Oracle® Identity Manager

Connector Guide for Database Applications Table

Release 9.0.4

E10426-02

July 2009

Oracle Identity Manager Connector Guide for Database Applications Table, Release 9.0.4

E10426-02

Primary Author: Shiladitya Guha

Contributing Authors: Debapriya Datta, Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Guide for Database Application Table provides information about integrating Oracle Identity Manager with database application tables.

> **Note:** Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to integrate Oracle Identity Manager with database application tables.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

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

Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation library:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack Release 9.0.4 documentation library, 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 Database Applications Table?

This chapter provides an overview of the updates made to the software and documentation for the Database Applications Table connector in release 9.0.4.1 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.4 release of this guide for information about updates that were new for the 9.0.4 release

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.

> **See Also:** *Oracle Identity Manager Release Notes*

Software Updates

This section discusses updates made to this release of the connector software.

Support for IBM DB2 UDB

In this release of the connector, IBM DB2 UDB and Oracle Database 10*g* have been added to the existing list of certified databases. Changes pertaining to this enhancement have been made at appropriate places in this guide.

Documentation-Specific Updates

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

- In the "Modifying the Configuration XML File for Reconciliation" section on page 3-6, the title of the "Batched Reconciliation" section has been changed to "Specifying the Number of Records to Be Reconciled." This connector does not support batched reconciliation.

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 database application tables.

> **Note:** Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

This chapter contains the following sections:

- Reconciliation Module
- Supported Functionality
- Multilanguage Support
- 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, database application tables has been referred to as the *target system.*

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 Framework Guide* for conceptual information about reconciliation configurations

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

You use a configuration XML file to enable or disable the reconciliation of created, updated, and deleted users. The default data fields of each reconciliation event record are taken from this XML file.

The various configuration XML files that are shipped with this connector are introduced in the "Files and Directories That Comprise the Connector" section on page 1-4. Chapter 3, "Configuring the Connector" describes procedures that you can perform to customize the reconciliation module. These procedures involve making changes in the configuration XML file.

Supported Functionality

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

Function	Type	Description
Create User	Provisioning	Creates a user
Delete User	Provisioning	Deletes a user
Enable User or Disable User	Provisioning	Enables or disables a user
Reset User's Password	Provisioning	Resets a user's password
Update User's First Name	Provisioning	Updates a user's first name
Update User's Last Name	Provisioning	Updates a user's last name
Update User's Group	Provisioning	Updates a user's group
Update User's Title	Provisioning	Updates a user's title
Update User's Department	Provisioning	Updates a user's department
Update User's Communication Language	Provisioning	Updates a user's communication language preference
Update User's Logon Language	Provisioning	Updates a user's logon language preference
Update User's Email Address	Provisioning	Updates a user's e-mail address
Update User's Telephone Number	Provisioning	Updates a user's telephone number
Update User's Time Zone	Provisioning	Updates a user's time zone
Update User's Date Format	Provisioning	Updates a user's date format
Update User's Role	Provisioning	Updates a user's role
Create User (Account Discovery)	Reconciliation	Reconciles new user accounts
Delete User	Reconciliation	Reconciles user accounts that are deleted from the target system

Function	Type	Description
Enable User or Disable User	Reconciliation	Reconciles user accounts that are enabled or disabled
Reset User's Password	Reconciliation	Reconciles user accounts with modified password
Update User's First name	Reconciliation	Reconciles user accounts with modified first name
Update User's Last Name	Reconciliation	Reconciles user accounts with modified last name
Update User's Group	Reconciliation	Reconciles user accounts with modified group
Update User's Title	Reconciliation	Reconciles user accounts with modified title
Update User's Department	Reconciliation	Reconciles user accounts with modified department
Update User's Communication Language	Reconciliation	Reconciles user accounts with modified communication language preference
Update User's Logon Language	Reconciliation	Reconciles user accounts with modified logon language preference
Update User's Email Address	Reconciliation	Reconciles user accounts with modified e-mail address
Update User's Telephone Number	Reconciliation	Reconciles user accounts with modified telephone number
Update User's Time Zone	Reconciliation	Reconciles user accounts with modified time zone
Update User's Date Format	Reconciliation	Reconciles user accounts with modified date format
Update User's Decimal Notation	Reconciliation	Reconciles user accounts with modified decimal notation
Update User's Role	Reconciliation	Reconciles user accounts with modified role

Multilanguage Support

The connector supports the following languages:

