Oracle® Identity Manager

Connector Guide for Oracle E-Business User Management

Release 9.0.4

E10435-04

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for Oracle E-Business User Management, Release 9.0.4

E10435-04

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

Preface

This guide provides information about Oracle Identity Manager Connector for Oracle E-Business User Management.

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.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For 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 Oracle Identity Manager Connector for Oracle E-Business User Management?

This chapter provides an overview of the updates made to the software and documentation for the Oracle E-Business User Management connector in release 9.0.4.3.

> **See Also:** The earlier release of this guide for information about updates that were new for that release

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following sections discuss updates made from release 9.0.4 to the current release of the connector:

- Software Updates in Release 9.0.4.1_6728653
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3

Software Updates in Release 9.0.4.1_6728653

The following are software updates in release 9.0.4.1_6728653:

- Script to Create the Target System Account for Connector Operations
- Resolved Issues in Release 9.0.4.1_6728653

Script to Create the Target System Account for Connector Operations

Instead of using the `apps` target system account for connector operations, you can now use scripts provided in the connector installation package to create an account and assign the minimum required privileges to the account.

See "Configuring the Target System" on page 2-2 for more information.

Resolved Issues in Release 9.0.4.1_6728653

The following are issues resolved in release 9.0.4.1_6728653:

Bug Number	Issue	Resolution
6006892 and 6656960	You had to use the APPS User with full privileges for connector operations.	You can now create a target system account for connector operations with the required privileges. Scripts have been provided in the connector installation package for creating this target system account. See "Configuring the Target System" on page 2-2 for more information.
6597512	If you used release 11.5.10 of the target system with Oracle Database 10*g*, then the following exception was thrown during Update User provisioning operations: `Unable to call fnd_ldap_wrapper.create_user since database upgraded to 10g from 9i.`	This issue has been resolved. You can now use any combination of the supported target system and database releases.
6436324	The connector did not support the Change User Name provisioning operation.	This issue has been resolved. The connector now supports the Change User Name provisioning operation.
6686927	Names of some of the connector objects were not clear.	This issue has been resolved. Where required, names of the connector objects have been modified.
6666957	When you performed an Enable User provisioning operation, the Start Date of the user of user account on the target system is set to the current date and the end date is set to NULL. When you performed a Disable User operation, the Start Date of the user of user account on the target system remains the same and the end date is set to the current date. This is expected behavior. However, the Start Date and End Date values on Oracle Identity Manager itself do not reflect the changes made on the target system.	This issue has been resolved. During an Enable or Disable User provisioning operation, the Start Date and End Date on Oracle Identity Manager reflect the changes made on the target system.

Bug Number	Issue	Resolution
6337981	The Password Expiration field of the target system is mapped to the Lifespan Type field of Oracle Identity Manager. During a Create User provisioning operation, the Lifespan Type field is set to `None`. During an Update User provisioning operation, the value of the Password Expiration field set to the Access option automatically changed to `0` (zero). This happened even when the value of the Lifespan Type field remained `None` on Oracle Identity Manager.	This issue has been resolved. If the Lifespan Type field is set to `None`, then the Password Expiration field is also set to `None`.

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- Using the Connector Installer
- Support for New Languages
- Resolved Issues in Release 9.0.4.2

Using 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 "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-3 for details.

Support for New Languages

The following languages have been added to the list of supported languages:

- Arabic
- Japanese

See "Multilanguage Support" on page 1-4 for more information.

Resolved Issues in Release 9.0.4.2

The following are issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
7271848	If you changed the user password during a provisioning operation, then the password field on the target system was updated but the password_date field on the target system was not set to the system date.	This problem has been resolved. When you change the user password during a provisioning operation, the password_date field is set to the system date of the target system.

Software Updates in Release 9.0.4.3

The following are issues resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
7175655	During a provisioning operation, the password field was automatically updated if you updated any of the other process form fields.	This issue has been resolved. The password field is not automatically updated when you update any other process form field.

Documentation-Specific Updates

The following documentation-specific updates have been made in this release of the guide:

- The "Target System Stored Procedures Used During Provisioning" section on page 1-3 has been added.
- In the "Known Issues" chapter, the following point has been added:

  "This release of the connector does not support the addition of custom child table attributes for provisioning."
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target system" row.

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 E-Business User Management.

This chapter contains the following sections:

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 E-Business User Management has been referred to as the *target system.*

1.1 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.

See Also: The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Concepts Guide* for conceptual information about reconciliation configurations

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

1.1.1 Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the Responsibility lookup field.

