Oracle® Identity Manager

Connector Guide for Oracle Retail Warehouse Management System

Release 9.0.4

E10454-04

November 2010

ORACLE®

Oracle Identity Manager Connector Guide for Oracle Retail Warehouse Management System, Release 9.0.4

E10454-04

Primary Author: Alankrita Prakash

Contributing Authors: Debapriya Datta, Devanshi Mohan, Lyju Vadassery

Contents

3 Configuring Connector Functionality

4 Testing and Troubleshooting

5 Known Issues

A   Attribute Mappings Between Oracle Identity Manager and Oracle Retail Warehouse Management System

Index

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Oracle Retail Warehouse Management Systems.

Audience

This guide is intended for resource administrators and target system integration teams.

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.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts.*

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

http://www.oracle.com/technology/documentation/oim.html

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at

http://www.oracle.com/technology/documentation/index.html

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.

What's New in the Oracle Identity Manager Connector for Oracle Retail Warehouse Management?

This chapter provides an overview of the updates made to the software and documentation for the Oracle Retail Warehouse Management connector in release 9.0.4.12.

> **Note:** Release 9.0.4.12 of the connector comes after release 9.0.4.1. Release numbers from 9.0.4.2 through 9.0.4.11 have not been used.

The updates discussed in this chapter are divided into the following categories:

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

Software Updates

The following section discusses software updates:

- Software Updates in Release 9.0.4.12

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning
- Support for the Connector Installer
- Resolved Issues

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See the "Certified Components" section for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See the "Request-Based Provisioning" section for more information.

Support for the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See the "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1" section for more information.

Resolved Issues

The following is the issue resolved in release 9.0.4.12:

Bug Number	Issue	Resolution
10114704	The connector supported only the English language.	This issue has been resolved. The resource bundles for languages other than English have been included in the connector package. See the "Certified Languages" section of the connector guide for the list of all languages that the connector supports.

Documentation-Specific Updates

The following section discusses documentation-specific updates:

- Documentation-Specific Updates in Release 9.0.4.12

Documentation-Specific Updates in Release 9.0.4.12

The following are the documentation-specific updates in release 9.0.4.12:

- The following sections have been added:
  - Certified Components
  - Copying the External Code Files
  - Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1
- The "Verifying Deployment Requirements" section has been removed and the information in this section has been moved to the following sections:
  - Certified Components
  - Securing the JDBC Connection to the Target System Database
  - Copying the External Code Files

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. This guide discusses the procedure to deploy the connector that is used to integrate Oracle Identity Manager with Oracle Retail Warehouse Management System.

This chapter contains the following sections:

- Certified Components
- Certified Languages
- Reconciliation Module
- Provisioning Module
- Supported Functionality
- Certified Languages
- Files and Directories That Comprise the Connector
- Determining the Release Number of the Connector

> **Note:** In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.
>
> At some places in this guide, Oracle Retail Warehouse Management System has been referred to as the *target system.*

1.1 Certified Components

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager:
	■ Oracle Identity Manager release 9.0.1 through release 9.0.3.*x*
	■ Oracle Identity Manager release 9.1.0.1 or later
	Note: In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector will support.
	■ Oracle Identity Manager 11*g* release 1 (11.1.1)
	Note: In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1).
	The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at
	http://www.oracle.com/technetwork/documentation/oim1014-097544.html
Target systems	Oracle Retail Warehouse Management System release 12.0
Target system user account	An Oracle Database user account that has been granted the CONNECT and RESOURCE privileges to the Oracle Retail Warehouse Management System database by the system administrator .
	See the "Additional Privileges" section for information about additional privileges to be granted to the preceding user account.
JDK	The JDK version can be one of the following:
	■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x*, use JDK 1.4.2 or a later release in the 1.4.2 series.
	■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or a later release in the 1.5 series.
	■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.

Additional Privileges

The following table specifies the privileges that the user must have on some of the Oracle Retail Warehouse Management System tables:

Table Name	Select	Insert	Delete	Update
DMS_USER	Yes	Yes	Yes	Yes
FACILITY	Yes	No	No	No
SUPPORTED_LANGUAGE	Yes	No	No	No
DC_DEPARTMENT	Yes	No	No	No
USER_CLASS	Yes	No	No	No

1.2 Certified Languages

The connector supports the following languages:

- Chinese Simplified

- Chinese Traditional

- Danish

- English

- French

- German

- Italian

- Japanese

- Korean

- Portuguese (Brazilian)

- Spanish

> **See Also:**   One of the following guides for information about supported special characters:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*:
>
>   *Oracle Identity Manager Globalization Guide*
>
> - For Oracle Identity Manager release 11.1.1:
>
>   *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

1.3 Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. It is an automated process initiated by a scheduled task that you configure.

The reconciliation module handles the reconciliation of new, updated, and deleted user profiles in Oracle Identity Manager. A reconciliation event is created for each user profile to be reconciled.

> **See Also:**   One of the following guides for conceptual information about reconciliation configurations:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.x: *Oracle Identity Manager Connector Concepts Guide*
>
> - For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

Based on the type of data reconciled from the target system, reconciliation can be divided into the following types:

- Lookup Fields Reconciliation

- User Reconciliation

1.3.1 Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the following lookup fields:

- FacilityID
- LanguageCode
- Department
- UserClass

1.3.2 User Reconciliation

User reconciliation involves reconciling the following fields:

- FacilityID
- UserID
- Department
- UserName
- User Privilege
- User LogDate
- Language Code
- Picking Percent QA
- Packing Percent QA
- DCDept
- User Class
- Equipment

1.4 Provisioning Module

Provisioning involves creating or modifying a user's account on the target system through Oracle Identity Manager. You use the Oracle Identity Manager Administrative and User Console to perform provisioning operations.

> **See Also:** One of the following guides for conceptual information about provisioning:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.x: *Oracle Identity Manager Connector Concepts Guide*
> - For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

In provisioning, you can specify values for the following fields:

- FacilityID
- UserID
- UserName
- User Privilege
- Language Code

- Picking Percent QA

- Packing Percent QA

- DCDept

- User Class

- Equipment

- User Password

Provisioning of a user in Oracle Retail Warehouse Management System depends on the `FacilityID` value. During provisioning, depending on the value that you select from the `FacilityID` lookup field, you must select corresponding values from the `DCDept` and `UserClass` lookup fields.

