Approval Workflow..... | 4-10 |
| 4.6 | Testing the Installation..... | 4-10 |

5 Configuring Oracle Role Manager

| | | |
|---------|--|------|
| 5.1 | Deploying the Integration Library Configuration | 5-1 |
| 5.2 | Creating the oimSystem System Identity | 5-3 |
| 5.3 | Loading the oimSystem System Identity Relationship Data | 5-4 |
| 5.4 | Resetting the Password for the oimSystem System Identity | 5-4 |
| 5.5 | Configuring Signed Messages (Encryption) | 5-5 |
| 5.5.1 | Enabling Encryption..... | 5-8 |
| 5.6 | Modifying Component Configuration..... | 5-9 |
| 5.6.1 | Obtaining the Standard Configuration Files | 5-9 |
| 5.6.2 | Modifying the Batch Resolution Timer | 5-10 |
| 5.6.2.1 | Batch Resolution Timer Configuration Settings | 5-11 |
| 5.6.3 | Modifying the Role Membership Update Timers..... | 5-11 |
| 5.6.3.1 | Role Membership Update Timers Configuration Settings..... | 5-12 |
| 5.6.4 | Modifying the Incoming Event Manager | 5-14 |
| 5.6.4.1 | Incoming Event Manager Settings | 5-14 |
| 5.6.5 | Modifying the Outgoing Event Manager..... | 5-15 |
| 5.6.5.1 | Outgoing Event Manager Settings | 5-16 |
| 5.6.6 | Modifying the Business Logic for User Reconciliation | 5-17 |
| 5.6.6.1 | Business Logic Settings..... | 5-17 |
| 5.6.7 | Packaging Configuration Modifications | 5-19 |

6 Configuring Oracle Identity Manager

| | | |
|-------|---|-----|
| 6.1 | Before You Configure | 6-1 |
| 6.2 | Configuring the Oracle Identity Manager Home Directory | 6-2 |
| 6.3 | Creating the System User and User Group for Oracle Role Manager (WebLogic)..... | 6-2 |
| 6.4 | Creating the System User and User Group for Oracle Role Manager (WebSphere and JBoss) | 6-3 |
| 6.5 | Creating the Proxy User for Role Grant Approval Workflow | 6-4 |
| 6.6 | Importing the Prepared Configuration..... | 6-5 |
| 6.6.1 | Importing the Base Configuration..... | 6-5 |
| 6.6.2 | Importing the Sample Configuration for Approver Role Resolution..... | 6-7 |
| 6.7 | Assigning the System User to the User Group..... | 6-7 |

| | | |
|------|--|------|
| 6.8 | Assigning the Proxy User to the System Group | 6-8 |
| 6.9 | Configuring the IT Resource | 6-9 |
| 6.10 | Configuring Role Grant Approval Workflow | 6-10 |

7 Configuring WebLogic Server

| | | |
|-------|---|------|
| 7.1 | Before You Configure | 7-1 |
| 7.2 | Configuring the Oracle Role Manager Server | 7-2 |
| 7.2.1 | Configuring the JMS Connection Factory | 7-2 |
| 7.2.2 | Configuring the Foreign JNDI Providers | 7-2 |
| 7.2.3 | Configuring the Security Credentials | 7-3 |
| 7.2.4 | (Clustered Mode Only) Configuring the Subdeployment of the Connection Factory | 7-4 |
| 7.2.5 | Disabling Authentication on the Oracle Role Manager Node | 7-4 |
| 7.3 | Configuring the Oracle Identity Manager Server | 7-4 |
| 7.3.1 | Modifying the Oracle Identity Manager Startup Script | 7-5 |
| 7.3.2 | Configuring the Shared Libraries | 7-6 |
| 7.3.3 | (Clustered Mode Only) Configuring JMS Queues and Connection Factories | 7-6 |
| 7.3.4 | (Nonclustered Mode Only) Configuring JMS Queues and Connection Factories | 7-7 |
| 7.3.5 | Configuring Foreign JMS Queues and Connection Factories | 7-9 |
| 7.3.6 | Configuring Security Credentials | 7-10 |
| 7.3.7 | (Clustered Mode Only) Adding the Integration Library System Properties | 7-10 |
| 7.4 | Deploying the Oracle Role Manager Integration Library Application on WebLogic | 7-11 |

8 Configuring IBM WebSphere

| | | |
|--------|---|------|
| 8.1 | Before You Configure | 8-1 |
| 8.2 | Configuring the Oracle Role Manager Server | 8-1 |
| 8.2.1 | Deploying the WebSphere Configuration | 8-2 |
| 8.2.2 | Creating the Custom User for the Integration | 8-3 |
| 8.2.3 | Creating the Alias for Custom User for the Integration | 8-3 |
| 8.2.4 | (Clustered Mode Only) Creating the Database Users for the JMS Engines | 8-3 |
| 8.2.5 | (Clustered Mode Only) Creating the Aliases for the JMS Engine Database Users | 8-4 |
| 8.2.6 | Creating the JMS Messaging Buses | 8-4 |
| 8.2.7 | Configuring the Oracle Role Manager Bus | 8-5 |
| 8.2.8 | Configuring the Role Update Bus | 8-6 |
| 8.2.9 | Configuring the JMS Queue Connection Factory | 8-8 |
| 8.2.10 | Configuring JMS Queues | 8-8 |
| 8.2.11 | Configuring Security Credentials on the Oracle Role Manager Bus | 8-8 |
| 8.2.12 | Configuring Security Credentials on the Role Update Bus | 8-9 |
| 8.2.13 | Granting Sender Roles to the System User | 8-10 |
| 8.2.14 | Disabling Transaction Security | 8-11 |
| 8.2.15 | Modifying the Oracle Role Manager Deployment Descriptor | 8-11 |
| 8.3 | Configuring the Oracle Identity Manager Server | 8-13 |
| 8.3.1 | (Clustered Mode Only) Creating the Oracle Identity Manager Database Users for the JMS Engines | 8-13 |
| 8.3.2 | Creating the Authentication Alias for connections to Oracle Role Manager | 8-14 |
| 8.3.3 | (Clustered Mode Only) Creating the Additional Authentication Aliases for the New Data Stores | 8-14 |

| | | |
|--------|--|------|
| 8.3.4 | (Clustered Mode Only) Creating the JDBC Data Sources for the New Data Stores | 8-15 |
| 8.3.5 | Creating the JMS Messaging Buses | 8-16 |
| 8.3.6 | Configuring the OIM ORM Bus | 8-18 |
| 8.3.7 | Configuring the Role Update Bus | 8-19 |
| 8.3.8 | Configuring JMS Queue Connection Factories | 8-20 |
| 8.3.9 | Creating the Oracle Role Manager JMS Queue | 8-21 |
| 8.3.10 | Creating the OIM ORM JMS Queue | 8-21 |
| 8.3.11 | Configuring JMS Activation Specifications | 8-21 |
| 8.3.12 | Configuring Security Credentials on the Role Update Bus | 8-22 |
| 8.3.13 | Configuring Security Credentials on the OIM ORM Bus | 8-22 |
| 8.3.14 | Configuring Outbound Authentication | 8-23 |
| 8.3.15 | Granting Sender Roles to the System User | 8-23 |
| 8.3.16 | Creating the Shared Libraries | 8-24 |
| 8.3.17 | Adding the Integration Library System Properties | 8-25 |
| 8.4 | Configuring Signer Certificates | 8-25 |
| 8.4.1 | Exporting the Oracle Role Manager Certificates | 8-25 |
| 8.4.2 | Importing and Exporting Certificates on Oracle Identity Manager | 8-26 |
| 8.4.3 | Importing the Oracle Identity Manager Certificates | 8-27 |
| 8.5 | Deploying the Oracle Role Manager Integration Library Application on WebSphere | 8-28 |

9 Configuring JBoss

| | | |
|-------|--|-----|
| 9.1 | Before You Configure | 9-1 |
| 9.2 | Configuring the Oracle Role Manager Server | 9-1 |
| 9.3 | Configuring the Oracle Identity Manager Server | 9-3 |
| 9.3.1 | Modifying the Oracle Identity Manager Startup Command | 9-4 |
| 9.4 | Deploying the Oracle Role Manager Integration Library Application on JBoss | 9-5 |

10 Testing the Oracle Role Manager Integration Library Installation

| | | |
|--------|--|-------|
| 10.1 | Testing User Reconciliation | 10-1 |
| 10.1.1 | Real-Time User Synchronization | 10-2 |
| 10.1.2 | Scheduled Tasks for User Reconciliation | 10-2 |
| 10.2 | Testing Entitlement Reconciliation | 10-3 |
| 10.3 | Testing Role and Role Membership Reconciliation | 10-4 |
| 10.3.1 | User Provisioning through Role/User Group Membership | 10-4 |
| 10.3.2 | User De-provisioning by Deleted Roles | 10-6 |
| 10.4 | Testing One-Time Import of User Groups | 10-7 |
| 10.5 | Testing One-Time Import of Access Policies | 10-7 |
| 10.6 | Testing Approver Role Resolution | 10-9 |
| 10.6.1 | Oracle Role Manager Setup | 10-9 |
| 10.6.2 | Oracle Identity Manager Setup | 10-10 |
| 10.6.3 | Performing the test | 10-11 |
| 10.7 | Testing Role Grant Approver Workflow | 10-12 |

11 Troubleshooting

| | | |
|------|---|------|
| 11.1 | Log Files | 11-1 |
| 11.2 | Oracle Role Manager Application Server Console Errors | 11-1 |

| | | |
|------|---|------|
| 11.3 | Oracle Identity Manager Application Server Console Errors | 11-2 |
|------|---|------|

A Cron Expressions

Index

List of Examples

| | | |
|-----|---|------|
| 5-1 | Batch Resolution Timer Default Values in XML | 5-11 |
| 5-2 | Example of Role Membership Update Default Values in XML | 5-13 |
| 5-3 | Incoming Event Manager Default Values in XML..... | 5-14 |
| 5-4 | Outgoing Event Manager Configuration Default Values in XML..... | 5-16 |
| 5-5 | Business Logic Configuration Default Values in XML..... | 5-17 |
| A-1 | Cron Expressions | A-1 |

List of Tables

| | | |
|-----|--|------|
| 2-1 | Supported Configurations | 2-1 |
| 2-2 | Oracle Role Manager Integration Library Files | 2-4 |
| 5-1 | Batch Resolution Timer Configuration Values..... | 5-11 |
| 5-2 | Role Membership Update Timers Configuration Values | 5-12 |
| A-1 | Cron Expressions Allowed Fields and Values..... | A-1 |

Preface

The *Oracle Role Manager Integration Guide* describes the Oracle Role Manager Integration Library and the steps needed for installation, configuration, and deployment.

Audience

This document is intended for those who are involved in the administration of Oracle Role Manager, and Oracle Identity Manager administrators and system administrators.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

<http://www.oracle.com/accessibility/>

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

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

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

Related Documents

For more information, see the following documents:

- *Oracle Role Manager Release Notes*
- *Oracle Role Manager User's Guide*
- *Oracle Role Manager Installation Guide*
- *Oracle Role Manager Administrator's Guide*
- *Oracle Role Manager Developer's Guide*
- *Oracle Role Manager Java API Reference*
- *Oracle Role Manager Licensing Information*

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. |
| <code>monospace</code> | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

Introducing the Oracle Role Manager Integration Library

This chapter provides an overview of the Oracle Role Manager Integration Library and includes the following sections:

- [About the Oracle Role Manager Integration Library](#)
- [Architecture](#)

1.1 About the Oracle Role Manager Integration Library

The section outlines the features available in the Oracle Role Manager Integration Library (Integration Library) used to integrate Oracle Role Manager with provisioning systems.

Oracle Role Manager manages roles and resolves role memberships, both memberships that result from direct grants and those that are derived based on rules and grant policies. Through the Integration Library, external systems can use these roles for role-based provisioning.

The Integration Library is currently available for Oracle Identity Manager and includes the following features:

- User provisioning and reconciliation
 - Real-time creation of a person record in Oracle Role Manager for every Oracle Identity Manager user.
Users must have Oracle Role Manager records before they can be granted roles in Oracle Role Manager and this feature automates the process.
 - Real-time update of user data from Oracle Identity Manager.
For all user attributes configured in XML to be sent to Oracle Role Manager, changes made to those values are sent as soon as they are submitted in Oracle Identity Manager. This ensures that Oracle Identity Manager remains the authoritative system of record for all people in the Oracle Role Manager system who are also users in Oracle Identity Manager.
 - Scheduled tasks for user reconciliation.
Scheduled tasks ensure that user data in both systems is synchronized. This consists of sending all user records from Oracle Identity Manager to Oracle Role Manager and ensures that all users denoted as originating from Oracle Identity Manager have a corresponding Oracle Role Manager person record.

There are two scheduled tasks for user reconciliation: *quick* user reconciliation and *full* user reconciliation. Quick user reconciliation can be run at periodic intervals to send to Oracle Role Manager all user data that has been created, updated or deleted since the last time the task was run or since a specified base time. Full user reconciliation additionally checks for users that have been either deleted or made inactive and reflects that change in status in Oracle Role Manager.

- Entitlement reconciliation

- Real-time creation of an entitlement in Oracle Role Manager for every Oracle Identity Manager entitlement.
- Real-time update of entitlement data from Oracle Identity Manager.

Data for entitlements in Oracle Identity Manager is sent in real time as soon as changes are submitted. This ensures that entitlement data in Oracle Role Manager is always aligned with entitlements in Oracle Identity Manager.

- Scheduled tasks for entitlement reconciliation.

Scheduled tasks ensure that entitlement data in both systems is synchronized. This consists of sending all entitlement records from Oracle Identity Manager to Oracle Role Manager, where entitlements are updated or created to match what is sent from Oracle Identity Manager. Any changes to mapping of entitlements in Oracle Identity Manager will also be made in Oracle Role Manager as part of entitlement reconciliation.

There are two scheduled tasks for entitlement reconciliation: *quick* entitlement reconciliation and *full* entitlement reconciliation. Quick entitlement reconciliation can be run at periodic intervals to send to Oracle Role Manager all entitlement data that has been created, updated or deleted since the last time the task was run or since a specified base time. Full entitlement reconciliation additionally checks for entitlements that have been deleted in Oracle Identity Manager, and deletes the corresponding entitlements in Oracle Role Manager.

- Business Role and role membership reconciliation

- One-time import of user groups from Oracle Identity Manager to Business Roles in Oracle Role Manager.

User groups from Oracle Identity Manager are represented in Oracle Role Manager as Business Roles. This scheduled task imports all user group data, user memberships, and mappings between user groups and access policies. It is recommended that the full entitlement reconciliation scheduled task be run before running this task.

- Scheduled creation and update of user groups in Oracle Identity Manager for all Business Roles in Oracle Role Manager.

Business Roles from Oracle Role Manager are represented in Oracle Identity Manager as user groups. (System Roles in Oracle Role Manager do not have corresponding user groups in Oracle Identity Manager.) This reconciliation event is scheduled through the configuration of the business role publishing timer in Oracle Role Manager.

- Scheduled updates of changed user groups and membership lists in Oracle Identity Manager that have corresponding Business Roles in Oracle Role Manager.

Deletions of roles in Oracle Role Manager that affect user groups in Oracle Identity Manager are reflected in Oracle Identity Manager. For example, if a Business Role is deleted in Oracle Role Manager, the corresponding user group in Oracle Identity Manager is deleted.

- IT role reconciliation
 - One-time import of access policies from Oracle Identity Manager to IT roles in Oracle Role Manager.

Access policies from Oracle Identity Manager are represented in Oracle Role Manager as IT roles. This scheduled task imports all access policy data and mappings between those access policies and entitlements. It is recommended that the full entitlement reconciliation scheduled task be run before running this task.
 - Scheduled creation and update of access policies in Oracle Identity Manager for all IT roles in Oracle Role Manager.

IT roles from Oracle Role Manager are represented in Oracle Identity Manager as access policies. This reconciliation event is scheduled through the configuration of the IT role publishing timer and the in Oracle Role Manager. It is recommended that the full entitlement reconciliation scheduled task be run before running this task.
- Approval role reconciliation

Scheduled creation and update of user groups in Oracle Identity Manager for all Approver Roles in Oracle Role Manager.

Approver Roles from Oracle Role Manager are represented in Oracle Identity Manager as user groups. This reconciliation event is scheduled through the configuration of the approver role publishing timer and the in Oracle Role Manager.
- Role grant approval

Real-time approver event messages for role grants in Oracle Role Manager are sent to Oracle Identity Manager. These messages can be used to trigger workflows, for example, for a sequence of selected users as approvers of a role grant.

1.2 Important Considerations

Before using the Oracle Role Manager Integration Library, you may want to modify existing access policies in Oracle Identity Manager, depending on whether you have complex access policies in your system.

Access policies that contain only entitlement information will be reconciled by the Oracle Role Manager Integration Library. If any access policies exist in Oracle Identity Manager that have extra information attached to them (such as complex rules or accounts), the extra information will not be retained when imported into Oracle Role Manager. Similarly, any access policies that do not contain entitlement information will not be imported into Oracle Role Manager.

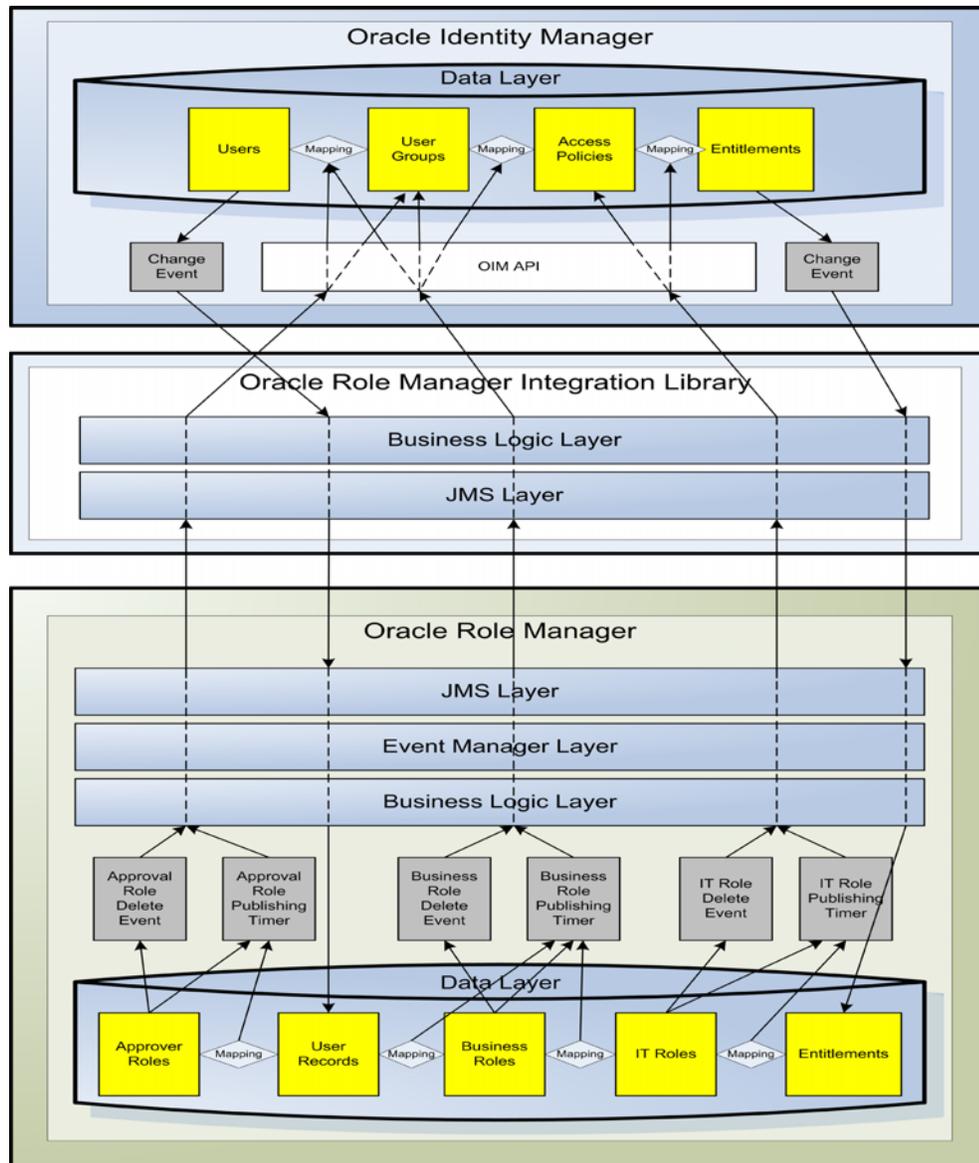
It is recommended that an Oracle Identity Manager administrator break up any access policies with extra information into separate access policies for management purposes. When making these kinds of changes to access policies, it is strongly recommended that administrators review and analyze the impact that these changes might have to their operational system.

1.3 Architecture

Figure 1-1 illustrates the deployment and communication architecture of the Integration Library architecture with Oracle Role Manager and Oracle Identity Manager.

The Integration Library is run in the same application server as Oracle Identity Manager. It communicates with Oracle Identity Manager through the Oracle Identity Manager Java API and a JMS message bus. It communicates with Oracle Role Manager through the EJB-based Oracle Role Manager Java API.

Figure 1-1 High-Level Architecture



Installing the Oracle Role Manager Integration Library

This chapter provides information you should know and the steps to perform before installing the Oracle Role Manager Integration Library with Oracle Identity Manager in your environment for the first time.

Note: If you have a previous installation of Oracle Role Manager Integration Library, see [Chapter 3, "Upgrading the Oracle Role Manager Integration Library."](#)

This chapter includes the following sections:

- [Verifying Requirements](#)
- [Before You Start](#)
- [Overview of Installation and Deployment steps](#)
- [Distributing the Oracle Role Manager Integration Library Software](#)
- [Configuring the Commons Logging Level](#)
- [The Integration Library Files and Directories](#)
- [Determining the Release Number of the Integration Library](#)

2.1 Verifying Requirements

[Table 2–1](#) lists the requirements for the three supported configurations of Oracle Role Manager Integration Library 10.1.4.2 with Oracle Identity Manager 9.1.0.2. For detailed requirements, such as JDK certification, see *Oracle Role Manager Release Notes*.

Table 2–1 Supported Configurations

| Oracle Role Manager | Oracle Identity Manager |
|---|---|
| Oracle Role Manager release 10.1.4.2 on JBoss 4.2.3. | Oracle Identity Manager release 9.1.0.2 on JBoss 4.2.3. |
| Oracle Role Manager release 10.1.4.2 on WebSphere 6.1.0.21. | Oracle Identity Manager release 9.1.0.2 on WebSphere 6.1.0.21 |
| Oracle Role Manager release 10.1.4.2 on WebLogic 10.3. | Oracle Identity Manager release 9.1.0.2 on WebLogic 10.3 |

2.2 Before You Start

Before you begin the deployment of the Oracle Role Manager Integration Library the following prerequisites must be met:

- **Oracle Role Manager**
 - Oracle Role Manager has been installed and the standard model has been deployed following the instructions in *Oracle Role Manager Installation Guide*.
 - The database instance for Oracle Role Manager has been started.
 - Oracle Role Manager has been successfully deployed on the application server.
 - The application server for Oracle Role Manager is not running.
- **Oracle Identity Manager**
 - You have `WRITE` permission on the directories specified for deployment and appropriate permissions on the parent directories for subdirectories to be created.
 - You have access to file system on the Oracle Identity Manager host.
 - You know the Oracle Identity Manager administrator user name and password to access both the Design Console and the Administrative and User Console.
 - The application server for Oracle Identity Manager is on the same host as the Oracle Identity Manager installation directory.

If any of these prerequisites are not met, see *Oracle Role Manager Installation Guide* and *Oracle Identity Manager Installation Guide* for more information.

Note: It is recommended that Oracle Role Manager and Oracle Identity Manager are deployed on separate hosts to avoid port conflicts.

2.3 Overview of Installation and Deployment steps

The following list outlines the high-level steps of installing, configuring, and deploying Oracle Role Manager with the Integration Library.

1. Ensure that all the prerequisites and requirements are met as described in [Section 2.1](#) and [Section 2.2](#).
2. Prepare Oracle Role Manager with the Integration Library configuration and business model.
3. Prepare Oracle Identity Manager for the integration (modify startup command, import configuration, create the Oracle Role Manager user, and create a system property).
4. Prepare the Oracle Identity Manager application server for deployment and deploy the Integration Library application.
5. Test the installation and configuration using procedures in [Chapter 10](#) (user and role reconciliation, group membership reconciliation, and approval role resolution).

2.4 Distributing the Oracle Role Manager Integration Library Software

Distribute the Oracle Role Manager Integration Library software onto the application server host where Oracle Identity Manager is deployed as described in this section.

Certain files must be distributed into Oracle Identity Manager directories, as described in this section. For a detailed description of the individual files in the Integration Library, see [Section 2.6](#).

Note: The Integration Library must be installed on the same host as Oracle Identity Manager.

Note: If you have a clustered server configuration, the Integration Library software files must be distributed on all managed nodes.

Note: If you are configuring the Integration Library on WebLogic, and plan to use the automated configuration scripts, perform only the first two steps in the following procedure. The JAR files and class files will be automatically copied as part of the automated configuration.

To access and distribute the software:

1. On the Oracle Role Manager installation host, navigate to *ORM_HOME/Integration_Library*.
2. Copy the contents of the *Integration_Library* directory to a directory that will become the *ORMINT_HOME* root directory on the Oracle Identity Manager application server.

Note: You may want to create and name the root directory such as *C:\ORMINT_HOME* for convenience. To avoid confusion, this guide refers to this directory in uppercase italic as with other home directory variables.

Make a note of the root directory for application server configuration later in this guide. For more information, see the application server configuration sections.

3. On the Oracle Identity Manager host, copy the following files into *OIM_HOME/xellerate/EventHandlers*:

```
ORMINT_HOME/oimlib/OIM-IntegrationSupport.jar
ORMINT_HOME/oimlib/OIM-IntegrationTransport.jar
```

4. Copy the following files into *OIM_HOME/xellerate/JavaTasks*:

```
ORMINT_HOME/oimlib/OIM-Integration.jar
ORMINT_HOME/lib/server_api_14.jar
ORMINT_HOME/lib/websphere_stubs.jar (For WebSphere only)
```

5. Copy the following files into *OIM_HOME/xellerate/ScheduleTask*.

```
ORMINT_HOME/oimlib/ScheduledAccessPoliciesReconciliation.class
ORMINT_HOME/oimlib/ScheduledEntitlementReconciliation.class
```

```

ORMINT_HOME/oimlib/ScheduledFullEntitlementReconciliation.class
ORMINT_HOME/oimlib/ScheduledFullUserReconciliation.class
ORMINT_HOME/oimlib/ScheduledIntegrationTask.class
ORMINT_HOME/oimlib/ScheduledQuickEntitlementReconciliation.class
ORMINT_HOME/oimlib/ScheduledQuickUserReconciliation.class
ORMINT_HOME/oimlib/ScheduledRoleReconciliation.class
ORMINT_HOME/oimlib/ScheduledUserGroupsCleanup.class
ORMINT_HOME/oimlib/ScheduledUserGroupsReconciliation.class
ORMINT_HOME/oimlib/ScheduledUserReconciliation.class
    
```

2.5 Configuring the Commons Logging Level

It can be helpful to enable logging for the Integration Library application on the application server. This optional procedure sets the logging level to use when logging is enabled in the application server. The procedures for enabling logging in the application server can be found in the appropriate application server configuration sections later in this document.

Note: If you have a clustered server configuration, this procedure must be followed for each managed server.

To set up commons logging for the Integration Library:

1. On the Oracle Identity Manager host, navigate to `ORMINT_HOME/config`.
2. Open the `logging.properties` file with a text editor.
3. Add the Integration Library log level to the file. For example:


```
oracle.iam.rm.imframework.level=FINEST
```
4. Save and close the `logging.properties` file.

2.6 The Integration Library Files and Directories

Table 2–2 describes the files required by the Integration Library. It is recommended that you familiarize yourself with these files as several of them must be copied to different locations or edited for configuration.