1.1.2 User Reconciliation

User reconciliation involves reconciling the following fields:

1.1.2.1 Reconciled Resource Object Fields

The following target system fields are reconciled:

- User ID
- username
- E-mail
- Desc
- lifeSpanType
- lifeSpanValue
- startDate
- endDate
- employeeId
- respName
- respStartDate
- respEndDate

1.1.2.2 Reconciled Xellerate User (OIM User) Fields

The following target system fields are reconciled only if trusted source reconciliation is implemented:

- User ID
- First Name
- Last Name
- Organization
- User Type
- Employee Type

1.2 Provisioning Module

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

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Concepts Guide* for conceptual information about provisioning

For this target system, the following fields are provisioned:

- User ID (read-only)
- userName
- password

- confPassword
- lifeSpanType
- lifeSpanValue
- startDate
- endDate
- email
- employeeId
- description
- respName
- respStartDate
- respEndDate

Note: During provisioning, if you want to link a newly created user account with an employee account, then you must ensure that the `OracleHR.Employees` lookup field is populated. For this, you must install the Oracle E-Business Employee Reconciliation connector and reconcile employee data.

If you do not want to link a newly created user account with an employee account, then the `OracleHR.Employees` lookup field is not required.

Target System Stored Procedures Used During Provisioning

The following target system stored procedures are used for provisioning operations:

- fnd_global.APPS_INITIALIZE
- FND_USER_PKG.CreateUser
- FND_USER_PKG.UpdateUser
- FND_USER_PKG.DisableUser
- FND_USER_PKG.EnableUser
- FND_USER_PKG.AddResp
- FND_USER_PKG.DelResp
- FND_USER_PKG.change_user_name

1.3 Supported Functionality

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

Function	Type	Description
Create User	Provisioning	Creates a user
Disable User	Provisioning	Disables a user When this function is run, the end date assigned to the user account is changed to the current date.
Email Updated	Provisioning	Updates the e-mail address of a user

Function	Type	Description
Password Updated	Provisioning	Updates the password of a user
Description Updated	Provisioning	Updates the description of a user
Start Date Updated	Provisioning	Updates the start date of a user's account validity period
End Date Updated	Provisioning	Updates the end date of a user's account validity period
LifeSpan Type Updated	Provisioning	Updates the Life Span type of a user
LifeSpan Updated	Provisioning	Updates the Life Span value of a user
Enable User	Provisioning	Enables a user so that the user is able to log in to Oracle E-Business User Management When this function is run on a disabled user account, the end date of the user account is changed to a null value.
Add Responsibility	Provisioning	Adds a responsibility to a user
Remove Responsibility	Provisioning	Removes a responsibility from a user When this function is run, the end date of the responsibility allocation is changed to the current date.
Update user name	Provisioning	Updates the user name of a user.
Employee Id Updated	Provisioning	Updates the employee ID of a user
Update Xellerate User (OIM User)	Reconciliation	Updates an Oracle Identity Manager user with data received from Oracle E-Business User Management
Update Apps Resource	Reconciliation	Updates an Oracle Identity Manager resource with data received from Oracle E-Business User Management
Create Link with Oracle HR Employee	Reconciliation	Sets the employee ID of an Xellerate User (OIM User) to the corresponding Oracle E-Business User Management user

See Also: Appendix A for information about attribute mappings between Oracle Identity Manager and Oracle E-Business User Management

1.4 Multilanguage Support

The connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)

- Spanish

See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

1.5 Files and Directories on the Installation Media

The files and directories on the installation media are listed and described in Table 1–1.

Table 1–1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
`configuration/Oracle EBS User Management-CI.xml`	This XML file contains configuration information that is used during connector installation.
`config/attributemapping_prov.properties`	This file contains the dynamic attributes required for provisioning.
`config/attributemapping_recon.properties`	This file contains the dynamic attributes required for reconciliation.
`config/storedprocedures.properties`	This files contains the information regarding the stored procedures and various parameters that are used at the time of provisioning.
`lib/xlHostAccess.jar`	This file contains the class files that are required for provisioning. During connector deployment, this file is copied into the following directories: *OIM_HOME*`/xellerate/JavaTasks`
`lib/xlReconOracleApps.jar`	This file contains the class files that are required for reconciliation. During connector deployment, this file is copied into the following directories: *OIM_HOME*`/xellerate/ScheduleTask`
Files in the `resources` directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied into the following directories: *OIM_HOME*`/xellerate/connectorResources` **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
`scripts/OimUserSynonyms.sql`	This file contains commands to create synonyms for the OIM wrapper and various tables used in the target system schema for reconciliation.
`scripts/OimUserGrants.sql`	This file contains commands to provide the required grants to the target system account that is used for connector operations.
`scripts/OimUser.sql`	This file contains commands to create and configure the target system account that is used for connector operations.
`scripts/OIM_FND_USER_PKG.pck`	This file contains the package declaration and body for the OIM wrapper for FND_USER_PKG.
`scripts/OIM_FND_GLOBAL.pck`	This file contains the package declaration and body for the OIM wrapper for FND_GLOBAL.
`scripts/OIM.sh` `scripts/OIM.bat`	This script contains commands to call the SQL files in the `scripts` directory.

