Oracle® Role Manager

Integration Guide

Release 10*g* (10.1.4)

E12030-05

February 2009

ORACLE®

Oracle Role Manager Integration Guide Release 10*g* (10.1.4)

E12030-05

Copyright © 2008, 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Carla Fabrizio

Contributing Authors: Prakash Huliker, Alankrita Prakash

Contributors: Miles Chaston, Ashish Chugh, April Escamilla, Bennett Falk, Stephen Grenholm, Ashish Gupta, Parvinder Kaur, Gopal Kumarappan, Avinash Mittal, Devender Sharma

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

7 Testing the Oracle Role Manager Integration Library Installation

8 Troubleshooting

A Cron Expressions

Index

List of Examples

List of Tables

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.

TTY Access to Oracle Support Services

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

Assistant contacts Oracle Support Services, an Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

Related Documents

For more information, see the 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*

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introducing the Oracle Role Manager Integration Library

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

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 (Role Manager) with provisioning systems.

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 (Identity Manager) and includes the following features:

- User provisioning and reconciliation
  - Real-time creation of an account (person) in Role Manager for every Identity Manager user.

    Users must have Role Manager accounts before they can be granted roles in Role Manager and this feature automates the process.
  - Real-time update of user data from Identity Manager.

    For all user attributes configured in XML to be sent to Role Manager, changes made to those values are sent as soon as they are submitted in Identity Manager. This ensures that for all people in the Role Manager system who are also users in Identity Manager, Identity Manager remains the authoritative system of record for users and user attributes.
  - Scheduled tasks for user reconciliation.

    Scheduled tasks ensure that user data in both systems is synchronized. This consists of sending all user records from Identity Manager to Role Manager and ensuring that all users denoted as originating from Identity Manager have a corresponding Identity Manager user record.

- Roles and role membership reconciliation
  - Scheduled creation of user groups in Identity Manager for all Business Roles and IT roles in Role Manager.

    Business Roles and IT roles from Role Manager are represented in Identity Manager as user groups. System Roles and Approver Roles in Role Manager do not have corresponding user groups in Identity Manager.
  - Scheduled updates to status of user groups and membership lists in Identity Manager that have corresponding Business Roles or IT roles in Role Manager.

    Any status changes to roles in Role Manager that affect user groups in Identity Manager are reflected in Identity Manager. For example, if a Business Role or IT role is deleted in Role Manager, the corresponding user group in Identity Manager is deleted. In addition, if a Business Role or IT Role in Role Manager has been made inactive, the membership lists of the corresponding user group in Identity Manager is updated to remove invalid memberships.
  - Scheduled updates to user group membership lists in Identity Manager based on both directly granted and dynamically derived role memberships in Role Manager.
- Approver roles for approval processes
  - Real-time queries from Identity Manager for approvers in Role Manager.

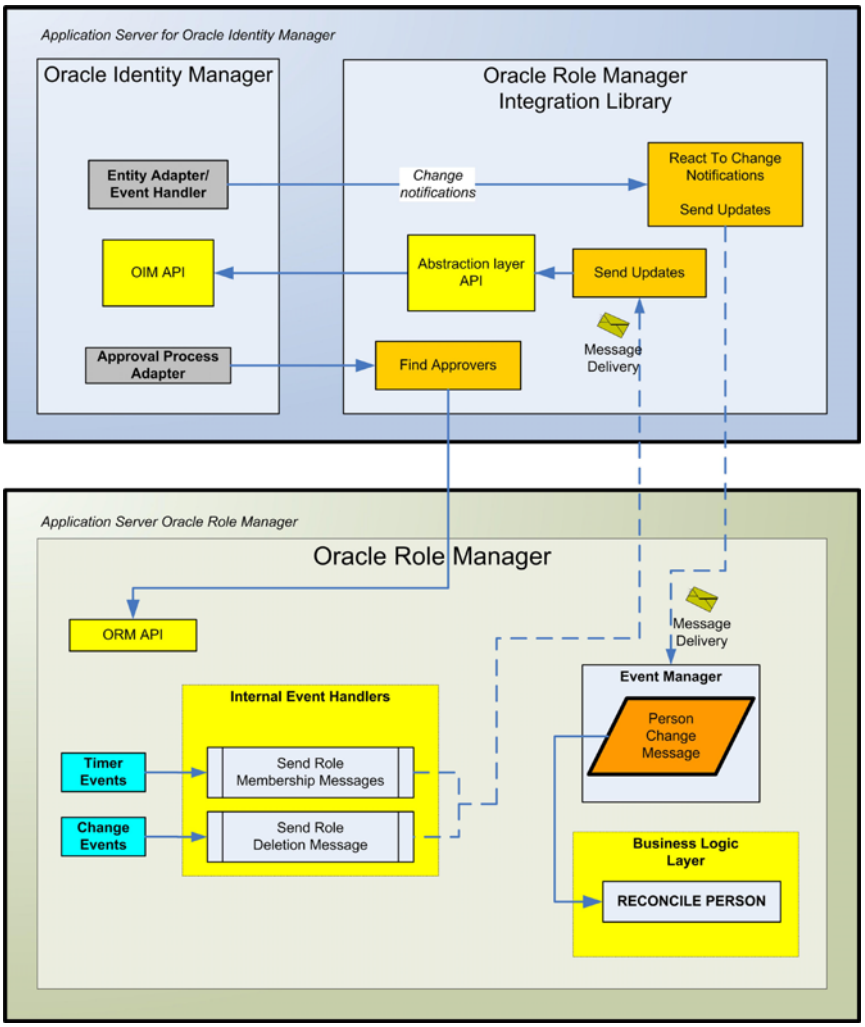
    Identity Manager can dynamically query Approver Roles in Role Manager to find qualified approvers to use in approval processes.

1.2 Architecture

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

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

Figure 1–1 High-Level Architecture



2

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 (Role Manager) Integration Library with Oracle Identity Manager (Identity Manager) in your environment.

This chapter includes the following sections:

2.1 Verifying Requirements

Table 2–1 lists the requirements for the three supported configurations of Role Manager Integration Library with Oracle Identity Manager. 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 10.1.4.1.1 on JBoss 4.2.3.	Oracle Identity Manager release 9.1.0.1 on JBoss 4.2.3.
Oracle Role Manager release 10.1.4.1.1 on WebLogic 10.3.	Oracle Identity Manager release 9.1.0.1 on WebLogic 10.3

2.2 Before You Start

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

- **Role Manager**
  - 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 Role Manager has been started.
  - Role Manager has been successfully deployed on the application server.
  - The application server for Role Manager is not running.
- **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 Identity Manager host.
  - You know the Identity Manager administrator user name and password to access both the Design Console and the Administrative and User Console.
  - The application server for Identity Manager is on the same host as the Identity Manager installation directory.