Table 2–2 Oracle Role Manager Integration Library Files

| File in Integration Library Home | Description |
|---|---|
| <ul style="list-style-type: none"> ■ MANIFEST.MF | Contains version information for the deployed integration code. |
| <ul style="list-style-type: none"> ■ readme.txt | Contains a pointer to this guide. |
| bin/ | |
| <ul style="list-style-type: none"> ■ create_ear.bat ■ create_bat.sh | Script that creates the Integration Library application EAR file that is bundled with JAR files from the local installation of Oracle Identity Manager. |
| <ul style="list-style-type: none"> ■ create_keystore.bat ■ create_keystore.sh | Script that creates the key store password and stores it to a file named <code>keystore.store</code> , creates a random symmetric key for that password and serializes it to a file named <code>keystore.key</code> , and creates a property file named <code>keystore.properties</code> and adds a single property whose value is a base64-encoded encrypted value of the key store password, encrypted using the symmetric key. |

Table 2–2 (Cont.) Oracle Role Manager Integration Library Files

| File in Integration Library Home | Description |
|---|--|
| <ul style="list-style-type: none"> ■ create_key_pair.bat ■ create_key_pair.sh | <p>Script that creates an asymmetric key pair for the provided alias and the certificate target file. It adds a property to keystore.properties called <i>alias.password</i>, for the provided alias whose value is a base64-encoded encrypted value of the alias password, encrypted using the symmetric key.</p> |
| <ul style="list-style-type: none"> ■ import_certificate.bat ■ import_certificate.sh | <p>Script that reads the public key (in X.509 format) from the provided certificate file, accesses the key store with the provided password, and adds the certificate to the key store with the provided alias.</p> |
| <hr/> | |
| config/ | |
| <ul style="list-style-type: none"> ■ IMConfig.xml | <p>Shared by the integration code handling incoming messages and the Oracle Role Manager Integration Library functionality contained in the Oracle Identity Manager extension directories (JavaTasks, EventHandlers, and ScheduleTask).</p> <p>This file contains the editable prefix that is used to identify user groups in Oracle Identity Manager that correspond with roles in Oracle Role Manager. The default value is either <code>ORM_AR</code>, <code>ORM_BR</code>, or <code>ORM_IR</code> followed by an underscore (<code>_</code>) that is added by the system.</p> <p>The XML schema definition that governs this file is <code>oracle.iam.rm.imframework.imconfig_1_0.xsd</code> located in <code>ORMINT_HOME/schema</code>.</p> |
| <ul style="list-style-type: none"> ■ jboss_config.car | <p>Contains the configuration needed to support the attachment of authentication credentials in JMS messages from JBoss.</p> |
| <ul style="list-style-type: none"> ■ logging.properties | <p>Used for setting the logging level for the Integration Library.</p> |
| <ul style="list-style-type: none"> ■ oim_integration.car | <p>Contains the extensions to the standard model (data model and business logic) necessary for the Integration Library to function with Oracle Identity Manager.</p> <p>This file is manually copied to <code>ORM_HOME/config</code> for deployment convenience.</p> |
| <ul style="list-style-type: none"> ■ oim_systemIdentity.car | <p>Contains the configuration that when deployed, configures the <code>oimSystem</code> system identity for connections to the Oracle Identity Manager system.</p> <p>This file is manually copied to <code>ORM_HOME/config</code> for deployment convenience.</p> |
| <ul style="list-style-type: none"> ■ oim_systemIdentity.dar | <p>Contains the data that must be loaded to complete the creation of the <code>oimSystem</code> system identity.</p> <p>This file is manually copied to <code>ORM_HOME/config</code> for deployment convenience.</p> |
| <ul style="list-style-type: none"> ■ ormoimBase.xml | <p>Contains the base Oracle Identity Manager configuration needed to support the Integration Library. The settings in this file are manually imported into Oracle Identity Manager.</p> |
| <ul style="list-style-type: none"> ■ websphere_config.car | <p>Contains the configuration needed to support the attachment of authentication credentials in JMS messages from WebSphere.</p> <p>This file is manually copied to <code>ORM_HOME/config</code> for deployment convenience.</p> |

Table 2–2 (Cont.) Oracle Role Manager Integration Library Files

| File in Integration Library Home | Description |
|--|--|
| lib/ | |
| <ul style="list-style-type: none"> ■ commons-logging.jar | <p>Contains logging libraries needed to support J2EE 1.3 logging.</p> <p>For WebLogic, this file is manually added as a shared library.</p> <p>NOTE: This file is needed only if Oracle Identity Manager is deployed on WebLogic.</p> |
| <ul style="list-style-type: none"> ■ orm_encryption.jar | <p>Contains classes supporting PKI encryption/decryption and utilities for the management of public and private keys used for the encryption/decryption process. Contained classes are JDK 1.4 compatible.</p> <p>For JBoss, the file is manually copied to <i>JBOSS_HOME</i>/server/default/lib. For other application servers, this file is added as a shared library.</p> |
| <ul style="list-style-type: none"> ■ roleManagerIntegration_JBoss4.2.3.ear.template ■ roleManagerIntegration_WebLogic10.3.ear.template ■ roleManagerIntegration_WebSphere6.1.ear.template | <p>Template used by the create_ear command. Responsible for the initial handling of messages arriving from Oracle Role Manager. This is a J2EE enterprise archive containing a message-driven bean (MDB) and support code. Its core functionality is extended by Java code and configurations deployed in the Integration Library plug-in directories.</p> <p>For JBoss, the file is manually copied to <i>OIM_appserver</i>/deploy as part of the deployment process. For other application servers, this file is deployed through the administrative console user interface.</p> |
| <ul style="list-style-type: none"> ■ server_api_14.jar | <p>Contains additional shared libraries required for a deployment on an application server (a copy is also located in <i>OIM_HOME</i>/xellerate/JavaTasks).</p> <p>For JBoss, this file is manually copied to <i>OIM_appserver</i>/lib and <i>OIM_HOME</i>/xellerate/JavaTasks. For other application servers, this file is added as a shared library.</p> |
| <ul style="list-style-type: none"> ■ websphere_stubs.jar | <p>Contains the generated stubs of the Role Manager public API, which is provided through an Enterprise Java Bean (EJB). Such stubs are required for remote invocation of EJBs.</p> <p>This file is manually added to the WebSphere application server configuration as a shared library.</p> <p>NOTE: This file is needed only if Identity Manager is deployed on WebSphere.</p> |
| <ul style="list-style-type: none"> ■ xercesImpl.jar ■ xml-apis.jar | <p>Contains libraries needed to support J2EE 1.3 JAXP 1.1 for XML parsing.</p> <p>If running the WebLogic configuration script, these files are automatically added to the <i>OIM_appserver</i>/jdk/jre/lib/endorsed directory.</p> <p>NOTE: These files are not needed if Oracle Identity Manager is deployed on JBoss.</p> |
| oimlib/ | |
| <ul style="list-style-type: none"> ■ OIM-Integration.jar | <p>Contains the class files for handling approval role resolution between roles in Oracle Role Manager and user groups in Oracle Identity Manager.</p> <p>This file is copied to <i>OIM_HOME</i>/xellerate/JavaTasks.</p> |

Table 2–2 (Cont.) Oracle Role Manager Integration Library Files

| File in Integration Library Home | Description |
|---|---|
| <ul style="list-style-type: none"> ■ OIM-IntegrationSupport.jar | <p>Contains the class files that support the underlying integration framework (a copy is also located in <code>EventHandlers</code>).</p> <p>This file is copied to <code>OIM_HOME/xellerate/EventHandlers</code>.</p> |
| <ul style="list-style-type: none"> ■ OIM-IntegrationTransport.jar | <p>Contains the class files that support sending messages from the integration to Oracle Role Manager.</p> <p>This file is copied to <code>OIM_HOME/xellerate/EventHandlers</code>. For JBoss, this file is also copied to <code>JBOSS_HOME/server/default/lib</code>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledAccessPoliciesReconciliation.class | <p>Task for reconciliation of Oracle Identity Manager access policies.</p> <p>This file is copied to <code>OIM_HOME/xellerate/ScheduleTask</code>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledEntitlementReconciliation.class | <p>Base task used by the entitlement scheduled tasks.</p> <p>This file is copied to <code>OIM_HOME/xellerate/ScheduleTask</code>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledFullEntitlementReconciliation.class | <p>Task for reconciliation of newly created, updated, and deleted Oracle Identity Manager entitlements.</p> <p>This file is copied to <code>OIM_HOME/xellerate/ScheduleTask</code>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledFullUserReconciliation.class | <p>Task for Full reconciliation of users including synchronous inspection of the Oracle Role Manager state.</p> <p>This file is copied to <code>OIM_HOME/xellerate/ScheduleTask</code>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledIntegrationTask.class | <p>Base task used by all other Oracle Role Manager scheduled tasks.</p> <p>This file is copied to <code>OIM_HOME/xellerate/ScheduleTask</code>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledQuickEntitlementReconciliation.class | <p>Task for reconciliation of newly created and updated Oracle Identity Manager entitlements.</p> <p>This file is copied to <code>OIM_HOME/xellerate/ScheduleTask</code>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledQuickUserReconciliation.class | <p>Task for reconciliation of new, updated, and deleted users based on an input timestamp.</p> <p>This file is copied to <code>OIM_HOME/xellerate/ScheduleTask</code>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledRoleReconciliation.class | <p>Task to reconcile Oracle Role Manager roles and Oracle Identity Manager user groups. Cleans up any deleted user groups on Oracle Identity Manager where there is no corresponding role in Oracle Role Manager.</p> <p>This file is copied to <code>OIM_HOME/xellerate/ScheduleTask</code>.</p> |

Table 2–2 (Cont.) Oracle Role Manager Integration Library Files

| File in Integration Library Home | Description |
|--|---|
| <ul style="list-style-type: none"> ■ ScheduledUserGroupsCleanup.class | <p>Task used as part of the upgrade process to remove user groups that were created as a part of Oracle Role Manager role updates. Because the current version of Oracle Role Manager has Entitlements instead of IT roles, this task also removes entitlements and user groups from the access policies that were created as a result of IT role updates in the previous version of Oracle Role Manager Integration Library.</p> <p>This file is copied to <i>OIM_HOME/xellerate/ScheduleTask</i>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledUserGroupsReconciliation.class | <p>Task for one-time import of Oracle Identity Manager user groups. On running this task all Oracle Identity Manager user groups are created as Business Roles in Oracle Role Manager.</p> <p>This file is manually copied to <i>OIM_HOME/xellerate/ScheduleTask</i>.</p> |
| <ul style="list-style-type: none"> ■ ScheduledUserReconciliation.class | <p>Base task used by the user reconciliation scheduled tasks. Sends all Oracle Identity Manager user records to Oracle Role Manager except for system user records.</p> <p>This file is manually copied to <i>OIM_HOME/xellerate/ScheduleTask</i>.</p> |
| <p>pluginConfigdir/</p> <ul style="list-style-type: none"> ■ ApprovalRequestHandler.xml ■ ApproverRolePublishing.xml ■ BusinessRolePublishing.xml ■ ITRolePublishing.xml ■ RoleDeletion.xml | <p>Contains XML files of handler configurations that map message types for messages arriving from Oracle Role Manager to plug-in Java code that handles the messages. Also contains the XML schema definitions required to interpret the message payloads.</p> <p>Note: Integrators who add functionality to the integration can add their own XML files to this directory. A new XML handler configuration must be created for each additional message type.</p> |
| <p>pluginSchema/</p> <ul style="list-style-type: none"> ■ approvalrequest_1_0.xsd ■ objectdeletion_1_0.xsd ■ roleusersassignment_1_0.xsd | <p>Contains the XML schema definitions for interpreting payloads sent in messages from Oracle Role Manager. These definitions must exactly correspond with the schema of the business logic plug-ins in Oracle Role Manager used by the originators of the messages.</p> <p>Note: Integrators who add functionality to the integration can add their own XML schema files to this directory.</p> <p>The provided XSD files are (prepended by <i>oracle.iam.rm.bizlogic</i> to be fully qualified).</p> |
| <p>samples/</p> <ul style="list-style-type: none"> ■ ormoimSample.xml | <p>The file used to import a sample approval workflow into Oracle Identity Manager. This is used when testing the installation as described in Section 10.6, "Testing Approver Role Resolution."</p> |

Table 2–2 (Cont.) Oracle Role Manager Integration Library Files

| File in Integration Library Home | Description |
|--|--|
| samples/jboss/ | |
| <ul style="list-style-type: none"> ■ oimorm-service.xml | <p>Sample configuration for the JMS queues required to support the Oracle Role Manager Integration Library. Some values in this file can be modified to reflect the actual deployment environment, for example, to change the queue names if the default values were not used.</p> <p>This file is manually copied to <i>OIM_appserver</i>/deploy. This file is only applicable to JBoss. Other application servers provide a Web-based administration console to use for JMS queue configuration.</p> |
| <ul style="list-style-type: none"> ■ ormoim-service.xml | <p>Configuration file for the JMS queues required to support the Integration Library on the Oracle Role Manager application server.</p> <p>Some values in this file can be modified to reflect the actual deployment environment, for example, to change the queue names if the default values were not used.</p> <p>This file is manually copied to <i>ORM_appserver</i>/deploy. Other application servers provide a Web-based administration console to use for JMS queue configuration.</p> |
| schema/ | <p>Contains the standard XML schema used by the Integration Library. Unlike the three previous directories, there is no requirement to add new files to this directory when adding integration functionality.</p> <p>The schema file names are prepended with oracle.iam.rm to be fully qualified.</p> |
| <ul style="list-style-type: none"> ■ event.event_1_0.xsd | <p>Description of the standard Oracle Role Manager event type to which messages sent from Oracle Role Manager to Oracle Identity Manager adhere.</p> |
| <ul style="list-style-type: none"> ■ imframework.imconfig_1_0.xsd | <p>Schema of the Oracle Role Manager Integration Library configuration file (IMConfig.xml).</p> |
| <ul style="list-style-type: none"> ■ imframework.pluginconfig_1_0.xsd | <p>Schema of the files in the Oracle Role Manager Integration Library pluginConfigdir directory.</p> |
| tools/Weblogic_Automation | <p>Contains the scripts used for automatic configuration of the Oracle Role Manager Integration Library on a single WebLogic deployment.</p> |

2.7 Determining the Release Number of the Integration Library

Release information for the Oracle Role Manager Integration Library is stored in a manifest file.

To find the release number:

1. On the command line, navigate to the directory where the Oracle Role Manager Integration Library software was installed:
2. View the contents of the MANIFEST.MF file.

In this file you can view the version number, build number, build label, and build date of the Integration Library.

Upgrading the Oracle Role Manager Integration Library

This chapter provides the steps to perform an upgrade of the Oracle Role Manager Integration Library with Oracle Identity Manager.

This chapter includes the following sections:

- [Before You Start](#)
- [Upgrading the Oracle Role Manager Integration Library Software and Configuration](#)
- [Resetting the oimSystem System User Privileges](#)
- [Running the User Groups Cleanup Task](#)

3.1 Before You Start

Before you begin the upgrade of the Oracle Role Manager Integration Library the following prerequisites steps must be completed:

1. Stop the application server for Oracle Identity Manager.
2. Stop the application server for Oracle Role Manager.
3. Upgrade Oracle Role Manager following the instructions in the *Oracle Role Manager Installation Guide*. This includes backing up the Oracle Role Manager application user and database owner users/schemas.

Note: Ensure that when running the upgrade script, the `oim_integration.car` is in the path of configurations to upgrade. If the upgrade of Oracle Role Manager did not include the `oim_integration.car`, deploy it now following the steps in [Section 5.1, "Deploying the Integration Library Configuration."](#)

4. If you are using a version of Oracle Identity Manager prior to version 9.1.0.2, upgrade to version 9.1.0.2 following the instructions in the *Oracle Identity Manager Installation Guide*.
5. Configure role grant approval workflow as follows:
 - a. Complete the procedure described in [Section 6.5, "Creating the Proxy User for Role Grant Approval Workflow."](#)
 - b. Complete the procedure described in [Section 6.8, "Assigning the Proxy User to the System Group."](#)

- c. Complete the procedure described in [Section 6.10, "Configuring Role Grant Approval Workflow."](#)

3.2 Upgrading the Oracle Role Manager Integration Library Software and Configuration

Certain files must be copied into the *ORMINT_HOME* and Oracle Identity Manager directories, as described in this section.

Note: If you have a clustered server configuration, perform the steps in this procedure on all managed nodes.

To upgrade the software:

1. On the Oracle Identity Manager application server host, copy *ORMINT_HOME* to different location on the same host and rename it, for example, *ORMINT_10141*.

Make a note of this location. Files must be copied from this location to the upgraded *ORMINT_HOME* directory later in this procedure.
2. Make a note of the full path to *ORMINT_HOME* root directory so that you can use that exact path for the upgrade.
3. Delete *ORMINT_HOME*.
4. On the Oracle Role Manager installation host, navigate to *ORM_HOME/Integration_Library*.
5. Copy the *Integration_Library* directory to the Oracle Identity Manager application server host to replace the directory the *ORMINT_HOME* root directory.
6. Copy the following files from *ORMINT_10141/bin* to *ORMINT_HOME/bin*, where *ORMINT_HOME* is the new root directory and *ORMINT_10141* is the directory copied in Step 1.

```
keystore.properties
keystore.key
keystore.store
oim_orm_cert
```

Note: If the new *ORMINT_HOME* location is different than what was used for the previous version of the Integration Library, you must reconfigure the *keystore_dir* system property in the application server configuration to point to the new location. For more information, see the steps for your application server in [Section 5.5, "Configuring Signed Messages \(Encryption\)."](#)

7. Copy the following file from *ORMINT_10141/config* to *ORMINT_HOME/config*:

`logging.properties`
8. Copy the following files into *OIM_HOME/xellerate/EventHandlers*:

`ORMINT_HOME/oimlib/OIM-IntegrationSupport.jar`
`ORMINT_HOME/oimlib/OIM-IntegrationTransport.jar`
9. Copy the following files into *OIM_HOME/xellerate/JavaTasks*:

```

ORMINT_HOME/oimlib/OIM-Integration.jar
ORMINT_HOME/lib/server_api_14.jar
ORMINT_HOME/lib/websphere_stubs.jar (For WebSphere only)

```

10. Copy all of the class files from `ORMINT_HOME/oimlib` into `OIM_HOME/xellerate/ScheduleTask`.
11. Modify the `IMConfig.xml` file as follows:
 - a. Navigate to `ORMINT_HOME/config`.
 - b. Open the `IMConfig.xml` file for editing.
 - c. If your installation of Oracle Identity Manager does not use `C:\OIM` as the root directory, in the policies section, edit the `oimRootdir` policy to change `C:\OIM` to the appropriate root directory as follows:

```

<policy>
  <parameters>
    <parameter>
      <id>oimRootdir/id</id>
      <string>C:\oracle\oim</string>
    </parameter>
  </parameters>
</policy>

```

- d. If your deployment is on WebLogic Server, in the policies section, edit the `oimORMUser` policy to change `ormSystem` to `Internal` as follows:

```

<policy>
  <parameters>
    <parameter>
      <id>oimORMUser</id>
      <string>Internal</string>
    </parameter>
  </parameters>
</policy>

```

- e. Save and close the `IMConfig.xml` file.
12. Re-import the base and sample configuration into Oracle Identity Manager as described in [Section 6.6, "Importing the Prepared Configuration."](#)
13. Redeploy the Integration Library application as described in one of the following sections, depending on your application server platform:
 - [Section 7.4, "Deploying the Oracle Role Manager Integration Library Application on WebLogic"](#)
 - [Section 8.5, "Deploying the Oracle Role Manager Integration Library Application on WebSphere"](#)
 - [Section 9.4, "Deploying the Oracle Role Manager Integration Library Application on JBoss"](#)

3.3 Resetting the oimSystem System User Privileges

After Oracle Role Manager is upgraded, there are three privileges that must be reset for the `oimSystem` system user: `grant person`, `grant business role`, and `manage IT privilege`.

To reset the oimSystem system user privileges:

1. On the Oracle Role Manager host, navigate to `ORM_HOME/Integration_Library/config`.
You should see the `oim_systemIdentity.dar` file.
2. Using a utility like WinZip or jar, extract the entire contents of `oim_systemIdentity.dar` into a temporary location, such as `ORM_HOME/Integration_Library/config/oim_systemIdentity_upgrade`.

In the temporary location, you should see the following five files:

```
load-request.xml
systemIdentity-orm.csv
systemRoleGrant-orm.csv
systemRole-orm.csv
systemRolePrivilegeMapping-orm.csv
```

3. Remove the following three files:

```
systemIdentity-orm.csv
systemRoleGrant-orm.csv
systemRole-orm.csv
```

4. Edit the `load-request.xml` file to change the values of `load-script-id` and `procedure-id` to the values shown in bold below. In addition, remove all `resource-ref` elements except the one named `system_role_privilege_file`.

The complete content of the file should be as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<load-request xmlns="http://xmlns.oracle.com/iam/rm/loader/data/1_0"
load-script-id="oim_systemrole_to_privilege_script"
procedure-id="loadSystemRolePrivilegeMappings"
ordering-mode="dependency-based-sequential">
  <parameters>
    <resource-ref name="system_role_privilege_file">
      <resource-path>systemRolePrivilegeMapping-orm.csv</resource-path>
    </resource-ref>
  </parameters>
</load-request>
```

5. Edit the `systemRolePrivilegeMapping-orm.csv` file to contain only the following values:

```
grant, person, oimSystem
grant, businessRole, oimSystem
manage, itPrivilege, oimSystem
```

6. Using a utility like WinZip or jar, repackage the two files in the temporary location and create a file appended with the `.dar` extension, for example, `oim_systemIdentity_upgrade.dar`.

7. Load the new DAR file as follows:

- a. Start the Oracle Role Manager application server.
- b. From the Oracle Role Manager installation host, using a Web browser, go to the Oracle Role Manager Administrative Console. By default:

WebLogic: `http://host:7001/ormconsole`

WebSphere: `http://host:9080/ormconsole`

JBoss: `http://host:8080/ormconsole`

- c. Enter the user name and password of the Oracle Role Manager administrator, then click **Log In**.
- d. Click **Upload**.
- e. Click **Browse**, and navigate to select the new DAR file created earlier, for example, `oim_systemIdentity_upgrade.dar`.
- f. Click **Load**.

You can click **refresh** to verify that all processes are finalized.

3.4 Running the User Groups Cleanup Task

The User Groups Cleanup task removes user groups that were created as a part of Oracle Role Manager IT role updates in older versions of Oracle Role Manager. The current version of Oracle Role Manager creates access policies for IT role updates. This should be run manually as part of the upgrade process.

To run the User Groups Cleanup Task

1. View an existing user group from Oracle Role Manager as follows:
 - a. In the Oracle Identity Manager Design Console, expand **User Groups**, then double-click **Manage**.
 - b. Search for and select any user group whose name begins with `ORM_` and has role type as `itRole`.
On the Details page of the selected user group, make note of the name for use later in this procedure.
2. Run the User Groups Cleanup task as follows:
 - a. In the Oracle Identity Manager Design Console (Oracle Identity Manager client), expand **Administration**, then double-click **Task Scheduler**.
 - b. Click the Lookup button, and then the Go to End button to go to the last defined task.
 - c. Click the left arrow button until you see the `RoleManagerUserGroupsCleanup` task.
 - d. Clear the **Disabled** box then click the Save button.
 - e. In the **Status** field, change the status to **ACTIVE**.
 - f. In the **Start Time** field, enter the timestamp of the current date and time plus one minute.
 - g. Click the **Save** button.
3. Search for the same user group viewed in Step 1 as follows:
 - a. In the Oracle Identity Manager Design Console, expand **User Groups**, then double-click **Manage**.
 - b. Search for the same user group viewed in Step 1.
The group should not be present.

Automated Configuration for Oracle WebLogic Server

This chapter describes the steps to use the automated scripts to configure Oracle Role Manager for the Oracle Role Manager Integration Library and the application servers for both Oracle Role Manager and Oracle Identity Manager. The procedures in this chapter are expected to be performed in the sequence they are presented.

Note: This chapter assumes that an instance of Oracle Role Manager is installed with the standard model following the instructions in *Oracle Role Manager Installation Guide*.

This chapter includes the following sections:

- [Overview](#)
- [Prerequisites](#)
- [Running the Configuration Script for Oracle Identity Manager](#)
- [Running the Configuration Script for Oracle Role Manager](#)
- [Required Manual Configuration](#)
- [Testing the Installation](#)

4.1 Overview

Configuring and deploying Oracle Role Manager Integration Library on Oracle WebLogic Server using the automated configuration scripts involves the following high-level steps:

1. Checking prerequisites
2. Setting values in the properties files used by the script
3. Running the scripts
4. Performing the required manual procedures

The automated scripts use values that are set in properties files to configure your environment as described in the following sections.

4.1.1 Oracle Identity Manager Setup Script

The script used to configure Oracle Identity Manager does the following configuration:

- Creates and configures the System User and User Group system identity on the Oracle Identity Manager system for access to Oracle Role Manager.
- Imports the prepared configuration from an XML file into the Oracle Identity Manager system.
- Modifies the Oracle Identity Manager startup script with the Integration Library classpath and other system properties.
- Copies shared libraries to the Oracle Identity Manager file system.
- Configures the following on the Oracle Identity Manager application server:
 - JMS queues and connection factories
 - Security credentials
 - System properties
- Deploys the Oracle Role Manager Integration Library EAR file on the application server.

4.1.2 Oracle Role Manager Setup Script

The script used to configure Oracle Role Manager does the following configuration:

- Deploys the Integration Library base model and default component configuration to the Oracle Role Manager database.
- Creates and configures the oimSystem system identity on the Oracle Role Manager database to be used for access by Oracle Identity Manager.
- Sets the Oracle Identity Manager home directory for the Integration Library in the IMConfig.xml file.
- Creates and copies key store information for signed messages (encryption).
- Configures the following on the Oracle Role Manager application server:
 - JMS connection factory
 - Foreign JNDI providers
 - Security credentials
 - Node manager authentication
- Starts the Oracle Identity Manager application server.

4.2 Prerequisites

This chapter assumes that all of the prerequisites described in this section have been met.

4.2.1 Oracle Identity Manager Prerequisites

Ensure that the following prerequisites for Oracle Identity Manager are met:

- The WebLogic Node Manager is running.
- The Oracle Identity Manager application server is installed and running.
- You know the name of the domain credential to be shared between Oracle Role Manager and Oracle Identity Manager application servers.

- You know the Oracle Identity Manager user/schema name and password.
- You have the appropriate permission to stop and start the application server on which Oracle Identity Manager is deployed.
- You know the administrator user name and password to access the Oracle Identity Manager Administrative and User Console and the Oracle Identity Manager Design Console.
- You have the appropriate permission to modify files in the *ORMINT_HOME* directory on the Oracle Identity Manager host.

4.2.2 Oracle Role Manager Prerequisites

Ensure that the following prerequisites for Oracle Role Manager are met:

- You have the access to the files in *ORM_HOME/Integration_Library* on the Oracle Role Manager installation host.
- You have the appropriate permission to add and modify files in the application server host where Oracle Role Manager is deployed.
- You have the appropriate permission to stop and start the application server where Oracle Role Manager is deployed.
- You know the name of the application server where Oracle Role Manager is deployed.
- You know the names of the Oracle Role Manager JMS module on the application server.
- You know the URL to the JNDI server for Oracle Identity Manager.
- You know the ID and password for the Oracle Role Manager owner and application user schemas.
- You know the JDBC connection string of the Oracle Role Manager database instance.
- You have access to the WebLogic Server Administrative Console and know the administrator user ID and password for the domains where Oracle Identity Manager and Oracle Role Manager are deployed.
- The WebLogic Node Manager is running.

4.2.3 Configuring Signed Messages (Encryption)

The configuration of signed messages in Oracle Role Manager and Oracle Identity Manager must be done manually prior to running the scripts for automated configuration. Complete the steps described in [Section 5.5, "Configuring Signed Messages \(Encryption\)."](#)

4.3 Running the Configuration Script for Oracle Identity Manager

To configure Oracle Identity Manager and its application server:

1. Set the environment variables for the setup script as follows:
 - a. Navigate to *ORMINT_HOME/tools/WebLogic_Automation*.
 - b. Open the following file with a text editor:

For UNIX-based systems: oim-setup.sh

For Windows systems: oim-setup.bat

- c. Set the values of the following environment variables to match your environment:

```
WLSHOME
JAVA_HOME
OIM_HOME
```

2. Navigate to *ORMINT_HOME*/tools/WebLogic_Automation/properties.
3. Open the *OIMConfig.properties* file with a text editor and edit values to match your environment as follows:
 - a. In the **wlshost** value, enter the host name or IP address of WebLogic host where Oracle Identity Manager is deployed.
 - b. In the **wlsport** value, enter the port used to access the WebLogic administrative console.
 - c. In the **wlsadmin** value, enter the ID of the WebLogic administrator.
 - d. In the **oimdomain** value, enter the name of the domain for Oracle Identity Manager as configured in WebLogic.
 - e. In the **oimadminserver** value, enter the name of the server where Oracle Identity Manager admin server is deployed.
 - f. In the **OIM_WEBLOGIC_HOME** value, enter the full path to the WebLogic installation directory.
 - g. In the **OIM_APPSERVER_JDK_HOME** value, enter the full path to the JDK being used to run the Oracle Identity Manager application server.
 - h. In the **ormwlshost** value, enter the host name or IP address of the WebLogic host where Oracle Role Manager is deployed.
 - i. In the **ormwlsport** value, enter the port used to access the Oracle Role Manager administrative console.
 - j. In the **ORMINT_HOME** value, enter the full path to the Oracle Role Manager Integration Library root directory.
 - k. In the **XLHOMEDIR** value, enter the full path to the Oracle Identity Manager xellerate directory.
 - l. In the **xladminuser** value, enter the ID of the Oracle Identity Manager administrator.
 - m. In the **xelddbhost** value, enter the host name or IP address of the Oracle Identity Manager database host.
 - n. In the **xelddbuser** value, enter the name of the Oracle Identity Manager database user/schema. By default, this is `xladm`.
 - o. In the **xelddbSID** value, enter the database instance service name for the Oracle Identity Manager schema.
 - p. In the **xelddbport** value, enter the port to access the database instance for the Oracle Identity Manager schema.
 - q. If you want to repeat only certain steps using the configuration, at the bottom of the file, uncomment the steps that you want to skip, leaving the ones you want to run commented out.

For example, to run only the step to deploy the Integration Library application to the application server, the comments should be as follows:

```
done.copy-oim-binaries=true
done.domain-credential-setup=true
done.startup-script-preparation=true
done.update-IMConfig-oimRootdir=true
done.create-jms-resources=true
done.create-user-group=true
done.import-prepared-configuration=true
done.create-itresource-systemproperty=true
#done.deploy-integration-library-ear=true
```

- r. Save and close the OIMConfig.properties file.
4. In a command window, navigate to `ORMINT_HOME/tools/WebLogic_Automation` and run the following command:
For UNIX-based systems: `sh oim-setup.sh`
For Windows systems: `oim-setup.bat`
5. At the prompt, enter a value to use as the domain credential that is shared between Oracle Role Manager and Oracle Identity Manager application servers.
6. At the prompt, enter the a password to use for the oimSystem system identity created by the configuration script.
Make a note of this password. You will need to provide it later when running the configuration script and when configuring the IT resource manually.
7. At the prompt, enter the password of the WebLogic administrator for the server where Oracle Identity Manager is deployed.
8. At the prompt, enter the password of the Oracle Identity Manager user/schema.
9. At the prompt, enter the password of the Oracle Identity Manager system administrator.
10. Restart the Oracle Identity Manager server.
11. Proceed with the manual steps described in this chapter.

4.4 Running the Configuration Script for Oracle Role Manager

To configure Oracle Role Manager and its application server:

1. Stop the Oracle Role Manager server if it is running by using the **Shutdown When work completes option**.

Ensure the shutdown has completed and there are no connections open to the Oracle Role Manager Web application or Oracle Role Manager administrative console before proceeding.

Note: For clarification, the WebLogic admin server must be running, but with the Oracle Role Manager server stopped.

2. If you require any customizations to configurable components, such as setting custom timer intervals, follow the procedures in [Section 5.6](#) to create a custom CAR file that includes your changes.

Note: You can make customizations to the configurable components at any time. For more information, see [Section 5.6, "Modifying Component Configuration."](#)

3. On the Oracle Role Manager host, set the environment variables as follows:
 - a. Navigate to `ORM_HOME/Integration_Library/tools/WebLogic_Automation`
 - b. Open the following file with a text editor:
For UNIX-based systems: `orm-setup.sh`
For Windows systems: `orm-setup.bat`
 - c. Set the values of the following environment variables to match your environment:

```
ORM_INSTALL_ROOT  
WEBLOGIC_INSTALL_ROOT  
JAVA_HOME  
ORMINT_HOME
```
 - d. Save and close the setup file.
4. Navigate to `ORM_HOME/Integration_Library/tools/WebLogic_Automation/properties`.
5. Open the `ORMConfig.properties` file with a text editor and edit values to match your environment as follows:
 - a. In the `ormdb.url` value, enter the JDBC connection string for the database instance for Oracle Role Manager.
 - b. In the `ormdb.driverclass` value, accept the default value of `oracle.jdbc.OracleDriver`.
 - c. In the `ormdb.dboowner` value, enter the name of the database owner user/schema created during installation of Oracle Role Manager.
 - d. In the `ormdb.appuser` value, enter the name of the database application user user/schema created during installation of Oracle Role Manager.
 - e. In the `ormadm` value, enter the ID of the Oracle Role Manager system administrator as set during installation of Oracle Role Manager.

This is the user to connect to the Oracle Role Manager administrative console.
 - f. In the `ormurl` value, enter the address of the application server where Oracle Role Manager administrative console is deployed. For example, `http://host_name_or_ip_address:port`.
 - g. Optionally, if you have created a custom CAR file to deploy, for the `configurations` value, replace `oim_integration.car` with the name of your custom CAR file.
 - h. In the `weblogic.adminurl` value, enter the address of the WebLogic Server administrative console.
 - i. In the `weblogic.username` value, enter the ID of the WebLogic Server administrator.
 - j. In the `weblogic.servername` value, enter the name given to the Oracle Role Manager server when deploying to WebLogic Server during installation of Oracle Role Manager.

- k. In the **weblogic.jmsmodule** value, ensure the value is the same as what was configured during installation of Oracle Role Manager.
- l. In the **weblogic.remote.url** value, enter the address to the remote JNDI server for Oracle Identity Manager.
- m. If you want to repeat only certain steps using the configuration, at the bottom of the file, uncomment the steps that you want to skip, leaving the ones you want to run commented out.

For example, to redeploy modified configuration to the Oracle Role Manager database, the comments should be as follows:

```
#done.configurations=true
done.appserver=true
done.encryption_config=true
done.datafile=true
```

- n. Save and close the `ORMConfig.properties` file.
6. In a command window, navigate to `ORM_HOME/Integration_Library/tools/WebLogic_Automation` and run the following command:
 For UNIX-based systems: `csh orm-setup.sh`
 For Windows systems: `orm-setup.bat`
 7. At the prompt, enter the password of the WebLogic administrator for the server where Oracle Role Manager is deployed.
 8. At the prompt, enter the same value used when running the setup script for Oracle Identity Manager to use as the WebLogic shared domain credential.
 9. At the prompt, re-enter the WebLogic shared domain credential.
 10. At the prompt, enter the password of the Oracle Role Manager database user/schema.
 11. At the prompt, enter the password of the Oracle Role Manager administrator.
 12. At the prompt, enter the same password for the `oimSystem` system user as was set in [Section 4.3](#)
 Make note of this password because you will provide it when configuring the IT resource in [Section 6.9](#).
 13. At the prompt, re-enter the password for the `oimSystem` system user.
 14. At the prompt, enter the Oracle Role Manager key store password (created in Step 10 of [Section 5.5](#)).
 The automated configuration can take a few moments while configuration files are deployed into the Oracle Role Manager database and the WebLogic server is configured.
 15. At the prompt, restart the WebLogic server.
 16. Once the server has started, press any key to continue the automated configuration.
 17. Proceed with the manual steps described in this chapter.

4.5 Required Manual Configuration

This section contains the procedures that must be performed both after running the WebLogic automation scripts on Oracle Identity Manager and Oracle Role Manager.

This section contains the following manual steps:

- [Configuring the IT Resource](#)
- [Modifying the oimORMUser ID](#)
- [Resetting the System User Passwords](#)
- [Configuring the JMS Connection Factory for XA on the Oracle Role Manager Server](#)
- [Configuring the JMS Connection Factory for XA on the Oracle Identity Manager Server](#)
- [Disabling Authentication on the Oracle Role Manager Node](#)
- [Configuring the Role Grant Approval Workflow](#)

4.5.1 Configuring the IT Resource

Configuration of the IT resource in Oracle Identity Manager must be done manually. Complete the steps described in [Section 6.9, "Configuring the IT Resource."](#)

4.5.2 Modifying the oimORMUser ID

The oimORMUser ID is by default set to ormSystem. For WebLogic, it must be changed to Internal as described in the procedure in this section.

Note: If you have a clustered server configuration, this procedure must be performed on all managed nodes.

To set the oimORMUser ID:

1. On the Oracle Identity Manager host, navigate to *ORMINT_HOME*/config.
2. Open the IMConfig.xml file for editing.
3. In the policies section, edit the oimORMUser policy to change ormSystem to Internal as follows:

```
<policy>
  <parameters>
    <parameter>
      <id>oimORMUser</id>
      <string>Internal</string>
    </parameter>
  </parameters>
</policy>
```

4. Save and close the IMConfig.xml file.

4.5.3 Resetting the System User Passwords

The automated configuration script for configuring Oracle Identity Manager creates two system users: the Internal user and the ormProxyUser. By default, these users are assigned the same password as the one provided for the Oracle Identity Manager

administrator. It is recommended that these passwords be reset as described in this section.

To reset the system user passwords:

1. Start the application server for Oracle Identity Manager if it is not running.
2. In a Web browser, connect to the Oracle Identity Manager Administrative and User Console. For example:

`http://appserverhost:7001/xlWebApp`

3. Reset the password for the Internal user as follows:
 - a. In the User ID field, enter `Internal`.
 - b. In the Password field, enter the password of the Oracle Identity Manager system administrator.
 - c. In the Manage Your Account area, click **Change Password**.
 - d. In the **Old Password** field, enter the password you just used to log in.
 - e. In the **New Password** field, enter a new password.
 - f. In the **Confirm Password** field, enter the password again.
 - g. Click **Save**, then log out.
4. Reset the password for the `ormProxyUser` user as follows:
 - a. Click **Click here to log in to Oracle Identity Manager**.
 - b. In the User ID field, enter `ormProxyUser`.
 - c. In the Password field, enter the password of the Oracle Identity Manager system administrator.
 - d. In the Manage Your Account area, click **Change Password**.
 - e. In the **Old Password** field, enter the password you just used to log in.
 - f. In the **New Password** field, enter a new password.
 - g. In the **Confirm Password** field, enter the password again.
 - h. Click **Save**, then log out.
5. Reset the password of the Internal in WebLogic as follows:
 - a. In a Web browser, connect to the WebLogic Server Console for Oracle Role Manager. For example:

`http://orm_appserverhost:7001/console`
 - b. From **Services**, select **Foreign JNDI Providers**.
 - c. Click **Remote OIM ForeignJNDIProvider**.
 - d. In the **User** field, ensure the value is `Internal`.
 - e. In the **Password** field, enter the new password of the Internal user.
 - f. In the **Confirm Password** field, enter the password again.
 - g. Click **Save**.

4.5.4 Configuring the JMS Connection Factory for XA on the Oracle Role Manager Server

To configure the JMS connection factory:

1. Start the Oracle Role Manager Admin server if it is not already started.
2. In a Web browser, log in to the WebLogic Server Console for Oracle Role Manager. For example:

`http://orm_appserverhost:7001/console`

3. From **Services**, select **Messaging**, then select **JMS Modules**.
4. Click **ORM JMSModule**.
5. Click **OIM ConnectionFactory**.
6. On the Transactions tab, select **XA Connection Factory Enabled**.
7. Click **Save**.

4.5.5 Configuring the JMS Connection Factory for XA on the Oracle Identity Manager Server

To configure the JMS connection factory:

1. Start the Oracle Identity Manager Admin server if it is not already started.
2. In a Web browser, log in to the WebLogic Server Console for Oracle Identity Manager. For example:

`http://oim_appserverhost:7001/console`

3. From **Services**, select **Messaging**, then select **JMS Modules**.
4. Click **OIM-ORM JMS Module**.
5. Click **ormJMSConnectionFactory**.
6. On the Transactions tab, select **XA Connection Factory Enabled**.
7. Click **Save**.

4.5.6 Disabling Authentication on the Oracle Role Manager Node

Disabling transaction authentication for Oracle Role Manager transactions must be done manually. Disabling transaction authentication is required when the node manager is not accepting connection due to wrong certificate configuration. Complete the steps described in [Section 7.2.5, "Disabling Authentication on the Oracle Role Manager Node."](#)

4.5.7 Configuring the Role Grant Approval Workflow

Configuration for role grant approval workflow must be done manually. Complete the steps described in [Section 6.10, "Configuring Role Grant Approval Workflow."](#)

4.6 Testing the Installation

Test the installation by following the steps in [Chapter 10, "Testing the Oracle Role Manager Integration Library Installation."](#)

Configuring Oracle Role Manager

This chapter describes the manual steps to configure Oracle Role Manager for the Oracle Role Manager Integration Library (Integration Library). The procedures in this chapter are expected to be performed in the sequence they are presented.

Note: This chapter assumes that an instance of Oracle Role Manager is installed with the standard model following the instructions in *Oracle Role Manager Installation Guide*.

Note: If you are configuring on WebLogic and have run the automated configuration scripts as described in [Chapter 4](#), you do not need to perform the manual steps in this chapter.

This chapter includes the following sections:

- [Deploying the Integration Library Configuration](#)
- [Creating the oimSystem System Identity](#)
- [Loading the oimSystem System Identity Relationship Data](#)
- [Resetting the Password for the oimSystem System Identity](#)
- [Configuring Signed Messages \(Encryption\)](#)
- [Modifying Component Configuration](#)

5.1 Deploying the Integration Library Configuration

The procedure in this section deploys the Integration Library model and configuration in the Oracle Role Manager system.

Note: If you want to modify the standard configuration of the Integration Library components, for example, to bring over additional data elements, it is recommended that you make your changes before performing the procedure in this section. For more information, see [Section 5.6, "Modifying Component Configuration."](#)

To deploy the Integration Library configuration:

1. On the Oracle Role Manager installation host, copy the oim_integration.car file from *ORM_HOME/Integration_Library/config* to *ORM_HOME/config*.

2. On the Oracle Role Manager installation host, ensure that the `db.properties` file in `ORM_HOME/config` contains the correct information. If it does not, modify it so it contains the following two lines:

```
db.driverClass=oracle.jdbc.driver.OracleDriver
db.connection_string=jdbc:oracle:thin:@$HOST$: $PORT$: $SERVICE$
```

where `$HOST$` is the database host name, `$PORT$` is the database listener port, and `$SERVICE$` is the database instance on which the Oracle Role Manager users were created.

3. Stop the Oracle Role Manager application server if it is running.
4. In a command window, navigate to `ORM_HOME/bin`.
5. Run the `deploy` command to load configuration data to the Oracle Role Manager database.

If you have no Integration Library customizations:

```
deploy.bat "../config/oim_integration.car" orm-owner ormapp-user admin-user
```

In this command:

- `orm-owner` is the user name of the Oracle Role Manager database owner user/schema
- `ormapp-user` is the user name of the Oracle Role Manager application user/schema
- `admin-user` is the user name of the Oracle Role Manager system administrator

If you have Integration Library customizations:

```
deploy.bat "collection_of_cars" orm-owner ormapp-user admin-user
```

In this command:

- `collection_of_cars` contains the relative paths and file names of the CAR files to deploy, separated by semicolon (for Windows) or colon (UNIX-based systems).

For example, in a customized deployment, the collection of CAR files on a UNIX-based system might be similar to:

```
"../config/configurations_custom.car:../config/oim_integration_custom.car"
```

- `orm-owner` is the user name of the Oracle Role Manager database owner user/schema
- `ormapp-user` is the user name of the Oracle Role Manager application user/schema
- `admin-user` is the user name of the Oracle Role Manager system administrator

Note: The collection must be enclosed within double quotation marks. The delimiters to be used are:

- For Windows systems, use semicolon (;)
 - For UNIX-based systems, use a colon (:)
-
-

(For information about modifying the standard configuration for components affecting the Integration Library, see [Section 5.6, "Modifying Component Configuration."](#))

6. At the prompts, enter the passwords of the Oracle Role Manager database owner, Oracle Role Manager application user, and Oracle Role Manager administrator.

You should see the message "Deployment successfully completed" in the command window.

5.2 Creating the oimSystem System Identity

The procedure in this section creates the oimSystem system identity to use for access to the Oracle Role Manager system by Oracle Identity Manager.

System identities are system user objects that are created for access the Oracle Role Manager system. System identities normally represent external systems, such as a user provisioning system that accesses Oracle Role Manager for role resolution for workflows or access provisioning.

To create the oimSystem system identity:

1. On the Oracle Role Manager installation host, copy the following files from `ORM_HOME/Integration_Library/config` to `ORM_HOME/config`:
 - `oim_systemIdentity.car`
 - `oim_systemIdentity.dar`
2. Stop the Oracle Role Manager application server if it is running.
3. In a command window, navigate to `ORM_HOME/bin` on the Oracle Role Manager host.
4. Run the deploy command to load the system identity data and relationships to the Oracle Role Manager database.

For UNIX-based systems:

```
sh deploy.sh "../config/oim_systemIdentity.car" orm-owner ormapp-user
admin-user
```

For Windows systems:

```
deploy.bat "..\config\oim_systemIdentity.car" orm-owner ormapp-user admin-user
```

In this command:

- `orm-owner` is the user name of the Oracle Role Manager database owner user/schema
 - `ormapp-user` is the user name of the Oracle Role Manager application user/schema
 - `admin-user` is the user name of the Oracle Role Manager system administrator
5. At the prompts, enter the passwords of the Oracle Role Manager database owner, Oracle Role Manager application user, and Oracle Role Manager administrator.

You should see the message "Deployment successfully completed" in the command window.

5.3 Loading the oimSystem System Identity Relationship Data

The oimSystem system identity is not fully functional until the relationships it needs are created. Those relationships are defined in data files and loaded through the Oracle Role Manager Administrative Console.

To load the oimSystem system identity relationship data:

1. Start the Oracle Role Manager application server.
2. From the Oracle Role Manager installation host, using a Web browser, go to the Oracle Role Manager Administrative Console. By default:
WebLogic: `http://host:7001/ormconsole`
WebSphere: `http://host:9080/ormconsole`
JBoss: `http://host:8080/ormconsole`
3. Enter the user name and password of the Oracle Role Manager administrator, then click **Log In**.
4. Click **Upload**.
5. Click **Browse**, and navigate to select the `oim_systemIdentity.dar` file found in `ORM_HOME/config`.
6. Click **Load**.

You can click **refresh** to verify that all processes are finalized.

5.4 Resetting the Password for the oimSystem System Identity

It is recommended that you reset the password for the oimSystem system identity in order for the system to store an encrypted value.

To reset the oimSystem system identity password:

1. Stop the Oracle Role Manager server.
2. On the Oracle Role Manager installation host, navigate to `ORM_HOME/config`.
3. Create a text file named `oimSystemProps.txt` containing the following system identity properties:

```
displayName = oimSystem
status = active
description = The System Identity used by the Integration Library for OIM
```

4. Navigate to `ORM_HOME/bin` and run the following command to update the system identity.

For UNIX-based systems:

```
sh systemidentity_update.sh ormapp-user oimSystem ../config/oimSystemProps.txt
```

For Windows systems:

```
systemidentity_update.bat ormapp-user oimSystem ..\config\oimSystemProps.txt
```

In this command, `ormapp-user` is the user name of the database Oracle Role Manager application user/schema.

Note: The name of the system identity must be `oimSystem` and must not be changed.

5. At the prompt, enter the password of the Oracle Role Manager application user/schema.
6. At the prompt, enter a new password for the `oimSystem` system identity.

5.5 Configuring Signed Messages (Encryption)

It is recommended that you configure the Integration Library so that your system uses digital signatures to authenticate the `oimSystem` system identity when sending messages from Oracle Identity Manager to Oracle Role Manager.

The procedure in this section first creates the key store password on the Oracle Identity Manager host and stores it to a file named `keystore.store`, then creates a random symmetric key for that password and serializes it to a file named `keystore.key`, and finally, creates a property file named `keystore.properties` and adds a single property whose value is a base64-encoded encrypted value of the key store password, encrypted using the symmetric key.

Note: Encryption must be enabled before you can perform this procedure. By default, encryption is enabled when the Integration Library is installed. For more information, see [Section 5.5.1](#).

To configure encryption:

1. On the Oracle Identity Manager host, navigate to `ORMINT_HOME/bin`.
2. Run the following command to create the Oracle Identity Manager key store.

For UNIX-based systems:

```
sh create_keystore.sh
```

For Windows systems:

```
create_keystore.bat
```

Note: If you have trouble running this command, ensure that the `JAVA_HOME` environment variable is set to an existing Java JRE location (version 1.4 or later). For WebSphere, ensure that it is set to the IBM WebSphere JDK.

The JDK used while creating the signature must be same as the application server is running on. For example, WebSphere runs by default on the IBM JDK, so while configuring the Integration Library with Oracle Identity Manager on WebSphere, signatures must be also created using the IBM JDK.

3. At the prompt, enter a password for the Oracle Identity Manager key store. You should see three files created by this command as follows:
 - `keystore.store`

This file contains the private key or the public certificate of each pair of asymmetric encryption keys for passing credentials from the integration system to Oracle Role Manager.

- keystore.key

This file contains the serialized form of a symmetric key that is used for encrypting the passwords necessary for key store and private key access.

- keystore.properties

This file contains a set of key store passwords, the values of which have been encrypted by the symmetric key in the key file and base64-encoded.

4. In the same location, run the command to create the private key for the Integration Library alias and to generate the certificate containing the public key.

For UNIX-based systems:

```
sh create_key_pair.sh oimSystem oim_orm_cert
```

For Windows systems:

```
create_key_pair.bat oimSystem oim_orm_cert
```

In this command, *oim_orm_cert* is the name to use for the certificate file.

Note: The alias must be oimSystem.

You should see the resulting certificate file named as specified with the command.

5. At the prompt, enter the key store password set in step 3.
6. At the prompt, enter a new password for the private key pair, then re-enter to confirm.
7. On the Oracle Identity Manager host, copy the new certificate file from *ORMINT_HOME/bin* to *ORM_HOME/bin* on the Oracle Role Manager host.
8. On the Oracle Role Manager host, navigate to *ORM_HOME/bin*.
9. Modify *create_keystore.sh* and *import_certificate.sh* files.

For UNIX-based systems:

- a. Open *create_keystore.sh* using vi editor.
- b. Search and replace `"../jdk/bin/java"` with `"$JAVA_HOME/bin/java"`.
- c. Save and close.
- d. Repeat the steps a,b, and c for *import_certificate.sh*.
- e. Set *JAVA_HOME* variable with the java used by ORMServer.

10. Run the command to create the Oracle Role Manager key store.

For UNIX-based systems:

```
sh create_keystore.sh
```

For Windows systems:

```
creat_keystore.bat
```

11. At the prompt, enter a password for the Oracle Role Manager key store.

12. For automated WebLogic configuration, you can stop here. The automated configuration scripts will complete the necessary configuration.

To continue with automated configuration, return to [Section 4.3, "Running the Configuration Script for Oracle Identity Manager."](#)

13. Run the command to import the certificate that was generated earlier into the Oracle Role Manager key store.

For UNIX-based systems:

```
sh import_certificate.sh oimSystem oim_orm_cert
```

For Windows systems:

```
import_certificate.bat oimSystem oim_orm_cert
```

In this command:

oim_orm_cert is the certificate file named and generated in step 4.

Note: The alias must be oimSystem.

14. At the prompt, enter the keystore password set in step 11.
15. For WebLogic manual configuration, set the system property for the Oracle Role Manager key store directory as follows:
- Log on to the WebLogic Server Console using a Web browser.
 - From **Environment**, select **Servers**, then select the server on which Oracle Role Manager is deployed.
 - On the Configuration tab, click the **Server Start** subtab.
 - In the Arguments field, append the following argument to any existing arguments:


```
-Doracle.iam.rm.encrypted.keystore_dir=ORM_HOME/bin
```

 where *ORM_HOME* is the Oracle Role Manager installation directory
 - Apply and save your changes.
 - If you are configuring a clustered server environment, repeat these steps for each server on which Oracle Role Manager is deployed.
16. For WebSphere, set the system property for the Oracle Role Manager key store directory as follows:
- Log on to the WebSphere Administrative Console using a Web browser.
 - From **Servers**, select **Application Servers**, then select the server on which Role Manager is deployed.
 - Under Server Infrastructure, expand **Java and Process Management**, then click **Process Definition**.
 - Under Additional Properties, click **Java Virtual Machine**.
 - Under Additional Properties, click **Custom Properties**.
 - Click **New**.
 - In the **Name** field, enter `oracle.iam.rm.encrypted.keystore_dir`.

- h. In the **Value** field, enter `ORM_HOME/bin` where `ORM_HOME` is the Role Manager installation directory.
 - i. In the **Description** field, enter Location of the Oracle Role Manager encryption directory.
 - j. Click **Apply**, then save your changes.
 - k. If you are configuring a clustered server environment, repeat these steps for each server on which Oracle Role Manager is deployed.
17. For JBoss, set the system property for the Oracle Role Manager key store directory as follows:
- a. On the Oracle Role Manager application server host, navigate to `JBOSS_HOME/bin`.
 - b. On Windows, open the `run.bat` file for editing, and set the system property as follows:


```
set JAVA_OPTS=-Doracle.iam.rm.encryption.keystore_dir=ORM_HOME/bin
%JAVA_OPTS%
```

where `ORM_HOME` is the Oracle Role Manager installation directory.
 - c. On UNIX-based systems, open the `run.sh` file for editing, and set the system property as follows:


```
JAVA_OPTS="-Doracle.iam.rm.encryption.keystore_dir=ORM_HOME\bin $JAVA_OPTS"
```

where `ORM_HOME` is the Oracle Role Manager installation directory.
 - d. Save and close the file.
 - e. If you are configuring a clustered server environment, repeat these steps for each server on which Oracle Role Manager is deployed.

5.5.1 Enabling Encryption

Encryption is enabled by default the Integration Library is installed. Use this procedure to re-enable encryption if encryption had been disabled previously.

Note: If you have a clustered server configuration, this procedure must be performed on all managed nodes.

To re-enable encryption:

1. On the Oracle Identity Manager host, navigate to `ORMINT_HOME/config`.
2. Open the `IMConfig.xml` file for editing.
3. In the `ormEncrypt` policy definition, set the value of the boolean element to `true` as follows:

```
<policy>
  <parameters>
    <parameter>
      <id>ormEncrypt</id>
      <boolean>true</boolean>
    </parameter>
  </parameters>
</policy>
```

4. Save and close the IMConfig.xml file.

5.6 Modifying Component Configuration

Note: If this is the first time the Integration Library is installed, perform the procedures described in this section *only* to change the configuration from the default settings. Default settings are described in the subsections below for each configurable component.

The Integration Library component configuration is deployed in the same way as other Oracle Role Manager component configuration. Configuration settings are defined in XML files and packaged as a CAR (configuration archive) file that is deployed to Oracle Role Manager system. To simplify the deployment process, it is recommended that you make all your changes to the XML files for all components that you want to reconfigure before packaging the CAR file.

This section includes the following topics:

- [Obtaining the Standard Configuration Files](#)
- [Modifying the Batch Resolution Timer](#)
- [Modifying the Role Membership Update Timers](#)
- [Modifying the Incoming Event Manager](#)
- [Modifying the Outgoing Event Manager](#)
- [Modifying the Business Logic for User Reconciliation](#)
- [Packaging Configuration Modifications](#)

5.6.1 Obtaining the Standard Configuration Files

It is recommended that the standard configuration files be used as a starting place for your configuration changes as a convenience.

To view or edit these configuration XML files, you must extract them from CAR files. There are two CAR files that contain configuration that pertains to Integration Library components: `configurations.car`, which includes the Batch Resolution Timer configuration (described in [Section 5.6.2](#)) and the configuration files for all the configurable Oracle Role Manager server components; and `oim_integration.car`, which includes the configuration files described in the subsequent sections of this chapter.

To get the standard configuration files:

1. On the Oracle Role Manager host, copy the `oim_integration.car` file in `ORM_HOME/Integration_Library/config` directory to `ORM_HOME/config`.
2. Navigate to the `ORM_HOME/config` directory.
3. Using a utility like WinZip or jar, extract the entire contents of `oim_integration.car` into a temporary location, such as `ORM_HOME/config/oim_integration_custom`.

The `oim_integration_custom` directory contains subdirectories for all the configurable components of the Integration Library. Once expanded, the files that contain configuration pertaining to the Integration Library can be found in the following layout:

```
oim_integration_custom/
```

```

config/
  oracle.iam.rm.approval.def/
    approval.oim_integration.xml
  oracle.iam.rm.bizlogic.def/
    bizlogic.oim_integration.xml
  oracle.iam.rm.event.incoming/
    oim_integration.xml
  oracle.iam.rm.event.outgoing/
    oim_integration.xml
  oracle.iam.rm.temporal/
    oim_integration.xml
  oracle.iam.rm.timer/
    approverRolePublishingTimer.xml
    businessRolePublisingTimer.xml
    itRolePublishingTimer.xml

```

The settings in these files are described in [Section 5.6.3](#) through [Section 5.6.6](#)

4. If not performed previously, extract the entire contents of configurations.car into the temporary location, such as `ORM_HOME/config/configurations_custom`.

The configurations_custom directory contains many subdirectories for all the configurable components of the Oracle Role Manager. The one subdirectory that pertains to the Integration Library can be found in the following layout:

```

configurations_custom/
  config/
    oracle.iam.rm.timer/
      batchResolutionTimer.xml

```

For more information about the settings in this file, see [Section 5.6.2](#). For information about the other configurable Oracle Role Manager server components, see *Oracle Role Manager Administrator's Guide*.

5.6.2 Modifying the Batch Resolution Timer

The batch resolution timer is included with the standard Oracle Role Manager configuration bundle and sets preferences for the batch resolution job for periodic update of user-to-role assignments calculated for complex dynamic roles (roles that have complex rules that dynamically determine membership). The batch resolution timer can have multiple jobs configured (identified by the job ID), used for integrations with external systems.

To modify the Batch Resolution Timer configuration:

1. Navigate to `ORM_HOME` on the Oracle Role Manager installation host.
2. From the temporary location where configurations.car was extracted, navigate to `configurations/config/oracle.iam.rm.timer`.
3. Edit the values in the `batchResolutionTimer.xml` file as needed.

For detailed information about the configuration settings, see [Section 5.6.2.1](#)

4. Using a utility like WinZip or jar, repackage everything in the configurations directory and create a file appended with the .car extension, for example, `configurations_custom.car`.

Ensure that the CAR file directory layout is as follows:

```

configurations/
  config/

```

```
oracle.iam.rm.timer/
  batchResolutionTimer.xml
```

If it does not match this layout, fix the layout, then repackage the CAR file.

5. Include this file in the collection of CAR files as part of the deploy command described in [Section 5.1, "Deploying the Integration Library Configuration."](#)

5.6.2.1 Batch Resolution Timer Configuration Settings

[Table 5–1](#) shows the default configuration values for the implementing Java class and whether the timer type is `simple` (defining a repeat interval of *n* milliseconds between invocations) or a `cron` timer (defining a UNIX-style cron timer). The default is the `simple` timer type. (For more information about cron expressions, see [Appendix A](#).)

Table 5–1 *Batch Resolution Timer Configuration Values*

| Element | Default Value |
|------------------------|---|
| factory-classname | oracle.iam.rm.resolution.impl.BatchResolutionTimerFactory |
| job-id | BatchResolutionJob |
| singleton | true |
| simple repeat-interval | 14400000 |
| cron cron-expression | N/A |

Note: For repeat intervals, use 3600000 for 1 hour, 7200000 for 2 hours, 14400000 for 4 hours, 28800000 for 8 hours, 86400000 for 1 day, and so forth.

The following example shows the default configuration in XML format. If you want, you can use this as a starting place for customization.

Example 5–1 *Batch Resolution Timer Default Values in XML*

```
<?xml version="1.0" encoding="UTF-8"?>
<timer-config xmlns="http://xmlns.oracle.com/iam/rm/timer/config/1_0">
  <job-configs>
    <job-config>
      <factory-classname>
        oracle.iam.rm.resolution.impl.BatchResolutionTimerFactory
      </factory-classname>
      <job-id>BatchResolutionJob</job-id>
      <group-id>BatchGroup</group-id>
      <parameters/>
      <singleton>true</singleton>
      <simple>
        <repeat-interval>14400000</repeat-interval>
      </simple>
    </job-config>
  </job-configs>
</timer-config>
```

5.6.3 Modifying the Role Membership Update Timers

The role membership update timers control the periodic process on Oracle Role Manager responsible for creating the messages for updates of role membership

information (user-to-role assignments) from Oracle Role Manager to external systems. For example, for Oracle Identity Manager, this timer triggers the update of User Group memberships based on role memberships in Oracle Role Manager.

There are three separately configurable timers for role membership updates of the following roles in Oracle Role Manager:

- Approval Roles
- Business Roles
- IT Roles

The three role membership update timer configuration files are included with the `oim_integration.car` configuration bundle and set preferences for the role membership resolution jobs. Each role membership update timer can have multiple jobs configured (identified by the job ID), used for integrations with different external systems.

It is recommended that the timer interval for any of the role membership updates is equal to or longer than the batch resolution timer interval.

To modify the Role Membership Update Timers:

1. Navigate to `ORM_HOME` on the Oracle Role Manager installation host.
2. From the temporary location where `oim_integration.car` was extracted, navigate to `oim_integration/config/oracle.iam.rm.timer`.
3. Edit the values in the any of the three timer configuration files as needed:
 - `approverRolePublishingTimer.xml`
 - `businessRolePublishingTimer.xml`
 - `itRolePublishingTimer.xml`

For detailed information about the settings in these files, see [Section 5.6.3.1](#).

4. Package your configuration changes with any other changes as described in [Section 5.6.7](#) for deployment.

5.6.3.1 Role Membership Update Timers Configuration Settings

The three configuration files for role membership update share the same default configuration. [Table 5–2](#) shows the default configuration values for the implementing Java class and whether the timer type is `simple` (defining a repeat interval of *n* milliseconds between invocations) or a `cron` timer (defining a UNIX-style cron timer). The default is the `simple` timer type. (For more information about cron expressions, see [Appendix A](#).)

Table 5–2 Role Membership Update Timers Configuration Values

| Element | Default Value |
|-------------------|---|
| factory-classname | <ul style="list-style-type: none"> ■ For Approver Roles: <code>oracle.iam.rm.resolution.impl.ApproverRolePublishingTimerFactory</code> ■ For Business Roles: <code>oracle.iam.rm.resolution.impl.BusinessRolePublishingTimerFactory</code> ■ For IT Roles: <code>oracle.iam.rm.resolution.impl.ITRolePublishingTimerFactory</code> |

Table 5–2 (Cont.) Role Membership Update Timers Configuration Values

| Element | Default Value |
|------------------------|---|
| job-id | <ul style="list-style-type: none"> ■ For Approver Roles: ApproverRolePublishingJob ■ For Business Roles: BusinessRolePublishingJob ■ For IT Roles: ITRolePublishingJob |
| singleton | true |
| simple repeat-interval | 14400000 |
| cron cron-expression | N/A |

Note: For repeat intervals, use 3600000 for 1 hour, 7200000 for 2 hours, 14400000 for 4 hours, 28800000 for 8 hours, 86400000 for 1 day, and so forth.

The following example shows the default configuration in XML format. If you want, you can use this as a starting place for customization.

Example 5–2 Example of Role Membership Update Default Values in XML

```
<?xml version="1.0" encoding="UTF-8"?>
<timer-config xmlns="http://xmlns.oracle.com/iam/rm/timer/config/1_0">
  <job-configs>
    <job-config>
      <factory-classname>
        oracle.iam.rm.resolution.impl.ApproverRolePublishingTimerFactory
      </factory-classname>
      <job-id>ApproverRolePublishingJob</job-id>
      <group-id>BatchGroup</group-id>
      <parameters>
        <parameter>
          <id>roleTypes</id>
          <string>approverRole</string>
        </parameter>
        <parameter>
          <id>userAttributes</id>
          <string>oimId,givenName,sn,displayName</string>
        </parameter>
      </parameters>
      <singleton>true</singleton>
      <simple>
        <repeat-interval>14400000</repeat-interval>
      </simple>
    </job-config>
  </job-configs>
</timer-config>
```

5.6.4 Modifying the Incoming Event Manager

The Incoming Event Manager configuration maps incoming parameters from Oracle Identity Manager to arguments required by the Oracle Role Manager business logic layer.

To modify the Incoming Event Manager component:

1. Navigate to `ORM_HOME` on the Oracle Role Manager installation host.
2. From the temporary location where `oim_integration.car` was extracted, navigate to `oim_integration/config/oracle.iam.rm.event.incoming`.
3. Edit the values in the `oim_integration.xml` file as needed.

For detailed information about the settings in this file, see [Section 5.6.4.1](#).

4. Package your configuration changes with any other changes as described in [Section 5.6.7](#) for deployment.

5.6.4.1 Incoming Event Manager Settings

The following example shows the default configuration for the Incoming Event Manager component of the Integration Library. You can use this XML content as a starting place for customization. Note that these mappings are simply samples for demonstration. In a production environment, these mappings most likely encompass custom data fields on Oracle Identity Manager and custom business logic on Oracle Role Manager.

Example 5-3 Incoming Event Manager Default Values in XML