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

File in the Installation Media Directory	Description
`test/config/config.properties`	This file contains the parameters required to connect to and perform provisioning on the target system.
`test/config/log.properties`	This file is used for storing log information.
`test/scripts/OracleEbiz.bat` `test/scripts/OracleEbiz.sh`	This file is used to start the testing utility.
`xml/oracleAppsResAdp.xml`	This file contains definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Process form ■ Process tasks and adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Scheduled tasks for lookup fields and user reconciliation
`xml/XellUserOraApps.xml`	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

File in the Installation Media Directory	Description
`configuration/Oracle EBS User Management-CI.xml`	This XML file contains configuration information that is used during connector installation.
`config/attributemapping_prov.properties`	This file contains the dynamic attributes required for provisioning.
`config/attributemapping_recon.properties`	This file contains the dynamic attributes required for reconciliation.
`config/storedprocedures.properties`	This files contains the information regarding the stored procedures and various parameters that are used at the time of provisioning.
`lib/xlHostAccess.jar`	This file contains the class files that are required for provisioning. During connector deployment, this file is copied into the following directories: *OIM_HOME*`/xellerate/JavaTasks`
`lib/xlReconOracleApps.jar`	This file contains the class files that are required for reconciliation. During connector deployment, this file is copied into the following directories: *OIM_HOME*`/xellerate/ScheduleTask`
Files in the `resources` directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied into the following directories: *OIM_HOME*`/xellerate/connectorResources` **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.

File in the Installation Media Directory	Description
scripts/OimUserSynonyms.sql	This file contains commands to create synonyms for the OIM wrapper and various tables used in the target system schema for reconciliation.
scripts/OimUserGrants.sql	This file contains commands to provide the required grants to the target system account that is used for connector operations.
scripts/OimUser.sql	This file contains commands to create and configure the target system account that is used for connector operations.
scripts/OIM_FND_USER_PKG.pck	This file contains the package declaration and body for the OIM wrapper for FND_USER_PKG.
scripts/OIM_FND_GLOBAL.pck	This file contains the package declaration and body for the OIM wrapper for FND_GLOBAL.
scripts/OIM.sh scripts/OIM.bat	This script contains commands to call the SQL files in the scripts directory.
test/config/config.properties	This file contains the parameters required to connect to and perform provisioning on the target system.
test/config/log.properties	This file is used for storing log information.
test/scripts/OracleEbiz.bat test/scripts/OracleEbiz.sh	This file is used to start the testing utility.
xml/oracleAppsResAdp.xml	This file contains definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Process form ■ Process tasks and adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Scheduled tasks for lookup fields and user reconciliation
xml/XellUserOraApps.xml	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

1.6 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME/xellerate/ScheduleTask/xlReconOracleApps.jar

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

Deploying the connector involves the following steps:

- Verifying Deployment Requirements
- Using External Code Files
- Configuring the Target System
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
  - Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later
  - Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x
- Configuring the Oracle Identity Manager Server

2.1 Verifying Deployment Requirements

The following table lists the deployment requirements for the connector:

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target system	Oracle E-Business Suite 11.5.10, 12.0.*x*
External code	JDBC class library (`classes12.jar/ojdbc14.jar`) Refer to the "Copying the Connector Files" section on page 2-7 for information about the location of this file.
Target system user account	APPS system user with the required privileges You provide the credentials of this user account while configuring the IT resource. The procedure to configure the IT resource is described later in this guide. See "Configuring the Target System" on page 2-2 for information about the procedure to create the APPS system user account. In this guide, this user account is also referred to as the target system account for connector operations.

2.2 Using External Code Files

If the connector is used with Oracle8*i* Database, then the required external code file is `classes12.jar`.

If the connector is used with Oracle9*i* Database or Oracle Database 10*g*, then you can use either `ojdbc14.jar` or `classes12.jar`.

These JAR files are available in the Oracle Database installation at, for example, the following path:

ORACLE_HOME/jdbc/lib

In this directory path, *ORACLE_HOME* is the location where Oracle Database is installed. For example, C:\Oracle\ora92.

You must copy the required JAR file (classes12.jar or ojdbc14.jar) into the *ORACLE_HOME*/xellerate/ThirdParty directory.

2.3 Configuring the Target System

The connector uses a target system account to connect to the target system during reconciliation. You can use the script provided in the scripts directory on the installation media to create this account.