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

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

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are in the following directory on the installation media:

```
Database Servers/Database Application Table
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`lib/dbadapter.jar`	This JAR file contains the class files that are used to implement provisioning and reconciliation.
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. **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.
`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 to specify the log level and the directory in which the log file is to be created when you run the testing utility.
`test/scripts/DBTable.bat` `test/scripts/DBTable.sh`	This BAT file or UNIX shell script calls the testing utility when the Oracle Identity Manager server is running Microsoft Windows or UNIX, respectively.
Files in the `xml/DB Schema XML` directory	These files contain information about the configuration of the target database schema mapping.
`xml/DB Schema XML/DBApp1.xml`	For an IBM DB2 UDB installation, you must use this configuration XML file if all the user attributes are stored in a single table.
`xml/DB Schema XML/DBApp2.xml`	For an IBM DB2 UDB installation, you must use this configuration XML file if all the user attributes are stored in two tables, a parent table and a child table.
`xml/DB Schema XML/MSSQL2005App1.xml`	For a Microsoft SQL Server 2005 installation, you must use this configuration XML file if all the user attributes are stored in a single table.
`xml/DB Schema XML/MSSQL2005App2.xml`	For a Microsoft SQL Server 2005 installation, you must use this configuration XML file if all the user attributes are stored in two tables, a parent table and a child table.

File in the Installation Media Directory	Description
`xml/DB Schema XML/OraApp1.xml`	For an Oracle Database installation, you must use this configuration XML file if all the user attributes are stored in a single table. If you use this file, then you cannot update the attributes of users you disable during provisioning.
`xml/DB Schema XML/OraApp2.xml`	For an Oracle Database installation, you must use this configuration XML file if all the user attributes are stored in two tables, a parent table and a child table. **Note:** In this guide, the `OraApp2.xml` file has been used to illustrate some of the procedures described in this guide.
`xml/DB Schema XML/OraPerf1.xml`	For an Oracle Database installation, you must use this configuration XML file if all the user attributes are stored in a single table. If you use this file, then you can update the attributes of users, regardless of whether or not the user accounts are disabled.
`xml/DB Schema XML/SybApp1.xml`	For a Sybase installation, you must use this configuration XML file if all the user attributes are stored in a single table.
`xml/DB Schema XML/SybApp2.xml`	For a Sybase installation, you must use this configuration XML file if all the user attributes are stored in two tables, a parent table and a child table.
`xml/DB Schema XML/xdb_app_map.xsd`	This XML file contains information about the validation rules of the configuration XML files that are placed in the same directory.
`xml/Xellerate Config/DBTable_nonTrusted.xml`	This XML file contains definitions for the following connector components: ■ IT resource type ■ Process form ■ Process task and task adapter ■ Resource object
`xml/Xellerate Config/DBTable_trusted.xml`	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.

The "Step 3: Copying the Connector Files and External Code Files" section on page 2-2 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

You can use any one of the following methods to determine the release number of the connector.

Before Deployment

To determine the release number of a connector:

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

   ```
   Database Servers/Database Application Table/lib
   ```

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

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

> **Note:** If you maintain a copy of the `dbadapter.jar` file after deployment, you can use this method to determine the release number of the connector at any stage. After you deploy the connector, it is recommended that you use the "After Deployment" method, which is described in the following section.

After Deployment

To determine the release number of a connector that has already been deployed:

> **See Also:** *Oracle Identity Manager Design Console Guide* for more information about the following steps

1. Open the Oracle Identity Manager Design Console.
2. In the Form Designer, open the process form. The release number of the connector is the value of the **Version** field.

2

Deploying the Connector

Deploying the connector involves the following steps:

- Step 1: Verifying Deployment Requirements
- Step 2: Configuring the Target System
- Step 3: Copying the Connector Files and External Code Files
- Step 4: Configuring the Oracle Identity Manager Server
- Step 5: Importing the Connector XML File
- Step 6: Configuring Reconciliation
- Step 7: Compiling Adapters

If you want to configure the connector for multiple sets of database application tables, then perform the following procedure:

- Configuring the Connector for Multiple Sets of Database Applications Table

Step 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 or later
Target systems	The target system can be any one of the following: ■ IBM DB2 UDB version 9.1 ■ Microsoft SQL Server 2000, Microsoft SQL Server 2005 ■ Oracle8*i* Database, Oracle9*i* Database, Oracle Database 10*g* ■ Sybase 12.5.2
External code	■ `xerces.jar` (the XML parser) ■ `db2jcc.jar` and `db2jcc_license_cu.jar` (for IBM DB2 UDB) ■ `classes12.jar` (for Oracle Database) ■ `jconn2.jar` (for Sybase) ■ `mssqlserver.jar`, `msbase.jar`, and `msutil.jar` (Microsoft SQL Server 2000) ■ `sqljdbc.jar` (Microsoft SQL Server 2005)

Item	Requirement
Target system user account	If target database tables are to be created, then the user account must have the CONNECT privilege. If existing target database tables are to be used, then the user account must have the following privileges on the tables: ■ CONNECT ■ INSERT ■ DELETE ■ UPDATE ■ SELECT You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-7. If the specified privileges were not assigned to the target system user account, then the "Insufficient Privileges Assigned" message would be displayed.

In addition to the requirements mentioned in the preceding table, you must ensure that the following requirements are addressed:

- JDBC connectivity is available to the target database.
- The target database application schema is analyzed and the corresponding XML file is available according to the IT resource definition.
- The JDBC driver and Xerces classes are available in the `CLASSPATH` environment variable on the Oracle Identity Manager server.
- For secure connectivity to the target database, the required configuration has been performed on the database server.

Step 2: Configuring the Target System

You do not need to perform any configuration steps on the target system. However, to enable provisioning, reconciliation, or a combination of provisioning and reconciliation, you must modify and use one of the configuration XML files shipped on the installation media. Chapter 3 provides instructions to perform this procedure.

Step 3: 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.

> **Note:** The directory paths given in the first column of this table correspond to the location of the connector files in the following directory on the installation media:
>
> `Database Servers/Database Application Table`
>
> Refer to the "Files and Directories That Comprise the Connector" section on page 1-4 for more information about these files.

Files in the Installation Media Directory	Destination Directory
`lib/dbadapter.jar`	*OIM_home*/xellerate/JavaTasks *OIM_home*/xellerate/ScheduleTask
Files in the `resources` directory	*OIM_home*/xellerate/connectorResources
Files and directories in the `test` directory	*OIM_home*/xellerate/DBAppTables
Files in the `xml/Xellerate Config` directory	*OIM_home*/xellerate/XLIntegrations/DBAppTables/xml/Xellerate_Config **Note:** You must ensure that there are no spaces in this directory path.
Files in the `xml/DB Schema XML` directory	*OIM_home*/xellerate/XLIntegrations/DBAppTables/xml/DB_Schema

After you copy the connector files listed in the preceding table, copy the following files to the *OIM_home*/`xellerate/ThirdParty` directory:

- The following table gives the source location of the files to be copied.

Database	File to Be Copied
IBM DB2 UDB	*IBMDB2UDB_installation*/SQLLIB/java/db2jcc.jar *IBMDB2UDB_installation*/SQLLIB/java/db2jcc_license_cu.jar Here, *IBMDB2UDB_installation* is the full path of the directory in which you install the database.
Microsoft SQL Server 2000	`mssqlserver.jar`, `msbase.jar`, and `msutil.jar` You can download these JAR files from the Microsoft Web site.
Microsoft SQL Server 2005	`sqljdbc.jar` You can download this JAR file from the Microsoft Web site.
Oracle Database	*ORACLE_HOME*/ora92/jdbc/lib/classes12.jar Here, *ORACLE_HOME* is the full path of the directory in which you install the database.
Sybase	*sybase_installation*/jConnect-5_2/classes/jconn2.jar Here, *sybase_installation* is the full path of the directory in which you install the database.

> **Note:** You must ensure that either the JAR files for SQL Server 2000 or the JAR files for SQL Server 2005 are copied into the `ThirdParty` directory. If you copy both sets of JAR files, then the connector would not work.

- `xerces.jar`

  This file is already present in the *OIM_home*/`xellerate/ext` directory. If you are using Oracle Containers for J2EE (OC4J), then you must also copy this file into the following directory:

  OIM_home/xellerate/ThirdParty

After you copy the JAR files to the required directories, it is recommended that you restart Oracle Identity Manager to refresh the classpath.

> **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.

Step 4: 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

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.

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Step 3: Copying the Connector Files and External Code Files" section on page 2-2, 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
```

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 informational messages that highlight the progress of the application at 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 still 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**

  To enable logging:

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

     ```
     log4j.logger.DBAdapterLogger=log_level
     ```

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

For example:

```
log4j.logger.DBAdapterLogger=INFO
```

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

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

- **IBM WebSphere**

  To enable logging:

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

     ```
     log4j.logger.DBAdapterLogger=log_level
     ```

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

     For example:

     ```
     log4j.logger.DBAdapterLogger=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="DBAdapterLogger">
        <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="DBAdapterLogger">
        <priority value="INFO"/>
     </category>
     ```

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

  ```
  JBoss_home/server/default/log/server.log
  ```

- **OC4J**

  To enable logging:

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

     ```
     log4j.logger.DBAdapterLogger=log_level
     ```

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

     For example:

     ```
     log4j.logger.DBAdapterLogger=INFO
     ```

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

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

Step 5: 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 `DBTable_nonTrusted.xml` file, which is in the *`OIM_home`*`/xellerate/XLIntegrations/DBAppTables/xml/Xellerate_Config` 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 IT resource is displayed.
8. Specify values for the parameters of the IT resource. Refer to the table given in the "Defining IT Resources" section on page 2-7 for information about the values to be specified.
9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `Database` 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 Tools Reference 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 file is imported into Oracle Identity Manager.