For example:

Suppose you select `AY` as the `FacilityID` value. The description of this `FacilityID` value is `ANUSRINI Customer Support LR=Y`. Based on this description, you must select the following values in the `DCDept` and `UserClass` lookup fields:

DCDept:

```
ACCOUNTING (ANUSRINI Customer Support LR=Y)
```

UserClass:

```
DEFAULT (ANUSRINI Customer Support LR=Y)
```

> **Caution:** If you do not select corresponding values from the `DCDept` and `UserClass` lookup fields, then the provisioning operation would fail. However, Oracle Identity Manager does not display an error message if you do not select the correct `DCDept` and `UserClass` values.
>
> This point is also mentioned in the "Known Issues" chapter.

1.5 Supported Functionality

The following table lists the functions that are available with this connector.

Function	Type
Create User	Provisioning
Reset User's Password	Provisioning
Update User's Name	Provisioning
Update User's Privilege	Provisioning
Update User's Department	Provisioning
Update User's Language Code	Provisioning
Update User's Picking Percent QA	Provisioning
Update User's Packing Percent QA	Provisioning
Update User's User Class	Provisioning
Update User's Equipment	Provisioning
Delete User	Provisioning

Function	Type
Create User (Account Discovery)	Reconciliation
Update User's Name	Reconciliation
Update User's Department	Reconciliation
Update User's Language Code	Reconciliation
Update User's Picking Percent QA	Reconciliation
Update User's Packing Percent QA	Reconciliation
Update User's User Class	Reconciliation
Update User's Equipment	Reconciliation

1.6 Files and Directories That Comprise the Connector

The files and directories that comprise this connector are listed in Table 1–1.

Table 1–1   Files and Directories on the Installation Media

File in the Installation Media Directory	Description
config/attributemapping_prov.properties	This file contains the parameters required for provisioning.
config/attributemapping_recon.properties	This file contains the parameters required for reconciliation.
lib/rwmsadapter.jar	This JAR file contains the class files that are used to implement provisioning and reconciliation. During connector installation, this file is copied to the following location: ■ For an Oracle Identity Manager release from 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*, this file is copied to the following directories: *OIM_HOME*/xellerate/JavaTasks *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
Files in the dataset directory	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
File in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location: ■ For Oracle Identity Manager release 9.0.1 through release 9.0.3.*x* and release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
scripts/DB Schema XML/xdb_app_map.xsd	This XML file contains information about the validation rules to which the RWMS.xml file conforms.
scripts/RWMS.xml	This XML file contains the configuration information of Oracle Retail Warehouse Management System users.

Table 1–1   (Cont.) Files and Directories on the Installation Media

File in the Installation Media Directory	Description
scripts/RWMSTrigger/TriggerRWMS.sql	This file contains the SQL code for creating a temporary table and the trigger that is used to implement the reconciliation of user account deletion on the target system.
test/config/config.properties	This file is used to specify the parameters and settings required to connect to the target system by using the testing utility.
test/config/log.properties	This file is used for storing log information.
test/scripts/rwms.bat test/scripts/rwms.sh	This file is used to run the test utility.
xml/xlRWMSNonTrusted.xml	This file contains definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Resource object ■ Process form ■ Process definition ■ Process tasks ■ Adapters
xml/xlRWMSTrusted.xml	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector for trusted source reconciliation.

> **Note:**   The files in the test directory are used only to run tests on the connector.

The "Copying the Connector Files and External Code Files" section on page 2-6 provides instructions to copy these files into the required directories.

1.7 Determining the Release Number of the Connector

> **Note:**   If you are using Oracle Identity Manager release 9.0.1 through release 9.0.3.*x* and release 9.1.0.*x*, then the procedure described in this section is optional.
>
> If you are using Oracle Identity Manager release 11.1.1, then skip this section.

You can use the following method to determine the release number of the connector:

1. Extract the contents of the rwmsadapter.jar file. This file is in the following directory on the installation media:

    Enterprise Applications/Oracle Retail Applications/Oracle Retail Warehouse Mgmt

2. Open the manifest.mf file in a text editor. The manifest.mf file is one of the files bundled inside the rwmsadapter.jar file.

In the `manifest.mf` file, the release number of the connector is displayed as the value of the `Version` property.

2

Deploying the Connector

The following sections describe procedures involved in deploying the connector:

- Securing the JDBC Connection to the Target System Database
- Copying the External Code Files
- Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1
- Installing the Connector on Oracle Identity Manager Release 9.0.1 Through Release 9.0.3.x
- Configuring the Oracle Identity Manager Server
- Configuring the Target System

2.1 Securing the JDBC Connection to the Target System Database

> **Note:** It is recommended that you perform the procedure described in this section to secure the JDBC connection between the target system and Oracle Identity Manager.

You can establish secure JDBC connectivity with the target system database by adding the following parameters in the *ORACLE_HOME*/network/admin/sqlnet.ora file:

```
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER= (MD5)
SQLNET.AUTHENTICATION_SERVICES= (NTS)
SQLNET.ENCRYPTION_TYPES_SERVER= (DES40C)
SQLNET.CRYPTO_SEED = xelsysadmin_seed
```

2.2 Copying the External Code Files

Copy the xerces class file to one of the following directories:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

  OIM_HOME/xellerate/ThirdParty

- For Oracle Identity Manager release 11.1.1:

  OIM_HOME/server/ThirdParty

Include the xerces class file in the CLASSPATH environment variable.

Copy the JDBC class library (`ojdbc14.jar`) from the *ORACLE_HOME*/ora92/jdbc/lib/ directory on the Oracle Database host machine to one of the following directories:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

  OIM_HOME/xellerate/ThirdParty

- For Oracle Identity Manager release 11.1.1:

  OIM_HOME/server/ThirdParty

In this source directory path, *ORACLE_HOME* is the directory in which Oracle Database is installed. For example, `C:\Oracle`. The actual source directory path would depend on the release of Oracle Database that you are using.

Include the following file path in the `CLASSPATH` environment variable:

OIM_HOME/xellerate/ThirdParty/ojdbc14.jar

2.3 Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1

> **Note:** In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

Installing the connector on Oracle Identity Manager release 9.1.0.*x* or release 11.1.1 or later involves the following procedures:

- Running the Connector Installer
- Copying Files to the Oracle Identity Manager Host Computer
- Configuring the IT Resource

2.3.1 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

   > **Note:** In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

   - For Oracle Identity Manager release 9.1.0.*x*:
     OIM_HOME/xellerate/ConnectorDefaultDirectory
   - For Oracle Identity Manager release 11.1.1:
     OIM_HOME/server/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Oracle Identity Manager Administrative and User Console Guide

■ For Oracle Identity Manager release 11.1.1:

Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   ■ For Oracle Identity Manager release 9.1.0.*x*:

   Click **Deployment Management**, and then click **Install Connector**.