To create the target system user account for connector operations:

1. Copy the scripts directory from the installation media to a temporary directory on either the target system server or to a computer on which the Oracle Database client has been installed.
2. On the computer where you copy the scripts directory, verify that there is a TNS Entry in the tnsnames.ora file for the target system database.
3. Depending on the host platform, run either the OIM.sh or OIM.bat file.
4. When you run the script, you are prompted for the following information:
   - ORACLE_HOME path

     This prompt is displayed only if the ORACLE_HOME environment variable has not been set on the computer on which you are running the script.
   - Enter the system user name

     Enter the login (user name) of a DBA account with the privileges to create and configure a new target system user.
   - Enter the name of the database

     Enter the connection string or service name given in the tnsnames.ora file to connect to the target system database.
   - Enter password

     Enter the password of the DBA account whose login you enter earlier.
   - Details of the target system account that you want to create

     Enter a user name and password for the target system account that you want to create.
   - Connecting with APPS User

     Enter the password of the APPS User that can grant the required privileges to the target system account that you want to create.
   - Connecting with newly created database user

     Enter the connection string or service name that you provided earlier.

During the account creation process, the following privileges are granted to the account:

Note: The `OimUserGrants.sql` file contains commands to grant these permissions.

- select on applsys.fnd_application
- select on applsys.fnd_responsibility
- select on applsys.fnd_responsibility_tl
- select, update on applsys.fnd_user
- select on apps.fnd_responsibility_vl
- select on apps.fnd_user_resp_groups_direct
- execute on APPS.FND_USER_PKG
- execute on APPS.OIM_FND_USER_PKG
- execute on APPS.fnd_global
- execute on APPS.OIM_FND_GLOBAL
- create session
- create synonym
- create table
- drop any table

At the end of the operation, a log file (`OIM_APPS_USER.log`) is created in the `scripts` directory. If no error messages are recorded in the log file, then the account has been created successfully.

2.4 Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later

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 or later involves the following procedures:

- Running the Connector Installer
- Configuring the IT Resource

2.4.1 Running the Connector Installer

To run the Connector Installer:

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

   OIM_HOME`/xellerate/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 *Oracle Identity Manager Administrative and User Console*.

3. Click **Deployment Management**, and then click **Install Connector**.
4. From the Connector List list, select **Oracle EBS User Management 9.0.4.3**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

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

   a. In the **Alternative Directory** field, enter the full path and name of that directory.
   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
   c. From the Connector List list, select **Oracle EBS User Management 9.0.4.3**.
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 "Configuring the Target System As a Trusted Source" on page 3-3.
   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 `PurgeCache` utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-10 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

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

8. Copy the files in the config directory on the installation media to the *OIM_HOME*/xellerate/XLIntegrations/OracleEBiz/config directory.

Note: 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 clustered environment, 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 "Files and Directories on the Installation Media" on page 1-5 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.4.2 Configuring the IT Resource

Note: Perform this procedure if you are installing the connector on Oracle Identity Manager release 9.1.0 or later.

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

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter EBS_ITR 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. The following table describes each parameter:

Parameter	Description
Admin	User ID to connect to the target system database The default value is apps. **See Also:** "Configuring the Target System" on page 2-2 for information about creating this account and assigning the required privileges to it
AdminCredentials	Password of the administrator
Host	Host name or IP address of the Oracle E-Business User Management server
Port	TCP/IP port at which the Oracle E-Business User Management server is listening. The default value is 1521.
SID	SID for the Oracle E-Business User Management server

Parameter	Description
TrustedTimeStamp	This parameter is used for trusted source reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is 0. The time-stamp value that this parameter accepts is of the LONG data type, which stores the date and time value in milliseconds. You can determine the LONG data type equivalent of the required time-stamp value by using a SQL query. For example, to determine the TimeStamp parameter value for the date 31-Jan-2006, run the following SQL query: `SELECT ROUND((TO_DATE('31012006','ddmmyyyy') - TO_DATE('01011970', 'ddmmyyyy')) * 1440 * 60 * 1000) FROM dual;` When you specify the output of this query as the value of the TimeStamp parameter, all records that are created or updated after 31-Jan-2006 are reconciled during the next reconciliation run.
NonTrustedTimeStamp	This parameter is used for target resource reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is 0. The time-stamp value that this parameter accepts is of the LONG data type, which stores the date and time value in milliseconds. You can determine the LONG data type equivalent of the required time-stamp value by using a SQL query. For example, to determine the TimeStamp parameter value for the date 31-Jan-2006, run the following SQL query: `SELECT ROUND((TO_DATE('31012006','ddmmyyyy') - TO_DATE('01011970', 'ddmmyyyy')) * 1440 * 60 * 1000) FROM dual;` When you specify the output of this query as the value of the TimeStamp parameter, all records that are created or updated after 31-Jan-2006 are reconciled during the next reconciliation run.
ResetPswdOnFirstLogon	Specifies whether or not users are to be prompted to change their passwords at first logon The value can be Yes or No. The default value is Yes.
isSecure	This parameter is meant for use in a future release of the connector. The default value is No. Do not change the default value.
UserID	The User ID number This parameter is used when the fnd_global.APPS_INITIALIZE package is run. See "Target System Stored Procedures Used During Provisioning" for the full list of packages. The default value is 0.
RespID	The ID number of the responsibility. This parameter is used when the fnd_global.APPS_INITIALIZE package is run. See "Target System Stored Procedures Used During Provisioning" for the full list of packages. The default value is 0.