If any of the Role Manager prerequisites are not met, see *Oracle Role Manager Installation Guide* for instructions.

Note: It is recommended that Role Manager and 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 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. Obtain and distribute the Role Manager Integration Library software files.
3. Prepare Role Manager with the Integration Library configuration and business model.
4. Prepare Identity Manager for the integration (modify startup command, import configuration, create the Role Manager user, and create a system property).
5. Prepare the Identity Manager application server for deployment and deploy the Integration Library application.
6. Test the installation and configuration using procedures in Chapter 7 (user and role reconciliation, group membership reconciliation, and approval role resolution).

2.4 Obtaining the Role Manager Integration Library Software

Copy the Role Manager Integration Library software onto the application server host where Identity Manager is deployed as described in the following procedure.

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

To obtain the software:

1. From the application server host where Identity Manager is deployed, go to the following address using a Web browser:

   `http://www.oracle.com/technology/software`

2. Click **Identity Management**.
3. Accept the Oracle license terms.
4. Click the link next to **Oracle Role Manager Integration Library** and save the ORMIntegration_OIM.zip file to a temporary location.
5. Extract the contents of the zip file to the location to contain the root installation directory for the Integration Library.

   > **Note:** When selecting the root directory, consider that the zip file by default creates the directory ORMINT_HOME into which the Integration Library files are extracted. For example, if you choose C:\, the files is be placed into C:\ORMINT_HOME.
   >
   > The Integration Library expects to find its configuration and binary files in ORMINT_HOME. If you change the name of this directory, you must also change it in the application server configuration. For more information, see the application server configuration sections. To avoid confusion, this guide refers to this directory in uppercase italic as with other home directory variables.

   For a detailed description of the individual files in the Integration Library, see Section 2.6.

2.5 Distributing the Integration Library Software

After you have extracted the files from the downloaded zip file, you must distribute some of those files into Identity Manager directories as described in this section.

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

To distribute the Integration Library software:

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

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

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

```
ORMINT_HOME/oimlib/OIM-Integration.jar
ORMINT_HOME/lib/server_api_14.jar
```

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

```
ORMINT_HOME/oimlib/ScheduledFullUserReconciliation.class
ORMINT_HOME/oimlib/ScheduledIntegrationTask.class
ORMINT_HOME/oimlib/ScheduledRoleReconciliation.class
ORMINT_HOME/oimlib/ScheduledUserReconciliation.class
```

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 many 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
■ MANIFEST.MF	Contains version information for the deployed integration code.
■ readme.txt	Contains a pointer to this guide.
bin/	
■ create_keystore.bat ■ create_keystore.sh	Script that creates the key store password and stores it to a file named keystore.store, creates a random symmetric key for that password and serializes it to a file named keystore.key, and 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.
■ create_key_pair.bat ■ create_key_pair.sh	Script that creates an asymmetric key pair for the provided alias and the certificate target file. It adds a new property to keystore.properties called *alias*.password, for the provided alias whose value is a base64-encoded encrypted value of the alias password, encrypted using the symmetric key.
■ import_certificate.bat ■ import_certificate.sh	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.
config/	
■ IMConfig.xml	Shared by the integration code handling incoming messages and the Role Manager Integration Library functionality contained in the Identity Manager extension directories (JavaTasks, EventHandlers, and ScheduleTask). This file contains the editable prefix that is used to identify user groups in Identity Manager that correspond with roles in Role Manager. The default value is ORM followed by an underscore (_) that is added by the system.

Table 2–2 (Continued) Oracle Role Manager Integration Library Files

File in Integration Library Home	Description
▪ oim_integration.car	Contains the extensions to the standard model (data model and business logic) necessary for the Integration Library to function with Identity Manager. This file is manually copied to *ORM_HOME*/config for deployment convenience.
▪ oim_systemIdentity.car	Contains the configuration that once deployed, configures the oimSystem system identity for connections to the Identity Manager system. This file is manually copied to *ORM_HOME*/config for deployment convenience
▪ oim_systemIdentity.dar	Contains the data that must be loaded to complete the creation of the oimSystem system identity. This file is manually copied to *ORM_HOME*/config for deployment convenience
▪ ormoimBase.xml	Contains the base Identity Manager configuration needed to support the Integration Library. The settings in this file are manually imported into Identity Manager.
lib/	
▪ commons-logging.jar	Contains logging libraries needed to support J2EE 1.3 logging. For WebLogic, this file is manually added as a shared library. **NOTE**: This file is needed only if Identity Manager is deployed on WebLogic.
▪ orm_encryption.jar	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. For JBoss, the file is manually copied to *JBOSS_HOME*/server/default/lib. For other application servers, this file is manually added as a shared library.
▪ roleManagerIntegration_JBoss4.2.3.ear ▪ roleManagerIntegration_WebLogic10.3.ear	Responsible for the initial handling of messages arriving from 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. For JBoss, the file is manually copied to *OIM_appserver*/deploy as part of the deployment process. For other application servers, this file is manually deployed through the administrative console user interface.
▪ server_api_14.jar	Contains additional shared libraries required for a deployment on an application server (a copy is also located in *OIM_HOME*/xellerate/JavaTasks). For JBoss, this file is manually copied to *OIM_appserver*/lib and *OIM_HOME*/xellerate/JavaTasks. For other application servers, this file is manually added as a shared library.

Table 2–2 (Continued) Oracle Role Manager Integration Library Files

File in Integration Library Home	Description
■ xercesImpl.jar ■ xml-apis.jar	Contains libraries needed to support J2EE 1.3 JAXP 1.1 for XML parsing. These files are manually added to the *OIM_appserver*/jdk/jre/lib/endorsed directory. **NOTE**: These files are needed only if Identity Manager is deployed on WebLogic. If Identity Manager is on JBoss, these files are not used.
oimlib/	
■ OIM-Integration.jar	Contains the class files for handling approval role resolution between roles in Role Manager and user groups in Identity Manager. This file is manually copied to *OIM_HOME*/xellerate/JavaTasks.
■ OIM-IntegrationSupport.jar	Contains the class files that support the underlying integration framework (a copy is also located in `EventHandlers`). This file is manually copied to *OIM_HOME*/xellerate/EventHandlers.
■ OIM-IntegrationTransport.jar	Contains the class files that support sending messages from the integration to Role Manager. This file is manually copied to *OIM_HOME*/xellerate/EventHandlers. For JBoss, this file is also copied to *JBOSS_HOME*/server/default/lib.
■ ScheduledFullUserReconciliation.class	Task for Full reconciliation of users including synchronous inspection of the Role Manager state. This file is manually copied to *OIM_HOME*/xellerate/ScheduleTask.
■ ScheduledIntegrationTask.class	Base task used by all other Role Manager scheduled tasks. This file is manually copied to *OIM_HOME*/xellerate/ScheduleTask.
■ ScheduledRoleReconciliation.class	Inspects the state of roles in Role Manager. This file is manually copied to *OIM_HOME*/xellerate/ScheduleTask.
■ ScheduledUserReconciliation.class	Sends all Identity Manager user records to Role Manager except for system user records This file is manually copied to *OIM_HOME*/xellerate/ScheduleTask.
pluginConfigDir/ ■ RoleDeletion.xml ■ RoleUsersAssignment.xml	Contains XML files of handler configurations that map message types for messages arriving from Role Manager to plug-in Java code that handles the messages. Also contains the XML schema definitions required to interpret the message payloads. **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.