   ■ For Oracle Identity Manager release 11.1.1:

   On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.

4. From the Connector List list, select **Oracle Retail Warehouse Management System *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the Connector List list, select **Oracle Retail Warehouse Management System *RELEASE_NUMBER***.

5. Click **Load**.

6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see the "Configuring Trusted Source Reconciliation" section on page 3-1.

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   ■ Retry the installation by clicking **Retry.**

   ■ Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

> **Note:** At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See the "Clearing Content Related to Connector Resource Bundles from the Server Cache" section on page 2-8 for information about running the PurgeCache utility.
>
> There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

   Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks that are created when you installed the connector

> **Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

   Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 1–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Section 1.6, "Files and Directories That Comprise the Connector" for information about the files that you must copy and their destination locations on the Oracle Identity Manager host computer.

2.3.2 Copying Files to the Oracle Identity Manager Host Computer

After you run the Connector Installer, you must manually copy the files listed in Table 1–1.

> **Note:** If a particular destination directory does not exist on the Oracle Identity Manager host computer, then create it.

Table 2–1   Files to Be Copied to the Oracle Identity Manager Host Computer

Files on the Installation Media	Destination Directory on the Oracle Identity Manager Release 9.1.0.*x* Host Computer	Destination Directory on the Oracle Identity Manager Release 11.1.1 Host Computer
Files in the config directory	*OIM_HOME*/xellerate/XLIntegrations/RWMS/config	*OIM_HOME*/server/XLIntegrations/RWMS/config
Files in the test/config directory	*OIM_HOME*/xellerate/XLIntegrations/RWMS/config	*OIM_HOME*/server/XLIntegrations/RWMS/config
Files in the test/scripts directory	*OIM_HOME*/xellerate/XLIntegrations/RWMS/scripts	*OIM_HOME*/server/XLIntegrations/RWMS/scripts

2.3.3 Configuring the IT Resource

You must specify values for the parameters of the RWMS IT resource as follows:

1. Log in to the Administrative and User Console.

2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.

3. If you are using Oracle Identity Manager release 11.1.1, then:

   ■ On the Welcome page, click **Advanced** in the upper-right corner of the page.

   ■ On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.

4. In the IT Resource Name field on the Manage IT Resource page, enter RWMS and then click **Search**.

5. Click the edit icon for the IT resource.

6. From the list at the top of the page, select **Details and Parameters**.

7. Specify values for the parameters of the IT resource. Table 2–2 describes each parameter.

Table 2–2   IT Resource Parameters

Parameter	Description
Host	Host name or IP address of the Oracle Retail Warehouse Management System server
Port	TCP/IP port at which the Oracle Retail Warehouse Management System server is listening The default value is 0.
Admin	User ID to connect to the Oracle Retail Warehouse Management System database
Admin Credential	Password of the administrator
SID	SID for the Oracle Retail Warehouse Management System database
IsSecure	Specifies whether or not the SSL feature is enabled The value can be YES or NO. The default value is YES.
Schema Name	Name of the schema owner of the Oracle Retail Warehouse Management System

8. To save the values, click **Update**.

2.4 Installing the Connector on Oracle Identity Manager Release 9.0.1 Through Release 9.0.3.*x*

> **Note:** Perform the procedure described in this section only if you are installing the connector on any Oracle Identity Manager release from 9.0.1 through 9.0.3.*x*.

Installing the connector on an Oracle Identity Manager release from 9.0.1 through 9.0.3.*x* involves the following procedures:

- Copying the Connector Files and External Code Files
- Importing the Connector XML File

2.4.1 Copying the Connector Files and External Code Files

The connector files to be copied and the directories to which you must copy them are given in the following table.

> **See Also:** See the "Files and Directories That Comprise the Connector" section on page 1-6 for more information about these files.

File in the Installation Media Directory	Destination Directory
Files in the `config` directory	*OIM_HOME*/xellerate/XLIntegrations/RWMS/config
`lib/rwmsadapter.jar`	*OIM_HOME*/xellerate/JavaTasks *OIM_HOME*/xellerate/ScheduleTask
File in the `resources` directory	*OIM_HOME*/xellerate/connectorResources
`scripts/RWMS.xml`	*OIM_HOME*/xellerate/XLIntegrations/RWMS/Config
`scripts/DB Schema XML/xdb_app_map.xsd`	*OIM_HOME*/xellerate/XLIntegrations/RWMS
Files in the `scripts/RWMSTrigger` directory	*OIM_HOME*/xellerate/RWMSTrigger
Files in the `test/config` directory	*OIM_HOME*/xellerate/XLIntegrations/RWMS/config
Files in the `test/scripts` directory	*OIM_HOME*/xellerate/XLIntegrations/RWMS/scripts
`xml/xlRWMSNonTrusted.xml` `xml/xlRWMSTrusted.xml`	*OIM_HOME*/xlclient

> **Note:** While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the contents of the `connectorResources` directory and the JAR files to the corresponding directories on each node of the cluster.

2.4.2 Importing the Connector XML File

As mentioned in the "Files and Directories That Comprise the Connector" section on page 1-6, the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.

2. Click the **Deployment Management** link on the left navigation bar.

3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.

4. Locate and open the `xlRWMSNonTrusted.xml` file, which is in the `OIM_HOME\xlclient` directory. Details of this XML file are shown on the File Preview page.

5. Click **Add File.** The Substitutions page is displayed.

6. Click **Next**. The Confirmation page is displayed.

7. Click **Next.** The Provide IT Resource Instance Data page for the `RWMS` IT resource is displayed.

8. Specify values for the parameters of the IT resource. See the table in the "Configuring the IT Resource" section on page 2-5 for information about the values to be specified.

9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `RWMS` IT resource type is displayed.

10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

> **See Also:** If you want to define another IT resource, then refer to *Oracle Identity Manager Administrative and User Console Guide* for instructions.

11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You *may* see a cross-shaped icon along with some nodes. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.

12. Click **Import**. The connector XML file is imported into Oracle Identity Manager.

After you import the connector XML file, proceed to the next chapter.

2.5 Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

> **Note:** In a clustered environment, you must perform this step on each node of the cluster.

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging
- Configuring Oracle Identity Manager for Request-Based Provisioning

2.5.1 Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

You may require the assistance of the system administrator to change to the required input locale.

2.5.2 Clearing Content Related to Connector Resource Bundles from the Server Cache

> **Note:** In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME/*xellerate/connectorResources directory for Oracle Identity Manager release 9.0.3.*x* and release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then switch to the *OIM_HOME/*xellerate/bin directory.

   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME/*server/bin directory.