Parameter	Description
RespAppID	The ID number of the application to which the responsibility belongs. This parameter is used when the fnd_global.APPS_INITIALIZE package is run. See "Target System Stored Procedures Used During Provisioning" for the full list of packages. The default value is 0.

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

2.5 Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x

Installing the connector on any Oracle Identity Manager release between releases 8.5.3.1 and 9.0.3.x involves the following procedures:

- Copying the Connector Files
- Importing the Connector XML File

2.5.1 Copying the Connector Files

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

See Also: "Files and Directories on the Installation Media" section on page 1-5 for more information about these files

File in the Installation Media Directory	Destination Directory
Files in the config directory	*OIM_HOME*/xellerate/XLIntegrations/OracleEBiz/config
lib/xlHostAccess.jar	*OIM_HOME*/xellerate/JavaTasks
lib/xlReconOracleApps.jar	*OIM_HOME*/xellerate/ScheduleTask
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources
Files in the xml directory	*OIM_HOME*/xellerate/XLIntegrations/OracleEBiz/xml
Files in the test/config directory	*OIM_HOME*/xellerate/XLIntegrations/OracleEBiz/config
Files in the test/scripts directory	*OIM_HOME*/xellerate/XLIntegrations/OracleEBiz/scripts

Note: In a clustered environment, copy the JAR files and the contents of the connectorResources directory to the corresponding directories on each node of the cluster.

2.5.2 Importing the Connector XML File

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 `OracleAppsResAdp.xml` file, which is in the *`OIM_HOME`*`/xellerate/XLIntegrations/OracleEBiz/xml` 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 `EBS_ITR` IT resource is displayed.
8. Specify values for the parameters of the `EBS_ITR` IT resource. Refer to the following table for information about the values to be specified:

Parameter	Description
`Admin`	User ID to connect to the target system database The default value is `apps`. **See Also:** "Configuring the Target System" on page 2-2 for information about creating this account and assigning the required privileges to it
`AdminCredentials`	Password of the administrator
`Host`	Host name or IP address of the Oracle E-Business User Management server
`Port`	TCP/IP port at which the Oracle E-Business User Management server is listening. The default value is `1521`.
`SID`	SID for the Oracle E-Business User Management server
`TrustedTimeStamp`	This parameter is used for trusted source reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is `0`. The time-stamp value that this parameter accepts is of the LONG data type, which stores the date and time value in milliseconds. You can determine the LONG data type equivalent of the required time-stamp value by using a SQL query. For example, to determine the `TimeStamp` parameter value for the date 31-Jan-2006, run the following SQL query: `SELECT ROUND((TO_DATE('31012006','ddmmyyyy') - TO_DATE('01011970', 'ddmmyyyy')) * 1440 * 60 * 1000) FROM dual;` When you specify the output of this query as the value of the `TimeStamp` parameter, all records that are created or updated after 31-Jan-2006 are reconciled during the next reconciliation run.

Parameter	Description
NonTrustedTimeStamp	This parameter is used for target resource reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is 0. The time-stamp value that this parameter accepts is of the LONG data type, which stores the date and time value in milliseconds. You can determine the LONG data type equivalent of the required time-stamp value by using a SQL query. For example, to determine the TimeStamp parameter value for the date 31-Jan-2006, run the following SQL query: `SELECT ROUND((TO_DATE('31012006','ddmmyyyy') - TO_DATE('01011970', 'ddmmyyyy')) * 1440 * 60 * 1000) FROM dual;` When you specify the output of this query as the value of the TimeStamp parameter, all records that are created or updated after 31-Jan-2006 are reconciled during the next reconciliation run.
ResetPswdOnFirstLogon	Specifies whether or not users are to be prompted to change their passwords at first logon The value can be Yes or No. The default value is Yes.
isSecure	This parameter is meant for use in a future release of the connector. The default value is No. Do not change the default value.
UserID	The User ID number This parameter is used when the fnd_global.APPS_INITIALIZE package is run. See "Target System Stored Procedures Used During Provisioning" for the full list of packages. The default value is 0.
RespID	The ID number of the responsibility. This parameter is used when the fnd_global.APPS_INITIALIZE package is run. See "Target System Stored Procedures Used During Provisioning" for the full list of packages. The default value is 0.
RespAppID	The ID number of the application to which the responsibility belongs. This parameter is used when the fnd_global.APPS_INITIALIZE package is run. See "Target System Stored Procedures Used During Provisioning" for the full list of packages. The default value is 0.

9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the ORACLE 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.

2.6 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

2.6.1 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.