After you import the connector XML file, proceed to the "Step 6: Configuring Reconciliation" section on page 2-9.

Defining IT Resources

You must specify values for the IT resource parameters listed in the following table.

Parameter	Description
`Database User ID`	Database user ID on the target database Sample value: `xeluser`
`Database Password`	Database user password on the target database

Parameter	Description

`Database URL`	JDBC URL for the target database
	Format and sample values for Oracle Database:
	`jdbc:oracle:thin:@`*`host`*`:`*`port`*`:`*`sid`*
	`jdbc:oracle:thin@145.125.23.26:1521:cust_db`
	`jdbc:oracle:oci:`*`userid`*`/`*`password`*`@`*`host`*`:`*`port`*`:`*`sid`*
	`jdbc:oracle:oci:scott/tiger@145.125.23.26:1521:cust_db`
	Format and sample values for SQL Server 2000:
	`jdbc:microsoft:sqlserver://Target_host:1433;DatabaseName=databaseName`
	`jdbc:microsoft:sqlserver://172.21.106.76:1433;DatabaseName=master`
	Format and sample values for SQL Server 2005:
	`jdbc:sqlserver://`*`Target_host`*`:1433;database=databaseName`
	`jdbc:sqlserver://172.21.106.76:1433;database=master`
	Format and sample values for IBM DB2 UDB:
	`jdbc:db2://`*`Target_host`*`:50000/DatabaseName`
	`jdbc:db2://172.21.106.76:50000/master`
	Note: Use the IP address, not the computer name or the host name in the URL. The port number used in the example is the default port number. It may change depending on the port on which your application is running.
	Format and sample values for Sybase:
	`jdbc:sybase:Tds:`*`host`*`:`*`port`*`/`*`database`*
	`jdbc:sybase:Tds:123.432.154.12:2639/sales`

`Database Driver`	JDBC driver class
	Value for Oracle Database:
	`oracle.jdbc.driver.OracleDriver`
	Value for SQL Server 2000:
	`com.microsoft.jdbc.sqlserver.SQLServerDriver`
	Value for SQL Server 2005:
	`com.microsoft.sqlserver.jdbc.SQLServerDriver`
	Value for IBM DB2 UDB:
	`com.ibm.db2.jcc.DB2Driver`
	Value for Sybase:
	`com.sybase.jdbc3.jdbc.SybDriver`

`Application Name`	Target application name Sample value: `myapplication`

Parameter	Description
`Configuration XML Path`	Directory path and name of the configuration XML file Sample value: *OIM_home*/xellerate/XLIntegrations/DBAppTables/xml/DB_Schema/OraApp2.xml **Note:** You must ensure that the path that you specify does not contain spaces. **See Also:** The "Files and Directories That Comprise the Connector" section on page 1-4 for information about the various configuration XML files that are available in the connector installation media directory. Based on the description of each configuration XML file, select an XML file that meets your requirements.
`Reconciliation Timestamp`	Last create/update reconciliation time This value is updated by the reconciliation adapter. You need not manually provide any data.

After you specify values for these IT resource parameters, proceed to Step 9 of the procedure to import connector XML files.

Step 6: 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
- Configuring the Reconciliation Scheduled Tasks

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.

Configuring trusted source reconciliation involves the following steps:

> **Note:** You can 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, `DBTable_trusted.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 `DBTable_trusted.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

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

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 `DBTable_trusted.xml` file, which is in the *`OIM_home`*`/xellerate/XLIntegrations/DBAppTables/xml/Xellerate_Config` 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**.

Configuring the Reconciliation Scheduled Tasks

To create the reconciliation scheduled tasks:

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 task are displayed.
5. 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 `ERROR` 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 2-11 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.

After you define the scheduled task, proceed to the "Step 7: Compiling Adapters" section on page 2-12.

Specifying Values for the Scheduled Task Attributes

Depending on whether you want to implement trusted or nontrusted soured reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled tasks:

- `dbTableReconcile_trustedmode` (Scheduled task for trusted source reconciliation)
- `dbTableReconcile` (Scheduled task for nontrusted source 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
`resource`	Name of the IT resource for which the reconciliation process is to be run Sample value: `Oracle Application2`
`application`	Name of the target database application that should be reconciled Sample value: `Oracle Application2`
`objectName`	Resource object name of the connector Sample value: `Database Application Resource`
`isTrusted`	Specifies whether or not reconciliation is to be carried out in trusted mode For trusted source reconciliation, set the value of this attribute to `Yes`. For nontrusted source reconciliation, set the value of this attribute to `No`.
`isFilter`	Specifies whether or not partial reconciliation is to be applied The value can be `Yes` or `No`.
`record_count`	Specifies the number of records to be reconciled during trial reconciliation The value can be any integer. If you do not want to use this feature, then specify `nodata`.

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

Step 7: Compiling Adapters

> **Note:** Configuring provisioning involves modifying the configuration XML file for provisioning and compiling adapters. This section describes the procedure to compile adapters. Refer to Chapter 3 for information about modifying the configuration XML file for provisioning.

The following adapters are imported into Oracle Identity Manager when you import the XML connector file:

- `DBRES Create User`
- `DBRES Update First Name`
- `DBRES Update Last Name`
- `DBRES Update Password`
- `DBRES Update Status`
- `DBRES Update Title`
- `DBRES Update Department`
- `DBRES Update Email`
- `DBRES Update Communication Language`
- `DBRES Update Logon Language`
- `DBRES Update Time Zone`
- `DBRES Update Date Format`
- `DBRES Update Telephone Number`
- `DBRES Update Decimal Notation`
- `DBRES Delete User`
- `DBRES Update Role`
- `DBRES Update Group`
- `DB Transfer Value`

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.

Configuring the Connector for Multiple Sets of Database Applications Table

> **Note:** Perform this procedure only if you want to configure the connector for multiple database application tables. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

To configure the connector for multiple sets of database application tables:

1. Create and configure one IT resource for each set of database application tables.

   The IT Resources form is in the Resource Management folder. The `Oracle Application2` 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 resource type.