   > **Note:** You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:
   >
   > For Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*:
   >
   > `OIM_HOME/xellerate/bin/SCRIPT_FILE_NAME`
   >
   > For Oracle Identity Manager release 11.1.1:
   >
   > `OIM_HOME/server/bin/SCRIPT_FILE_NAME`

2. Enter one of the following commands:

> **Note:** You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *CATEGORY_NAME* on Microsoft Windows or `PurgeCache.sh` *CATEGORY_NAME* on UNIX. The *CATEGORY_NAME* argument represents the name of the content category that must be purged.
>
> For example, the following commands purge Metadata entries from the server cache:
>
> `PurgeCache.bat MetaData`
>
> `PurgeCache.sh MetaData`

- For Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*:

  On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`

  On UNIX: `PurgeCache.sh ConnectorResourceBundle`

  > **Note:** You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

  In this command, `ConnectorResourceBundle` is one of the content categories that you can delete from the server cache. See the following file for information about the other content categories:

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

  When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

  `t3://`*OIM_HOST_NAME*`:`*OIM_PORT_NUMBER*

  In this format:

  – Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.

  – Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.5.3 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform instructions in one of the following sections:

- Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.x or Release 9.1.0.x

- Enabling Logging on Oracle Identity Manager Release 11.1.1

2.5.3.1 Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.*x* or Release 9.1.0.*x*

> **Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- `ALL`

  This level enables logging for all events.

- `DEBUG`

  This level enables logging of information about fine-grained events that are useful for debugging.

- `INFO`

  This level enables logging of messages that highlight the progress of the application at a coarse-grained level.

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

  This level enables logging of information about error events that might allow the application to continue running.

- `FATAL`

  This level enables logging of information about very severe error events that could cause the application to stop functioning.

- `OFF`

  This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **IBM WebSphere Application Server**

  To enable logging:

  1. Add the following line in the
     OIM_HOME/xellerate/config/log.properties file:

     ```
     log4j.logger.RWMSAdapterLogger=log_level
     ```

  2. In this line, replace *log_level* with the log level that you want to set.

     For example:

     ```
     log4j.logger.RWMSAdapterLogger=INFO
     ```

  After you enable logging, log information is written to the following file:

  ```
  WEBSPHERE_HOME/AppServer/logs/server_name/startServer.log
  ```

■ **JBoss Application Server**

To enable logging:

1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, locate the following lines:

```
<category name="RWMSAdapterLogger">
    <priority value="log_level"/>
</category>
```

2. In the second XML code line, replace *log_level* with the log level that you want to set. For example:

```
<category name="RWMSAdapterLogger">
    <priority value="INFO"/>
</category>
```

After you enable logging, log information is written to the following file:

JBOSS_HOME/server/default/log/server.log

■ **Oracle Application Server**

To enable logging:

1. Add the following line in the
OIM_HOME/xellerate/config/log.properties file:

```
log4j.logger.RWMSAdapterLogger=log_level
```

2. In this line, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.RWMSAdapterLogger=INFO
```

After you enable logging, log information is written to the following file:

OAS_HOME/opmn/logs/default_group~home~default_group~1.log

■ **Oracle WebLogic Server**

To enable logging:

1. Add the following line in the
OIM_HOME/xellerate/config/log.properties file:

```
log4j.logger.RWMSAdapterLogger=log_level
```

2. In this line, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.RWMSAdapterLogger=INFO
```

After you enable logging, the log information is written to the following file:

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

2.5.3.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

> **Note:** In an Oracle Identity Manager cluster, perform this procedure
> on each node of the cluster. Then, restart each node.

Oracle Identity Manager release 11.1.1 uses Oracle Java Diagnostic Logging (OJDL) for
logging. OJDL is based on java.util.logger. To specify the type of event for which you
want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle
  Identity Manager to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

  This level enables logging of messages that highlight the progress of the
  application.

- CONFIG

  This level enables logging of information about fine-grained events that are useful
  for debugging.

- FINE, FINER, FINEST

  These levels enable logging of information about fine-grained events, where
  FINEST logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in
Table 2–3.

Table 2–3   Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name
specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

   ```
   <log_handler name='rwms-handler' level='[LOG_LEVEL]'
   class='oracle.core.ojdl.logging.ODLHandlerFactory'>
   <property name='logreader:' value='off'/>
        <property name='path' value='[FILE_NAME]'/>
        <property name='format' value='ODL-Text'/>
        <property name='useThreadName' value='true'/>
        <property name='locale' value='en'/>
        <property name='maxFileSize' value='5242880'/>
        <property name='maxLogSize' value='52428800'/>
        <property name='encoding' value='UTF-8'/>
     </log_handler>

   <logger name="RWMSAdapterLogger" level="[LOG_LEVEL]"
   useParentHandlers="false">
        <handler name="rwms-handler"/>
        <handler name="console-handler"/>
     </logger>
   ```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–3 lists the supported message type and level combinations.

   Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

   The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]**:

   ```
   <log_handler name='rwms-handler' level='NOTIFICATION:1'
   class='oracle.core.ojdl.logging.ODLHandlerFactory'>
   <property name='logreader:' value='off'/>
        <property name='path'
   value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
   im_server1\logs\oim_server1-diagnostic-1.log'/>
        <property name='format' value='ODL-Text'/>
        <property name='useThreadName' value='true'/>
        <property name='locale' value='en'/>
        <property name='maxFileSize' value='5242880'/>
        <property name='maxLogSize' value='52428800'/>
        <property name='encoding' value='UTF-8'/>
     </log_handler>

   <logger name="RWMSAdapterLogger" level="NOTIFICATION:1"
   useParentHandlers="false">
        <handler name="rwms-handler"/>
        <handler name="console-handler"/>
     </logger>
   ```

   With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

2. Save and close the file.

3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

Replace *FILENAME* with the location and name of the file to which you want to redirect the output.

4. Restart the application server.

2.5.4 Configuring Oracle Identity Manager for Request-Based Provisioning

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

> **Note:** Direct provisioning allows the provisioning of multiple target system accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- Copying Predefined Request Datasets
- Importing Request Datasets into MDS
- Enabling the Auto Save Form Feature
- Running the PurgeCache Utility

2.5.4.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following are the predefined request datasets available in the dataset directory on the installation media:

- ProvisionResource_RWMSRO.xml
- ModifyProvisionedResource_RWMSRO.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\ORWMS

> **Note:** Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide* for Oracle Identity Manager for information on modifying request datasets.