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

While performing the instructions described in the "Copying the Connector Files" section on page 2-7, you copy files from the `resources` directory on the installation media into the *`OIM_HOME`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in 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, change to the *`OIM_HOME`*`/xellerate/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:

   `OIM_HOME``\xellerate\bin\`*`batch_file_name`*

2. Enter one of the following commands:

   - 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.

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

OIM_HOME/xellerate/config/xlConfig.xml

2.6.3 Enabling Logging

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 may 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 depends on the application server that you use:

- **BEA WebLogic Server**

  To enable logging:

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

     log4j.logger.ADAPTER.ORACLE-EBIZUM=*log_level*

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

     For example:

     log4j.logger.ADAPTER.ORACLE-EBIZUM=INFO

After you enable logging, log information is displayed on the server console.

- **IBM WebSphere Application Server**

  To enable logging:

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

     ```
     log4j.logger.ADAPTER.ORACLE-EBIZUM=log_level
     ```

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

     For example:

     ```
     log4j.logger.ADAPTER.ORACLE-EBIZUM=INFO
     ```

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

  WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/SystemOut.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBoss_home*/server/default/conf/log4j.xml file, add the following lines if they are not already present in the file:

     ```
     <category name="ADAPTER.ORACLE-EBIZUM">
        <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="ADAPTER.ORACLE-EBIZUM">
        <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.ADAPTER.ORACLE-EBIZUM=log_level
     ```

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

     For example:

     ```
     log4j.logger.ADAPTER.ORACLE-EBIZUM=INFO
     ```

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

  OC4J_home/opmn/logs/default_group~home~default_group~1.log

3

Configuring the Connector

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

> **Note:** These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- Configuring Reconciliation
- Configuring Provisioning

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:

- Partial Reconciliation
- Batched Reconciliation
- Configuring the Target System As a Trusted Source
- Configuring the Reconciliation Scheduled Tasks
- Adding Custom Attributes for Reconciliation

3.1.1 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:

- UserName
- EmployeeID

- StartDate

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:

- UserName: `jdoe`
- EmployeeID: `1524`
- StartDate: `2006/10/19`
- Operator: `OR`

Because you are using the `OR` operator, during reconciliation, user records for which *any one* of these criteria is met are reconciled. If you were to use the `AND` operator, then only user records for which *all* of these criteria are met are reconciled.

You can also use a combination of the following operators in the query condition:

- Greater than symbol (>)
- Less than symbol (<)
- Equal sign (=)
- Percent sign (%) as a wildcard character in the UserName attribute value

Suppose you specify the following values for the attributes:

- UserName: `=jdoe`
- StartDate: `<2006/10/19`
- Operator: `OR`

The query condition that is created when you submit these attribute values is as follows:

```
UserName =jdoe OR StartDate <2006/10/19
```

While deploying the connector, follow the instructions in the "Specifying Values for the Scheduled Task Attributes" section on page 3-5 to specify values for these attributes and the logical operator that you want to apply.

3.1.2 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.
- `NumOfBatches`: 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 reconciled during the current reconciliation run. The following example illustrates this:

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

- `BatchSize`: 20
- `NumOfBatches`: 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 `NumOfBatches` attributes by following the instructions described in the "Specifying Values for the Scheduled Task Attributes" section on page 3-5.

3.1.3 Configuring the Target System As a Trusted Source

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

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

1. Import the XML file for trusted source reconciliation, `XellUserOraApps.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.

> **Note:** Only one target system can be designated as a trusted source. If you import the `XellUserOraApps.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Specify values for the attributes of the `EBS_TS_User` scheduled task. This procedure is described later in this guide.

To import the XML file for 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 `XellUserOraApps.xml` file, which is in the *OIM_HOME*`/xellerate/XLIntegrations/OracleEBiz/xml` 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**.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Importing the Connector XML File" section on page 2-7, the scheduled tasks for lookup fields, trusted source user, and target resource user reconciliations are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **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 should 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 3-5 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 create the second scheduled task.

After you create both scheduled tasks, proceed to the "Adding Custom Attributes for Reconciliation" section on page 3-7.

3.1.4.1 Specifying Values for the Scheduled Task Attributes

This section provides information about the values to be specified for the following scheduled tasks:

- Lookup Fields Reconciliation Scheduled Task
- User Reconciliation Scheduled Tasks

3.1.4.1.1 Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the `Oracle Apps Lookup Reconciliation` 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.
- 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	Default/Sample Value
`Server`	Name of the IT resource instance for Oracle E-Business User Management	`EBS_ITR`
`LookupField Name`	Lookup field to be reconciled	`Oracle.Responsibility. Name`