2. Configure reconciliation for each set of database application tables. Refer to the "Step 6: Configuring Reconciliation" section on page 2-9 for instructions. Note that only the value of the `resource` attribute needs to be changed for each reconciliation scheduled task.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the set of database application tables to which you want to provision the user.

3

Configuring the Connector

You configure the connector by modifying the configuration XML file that you decide to use for enabling provisioning and reconciliation. This chapter describes how to analyze and modify the configuration XML file so that it matches the structure of the target database application tables.

Refer to the "Files and Directories That Comprise the Connector" section on page 1-4 for information about the sample configuration XML.

In this chapter, a sample configuration exercise is used to explain the various changes that you can make to customize the configuration XML file that you decide to use.

The configuration XML file is validated against the schema definition in the `xdb_app_map.xsd` file to ensure that changes you make in the configuration XML file conform to the schema definition. Therefore, it is recommended that you review the schema definition in the `xdb_app_map.xsd` file before modifying the configuration XML file.

Note: In the configuration XML file that you decide to use, you must specify `xdb_app_map.xsd` as the value of the `xsi:noNamespaceSchemaLocation` attribute. For example:

```
<xdb_app_map xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="xdb_app_map.xsd" name="OracleApp1">
```

If the `xdb_app_map.xsd` file and configuration XML file are not in the same directory, then you must specify the absolute path and name of this file as the value of the `xsi:noNamespaceSchemaLocation` attribute. For example:

```
<xdb_app_map xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="Absolute_path/xdb_app_map.xsd"
name="OracleApp1">
```

The configuration XML file can be divided into the following sections:

- target_application
- target_database
- mapping_data
- database_adapter

target_application

This section is used to identify the target application. The purpose of this section is to provide information that simplifies maintenance of the configuration file.

Section	Description	Attributes
Database	Name of the database	name
target_app_name	Name of the application	None
target_app_ver	Version of the application	None
target_app_provider	Vendor or provider of the application	None

target_database

This section contains information that is used to configure the database connection properties.

mapping_data

This section is used to keep track of the configuration files modification history.

database_adapter

This section is divided into operations. Each operation is further divided into one or more tasks. The number of tasks in an operation depends on the number of tables involved in the operation. Tasks are divided into columns depending on the target application table.

The following table explains the organization of the database_adapter section.

Description of the Section	Description of the Attributes	Possible Values of the Attributes
operation Each operation is linked with an Oracle Identity Manager connector.	name Type of Oracle Identity Manager operation	create, update, delete, reconcileCreateUpdate, or reconcileDelete
task Each operation is divided into one or more tasks. The number of tasks in an operation depends on the number of tables involved in the operation.	table_name Name of the table on which the task is going to operate	Any valid table name
	xeltask_type Type of task in the database	insert, update, delete, or select
column It is a representation of a single column in the target application table.	col_name Name of the column	Any valid column name
	data_type Data type	VARCHAR, VARCHAR2, CHAR, LONGVARCHAR, REAL, DOUBLE, NUMERIC, DECIMAL, FLOAT, DATE, TIME, TIMESTAMP, NULL, BOOLEAN, OTHER, or INTEGER

Description of the Section	Description of the Attributes	Possible Values of the Attributes
	`data_typ_size` Data type size	`20`
	`col_info` Table indexing and relation to other tables	`primary` or `foreign`
	`required` Specifies whether or not the value of this column can be NULL	`true` or `false`
	`col_type` Data source for the column to be used while creating a user	■ `substitute:` To use, for example, `SYSDATE.` ■ `xellerate:` Provided by Oracle Identity Manager ■ `default:` Some default value

	`xel_data_source`
	If `col_type` is `substitute,` then `xel_data_source` holds the substitution string (can be used for functions like `sysdate` and `sequence.nextVal`).
	If `col_type` is `default,` then `xel_data_source` holds the default value.
	If `col_type` is `xellerate,` then `xel_data_source` holds the mapped Oracle Identity Manager attribute name.
		■ Sample string value if `col_type` is `substitute:`
		`column col_name="USR_LAST_UPDATE" data_type="DATE" data_typ_size="60" required="false" col_type="substitute"`
		■ Sample string value if `col_type` is `default:`
		`col_name="USR_STATUS" data_type="VARCHAR2" data_typ_size="5" required="true" col_type="default" xel_data_source="true"`
		■ Sample string value if `col_type` is `xellerate:`
		`col_name="USR_ID" data_type="VARCHAR2" data_typ_size="20" col_info="primary" required="true" col_type="xellerate" xel_data_source="xel_usr_id"`

	`encrypt` Specifies whether or not this data must be encrypted	`true` or `false`

Description of the Section	Description of the Attributes	Possible Values of the Attributes
	`reconcile` Specifies whether or not this field can be reconciled	`true` or `false`
	`encryption_impl` Encryption method implementation class that provides this operation	Any fully qualified class name
`look_up_group` Grouping of lookup fields	`logic_operator` Used to connect two lookup groups with an operator	`AND` or `OR`
`record_lookup_key` This tag is used to collect the information required to identify a particular record in a table. Note that multiple lookup keys can be used to identify a record in a table.	`logic_operator` Used to connect two record lookup keys (columns) with an operator in a group	`AND` or `OR`

	`comparison_operator`
	Operator used to compare the data with the given data for the column
		`&lt;`
		`&gt;`
		`=`
		`&gt;=`
		`&lt;=`
		`!=`

	`table_name` Name of the table	Any table name
	`col_name` Name of the column	Any column name
	`data_type` Data type	`VARCHAR`, `VARCHAR2`, `CHAR`, `LONGVARCHAR`, `REAL`, `DOUBLE`, `NUMERIC`, `DECIMAL`, `FLOAT`, `DATE`, `TIME`, `TIMESTAMP`, `NULL`, `BOOLEAN`, `OTHER`, or `INTEGER`
	`data_typ_size` Data type size	`20`
	`col_info` Table indexing and relation to other tables	`primary` or `foreign`
	`required` Specifies whether or not the value of this column can be NULL	`true` or `false`

Description of the Section	Description of the Attributes	Possible Values of the Attributes
	col_type Data source for the column to be used while creating a user In addition to substitute, xellerate, and default, the following tag is also applicable for record_lookup_key: join This tag contains the name of the column that is common to multiple tables.	Xellerate or Default
	xel_data_source In addition to the description in the column section above, if col_type is join, then the value of xel_data_source is the mapped Oracle Identity Manager attribute name that is to be logically compared by using the logic_operator.	<record_lookup_key logic_operator="NA" comparison_operator="=" table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_ID" data_type="VARCHAR2" data_typ_size="20" col_info="primary" required="true" col_type="join" xel_data_source="xel_usr_id" /> <record_lookup_key logic_operator="AND" comparison_operator="=" table_name="XELUSER1.MDL2_USER_ADDN_DET" col_name="USR_ID" data_type="VARCHAR2" data_typ_size="20" col_info="foreign" required="true" col_type="join" xel_data_source="xel_usr_id"/>

The sample configuration discussed in this chapter is based on code from the OraApp2.xml configuration XML file. However, instructions described in this section apply to any configuration XML file that you decide to use.