Table 2–2 (Continued) Oracle Role Manager Integration Library Files

File in Integration Library Home	Description
pluginSchema/ ▪ objectdeletion_1_0.xsd ▪ roleusersassignment_1_0.xsd	Contains the XML schema definitions for interpreting payloads sent in messages from Role Manager. These definitions must exactly correspond with the schema of the business logic plug-ins in Role Manager used by the originators of the messages. **Note:** Integrators who add functionality to the integration can add their own XML schema files to this directory. The provided XSD files are (prepended by oracle.iam.rm.bizlogic to be fully qualified).
samples/	
▪ ormoimSample.xml	The file used to import a sample approval workflow into Identity Manager. This is used when testing the installation as described in Section 7.3, "Testing Approval Role Resolution."
samples/jboss/	

▪ oimorm-service.xml	Sample configuration for the JMS queues required to support the Role Manager Integration Library. The values in this file can be modified to reflect the actual deployment environment, including the JNDI location of Role Manager, for example, to change the message bean properties java.naming.provider.url attribute.
	For example, if the Role Manager application server is run on a host named Server_ORM, and the jnp bind address is 1099 as specified in the jboss-service.xml file where it is deployed, then the values for java.naming.provider.url should be:
	`jnp://Server_ORM:1099/queue`
	`jnp://Server_ORM:1099/ejb/orm`
	This file is manually copied to *OIM_appserver*/deploy. This file is only applicable to JBoss. Other application servers have other means for JMS queue configuration.

▪ ormoim-service.xml	Configuration file for the JMS queues required to support the Integration Library on the Role Manager application server. This file is manually placed into the application server's deploy directory. The settings in this file may have to be modified to reflect your deployment environment, including the JNDI location of Identity Manager, for example, to change the message bean properties java.naming.provider.url attribute. For example, if the 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 values for java.naming.provider.url should be: `jnp://Server_OIM:1099/queue` This file is manually copied to *ORM_appserver*/deploy. Other application servers have other means for JMS queue configuration.

Table 2–2 (Continued) Oracle Role Manager Integration Library Files

File in Integration Library Home	Description
schema/	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. The schema file names are prepended with oracle.iam.rm to be fully qualified.
■ event.event_1_0.xsd	Description of the standard Role Manager event type to which messages sent from Role Manager to Identity Manager adhere.
■ imframework.imconfig_1_0.xsd	Schema of the Role Manager Integration Library configuration file (IMConfig.xml).
■ imframework.pluginconfig_1_0.xsd	Schema of the files in the Role Manager Integration Library pluginConfigDir directory.

2.7 Determining the Release Number of the Integration Library

Release information for the 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 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.

3

Configuring Oracle Role Manager

This chapter describes the steps to configure Oracle Role Manager (Role Manager) for the Oracle Role Manager Integration Library (Integration Library).

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

This chapter includes the following sections:

3.1 Deploying the Integration Library Configuration

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

> **Note:** If you want to modify the standard configuration of the Integration Library components, for example, if you want 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 3.7, "Modifying Component Configuration."

To deploy the Integration Library configuration:

1. On the Role Manager installation host, navigate to *ORM_HOME*/config.
2. Ensure that the db.properties file 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 Role Manager users were created.

3. Stop the Role Manager application server if it is running.
4. In a command window, navigate to *ORM_HOME*/bin and run the following command:

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

> **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 (:)

In this command:

- *collection_of_cars* contains the relative paths and file names of the CAR files to deploy
- *orm-owner* is the user name of the Role Manager database owner user/schema
- *ormapp-user* is the user name of the Role Manager application user/schema
- *admin-user* is the user name of the Role Manager system administrator

For example, if you have no customizations, the collection of CAR files on Windows would be:

```
"..\config\oim_integration.car"
```

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"
```

(For information about modifying the standard configuration for components affecting the Integration Library, see Section 3.7, "Modifying Component Configuration.")

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

3.2 Creating the oimSystem System Identity

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

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

To create the oimSystem system identity:

1. On the Integration Library installation host, copy the following files from *ORMINT_HOME*/config into the *ORM_HOME*/config directory on the Role Manager installation:

   ORMINT_HOME/config/oim_systemIdentity.car
   ORMINT_HOME/config/oim_systemIdentity.dar

2. Navigate to *ORM_HOME*/config on the Role Manager installation host.
3. Stop the Role Manager application server if it is running.
4. In a command window, navigate to *ORM_HOME*/bin and run the following command.

   For UNIX-based systems:

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

   For Windows systems:

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

   In this command:

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

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

3.3 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 Role Manager Administrative Console.

To load the oimSystem system identity relationship data:

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

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

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

3. Enter the user name and password of the 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.

3.4 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 Role Manager server.
2. On the 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:

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

   For Windows systems:

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

   In this command, *ormapp-user* is the user name of the database 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 Role Manager application user/schema.
6. At the prompt, enter a new password for the oimSystem system identity.

3.5 Configuring the Oracle Identity Manager Home Directory

Depending on where 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 Role Manager.

Note: If 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 Identity Manager home directory:

1. On the 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 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 Identity Manager.
4. Save and close the IMConfig.xml file.

3.6 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 Identity Manager to Role Manager.

The procedure in this section first creates the key store password on the 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 3.6.1.

To configure encryption:

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

   For UNIX-based systems:

   ```
   bash 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).

3. At the prompt, enter a password for the Identity Manager key store.

   You should see three new 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 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, depending on your operating system, 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:

   ```
   bash 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. Copy the new certificate file from *ORMINT_HOME*/bin to the Role Manager host into *ORM_HOME*/bin.

6. On the Role Manager host, navigate to *ORM_HOME*/bin.

7. Run the command to create the Role Manager key store.

   For UNIX-based systems:

   ```
   bash create_keystore.sh
   ```

   For Windows systems:

   ```
   create_keystore.bat
   ```

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

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

   For UNIX-based systems:

   ```
   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.