2.5.4.2 Importing Request Datasets into MDS

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

> **Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.5.4.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\ORWMS directory, then set the value of the metada_from_loc property to `E:\MyDatasets.`

2. In a command window, change to the *OIM_HOME*\server\bin directory.

3. Run one of the following commands:

   - On Microsoft Windows

     `weblogicImportMetadata.bat`

   - On UNIX

     `weblogicImportMetadata.sh`

4. When prompted, enter the following values:

   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

Enter the password used to log in to the WebLogic server.

- `Please enter your server URL [t3://localhost:7001]`

    Enter the URL of the application server in the following format:

    `t3://HOST_NAME_IP_ADDRESS:PORT`

    In this format, replace:

    – *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

    – *PORT* with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS.

2.5.4.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.

2. Expand **Process Management,** and then double-click **Process Definition.**

3. Search for and open the **RWMSProcess** process definition.

4. Select the **Auto Save Form** check box.

5. Click the Save icon.

2.5.4.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.5.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to configure request-based provisioning ends with this step.

2.6 Configuring the Target System

Configuring the target system involves the following steps:

1. Copy the `scripts/RWMSTrigger/TriggerRWMS.sql` file from the installation media directory to a temporary directory on the target system.

    Note: This file is mentioned in the "Files and Directories That Comprise the Connector" section on page 1-6.

    ---

2. Open the `TriggerRWMS.sql` file in a text editor, and change the following line in the file:

    `ALTER SESSION SET CURRENT_SCHEMA=<SchemaOwnerName>`

    In this line, replace `<SchemaOwnerName>` with the name of the schema owner of the Oracle Retail Warehouse Management System database tables.

3. Log in to the Oracle Retail Warehouse Management System database by using Oracle SQL*Plus.

4. At the SQL prompt, copy the SQL code from the `TriggerRWMS.sql` file.

5. Run the SQL code to create the table and trigger that is used to implement reconciliation of deleted user accounts.

3

Configuring Connector Functionality

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

- Configuring Reconciliation
- Configuring Provisioning
- Configuring the Connector for Multiple Installations of the Target System
- Provisioning Provisioning Operations
- Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

> **Note:** This chapter provides both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

3.1 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Configuring Trusted Source Reconciliation
- Partial Reconciliation
- Batched Reconciliation
- Configuring the Reconciliation Scheduled Tasks
- Adding Custom Attributes for Reconciliation

3.1.1 Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or a target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

> **Note:** You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

To configure trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.

2. Click the **Deployment Management** link on the left navigation bar.

3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.

4. Locate and open the `xlRWMSTrusted.xml` file, which is in the `OIM_HOME`/xlclient directory. Details of this XML file are shown on the File Preview page.

5. Click **Add File**. The Substitutions page is displayed.

6. Click **Next**. The Confirmation page is displayed.

7. Click **Import**.

8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

After you import the XML file for trusted source reconciliation, you must set the value of the `IsTrusted` reconciliation scheduled task attribute to `Yes`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-3.

3.1.2 Partial Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

Creating a filter involves specifying a value for a target system attribute, which will be used in the query SELECT criteria to retrieve the records to be reconciled. You can specify values for any one or a combination of the following target system attributes:

Filter Attribute	Oracle Identity Manager Attribute
FacilityID Sample value: `'AY'`	Facility ID
DCDept Sample value: `'Accounting'`	Department

If you want to use multiple target system attributes to filter records, then you must also specify the logical operator (AND or OR) that you want to apply to the combination of target system attributes that you select.

Suppose you specify the following values for these attributes:

- FacilityID: `AY`

- DCDept: `Accounting`

- Operator: `OR`

Because you are using the `OR` operator, during reconciliation, user records for which any one of these criteria is met are reconciled. Therefore, users with either `FacilityID` as `AY` or `DCDept` as `Accounting` are reconciled. If you were to use the `AND` operator, then only user records for which all of these criteria are met are reconciled.

While deploying the connector, follow the instructions in the "Specifying Values for the Scheduled Task Attributes" section on page 3-6 to specify values for these attributes and the logical operator that you want to apply.

3.1.3 Batched Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid these problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- `BatchSize`: Use this attribute to specify the number of records that must be included in each batch. The default value is 1000.

- `NumberOfBatches`: Use this attribute to specify the total number of batches that must be reconciled. The default value is `All`.

If you specify a value other than `All`, then some of the newly added or modified user records may not get modified during the current reconciliation run. The following example illustrates this:

Suppose you specify the following values while configuring the scheduled tasks:

- `BatchSize`: 20

- `NumberOfBatches`: 10

Suppose that 314 user records were created or modified after the last reconciliation run. Of these 314 records, only 200 records would be reconciled during the current reconciliation run. The remaining 114 records would be reconciled during the next reconciliation run.

You specify values for the `BatchSize` and `NumberOfBatches` attributes by following the instructions described in the "Specifying Values for the Scheduled Task Attributes" section on page 3-6.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Importing the Connector XML File" section on page 2-6, the scheduled tasks for lookup fields, trusted source user, and target resource user reconciliations are automatically created in Oracle Identity Manager.

Depending on the Oracle Identity Manager release that you are using, perform the procedure described in one of the following sections:

- Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.x

- Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1

3.1.4.1 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.*x*

To configure a scheduled task:

1. Open the Oracle Identity Manager Design Console.

2. Expand the **Xellerate Administration** folder.

3. Select **Task Scheduler.**

4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.

5. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the FAILED status to the task.

6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.

7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.

8. In the Interval region, set the following schedule parameters:

   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.

   - To set the task to run only once, select the **Once** option.

9. Provide values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 3-6 for information about the values to be specified.

   > **See Also:** *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes

10. Click **Save**. The scheduled task is created. The INACTIVE status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.

11. Repeat Steps 5 through 10 to configure the second scheduled task.

After you configure both scheduled tasks, proceed to the "Configuring Provisioning" section on page 3-10.

3.1.4.2 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.*x* or Release 11.1.1

To configure a scheduled task:

1. Log in to the Administrative and User Console.

2. Perform one of the following:

   a. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**

   b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.

3. Search for and open the scheduled task as follows:

- If you are using Oracle Identity Manager release 9.1.0.*x*, then:

  a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.

  b. In the search results table, click the edit icon in the Edit column for the scheduled task.

  c. On the Scheduled Task Details page where the details of the scheduled task that you selected is displayed, click **Edit**.

- If you are using Oracle Identity Manager release 11.1.1, then:

  a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

  b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

  c. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. Modify the details of the scheduled task. To do so:

   a. If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

      – **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

      – **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.