The following sample tables correspond to the records defined in the OraApp2.xml configuration XML file.

MDL2_USER_PROF

Field Name	Type and Length	Comments	Required/Optional
USR_ID	VARCHAR(20)	Primary Key	Required
USR_FIRST_NAME	VARCHAR(60)	None	Required
USR_LAST_NAME	VARCHAR(60)	None	Required

Field Name	Type and Length	Comments	Required/Optional
USR_PASSWORD	VARCHAR(40)	None	Required
USR_STATUS	VARCHAR(5)	Default value is true	Required
USR_LAST_UPDATE	DATE	SYSDATE	Required

MDL2_USER_ADDN_DET

Field Name	Type and Length	Comments	Required/Optional
USR_ID	VARCHAR(20)	Foreign Key	Required
USR_GROUP	VARCHAR(50)	None	Optional
USR_ROLE	VARCHAR(50)	None	Optional
USR_TITLE	VARCHAR(50)	None	Optional
USR_DEPT	VARCHAR(50)	None	Optional
USR_EMAIL	VARCHAR(60)	None	Optional
USR_COMM_LANG	VARCHAR(50)	None	Optional
USR_LOGON_LANG	VARCHAR(50)	None	Optional
USR_TEL_NO	VARCHAR(15)	None	Optional
USR_TIME_ZONE	VARCHAR(50)	None	Optional
USR_DATE_FMT	VARCHAR(50)	None	Optional
USR_DEC_NTN	VARCHAR(50)	None	Optional
USR_LAST_UPDATE	DATE	SYSDATE	Required

Based on these sample tables, the following sections provide information about modifying the configuration XML file:

- Modifying the Configuration XML File for Reconciliation
- Modifying the Configuration XML File for Provisioning
- Modifying the Configuration XML File to Address Security Considerations

> **Note:** In the XML code samples discussed in these sections, XELUSER1 is a dummy login ID for the database user.

Modifying the Configuration XML File for Reconciliation

Instructions to enable the connector for various reconciliation actions are described in the following sections:

- Configuring the Reconciliation of New and Updated User Profiles
- Configuring the Reconciliation of Deleted User Profiles
- Partial Reconciliation
- Specifying the Number of Records to Be Reconciled

These sections explain the instructions based on changes to be made in code from the OraApp2.xml configuration XML file. You must make similar changes in the configuration XML file that you specify as the value of the `Configuration XML Path` parameter listed in the "Defining IT Resources" section on page 2-7.

> **See Also:** The "Files and Directories That Comprise the Connector" section on page 1-4 for information about the various configuration XML files that are available in the connector installation media directory

Configuring the Reconciliation of New and Updated User Profiles

> **Note:** You must perform the procedure described in this section. In nontrusted source reconciliation mode, the reconciliation of new user profiles results in the creation of resource objects (for this target system) in Oracle Identity Manager.

The default data fields of each reconciliation event record are taken from the configuration XML file. For reconciliation of new and updated user profiles, the data fields are declared in the `reconcileCreateUpdate` section of the XML file.

The following is sample code from the `OraApp2.xml` file for reconciliation of new and updated user profiles.