10. For WebLogic, set the system property for the Role Manager key store directory as follows:

    a. Log on to the WebLogic Server Console using a Web browser.

    b. From **Environment**, select **Servers**, then select the server on which Role Manager is deployed.

    c. On the Configuration tab, click the **Server Start** subtab.

    d. In the Arguments field, append the following argument to any existing arguments:

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

       where *ORM_HOME* is the Role Manager installation directory

11. For JBoss, set the system property for the Role Manager key store directory as follows:

    a. On the 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 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 Role Manager installation directory.

    d. Save and close the file.

3.6.1 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 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.

3.7 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 Role Manager component configuration. Configuration settings are defined in XML files and packaged as a CAR (configuration archive) file that is deployed to 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:

3.7.1 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 3.7.2) and the configuration files for all the configurable 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. From the Identity Manager host, copy the oim_integration.car file in the *ORMINT_HOME*/config directory to the *ORM_HOME*/config directory on the Role Manager host.
2. Navigate to the *ORM_HOME*/config directory on the Role Manager host.
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_temp/oim_integration.

   The oim_integration 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/
       config/
            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/
                 roleMembershipUpdateTimer.xml
   ```

   The settings in these files are described in Section 3.7.3 through Section 3.7.6
4. If not performed previously, extract the entire contents of configurations.car into the temporary location, such as *ORM_HOME*/config_temp/configurations.

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

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

   For more information about the settings in this file, see Section 3.7.2. For information about the other configurable Role Manager server components, see *Oracle Role Manager Administrator's Guide*.

3.7.2 Modifying the Batch Resolution Timer

The batch resolution timer is included with the standard 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 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 3.7.2.1
4. Using a utility like WinZip or jar, repackage everything in the configurations directory and create a new 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 3.1, "Deploying the Integration Library Configuration.".

3.7.2.1 Batch Resolution Timer Configuration Settings

Table 3–1 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 3–1 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 3–1 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>
```

3.7.3 Modifying the Role Membership Update Timer

The role membership update timer controls the periodic process on Role Manager responsible for creating the messages for updates of role membership information (user-to-role assignments) from Role Manager to external systems. For example, for Identity Manager, this timer triggers the update of User Group memberships based on role memberships in Role Manager.

The role membership update timer configuration file is included with the oim_integration.car configuration bundle and sets preferences for the role membership resolution job. The 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 role membership update is equal to or longer than the batch resolution timer interval.

To modify the Role Membership Update Timer component:

1. Navigate to *ORM_HOME* on the 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 roleMembershipUpdateTimer.xml file as needed.

   For detailed information about the settings in this file, see Section 3.7.3.1.
4. Package your configuration changes with any other changes as described in Section 3.7.7 for deployment.

3.7.3.1 Role Membership Update Timer Configuration Settings

Table 3–2 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 3–2 Role Membership Update Timer Configuration Values

Element	Default Value
factory-classname	oracle.iam.rm.resolution.impl.RoleMembershipUpdateTimerFactory
job-id	RoleMembershipUpdateJob
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 3–2 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.RoleMembershipUpdateTimerFactory
         </factory-classname>
         <job-id>RoleMembershipUpdateJob</job-id>
         <group-id>BatchGroup</group-id>
         <parameters>
              <parameter>
                 <id>roleTypes</id>
                 <string>businessRole,itRole</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>
```

3.7.4 Modifying the Incoming Event Manager

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

To modify the Incoming Event Manager component:

1. Navigate to *ORM_HOME* on the 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 3.7.4.1.

4. Package your configuration changes with any other changes as described in Section 3.7.7 for deployment.

3.7.4.1 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 Identity Manager and custom business logic on Role Manager.

Example 3–3 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>
               <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 Role Manager during reconciliation. By default, this is set to false.

3.7.5 Modifying the Outgoing Event Manager

The Outgoing Event Manager configuration defines how messages generated by 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 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 3.7.5.1.
4. Package your configuration changes with any other changes as described in Section 3.7.7 for deployment.

3.7.5.1 Outgoing Event Manager Settings

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

Example 3–4 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>
```

3.7.6 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 new attributes to the user data to be sent to Role Manager from an external system.

To modify the Business Logic component:

1. Navigate to *ORM_HOME* on the 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 3.7.6.1.

4. Package your configuration changes with any other changes as described in Section 3.7.7 for deployment.

3.7.6.1 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 3–5 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>
          <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_ex
                t/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>
      <effective-date>
        <argument-id>startTime</argument-id>
      </effective-date>
      </snapshot-logic-definition>
    </business-transaction>
</operations>
</config>
```

3.7.7 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 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 new 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.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/
              roleMembershipUpdateTimer.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 3.1, "Deploying the Integration Library Configuration."

4

Configuring Oracle Identity Manager

This chapter contains procedures for configuring Oracle Identity Manager (Identity Manager) in preparation for the deployment of the Oracle Role Manager (Role Manager) Integration Library.

This chapter includes the following sections:

4.1 Before You Configure

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

The procedures in this chapter assume the following:

- You have the appropriate permission to add and modify files in the Identity Manager home directory on the host system.
- You have the appropriate permission to add and modify files in the application server on which Identity Manager is deployed.
- You have the appropriate permission to stop and start the application server on which Identity Manager is deployed.
- You know the administrator user name and password to access the Identity manager Administrative and User Console.
- You know the administrator user name and password to access the Identity Manager Design Console.

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

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

If you are updating an existing installation, you can skip this procedure.

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

To create and configure the Role Manager user:

1. On the 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 Identity Manager server if it is not running.
6. Connect to the Identity Manager Administrative and User Console.
7. If the user named Internal does not exist, create it as follows:
   a. Select **Users**, then select **Create**.

   > **Note:** For 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 **Organization** field, click the magnifying icon.
   f. In the Lookup Form window, select the organization in which you want to create the Internal user.
   g. Click **Select**.
   h. Click **Create User**.
8. If the user group named User does not exist, create it as follows:
   a. Select **Users Groups**, then select **Create**.

b. In the **Name** field, enter `User`.

c. Click **Create**.

9. Assign the `User Groups` and `User Groups.User Members` permissions to the User user group as follows:

> **Note:** If you have just created the user group named User, skip to step d.

a. Select **Users Groups**, then select **Manage**.

b. Serach for and select the **User** user group.

c. Click **Permissions**.

d. Click **Assign**.

e. In the results table, search for the `User Groups` permission, then select **Insert**, **Write Access**, **Delete Access** and **Assign** for the `User Groups` permission.

f. On the Confirmation page, click **Confirm Assign**.

g. Click **Assign**.

h. In the results table, search for the `User Groups.User Members` permission, then select **Insert**, **Write Access**, **Delete Access** and **Assign** for the `User Groups.User Members` permission.

i. On the Confirmation page, click **Confirm Assign**.

4.3 Creating the System User and User Group for Role Manager (JBoss)

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

If you are updating an existing installation, you can skip this procedure.

To create the Role Manager user:

1. Start the Identity Manager server if it is not running.
2. Connect to the Identity Manager Administrative and User Console.
3. Create the ormSystem user as follows:

a. Select **Users**, then select **Create**.

b. In the **User ID** field, enter `ormSystem`.

> **Note:** For Identity Manager on JBoss, 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 **Organization** field, click the magnifying icon.

f. In the Lookup Form window, select the organization in which you want to create the ormSystem user.

g. Click **Select**.

h. Click **Create User**.

4. Create the ormSystem user group as follows:

   a. Select **Users Groups**, then select **Create**.

   b. In the **Name** field, enter `ormSystem`.

   c. Click **Create**.

5. Assign the `User Groups` and `User Groups.User Members` permissions to the ormSystem user group as follows:

   a. Click **Permissions**.

   b. Click **Assign**.

   c. In the results table, search for the `User Groups` permission, then select **Insert**, **Write Access**, **Delete Access** and **Assign** for the `User Groups` permission.

   d. On the Confirmation page, click **Confirm Assign**.

   e. Click **Assign**.

   f. In the results table, search for the `User Groups.User Members` permission, then select **Insert**, **Write Access**, **Delete Access** and **Assign** for the `User Groups.User Members` permission.

   g. On the Confirmation page, click **Confirm Assign**.

6. Click the Save icon to save your changes.

4.4 Importing the Prepared Configuration

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

The first file, ormoimBase.xml, contains the essential configurations for a working integration. 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 Role Manager for approvers for a role, before creating similar resources and workflows for a production environment.

> **Note:** The following procedures assume that the Identity Manager administrator user ID is xelsysadm. If your installation of 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 Role Approvals

4.4.1 Importing the Base Configuration

The base configuration provides the framework configuration for the 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 Identity Manager server if it is not running.
2. Connect to the Identity Manager Administrative and User Console.
3. Select **Deployment Management**, then select **Import**.
4. In the Select File to 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 Identity Manager is deployed, define the parameters of the IT Resource for 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 3.2, "Creating the oimSystem System Identity."

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

- **For JBoss**

Field	Value
ormJMSQueue	`external/srqueues/orm/IncomingEventQueue`
ormAdmin	`oimSystem`
ormPassword	Enter the password of the oimSystem system identity that was set in Section 3.2, "Creating the oimSystem System Identity."
initialContextFactory	`org.jnp.interfaces.NamingContextFactory`
ormServerJNDI	`external/srserver/ServerEJB`
ormServerURL	Do not enter any value in this field.
ormJMSConnectionFactory	`external/srqueues/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. Right-click **ALL USERS**, then select **Remove**.
11. Right-click **SYSTEM ADMINISTRATORS**, then select **Remove**.
12. Click **Import**.
13. Click **OK** to confirm.

    You should see a confirmation message that import was successful.

4.4.2 Importing the Sample Configuration for Role Approvals

This procedure is necessary only if you want to test the 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 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, two processes, one process form, one data object definition, and one task adapter.
4. Click **Import**.
5. Click **OK** to confirm.

4.5 Assigning the System User to a User Group

Depending on the application server on which 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 Identity Manager Administration and User Console, select **Users**, then select **Manage**.
2. Search for the user named Internal (created in Section 4.2).
3. Click **Internal** to view details.
4. On the User Details page, select **Group Membership** from the list.
5. On the Assign Permissions page, click **Assign**.
6. Select the box next to the group named **User** (created in Section 4.2).
7. Click **Assign Group**.
8. Click **Confirm Assign** to confirm.

(Jboss) To assign the ormSystem user to the ormSystem user group:

1. From the Identity Manager Administration and User Console, select **Users**, then select **Manage**.
2. Search for the user named ormSystem (created in Section 4.3).
3. Click **ormSystem** to view details.
4. On the User Details page, select **Group Membership** from the list.
5. On the Assign Permissions page, click **Assign**.
6. Select the box next to the group named **ormSystem** (created in Section 4.3).
7. Click **Assign Group**.
8. Click **Confirm Assign** to confirm.

4.6 Configuring the IT Resource System Property

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

To configure the IT Resource system property:

1. Log in to the Identity Manager Design Console (Identity Manager client) using the user name and password entered in the Admin User Information page when installing Identity Manager.
2. On the left pane, expand the **Administration** folder.
3. Double-click **System Configuration**.