```
<incoming-action-mapping
xmlns="http://xmlns.oracle.com/iam/rm/event/incoming/1_0">
  <dependencies>
    <business-logic-dependency def-id="bizlogic.oim_integration"
version="10.1.4" />
  </dependencies>
  <actions>
    <action id="OIM_reconcile_user" definition-id="bizlogic.oim_integration"
operation="reconcileUser">
      <parameters>
        <parameter mandatory="true">
          <source-name>Users.Key</source-name>
          <dest-name>oimId</dest-name>
          <dest-type>java.lang.Long</dest-type>
        </parameter>
        <parameter>
          <source-name>Users.First Name</source-name>
          <dest-name>givenName</dest-name>
          <dest-type>java.lang.String</dest-type>
          <default>NULL_IF_NULL</default>
        </parameter>
        <parameter>
          <source-name>Users.Last Name</source-name>
          <dest-name>sn</dest-name>
          <dest-type>java.lang.String</dest-type>
          <default>NULL_IF_NULL</default>
        </parameter>
        <parameter>
          <source-name>displayName</source-name>
          <dest-name>displayName</dest-name>
          <dest-type>java.lang.String</dest-type>
        </parameter>
      </parameters>
    </action>
  </actions>
</incoming-action-mapping>
```

```

        <default>No display name provided</default>
    </parameter>
    <parameter>
        <source-name>Users.Email</source-name>
        <dest-name>mail</dest-name>
        <dest-type>java.lang.String</dest-type>
        <default>NULL_IF_NULL</default>
    </parameter>
    <parameter>
        <source-name>Users.Xellerate Type</source-name>
        <dest-name>jobTitle</dest-name>
        <dest-type>java.lang.String</dest-type>
        <default>NULL_IF_NULL</default>
    </parameter>
    <parameter>
        <source-name>Users.Status</source-name>
        <dest-name>status</dest-name>
        <dest-type>java.lang.String</dest-type>
        <default>active</default>
    </parameter>
    <parameter>
        <source-name>Users.Manager Key</source-name>
        <dest-name>oimManagerKey</dest-name>
        <dest-type>java.lang.Long</dest-type>
    </parameter>
    <parameter>
        <source-name>deleted</source-name>
        <dest-name>deleteFlag</dest-name>
        <dest-type>java.lang.Boolean</dest-type>
        <default>>false</default>
    </parameter>
</parameters>
</action>
</actions>
</incoming-action-mapping>

```

Note: If an element is found with an empty value, the default value is used. Two special values of the `default` element indicate one of two possible treatments: 1) A value of `NULL_IF_NULL` is set to null by the incoming event manager when sent to the consuming function. This behavior is the default if there is an empty element and no default at all. 2) A value of `EMPTY_STRING_IF_NULL` is sent as an empty String.

Note: The parameter with the source-name value of `deleted` is used to control the deletion of users in Oracle Role Manager during reconciliation. By default, this is set to false.

5.6.5 Modifying the Outgoing Event Manager

The Outgoing Event Manager configuration defines how messages generated by Oracle Role Manager for role creation and role membership updates are sent to the appropriate integration queue.

To modify the Outgoing Event Manager component:

1. Navigate to *ORM_HOME* on the Oracle Role Manager installation host.
2. From the temporary location where *oim_integration.car* was extracted, navigate to *oim_integration/config/oracle.iam.rm.event.outgoing*.
3. Edit the values in the *oim_integration.xml* file as needed.

For detailed information about the settings in this file, see [Section 5.6.5.1](#).

4. Package your configuration changes with any other changes as described in [Section 5.6.7](#) for deployment.

5.6.5.1 Outgoing Event Manager Settings

The following example shows a configuration for Oracle Role Manager's Outgoing Event Manager. The configuration shown here is the default configuration supporting the Integration Library with Oracle Identity Manager.

Note: The two events in this configuration, *role_membership* and *delete_object*, are configured in this file to send updates to the specified JMS endpoint using the named connection factory. These named resources must correspond to JNDI names defined on the application server hosting Oracle Identity Manager.

Example 5–4 Outgoing Event Manager Configuration Default Values in XML

```
<event-actions-mapping xmlns="http://xmlns.oracle.com/iam/rm/event/outgoing/1_0">
  <event-actions>
    <event-action>
      <event-type>role_membership</event-type>
      <event-dests>
        <event-dest>
          <endpoint>oim/OIMserver/RoleManagerQueue</endpoint>
          <connection-factory>/oim/OIMserver/QueueConnectionFactory
          </connection-factory>
          <message-version-uri>
            http://xmlns.oracle.com/iam/rm/schema/event/event/1_0
          </message-version-uri>
        </event-dest>
      </event-dests>
    </event-action>
    <event-action>
      <event-type>delete_object</event-type>
      <event-dests>
        <event-dest>
          <endpoint>oim/OIMserver/RoleManagerQueue</endpoint>
          <connection-factory>/oim/OIMserver/QueueConnectionFactory
          </connection-factory>
          <message-version-uri>
            http://xmlns.oracle.com/iam/rm/schema/event/event/1_0
          </message-version-uri>
        </event-dest>
      </event-dests>
    </event-action>
  </event-actions>
</event-actions-mapping>
```

Note: If Oracle Role Manager is deployed on IBM WebSphere Application Server, the default value of both `connection-factory` elements is `orm/jms/QueueConFac`.

5.6.6 Modifying the Business Logic for User Reconciliation

The Business Logic configuration defines the `reconcileUser` operation by associating incoming event parameters with those required by the underlying `reconcileEntity` plug-in. You may want to edit this file to add attributes to the user data to be sent to Oracle Role Manager from an external system.

To modify the Business Logic component:

1. Navigate to `ORM_HOME` on the Oracle Role Manager installation host.
2. From the temporary location where `oim_integration.car` was extracted, navigate to `oim_integration/config/oracle.iam.rm.bizlogic.def`.
3. Edit the values in the `bizlogic.oim_integration.xml` file as needed.

For detailed information about the settings in this file, see [Section 5.6.6.1](#).

4. Package your configuration changes with any other changes as described in [Section 5.6.7](#) for deployment.

5.6.6.1 Business Logic Settings

The following example shows the default configuration for the Business Logic component of the Integration Library. You can use this XML content as a starting place for customization.

Example 5–5 Business Logic Configuration Default Values in XML

```
<config xmlns="http://xmlns.oracle.com/iam/rm/bizlogic/def/1_0"
  xmlns:i18n="http://xmlns.oracle.com/iam/rm/i18n/config/1_0"
  xmlns:t="http://xmlns.oracle.com/iam/rm/type/def/1_0"
  id="bizlogic.oim_integration" version="10.1.4">

<dependencies>
  <model-dependency id="standard_permissions" version 3.0.0"/>
</dependencies>
<operations>
  <business-transaction id="reconcileUser" related-object-type="person"
  permission="manage">
    <title>Reconcile User</title>
    <arguments>
      <argument id="startTime">
        <title>Start Date</title>
        <t:datetime>
          <t:default-value>transaction</t:default-value>
        </t:datetime>
      </argument>
      <argument id="deleteFlag">
        <title>Delete Flag</title>
        <t:boolean/>
      </argument>
      <argument id="oimId">
        <title>OIM Identifier</title>
        <related-object-type>person</related-object-type>
        <related-object-attribute>oimId</related-object-attribute>
      </argument>
    </arguments>
  </business-transaction>
</operations>
```

```

        </argument>
        <argument id="givenName">
            <title>First Name</title>
            <related-object-type>person</related-object-type>
            <related-object-attribute>givenName</related-object-attribute>
        </argument>
        <argument id="sn">
            <title>Last Name</title>
            <related-object-type>person</related-object-type>
            <related-object-attribute>sn</related-object-attribute>
        </argument>
        <argument id="displayName">
            <title>Display Name</title>
            <related-object-type>person</related-object-type>
            <related-object-attribute>displayName</related-object-attribute>
        </argument>
        <argument id="jobTitle">
            <title>Job Title</title>
            <related-object-type>person</related-object-type>
            <related-object-attribute>jobTitle</related-object-attribute>
        </argument>
        <argument id="status">
            <title>Status</title>
            <related-object-type>person</related-object-type>
            <related-object-attribute>status</related-object-attribute>
        </argument>
        <argument id="mail">
            <title>Email</title>
            <related-object-type>person</related-object-type>
            <related-object-attribute>mail</related-object-attribute>
        </argument>
        <argument id="oimManagerKey">
            <title>OIM Manager Key</title>
            <related-object-type>person</related-object-type>
            <related-object-attribute>oimManagerKey</related-object-attribute>
        </argument>
    </arguments>
    <snapshot-logic-definition
    plugin-pack-id="oracle.iam.rm.bizlogic.plugin.standard_ext"
    plugin-id="reconcile_entity">
        <ext config-version="1.0">
            <config>
                <![CDATA[
                <reconcile-entity
                xmlns="http://xmlns.oracle.com/iam/rm/bizlogic/plugin/standard_ext/1_0"
                entity-type="person"
                identifying-attribute="oimId"
                delete-flag-attribute="deleteFlag">
                    <attributes>
                        <attribute attribute-id="oimId" argument-id="oimId"/>
                        <attribute attribute-id="givenName" argument-id="givenName"/>
                        <attribute attribute-id="sn" argument-id="sn"/>
                        <attribute attribute-id="displayName" argument-id="displayName"/>
                        <attribute attribute-id="jobTitle" argument-id="jobTitle"/>
                        <attribute attribute-id="mail" argument-id="mail"/>
                        <attribute attribute-id="oimManagerKey" argument-id="oimManagerKey"/>
                        <attribute attribute-id="status" argument-id="status"/>
                    </attributes>
                </reconcile-entity>
                ]]>
            </config>
        </ext>
    </plugin-id>
</plugin-pack-id>

```

```

        </config>
    </ext>
    <effective-date>
        <argument-id>startTime</argument-id>
    </effective-date>
    </snapshot-logic-definition>
</business-transaction>
</operations>
</config>

```

5.6.7 Packaging Configuration Modifications

After you have made your modifications, the modified XML files must be repackaged into a new CAR (configuration archive) file before they can be deployed to the Oracle Role Manager system.

Note: The layout of files and directories in the new CAR file must match the layout of the original CAR file before extraction.

To package the modified configuration:

1. Navigate to the temporary location where oim_integration.car was extracted and where the XML files were modified.
2. Using a utility like WinZip or jar, repackage everything in the oim_integration directory and create a file appended with the .car extension, for example, oim_integration_custom.car.

Ensure that the CAR file directory layout is as follows:

```

oim_integration/
  config/
    oracle.iam.rm.approval.def/
      approval.oim_integration.xml
    oracle.iam.rm.bizlogic.def/
      bizlogic.oim_integration.xml
    oracle.iam.rm.event.incoming/
      oim_integration.xml
    oracle.iam.rm.event.outgoing/
      oim_integration.xml
    oracle.iam.rm.temporal/
      oim_integration.xml
    oracle.iam.rm.timer/
      approverRolePublishingTimer.xml
      businessRolePublishingTimer.xml
      itRolePublishingTimer.xml

```

If it does not match this layout, fix the layout and repackage the CAR file.

3. Include this file in the collection of CAR files as part of the deploy command described in [Section 5.1, "Deploying the Integration Library Configuration."](#)

Configuring Oracle Identity Manager

This chapter contains the manual procedures for configuring Oracle Identity Manager in preparation for the deployment of the Oracle Role Manager Integration Library. The procedures in this chapter are expected to be performed in the sequence they are presented.

Note: If you are configuring on WebLogic and have run the automated configuration scripts as described in [Chapter 4](#), you do not need to perform the manual steps in this chapter.

This chapter includes the following sections:

- [Before You Configure](#)
- [Configuring the Oracle Identity Manager Home Directory](#)
- [Creating the System User and User Group for Oracle Role Manager \(WebLogic\)](#)
- [Creating the System User and User Group for Oracle Role Manager \(WebSphere and JBoss\)](#)
- [Creating the Proxy User for Role Grant Approval Workflow](#)
- [Importing the Prepared Configuration](#)
- [Assigning the System User to the User Group](#)
- [Assigning the Proxy User to the System Group](#)
- [Configuring the IT Resource](#)
- [Configuring Role Grant Approval Workflow](#)

6.1 Before You Configure

The Oracle Role Manager Integration Library is intended to be deployed on the application server on which Oracle Identity Manager is deployed.

The procedures in this chapter assume the following:

- You have the appropriate permission to modify files in the *ORMINT_HOME* directory on the Oracle Identity Manager host.
- You have the appropriate permission to stop and start the application server on which Oracle Identity Manager is deployed.

- You know the administrator user name and password to access the Oracle Identity Manager Administrative and User Console and the Oracle Identity Manager Design Console.

6.2 Configuring the Oracle Identity Manager Home Directory

The home directory for Oracle Identity Manager is the directory that contains the xellerate directory. Depending on where Oracle Identity Manager is installed on the file system, you might need to reconfigure the Integration Library to point to the correct location for the home directory. This configuration allows localized values (such as *active* or *deleted*) to be interpreted properly when sent to Oracle Role Manager.

Note: If Oracle Identity Manager is installed in C:\oim, the default value for the Integration Library configuration, you can skip this procedure.

Note: If you have a clustered server configuration, this procedure must be performed on all managed nodes.

To configure the Oracle Identity Manager home directory:

1. On the Oracle Identity Manager host, navigate to *ORMINT_HOME*/config.
2. Open the IMConfig.xml file for editing.
3. In the policies section, edit the *oimRootdir* policy to change C:\oim to the Oracle Identity Manager installation directory as follows:

```
<policy>
  <parameters>
    <parameter>
      <id>oimRootdir</id>
      <string>OIM_HOME</string>
    </parameter>
  </parameters>
</policy>
```

where *OIM_HOME* is the full path to the installation directory of Oracle Identity Manager.

4. Save and close the IMConfig.xml file.

6.3 Creating the System User and User Group for Oracle Role Manager (WebLogic)

The configuration of Oracle Identity Manager running on the WebLogic application server requires specific naming for system users and groups for integrations. This procedure creates a user in Oracle Identity Manager to receive messages from Oracle Role Manager for user group additions, modifications or deletions.

Note: If you have a clustered server configuration, this procedure must be performed on all managed nodes.

To create and configure the Oracle Role Manager user:

1. On the Oracle Identity Manager host, navigate to *ORMINT_HOME/config*.
2. Open the *IMConfig.xml* file for editing.
3. In the policies section, edit the *oimORMUser* policy to change *ormSystem* to **Internal** as follows:

```
<policy>
  <parameters>
    <parameter>
      <id>oimORMUser</id>
      <string>Internal</string>
    </parameter>
  </parameters>
</policy>
```

4. Save and close the *IMConfig.xml* file.
5. Start the Oracle Identity Manager server if it is not running.
6. Connect to the Oracle Identity Manager Administrative and User Console. By default:

`http://host:port/xlWebApp`

7. If the user named **Internal** does not exist, create it as follows:
 - a. Select **Users**, then select **Create**.

Note: For Oracle Identity Manager on WebLogic, the user ID must be **Internal** and should not be changed.

- b. In the **User ID** field, enter **Internal**.
- c. In the **Password** field, enter a password for the user.
- d. In the **Confirm Password** field, enter the same password.
- e. In the **First Name** field, enter a value.
- f. In the **Last Name** field, enter a value.
- g. In the **Organization** field, click the Lookup icon.
- h. Select the organization in which you want to create the **Internal** user, for example, **Xellerate Users**.
- i. Click **Select**, then click **Create User**.

6.4 Creating the System User and User Group for Oracle Role Manager (WebSphere and JBoss)

This procedure creates a user in Oracle Identity Manager to receive messages from Oracle Role Manager for user group additions, modifications or deletions.

To create the Oracle Role Manager user:

1. Start the Oracle Identity Manager server if it is not running.
2. Connect to the Oracle Identity Manager Administrative and User Console. By default:

`http://host:port/xlWebApp`

3. Create the `ormSystem` user as follows:

- a. Select **Users**, then select **Create**.
- b. In the **User ID** field, enter `ormSystem`.

Note: For Oracle Identity Manager on JBoss and WebSphere application servers, the user ID must be `ormSystem` and must not be changed.

- c. In the **Password** field, enter `ormSystem`.
- d. In the **Confirm Password** field, enter `ormSystem`.
- e. In the **First Name** field, enter a first name for the user, such as `orm`.
- f. In the **Last Name** field, enter a last name for the user, such as `System`.
- g. In the **Organization** field, click the magnifying icon.
- h. In the Lookup Form window, select the organization in which you want to create the `ormSystem` user.
- i. Click **Select**.
- j. Click **Create User**.

6.5 Creating the Proxy User for Role Grant Approval Workflow

Note: If you have a clustered server configuration, this procedure must be performed on all managed nodes.

To create and configure the Oracle Role Manager proxy user:

1. Start the Oracle Identity Manager server if it is not running.
2. Connect to the Oracle Identity Manager Administrative and User Console.
3. Select **Users**, then click **Create**.
4. In the **User ID** field, enter `ormProxyUser`.

Note: The user ID must be `ormProxyUser` and should not be changed.

5. In the **Password** field, enter a password for the user.
6. In the **Password** field, enter a password for the user.
7. In the **Confirm Password** field, enter the same password.
8. In the **First Name** field, enter a value.
9. In the **Last Name** field, enter a value.
10. In the **Organization** field, click the Lookup icon, then select the organization in which you want to create the user, for example, **Xellerate Users**.
11. Click **Select**, then click **Create User**.

6.6 Importing the Prepared Configuration

The Oracle Role Manager Integration Library requires significant configuration of Oracle Identity Manager. For convenience, there are two pre-built XML files to use to easily import configuration data into Oracle Identity Manager. These two files are `ormoimBase.xml` and `ormoimSample.xml`.

The first file, `ormoimBase.xml`, contains the essential configurations for a working integration and includes the configurations for role grant approvals. The second file, `ormoimSample.xml`, contains configurations for a sample resource and approval process. This sample is helpful in understanding and demonstrating a working approval process that looks to Oracle Role Manager for approvers for a role, before creating similar resources and workflows for a production environment.

Note: The following procedures assume that the Oracle Identity Manager administrator user ID is `xelsysadm`. If your installation of Oracle Identity Manager uses a different user for access, you must modify the `ormoimBase.xml` file and the `ormoimSample.xml` file to match.

This section includes the following topics:

- [Importing the Base Configuration](#)
- [Importing the Sample Configuration for Approver Role Resolution](#)

6.6.1 Importing the Base Configuration

The base configuration provides the framework configuration for the Oracle Role Manager Integration Library and is a prerequisite to any additional configuration relating to the integration.

To import the Integration Library base configuration:

1. Start the Oracle Identity Manager server if it is not running.
2. Connect to the Oracle Identity Manager Administrative and User Console.
3. Select **Deployment Management**, then select **Import**.
4. In the Select File for Import window, browse to `ORMINT_HOME/config` and select `ormoimBase.xml`, then click **Add File**.
5. On the Substitutions page, click **Next** to make no substitutions, then click **Next** again to confirm.
6. Depending on the application server on which Oracle Identity Manager is deployed, define the parameters of the IT Resource for Oracle Role Manager as follows:

Note: All values are case-sensitive and must be entered exactly as shown here.

- **For WebLogic**

| Field | Value |
|-------------------------|---|
| ormJMSConnectionFactory | external/srqueues/orm/QueueConnectionFactory |
| ormJMSQueue | orm/queue/IncomingEventQueue |
| ormServerURL | t3://ORM_appserver:port |
| initialContextFactory | weblogic.jndi.WLInitialContextFactory |
| ormServerJNDI | ejb/orm/ServerEJB |
| ormAdmin | oimSystem |
| ormPassword | Enter the password of the oimSystem system identity that was set in Section 5.2 . |

Note: The ormServerURL port value must be the port for access to the Oracle Role Manager Web UI and administrative console.

Note: In a clustered environment, ormServerURL must be populated with all the managed servers for Oracle Role Manager. For example, t3://ORM_appserver1:port1,ORM_appserver2:port2

■ **For WebSphere**

| Field | Sample Value |
|-------------------------|---|
| ormServerJNDI | orm/ejb/ServerEJB |
| ormAdmin | oimSystem |
| ormPassword | Enter the password of the oimSystem system identity that was set in Section 5.2 , "Creating the oimSystem System Identity." |
| ormServerURL | corbaloc:iiop:orm_appserver:bootstrap_address Note: In a clustered environment, this value must include each managed server for Oracle Role Manager, separated by a comma. For example, corbaloc:iiop:orm_appserver1:bootstrap_address1,orm_appserver2:bootstrap_address2 |
| ormJMSQueue | orm/jms/IncomingEventQueue |
| initialContextFactory | com.ibm.websphere.naming.WsnInitialContextFactory |
| ormJMSConnectionFactory | orm/jms/QueueConFac |

■ **For JBoss**

| Field | Value |
|-------------|---|
| ormJMSQueue | queue/orm/IncomingEventQueue |
| ormAdmin | oimSystem |
| ormPassword | Enter the password of the oimSystem system identity that was set in Section 5.2 , "Creating the oimSystem System Identity." |

| Field | Value |
|-------------------------|--|
| initialContextFactory | org.jnp.interfaces.NamingContextFactory |
| ormServerJNDI | ejb/orm/ServerEJB |
| ormServerURL | jnp://orm_appserver:jndi_port where <i>orm_appserver</i> is the IP address or host name of the Oracle Role Manager host, and <i>jndi_port</i> is the JNDI port of that host. Note: In a clustered environment, this value must include each managed server for Oracle Role Manager, separated by a comma. For example, <i>jnp://orm_appserver1:jndi_port1,orm_appserver2:jndi_port2</i> . The default JNDI port in JBoss is 1100. |
| ormJMSConnectionFactory | queue/QueueConnectionFactory |

7. Click **Next**, then click **Skip** to skip the current resource instance.
8. On the Confirmation page, ensure that the information is correct.
To make changes, click **Back**.
9. Click **View Selections**.
10. Click **Import**, then click **Import** to confirm.
You should see a confirmation message that import was successful.
11. Click **OK**, then close the Import window.

6.6.2 Importing the Sample Configuration for Approver Role Resolution

This procedure is necessary only if you want to test the Oracle Role Manager Integration Library with a sample workflow for role approvals using the configuration provided as a convenience for demonstration purposes.

To import the Integration Library sample configuration:

1. From the Oracle Identity Manager Administration and User Console, select **Deployment Management**, then select **Import**.
2. Browse to the *ORMINT_HOME*/samples directory, select *ormoimSample.xml*, then click **Add File**.
3. Click **Next** to make no substitutions, then click **Next** again to confirm.
In the Summary pane, you should see that six objects are ready to be imported, including one resource, one data object definition, one process form, one task adapter, and two processes.
4. Click **Import**, then click **Import** to confirm.
5. Click **OK**, then close the Import window.

6.7 Assigning the System User to the User Group

Depending on the application server on which Oracle Identity Manager is deployed, perform either of the two following procedures.

(WebLogic) To assign the Internal system user to the User user group:

1. From the Oracle Identity Manager Administration and User Console, select **Users**, then select **Manage**.
2. Search for the user named Internal.
3. Click **INTERNAL** to view details.
4. On the User Details page, select **Group Membership** from the list.
5. Click **Assign**.
6. Select the box in the row for the group named **User**.
7. Click **Assign Group**.
8. Click **Confirm Assign** to confirm.

(WebSphere and JBoss) To assign the ormSystem user to the ormSystem user group:

1. From the Oracle Identity Manager Administration and User Console, select **Users**, then select **Manage**.
2. Search for the user named ormSystem (created in [Section 6.4](#)).
3. Click **ormSystem** to view details.
4. On the User Details page, select **Group Membership** from the list.
5. Click **Assign**.
6. Select the box in the row for the group named **ormSystem**.
7. Click **Assign Group**.
8. Click **Confirm Assign** to confirm.

6.8 Assigning the Proxy User to the System Group

Depending on the application server on which Oracle Identity Manager is deployed, perform either of the two following procedures.

(WebLogic) To assign the proxy user to the User user group:

1. From the Oracle Identity Manager Administration and User Console, select **Users**, then select **Manage**.
2. Search for the user named ormProxyUser (created in [Section 6.5](#)).
3. Click **ORMPROXYUSER** to view details.
4. On the User Details page, select **Group Membership** from the list.
5. Click **Assign**.
6. Select the box in the row for the group named **User**.
7. Click **Assign Group**.
8. Click **Confirm Assign** to confirm.

(WebSphere and JBoss) To assign the proxy user to the ormSystem user group:

1. From the Oracle Identity Manager Administration and User Console, select **Users**, then select **Manage**.
2. Search for the user named ormProxyUser (created in [Section 6.5](#)).

3. Click **ORMPROXYUSER** to view details.
4. On the User Details page, select **Group Membership** from the list.
5. Click **Assign**.
6. Select the box in the row for the group named **ormSystem**.
7. Click **Assign Group**.
8. Click **Confirm Assign** to confirm.

6.9 Configuring the IT Resource

The IT Resource system property provides the name of the IT Resource in Oracle Identity Manager to access the Oracle Role Manager Integration Library software through the Oracle Role Manager IT Resource.

Note: The Oracle Identity Manager Design Console is not available on UNIX-based systems. To perform this procedure, use an installation on a Windows host.

To configure the IT Resource

1. Start the Oracle Identity Manager server if it is not already running.
2. Start the Oracle Identity Manager Design Console, either from the Windows Start menu or with the `xlclient.cmd` command.
3. Log in as the Oracle Identity Manager Administrator.
4. On the left pane, expand the **Administration** folder.
5. Double-click **System Configuration**.
6. Choose the **Server** option.
7. In the **Name** field, enter `ORMITResourceName` as the name of the system property to create.
8. In the **Keyword** field, enter `XL.ORMITResourceName`.
9. In the **Value** field, enter `ORM ITResource`.

Note: The key should not be supplied as it is generated automatically the system.

10. Click the Save icon on the toolbar.
11. Ensure that the values for the IT resource parameters are correct:
 - a. Connect to the Oracle Identity Manager Administrative and User Console. By default:
`http://host:port/xlWebApp`
 - b. Select **Resource Management**, then click **Manage IT Resource**.
 - c. Search for and select the IT resource named `ORM ITResource`.
 - d. On the View IT Resource Details and Parameters page, verify that the values displayed in the fields are the same as the values mentioned in step 6 of [Section 6.6.1](#).

If the values are different, Click **Edit** to modify the values, as appropriate, then click **Update**.

- e. For WebLogic, if you have used the automated configuration, click **Edit** to enter a new password in the `ormPassword` field for the `oimSystem` system identity, then click **Update**.
12. If Oracle Identity Manager is installed on WebLogic, assign permissions as follows:
- a. From the **You can view additional information about this IT resource** list, select **Administrative Groups**.
 - b. Click **Assign Group**.
 - c. For the `User` user group, select **Write Access**, **Delete Access**, and **Assign**.
 - d. Click the **Assign** button.

6.10 Configuring Role Grant Approval Workflow

Note: The Oracle Identity Manager Design Console is not available on UNIX-based systems. To perform this procedure, use an installation on a Windows host. Refer to *Oracle Identity Manager Installation Guide* for more information.

To configure the role grant approval workflow:

1. Start the Oracle Identity Manager server if it is not already running.
2. Connect to the Oracle Identity Manager Administrative and User Console. By default:

```
http://host:port:/xlWebApp
```
3. Assign the `User` and `ormSystem` user groups as administrative groups as follows:
 - a. Select **User Groups**, then select **Manage**.
 - b. Search for and select **System Administrators**.
 - c. Select **Members and Sub-Groups** from the list.
 - d. Click **Assign Subgroups**.
 - e. If your deployment is on WebLogic, for the `User` user group, select **Assign**.
 - f. If your deployment is on WebSphere or JBoss, for the `ormSystem` user group, select **Assign**.
 - g. Click the **Assign** button, then click **Confirm Assign**.
4. Start the Oracle Identity Manager Design Console, either from the Windows Start menu or with the `xlclient.cmd` command, then log in as the Oracle Identity Manager Administrator.
5. Suppress the standard approval as follows:
 - a. On the left pane, expand the **Process Management** folder.
 - b. Double-click **Process Definition**.
 - c. Click the Lookup icon, then click the right arrow to navigate to the Standard Approval process definition.
 - d. On the Tasks tab, double-click the row number to the left of the **Approve** task.

- e. On the Integration tab, click **Add**.
 - f. Choose the **System** option, select **tcCompleteTask**, then click the Save icon.
 - g. Click **OK**, then close the window.

You should see the tcCompleteTasks event handler listed for the Approve task in the process definition.
6. Assign the proxy user as the default assignee for the Role Grant Approval task as follows:
 - a. Click the right arrow and navigate to the RoleGrantApprovalApProcDef process definition.
 - b. On the Tasks tab, double-click the row number to the left of the **Approval Task** task.
 - c. On the Assignment tab, double-click the User field that contains XELSYSADM.
 - d. Select **ORMPROXYUSER**, then click **OK**.
 - e. Click the Save icon, click **OK**, then close the window.
 - f. Click the Save icon on the toolbar.
 7. Optionally, change the assignee for Second Approval as follows:
 - a. In the same process definition, on the Tasks tab, double-click the row number to the left of the **Second Approval** task.
 - b. On the Assignment tab, double-click the User field that contains XELSYSADM.
 - c. Select the user that would be the second approval, then click **OK**.
 - d. Click the Save icon, click **OK**, then close the window.
 - e. Click the Save icon on the toolbar.
 8. Optionally, change the assignee for Third Approval as follows:
 - a. In the same process definition, on the Tasks tab, double-click the row number to the left of the **Third Approval** task.
 - b. On the Assignment tab, double-click the User field that contains XELSYSADM.
 - c. Select the user that would be the third approval, then click **OK**.
 - d. Click the Save icon, click **OK**, then close the window.
 - e. Click the Save icon on the toolbar.
 9. Configure the OfflineRequestSubmission system property as follows:
 - a. In the left pane, expand **Administration**.
 - b. Double-click **System Configuration**.
 - c. Choose the **Server** option.
 - d. In the **Name** field, enter `OfflineRequestSubmission`.
 - e. In the **Keyword** field, enter `XL.OfflineRequestSubmission`.
 - f. In the **Value** field, enter `off`.
 - g. Click the Save icon on the toolbar.

You should see that the key value has been generated automatically.

Configuring WebLogic Server

This chapter contains procedures for manual configuration of the WebLogic application servers for Oracle Identity Manager and Oracle Role Manager in preparation for deployment of the Oracle Role Manager Integration Library (Integration Library). The procedures in this chapter are expected to be performed in the sequence they are presented.

Note: If you run the automated configuration scripts as described in [Chapter 4](#), you do not need to perform the manual steps in this chapter.

This chapter includes the following sections:

- [Before You Configure](#)
- [Configuring the Oracle Role Manager Server](#)
- [Configuring the Oracle Identity Manager Server](#)
- [Deploying the Oracle Role Manager Integration Library Application on WebLogic](#)

7.1 Before You Configure

The Oracle Role Manager Integration Library is intended to be deployed on the application server on which Oracle Identity Manager is deployed. The procedures in this chapter assume the following:

- You have the access to the files in *ORMINT_HOME*.
- You have the appropriate permission to add and modify files in the application servers where Oracle Identity Manager and Oracle Role Manager are deployed.
- You have the appropriate permission to stop and start the application servers where Oracle Identity Manager and Oracle Role Manager are deployed.
- You have access to the WebLogic Server Administrative Console and know the administrator user ID and password for the domains where Oracle Identity Manager and Oracle Role Manager are deployed.
- For clustered environments, the managed servers in the cluster can be started and stopped remotely on the administrative console.

7.2 Configuring the Oracle Role Manager Server

This procedure assumes that a WebLogic server and domain have been created for Oracle Role Manager with a host alias set for port access to Oracle Role Manager.

This section includes the following subsections:

- [Configuring the JMS Connection Factory](#)
- [Configuring the Foreign JNDI Providers](#)
- [Configuring the Security Credentials](#)
- [\(Clustered Mode Only\) Configuring the Subdeployment of the Connection Factory](#)
- [Disabling Authentication on the Oracle Role Manager Node](#)

7.2.1 Configuring the JMS Connection Factory

To configure the JMS module connection factory:

1. Start the Oracle Role Manager server if it is not already started.
2. In a Web browser, log in to the WebLogic Server Console. For example:
`http://appserverhost:7001/console`
3. From **Services**, select **Messaging**, then select **JMS Modules**.
4. Click **ORM JMSModule**.
5. Click **New**.
6. Select the **Connection Factory** option.
7. Click **Next**.
8. In the **Name** field, enter `OIM ConnectionFactory`.
9. In the **JNDI Name** field, enter `external/srqueues/orm/QueueConnectionFactory`.
10. Click **Next**, then click **Finish**.
11. Click **OIM ConnectionFactory**.
12. Ensure that Default Targeting is enabled.
13. On the Transactions tab, select **XA Connection Factory Enabled**.
14. Click **Save**.

You should see the new connection factory in the list.

7.2.2 Configuring the Foreign JNDI Providers

To configure the foreign JNDI providers:

1. From **Services**, select **Foreign JNDI Providers**.
2. Click **New**.
3. In the **Name** field, enter `Remote OIM ForeignJNDIProvider`.
4. Click **OK**.
5. Click **Remote OIM ForeignJNDIProvider**.

6. In the **Initial Context Factory** field, enter `weblogic.jndi.WLInitialContextFactory`.
7. In the **Provider URL** field, enter `t3://oim_ipaddress:oim_port` where
oim_ipaddress is the IP address of the Oracle Identity Manager application server host
oim_port is the port for access to the Oracle Identity Manager server

Note: If you are configuring a clustered server environment, the URL must be in the form `t3://oim_ipaddress1:port,oim_ipaddress2:port`

8. In the **User** field, enter `Internal`.
9. In the **Password** field, enter the password of the Internal user.
10. In the **Confirm Password** field, enter the password again.
11. Click **Save**.
12. Configure the Remote OIM Connection Factory as follows:
 - a. From **Services**, select **Foreign JNDI Providers**.
 - b. Click **Remote OIM ForeignJNDIProvider**.
 - c. On the Links tab, click **New**.
 - d. In the **Name** field, enter `RoleUpdateQCF`.
 - e. In the **Local JNDI Name** field, enter `oim/OIMserver/QueueConnectionFactory`.
 - f. In the **Remote JNDI Name** field, enter `oim/OIMserver/QueueConnectionFactory`.
 - g. Click **OK**.
13. Configure the Remote OIM Queue as follows:
 - a. On the Links tab, click **New**.
 - b. In the **Name** field, enter `RoleUpdateQueue`.
 - c. In the **Local JNDI Name** field, enter `oim/OIMserver/RoleManagerQueue`.
 - d. In the **Remote JNDI Name** field, enter `oim/OIMserver/RoleManagerQueue`.
 - e. Click **OK**.

7.2.3 Configuring the Security Credentials

To configure the credentials:

1. Click the domain on which Oracle Role Manager is deployed.
2. On the Security tab, expand **Advanced**.
3. Clear any value in the **Credential** field.
4. In the **Credential** field, enter the domain credential of the Oracle Identity Manager server.

Note: The domain credential is generated when the server is started and ensures that by default no two WebLogic server domains have the same credential. In this case, the same credentials are entered for both Oracle Identity Manager and Oracle Role Manager.

5. In the **Confirm Credential** field, enter the credential again.
6. Click **Save**.
7. Restart the Oracle Role Manager server.

7.2.4 (Clustered Mode Only) Configuring the Subdeployment of the Connection Factory

Note: In you are configuring a clustered environment, perform this procedure for each managed server.

To change the subdeployment of the Oracle Identity Manager connection factory:

1. In the domain tree, select **Services**, then select **Messaging**.
2. Select **JMS Modules**, then click **ORM JMSModule**.
3. Click **OIM ConnectionFactory**.
4. Deselect the **Default Targeting Enabled** box, then click **Save**.
5. Click the **Subdeployment** tab.
6. In the **Subdeployment** list, select **cf-sub**.
7. Click **Save**.

7.2.5 Disabling Authentication on the Oracle Role Manager Node

This procedure disables transaction authentication for Oracle Role Manager transactions. Disabling transaction authentication is required when the node manager is not accepting connection due to wrong certificate configuration.

Note: In you are configuring a clustered environment, perform this procedure for each managed node.

To disable authentication on the Oracle Role Manager node:

1. Navigate to `WEBLOGIC_HOME\common\nodemanager` folder and edit the `nodemanager.properties` file.
2. Change the value of the `AuthenticationEnabled` property to `false`.
3. Restart all the servers on the Oracle Role Manager domain including the admin server.

7.3 Configuring the Oracle Identity Manager Server

This procedure assumes that a WebLogic server and domain has been created for Oracle Identity Manager.

For clustered environments, it is assumed that the managed servers in the cluster can be started and stopped remotely on the administrative console and that the Integration Library software has been distributed on all managed nodes.

This section includes the following subsections:

- [Modifying the Oracle Identity Manager Startup Script](#)
- [Configuring the Shared Libraries](#)
- [\(Clustered Mode Only\) Configuring JMS Queues and Connection Factories](#)
- [\(Nonclustered Mode Only\) Configuring JMS Queues and Connection Factories](#)
- [Configuring Foreign JMS Queues and Connection Factories](#)
- [Configuring Security Credentials](#)
- [\(Clustered Mode Only\) Adding the Integration Library System Properties](#)

7.3.1 Modifying the Oracle Identity Manager Startup Script

If you are invoking Oracle Identity Manager using a startup script, you must edit the script to include the path to the Integration Library software and add the Integration Library binaries to the classpath before you can start using the Oracle Role Manager Integration Library. Making this change before the Integration Library software is deployed does not affect the operation of Oracle Identity Manager until it is restarted.

To modify the startup script:

1. On the Oracle Identity Manager host, navigate to the bin directory on the domain on which Oracle Identity Manager is deployed. For example, `WEBLOGIC_HOME/user_projects/domains/oimdomain/bin`.
2. Open the start script for editing
 - For UNIX-based systems, open `xlStartWLS.sh`.
 - For Windows systems, open `xlStartWLS.cmd`

Note: If you have a managed server environment where the server is started from this script, open the `xlStartManagedWebLogic.sh` or `xlStartManagedWebLogic.cmd` instead.

3. Add the following libraries to the CLASSPATH environment setting:

```
ORMINT_HOME/lib/commons-logging.jar;ORMINT_HOME/lib/orm_encryption.jar;
ORMINT_HOME/lib/server_api_14.jar
```

where `ORMINT_HOME` is the full path to the home directory of the Oracle Role Manager Integration Library.

4. Modify the `JAVA_OPTIONS` entry as follows:
 - a. For UNIX-based systems, add a backslash (\) at the end of the `-Djava.awt.headless=true` argument.
 - b. For Windows system, add a caret (^) at the end of the `-Djava.awt.headless=true` argument.
 - c. Add the following argument to the end of the `JAVA_OPTIONS` entry:


```
-DORMINT_ROOT_DIR=ORMINT_HOME
```

where *ORMINT_HOME* is the full path to the home directory of the Oracle Role Manager Integration Library.

- d. Optionally, to enable logging for the Integration Library, add the following argument to the end of the *JAVA_OPTIONS* entry:

```
-Djava.util.logging.config.file=ORMINT_HOME/config/logging.properties
```

where *ORMINT_HOME* is the full path to the home directory of the Oracle Role Manager Integration Library.

5. Save and close the start script.

7.3.2 Configuring the Shared Libraries

Note: In a clustered server environment, perform this procedure on all managed nodes.

To configure the shared libraries:

1. On the file system where Oracle Identity Manager is deployed, create the following directory if it does not exist:

```
OIM_appserver/jdk/jre/lib/endorsed
```

where *OIM_appserver/jdk* is the JDK directory for WebLogic, either Sun JDK or WebLogic JRockit.

2. Copy the following libraries into the *endorsed* directory:

```
ORMINT_HOME/lib/xercesImpl.jar  
ORMINT_HOME/lib/xml-apis.jar
```

3. Restart the Oracle Identity Manager server.

7.3.3 (Clustered Mode Only) Configuring JMS Queues and Connection Factories

To configure JMS queues and connection factories:

1. In a Web browser, log in to the WebLogic Server Console. For example:

```
http://appserverhost:7001/console
```

2. Configure a JMS queue connection factory as follows:

- a. From **Services**, select **Messaging**, then select **JMS Modules**.
- b. Click **New**.
- c. In the **Name** field, enter *OIM-ORM JMS Module*, then click **Next**.
- d. Assign the JMS module to the Oracle Identity Manager cluster, for example **OIM_Cluster**, then click **Next**.
- e. Click **Next**.
- f. Select the **Would you like to add resources** box, then click **Finish**.
- g. On the Settings page, click **New**.
- h. Select **ConnectionFactory**, then click **Next**.
- i. In the **Name** field, enter *ormJMSConnectionFactory*.

- j. In the **JNDI Name** field, enter `/oim/OIMserver/QueueConnectionFactory`.
 - k. Click **Next**, then click **Finish**.
 - l. Click **ormJMSConnectionFactory**.
 - m. On the Transactions tab, select **XA Connection Factory Enabled**.
 - n. Click **Save**.
3. Configure a JMS server for each Oracle Identity Manager managed server as follows:
 - a. From **Services**, select **Messaging**, then select **JMS Servers**.
 - b. Click **New**.
 - c. In the **Name** field, enter `ORMIntegration1`, then click **Next**.
 - d. Click **Finish**.
 - e. Click the newly created JMS server, for example **ORMIntegration1**.
 - f. Select the Targets tab and assign the JMS server to the first Oracle Identity Manager managed server, for example, **OIM_Server1**.
 - g. Click **Save**.
 - h. Repeat these steps for each managed server. For example, create `ORMIntegration2` and assign it to `OIM_Server2`, and so on.
4. Configure a distributed JMS queue as follows:
 - a. From **Services**, select **Messaging**, then select **JMS Modules**.
 - b. Click **OIM-ORM JMS Module**, then click **New**.
 - c. Select **Distributed Queue**, then click **Next**.
 - d. In the **Name** field, enter `ormJMSQueue`.
 - e. In the **JNDI Name** field, enter `oim/OIMserver/RoleManagerQueue`.
 - f. Click **Next**.
 - g. Click **Advanced Targeting**.
 - h. Click **Create a New Subdeployment**.
 - i. In the **Subdeployment Name** field, enter `ormJMSQueue subdeployment`.
 - j. Click **OK**.
 - k. Select each of the JMS servers created in step 3. For example, **ORMIntegration1** and **ORMIntegration2**.
 - l. Click **Finish**.

7.3.4 (Nonclustered Mode Only) Configuring JMS Queues and Connection Factories

To configure JMS queues and connection factories:

1. In a Web browser, log in to the WebLogic Server Console. For example:
`http://appserverhost:7001/console`
2. Configure a JMS queue connection factory as follows:

- a. From **Services**, select **Messaging**, then select **JMS Modules**.
 - b. Click **New**.
 - c. In the **Name** field, enter `OIM-ORM JMS Module`, then click **Next**.
 - d. Select **AdminServer**, then click **Next**.
 - e. Select **Would you like to add resources**, then click **Finish**.
 - f. On the Settings page, click **New**.
 - g. Choose the **ConnectionFactory** option, then click **Next**.
 - h. In the **Name** field, enter `ormJMSConnectionFactory`.
 - i. In the **JNDI Name** field, enter `/oim/OIMserver/QueueConnectionFactory`.
 - j. Click **Next**, then click **Finish**.
 - k. Click **ormJMSConnectionFactory**.
 - l. On the Transactions tab, select **XA Connection Factory Enabled**.
 - m. Click **Save**.
3. Configure a JMS server as follows:
- a. From **Services**, select **Messaging**, then select **JMS Servers**.
 - b. Click **New**.
 - c. In the **Name** field, enter `ORMIntegration`.
 - d. Click **Finish**.
 - e. Click **ORMIntegration**.
 - f. On the Targets tab, select **AdminServer** from the Targets list.
 - g. Click **Save**.
4. Configure a JMS queue as follows:
- a. From **Services**, select **Messaging**, then select **JMS Modules**.
 - b. Click **OIM-ORM JMS Module**, then click **New**.
 - c. Choose the **Queue** option, then click **Next**.
 - d. In the **Name** field, enter `ormJMSQueue`.
 - e. In the **JNDI Name** field, enter `oim/OIMserver/RoleManagerQueue`.
 - f. Click **Next**.
 - g. Click **Create a New Subdeployment**.
 - h. In the **Subdeployment Name** field, enter `ormJMSQueue subdeployment`.
 - i. Click **OK**, then click **Next**.
 - j. Select **ORMIntegration** as the JMS Server.
 - k. Click **Finish**.

7.3.5 Configuring Foreign JMS Queues and Connection Factories

To configure Foreign JMS queues and connection factories:

1. Configure a foreign JNDI provider as follows:
 - a. From **Services**, select **Foreign JNDI Providers**, then click **New**.
 - b. In the **Name** field, enter `OIM ORM server`.
 - c. Click **OK**.
 - d. Click **OIM ORM server**.
 - e. In the **Initial Context Factory** field, enter `weblogic.jndi.WLInitialContextFactory`.
 - f. In the **Provider URL** field, enter `t3://orm_ipaddress:orm_port` where
 where
`orm_ipaddress` is the IP address of the Oracle Role Manager application server host
`orm_port` is the port for access to the Oracle Role Manager administrative console and Web UI.

Note: If you are configuring a clustered server environment, the URL must be in the form `t3://orm_ipaddress1:port,orm_ipaddress2:port`

 - g. In the **User** field, enter the user name of the WebLogic Administrator.
 - h. In the **Password** field and **Confirm Password** field, enter the password of the WebLogic Administrator.
 - i. Click **Save**.
2. Configure foreign JNDI links as follows:
 - a. From **Services**, select **Foreign JNDI Providers**.
 - b. Click **OIM ORM server**.
 - c. On the **Links** tab, click **New**.
 - d. In the **Name** field, enter `OIMORMQueueConnectionFactory`.
 - e. In the **Local JNDI Name** field, enter `external/srqueues/orm/QueueConnectionFactory`.
 - f. In the **Remote JNDI Name** field, enter `external/srqueues/orm/QueueConnectionFactory`.

Note: The locale and remote JNDI names must be the same as the JNDI name set in [Section 7.2.1, "Configuring the JMS Connection Factory."](#)

 - g. Click **OK**.
 - h. On the **Links** tab, click **New**.
 - i. In the **Name** field, enter `OIM ORM Queue`.
 - j. In the **Local JNDI Name** field, enter `orm/queue/IncomingEventQueue`.

- k. In the **Remote JNDI Name** field, enter `orm/queue/IncomingEventQueue`.
- l. Click **OK**.

7.3.6 Configuring Security Credentials

To configure the credentials:

1. Click the domain where the Oracle Identity Manager server resides.
2. On the Security tab, expand the **Advanced** link at the bottom of the page.
3. In the **Credential** field, clear any existing credential, then enter the same domain credential that was used for the Oracle Role Manager server (see step 4 of [Section 7.2.3](#)).

Note: The domain credential is generated when the server is started and ensures that by default no two WebLogic server domains have the same credential. In this case, the same credentials are entered for both Oracle Identity Manager and Oracle Role Manager.

4. In the **Confirm Credential** field, enter the credential again.
5. Click **Save**.
6. If you have a non-clustered server environment, restart the Oracle Identity Manager server. For clustered server environments, continue configuration steps in the next section before restarting the server.

7.3.7 (Clustered Mode Only) Adding the Integration Library System Properties

Note: Perform this procedure on all managed nodes.

To add the Integration Library JVM system properties:

1. Log on to the WebLogic Server administrative console using a Web browser.
2. For each managed server, configure the system properties as follows:
 - a. On the Oracle Identity Manager domain of the primary node, select the domain name, then select **Servers**.
 - b. Select the first managed server, for example, **OIM_Server1**.
 - c. On the Configuration tab, click the **Server Start** subtab.
 - d. In the **ClassPath** field, add the following Integration Library paths to the existing classpath settings:

```
ORMINT_HOME\lib\commons-logging.jar
ORMINT_HOME\lib\orm_encryption.jar
ORMINT_HOME\lib\server_api_14.jar
```

- e. In the **Arguments** field, append the following argument to any existing arguments:

```
-DORMINT_ROOT_DIR=ORMINT_HOME
```

where *ORMINT_HOME* is the Integration Library installation directory. For example, *C : /ORMINT_HOME*.

- f. Optionally, to enable logging for the Integration Library, in the **Arguments** field, add the following argument:

```
-Djava.util.logging.config.file=ORMINT_HOME/config/logging.properties
```

where *ORMINT_HOME* is the Integration Library installation directory. For example, *C : /ORMINT_HOME*.

- g. Click **Save**.
3. Restart the node manager on each managed server, then start each managed server.

7.4 Deploying the Oracle Role Manager Integration Library Application on WebLogic

To deploy the Integration Library application:

1. On the Oracle Identity Manager host, create the EAR file for the Integration Library application that contains JAR files from Oracle Identity Manager as follows:
 - a. In a command window, navigate to *ORMINT_HOME/bin*.
 - b. Run the following command:

For UNIX-based systems: `sh create_ear.sh OIM_HOME/xellerate`

For Windows systems: `create_ear.bat OIM_HOME/xellerate`

where *OIM_HOME* is the root installation directory for Oracle Identity Manager.
2. From the Oracle Identity Manager host, connect to the WebLogic Server Console in a Web browser. For example:


```
http://appserverhost:7001/console
```
3. Select **Deployments**.
4. Click **Install**.
5. Browse to navigate to the *ORMINT_HOME/lib* directory.
6. Choose **roleManagerIntegration_WebLogic10.3.ear**, then click **Next**.
7. Choose **Install this deployment as an application**, then click **Next**.
8. In the **Target** list, select the target server on which to deploy Oracle Role Manager, then click **Next**.

Note: If you are configuring a clustered environment, select the cluster for Oracle Role Manager from the **Target** list.

9. Accept the defaults on the next page, then click **Next**.
10. Click **Finish**.
11. Click **Deployments**.

You should see indication of successful deployment

- 12.** If you have a clustered server environment, restart the admin server and all managed servers.

Configuring IBM WebSphere

This chapter contains procedures for configuring the IBM WebSphere application servers for Oracle Identity Manager and Oracle Role Manager in preparation for deployment of the Oracle Role Manager Integration Library. The procedures in this chapter are expected to be performed in the sequence they are presented.

This chapter includes the following sections:

- [Before You Configure](#)
- [Configuring the Oracle Role Manager Server](#)
- [Configuring the Oracle Identity Manager Server](#)
- [Configuring Signer Certificates](#)
- [Deploying the Oracle Role Manager Integration Library Application on WebSphere](#)

8.1 Before You Configure

The Oracle Role Manager Integration Library is intended to be deployed on the application server on which Oracle Identity Manager is deployed. The procedures in this chapter assume the following:

- You have the access to the files installed in *ORMINT_HOME*.
- You know the administrator user name and password to access the Oracle Identity Manager Administrative and User Console and the Design Console.
- You know the WebSphere administrator user name and password to run wsadmin commands.
- You have the appropriate permission to add and modify files in the application servers where Oracle Identity Manager and Oracle Role Manager are deployed.
- You have the appropriate permission to stop and start the application servers where Oracle Identity Manager and Oracle Role Manager are deployed.
- For clustered environments, the database users and aliases for JMS engines have been created following the instructions in the *Oracle Role Manager Installation Guide*.

8.2 Configuring the Oracle Role Manager Server

This procedure assumes that a WebSphere application server has been created for Oracle Role Manager with a host alias set for port access to Oracle Role Manager.

Note: When configuring WebSphere, it is recommended that you save your settings after every task.

This section includes the following subsections:

- [Deploying the WebSphere Configuration](#)
- [Creating the Custom User for the Integration](#)
- [Creating the Alias for Custom User for the Integration](#)
- [\(Clustered Mode Only\) Creating the Database Users for the JMS Engines](#)
- [\(Clustered Mode Only\) Creating the Aliases for the JMS Engine Database Users](#)
- [Creating the JMS Messaging Buses](#)
- [Configuring the Oracle Role Manager Bus](#)
- [Configuring the Role Update Bus](#)
- [Configuring the JMS Queue Connection Factory](#)
- [Configuring JMS Queues](#)
- [Configuring Security Credentials on the Oracle Role Manager Bus](#)
- [Configuring Security Credentials on the Role Update Bus](#)
- [Granting Sender Roles to the System User](#)
- [Disabling Transaction Security](#)
- [Modifying the Oracle Role Manager Deployment Descriptor](#)

8.2.1 Deploying the WebSphere Configuration

The procedure in this section deploys the configuration needed to update the JNDI destinations of the Outgoing Event Manager in Oracle Role Manager, used for communication with Oracle Identity Manager.

To deploy the WebSphere configuration:

1. Stop the Oracle Role Manager application server if it is running.
2. On the Oracle Role Manager installation host, copy the `websphere_config.car` file from `ORM_HOME/Integration_Library/config` to `ORM_HOME/config`.
3. In a command window, navigate to `ORM_HOME/bin` on the Oracle Role Manager host.
4. Run the `deploy` command to load the WebSphere configuration to the Oracle Role Manager database.

```
deploy.bat "../config/websphere_config.car" orm-owner ormapp-user admin-user
```

In this command:

- `orm-owner` is the user name of the Oracle Role Manager database owner user/schema
- `ormapp-user` is the user name of the Oracle Role Manager application user/schema

- *admin-user* is the user name of the Oracle Role Manager system administrator
5. At the prompts, enter the passwords of the Oracle Role Manager database owner, Oracle Role Manager application user, and Oracle Role Manager administrator.
You should see the message "Deployment successfully completed" in the command window.

8.2.2 Creating the Custom User for the Integration

To create a custom user:

1. If not already on the WebSphere administrative console, in a Web browser, enter the URL. For example:

```
http://appserverhost:9060/ibm/console
```

2. Select **Users and Groups**, then select **Manage Users**.
3. Click **Create** and enter the following:

- a. In the **User ID** field, enter `ormSystem`.

Note: The user ID must be `ormSystem`.

- b. In the **First name** field, enter `ORM`.
- c. In the **Last name** field, enter `System`.
- d. In the **Password** field, enter a password for the user, for example, `ormSystem`.
- e. Click **Create** and then click **Close**.

8.2.3 Creating the Alias for Custom User for the Integration

To create alias for the custom user:

1. Click **Security**, then select **Secure administration, applications, and infrastructure**.
2. In the Authentication section, expand **Java Authentication and Authorization Service**, then click **J2C authentication data**.
3. Click **New** and enter the following:
 - a. In the **Alias** field, enter `OIMALIAS`.
 - b. In the **User** field, enter `ormSystem`.
 - c. In the **Password** field, enter the password set in step 3 of [Section 8.2.2](#)
 - d. Click **OK**, then save your changes.

8.2.4 (Clustered Mode Only) Creating the Database Users for the JMS Engines

For each planned server in the cluster, use this procedure to create a database user, such as `WSOIMMMsgEng1`, `WSOIMMMsgEng2`, and so forth.

To create the database users for the JMS engines:

1. On the Oracle Role Manager host, open a command window.

2. Using sqlplus or a similar utility, connect to the database instance into which the Oracle Role Manager schema is installed.
3. As the SYSTEM user, run the following commands:

```
create user WSOIMMsgEng1 identified by password default tablespace ORM_DATA
temporary tablespace ORM_TEMP;
grant connect to WSOIMMsgEng1;
grant create session to WSOIMMsgEng1;
grant resource to WSOIMMsgEng1;
commit;
```

where *WSOIMMsgEng1* is the name of the new user and *password* is the password for the new user.

4. Repeat these commands for additional users, as appropriate.

8.2.5 (Clustered Mode Only) Creating the Aliases for the JMS Engine Database Users

Follow this procedure to create an alias for each database user created in [Section 8.2.4](#).

To create alias for a custom database user:

1. Click **Security**, then select **Secure administration, applications, and infrastructure**.
2. In the Authentication section, expand **Java Authentication and Authorization Service**, then click **J2C authentication data**.
3. Click **New** and enter the following:
 - a. In the **Alias** field, enter a name, such as `WSOIMMsgEng1`.
 - b. In the **User** field, enter `WSOIMMsgEng1`.

Note: The user entered here must match the database user name set using the commands in [Section 8.2.4](#).

- c. In the **Password** field, enter the same password as the one set using the commands in [Section 8.2.4](#) for this user.
 - d. Click **OK**.
4. Repeat this procedure for additional database users created in [Section 8.2.4](#).

8.2.6 Creating the JMS Messaging Buses

To create the JMS messaging buses:

1. Select **Service integration**, then select **Buses**.
2. Click **New**.
3. In the **Name** field, enter `ORMRoleUpdateBus`.
4. Select **Bus security**, then click **Next**.
5. Click **Finish**.
6. For clustered server environments, add the cluster to the `ORMRoleUpdateBus` as follows:
 - a. Click `ORMRoleUpdateBus`, then click **Bus members**.

- b. Click **Add**.
 - c. Choose the **Cluster** option, select the cluster for Oracle Role Manager, then click **Next**.
 - d. In the **Select the type of message store** list, select **Data Store**, then click **Next**.
 - e. In the **Data source JNDI name** field, enter `orm/jdbc/WSMsgEngDS`.
 - f. In the **Schema name** field, enter `WSOIMMsgEng1`.
 - g. In the **Authentication alias** list, select **WSOIMMsgEng1**.
 - h. Ensure that **Create Tables** is selected.
 - i. Click **Next**.
7. For nonclustered environments, add the server to the `ORMRoleUpdateBus` as follows:
 - a. Click `ORMRoleUpdateBus`, then click **Bus members**.
 - b. Click **Add**.
 - c. Select the server used for Oracle Role Manager, then click **Next**.
 - d. In the **Select the type of message store** list, select **File Store**, then click **Next**, then click **Next** again.
 8. Click **Finish**, then save your changes.

8.2.7 Configuring the Oracle Role Manager Bus

To configure the Oracle Role Manager bus:

1. Select **Service integration**, then select **Buses**.
2. Select **ORM Bus**.
3. Create the foreign bus as follows:
 - a. Under **Topology**, click **Foreign buses**.
 - b. Click **New**.
 - c. In the **Name** field, enter `OIM ORM Bus`, then click **Next**.

Note: Take note of this bus name to use later when configuring buses on the Oracle Identity Manager application server.

 - d. Select **Direct, service Integration bus link** as the routing type, then click **Next**.
 - e. Click **Next** again.
 - f. Click **Finish**, then save your changes.
 - g. Click **ORM Bus** to return to that page.
4. Create the foreign bus link as follows:
 - a. Under **Topology**, click **Messaging engines**.
 - b. Select the messaging engine to which you want to add the service integration bus links.
 - c. Under **Additional properties**, click **Service integration bus links**.

- d. Click **New**.
- e. In the **Name** field, enter OIM ORM Link.
- f. In the **Foreign bus name** list, select **OIM ORM Bus**.

Note: Take note of this bus name to use later when configuring buses on the Oracle Identity Manager application server.

- g. In the **Remote messaging engine name** field, enter the messaging engine name of the OIM ORM Bus. For example:

oim_server_node.server_name-OIM ORM Bus.

Note: For nonclustered environments, the remote messaging engine name must be in the form *oim_server_node_name.oim_server_name* followed by a hyphen and the name of the foreign bus. For clustered environments, the name must be in the form *oim_cluster_name.index-OIM ORM Bus*, for example, *XL_JMS_CLUSTER.000-OIM ORM Bus*.

- h. Click **OK**, then save your changes.

8.2.8 Configuring the Role Update Bus

To configure the role update bus:

1. Click **Service integration**, then select **Buses**.
2. Click **ORMRoleUpdateBus**.
3. Create the foreign bus as follows:
 - a. Under Topology, click **Foreign buses**.
 - b. Click **New**.
 - c. In the **Name** field, enter `ORMRoleUpdateBus`, then click **Next**.

Note: Take note of this bus name to use later when configuring buses on the Oracle Identity Manager application server.

- d. Select **Direct, Service Integration bus link** as the routing type, then click **Next**.
- e. In the Outbound user ID field, enter `ormSystem`, then click **Next**.
- f. Click **Finish**, then save your changes.
- g. Click **ORMRoleUpdateBus** to return to that page.
4. Create the foreign bus link as follows:
 - a. Under Topology, click **Messaging engines**.
 - b. Select the messaging engine to which you want to add the service integration bus links. For example, *orm_server_node.orm_server-ORMRoleUpdateBus*.

- c. Under Additional properties, click **Service integration bus links**.
- d. Click **New**.
- e. In the **Name** field, enter RoleUpdateLink.
- f. In the **Foreign Bus Name** list, select **OIMRoleUpdateBus**.

Note: Take note of this bus name to use later when configuring buses on the Oracle Identity Manager application server.

- g. In the **Remote messaging engine name** field, enter the messaging engine name of the OIMRoleUpdateBus. For example:

```
oim_server_node.oim_server_name-OIMRoleUpdateBus.
```

Note: The remote message engine name must be in the form *oim_server_node_name.oim_server_name* followed by a hyphen and the name of the foreign bus. For clustered environments, the name must be in the form *oim_cluster_name.index-OIMRoleUpdateBus*, for example, *XL_JMS_CLUSTER.000-OIMRoleUpdateBus*.

- h. In the **Target inbound transport chain** field, enter InboundSecureMessaging.
- i. In the **Bootstrap endpoints** field, enter the Oracle Identity Manager server's host name followed by a colon (:), the SIB endpoint secure address followed by a colon (:), then BootstrapSecureMessaging. For example, *oim_host:secure_sib:BootstrapSecureMessaging*

Note: For clustered environments, endpoints should be in the form *oim_host:secure_sib:BootstrapSecureMessaging,oim_host:secure_sib:BootstrapSecureMessaging* where *oim_host* is the foreign server and *secure_sib* is the foreign server's SIB_ENDPOINT_SECURE_ADDRESS.

- j. In the **Authentication alias** list, select **OIMALIAS**.
 - k. Click **OK**, then save your changes.
 - l. Click **ORMRoleUpdateBus** to return to that page.
5. Create the foreign bus destination as follows:
- a. In the Destination resources area, click **Destinations**.
 - b. Click **New**.
 - c. Choose **Foreign** as the destination type, then click **Next**.
 - d. Enter RoleUpdateDest as the identifier.

Note: Take note of this destination name to use when configuring the OIM Role Update Bus on the Oracle Identity Manager application server.

- e. Select **OIMRoleUpdateBus** as the bus, then click **Next**.
- f. Click **Finish**, then save your changes.

8.2.9 Configuring the JMS Queue Connection Factory

To configure JMS queue connection factory for ORM Role Update:

1. From **Resources**, select **JMS**, then select **Queue connection factories**.
2. For clustered configuration, select the cluster scope used previously, then click **New**.
3. For nonclustered configuration, select the cell scope used previously, then click **New**.
4. Choose **Default messaging provider**, then click **OK**.
5. In the **Name** field, enter `RoleUpdateQCF`.
6. In the **JNDI name** field, enter `/oim/OIMserver/QueueConnectionFactory`.
7. In the **Bus name** list, select **ORMRoleUpdateBus**.
8. In the **Target inbound Transport chain** field, enter `InboundSecureMessaging`.
9. In the Advanced Administration area, in the Component-managed authentication alias list, select **OIMALIAS**.
10. Click **OK**, then save your changes.

8.2.10 Configuring JMS Queues

To configure the ORM Role Update queue:

1. From **Resources**, select **JMS**, then click **Queues**.
2. For clustered configuration, select the cluster scope used previously, then click **New**.
3. For nonclustered configuration, select the cell scope used previously, then click **New**.
4. Choose **Default messaging provider**, then click **OK**.
5. In the **Name** field, enter `RoleUpdateQueue`.
6. In the **JNDI name** field, enter `oim/OIMserver/RoleManagerQueue`.
7. In the **Bus name** list, select **OIMRoleUpdateBus**.
8. In the **Queue name** list, select **RoleUpdateDest**.
9. Click **OK**, then save your changes.

8.2.11 Configuring Security Credentials on the Oracle Role Manager Bus

To configure security credentials on the Oracle Role Manager bus:

1. Click **Service integration**, then select **Buses**.
2. Click **ORM Bus**.
3. In the Additional Properties section, click **Security**.
4. Select **Enable bus security** if it is not already selected.

5. In the **Inter-engine authentication alias** field, select **OIMALIAS**.
6. In the Permitted transports section, select **Restrict the use of defined transport channel chains to those protected by SSL**.
7. Click **OK**.
8. Click **ORM Bus** to return to that page.
9. Set the foreign bus link authentication alias as follows:
 - a. In the Topology section, click **Messaging engines**.
 - b. Select the messaging engine link to which you want to add the integration bus links.
 - c. In the Additional Properties section, click **Service integration bus links**.
 - d. Select **OIM ORM Link**.
 - e. In the **Authentication alias** field, select **OIMALIAS**.
 - f. Click **OK**.
 - g. Click **ORM Bus** to return to that page.
10. Configure users for the bus connector as follows:
 - a. In the Additional Properties area, click **Security**.
 - b. In the Additional Properties area, click **Users and groups in the bus connector role**.
 - c. Click **New**.
 - d. Select **User name** and enter `ormSystem`.
 - e. Click **OK**.
 - f. Click **ORM Bus** to return to that page.
11. Set the foreign bus link routing properties as follows:
 - a. In the Topology section, click **Foreign buses**.
 - b. Click **OIM ORM Bus**.
 - c. In the Additional Properties section, click **Service integration bus link routing properties**.
 - d. In the Inbound user ID field, enter `ormserver`.

Note: `ormserver` is the user ID of the custom user associated with the Oracle Role Manager server application. If you have associated a different user, you must specify that user ID instead.

- e. Click **OK**, then save your changes.

8.2.12 Configuring Security Credentials on the Role Update Bus

To configure security credentials on the role update bus:

1. Click **Service integration**, then select **Buses**.
2. Click **ORMRoleUpdateBus**.

3. In the Additional Properties area, click **Security**.
4. From the **Inter-engine authentication alias** list, select OIMALIAS.
5. In the Permitted transports section, select **Restrict the use of defined transport channel chains to those protected by SSL**.
6. Click **OK**, then save your changes.
7. Click **ORMRoleUpdateBus** to return to that page.
8. Set the users for the bus connector as follows:
 - a. In the Additional Properties area, click **Security**.
 - b. In the Additional Properties area, click **Users and groups in the bus connector role**.
 - c. Click **New**.
 - d. Select **User name**, then enter `ormSystem`.
 - e. Click **OK**, then save your changes.

8.2.13 Granting Sender Roles to the System User

This task must be performed using the `wsadmin` command-line tools provided by WebSphere. WebSphere must be running before performing this procedure.

Note: The commands in this procedure require the WebSphere Administrator user name and password. If you do not have those values, contact a WebSphere administrator.

Note: The user ID specified in the commands in the following procedure is `ormSystem`. If you have a different user associated with Oracle Role Manager or if you did not use the default bus names from this document, you must specify those values instead.

To grant the Sender roles:

1. On the host where Oracle Role Manager is deployed, run the following command:

```
DEPLOYMENT_MANAGER_HOME/bin/wsadmin.bat
```

Where `DEPLOYMENT_MANAGER_HOME` is the home directory of the deployment manager. For example,
`C:\IBM\WebSphere\AppServer\profiles\Dmgr02`

2. At the prompt, grant the Sender role for the Incoming Event Queue with the following command:

```
$AdminTask addUserToDestinationRole {-type Queue -bus "ORM Bus" -destination  
"Incoming Event Queue" -role Sender -user ormserver}  
$AdminConfig save
```

3. Grant the Sender role to foreign destinations with the following command:

```
$AdminTask addUserToDestinationRole {-type foreignDestination -bus  
"ORMRoleUpdateBus" -destination "RoleUpdateDest" -foreignBus "OIMRoleUpdateBus"  
-role Sender -user ormSystem}
```

```

$AdminTask addUserToForeignBusRole {-bus "ORMRoleUpdateBus" -foreignBus
"OIMRoleUpdateBus" -role Sender -user ormSystem}
$AdminConfig save
quit

```

8.2.14 Disabling Transaction Security

To disable transaction security:

1. Log in to the WebSphere Administrative Console for the server on which Oracle Role Manager is deployed.
2. Select **Servers**, then select **Application servers**.
3. Click the server name link corresponding to the server on which Oracle Role Manager is deployed.
4. In the Container Settings section, expand **Container Services**, then click **Transaction Service**.
5. In the Additional Properties section, click **Custom Properties**.
6. Click **New**.
7. In the **Name** field, enter `DISABLE_PROTOCOL_SECURITY`.
8. In the **Value** field, enter `true`.
9. In the **Description** field, enter `Disable transaction protocol security`.
10. Click **OK**, then save your changes.

8.2.15 Modifying the Oracle Role Manager Deployment Descriptor

Running the Oracle Role Manager Integration Library in a secured environment requires modifying the deployment descriptor for Oracle Role Manager on the application server host before deploying the Integration Library application.

Note: For clustered environments, perform this procedure on all managed servers.

To modify the deployment descriptor:

1. On the Oracle Role Manager host, copy the `server.ear` file from `ORM_HOME/lib` to a temporary location.
2. In the temporary location, using a utility such as WinZip or `jar`, extract the contents of the `server.ear` file.
You should see the `server.jar` file.
3. Copy and extract the contents of the `server.jar` file to a separate temporary location.
4. In the second temporary location, navigate to the `META-INF` directory
You should see the `ejb-jar.xml` file.
5. Open the `ejb-jar.xml` file with a text editor and edit it as follows:
 - a. Find the `session` element with the `ejb-name` element defined as `SingletonEJB`.

- b. Add a `resource-ref` element as the last `resource-ref` element in the `SingletonEJB` session element and define it as follows:

```
<resource-ref id="ResourceRef_117777777777">
  <res-ref-name>OIM/IntegrationConnectionFactory</res-ref-name>
  <res-type>javax.jms.QueueConnectionFactory</res-type>
  <res-auth>Container</res-auth>
  <res-sharing-scope>Shareable</res-sharing-scope>
</resource-ref>
```

Note: The new `resource-ref` element should be the last of its type and preceding the first `resource-env-ref` element.

6. Using a utility such as WinZip or jar, repackage the contents of `server.jar`, then copy `server.jar` to the first temporary location to overwrite the existing `server.jar` file.
7. In the first temporary location, repackage the contents of `server.ear`, then redeploy `server.ear` to the application server on which Oracle Role Manager is deployed.

For instructions on deploying the `server.ear` file, refer to the *Oracle Role Manager Installation Guide*.

Note: On redeployment of the `server.ear` file, in the Target Resource JNDI Name field for the `OIM/IntegrationConnectionFactory` resource reference, browse to select **RoleUpdateQCF**, then click **Apply**.

8. Start the application server on which Oracle Role Manager is deployed.
9. Ensure that deployment descriptor changes are present for the Oracle Role Manager server follows:
 - a. Log in to the WebSphere Administrative Console for the server on which Oracle Role Manager is deployed.
 - b. Select **Applications**, then click **Enterprise Applications**.
 - c. Click the name of the server for Oracle Role Manager, for example **ORM Server**.
 - d. In the References area, click **Resource references**.
 - e. Go to the table in the `javax.jms.QueueConnectionFactory` section.
 - f. For the resource reference named `OIM/IntegrationConnectionFactory`, look at the value in the Target Resource JNDI Name column.
It should be `/oim/OIMserver/QueueConnectionFactory`.
If it is not, click **Browse** to select `/oim/OIMserver/QueueConnectionFactory`. Then select **OIM/IntegrationConnectionFactory**, then click **Apply**.
 - g. For the resource reference named `OIM/IntegrationConnectionFactory`, look at the final cell in that row.

It should contain a value similar to:

```
Resource authorization:
Container Authentication method:
DefaultPrincipalMapping
staco18Node01/OIMALIAS
```

If it does not, select **Use default method** for authentication. Then from the **Authentication data entry** list, select **OIMALIAS**, then click **Apply**.

- h. If you have made any changes while verifying these settings, click **OK**, then save your changes.

8.3 Configuring the Oracle Identity Manager Server

This procedure assumes that a WebSphere application server has been created for Oracle Identity Manager with a host alias set for port access to Oracle Identity Manager.

Note: When configuring WebSphere, it is recommended that you save your settings after every task.

This section includes the following subsections:

- [\(Clustered Mode Only\) Creating the Oracle Identity Manager Database Users for the JMS Engines](#)
- [Creating the Authentication Alias for connections to Oracle Role Manager](#)
- [\(Clustered Mode Only\) Creating the Additional Authentication Aliases for the New Data Stores](#)
- [\(Clustered Mode Only\) Creating the JDBC Data Sources for the New Data Stores](#)
- [Creating the JMS Messaging Buses](#)
- [Configuring the OIM ORM Bus](#)
- [Configuring the Role Update Bus](#)
- [Configuring JMS Queue Connection Factories](#)
- [Creating the Oracle Role Manager JMS Queue](#)
- [Creating the OIM ORM JMS Queue](#)
- [Configuring JMS Activation Specifications](#)
- [Configuring Security Credentials on the Role Update Bus](#)
- [Configuring Security Credentials on the OIM ORM Bus](#)
- [Configuring Outbound Authentication](#)
- [Granting Sender Roles to the System User](#)
- [Creating the Shared Libraries](#)
- [Adding the Integration Library System Properties](#)

8.3.1 (Clustered Mode Only) Creating the Oracle Identity Manager Database Users for the JMS Engines

To create the database user and role for the JMS engines:

1. On the Oracle Identity Manager host, open a command window.
2. Using sqlplus or a similar utility, connect to the database instance into which the Oracle Identity Manager schema is installed.

3. As the SYSTEM user, run the following commands to create the IntegrationORM user, the IntegrationRole user and the IntegrationJMS role:

```
create user IntegrationORM identified by ormSystem default tablespace
OIM_TABLESPACE temporary tablespace OIM_TEMP_TABLESPACE;
create user IntegrationRole identified by ormSystem default tablespace
OIM_TABLESPACE temporary tablespace OIM_TEMP_TABLESPACE;
create role IntegrationJMS;
grant connect, create session, resource to IntegrationJMS;
grant create tablespace, drop any table to IntegrationJMS;
grant unlimited tablespace to IntegrationORM;
grant unlimited tablespace to IntegrationRole;
grant IntegrationJMS to IntegrationORM;
grant IntegrationJMS to IntegrationRole;
commit;
```

where *OIM_TABLESPACE* and *OIM_TEMP_TABLESPACE* are the appropriate tablespace names for the Oracle Identity Manager schema.

8.3.2 Creating the Authentication Alias for connections to Oracle Role Manager

Java 2 Connector authentication data entry settings are used for administrators to define authentication data, which includes user identities and passwords. Using aliases, these values can reference authentication data entries by resource adapters, data sources, and other configurations that require authentication.

To create the alias for connections to Oracle Role Manager:

1. If not already on the WebSphere administrative console, in a Web browser, enter the URL. For example:

```
http://appserverhost:9060/ibm/console
```

2. Select **Security**, then select Secure administration, applications, and infrastructure.
3. In the **Authentication** area, select **Java Authentication and Authorization Service**, then select J2C authentication data.
4. Click **New**.
5. In the **Alias** field, enter OIMALIAS.
6. In the **User ID** field, enter ormSystem.

Note: The user ID must be ormSystem.

7. In the **Password** field, enter ormSystem.
8. Click **OK**, then save your changes.
9. If you are configuring a nonclustered environment, skip to [Section 8.3.5](#).

8.3.3 (Clustered Mode Only) Creating the Additional Authentication Aliases for the New Data Stores

To create the alias for connections to Oracle Role Manager:

1. If not already on the WebSphere administrative console, in a Web browser, enter the URL. For example:

`http://appserverhost:9060/ibm/console`

2. Select **Security**, then select Secure administration, applications, and infrastructure.
3. In the **Authentication** area, select **Java Authentication and Authorization Service**, then select J2C authentication data.
4. Create the alias for the IntegrationORM user as follows:
 - a. Click **New**.
 - b. In the **Alias** field, enter `IntegrationORMBus`.
 - c. In the **User ID** field, enter `IntegrationORM`.
 - d. In the **Password** field, enter `ormSystem`.
 - e. Click **OK**, then save your changes.
5. Create the alias for the IntegrationRole user as follows:
 - a. Click **New**.
 - b. In the **Alias** field, enter `IntegrationRoleBus`.
 - c. In the **User ID** field, enter `IntegrationRole`.
 - d. In the **Password** field, enter `ormSystem`.
 - e. Click **OK**, then save your changes.

8.3.4 (Clustered Mode Only) Creating the JDBC Data Sources for the New Data Stores

To configure the data sources for the data stores:

1. In a Web browser, connect to the WebSphere administrative console.
2. Select **Resources**, then select **JDBC**.
3. Select **Data Sources**.
4. In the Scope list, select **Cell=XL_CELL**.
5. Create the data source for the IntegrationORM data store as follows:
 - a. Click **New**.
 - b. In the **Data source name** field, enter `Integration_ORM_DS`.
 - c. In the **JNDI name** field, enter `jdbc/Integration_ORM_DS`.
 - d. Click **Next**.
 - e. Choose the **Select an existing JDBC provider** option.
 - f. Select **XL XA Provider** from the list, then click **Next**.
 - g. In the **URL** field, enter the JDBC connection string for of the XL XA Provider. For example, `jdbc:oracle:thin:@ip_address:port:instance`.

Note: The URL entered here is the same as that entered for the XA data source for Oracle Identity Manager.

- h. In the **Data store helper class name** list, select either **Oracle10g data store helper** or **Oracle11g data store helper**, depending on your database.

- i. Select **Use this data source in container managed persistence (CMP)**, then click **Next**.
 - j. Click **Finish**.
 - k. Click **Integration_ORM_DS**.
 - l. In the Additional Properties section, click **Connection Pool Properties**.
 - m. In the **Maximum connections** field, enter 50.
 - n. In the **Minimum connections** field, enter 30.
 - o. In the **Aged Timeout** field, enter 10000.
 - p. Click **OK**.
6. Create the data source for the IntegrationRole data store as follows:
- a. Click **New**.
 - b. In the **Data source name** field, enter `Integration_Role_DS`.
 - c. In the **JNDI name** field, enter `jdbc/Integration_Role_DS`.
 - d. Click **Next**.
 - e. Choose the **Select an existing JDBC provider** option.
 - f. Select **XL XA Provider** from the list, then click **Next**.
 - g. In the **URL** field, enter the JDBC connection string for the data source. For example, `jdbc:oracle:thin:@ip_address:port:instance`.

Note: The URL entered here is the same as that entered for the XA data source for Oracle Identity Manager.

- h. In the **Data store helper class name** list, select either **Oracle10g data store helper** or **Oracle11g data store helper**, depending on your database.
- i. Select **Use this data source in container managed persistence (CMP)**, then click **Next**.
- j. Click **Finish**.
- k. Click **Integration_Role_DS**.
- l. In the Additional Properties section, click **Connection Pool Properties**.
- m. In the **Maximum connections** field, enter 50.
- n. In the **Minimum connections** field, enter 30.
- o. In the **Aged Timeout** field, enter 10000.
- p. Click **OK**.

8.3.5 Creating the JMS Messaging Buses

To create the JMS messaging buses:

1. Select **Service integration**, then select **Buses**.
2. Create the Role Update bus as follows:
 - a. Click **New**.

- b. Enter `OIMRoleUpdateBus` as the name for the Role Update bus.
 - c. Select **Bus security**, then click **Next**.
 - d. Click **Finish**, then save your changes.
3. Create the OIM ORM bus as follows:

This is the bus for sending messages from Oracle Identity Manager to Oracle Role Manager. For example, this bus is used for create user scenarios.

 - a. Click **New**.
 - b. Enter `OIM ORM Bus` as the name for the bus.

Note: Bus names used here on the Oracle Identity Manager server must not duplicate the nonforeign bus names used on the Oracle Role Manager server.

- c. Select **Bus security**, then click **Next**.
 - d. Click **Finish**, then save your changes.
4. If you are configuring a clustered server environment, add the cluster to each of the newly created buses as follows:
 - a. Click the bus link, then click **Bus members**.
 - b. Click **Add**.
 - c. Choose the **Cluster** option, the cluster to use from the list, for example `XL_JMS_CLUSTER`.
 - d. Click **Next**.
 - e. In the **Select the type of message store** list, select **Data Store**, then click **Next**.
 - f. In the **Data source JNDI name** field, enter either of following names, depending on which bus you are modifying.
 - For the OIM ORM Bus, enter `jdbc/Integration_ORM_DS`.
 - For the OIMRoleUpdateBus, enter `jdbc/Integration_Role_DS`.
 - g. In the **Schema Name** field, enter either of the following names, depending on which bus you are modifying:
 - For the OIM ORM Bus, enter `IntegrationORM`.
 - For the OIMRoleUpdateBus, enter `IntegrationRole`.
 - h. In the **Authentication alias** list, select either of following aliases, depending on which bus you are modifying:
 - For the OIM ORM Bus, select `XL_MANAGER_NODE/IntegrationORMBus`.
 - For the OIMRoleUpdateBus, select `XL_MANAGER_NODE/IntegrationRoleBus`.
 - i. Ensure that **Create Tables** is selected.
 - j. Click **Next**, click **Finish**, then save your changes.
 5. For nonclustered environments, add the server to each of the newly created buses as follows:
 - a. Click the bus link, then click **Bus members**.

- b. Select the server used for Oracle Identity Manager, then click **Next**.
- c. In the **Select the type of message store** list, select **File Store**, then click **Next**, then click **Next** again.
- d. Click **Finish**, then save your changes.

8.3.6 Configuring the OIM ORM Bus

To add the foreign bus to the OIM ORM Bus:

1. Click **Service integration**, then select Buses.
2. Select **OIM ORM Bus**.
3. Create the foreign bus as follows:
 - a. Under Topology, click **Foreign buses**.
 - b. Click **New**.
 - c. In the **Name** field, enter `ORM Bus`, then click **Next**.

Note: This foreign bus name must exactly match the bus name on the Oracle Role Manager server.

 - d. Select **Direct, service Integration bus link** as the routing type, then click **Next**.
 - e. Click **Next** again.
 - f. Click **Finish**, then save your changes.
4. Add the foreign bus link as follows:
 - a. Click **OIM ORM Bus**.
 - b. Under Topology, click **Messaging engines**.
 - c. Select the messaging engine to which you want to add the service integration bus links.
 - d. Under Additional properties, click **Service integration bus links**.
 - e. Click **New**.
 - f. In the **Name** field, enter `OIM ORM Link`.
 - g. In the **Foreign Bus Name** list, select **ORM Bus**.

Note: This foreign bus name must exactly match the bus name on the Oracle Role Manager server.

 - h. In the **Remote message engine name** field, enter the messaging engine name of the ORM Bus. For example, `orm_server_node.orm_server-ORM Bus`

Note: The remote message engine name must be in the form `orm_server_node_name.orm_server_name` followed by a hyphen and the name of the foreign bus. For clustered environments, the name must be in the form `orm_cluster_name.index-ORM Bus`, for example `ORM_CLUSTER.000-ORM Bus`.

- i. In the **Bootstrap endpoints** field, enter the Oracle Role Manager server's host name followed by a colon (:), the SIB endpoint secure address followed by a colon (:), then `BootstrapSecureMessaging`. For example, `orm_host:secure_sib:BootstrapSecureMessaging`.

Note: For clustered environments, endpoints should be in the form `orm_host:secure_sib:BootstrapSecureMessaging,orm_host:secure_sib:BootstrapSecureMessaging` where `orm_host` is the foreign server and `secure_sib` is the foreign server's `SIB_ENDPOINT_SECURE_ADDRESS`.

- j. In the **Target inbound transport chain** field, enter `InboundSecureMessaging`.
 - k. Click **OK**.
5. Configure foreign bus destinations as follows:
 - a. Click **OIM ORM Bus**, then click **Destinations**.
 - b. Click **New**.
 - c. Choose **Foreign** as the destination type, then click **Next**.
 - d. Enter `Incoming Event Queue` as the identifier.

Note: This name must exactly match the name of the incoming event queue destination on the Oracle Role Manager server.

- e. Specify **ORM Bus** as the bus member to own the queue, then click **Next**.
- f. Click **Finish**, then save your changes.

8.3.7 Configuring the Role Update Bus

To configure the role update bus:

1. Click **Service integration**, then select **Buses**.
2. Select **OIMRoleUpdateBus**.
3. Create the foreign bus as follows:
 - a. Under **Topology**, click **Foreign buses**.
 - b. Click **New**.
 - c. In the **Name** field, enter `ORMRoleUpdateBus`, then click **Next**.

Note: The foreign bus name must exactly match the bus name on the Oracle Role Manager server.

- d. Select **Direct, service Integration bus link** as the routing type, then click **Next**.
 - e. Click **Next**.
 - f. Click **Finish**, then save your changes.
4. Create the foreign bus link as follows:

- a. Click **OIMRoleUpdateBus**.
- b. Under Topology, click **Messaging engines**.
- c. Select the messaging engine to which you want to add the service integration bus links.
- d. Under Additional properties, click **Service integration bus links**.
- e. Click **New**.
- f. In the **Name** field, enter `RoleUpdateLink`.
- g. In the **Foreign Bus Name** list, select **ORMRoleUpdateBus**.

Note: This foreign bus name must exactly match the bus name on the Oracle Role Manager server.

- h. In the **Remote message engine name** field, enter the messaging engine name of **ORMRoleUpdateBus**. For example:
`orm_server_node.orm_server-ORMRoleUpdateBus`.

Note: The remote message engine name must be in the form `orm_server_node_name.orm_server_name` followed by a hyphen and the name of the foreign bus.

- i. Click **OK**.
5. Configure bus destinations as follows:
 - a. Click **OIMRoleUpdateBus** to return to that page.
 - b. Click **Destinations**.
 - c. Click **New**.
 - d. Choose **Queue** as the destination type, then click **Next**.
 - e. Enter `RoleUpdateDest` as the identifier, then click **Next**.
 - f. Specify the **bus member** to own the queue, then click **Next**.
 - g. Click **Finish**, then save your changes.

8.3.8 Configuring JMS Queue Connection Factories

To configure JMS queue connection factories:

1. From **Resources**, select **JMS**, then select **Queue connection factories**.
2. Select the cell scope used for Oracle Identity Manager, then click **New**.
3. Choose **Default messaging provider**, then click **OK**.
4. In the **Name** field, enter `ormJMSConnectionFactory`.
5. In the **JNDI name** field, enter `/oim/OIMserver/QueueConnectionFactory`.
6. In the **Bus name** list, select **OIMRoleUpdateBus**.
7. In the Advanced Administration area, in the **Component-managed authentication alias** list, select **OIMALIAS**.

8. Click **OK**, then save your changes.
9. Click **New**.
10. Choose **Default messaging provider**, then click **OK**.
11. In the **Name** field, enter `OIM ORM QCF`.
12. In the **JNDI name** field, enter `orm/jms/QueueConFac`.
13. In the **Bus name** list, select **OIM ORM Bus**.
14. In the **Advanced Administration** area, in the **Component-managed authentication alias** list, select **OIMALIAS**.
15. In the **Target inbound transport chain** field, enter `InboundSecureMessaging`.
16. Click **OK**, then save your changes.

8.3.9 Creating the Oracle Role Manager JMS Queue

To configure the Oracle Role Manager queue:

1. From **Resources**, select **JMS**, then select **Queues**.
2. Select the cell scope used previously, then click **New**.
3. Choose **Default messaging provider**, then click **OK**.
4. In the **Name** field, enter `ormJMSQueue`.
5. In the **JNDI name** field, enter `oim/OIMserver/RoleManagerQueue`.
6. In the **Bus name** list, select **OIMRoleUpdateBus**.
7. In the **Queue name** list, select **RoleUpdateDest**.
8. Click **OK**, then save your changes.

8.3.10 Creating the OIM ORM JMS Queue

To configure the OIM ORM queue:

1. From **Resources**, select **JMS**, then select **Queues**.
2. Select the cell scope used previously, then click **New**.
3. Choose **Default messaging provider**, then click **OK**.
4. In the **Name** field, enter `OIM ORM Queue`.
5. In the **JNDI name** field, enter `orm/jms/IncomingEventQueue`.
6. In the **Bus name** list, select **ORM Bus**.
7. In the **Queue name** list, select **Incoming Event Queue**.
8. Click **OK**, then save your changes.

8.3.11 Configuring JMS Activation Specifications

To configure the Oracle Role Manager JMS AS:

1. From **Resources**, select **JMS**, then select **Activation specifications**.
2. Select the same cell scope used previously, then click **New**

3. Choose **Default messaging provider**, then click **OK**.
4. In the **Name** field, enter `ormJMSActiveSpec`.
5. In the **JNDI name** field, enter `orm/jms/ormJMSActiveSpec`.
6. In the **Destination type** list, select **Queue**.
7. In the **Destination JNDI name** field, enter `oim/OIMserver/RoleManagerQueue`.
8. In the **Bus name** list, select **OIMRoleUpdateBus**.
9. In the **Authentication Alias** list, select **OIMALIAS**.
10. Click **OK**, then save your changes.

8.3.12 Configuring Security Credentials on the Role Update Bus

To configure security credentials for the Role Update Bus:

1. Configure users and authentication for the bus as follows:
 - a. From **Security**, select **Bus security**.
 - b. Click **OIMRoleUpdateBus**.
 - c. In the Additional Properties area, click **Security**.
 - d. In the Additional Properties area, select **Users and groups in the bus connector role**, then click **New**.
 - e. Select **User name**, then enter `ormSystem`.
 - f. Click **OK**, then save your changes.
2. Set the foreign bus link authentication alias as follows:
 - a. Click **OIMRoleUpdateBus** to return to that page.
 - b. In the Topology section, click **Messaging engines**.
 - c. Select the messaging engine link to which you want to add the service integration bus links.
 - d. In the Additional Properties section, click **Service integration bus links**.
 - e. Click **RoleUpdateLink**.
 - f. In the **Authentication alias** field, select **OIMALIAS**.
 - g. Click **OK**.
3. Save your changes.

8.3.13 Configuring Security Credentials on the OIM ORM Bus

To configure users for the OIM ORM Bus:

1. Click **Service integration**, then select **Buses**.
2. Click **OIM ORM Bus**.
3. Configure users and authentication for the bus as follows:
 - a. In the Additional Properties area, click **Security**.

- b. In the **Inter-engine authentication alias** field, select **OIMALIAS**, then click **Apply**.
 - c. Click **OK**, then save your changes.
 - d. Click **OIM ORM Bus**.
 - e. In the Additional Properties area, select **Security**.
 - f. In the Additional Properties area, select **Users and groups in the bus connector role**, then click **New**.
 - g. Select **User name**, then enter `ormSystem`.
 - h. Click **OK**, then save your changes.
4. Set the foreign bus link authentication alias as follows:
 - a. Click **OIM ORM Bus** to return to that page.
 - b. In the Topology section, click **Messaging engines**.
 - c. Select the messaging engine link to which you want to add the service integration bus links.
 - d. In the Additional Properties section, click **Service integration bus links**.
 - e. Click **OIM ORM Link**.
 - f. In the **Authentication alias** field, select **OIMALIAS**.
 - g. Click **OK**, then save your changes.

8.3.14 Configuring Outbound Authentication

Configuring outbound authentication prevents the Oracle Identity Manager server from sending confidential credentials to the Oracle Role Manager server.

To configure outbound authentication:

1. From **Security**, select **Secure administration, applications, and infrastructure**.
2. Expand **RMI/IIOP security**, then click **CSIV2 outbound authentication**.
3. In the Basic authentication section, select **Never**.
4. Click **OK**, then save your changes.

8.3.15 Granting Sender Roles to the System User

This task must be performed using the `wsadmin` command-line tools provided by WebSphere. WebSphere must be running before performing this procedure.

Note: The commands in this procedure require the WebSphere Administrator user name and password. If you do not have those values, contact a WebSphere administrator.

Note: The user ID specified in the commands in the following procedure is `ormSystem`. If you have a different user associated with Oracle Role Manager or if you did not use the default bus names from this document, you must specify those values instead.

To grant the Sender roles:

1. On the host where Oracle Identity Manager is deployed, run the following command:

```
DEPLOYMENT_MANAGER_HOME/bin/wsadmin.bat
```

Where DEPLOYMENT_MANAGER_HOME is the home directory of the deployment manager. For example,
C:\IBM\WebSphere\AppServer\profiles\XL_MANAGER_PROFILE.

2. At the prompt, grant the Sender role for foreign destinations with the following command:

```
$AdminTask addUserToDestinationRole {-type foreignDestination -bus "OIM ORM Bus" -destination "Incoming Event Queue" -foreignBus "ORM Bus" -role Sender -user ormSystem}
$AdminTask addUserToForeignBusRole {-bus "OIM ORM Bus" -foreignBus "ORM Bus" -role Sender -user ormSystem}
$AdminConfig save
quit
```

8.3.16 Creating the Shared Libraries

To configure the shared libraries:

1. Create the IntegrationJars shared library as follows:
 - a. From **Environment**, select **Shared Libraries**, then select the same cell scope used for Oracle Identity Manager.
 - b. Click **New**.
 - c. In the **Name** field, enter `IntegrationJars`.
 - d. In the **Classpath** field, enter the full path to the following JAR files:


```
ORMINT_HOME/lib/orm_encryption.jar
ORMINT_HOME/lib/server_api_14.jar
ORMINT_HOME/lib/websphere_stubs.jar
OIM_HOME/lib/xlAPI.jar
```

Press Enter after each path to specify the class path for the next JAR file.
 - e. Click **OK**, then save your changes.
2. Create the IntegrationSecurity shared library as follows:
 - a. From **Environment**, select **Shared Libraries**, then select the same cell scope used for Oracle Identity Manager.
 - b. Click **New**.
 - c. In the **Name** field, enter `IntegrationSecurity`.
 - d. In the **Classpath** field, enter the full path to the following JAR files, press Enter.