> **See Also:** The `OraApp2.xml` file listed in the "Files and Directories That Comprise the Connector" section on page 1-4

```
<operation name = "reconcileCreateUpdate" enabled="true">
    <task table_name="XELUSER1.MDL2_USER_PROF" xeltask_type="select">
        <column table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_ID"
        data_type="VARCHAR2" data_typ_size="20" col_info="primary"
        required="true"
        col_type="xellerate" xel_data_source="xel_usr_id" />
        <column table_name="XELUSER1.MDL2_USER_ADDN_DET" col_name="USR_ID"
        data_type="VARCHAR2" data_typ_size="20" col_info="foreign"
        required="true"  col_type="xellerate" xel_data_source="xel_usr_id" />
        <look_up_group logic_operator="NA">
             <record_lookup_key table_name="XELUSER1.MDL2_USER_PROF"
             logic_operator="NA" comparison_operator="&gt;="
             col_name="USR_LAST_UPDATE" data_type="DATE" data_typ_size="50"
             col_type="join" xel_data_source="XEL_LAST_RECON_TIME"/>
             <record_lookup_key table_name="XELUSER1.MDL2_USER_ADDN_DET"
             logic_operator="AND" comparison_operator="&gt;="
             col_name="USR_LAST_UPDATE" data_type="DATE" data_typ_size="50"
             col_type="join" xel_data_source="XEL_LAST_RECON_TIME"/>
        </look_up_group>
        <look_up_group logic_operator="AND">
             <record_lookup_key logic_operator="NA" comparison_operator="="
             table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_ID"
             data_type="VARCHAR2" data_typ_size="20" col_info="primary"
             required="true" col_type="join" xel_data_source="xel_usr_id" />
             <record_lookup_key logic_operator="AND" comparison_operator="="
             table_name="XELUSER1.MDL2_USER_ADDN_DET" col_name="USR_ID"
             data_type="VARCHAR2" data_typ_size="20" col_info="foreign"
             required="true" col_type="join" xel_data_source="xel_usr_id" />
        </look_up_group>
    </task>
    <task table_name="XELUSER1.MDL2_USER_PROF" xeltask_type="select">
        <column table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_ID"
```

```
 data_type="VARCHAR2" data_typ_size="20" col_info="primary"
 required="true" col_type="xellerate" xel_data_source="xel_usr_id" />
 <column table_name="XELUSER1.MDL2_USER_PROF
 col_name="USR_FIRST_NAME" data_type="VARCHAR2" data_typ_size="60"
 required="true" col_type="xellerate" xel_data_source="xel_usr_first_
 name" />
 <column table_name="XELUSER1.MDL2_USER_PROF"
 col_name="USR_FIRST_NAME" data_type="VARCHAR2" data_typ_size="60"
 required="true" col_type="xellerate" xel_data_source="xel_usr_first_
 name" />
 <column table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_LAST_NAME"
 data_type="VARCHAR2" data_typ_size="60" required="true" col_
 type="xellerate" xel_data_source="xel_usr_last_name" />
 <column table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_PASSWORD"
 data_type="VARCHAR2" data_typ_size="40" required="true" col_
 type="xellerate" xel_data_source="xel_usr_password" encrypt="false"
 reconcile="true" encryption_impl=
 "com.thortech.xl.integration.dbadapter.security.EncryptionSupportImpl
 "/>
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET"
 col_name="USR_GROUP" data_type="VARCHAR2" data_typ_size="50"
 required="true" col_type="xellerate" xel_data_source="xel_usr_group"
 />
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET" col_name="USR_ROLE"
 data_type="VARCHAR2" data_typ_size="50" required="false" col_
 type="xellerate" xel_data_source="xel_usr_role" />
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET" col_name="USR_TITLE"
 data_type="VARCHAR2" data_typ_size="50" required="false" col_
 type="xellerate" xel_data_source="xel_usr_title" />
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET" col_name="USR_DEPT"
 data_type="VARCHAR2" data_typ_size="50" required="false" col_
 type="xellerate" xel_data_source="xel_usr_dept" />
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET" col_name="USR_EMAIL"
 data_type="VARCHAR2" data_typ_size="60" required="false" col_
 type="xellerate" xel_data_source="xel_usr_email" />
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET"
 col_name="USR_COMM_LANG" data_type="VARCHAR2" data_typ_size="50"
 required="false" col_type="xellerate" xel_data_source="xel_usr_comm_
 lang" />
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET"
 col_name="USR_LOGON_LANG" data_type="VARCHAR2" data_typ_size="50"
 required="false" col_type="xellerate" xel_data_source="xel_usr_logon_
 lang" />
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET"
 col_name="USR_TEL_NO" data_type="VARCHAR2" data_typ_size="15"
 required="false" col_type="xellerate" xel_data_source="xel_usr_tel_
 no" />
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET"
 col_name="USR_TIME_ZONE" data_type="VARCHAR2" data_typ_size="50"
required="false" col_type="xellerate" xel_data_source="xel_usr_time_zone"/>
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET"
 col_name="USR_DATE_FMT" data_type="VARCHAR2" data_typ_size="50"
 required="false" col_type="xellerate" xel_data_source="xel_usr_date_
 fmt" />
 <column table_name="XELUSER1.MDL2_USER_ADDN_DET"
 col_name="USR_DEC_NTN" data_type="VARCHAR2" data_typ_size="50"
 required="false" col_type="xellerate" xel_data_source="xel_usr_dec_
 ntn" />
 <look_up_group logic_operator="NA">
     <record_lookup_key table_name="XELUSER1.MDL2_USER_PROF"
```

```
            logic_operator="NA" comparison_operator="&gt;="
            col_name="USR_LAST_UPDATE" data_type="DATE" data_typ_size="50"
            col_type="join" xel_data_source="XEL_LAST_RECON_TIME"/>
            <record_lookup_key table_name="XELUSER1.MDL2_USER_ADDN_DET"
           logic_operator="AND" comparison_operator="&gt;="
           col_name="USR_LAST_UPDATE" data_type="DATE" data_typ_size="50"
           col_type="join" xel_data_source="XEL_LAST_RECON_TIME"/>
       </look_up_group>
       <look_up_group logic_operator="AND">
           <record_lookup_key logic_operator="NA" comparison_operator="="
           table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_ID"
           data_type="VARCHAR2" data_typ_size="20" col_info="primary"
           required="true" col_type="xellerate" xel_data_source="xel_usr_id"
           />
       </look_up_group>
       <look_up_group logic_operator="AND">
           <record_lookup_key logic_operator="NA" comparison_operator="="
           table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_ID"
           data_type="VARCHAR2" data_typ_size="20" col_info="primary"
           required="true" col_type="join" xel_data_source="xel_usr_id" />
           <record_lookup_key logic_operator="AND" comparison_operator="="
           table_name="XELUSER1.MDL2_USER_ADDN_DET" col_name="USR_ID"
           data_type="VARCHAR2" data_typ_size="20" col_info="foreign"
           required="true" col_type="join" xel_data_source="xel_usr_id" />
       </look_up_group>
    </task>
</operation>
```

In the preceding sample configuration XML, the names of the data elements are the values given for the `xel_data_source` tag. You can change these names. The same name is also used as the label for elements in each reconciliation event record.

The create or update reconciliation operation involves running two tasks. The first task identifies the users who have been created or modified after the last reconciliation. This returns a list of key field values for the new and modified users.

For example, if the key field to identify a user is the user ID, then this task returns a list of user IDs corresponding to the user profiles that have been created or modified after the last reconciliation run.

The second task collects all required information about all new and modified users for creating the reconciliation event. The division of tasks is designed for optimal use of memory.

The lookup groups in the task help to create lookup conditions for retrieving relevant data. The preceding sample configuration XML code implements the following lookup conditions:

- Join the two tables in which user profile information is stored, and retrieve nonrepeated data for these users.
- Perform incremental reconciliation by retrieving only those records that are modified after the last reconciliation.

The second task has one more lookup for the user ID, so that user information can be retrieved for each user ID by using the first task.

The time at which the previous reconciliation run was completed is stored in the `Reconciliation Timestamp` IT resource parameter. This value is updated with the new system timestamp after the end of the current reconciliation run. This value is compared against the last updated time in the target database tables, as given in the configuration XML file. In this file, the time at which the last reconciliation run was completed is represented as XEL_LAST_RECON_TIME. It is a connector configuration constant.

If you update any user field, then you must set the value of XEL_LAST_RECON_TIME to the current system date (sysdate) in both tables.

For example, suppose you update the first name of the user as follows:

```
UPDATE MDL2_USER_PROF SET usr_first_name = 'John' WHERE usr_id='jdoe'
```

Then, you must also make the following changes:

```
UPDATE MDL2_USER_PROF SET usr_last_update =sysdate WHERE usr_id='jdoe'
UPDATE MDL2_USER_ADDN_DET SET usr_last_update =sysdate WHERE usr_id=' jdoe'
```

Note: Incremental reconciliation is possible only if the target application is capable of updating the last update time in its database while modifying or creating records. If the target application does not have this feature, then you must not create the lookup group for comparing the last reconciliation time.

Configuring the Reconciliation of Deleted User Profiles

Note: You need not perform this procedure if you do not want to configure the reconciliation of deleted user profiles.

For reconciliation of deleted user profiles, the default data elements are declared in the reconcileDelete section of the configuration XML file.

The following is sample code from the OraApp2.xml configuration XML file for reconciliation of users deleted from the target system:

```
<operation name = "reconcileDelete" enabled="true">
     <task table_name="XELUSER1.MDL2_USER_PROF" xeltask_type="select">
          <column table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_ID"
          data_type="VARCHAR2" data_typ_size="20" col_info="primary"
          required="true" col_type="xellerate" xel_data_source="xel_usr_id"
          />
          <column table_name="XELUSER1.MDL2_USER_ADDN_DET"
          col_name="USR_ID" data_type="VARCHAR2" data_typ_size="20"
          col_info="foreign" required="true" col_type="xellerate"
          xel_data_source="xel_usr_id" />
          <look_up_group logic_operator="NA">
               <record_lookup_key logic_operator="NA" comparison_operator="="
               table_name="XELUSER1.MDL2_USER_PROF" col_name="USR_ID"
               data_type="VARCHAR2" data_typ_size="20" col_info="primary"
               required="true" col_type="join"xel_data_source="xel_usr_id"/>
               <record_lookup_key logic_operator="AND" comparison_
               operator="=" table_name="XELUSER1.MDL2_USER_ADDN_DET"
               col_name="USR_ID" data_type="VARCHAR2" data_typ_size="20"
               col_info="foreign" required="true" col_type="join
               xel_data_source="xel_usr_id" />
          </look_up_group>
     </task>
</operation>
```

Only user IDs are required for creating deletion reconciliation events. Therefore, the preceding configuration XML code shows only the user ID as the data element to be retrieved according to the conditions given in the lookup group.