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

3.1.4.1.2 User Reconciliation Scheduled Tasks 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:

- `EBS_TS_User` (Scheduled task for trusted source reconciliation)
- `EBS_TR_User` (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	Default/Sample Value
`Target System`	Name of the resource object	`E-Business RO`
`Server`	Name of the IT resource instance for Oracle E-Business User Management	`EBS_ITR`
`IsTrusted`	Specifies whether or not reconciliation is to be performed in trusted mode	For trusted source reconciliation, set the value of this attribute to `Yes`. For target resource reconciliation, set the value of this attribute to `No`.
`LinkKey`	Key to decide the linking condition to link an APPS user to an employee	`EMAIL` or `USERNAME`
`LinkField`	Name of the employee ID field used in the Oracle E-Business Employee Reconciliation connector	`USR_UDF_EMPLOYEE_ID`
`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 3-2	The default value is 1000.
`NumOfBatches`	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 3-2	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
`UserName`	This is a filter attribute. Use this attribute to specify the user name 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 3-1	The value can be either the user name or `nodata`. The default value is `nodata`.
`EmployeeID`	This is a filter attribute. Use this attribute to specify the employee 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 3-1	The value can be either the employee ID or `nodata`. The default value is `nodata`.
`StartDate`	This is a filter attribute. Use this attribute to specify the date of joining the company 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 3-1	The value can be either the start date or `nodata`. The default value is `nodata`.
`Operator`	Specifies the logical operator to be applied to the filter attribute **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be one of the following: ■ `AND` ■ `OR` The default value is `AND`.

Attribute	Description	Default/Sample Value
User_Type	This is a filter attribute. Use this attribute to specify the user type for which you want to reconcile records. If you do not want to use this attribute, then specify nodata. **Note:** This attribute is specific to the scheduled task for trusted source reconciliation.	Customer, Person, Supplier, nodata

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

3.1.5 Adding Custom Attributes for Reconciliation

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

By default, the attributes listed in the "Reconciliation Module" section on page 1-1 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.

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/OracleEBiz/config directory.

   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.Fax=FAX

   In this example, Fax is the reconciliation field and FAX 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 Design Console, add the new attribute as a field on the UD_ORACLE_A process form as follows:

   a. Open the Form Designer form. This form is in the Development Tools folder.

   b. Use the binoculars icon to search for and then open the UD_ORACLE_A form for editing.

   c. Click **Create New Version**.

d. 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.

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

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

g. Specify the name and other values of the new field.

h. Click **Make Version Active**.

3. 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. Use the binoculars icon to search for the `E-Business RO` resource object.

c. On the Resource Objects Table tab, double-click the `E-Business RO` 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.Fax=FAX` line in Step 2, then you must specify `Users.Fax` 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.

4. 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. Use the binoculars icon to search for the `OracleAppsUser` provisioning process.

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

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

e. 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.

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 the procedure described in this section if you want to use the provisioning features of Oracle Identity Manager for this target system.
>
> You need not perform the procedure to compile adapters if you have performed the procedure described in "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-3.

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 1-3 for a listing of the provisioning functions that are available with this connector

- `adpORACLEAPPSCREATEUSER`
- `adpORACLEAPPSRESETPASSWORD`
- `adpORACLEAPPSUPDATEUSER`
- `adpORACLEAPPSUPDATEUSERDATE`
- `adpORACLEAPPSENABLEUSER`
- `adpORACLEAPPSADDRESPONSIBILITY`
- `adpORACLEAPPSREMOVERESPONSIBILITY`
- `adpUPDATEORACLEAPPSLIFESPAN`
- `adpORACLEAPPSDISABLEUSER`
- `adpORACLEAPPSUPDATEUSERNAME`

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 "attributes" refers to the identity data fields that store user data.

By default, the attributes listed in the "Provisioning Module" section on page 1-2 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning as follows:

> **Note:**
>
> You need not perform this procedure if you do not want to add custom attributes for provisioning.
>
> The addition of custom child table attributes for provisioning is not supported. This limitation is also mentioned in the "Known Issues" chapter.

> **See Also:** *Oracle Identity Manager Design Console Guide*

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

   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 provisioning attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

   ```
   OimAttributeName=TargetAttribute_API_Field_Index
   ```

   For example:

   ```
   fax=15
   ```

   In this example, `fax` is the provisioning field and `15` is the index of the parameter (corresponding to the `fax` field) used in the stored procedure.

2. Add the new attribute as a field on the `UD_ORACLE_A` process form as follows:

a. Open the UD_ORACLE_A 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. Use the binoculars icon to search for the Oracle Apps Create User (adpORACLEAPPSCREATEUSER) adapter.

c. On the Adapter Factory Table tab, double-click the Oracle Apps Create User 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 Oracle Apps Create User 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 (Literal)" parameter:

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

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

iii. In the **Value** field, specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 1.

For example, if you uncomment the `homeDir=-d` line in Step 1, then you must specify `homeDir` as the attribute name.

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

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

ii. From the **Name** list, select the newly added adapter variable.

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. Use the binoculars icon to search for the `OracleAppsUser` provisioning process.

c. On the Process Definition Table tab, double-click the `OracleAppsUser` provisioning 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.