      – **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

      – **Frequency:** Specify the frequency at which you want the task to run.

   b. If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, you can modify the following parameters:

      – **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

      – **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

      Note: See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

      In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task. To do so:

> **Note:**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
>
> - Attributes of the scheduled task are discussed in the "Specifying Values for the Scheduled Task Attributes" section on page 3-6.

- If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

6. After specifying the attributes, perform one of the following:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

     > **Note:** The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

   - If you are using Oracle Identity Manager release 11.1.1, then click **Apply** to save the changes.

     > **Note:** The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

3.1.4.3 Specifying Values for the Scheduled Task Attributes

See the following sections for information about the attribute values to be specified for the scheduled tasks:

- Lookup Fields Reconciliation Scheduled Task

- User Reconciliation Scheduled Task

3.1.4.3.1 Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the lookup fields reconciliation scheduled task.

> **Note:** Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

Attribute	Description	Value
ServerName	Name of the IT resource	RWMS

Attribute	Description	Value
LookUpName	The type of data that is being looked up in the target system	The value can be any one of the following: ■ FacilityID ■ LanguageCode ■ Department ■ UserClass
LookUpCode	Name of the lookup definition configured in Oracle Identity Manager	The value can be any one of the following: ■ Lookup.RWMS.FacilityID ■ Lookup.RWMS.LanguageCode ■ Lookup.RWMS.Department ■ Lookup.RWMS.UserClass

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

3.1.4.3.2 User Reconciliation Scheduled Task Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled tasks:

■ RWMS User Reconciliation (Scheduled task for trusted source reconciliation)

■ RWMS User Reconciliation-Non Trusted (Scheduled task for target resource reconciliation)

The following table describes the attributes of both scheduled tasks.

> **Note:**
>
> ■ Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
>
> ■ Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Attribute	Description	Value
ServerName	Name of the IT resource	RWMS
IsTrusted	Specifies whether or not reconciliation is to be carried out in trusted mode	For the RWMS User Reconciliation scheduled task, the value of this attribute is set to Yes. For the RWMS User Reconciliation-Non Trusted scheduled task, the value of this attribute is set to No. This is the default value. **Caution:** For each scheduled task, you must not change the default value. If you change the default value, then the scheduled task would not run.
TargetRO	Name of the resource object	RWMSRO

Attribute	Description	Value
XellerateOrganisation	Default value for the Oracle Identity Manager Organization name This value is used to create the Xellerate User in trusted mode. **Note:** This attribute is specific to trusted source reconciliation.	Xellerate Users
BatchSize	Number of records in each batch that is reconciled You must specify an integer value greater than zero. **See Also:** The "Batched Reconciliation" section on page 3-3	The default value is 1000.
NoOfBatches	Number of batches to be reconciled The number of records in each batch is specified by the BatchSize attribute. **See Also:** The "Batched Reconciliation" section on page 3-3	Specify All if you want to reconcile all the batches. This is the default value. Specify an integer value if you want to reconcile only a fixed number of batches.
Facility ID	This is a filter attribute. Use this attribute to specify the Facility ID of the user whose records you want to reconcile. If you do not want to use this filter attribute, then specify Nodata. **See Also:** The "Partial Reconciliation" section on page 3-2	The value can be either the Facility ID or Nodata. The default value is Nodata. Sample value: AY
DCDept	This is a filter attribute. Use this attribute to specify the user DCDept for which you want to reconcile user records. If you do not want to use this filter attribute, then specify Nodata. **See Also:** The "Partial Reconciliation" section on page 3-2	The value can be either the DCDept or Nodata. The default value is Nodata. Sample value: Accounting
Operator	Specifies the logical operator to be applied to the filter attribute If you do not want to use this filter attribute, then specify None. **See Also:** The "Partial Reconciliation" section on page 3-2	The value can be one of the following: ■ AND ■ OR ■ None The default value is None.

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

3.1.5 Adding Custom Attributes for Reconciliation

By default, the attributes listed in the "Reconciliation Module" section on page 1-3 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for reconciliation as follows:

> **Note:** You need not perform this procedure if you do not want to add custom attributes for reconciliation.
>
> In this section, the term "attribute" refers to the identity data fields that store user data.

> **See Also:** *Oracle Identity Manager Design Console* for detailed instructions on performing the following steps

1. Modify the `attributemapping_recon.properties` file, which is in the `OIM_HOME`/`xellerate/XLIntegrations/RWMS/config` directory.

> **Note:** In this file, some of the attribute definitions are preceded by a comment saying that these attributes must not be changed. You must *not* change these attribute definitions.

At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to make it a part of the list of reconciliation attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

`OimAttributeName=TargetAttributeName`

For example:

`Users.LanguageCode=LANGUAGE_CODE`

In this example, `LanguageCode` is the reconciliation field and `LANGUAGE_CODE` is the equivalent target system attribute. As a standard, the prefix "`Users.`" is added at the start of all reconciliation field names.

2. In the resource object definition, add a reconciliation field corresponding to the new attribute as follows:

   a. Open the Resource Objects form. This form is in the Resource Management folder.

   b. Click **Query for Records**.

   c. On the Resource Objects Table tab, double-click the **RWMSRO** resource object to open it for editing.

   d. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.

   e. Specify a value for the field name.

   You must specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 2.

   For example, if you uncomment the `Users.LanguageCode=LANGUAGE_CODE` line in Step 2, then you must specify `Users.LanguageCode` as the attribute name.

   f. From the **Field Type** list, select a data type for the field.

   For example: `String`

   g. Save the values that you enter, and then close the dialog box.

     h. If required, repeat Steps d through g to map more fields.

3. Modify the process definition to include the mapping between the newly added attribute and the corresponding reconciliation field as follows:

     a. Open the Process Definition form. This form is in the Process Management folder.

     b. On the Reconciliation Field Mappings tab, click **Add Field Map** to open the Add Reconciliation Field Mapping dialog box.

     c. Enter the required values, save the values that you enter, and then close the dialog box.

     d. If required, repeat Steps b and c to map more fields.

3.2 Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. Refer to the "Supported Functionality" section on page 1-5 for a listing of the provisioning functions that are available with this connector.

This section discusses the following topics related to configuring provisioning:

- Compiling Adapters
- Adding Custom Attributes for Provisioning

3.2.1 Compiling Adapters

> **Note:** You must perform this procedure if you want to use the provisioning feature of the connector.

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

> **See Also:** The "Supported Functionality" section on page 1-5 for a listing of the provisioning functions that are available with this connector

- RWMSCreateUser
- RWMSUpdateUser
- RWMSDeleteUser
- RWMSResetPassword
- RWMSPrePopulate User Name

You must compile these adapters before they can be used in provisioning operations.

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.