```
ORMINT_HOME/lib/orm_encryption.jar
```
 - e. Click **OK**, then save your changes.
3. If you are configuring a clustered server environment, copy the libraries as follows on each managed node:

- a. In the file system where Oracle Identity Manager is deployed, create the following directory if it does not exist:

```
OIM_appserver/java/jre/lib/endorsed
```

where *OIM_appserver/java* is the JDK directory for WebSphere. For example, *C:\IBM\WebSphere\AppServer\java*.

- b. Copy the following libraries into the endorsed directory:

```
ORMINT_HOME/lib/xercesImpl.jar
```

```
ORMINT_HOME/lib/xml-apis.jar
```

8.3.17 Adding the Integration Library System Properties

To add the Integration Library JVM system properties:

1. From **Servers**, select **Application Servers**, then select the server on which Oracle Identity Manager is deployed.
2. Under Server Infrastructure, expand **Java and Process Management**, then click **Process Definition**.
3. Under Additional Properties, click **Java Virtual Machine**.
4. Under Additional Properties, click **Custom Properties**.
5. Click **New**.
6. In the **Name** field, enter *ORMINT_ROOT_DIR*.
7. In the **Value** field, enter the full path to the Oracle Role Manager Integration Library home directory, for example *C:/ORMINT_HOME*.
8. In the **Description** field, enter *Location of the Oracle Role Manager Integration Library home directory*.
9. Click **Apply**, then save your changes.
10. For these changes to go into effect, restart the Oracle Identity Manager server.
11. For clustered server environments, repeat these steps for each Oracle Role Manager server in the *XL_CLUSTER* cluster.

8.4 Configuring Signer Certificates

Configuring signer certificates for clustered and nonclustered server environments involves exporting and importing certificates from both the target and source systems as described in this section.

In this section:

- [Exporting the Oracle Role Manager Certificates](#)
- [Importing and Exporting Certificates on Oracle Identity Manager](#)
- [Importing the Oracle Identity Manager Certificates](#)

8.4.1 Exporting the Oracle Role Manager Certificates

To export the certificates from Oracle Role Manager:

1. On the application server host for the Oracle Role Manager, connect to the WebSphere administrative console.

Note: For clustered environments, connect to the WebSphere administrative console on the host server that is the primary node for the Oracle Role Manager cluster.

2. From **Security**, select **SSL certificate and key management**.
3. In the Related Items section, click **Key stores and certificates**.
4. For clustered environments, click **CellDefaultTrustStore**.
5. For nonclustered environments, click **NodeDefaultTrustStore**.
6. In the Additional Properties section, click **Signer certificates**.
7. Perform the following steps for each certificate named default or defaultx (where x is a number):
 - a. Select the certificate.
 - b. Click **Extract**.
 - c. In the **File name** field, enter a name for the certificate file. For example, `orm_signer.cer` or `orm_signer_x.cer`.
 - d. Click **OK**.
8. On the file system, navigate to `WAS_HOME/AppServer/profiles/server/etc`.
9. Copy the exported certificate to the equivalent directory on the Oracle Identity Manager host, for example, `C:\IBM\WebSphere\AppServer\profiles\WL_MANAGER_PROFILE\etc`.

These certificates must be imported into the Oracle Identity Manager cluster's primary node following the steps in [Section 8.4.2](#).

8.4.2 Importing and Exporting Certificates on Oracle Identity Manager

To import and export certificates on Oracle Identity Manager:

1. On the application server host for the Oracle Identity Manager, connect to the WebSphere administrative console.

Note: For clustered environments, connect to the WebSphere administrative console on the host server that is the primary node for the Oracle Identity Manager cluster.

2. From **Security**, select **SSL certificate and key management**.
3. In the Related Items section, click **Key stores and certificates**.
4. For clustered environments, click **CellDefaultTrustStore**.
5. For nonclustered environments, click **NodeDefaultTrustStore**.
6. In the Additional Properties section, click **Signer certificates**.
7. Import each of the certificates exported from Oracle Role Manager as follows:
 - a. Click **Add**.
 - b. In the **Alias** field, enter a unique alias for the certificate, for example, `ormcert1`.

- c. In the **File name** field, enter the file name, for example `orm_signer.cer`.
 - d. Click **OK**.
8. Export each certificate named default or defaultx (where x is a number) as follows:
 - a. Select the certificate.
 - b. Click **Extract**.
 - c. In the **Name** field, a file name. For example, `oim_signer.cer` or `oim_signer_x.cer`.
 - d. Click **OK**.
 9. On the file system, navigate to `WAS_HOME/AppServer/profiles/server/etc`.
 10. Copy the exported certificate to the equivalent directory on the Oracle Role Manager host.

These certificates must be imported into the Oracle Role Manager cluster's primary node following the steps in [Section 8.4.3](#).

8.4.3 Importing the Oracle Identity Manager Certificates

To import certificates on Oracle Role Manager:

1. On the application server host for the Oracle Role Manager, connect to the WebSphere administrative console.

Note: For clustered environments, connect to the WebSphere administrative console on the host server that is the primary node for the Oracle Role Manager cluster.

2. From **Security**, select **SSL certificate and key management**.
3. In the Related Items section, click **Key stores and certificates**.
4. For clustered environments, click **CellDefaultTrustStore**.
5. For nonclustered environments, click **NodeDefaultTrustStore**.
6. In the Additional Properties section, click **Signer certificates**.
7. For each of the certificates exported from Oracle Identity Manager, do the following:
 - a. Click **Add**.
 - b. In the **Alias** field, enter a unique alias for the certificate, for example, `oimcert1`.
 - c. In the **File name** field, enter the file name, for example `oim_signer.cer`.
 - d. Click **OK**.

8.5 Deploying the Oracle Role Manager Integration Library Application on WebSphere

Note: For clustered environments, perform this procedure on each server node, for example, `XL_SERVER1_ON_NODE1`, `XL_SERVER2_ON_NODE2`, and so forth.

Note: For clustered environments, this procedure assumes the following:

- `ORMINT_HOME` exists in an identical directory on each server host.
 - Each server host has the identical modified `IMConfig.xml` file in `OIMINT_HOME/config`.
-
-

To deploy the Integration Library application:

1. On the Oracle Identity Manager host, create the EAR file for the Integration Library application that contains JAR files from Oracle Identity Manager as follows:
 - a. In a command window, navigate to `ORMINT_HOME/bin`.
 - b. Run the following command:
For UNIX-based systems: `sh create_ear.sh OIM_HOME/xellerate`
For Windows systems: `create_ear.bat OIM_HOME/xellerate`
where `OIM_HOME` is the root installation directory for Oracle Identity Manager.
2. Connect to the WebSphere administrative console for the Oracle Identity Manager application server. For example:
`http://appserverhost:9060/ibm/console`
3. Select **Applications**, then select **Install New Application**.
4. Choose **Remote file system**, then click **Browse** to navigate to the `ORMINT_HOME/lib` directory.
5. Select **roleManagerIntegration_WebSphere6.1.ear**, then click **Next**.
6. On the Select installation options page, accept the defaults and click **Next**.
7. On the Map modules to servers page, select **roleManagerIntegration_WebSphere6.1.ear**, select the cluster or server on which to deploy the Integration Library, then click **Apply**.
8. Click **Next**.
9. Click **Finish**, then save your changes.
10. Add the IntegrationJars shared library (created in [Section 8.3.16](#)) to the Integration Library application as follows:
 - a. Select **Applications**, then select **Enterprise Applications**.
 - b. Click **RoleManagerIntegration**.

- c. Under references, click **shared library references**.
 - d. Select **RoleManagerIntegration** and then click **Reference shared libraries**.
 - e. Select **IntegrationJars** and click the right arrow button to move it from the **Available** list to the **Selected** list, then click **OK**.
11. Add the IntegrationSecurity shared library (created in [Section 8.3.16](#)) to the Oracle Identity Manager application as follows:
 - a. Select **Applications**, then select **Enterprise Applications**.
 - b. Click **Xellerate**.
 - c. Under references, click **shared library references**.
 - d. Select **Xellerate** and then click **Reference shared libraries**.
 - e. Select **IntegrationSecurity** and click the right arrow button to move it from the **Available** list to the **Selected** list, then click **OK**.
12. Click **OK**, then save your changes.
13. Copy the Oracle Identity Manager xlDataObjectBeans.jar file as follows:

Note: This step is necessary each time the Integration Library application is deployed. For clustered server environments, this step must be executed on each server node that is part of XL_CLUSTER.

- a. Select **Applications**, then select **Enterprise Applications**.
 - b. Select **RoleManagerIntegration**, then click **Start**.

You should see a message indicating that the application has started successfully.
 - c. On the WebSphere node where Oracle Identity Manager resides, find the extracted files from the Oracle Identity Manager EAR file. For example, *AppServer1\profiles\AppServer01\installedApps\localCell\Xellerate.ear*.
 - d. In the top level, find the library file named xlDataObjectBeans.jar.
 - e. Copy the xlDataObjectBeans.jar file into the lib folder of the extracted RoleManagerIntegration.ear file. For example, *AppServer1\profiles\AppServer01\installedApps\localCell\RoleManagerIntegration.ear\lib*.

Copying the JAR file to this directory overwrites the existing file of the same name with an installation-specific JAR file for Oracle Identity Manager.
14. Restart the application server.

Configuring JBoss

This chapter contains procedures for configuring the JBoss application servers for Oracle Identity Manager and Oracle Role Manager in preparation for deployment of the Oracle Role Manager Integration Library (Integration Library). The procedures in this chapter are expected to be performed in the sequence they are presented.

This chapter includes the following sections:

- [Before You Configure](#)
- [Configuring the Oracle Role Manager Server](#)
- [Configuring the Oracle Identity Manager Server](#)
- [Deploying the Oracle Role Manager Integration Library Application on JBoss](#)

9.1 Before You Configure

The Oracle Role Manager Integration Library is intended to be deployed on the application server on which Oracle Identity Manager is deployed. The procedures in this chapter assume the following:

- You have the access to the files installed in *ORMINT_HOME*.
- You have the appropriate permission to add and modify files in the application server where Oracle Identity Manager is deployed.
- You have the appropriate permission to stop and start the application server where Oracle Identity Manager is deployed.
- For clustered environments, Oracle Role Manager and Oracle Identity Manager have been installed and configured for on the server cluster and application server nodes as described in the *Oracle Role Manager Installation Guide* and *Oracle Identity Manager Installation Guide*.

Note: For clustered environments, use the *JBOSS_HOME/server/all* directory instead of the *JBOSS_HOME/server/default* directory when following the instructions in this chapter.

9.2 Configuring the Oracle Role Manager Server

Note: If you are configuring Oracle Role Manager Integration Library in a clustered environment, perform the first step in this procedure on the master node and all secondary nodes.

To configure the Oracle Role Manager server:

1. On the Oracle Role Manager application server host, copy the following file into the deploy directory of the application server for Oracle Role Manager (for example, C:\jboss-4.2.3\server\default\deploy for a nonclustered environment or C:\jboss-4.2.3\server\all\deploy-hasingleton\jms for a clustered environment):

```
ORM_HOME/Integration_Library/samples/jboss/ormoim-service.xml
```

2. Navigate to the `ORM_HOME/Integration_Library/config` directory.
3. Using a utility like WinZip or jar, extract the entire contents of `jboss_config.car` into a temporary location, such as `ORM_HOME/Integration_Library/config_temp/jboss_config`.
4. From the temporary location where `jboss_config.car` was extracted, navigate to `jboss_config/config/oracle.iam.rm.event.outgoing`.
5. Open the `oim_integration.xml` file with a text editor and modify the JNDI URL as appropriate.

This file contains configuration for the outgoing events required to support the Integration Library.

The settings in this file may have to be modified to reflect your deployment environment, including the JNDI location of Oracle Identity Manager.

- a. For each of the five events, modify the value of the `jndi-url` element to match your environment.

For clustered environments, the value must be in the form `jnp://oim_host1_ip_address:jndi_port1,oim_host2_ip_address:jndi_port2`.

For example, if the Oracle Identity Manager application servers are run on hosts named `Server_OIM_1` and `Server_OIM_2`, and the `ha-jndi jnp` bind address is 1100 as specified in the `deploy/jms/hajndi-jms-ds.xml` file, then the value for the `jndi-url` should be:

```
jnp://Server_OIM_1:1099,Server_OIM_2:1100
```

For nonclustered environments, the value must be in the form `jnp://oim_host_ip_address:jndi_port`.

For example, if the Oracle Identity Manager application server is run on a host named `Server_OIM`, and the `jnp` bind address is 1099 as specified in the `jboss-service.xml` file where it is deployed, then the value for the `jndi-url` should be:

```
jnp://Server_OIM:1099
```

- b. Save and close the `oim_integration.xml` file.
6. Using a utility like WinZip or jar, repackage everything in the `jboss_config` directory and create a file appended with the `.car` extension, for example, `jboss_custom.car`.

Ensure that the CAR file directory layout is as follows:

```
config/
oracle.iam.rm.event.outgoing
oim_integration.xml
```

If it does not match this layout, fix the layout, then repackage the CAR file.

7. Deploy the configuration changes to the Oracle Role Manager database as follows:

- a. Copy the new `jboss_custom.car` file from the temporary location to `ORM_HOME/config`.
- b. Ensure that the `db.properties` file in `ORM_HOME/config` contains the correct information. If it does not, modify it so it contains the following two lines:

```
db.driverClass=oracle.jdbc.driver.OracleDriver
db.connection_string=jdbc:oracle:thin:@$HOST$: $PORT$: $SERVICE$
```

where `$HOST$` is the database host name, `$PORT$` is the database listener port, and `$SERVICE$` is the database instance on which the Oracle Role Manager users were created.

- c. Stop the Oracle Role Manager application server if it is running.

Note: If you have a clustered environment, shut down all nodes on the Oracle Role Manager cluster.

- d. In a command window, navigate to `ORM_HOME/bin`.
- e. Run the deploy command as follows:

For UNIX-based systems:

```
sh deploy.sh "../config/jboss_custom.car" orm-owner ormapp-user admin-user
```

For Windows systems:

```
deploy.bat "../config/jboss_custom.car" orm-owner ormapp-user admin-user
```

In this command:

`orm-owner` is the user name of the Oracle Role Manager database owner user/schema

`ormapp-user` is the user name of the Oracle Role Manager application user/schema

`admin-user` is the user name of the Oracle Role Manager system administrator

- f. At the prompts, enter the passwords of the Oracle Role Manager database owner, Oracle Role Manager application user, and Oracle Role Manager administrator.

You should see the message "Deployment successfully completed" in the command window.

9.3 Configuring the Oracle Identity Manager Server

Note: If you are configuring Oracle Role Manager Integration Library in a clustered environment, perform this procedure on the master node and all secondary nodes.

To configure the Oracle Identity Manager server:

1. On the Oracle Identity Manager application server host, copy the following files into the deploy directory of the application server for Oracle Identity Manager (for example, `C:\jboss4.2.3\server\default\deploy` for a single installation or `C:\jboss4.2.3\server\all\deploy` for a clustered installation):

```
ORMINT_HOME/samples/jboss/oimorm-service.xml
ORMINT_HOME/lib/server_api_14.jar
```

2. Copy the following two files into the lib directory of the application server for Oracle Identity Manager. For example, C:\jboss4.2.3\server\default\lib.

```
ORMINT_HOME/lib/orm_encryption.jar  
ORMINT_HOME/oimlib/OIM-IntegrationTransport.jar
```

9.3.1 Modifying the Oracle Identity Manager Startup Command

Before you can start using the Oracle Role Manager Integration library, the Oracle Identity Manager startup command must include the path to the Integration Library software. Making this change before the Integration Library software is deployed does not affect the operation of Oracle Identity Manager until it is restarted.

Note: This step must be performed on the master node and all secondary nodes.

To modify how Oracle Identity Manager is invoked for the Integration Library:

1. Open the following file for editing:

For UNIX-based systems:

```
ORM_HOME/xellerate/bin/xlStartServer.sh
```

For Windows systems:

```
ORM_HOME\xellerate\bin\xlStartServer.bat
```

2. Add the following argument to the Oracle Identity Manager startup command:

```
-DORMINT_ROOT_DIR=ORMINT_HOME
```

where *ORMINT_HOME* is the full path to the home directory of the Oracle Role Manager Integration Library.

For example, on Windows, it might be similar to:

```
C:\jboss4.2.3\bin\run.bat -DXL.HomeDir=C:\OIM\xellerate  
-Djava.awt.headless=true -DORMINT_ROOT_DIR=C:\ORMINT_HOME
```

3. Optionally, to enable logging for the Integration Library, add the following argument:

```
-Djava.util.logging.config.file=ORMINT_HOME/config/logging.properties
```

where *ORMINT_HOME* is the full path to the home directory of the Oracle Role Manager Integration Library.

4. Save and close the start script.
5. For these changes to go into effect immediately, restart the Oracle Identity Manager server. Alternatively, you can restart the server after deploying the Oracle Role Manager Integration Library application as described in the next section.

9.4 Deploying the Oracle Role Manager Integration Library Application on JBoss

Note: If you are deploying the Oracle Role Manager Integration Library application in a clustered environment, perform this procedure on all nodes in the environment.

To deploy the Integration Library application:

1. On the Oracle Identity Manager application server host, create the EAR file for the Integration Library application that contains JAR files from Oracle Identity Manager as follows:
 - a. In a command window, navigate to *ORMINT_HOME*/bin.
 - b. Run the following command:
For UNIX-based systems: `sh create_ear.sh OIM_HOME/xellerate`
For Windows systems: `create_ear.bat OIM_HOME/xellerate`
where *OIM_HOME* is the root installation directory for Oracle Identity Manager.
2. Copy the following file into the deploy directory of the application server for Oracle Identity Manager (for example, `C:\jboss-4.2.3\server\default\deploy`):
`ORMINT_HOME/lib/roleManagerIntegration_JBoss4.2.3.ear`

Note: For clustered environments, use the *JBOSS_HOME*/server/all/farm directory. For example, `C:\jboss-4.2.3\server\all\farm`.

3. Restart the Oracle Role Manager application server.

Testing the Oracle Role Manager Integration Library Installation

After you deploy and configure the Oracle Role Manager Integration Library, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to testing the Integration Library:

- [Testing User Reconciliation](#)
- [Testing Entitlement Reconciliation](#)
- [Testing Role and Role Membership Reconciliation](#)
- [Testing One-Time Import of User Groups](#)
- [Testing One-Time Import of Access Policies](#)
- [Testing Approver Role Resolution](#)
- [Testing Role Grant Approver Workflow](#)

It is recommended to test your installation following the steps in the order they are presented in this chapter.

Note: Some of the tests in this chapter use the sample data provided with Oracle Role Manager. If you did not load the sample data, you can still use these tests but you must create objects in Oracle Role Manager similar to those described in each test.

10.1 Testing User Reconciliation

When changes to user data are made in Oracle Identity Manager, messages are sent to Oracle Role Manager so that data is synchronized in real time.

Because there may be situations when the Oracle Role Manager system is unavailable, such as for scheduled maintenance down time, the default configuration provides predefined tasks to be scheduled for user reconciliation to ensure that any user data updates, when connectivity to Oracle Role Manager is not available, are later propagated to Oracle Role Manager.

There are two scheduled tasks for user reconciliation provided as part of the Integration Library configuration imported into Oracle Identity Manager: User Reconciliation and Full User Reconciliation. The difference between these reconciliation tasks is that full reconciliation also inspects users in Oracle Role Manager (who are also Oracle Identity Manager users) to check if any users were either removed or made inactive in Oracle Identity Manager, and properly reflect their status in Oracle Role Manager.

You might want to use reserve Full User Reconciliation for less frequent schedules or at times when there is less activity for performance reasons.

10.1.1 Real-Time User Synchronization

The test in this section verifies that the event handlers are functioning and messages are sent and received by creating a user in Oracle Identity Manager who appears in Oracle Role Manager.

To test user reconciliation:

1. If not currently running, start Oracle Identity Manager and then Oracle Role Manager.
2. Using the Oracle Identity Manager Administrative and User Console, create at least one user.

For purposes of performing other tests later in this section, create at least one user whose first name begins with the letter C.

3. Find the new user or users in Oracle Role Manager as follows:
 - a. Select **Organizations & People**, then select **People**.
 - b. In the tree view, select **Unassigned**, then click **Filter** to display results.

The new user from Oracle Identity Manager should display in the search results.

10.1.2 Scheduled Tasks for User Reconciliation

The test in this section verifies that messages from the scheduled tasks are able to communicate effectively between the two systems by testing that a user modification made in Oracle Identity Manager while Oracle Role Manager was inaccessible is synchronized after connectivity is restored when a scheduled task for user reconciliation is run.

To test the scheduled task for user reconciliation:

1. Shut down the Oracle Role Manager application server.
2. Using the Oracle Identity Manager Administrative and User Console, edit the name of a user you just created.
3. Start Oracle Role Manager and log in to the application.
4. Find the user in Oracle Role Manager.

Note that the name change from Oracle Identity Manager has not been updated.
5. Enable the user reconciliation task as follows:
 - a. In the Oracle Identity Manager Design Console (Oracle Identity Manager client), expand **Administration**, then double-click **Task Scheduler**.
 - b. Click the Lookup button, and then the Go to End button to go to the last defined task.
 - c. Click the left arrow button until you see the RoleManagerUserReconciliation_Full task.
 - d. Clear the **Disabled** box then click the Save button on the tool bar.
 - e. In the **Status** field, change the status to **ACTIVE**.

- f. In the **Start Time** field, enter the timestamp of the current date and time plus one minute.
 - g. Click the **Save** button on the tool bar.
6. After a minute, in Oracle Role Manager, click **Search** again to refresh the search results.

Note that Oracle Role Manager now shows the name change that was done in Oracle Identity Manager while the Oracle Role Manager server was unavailable.

10.2 Testing Entitlement Reconciliation

Scheduled tasks ensure that entitlement data in both systems is synchronized. This consists of sending all entitlement records from Oracle Identity Manager to Oracle Role Manager, where entitlements are updated or created to match what is sent from Oracle Identity Manager. Any changes to mapping of entitlements in Oracle Identity Manager will also be made in Oracle Role Manager as part of entitlement reconciliation.

There are two scheduled tasks for entitlement reconciliation: *quick* entitlement reconciliation and *full* entitlement reconciliation. Quick entitlement reconciliation can be run at periodic intervals to send to Oracle Role Manager all entitlement data that has been created, updated or deleted since the last time the task was run or since a specified base time. Full entitlement reconciliation additionally checks for entitlements that have been deleted in Oracle Identity Manager, and deletes the corresponding entitlements in Oracle Role Manager.

To test scheduled entitlement reconciliation:

1. Enable the full entitlement reconciliation task as follows:
 - a. In the Oracle Identity Manager Design Console (Oracle Identity Manager client), expand **Administration**, then double-click **Task Scheduler**.
 - b. Click the Lookup button, and then the Go to End button to go to the last defined task.
 - c. Click the left arrow button until you see the RoleManagerEntitlementReconciliation_Full task.
 - d. Clear the **Disabled** box then click the Save button.
 - e. In the **Status** field, change the status to **ACTIVE**.
 - f. In the **Start Time** field, enter the timestamp of the current date and time plus one minute.
 - g. Click the Save icon on the tool bar.
2. Wait at least one minute for all entitlements to be reconciled.
3. Find the new entitlement in Oracle Role Manager as follows:
 - a. Connect to the Oracle Role Manager Web application as a user who has permission to view entitlements in the system.
 - b. Select **Roles**, then select **Entitlements**.
 - c. In the left pane, right-click **Entitlements**, then select **Search**.
 - d. Click **Search**.

Note that the search results now contain the entitlements from Oracle Identity Manager.

10.3 Testing Role and Role Membership Reconciliation

Updates to user groups in Oracle Identity Manager occur when the role membership update timers trigger Oracle Role Manager to send synchronization messages. Along with membership changes, new roles created in Oracle Role Manager are also received in Oracle Identity Manager as part of batch role resolution and the three role membership update timer processes.

The three role membership update timer processes are ApproverRolePublishing, businessRolePublishing, and itRolePublishing. For more information about these timers, see [Section 5.6.3, "Modifying the Role Membership Update Timers."](#) There is no real-time role or role membership resolution.

To ensure that there are no invalid user groups or memberships as a result of roles having been deleted in Oracle Role Manager, there is a scheduled task to use to correct user groups and memberships in Oracle Identity Manager. This task can be enabled and configured in the same way as the user reconciliation tasks described in [Section 10.1](#).

Note: The names of user groups in Oracle Identity Manager that correspond with roles in Oracle Role Manager by default begins with `ORM_AR_` for Approver Roles and `ORM_BR_` for Business Roles. The default prefix for the naming of access policies that correspond with IT roles is `ORM_IR_`. This naming helps administrators identify the user groups that are modified only in the Oracle Role Manager system. Any changes made to these user groups or access policies in Oracle Identity Manager could cause synchronization between the system to fail.

Note: Because the name attribute for user groups in Oracle Identity Manager is limited to 30 characters and is required to be unique, the names of roles reconciled from Oracle Role Manager may be truncated, thus potentially causing uniqueness constraint violations. You may want to check the Oracle Identity Manager console after running role reconciliation processes.

10.3.1 User Provisioning through Role/User Group Membership

The test in this section verifies that a user added as a member of a role in Oracle Role Manager is provisioned for the corresponding user group in Oracle Identity Manager. It also verifies that if a Business Role is mapped to an IT role in Oracle Role Manager, then the corresponding user group (created as a result of Business Role Publishing) is mapped to the access policy that corresponds with the mapped IT role (created as a result of IT role publishing).

To test role membership reconciliation:

1. If not currently running, start Oracle Identity Manager and then Oracle Role Manager.
2. View the Compliance Officer user group in Oracle Identity Manager to see its memberships as follows:
 - a. Connect to the Oracle Identity Manager Administrative and User Console.
 - b. Select **User Groups**, then select **Manage**.

- c. Search for and select **ORM_BR_Compliance Officer**.
 - d. Select **Member and Sub-Groups** from the list.
Note that no membership exist for this user group.
3. View the **ORM_IR_Telecom_Provisioner** access policy as follows:
 - a. Select **Access Policies**, then select **Manage**.
 - b. Search for and select **ORM_IR_Telecom Provisioner**.
On the Access Policy details screen, note that there are no groups for this access policy.
4. Grant the Compliance Officer role to a person who exists in Oracle Identity Manager as follows:
 - a. Connect to the Oracle Role Manager Web application as a user who has permission to grant roles in the system.
 - b. Select **Organization & People**, then select **People**.
 - c. Click the Details icon in the Actions column.
 - d. On the Business Roles tab, click **Grant Role**.
 - e. Search for and select the **Compliance Officer** role, then click **Finish**.
 - f. Click **Submit**.
5. Map the Compliance Officer Business Role in to Telecom Provisioner IT role in Oracle Role Manager as follows:
 - a. Select **Roles**, then select **Business Roles**.
 - b. In the left pane, right-click **Business Roles**, then select **Search**.
 - c. Search for and select **Compliance Officer**.
 - d. On the Mappings tab, click **Map IT Role**.
 - e. Search for and select **Telecom_Provisioner**.
 - f. Click **Finish**, then click **Submit**.
6. Depending on the role membership update timer configuration for Business Roles in Oracle Role Manager, wait that amount of time until the role membership update job for Business Roles has completed.
For more information about timer configuration repeat interval and cron job configuration, see *Oracle Role Manager Administrator's Guide*.
7. After the Oracle Role Manager role membership update job has run, view the **ORM_BR_Compliance Officer** user group in Oracle Identity Manager as follows:
 - a. Connect to the Oracle Identity Manager Administrative and User Console.
 - b. Select **User Groups**, then select **Manage**.
 - c. Search for and select **ORM_BR_Compliance Officer**.
 - d. Select **Member and Sub-Groups** from the list.
Note that the new membership displays.
8. View the **ORM_IR_Telecom_Provisioner** access policy in Oracle Identity Manager to see the mapping to a user group from Oracle Role Manager as follows:
 - a. Connect to the Oracle Identity Manager Administrative and User Console.

- b. Select **Access Policies**, then select **Manage**.
- c. Search for and select **ORM_IR_Telecom_Provisioner**.

On the Access Policies details screen, note that Compliance Officer user group is in the list.

10.3.2 User De-provisioning by Deleted Roles

The test in this section verifies that an IT role deleted in Oracle Role Manager unmaps the user groups and entitlements for the corresponding access policy in Oracle Identity Manager. It also verifies that a business role deleted in Oracle Role Manager deletes the corresponding user group in Oracle Identity Manager.

To test role deletion and de-provisioning:

1. If not currently running, start Oracle Identity Manager and then Oracle Role Manager.
2. Delete the Telecom Provisioner IT role in Oracle Role Manager as follows:
 - a. Connect to the Oracle Role Manager Web application as a user who has permission to manage IT roles in the system.
 - b. Select **Roles**, then select **IT Roles**.
 - c. In the left pane, right-click **IT Roles**, then select **Search**.
 - d. Search for and select **Telecom Provisioner**.
 - e. Click the Delete icon in the Actions column.
 - f. Click **OK** to confirm the deletion.
3. Search for the ORM_IR_Telecom_Provisioner access policy in Oracle Identity Manager as follows:
 - a. Connect to the Oracle Identity Manager Administrative and User Console.
 - b. Select **Access Policies**, then select **Manage**.
 - c. Search for and select **ORM_IR_Telecom_Provisioner**.

On the Access Policies details screen, note that the ORM_BR_Compliance Officer user group is no longer mapped.
4. Delete the Mail Sorter Business Role in Oracle Role Manager as follows:
 - a. Connect to the Oracle Identity Manager Administrative and User Console.
 - b. Select **Roles**, then select **Business Roles**.
 - c. In the left pane, right-click **Business Roles**, then select **Search**.
 - d. Search for and select **Mail Sorter**.
 - e. Click the Delete icon in the Actions column.
 - f. Click **OK** to confirm the deletion.
5. Search for the Mail Sorter user group in Oracle Identity Manager as follows:
 - a. Connect to the Oracle Identity Manager Administrative and User Console.
 - b. Select **User Groups**, then select **Manage**.
 - c. Search for and select **ORM_BR_Mail Sorter**.

Note that no user group exists by this name.

10.4 Testing One-Time Import of User Groups

User groups from Oracle Identity Manager are represented in Oracle Role Manager as Business Roles. This scheduled task imports all user group data, user memberships, and mappings between user groups and access policies. It is recommended that the full entitlement reconciliation scheduled task be run before running this task.

To test one-time import of user groups:

1. Create a user group in Oracle Identity Manager as follows:
 - a. Connect to the Oracle Identity Manager Administration and User Console.
 - b. Select **User Groups**, then select **Create**.
 - c. In the **Group Name** field, enter `TestOIMUserGroup`.
 - d. Click **Create**.
2. Enable the user group reconciliation task as follows:
 - a. In the Oracle Identity Manager Design Console (Oracle Identity Manager client), expand **Administration**, then double-click **Task Scheduler**.
 - b. Click the Lookup button, and then the Go to End button to go to the last defined task.
 - c. Click the left arrow button until you see the `RoleManagerUserGroupsReconciliation_Full` task.
 - d. Clear the **Disabled** box then click the Save button.
 - e. In the **Status** field, change the status to **ACTIVE**.
 - f. In the **Start Time** field, enter the timestamp of the current date and time plus one minute.
 - g. Click the Save icon on the tool bar.
3. Wait at least one minute for all user groups to be reconciled.
4. Find the new user group in Oracle Role Manager as follows:
 - a. Connect to the Oracle Role Manager Web application.
 - b. Select **Roles**, then select **Business Roles**.

Note that the search results now contain the role named `TestOIMUserGroup`.

10.5 Testing One-Time Import of Access Policies

Access policies from Oracle Identity Manager are represented in Oracle Role Manager as IT roles. This scheduled task imports all access policy data and mappings between those access policies and entitlements. It is recommended that the full entitlement reconciliation scheduled task be run before running this task.

Note: Only access policies that contain entitlement information alone will be reconciled by the Oracle Role Manager Integration Library. If any access policies exist in Oracle Identity Manager that have extra information attached to them (such as complex rules or accounts), the extra information will not be retained when imported into Oracle Role Manager. Similarly, any access policies that do not contain entitlement information will not be imported into Oracle Role Manager.

It is recommended that an Oracle Identity Manager administrator break up any access policies with extra information into separate access policies for management purposes.

To test one-time import of access policies:

1. Create an access policy in Oracle Identity Manager as follows:
 - a. Connect to the Oracle Identity Manager Administration and User Console.
 - b. Select **Access Policies**, then select **Create**.
 - c. In the **Access Policy Name** field, enter `TestOIMAccessPolicy`.
 - d. In the **Access Policy Description** field, enter `Testing one-time import of access policies`.
 - e. Click **Next**.
 - f. Select the resource you want to provision in the **Available** list and move it to the **Selected** list.
 - g. Click **Continue**.
 - h. Click **Create Access Policy**.
2. Enable the access policy reconciliation task as follows:
 - a. In the Oracle Identity Manager Design Console (Oracle Identity Manager client), expand **Administration**, then double-click **Task Scheduler**.
 - b. Click the **Lookup** button, and then the **Go to End** button to go to the last defined task.
 - c. Click the left arrow button until you see the `RoleManagerAccessPoliciesReconciliation_Full` task.
 - d. Clear the **Disabled** box then click the **Save** button.
 - e. In the **Status** field, change the status to **ACTIVE**.
 - f. In the **Start Time** field, enter the timestamp of the current date and time plus one minute.
 - g. Click the **Save** icon on the tool bar.
3. Wait at least one minute for all access policies to be reconciled.
4. Find the new IT role that represents the new access policy in Oracle Role Manager as follows:
 - a. Connect to the Oracle Role Manager Web application.
 - b. Select **Roles**, then select **IT Roles**.

Note that the search results now contain the role named `TestOIMAccessPolicy`.

10.6 Testing Approver Role Resolution

Testing the way Approver Roles in Oracle Role Manager are used with processes in Oracle Identity Manager involves several preparatory steps as described in the following sections.

For information about creating and editing roles in Oracle Role Manager, see *Oracle Role Manager User's Guide*.

10.6.1 Oracle Role Manager Setup

The steps in this section are necessary to prepare Oracle Role Manager with the Approver Role whose grant policy defines the possible people qualified to act as approvers.

Note: It is recommended that any Approver Roles in Oracle Role Manager that are referenced by processes in Oracle Identity Manager should have narrowly defined grant policies to reduce the number of returned records. Oracle Identity Manager supports only a single record to be considered as the approver, so the first member that meets the grant policy (determined by object key in ascending order) is sent through the Integration Library.

To set up the Approver Role in Oracle Role Manager:

1. Select **Roles**, then select Approver Roles.
2. In the tree view, right-click **Office of the CEO**, then select **New Approver Role** from the context menu.
3. In the **Display Name** field, enter OIM Approver.
4. On the Grant Policy tab, copy and paste the following rule example that determines which users are qualified to be approvers as members of this Approver Role.

This rule finds all users in Oracle Role Manager who are also users in Oracle Identity Manager and whose name begins with the letter C.

Note: Although the second condition in this example is provided only to narrow the results of this grant policy, the policy must include a condition using the attribute `oimID`. If Oracle Role Manager returns an approver who does not have an OIM ID, the approval process will fail.