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. However, you have the option to specify categories of target system records that must be reconciled. You do this by creating filters for the reconciliation module.

To create filters, in the `reconcileCreateUpdate` section of the configuration XML file, add lookup group tags for the filters that you want to create.

For example, if you want to create a filter that fetches only those records for which the value of the `USR_FIRST_NAME` field is `John,` then you add a lookup group tag similar to the following in the configuration XML file:

```
<look_up_group logic_operator="AND">
<record_lookup_key logic_operator="NA" comparison_operator="="
table_name="XELUSER1.TBL_USERS" col_name="USR_FIRST_NAME" data_type="VARCHAR2"
data_typ_size="100" col_type="substitute" xel_data_source="'John'" />
</look_up_group>
```

After you create filters, you must set the `IsFilter` scheduled task attribute to `Yes` while performing the procedure described in the "Specifying Values for the Scheduled Task Attributes" section on page 2-11. You can modify the value of this attribute to enable or disable filters.

Specifying the Number of Records to Be Reconciled

During the first reconciliation run, all the records in the target system are copied into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. This could translate into an unnecessary delay if you only want to perform a trial reconciliation run immediately after you deploy the connector.

To avoid this delay, you can specify the number of records that are to be reconciled. You do this by using the `record_count` scheduled task attribute. This attribute is described in the "Specifying Values for the Scheduled Task Attributes" section on page 2-11.

Modifying the Configuration XML File for Provisioning

Instructions to enable the connector for various provisioning actions are described in the following sections:

- Create User Configuration
- Update User Properties Configuration
- Update User Password Configuration
- Delete User Configuration

These sections explain the instructions based on changes to be made in code from the `OraApp2.xml` configuration XML file. You must make similar changes in the configuration XML file that you specify as the value of the `Configuration XML Path` parameter listed in the "Defining IT Resources" section on page 2-7.

> **See Also:** The "Files and Directories That Comprise the Connector" section on page 1-4 for information about the various configuration XML files that are available in the connector installation media directory

Create User Configuration

To create a user, the configuration XML file must contain the table name, column names, and properties of each column. This is illustrated in the following sample XML code from the OraApp2.xml configuration XML file.

```
<operation name="create">
    <task table_name="XELUSER1.MDL2_USER_PROF" xeltask_type="insert">
        <column col_name="USR_ID" data_type="VARCHAR2" data_typ_size="20"
        col_info="primary" required="true" col_type="xellerate"
        xel_data_source="xel_usr_id" />
        <column col_name="USR_FIRST_NAME" data_type="VARCHAR2"
        data_typ_size="60" required="true" col_type="xellerate"
        xel_data_source="xel_usr_first_name" />
        <column col_name="USR_LAST_NAME" data_type="VARCHAR2"
        data_typ_size="60" required="true" col_type="xellerate"
        xel_data_source="xel_usr_last_name" />
        <column col_name="USR_PASSWORD" data_type="VARCHAR2"
        data_typ_size="40" required="true" col_type="xellerate"
        xel_data_source="xel_usr_password" encrypt="false" reconcile="false"
        encryption_impl=
        "com.thortech.xl.integration.dbadapter.security.EncryptionSu
        pportImpl" />
        <column col_name="USR_LAST_UPDATE" data_type="DATE"
        data_typ_size="60" required="true" col_type="substitute"
        xel_data_source="sysdate" />
    </task>
    <task table_name="XELUSER1.MDL2_USER_ADDN_DET" xeltask_type="insert">
        <column col_name="USR_ID" data_type="VARCHAR2" data_typ_size="20"
        col_info="primary" required="true" col_type="xellerate"
        xel_data_source="xel_usr_id" />
        <column col_name="USR_GROUP" data_type="VARCHAR2"
        data_typ_size="50" required="true" col_type="xellerate"
        xel_data_source="xel_usr_group" />
        <column col_name="USR_ROLE" data_type="VARCHAR2"
        data_typ_size="50" required="false" col_type="xellerate"
        xel_data_source="xel_usr_role" />
        <column col_name="USR_TITLE" data_type="VARCHAR2"
        data_typ_size="50" required="false" col_type="xellerate"
        xel_data_source="xel_usr_title" />
        <column col_name="USR_DEPT" data_type="VARCHAR2"
        data_typ_size="50" required="false" col_type="xellerate"
        xel_data_source="xel_usr_dept" />
        <column col_name="USR_EMAIL" data_type="VARCHAR2"
        data_typ_size="60" required="false" col_type="xellerate"
        xel_data_source="xel_usr_email" />
        <column col_name="USR_COMM_LANG" data_type="VARCHAR2"
        data_typ_size="50" required="false" col_type="xellerate"
        xel_data_source="xel_usr_comm_lang" />
        <column col_name="USR_LOGON_LANG" data_type="VARCHAR2"
        data_typ_size="50" required="false" col_type="xellerate"
        xel_data_source="xel_usr_logon_lang" />
        <column col_name="USR_TEL_NO" data_type="VARCHAR2"
        data_typ_size="15" required="false" col_type="xellerate"
        xel_data_source="xel_usr_tel_no" />
        <column col_name="USR_TIME_ZONE" data_type="VARCHAR2"
        data_typ_size="50" required="false" col_type="xellerate"
        xel_data_source="xel_usr_time_zone" />
        <column col_name="USR_DATE_FMT" data_type="VARCHAR2"
        data_typ_size="50" required="false" col_type="xellerate"
        xel_data_source="xel_usr_date_fmt" />
        <column col_name="USR_DEC_NTN" data_type="VARCHAR2"
        data_typ_size="50" required="false" col_type="xellerate"
        xel_data_source="xel_usr_dec_ntn" />
        <column col_name="USR_LAST_UPDATE" data_type="DATE"
        data_typ_size="60" required="true" col_type="substitute"
        xel_data_source="sysdate"/>
    </task>
</operation>
```

Update User Properties Configuration

The update operation requires lookup information for identifying the user and properties of the columns that are to be updated. This is illustrated in the following sample code from the OraApp2.xml configuration XML file.

```
<operation name="update" xel_data_source="xel_usr_dept">
     <task table_name="XELUSER1.MDL2_USER_ADDN_DET" xeltask_type="update">
          <column col_name="USR_DEPT" data_type="VARCHAR2"
          data_typ_size="50" required="true" col_type="xellerate"
          xel_data_source="xel_usr_dept" />
          <column col_name="USR_LAST_UPDATE" data_type="DATE"
          data_typ_size="60"  required="true" col_type="substitute"
          xel_data_source="sysdate" />
          <look_up_group logic_operator="NA">
              <record_lookup_key
              table_name="XELUSER1.MDL2_USER_ADDN_DET"
              logic_operator="NA"  comparison_operator="=" col_name="USR_ID"
              data_type="VARCHAR2" data_typ_size="20" required="true"
              col_type="xellerate" xel_data_source="xel_usr_id"/>
          </look_up_group>
     </task>
</operation>
```

Update User Password Configuration

The update password operation works the same way as the update user operation. In addition, it performs data encryption if the encrypt attribute is set to true.