4. Choose the **Server** option.
5. In the **Name** field, enter `ORMITResourceName` as the name of the system property to create.
6. In the **Keyword** field, enter `XL.ORMITResourceName`.
7. In the **Value** field, enter `ORM ITResource.`

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

8. Click the Save icon on the toolbar.
9. Optionally, ensure that the values for the IT resource parameters are correct:
   a. On the left pane, expand the **Resource Management** folder.
   b. 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 4.4.1.

      If the values are different, enter the appropriate values.
10. If Identity Manager is installed on WebLogic, assign permissions as follows:
    a. Select **Resource Management**, then click **Manage IT Resource**.
    b. Search for and select **ORM ITResource**.
    c. From the **You can view additional information about this IT resource** list, select **Administrative Groups**.
    d. Select the box next to the group named **User** (created in Section 4.2).
    e. Click **Assign Group.**
    f. Select the appropriate boxes to specify the **Read** and **Write** permissions.
    g. Click **Assign.**
11. Click the Save icon on the toolbar.

5 Configuring WebLogic Server

This chapter contains procedures for configuring the WebLogic application servers for Oracle Identity Manager (Identity Manager) and Oracle Role Manager (Role Manager) in preparation for deployment of the Oracle Role Manager Integration Library (Integration Library).

This chapter includes the following sections:

5.1 Before You Configure

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

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

5.2 Configuring the Oracle Role Manager Server

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

This section includes the following subsections:

- (Clustered Mode Only) Configuring the Subdeployment of the Connection Factory
- (Clustered Mode Only) Disabling Authentication on the Oracle Role Manager Node

5.2.1 Configuring the JMS Connection Factory

To configure the JMS module connection factory:

1. If not currently on the WebLogic Server Console, in a Web browser, enter the URL. For example:

   `http://appserverhost:7001/console`

2. From **Services**, select **Messaging**, then select **JMS Modules**.
3. Click **ORM JMSModule**.
4. Click **New**.
5. Select the **Connection Factory** option.
6. Click **Next**.
7. In the **Name** field, enter `OIM ConnectionFactory`.
8. In the **JNDI Name** field, enter `external/srqueues/orm/QueueConnectionFactory`.
9. Click **Next**, then click **Finish**.

5.2.2 Configuring the Foreign JNDI Providers

To configure the foreign JNDI providers:

1. From **Services**, select **Foreign JNDI Provider**s.
2. Click **New**.
3. In the **Name** field, enter `Remote OIM ForeignJNDIProvider`.
4. Click **OK**.
5. To edit the settings, 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 Identity Manager application server host

   oim_port is the port for access to the Identity Manager server

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

8. In the **User** field, enter `Internal`.

9. In the **Password** field, enter the password of the Internal user (created in Section 4.2).
10. Click **Save**.
11. Configure the Remote OIM Connection Factory as follows:
    a. From **Services**, select **Foreign JNDI Providers**.
    b. On the Links tab, click **New**.
    c. In the **Name** field, enter `RoleUpdateQCF`.
    d. In the **Local JNDI Name** field, enter `oim/OIMserver/QueueConnectionFactory`.
    e. In the **Remote JNDI Name** field, enter `oim/OIMserver/QueueConnectionFactory`.
    f. Click **OK**.
12. Configure the Remote OIM Queue as follows:
    a. From **Services**, select **ForeignJNDI Providers**.
    b. On the Links tab, click **New**.
    c. In the **Name** field, enter `RoleUpdateQueue`.
    d. In the **Local JNDI Name** field, enter `oim/OIMserver/RoleManagerQueue`.
    e. In the **Remote JNDI Name** field, enter `oim/OIMserver/RoleManagerQueue`.
    f. Click **OK**.

5.2.3 Configuring the Security Credentials

To configure the credentials:

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

5. In the **Confirm Credential** field, enter the credential again.
6. Click **Apply** and save your changes.
7. Restart the Role Manager server for these changes to be in effect.

5.2.4 (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 Identity Manager connection factory:

1. In the domain tree, select **Services**, then select **Messaging**.
2. Select **JMS Modules**, then click **ORM JMS Module**.
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**.

5.2.5 (Clustered Mode Only) Disabling Authentication on the Oracle Role Manager Node

This procedure disables transaction authentication for 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 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 Role Manager domain including the admin server.

5.3 Configuring the Oracle Identity Manager Server

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

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

This section includes the following subsections:

- Modifying the Identity Manager Startup Script
- Configuring the Classpath and Shared Libraries
- (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

5.3.1 Modifying the Identity Manager Startup Script

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

For UNIX-based systems, to modify the startup script:

1. On the Identity Manager host, navigate to the domain on which Identity Manager is deployed. For example, *WEBLOGIC_HOME*/user_projects/domains/*mydomain*.
2. Open the xlStartWLS.sh file for editing

> **Note:** If you have a managed server environment where the server is started from this script, open the xlstartManagedWebLogic.sh file instead.

3. In the entry for JAVA_OPTIONS, add a backslash (\) at the end of the -Djava.awt.headless=true argument.
4. 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 Role Manager Integration Library.

   The complete entry might be similar to:

   ```
   JAVA_OPTIONS="-DXL.HomeDir=$XLHOME \
          -Djava.security.auth.login.config=$XLHOME/config/authwl.conf \
          -Dlog4j.configuration=file:$XLHOME/config/log.properties \
          -Djava.awt.headless=true \
          -DORMINT_ROOT_DIR=/opt/ormintegration"
   ```

5. Save and close the start script.
6. Restart the Identity Manager server for these changes to be in effect.

For Windows-based systems, to modify the startup script:

1. On the Identity Manager host, navigate to the domain on which Identity Manager is deployed. For example, *WEBLOGIC_HOME*/user_projects/domains/*mydomain*.
2. Open the xlStartWLS.bat file for editing:

> **Note:** If you have a managed server environment where the server is started from this script, open the xlstartManagedWebLogic.cmd file instead.

3. In the entry for JAVA_OPTIONS, add a caret (^) at the end of the -Djava.awt.headless=true argument.

4. 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 Role Manager Integration Library.

   The complete entry might be similar to:

   ```
   SET JAVA_OPTIONS=-DXL.HomeDir=%XLHOME% ^
      -Djava.security.auth.login.config=%XLHOME%\config\authwl.conf ^
      -Dlog4j.configuration=file:/%XLHOME%/config/log.properties ^
      -Djava.awt.headless=true ^
      -DORMINT_ROOT_DIR=C:\ormintegration
   ```

5. Save and close the start script.
6. Restart the Identity Manager server for these changes to be in effect.

5.3.2 Configuring the Classpath and Shared Libraries

Some libraries must be added to either the system classpath or to the WebLogic start script. The following procedure describes how to modify the start script, although you can optionally modify the system classpath if you prefer.

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

To configure the classpath in the WebLogic start script

1. On the file system where 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. On the file system where Identity Manager is deployed, navigate to the domain directory that contains the server for Identity Manager. For example, *OIM_appserver*`/user_projects/domains/oimdomain`.
4. For Windows systems, open the xlStartWLS.cmd file for editing.

   > **Note:** If you have a managed server environment, open the xlstartManagedWebLogic.cmd file instead.

5. For UNIX-based systems, open the xlstartWLS.sh file for editing.

   > **Note:** If you have a managed server environment , open the xlstartManagedWebLogic.sh ifile nstead.

6. 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

7. Save and close the start script.
8. Restart the Identity Manager server.

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

To configure JMS queues and connection factories:

1. 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 new JMS module to the 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. Select the Identity Manager cluster as the target, for example, **OIM_Cluster**, then click **Apply**.
2. Configure a JMS server for each 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. Select the Targets tab and assign the JMS server to the first Identity Manager managed server, for example, **OIM_Server1**.
   f. Click **Save**.
   g. Repeat these steps for each managed server. For example, create ORMIntegration2 and assign it to OIM_Server2, and so on.
3. 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 **Next**.

k. Select the Targets tab select each of the JMS servers created in step 2. For example, **ORMIntegration1** and **ORMIntegration2**.