```
<?xml version="1.0" encoding="UTF-8"?>
<predicate xmlns="http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0"
input-type="person">
<and-expression>
  <expressions>
    <attribute-expression>
      <attribute attribute-id="oimId" />
      <greater-than>
        <integer-constant>0</integer-constant>
      </greater-than>
    </attribute-expression>
    <attribute-expression>
```

```

    <attribute attribute-id="displayName"/>
      <starts-with>
        <string-constant>C</string-constant>
      </starts-with>
    </attribute-expression>
  </expressions>
</and-expression>
</predicate>

```

For details about how to define membership rules and grant policies, see *Oracle Role Manager User's Guide*.

5. On the Members tab, click **Recalculate**.
You should see the user created in [Section 10.1.1](#) whose name begins with C in the search results.
6. Click **Submit**.
7. Depending on how frequently the approval publishing timer is set to run on Oracle Role Manager, either wait that amount of time or reset the timer to another time. For information about resetting the timer, see [Section 5.6.3, "Modifying the Role Membership Update Timers."](#)

10.6.2 Oracle Identity Manager Setup

The steps in this section set up the sample resources and approval process that was imported into Oracle Identity Manager so that the display values match those referenced in [Section 10.6.3](#) that are more suitable for demonstration purposes.

To create an approval process:

1. Check for the OIM Approver in Oracle Identity Manager as follows:
 - a. Connect to the Oracle Identity Manager Administrative and User Console.
 - b. Select **User Groups**, then select **Manage**.
 - c. Select Group Name from the list, enter ORM_AR* in the field, then click **Search**.
You should see the user group ORM_AR_OIM Approver in the list. If you do not, make sure that the approval publishing job in Oracle Role Manager has completed.
2. Rename the sample resource as follows:
 - a. In the Oracle Identity Manager Design Console (Oracle Identity Manager client), expand **Resource Management**.
 - b. Double-click **Resource Objects**.
 - c. Click the Lookup button, and then the Go to End button to go to the last defined task.
You should see the ORM Samples task.
 - d. In the Name field, change ORM Samples to Oracle Financials.
 - e. Click the Save icon.
3. Map the sample form to the renamed resource as follows:
 - a. Expand **Development Tools**, then double-click **Form Designer**.
 - b. Click the Lookup button, and then the Go to End button to go to the last defined form.

You should see the form for the UD_ORAFIN table. If you do not, click the right arrow button until you see it display.

- c. Double-click in the Object Name field.
- d. Select **Oracle Financials** in the Lookup window, then click **OK**.
- e. Click the Save icon.
4. Go back to the Oracle Financials resource object you created previously, then double-click the Table Name field to add UD_ORAFIN.
5. Click the Save icon.
6. Rename the sample provisioning process as follows:

- a. Expand **Process Management**, then double-click **Process Definition**.
- b. Click the Lookup button, and then the Go to End button to go to the last defined process.

You should see the process ORM Samples Provisioning. If you do not, click the left arrow button until you see it display.

- c. In the Name field, rename ORM Samples Provisioning to Oracle Financials Provisioning.
- d. Click the Save icon.
7. Rename the sample approval process as follows:
 - a. Click the left arrow until the ORM Sample Approval displays.
 - b. In the Name field, rename it to Oracle Financials Approval.
 - c. Click the Save icon.
8. Add the group ORM_AR_OIM Approver to the task as follows:
 - a. Expand **Process Management**, then double-click **Process Definition**.
 - b. Click the Lookup icon, then click the Go to End icon to go to the last defined process.

You should see the process Oracle Financials Approval. If you do not, click the left arrow button until you see it display.

 - c. Double-click **Get Manager Approval Task**.
 - d. On the Assignments tab, double-click the field in the Target Type column, then enter `Group`.
 - e. Double-click the field in the Group column.
 - f. In the Lookup window, select **ORM_AR_OIM_Approver**, then click **OK**.
 - g. Ensure that the Adapter column is empty.
9. Click the save icon.

10.6.3 Performing the test

The test in this section verifies that the approval process in Oracle Identity Manager uses the Approver Role from Oracle Role Manager to get an appropriate approver based on the role's grant policy.

To run the approver test:

1. Using the Oracle Identity Manager Administrative and User Console, assign the Oracle Financials resource to the user created in [Section 10.1.1](#) as follows:
 - a. Select **Requests**, then select **Resources**.
 - b. Choose **Grant Resource**, then click **Continue**.
 - c. Choose **Users**, then click **Continue**.
 - d. Select the user created in [Section 10.1.1](#) and optionally any other users that you know also exist in the Oracle Role Manager system (non administrative or system users)
 - e. Click **Add** to move them to Selected box, then click **Continue**.
 - f. Select **Oracle Financials**.
 - g. Click **Add** to move it to the Selected box, then click **Continue**.

You should see the users and resource displayed.

2. Click **Submit Now**.
3. Click the link of the Request ID.
4. Select **Approval Details** from the list.
5. Select the box in the Action column, then click **Approve**.
6. Click **Confirm**.

The page should refresh with the status of the approval process.

7. Note the group assigned to the Get Role Manager Approval Task to use in the next steps.

This is the group that is automatically resolved as the resource approver after referencing the OIM Approver role in Oracle Role Manager.

8. Log out of the Administrative and User Console and log back in as any user who is a member of the group identified in the previous step.
9. Select **To-Do List**, then select **Pending Approvals**.

You should see the request listed as pending, available to be approved.

10.7 Testing Role Grant Approver Workflow

When role grants in Oracle Role Manager require approval, event messages are sent to Oracle Identity Manager where the configured approver or sequence of approvers can either approve or deny the role grant request.

To test role grant approver workflow:

1. Create a static business role in Oracle Role Manager as follows:
 - a. Connect to the Oracle Role Manager Web application as a user who has permission to manage roles.
 - b. Click **Roles**, then click **Business Roles**.
 - c. On the left pane, click the organization where you want to create the test role, then click **New Business Role**.
 - d. In the **Business Role Type** box, select **Static**, then click **Submit**.

- e. In the **Display Name** field, enter `TestRoleForWorkflow`.
 - f. In the **Approvers** field, select **Role Owner**.
 - g. In the **Owner** field, click **Edit**.
 - h. Specify the search criterion for people who are eligible to be role owners of this role.
 - i. Select the person to set as the role owner, then click **OK**.
Make a note of this person since it will be this user who can approve or deny the role grant request.
 - j. Click **Submit**.
2. Grant the role to a user in Oracle Role Manager as follows:
 - a. Select **Organizations & People**, then click **People**.
 - b. Right-click **People**, then click **Search**.
 - c. Specify the search criterion for people to display.
 - d. In the row for the person you want to grant the role, click the View/Edit icon.
Make a note of the person who has been granted the role and whose role grant is pending approval.
 - e. Click **Business Roles**, then click **Grant Role**.
 - f. Search for and select the new **TestRoleForWorkflow** role.
 - g. Click **Next**, then click **Submit**.
 - h. In the left pane, click **Outbox**.
You should see the submission of the role grant request transaction.
3. Approve the role grant request as follows:
 - a. Connect to the Oracle Identity Manager Administrative and User console as the user who is the role owner of the `TestRoleForWorkflow` role (set in Step 1).
 - b. Approve the role grant request.
 - c. If there are other approvers for the role grant request, log in as those users to approve the request.
4. Verify that the user now has the role grant:
 - a. Select **Organizations & People**, then click **People**.
 - b. Right-click **People**, then click **Search**.
 - c. Search for the person who was granted the role (set in Step 2).
 - d. In the row for that person, click the View/Edit icon.
 - e. Click **Memberships**.
You should see the `TestRoleForWorkflow` role in the list.

This chapter provides information about the log files where the Oracle Role Manager Integration Library writes messages along with some error conditions and solutions.

This chapter contains the following topics:

- [Log Files](#)
- [Oracle Role Manager Application Server Console Errors](#)
- [Oracle Identity Manager Application Server Console Errors](#)

11.1 Log Files

The Integration Library messages are written to the `server.log.*` files in both the Oracle Role Manager application server and the Oracle Identity Manager application server.

Depending on the application server that you use, log information is written to the following files:

- For JBoss:

`JBOSS_HOME/server/default/log/server.log`

- For IBM WebSphere:

`WEBSPPHERE_HOME/AppServer/profiles/profile_name/logs/server_name/SystemOut.log`

- For WebLogic Server:

`WEBLOGIC_HOME/user_projects/domains/domain_name/servers/server_name/server_name.log`

11.2 Oracle Role Manager Application Server Console Errors

The following table describes error conditions that may appear in the application server console for Oracle Role Manager.

| Problem Description | Solution |
|---|---|
| <p>Returned Warning Message:</p> <p>WARN [OutgoingEventManagerImpl] Explicitly committed to a non-XA queue from within a transaction. Please check the configuration for the /oim/OIMserver/QueueConnectionFactory connection factory.</p> | <p>This can be ignored.</p> <p>This occurs when the application server on which Oracle Identity Manager is deployed is non-transactional, where Oracle Role Manager explicitly commits a transaction on initialization of the Oracle Role Manager connection factory to ensure messages are sent from Oracle Role Manager to Oracle Identity Manager.</p> |

11.3 Oracle Identity Manager Application Server Console Errors

The following table describes error conditions that may appear in the application server console for Oracle Identity Manager.

| Problem Description | Solution |
|--|--|
| <p>Returned Warning Message:</p> <p>WARN [IntegrationContext] General error utilizing plugin class</p> | <p>This can be ignored. It is caused by an intermittent race condition and causes no harm or loss of functionality.</p> |
| <p>Returned Error Message:</p> <p>WARN [IntegrationContext] Truncating the ORM Role Name when creating a shadowing OIM Group was <i>xxxx</i>. Truncated to <i>yyyy</i>.</p> | <p>This occurs when the integration detects that the Oracle Role Manager role name (including role prefix ORM_) would attempt to create a group whose name length was greater than thirty characters. In this case, the integration truncates the name to the Oracle Identity Manager user group name limit of thirty characters.</p> |
| <p>Returned Error Message:</p> <p>javax.naming.NameNotFoundException: While trying to lookup 'connection factory'.</p> | <p>This occurs when the JNDI names for the JMS connection factory and the local and remote foreign JNDI providers are different. Check your WebLogic configuration to ensure that the values for all three are identical.</p> |
| <p>Returned Error Message:</p> <p>SECJ0055E: Authentication failed for <null>. The user id or password may have been entered incorrectly or misspelled. The user id may not exist, the account could have expired or disabled. The password may have expired.</p> | <p>This can occur for a variety of reasons. Common occurrences related to the Integration Library are as follows:</p> <ul style="list-style-type: none"> ■ For WebSphere deployments, bus security is mismatched. For example, the role update bus on the Oracle Role Manager server has security disabled but the foreign role update bus on the Oracle Identity Manager server has security enabled. ■ For WebSphere deployments, the steps regarding the xlDataObjectBeans.jar file during deployment of the Integration Library application were not correctly followed. (For instructions, refer to Section 8.5, "Deploying the Oracle Role Manager Integration Library Application on WebSphere.") |

Cron Expressions

Cron expressions are used to configure instances of `CronTrigger`, a subclass of `org.quartz.Trigger`. A cron expression is a string consisting of six or seven subexpressions (fields) that describe individual details of the schedule.

These fields, separated by white space, can contain any of the allowed values with various combinations of the allowed characters for that field. [Table A-1](#) shows the fields in the expected order.

Table A-1 Cron Expressions Allowed Fields and Values

| Name | Required | Allowed Values | Allowed Special Characters |
|--------------|----------|--------------------|----------------------------|
| Seconds | Y | 0-59 | , - * / |
| Minutes | Y | 0-59 | , - * / |
| Hours | Y | 0-23 | , - * / |
| Day of month | Y | 1-31 | , - * ? / L W C |
| Month | Y | 0-11 or JAN-DEC | , - * / |
| Day of week | Y | 1-7 or SUN-SAT | , - * ? / L C # |
| Year | N | empty or 1970-2099 | , - * / |

Example A-1 Cron Expressions

Cron expressions can be as simple as `* * * * ? *` or as complex as `0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010`.

Here are some more examples:

| Expression | Means |
|---------------------------------|---|
| <code>0 0 12 * * ?</code> | Fire at 12:00 PM (noon) every day |
| <code>0 15 10 ? * *</code> | Fire at 10:15 AM every day |
| <code>0 15 10 * * ?</code> | Fire at 10:15 AM every day |
| <code>0 15 10 * * ? *</code> | Fire at 10:15 AM every day |
| <code>0 15 10 * * ? 2005</code> | Fire at 10:15 AM every day during the year 2005 |
| <code>0 * 14 * * ?</code> | Fire every minute starting at 2:00 PM and ending at 2:59 PM, every day |
| <code>0 0/5 14 * * ?</code> | Fire every 5 minutes starting at 2:00 PM and ending at 2:55 PM, every day |

| Expression | Means |
|--------------------------|---|
| 0 0/5 14,18 * * ? | Fire every 5 minutes starting at 2:00 PM and ending at 2:55 PM, AND fire every 5 minutes starting at 6:00 PM and ending at 6:55 PM, every day |
| 0 0-5 14 * * ? | Fire every minute starting at 2:00 PM and ending at 2:05 PM, every day |
| 0 10,44 14 ? 3 WED | Fire at 2:10 PM and at 2:44 PM every Wednesday in the month of March |
| 0 15 10 ? * MON-FRI | Fire at 10:15 AM every Monday, Tuesday, Wednesday, Thursday and Friday |
| 0 15 10 15 * ? | Fire at 10:15 AM on the 15th day of every month |
| 0 15 10 L * ? | Fire at 10:15 AM on the last day of every month |
| 0 15 10 ? * 6L | Fire at 10:15 AM on the last Friday of every month |
| 0 15 10 ? * 6L | Fire at 10:15 AM on the last Friday of every month |
| 0 15 10 ? * 6L 2002-2005 | Fire at 10:15 AM on every last Friday of every month during the years 2002, 2003, 2004, and 2005 |
| 0 15 10 ? * 6#3 | Fire at 10:15 AM on the third Friday of every month |
| 0 0 12 1/5 * ? | Fire at 12 PM (noon) every 5 days every month, starting on the first day of the month |
| 0 11 11 11 11 ? | Fire every November 11 at 11:11 AM |

Index

A

accessibility, 0-xiii
activation specifications
 configuring Oracle Role Manager AS, 8-21
activation specifications (AS), configuring in
 WebSphere, 8-21
adding attributes to incoming event business
 logic, 5-17
administrator for Oracle Identity Manager, 6-5
application servers, supported platforms, 2-1
approval processes
 importing configuration for sample, 6-7
 sample configuration for, 2-8
Approver Roles
 creating, 10-9
 grant policies for, 10-9
authentication
 digital signatures for, 5-5
 disabling encryption, 5-8

B

Batch Resolution Timer
 configuration, 5-10
bundling configurations for deployment, 5-10, 5-19
Business Logic configuration, 5-17

C

CAR files (configuration archive files), 5-2
character limit for user group name, 10-4
class files
 for handling approval role resolution between
 systems, 2-6
 for scheduled reconciliation, 2-7
 for the underlying integration framework, 2-7
class loading order, configuring in WebSphere, 8-29
colons, as delimiters in CAR collections, 5-2
commons-logging.jar file
 about, 2-6
 adding to WebLogic class path, 7-5
configuration files, location for Oracle Role Manager
 Integration Library, 5-9
configuration settings
 deployment of, 5-1

 modifying, 5-9
configurations.car file, extracting files from, 5-10
connection errors, 11-1
connectivity, reconciliation after connection is
 restored, 10-2
create_ear script, about, 2-4
create_key_pair script, about, 2-5
create_keystore script, about, 2-4
credentials, setting in WebLogic, 7-10
cron job configuration, 5-10

D

data file archives (DAR), 5-4
data model, manual deployment of, 5-1
database alias, creating in WebSphere, 8-14, 8-15
database properties file, for manual deployment and
 other commands, 5-2, 9-3
db.properties file, modifying for the deploy tool, 5-2,
 9-3
default configuration values, 5-9
deleted users, reconciling, 10-1
deleting users during user reconciliation, 5-15
delimiters in CAR collections, 5-2
deployment of configuration, 5-1
digital signatures for authentication, 5-5

E

empty values in XML elements, 5-15
encryption
 configuring, 5-5
 disabling, 5-8
errors, connection, 11-1
event.event_1_0.xsd file, 2-9

F

Finisher Queue bus destination (WebSphere), 8-7
foreign JMS queue connection factories, configuring
 in WebLogic, 7-9

G

grant policies for Approver Roles, 10-9

I

IMConfig.xml file
 about, 2-5
 oimRootDir policy, 6-2
 ormEncrypt policy, 5-8
 XML schema definition for, 2-9
imframework.imconfig_1_0.xsd file, 2-9
imframework.pluginconfig_1_0.xsd file, 2-9
import_certificate script, about, 2-5
importing configuration into Oracle Identity Manager, 2-5
inactivated users, reconciling, 10-1
Incoming Event Manager, configuration, 5-14
Incoming Event Queue
 configuring for WebSphere, 8-8
 configuring in WebSphere, 8-19, 8-21
incoming messages, configuration for, 2-5
Internal system user in Oracle Identity Manager (WebLogic), 6-2
IT resource
 configuring system property for, 6-9
 defining parameters for, 6-5
IT Roles
 character limit for creating in Oracle Identity Manager, 10-4

J

JBoss
 configuration, 9-1
 Oracle Identity Manager JMS queue configuration, 2-9
 Oracle Role Manager JMS queue configuration, 2-9
 supported versions, 2-1
JDK, supported versions, 2-1
JMS activation specifications (WebSphere), 8-21
JMS listener queue, default value of (JBoss), 6-6
JMS messaging buses
 adding servers to (WebSphere), 8-5, 8-17
 configuring destinations (WebSphere), 8-7, 8-20
 for finalization (WebSphere), 8-17
 for Oracle Role Manager (WebSphere), 8-17
JMS queue configuration
 on the Oracle Identity Manager application server (JBoss), 2-9
 on the Oracle Role Manager application server, 2-9
JMS queue connection factories
 configuring in WebLogic, 7-6, 7-7
 configuring in WebSphere (OIM ORM QCF), 8-20
 configuring in WebSphere (RoleUpdateQueue), 8-8
JMS queues
 configuring in WebSphere, 8-21
 configuring Incoming Event Queue (WebSphere), 8-8, 8-21
JNDI location of Oracle Role Manager, 2-9
JNDI names
 configuring queue connection factory in

 WebLogic, 7-7, 7-8
 for Incoming Event Queue (WebSphere), 8-8, 8-21
 for Loader AS, 8-21
 for Oracle Role Manager Finalization queue connection factory (WebSphere), 8-21
 for Oracle Role Manager queue connection factory (WebSphere), 8-8, 8-20
job repeat interval configuration, 5-10
jobs, for batch role resolution, 5-10

K

key stores, configuring, 5-5
keystore_dir system property
 setting for JBoss, 5-8
 setting for WebLogic, 5-7
 setting for WebSphere, 5-7

L

limit of characters for user group names, 10-4
Loader activation specifications (AS), 8-21
localized values from Oracle Identity Manager, 6-2

M

manifest file for Oracle Role Manager Integration Library, 2-4, 2-9
membership updates, 10-4
message beans, properties for (JBoss), 2-9
messages
 event types for, 2-9
 mapping message types from Oracle Role Manager to plug-in Java code, 2-8

O

objectdeletion_1_0.xsd file, 2-8
OIM ORM bus, configuring in WebSphere, 8-17
OIM ORM QCF connection factory, configuring in WebSphere, 8-21
OIM ORM Queue, configuring in WebSphere, 8-21
oim_integration.car file
 about, 2-5
 extracting files from, 5-9
oim_systemIdentity.car file
 about, 2-5
 copying to Oracle Role Manager, 5-3
oim_systemIdentity.dar file
 about, 2-5
 copying to Oracle Role Manager, 5-3
 loading into Oracle Role Manager, 5-4
oimID attribute, 10-9
OIM-Integration.jar file
 about, 2-6
 copying to Oracle Identity Manager, 2-3, 3-3
OIM-IntegrationSupport.jar file
 about, 2-7
 copying to Oracle Identity Manager, 2-3, 3-2
oimorm-service.xml file
 about, 2-9

- copying to the Oracle Identity Manager application server (JBoss), 9-3
- OIMRoleUpdate Bus, configuring in WebSphere, 8-20
- oimRootDir policy, modifying, 6-2
- oimSystem system identity
 - resetting password for, 5-4
- oimSystemProps.txt file, about, 5-4
- Oracle Identity Manager
 - changing oimRootDir policy for, 6-2
 - configuration, 6-1
 - configuration for WebSphere, 8-13
 - creating system user for integration, 6-3
 - creating system user for integration (WebLogic), 6-2
 - importing configuration into, 2-5
 - start-up command modification for JBoss, 7-5, 9-4
 - supported versions, 2-1
 - users with oimID attribute, 10-9
- Oracle Role Manager
 - database alias in WebSphere, 8-14, 8-15
 - server configuration, 5-9
- Oracle Role Manager Integration Library
 - about, 1-1
 - architecture, 1-4
 - build and release information, 2-9
 - configuration files for, 5-9
 - creating system user in Oracle Identity Manager for, 6-3
 - manifest file, 2-4
 - schema definition file for configuration, 2-9
 - schema definition file for plug-in configuration, 2-9
 - schema for, 2-9
- orm_encryption.jar file
 - about, 2-6
 - adding to the WebLogic class path, 7-5
 - adding to the WebSphere shared library, 8-24
 - adding to WebLogic class path, 7-5
 - copying to JBoss, 9-4
- ORM_ROOT_DIR argument for start-up command
 - setting for JBoss, 7-5, 9-4
- ormEncrypt policy, modifying value for, 5-8
- ORMITResourceName system property, 6-9
- ormJMSConnectionFactory
 - configuring in WebSphere, 8-20
 - default value for JBoss, 6-7
 - value for WebSphere, 6-6
- ormJMSQueue
 - configuring in WebSphere, 8-21
 - default value for JBoss, 6-6
 - value for WebLogic, 6-6
 - value for WebSphere, 6-6
- ormoimBase.xml file
 - about, 2-5, 6-5
 - importing into Oracle Identity Manager, 6-5
 - modifying, 6-5
- ormoimSample.xml file
 - about, 2-8, 6-5
 - importing into Oracle Identity Manager, 6-7

- ormoim-service.xml file
 - about, 2-9
- ormServerJNDI
 - default value for JBoss, 6-7
 - value for WebLogic, 6-6
 - value for WebSphere, 6-6
- ormSystem system user, assigning to the system group, 6-8
- ormSystem system user, creating in Oracle Identity Manager (JBoss), 6-3
- ormSystem system user, creating in Oracle Identity Manager (WebSphere), 6-3
- Outgoing Event Manager configuration, 5-15

P

- passwords, resetting for system identities, 5-4
- performance, impact from Full User Reconciliation task, 10-2
- permissions, to deploy integration on Oracle Identity Manager host, 2-2
- plug-ins, XML schema definition for, 2-9
- prefix for role names from Oracle Role Manager, 2-5
- prerequisites, 2-2
- process definitions, modifying, 10-11

Q

- queue connection factory
 - default value for JBoss, 6-7
 - for Oracle Role Manager (WebSphere), 8-8
 - for Oracle Role Manager Finalization (WebSphere), 8-21

R

- reconciliation
 - of deleted or inactive users, 10-1
 - of user groups, 10-4
 - predefined tasks for user, 10-1
- release information for Oracle Role Manager Integration Library, 2-9
- repeat interval configuration, 5-10
- repeat interval, for batch resolution simple timer, 5-11, 5-13
- resource objects, modifying, 10-10
- role approvals, importing configuration for sample, 6-7
- role creation, configuring in Outgoing Event Manager, 5-15
- role grant policies, defining, 10-9
- role membership reconciliation, about, 1-2
- Role Membership Update timer configuration, 5-11
- role membership updates, 10-4
 - configuring in Outgoing Event Manager, 5-15
- role names
 - uniqueness constraint in Oracle Identity Manager, 10-4
- roleManagerIntegration EAR files, about, 2-6
- roleManagerIntegration_JBoss4.2.3.ear, deploying, 9-5

- roleManagerIntegration_WebLogic10.3.ear, deploying, 7-11
- roleManagerIntegration_WebSphere6.1.ear, deploying, 8-28
- RoleUpdateDest bus (WebSphere), 8-20
- roleuserassignment_1_0.xsd file, 2-8

S

- sample configuration for approver processes, 2-8
- sample data for testing purposes, 10-1
- sample XML files for configuration, 5-9
- scheduled tasks for user reconciliation, about, 1-1, 1-2
- schema for Oracle Role Manager Integration Library, 2-9
- security credentials, configuring in WebLogic, 7-10
- semicolons, as delimiter in CAR collections, 5-2
- server configuration, default configuration settings, 5-9
- server_api_14.jar file
 - about, 2-6
 - adding to the WebSphere shared library, 8-24
 - adding to WebLogic class path, 7-5
 - copying to Oracle Identity Manager, 2-3, 3-3
- servers, adding to JMS messaging buses (WebSphere), 8-5, 8-17
- signed messages, configuring, 5-5
- simple timer configuration, 5-10
- standard Batch Resolution Timer, configuration for, 5-10
- start-up command for Oracle Identity Manager (JBoss), 7-5, 9-4
- system identity, loading the oimSystem system identity into Oracle Role Manager, 5-4
- system property, configuring in Oracle Identity Manager, 6-9
- system users
 - creating in Oracle Identity Manager, 6-3
 - creating in Oracle Identity Manager (WebLogic), 6-2

T

- timer configuration
 - for batch role resolution, 5-10
 - for role membership reconciliation, 5-11
- timers, implementing class for, 5-11, 5-12
- truncated roles names from Oracle Role Manager, 10-4
- TTY access, 0-xiii

U

- uniqueness constraint violations, 10-4
- user groups
 - character limit for names, 10-4
 - membership updates, 10-4
 - prefix for names from Oracle Role Manager, 2-5
 - reconciling, 10-4
 - uniqueness constraint for names, 10-4

- user provisioning and reconciliation. about, 1-1
- user reconciliation
 - business logic for incoming event, 5-17
 - deleting users in Oracle Role Manager during, 5-15
 - predefined tasks for, 10-1
- User user group in Oracle Identity Manager (WebLogic), 6-2

V

- version of Oracle Role Manager Integration Library, 2-9

W

- WebLogic
 - configuration, 7-1
 - supported versions, 2-1
- WebSphere
 - configuration, 8-1
 - supported versions, 2-1
- websphere_stubs.jar file
 - about, 2-6
 - adding to the WebSphere shared library, 8-24
 - copying to Oracle Identity Manager, 2-3, 3-3

X

- xelsysadm user ID for Oracle Identity Manager, 6-5
- xercesImpl.jar file
 - about, 2-6
 - copying to the endorsed directory (WebLogic), 7-6, 8-25
- xlAPI.jar file
 - adding to the WebSphere shared library, 8-24
- xlStartServer command
 - modification for JBoss, 7-5, 9-4
- XML elements, empty values in, 5-15
- XML files, for configuration, 5-9
- XML schema definitions
 - for event types in messages, 2-9
 - for interpreting message payloads, 2-8
 - for object deletion, 2-8
 - for role and user assignment, 2-8
 - for the Oracle Role Manager Integration Library framework, 2-9
 - for the plug-in configuration, 2-9
- xml-apis.jar file
 - about, 2-6
 - copying to the endorsed directory (WebLogic), 7-6, 8-25