2. To compile all the adapters that you import into the current database, select **Compile All**.

To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select **Compile Selected**.

> **Note:** Click **Compile Previously Failed** to recompile only those adapters that were not compiled successfully. Such adapters do not have an `OK` compilation status.

3. Click **Start**. Oracle Identity Manager compiles the selected adapters.

4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *OIM_HOME*/xellerate/Adapter directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

If you want to compile one adapter at a time, then use the Adapter Factory form.

> **See Also:** *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.

2. Double-click the row header of the adapter, or right-click the adapter.

3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

3.2.2 Adding Custom Attributes for Provisioning

> **Note:** In this section, the term "attribute" refers to the identity data fields that store user data.

By default, the attributes listed in the "Provisioning Module" section on page 1-4 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning as follows:

> **See Also:** One of the following guides:
>
> ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.x: *Oracle Identity Manager Design Console Guide*
>
> ■ For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

1. Modify the attributemapping_prov.properties file, which is in the *OIM_HOME*/xellerate/XLIntegrations/RWMS/config directory.

> **Note:** In this file, some of the attribute definitions are preceded by a comment saying that these attributes must not be changed. You must *not* change these attribute definitions.

At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to make it a part of the list of reconciliation attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

```
OimAttributeName=TargetAttributeName
```

For example:

```
LanguageCode=LANGUAGE_CODE
```

In this example, `LanguageCode` is the provisioning field and `LANGUAGE_CODE` is the target system field.

2. Add a new column in the process form.

   a. Open the process form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

   b. Click **Create New Version**.

   c. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.

   d. From the **Current Version** list, select the newly created version.

   e. On the Additional Columns tab, click **Add**.

   f. Specify the new field name and other values.

3. Add a new variable in the variable list.

   a. Open the Adapter Factory form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

   b. Click the **Query for Records** icon.

   c. On the Adapter Factory Table tab, double-click the **adpRWMSCreateUser** adapter from the list.

   d. On the Variable List tab, click **Add**.

   e. In the Add a Variable dialog box, specify the required values and then save and close the dialog box.

4. Define an additional adapter task for the newly added variable in the `adpRWMSCreateUser` adapter.

   a. On the Adapter Tasks tab of the Adapter Factory form, click **Add**.

   b. In the Adapter Task Selection dialog box, select **Functional Task**, select **Java** from the list of functional task types, and then click **Continue**.

   c. In the Object Instance Selection dialog box, select **Persistent Instance** and then click **Continue**.

   d. In the Add an Adapter Factory Task dialog box, specify the task name, select the **setProperty** method from the **Method** list, and then click **Save**.

   e. Map the application method parameters, and then save and close the dialog box. To map the application method parameters:

      For the "Output: String Return variable (Adapter Variable)" parameter:

      i. From the **Map to** list, select **Literal**.

      ii. From the **Name** list, select **Return variable**.

For the "Input: String input (Adapter Variable)" parameter:

i. From the **Map to** list, select **Adapter Variables**.

ii. From the **Name** list, select **Input**.

For the "Input: String Status (Literal)" parameter:

i. From the **Map to** list, select **Literal**.

ii. From the **Name** list, select **String**.

iii. In the **Value** field, enter **Status**.

For the "Input: String Status (Adapter Variable)" parameter:

i. From the **Map to** list, select **Adapter Variables**.

ii. From the **Name** list, select **Status**.

   f. Repeat Steps b through g to create more adapter tasks.

5. Create an additional adapter task to set the input variable.

   a. Open the Adapter Factory form. This form is in the Development Tools folder in the Oracle Identity Manager Design Console.

   b. On the Adapter Tasks tab, click **Add**.

   c. In the Adapter Task Selection dialog box, select **Logic Task**, select **SET VARIABLE** from the list, and then click **Continue**.

   d. In the Edit Set Variable Task Parameters dialog box, select **input** from the **Variable Name** list, select **Adapter Task** from the **Operand Type** list, and the Operand Qualifier as the Adapter Task that you have created in the previous step. Then, click **Save**.

6. Map the process form columns and adapter variables for the Create User process task as follows:

   a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.

   b. Click the **Query for Records** icon.

   c. On the Process Definition Table tab, double-click the **RWMSProcess** process.

   d. On the Tasks tab, double-click the **Create User** task.

   e. In the Closing Form dialog box, click **Yes**.

   f. On the Integration tab of the Editing Task Columns Create User dialog box, map the unmapped variables, and then save and close the dialog box. To map an unmapped variable:

i. Double-click the row in which **N** is displayed in the Status column. The value N signifies that the variable is not mapped.

ii. From the **Map to** list in the Edit Data Mapping for Variables dialog box, select **Process Data**.

iii. From the **Qualifier** list, select the name of the variable.

Repeat Steps i through iii for all unmapped variables.

Repeat Steps 1 through 6 if you want to add more attributes.

3.3 Configuring the Connector for Multiple Installations of the Target System

> **Note:** Perform this procedure only if you want to configure the connector for multiple installations of Oracle Retail Warehouse Management System.

You may want to configure the connector for multiple installations of Oracle Retail Warehouse Management System. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Example Multinational Inc. have their own installations of Oracle Retail Warehouse Management System. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of Oracle Retail Warehouse Management System.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of Oracle Retail Warehouse Management System.

To configure the connector for multiple installations of the target system:

> **See Also:** One of the following guides for detailed instructions on performing each step of this procedure:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide*
>
> - For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

1. Create and configure one IT resource for each set of Oracle Retail Warehouse Management System.

    The IT Resources form is in the Resource Management folder. The `RWMS` IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same IT resource type.

2. Configure reconciliation for each set of Oracle Retail Warehouse Management System. See the "Configuring Reconciliation" section on page 3-1 for instructions.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the Oracle Retail Warehouse Management System installation to which you want to provision the user.

3.4 Provisioning Provisioning Operations

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps

described in the "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1" section on page 3-18.

This following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

> **See Also:** *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- Direct Provisioning
- Request-Based Provisioning

3.4.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.

2. If you want to first create an OIM User and then provision a target system account, then:

   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:

     a. From the Users menu, select **Create**.

     b. On the Create User page, enter values for the OIM User fields and then click **Create User**.

   - If you are using Oracle Identity Manager release 11.1.1, then:

     a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.

     b. On the Create User page, enter values for the OIM User fields, and then click **Save**.

3. If you want to provision a target system account to an existing OIM User, then:

   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:

     a. From the Users menu, select **Manage**.

     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.

   - If you are using Oracle Identity Manager release 11.1.1, then:

     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.

     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.