l. Click **Finish**.

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

To configure JMS queues and connection factories:

1. 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 new module to **AdminServer**, then click **Next**.
   e. Select the **Would you like to add resources** box, then click **Finish**.
   f. On the Settings page, click **New**.
   g. Select **ConnectionFactory**, 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**.
2. 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`, then click **Next**.
   d. Click **Finish**.
   e. Click **ORMIntegration**.
   f. Select the Targets tab and assign the new server to **AdminServer**.
   g. Click **Save**.
3. 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. Select **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 **Create a New Subdeployment**.

h. In the **Subdeployment Name** field, enter `ormJMSQueue subdeployment`.

i. Click **Next**.

j. Select the Targets tab select **ORMIntegration** as the JMS Server.

k. Click **Finish**.

5.3.5 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 **JNDI Initial Context Factory** field, enter `weblogic.jndi.WLInitialContextFactory`.

   f. In the **Provider URL** field, enter `t3://`*`orm_ipaddress`*`:`*`orm_port`*

   where

   `orm_ipaddress` is the IP address of the Role Manager application server host

   `orm_port` is the port for access to the Role Manager server.

   Note: If you a configuring a clustered server environment, the URL must be in the form `t3://`*`oim_ipaddress1`*`:`*`port`*`,t3://`*`oim_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 5.2.1, "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**.

5.3.6 Configuring Security Credentials

To configure the credentials:

1. Click the domain where the 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 Role Manager server (see step 4 of Section 5.2.3).

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 Identity Manager and Role Manager.

4. In the **Confirm Credential** field, enter the credential again.
5. Click **Save**.

5.3.7 (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 Console using a Web browser.
2. For each managed server, configure the system properties as follows:
   a. On the 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. Click **Apply** and save your changes.

3. Start the node manager on each managed server, then start each managed server.

5.4 Deploying the Role Manager Integration Library Application

To deploy the Integration Library application:

1. From the Identity Manager host, connect to the WebLogic Server Console in a Web browser. For example:

   http://*appserverhost*:7001/console

2. Select **Deployments**, then select **Applications**.
3. Click **Deploy a new Application**.
4. Choose **Upload your Files**, then click **Browse** to navigate to the *ORMINT_HOME*/lib directory.
5. Select **roleManagerIntegration_WebLogic10.3.ear**, then click **Continue**.
6. If you are configuring a clustered server environment, in the **Target** list, select **OIM cluster**.
7. Ensure that the name in the **Name** field is set as roleManagerIntegration, then click **Deploy**.

   In the Status of Last Action column, you should see indication of successful deployment

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

6

Configuring JBoss

This chapter contains procedures for configuring the JBoss application servers for Oracle Identity Manager (Identity Manager) and Oracle Role Manager (Role Manager) in preparation for deployment of the Oracle Role Manager Integration Library (Integration Library).

This chapter includes the following sections:

6.1 Before You Configure

The Role Manager Integration Library is intended to be deployed on the application server on which 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 Identity Manager is deployed.
- You have the appropriate permission to stop and start the application server where Identity Manager is deployed.

6.2 Configuring the Oracle Role Manager Server

To configure the Role Manager server:

1. On the Role Manager application server host, copy the following file into the deploy directory of the application server for Role Manager (for example, C:\jboss-4.2.3\server\default\deploy):

   ORMINT_HOME/samples/jboss/ormoim-service.xml

2. Edit the settings in the ormoim-service.xml file for your environment.

   This file contains sample configuration for the JMS queues 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 Identity Manager, for example, to change the message bean properties java.naming.provider.url attribute.

For example, if the 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 values for java.naming.provider.url should be:

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

6.3 Configuring the Oracle Identity Manager Server

To configure the Identity Manager server:

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

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

2. Edit the settings in the oimorm-service.xml file for your environment.

   This file contains sample configuration for the JMS queues 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 Role Manager, for example, to change the message bean properties java.naming.provider.url attribute.

   For example, if the Role Manager application server is run on a host named Server_ORM, and the jnp bind address is 1099 as specified in the jboss-service.xml file where it is deployed, then the values for java.naming.provider.url should be:

   ```
   jnp://Server_ORM:1099/queue
   jnp://Server_ORM:1099/ejb/orm
   ```

3. Copy the following two files into *JBOSS_HOME*/server/default/lib:

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

6.3.1 Modifying the Identity Manager Startup Command

Before you can start using the Role Manager Integration library, the 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 Identity Manager until it is restarted.

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

1. Open the following file for editing:

   For UNIX-based systems:

   ```
   $ $OIM_HOME/xellerate/bin/xlStartServer.sh
   ```

   For Windows systems:

   ```
   OIM_HOME\xellerate\bin\xlStartServer.bat
   ```

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

   ```
   -DORMINT_ROOT_DIR=ORMINT_HOME
   ```

   where *ORMINT_HOME* is the full path to the home directory of the 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. Save and close the start script.
4. For these changes to go into effect, restart the Identity Manager server.

6.4 Deploying the Role Manager Integration Library Application

To deploy the Integration Library application:

1. On the Identity Manager application server host, copy the following file into the deploy directory of the application server for Identity Manager (for example, C:\jboss-4.2.3\server\default\deploy):

   ```
   ORMINT_HOME/lib/roleManagerIntegration_JBoss4.2.3.ear
   ```

2. Restart the application server.

7

Testing the Oracle Role Manager Integration Library Installation

After you deploy and configure the Oracle Role Manager (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 Role and Role Membership Reconciliation
- Testing Approval Role Resolution

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 Role Manager. If you did not load the sample data, you can still use these tests but you must create objects in Role Manager similar to those described in each test.

7.1 Testing User Reconciliation

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

Because there may be situations when the 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 Role Manager is not available, are later propagated to Role Manager.

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

7.1.1 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 Identity Manager who appears in Role Manager.

To test user reconciliation:

1. If not currently running, start Identity Manager and then Role Manager.
2. Using the 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 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 Identity Manager should display in the search results.

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

   Note that the name change from Identity Manager has not been updated.
5. Enable the user reconciliation task as follows:
   a. In the Identity Manager Design Console (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.
   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.
6. After a minute, in Role Manager, click **Filter** again to refresh the search results.

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

7.2 Testing Role and Role Membership Reconciliation

Updates to user groups in Identity Manager (groups that correspond to Business Roles and IT Roles in Role Manager) occur when the role membership update timer triggers Role Manager to send synchronization messages. Along with membership changes, new roles created in Role Manager are also received in Identity Manager as part of batch role resolution and role membership update timer processes. 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 or made inactive in Role Manager, there is a scheduled task to use to correct user groups in Identity Manager. This task can be enabled and configured in the same way as the user reconciliation tasks described in Section 7.1.