4

Testing and Troubleshooting

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

- Running Test Cases
- Troubleshooting

4.1 Running Test Cases

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. Open the following file:

   OIM_HOME/xellerate/XLIntegrations/OracleEBiz/config/config.properties

2. Specify values for the attributes in this file. These attributes are described in the following table.

Attribute	Description	Sample Value
Action	Specifies the provisioning action to be performed by the testing utility	The required action can be any one of the following: CONNECT CREATE UPDATEUSER UPDATEUSER_LIFESPAN UPDATEPASSWORD DISABLEUSER ENABLEUSER ADD_RESPONSIBILITY REMOVE_RESPONSIBILITY
serverName	Specifies the IP address or computer name of the Oracle E-Business User Management server	`172.21.136.200`
serverPort	Port at which the Oracle E-Business User Management server is listening	1521
admin	User ID of the Oracle E-Business User Management server administrator	apps
userName	User login ID	`ORATEST`

Attribute	Description	Sample Value
description	Description of the user	ORATEST
lifeSpanType	LifeSpan type of the User	LifeSpan Days, LifeSpan Accesses, None
lifeSpanValue	LifeSpan value of the User	This value depends on the value assigned to the lifeSpanType attribute.
password	Password of the user	password
emailAddress	E-mail address of the user	test@example.com
startDate	Start date of employment of the user	2006-11-11
endDate	End date of employment of the user	2007-4-12
employeeId	Employee ID of the user	1452
resetPswdOnFirstLogon	Specifies whether or not the password of the user must be reset at first login	Yes, No
respName	Responsibility name	@Engineering
respStartDate	Start date of responsibility	2006-11-11
respEndDate	End date of responsibility	2006-11-12
attrName	Attribute to be updated	Email, Employee Id, End Date, Life Span Type, Life Span, Password, Start Date
attrValue	Value of the attribute to be updated	

See Also: The config.properties file for more information about these attributes

3. Run the testing utility file.
   - For Microsoft Windows, run the following file:

     OIM_HOME\xellerate\XLIntegrations\OracleEBiz\scripts\OracleEBiz.bat

   - For UNIX, run the following file:

     OIM_HOME\xellerate\XLIntegrations\OracleEBiz\scripts\OracleEBiz.sh

4. If the script runs without any error, then verify that the required provisioning action has been carried out on the target system.

4.2 Troubleshooting

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 E-Business User Management server.	■ Ensure that the Oracle E-Business User Management server is running. ■ Check if the user exists in Oracle E-Business User Management. ■ 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 the IP address, administrator ID, and administrator password are correct.
The Operation Failed message is displayed on the Oracle Identity Manager Administrative and User Console	■ Ensure that the values for the attributes do not contain delimiter characters (white space). ■ Ensure that the attribute values do not exceed the specified length.

One of the following error messages is thrown when Oracle Identity Manager tries to exchange data with the target system:
`table or view does not exist`
`insufficient privileges`
	This error message is thrown because the target system account for connector operations does not have the required privileges. See "Configuring the Target System" on page 2-2 for information about creating this account and assigning the required privileges to it.

5

Known Issues

The following are known issues associated with this release of the connector:

- **Bug 7167800**

  SSL communication is not supported.

- **Bug 7344350**

  When responsibilities are reconciled from Oracle E-Business User Management, responsibilities for which the end date is a past date are also reconciled. Responsibilities that are end-dated with a past date must not be reconciled.

- **Bug 7354517**

  On the Administrative and User Console, the `User Id` label has not been localized. This label is always displayed in English, regardless of the locale that you are using.

A

Attribute Mappings Between Oracle Identity Manager and Oracle E-Business User Management

The following table discusses attribute mappings between Oracle Identity Manager and Oracle E-Business User Management.

Note: Some Asian languages use multibyte character sets. If the character limit for the fields in the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

Oracle Identity Manager Attribute	Oracle E-Business User Management Attribute	Description
username	FND_USER.USER_NAME	User name
E-mail	FND_USER.EMAIL_ADDRESS	E-mail address
Desc	FND_USER.DESCRIPTION	User description
lifeSpanValue	FND_USER.PASSWORD LIFESPAN DAYS,FND_USER.PASSWORD LIFESPAN ACCESSES	One of the values is stored based on the values of Life Span type
startDate	FND_USER.START_DATE	Effective Dates From
endDate	FND_USER.END_DATE	Effective Dates To
employeeId	FND_USER.EMPLOYEE_ID	Employee ID
respName	FND_RESPONSIBILITY_VL.RESPONSIBILITY_NAME	Responsibility
respStartDate	FND_USER_RESP_GROUPS_DIRECT.START_DATE	Responsibility start date
respEndDate	FND_USER_RESP_GROUPS_DIRECT.END_DATE	Responsibility end date

Index

P

R

S

T

U

V

X