4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:

      a. On the User Detail page, select **Resource Profile** from the list at the top of the page.

      b. On the Resource Profile page, click **Provision New Resource**.

- If you are using Oracle Identity Manager release 11.1.1, then:

      a. On the user details page, click the **Resources** tab.

      b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

5. On the Step 1: Select a Resource page, select **RWMSRO** from the list and then click **Continue**.

6. On the Step 2: Verify Resource Selection page, click **Continue**.

7. On the Step 5: Provide Process Data for ORWMS Table User Details page, enter the details of the account that you want to create on the target system and then click **Continue**.

8. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.

9. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:

- If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.

- If you are using Oracle Identity Manager release 11.1.1, then:

      a. Close the window displaying the "Provisioning has been initiated" message.

      b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.4.2 Request-Based Provisioning

> **Note:** The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

> **Note:** The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- End User's Role in Request-Based Provisioning

- Approver's Role in Request-Based Provisioning

3.4.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

> **See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.

2. On the Welcome page, click **Advanced** in the upper-right corner of the page.

3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.

4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.

5. From the Request Template list, select **Provision Resource** and click **Next**.

6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.

7. From the **Available Users** list, select the user to whom you want to provision the account..

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.

8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.

9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.

10. From the Available Resources list, select **RWMSRO**, move it to the Selected Resources list, and then click **Next**.

11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.

12. On the Justification page, you can specify values for the following fields, and then click **Finish**.

    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.

13. If you click the request ID, then the Request Details page is displayed.

14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.4.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.

2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.

3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.

4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.

5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

3.5 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

> **Note:**   It is assumed that you have performed the procedure described in the "Configuring Oracle Identity Manager for Request-Based Provisioning" section on page 2-14.

On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.

2. Disable the Auto Save Form feature as follows:

   a. Expand **Process Management**, and then double-click **Process Definition**.

   b. Search for and open the **RWMSProcess** process definition.

   c. Deselect the Auto Save Form check box.

   d. Click the Save icon.

3. If the Self Request Allowed feature is enabled, then:

   a. Expand **Resource Management**, and then double-click **Resource Objects**.

   b. Search for and open the **RWMSRO** resource object.

   c. Deselect the Self Request Allowed check box.

   d. Click the Save icon.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.

2. Enable the Auto Save Form feature as follows:

   a. Expand **Process Management**, and then double-click **Process Definition**.

   b. Search for and open the **RWMSProcess** process definition.

   c. Select the **Auto Save Form** check box.

   d. Click the Save icon.

3. If you want to enable end users to raise requests for themselves, then:

   a. Expand **Resource Management**, and then double-click **Resource Objects**.

   b. Search for and open the **RWMSRO** resource object.

   c. Select the Self Request Allowed check box.

d. Click the Save icon.

4

Testing and Troubleshooting

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

- Testing the Connector
- Troubleshooting Connector Problems

4.1 Testing the Connector

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

To use the testing utility:

1. Specify values for the parameters in the `config.properties` file.

   This file is in one of the following directories:

   - For Oracle Identity Manager release 9.1.0 through 9.0.3.*x* and release 9.1.0.*x*:

     OIM_HOME/xellerate/XLIntegrations/RWMS/config

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/XLIntegrations/RWMS/config

2. Run one of the following files:

   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, then run the following script:

     For UNIX:

     OIM_HOME/xellerate/XLIntegrations/scripts/rwms.sh

     For Microsoft Windows:

     OIM_HOME\xellerate\XLIntegrations\scripts\rwms.bat

   - If you are using Oracle Identity Manager release 11.1.1, then run the following script:

     For UNIX:

     OIM_HOME/server/XLIntegrations/scripts/rwms.sh

     For Microsoft Windows:

     OIM_HOME\server\XLIntegrations\scripts\rwms.bat

4.1.1 Testing Partial and Batched Reconciliation

You can test both partial and batched reconciliation, in either trusted source or target resource mode, by specifying values for the following user reconciliation attributes:

- BatchSize
- NoOfBatches
- FacilityID
- DCDept
- Operator

These attributes are described in the "User Reconciliation Scheduled Task" section on page 3-7.

The following is a sample set of values for these attributes:

- BatchSize: 4
- NoOfBatches: 2
- FacilityID: AY
- DCDept: Accounts
- Operator: AND

Suppose you specify these values in the target resource user reconciliation scheduled task. After that task is run, all target system records for which the FacilityID and DCDept values are AY and Accounts respectively, are divided into batches of four records each. Of these batches, the first two are reconciled during the current reconciliation run.

4.2 Troubleshooting Connector Problems

The following table lists solutions to some commonly encountered errors associated with the connector.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with the Oracle Retail Warehouse Management System server.	■ Ensure that the Oracle Retail Warehouse Management System server is running. ■ Ensure that Oracle Identity Manager is running. ■ Ensure that all the adapters have been compiled. ■ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that values for all the IT resource parameters have been correctly specified.
The Operation Failed message is displayed on the Oracle Identity Manager Administrative and User Console.	■ Ensure that the values for the various attributes do not contain delimiter characters (white space). ■ Ensure that the attribute values do not exceed the allowable length.

5

Known Issues

The following is a known issue associated with this release of the connector:

- Provisioning of a user in Oracle Retail Warehouse Management System depends on the `FacilityID` value. During provisioning, depending on the value that you select from the `FacilityID` lookup field, you must select corresponding values from the `DCDept` and `UserClass` lookup fields.

  If you do not select corresponding values from the `DCDept` and `UserClass` lookup fields, then the provisioning operation would fail. However, Oracle Identity Manager does not display an error message if you do not select the correct `DCDept` and `UserClass` values.

A

Attribute Mappings Between Oracle Identity Manager and Oracle Retail Warehouse Management System

The following table discusses attribute mappings between Oracle Identity Manager and Oracle Retail Warehouse Management System.

Oracle Identity Manager Attribute	Oracle Retail Warehouse Management System Attribute	Description
Facility ID	FACILITY_ID	Unique identifier for an operating facility
User ID	USER_ID	Unique identifier for a user of the WMS
User Name	USER_NAME	Name of a user of RDM
User Privilege	USER_PRIVILEGE	Privilege level for a user of WMS
User Password	USER_PASSWORD	User's password
Language Code	LANGUAGE_CODE	User's selected language
Picking Percent QA	PICKING_PERCENT_QA	Percentage at which QA is performed when this user performs picking
Packing Percent QA	PACKING_PERCENT_QA	Percentage at which QA is performed when this user performs packing
DC Dept	DC_DEPT	DC department name
User Class	USER_CLASS	User's User class
Equipment	EQUIPMENT	User's Equipment

Index