Note: The names of user groups in Identity Manager that correspond with roles in Role Manager by default begins with `ORM_`. This configurable naming helps administrators identify the user groups that are modified only in the Role Manager system. Any changes made to these user groups in Identity Manager could cause synchronization between the systems to fail. It is recommended not to change role names in Role Manager after initial reconciliation has occurred.

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

7.2.1 User Provisioning through Role/User Group Membership

The test in this section verifies that a user added as a member of a role in Role Manager is provisioned for the corresponding user group in Identity Manager.

To test role membership reconciliation:

1. If not currently running, start Identity Manager and then Role Manager.
2. Log in to the Identity Manager Administrative and User Console and search for the Telecom Provisioner user group as follows:
   a. Select **User Groups**, then select **Manage**.
   b. Select **Group Name** from the list, enter `ORM_T*` in the field, then click **Search**.
   c. Click **ORM_Telecom_Provisioner**.
   d. Select **Member and Sub-Groups** from the list.

      Note that no memberships exist for this role.
3. Log in to the Role Manager application and add an Identity Manager user to the Telecom Provisioner IT Role as follows:

a. Select **Organizations & People**, then select **People**.

b. For a new user created in "Testing User Reconciliation" on page 7-1, click the Details icon in the Actions column.

c. Click the **IT Roles** tab.

d. Click **Grant Role**.

e. Search for and select the **Telecom Provisioner** IT Role, then click **Finish**.

f. Click **Submit**.

4. Depending on the role membership update timer configuration in Role Manager, wait that amount of time until the role membership update job has completed.

   For more information about timer configuration repeat interval and cron job configuration, see *Oracle Role Manager Administrator's Guide*.

5. After the Role Manager role membership update job has run, search for and select the ORM_Telecom_Provisioner group in the Identity Manager Administrative and User Console.

   Note that the new membership now displays in the Member and Sub-Groups results.

7.2.2 User De-provisioning by Deleted or Inactivated Roles

The test in this section verifies that a role made inactive in Role Manager de-provisions membership in the corresponding user group in Identity Manager. It also tests that a new role created in Role Manager creates a user group in Identity Manager using batch role resolution and role membership updates.

To test role reconciliation and de-provisioning:

1. If not currently running, start Identity Manager and then Role Manager.
2. Using the Identity Manager Administrative and User Console, create a user.
3. Make an active role in Role Manager inactive as follows:

   a. Select **Roles**, then select **IT Roles**.

   b. Search for and select the Telecom Provisioner role, then click the Details icon in the Actions column.

   c. On the Attributes tab, change the status from Active to Inactive, then click **Submit**.

4. Create a Business Role in Role Manager as follows:

   a. Select **Roles**, then select **Business Roles**.

   b. In the tree view, right-click **Office of the CEO**, then select **New Business Role** from the context menu.

   c. In the **Display Name** field, enter `Test Business Role`.

   d. In the **Status** list, select **Active**.

   e. Click **Submit**.

5. Depending on the batch resolution timer configuration in Role Manager, wait that amount of time until the batch resolution job has completed.

   For more information about timer configuration repeat interval and cron job configuration, see *Oracle Role Manager Administrator's Guide*.

6. After the Role Manager role membership update job has run, search for and select the ORM_Telecom_Provisioner user group in the Identity Manager Administrative and User Console.
7. Select **Member and Sub-Groups** from the list.

   Note that no memberships exist for this role.
8. Search for the new Test Business Role user group.

   The new user group should display in the search results as "ORM_Test Business Role."

Note: The names of user groups in Identity Manager that correspond with roles in Role Manager by default begins with `ORM_`. This naming helps administrators identify the user groups that are modified only in the Role Manager system. Any changes made to these user groups in Identity Manager could cause synchronization between the system to fail.

7.3 Testing Approval Role Resolution

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

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

7.3.1 Role Manager Setup

The steps in this section are necessary to prepare 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 Role Manager that are referenced by processes in Identity Manager should have narrowly defined grant policies to reduce the number of returned records. 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 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. In the **Status** list, select **Active**.
5. 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 Role Manager who are also users in 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 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*.

6. On the Members tab, click **Recalculate**.

   You should see the user created in Section 7.1.1 whose name begins with *C* in the search results.

7. Click **Submit**.

7.3.2 Identity Manager Setup

The steps in this section set up the sample resources and approval process that was imported into Identity Manager so that the display values match those referenced in Section 7.3.3 that are more suitable for demonstration purposes.

To create an approval process:

1. Rename the sample resource as follows:

   a. In the Identity Manager Design Console (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.

2. 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.
3. Go back to the Oracle Financials resource object you created previously, then double-click the Table Name field to add UD_ORAFIN.
4. Click the Save icon.
5. 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.
6. 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.

7.3.3 Performing the test

The test in this section verifies that the approval process in Identity Manager uses the Approver Role from Role Manager to get an appropriate approver based on the role's grant policy.

To run the approver test:

1. Using the Identity Manager Administrative and User Console, assign the Oracle Financials resource to the user created in Section 7.1.1 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 7.1.1 and optionally any other users that you know also exist in the 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 user assigned to the Get Role Manager Approval Task to use in the next steps.

   This is the user who is automatically resolved as the resource approver after referencing the OIM Approver role in Role Manager.

8. Log out of the Administrative and User Console and log back in as the user 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.

8

Troubleshooting

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:

8.1 Log Files

The Integration Library messages are written to the `server.log.*` files in both the Oracle Role Manager (Role Manager) application server and the Oracle Identity Manager (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 WebLogic Server:

  WEBLOGIC_HOME`/user_projects/domains/domain_name/server_name/server_name.log`

8.2 Role Manager Application Server Console Errors

The following table describes error conditions that may appear in the application server console for Role Manager.

Problem Description	Solution
Returned Warning Message: WARN [OutgoingEventManagerImpl] Explicitly committed to a non-XA queue from within a transaction. Please check the configuration for the /oim/OIMserver/QueueConnectionFactory connection factory.	This can be ignored. This occurs when the application server on which Identity Manager is deployed is non-transactional, where Role Manager explicitly commits a transaction on initialization of the Role Manager connection factory to ensure messages are sent from Role Manager to Identity Manager.

8.3 Identity Manager Application Server Console Errors

The following table describes error conditions that may appear in the application server console for Identity Manager.

Problem Description	Solution
Returned Warning Message: WARN [IntegrationContext] General error utilizing plugin class	This can be ignored. It is caused by an intermittent race condition and causes no harm or loss of functionality.
Returned Error Message WARN [IntegrationContext] Truncating the ORM Role Name when creating a shadowing OIM Group was *xxxx*. Truncated to *yyyy*.	This occurs when the integration detects that the 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 Identity Manager user group name limit of thirty characters.
Returned Error Message javax.naming.NameNotFoundException: While trying to lookup 'connection factory'.	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.

A

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
0 0 12 * * ?	Fire at 12:00 PM (noon) every day
0 15 10 ? * *	Fire at 10:15 AM every day
0 15 10 * * ?	Fire at 10:15 AM every day
0 15 10 * * ? *	Fire at 10:15 AM every day
0 15 10 * * ? 2005	Fire at 10:15 AM every day during the year 2005
0 * 14 * * ?	Fire every minute starting at 2:00 PM and ending at 2:59 PM, every day
0 0/5 14 * * ?	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

J

K

L

M

O

P

Q

R

S

T

U

V

W

X