This is illustrated in the following sample code from the OraApp2.xml configuration XML file.

```
<operation name="update" xel_data_source="xel_usr_password">
    <task table_name="XELUSER1.MDL1_USER_PROF" xeltask_type="update">
         <column col_name="USR_PASSWORD" data_type="VARCHAR2"
         data_typ_size="40" required="true" col_type="xellerate"
         xel_data_source="xel_usr_password" encrypt="true" reconcile="false"
         encryption_impl=
         "com.thortech.xl.integration.dbadapter.security.EncryptionSu
         pportImpl" />
         <column col_name="USR_LAST_UPDATE" data_type="DATE"
         data_typ_size="60"  required="true" col_type="substitute"
         xel_data_source="sysdate" />
         <look_up_group logic_operator="NA">
              <record_lookup_key table_name="XELUSER1.MDL1_USER_PROF"
              logic_operator="NA"  comparison_operator="=" col_name="USR_ID"
```

```
                data_type="VARCHAR2" data_typ_size="20" required="true"
                col_type="xellerate" xel_data_source="xel_usr_id"/>
            </look_up_group>
        </task>
    </operation>
```

Delete User Configuration

The delete operation requires only lookup information to find the user to be deleted. Column information is used to find the user in the table. This is illustrated in the following sample XML code from the `OraApp2.xml` configuration XML file.

The `lookup_up_group` tags are used to group lookup conditions provided in `record_lookup_key.`

> **Note:** Two tasks are run to delete user records from both tables. The task related to the secondary table must be run before the primary table task. If the order is not correct, then a referential integrity exception is thrown.

```
<operation name="delete">
    <task table_name="XELUSER1.MDL2_USER_ADDN_DET" xeltask_type="delete">
        <look_up_group logic_operator="NA">
             <record_lookup_key logic_operator="NA"  comparison_operator="="
             col_name="USR_ID" data_type="VARCHAR2" data_typ_size="20"
             required="true" col_type="xellerate" xel_data_source="xel_usr_
             id"/>
        </look_up_group>
    </task>
    <task table_name="XELUSER1.MDL2_USER_PROF" xeltask_type="delete">
        <look_up_group logic_operator="NA">
             <record_lookup_key logic_operator="NA"  comparison_operator="="
             col_name="USR_ID" data_type="VARCHAR2" data_typ_size="20"
             required="true" col_type="xellerate" xel_data_source="xel_usr_
             id"/>
        </look_up_group>
    </task>
</operation>
```

Adding Custom Database Columns for Provisioning and Reconciliation

To add a custom database column for provisioning or reconciliation:

1. Create a column tag for the database column that you want to add.

   Suppose you want to add the `USR_DESIGNATION` column of the `MDL2_USER_PROF` table to the list of database columns that are reconciled. To do this, create a `USR_DESTINATION` column tag similar to the following:

   ```
   <column table_name="XELUSER1.MDL2_USER_PROF"
   col_name="USR_DESIGNATION" data_type="VARCHAR2" data_typ_size="60"
   required="true" col_type="xellerate" xel_data_source="xel_usr_designation" />
   ```

2. Add the column tag in the operation tags for all the operations that you want to configure for that column.

   For example, suppose you want to reconcile the `USR_DESIGNATION` column values into Oracle Identity Manager as part of the reconciliation of new and updated user profiles. To achieve this, you must add the USR_DESIGNATION column tag add this column tag in the second task tag of the reconcileCreateUpdate operation tag. This operation tag is described in the "Configuring the Reconciliation of New and Updated User Profiles" section on page 3-7.

Similarly, suppose you want to propagate the designation value from Oracle Identity Manager to the USR_DESIGNATION column during the Create User provisioning action. To achieve this, you must add the USR_DESIGNATION column tag in the second task tag of the create operation tag.

As mentioned at the start of this step, if required, you can add the column tag in the operation tags of every operation covered in the preceding sections of this chapter.

3. Add a field in the resource object with the same name as the value of the xel_data_source attribute of the column tag

   For example, you must create the xel_usr_designation field in the resource object for adding the USR_DESIGNATION column tag.

Modifying the Configuration XML File to Address Security Considerations

This section outlines security considerations that you must address when working with this connector. The following topics are discussed in this section:

- Secure JDBC Connectivity
- Password Encryption and Decryption

These topics explain the procedure based on changes to be made in code from the OraApp2.xml configuration XML file. You must make similar changes in the configuration XML file that you specify as the value of the Configuration XML Path parameter listed in the "Defining IT Resources" section on page 2-7.

> **See Also:** The "Files and Directories That Comprise the Connector" section on page 1-4 for information about the various configuration XML files that are available in the connector installation media directory

Secure JDBC Connectivity

You can establish secure JDBC connectivity with the target database by providing information about security properties in the configuration XML file and enabling secure connectivity for the database server. The security configuration differs with respect to the target database.

The following sections discuss code from the OraApp2.xml configuration XML file. You must make similar changes in the configuration XML file that you specify in the IT resource definition as the value of the Configuration XML Path parameter.

> **See Also:**
>
> - The "Defining IT Resources" section on page 2-7 for information about the Configuration XML Path parameter.
> - The "Files and Directories That Comprise the Connector" section on page 1-4 for information about the various configuration XML files that are available in the connector installation media directory.

Depending on the database that you use, refer to one of the following sections for information about securing JDBC connectivity:

- Secure JDBC Connectivity Configuration for Oracle Database
- Secure JDBC Connectivity Configuration for Sybase

If you do not want to use secure JDBC connectivity, then refer to the following section:

- Disabling Secure JDBC Connectivity

Secure JDBC Connectivity Configuration for Oracle Database

In the configuration XML file, the following is the security configuration XML code for Oracle Database:

```
<target_database>
     <database name="Oracle">
          <properties>
          <encryption_nego_level impl_class_name="oracle.net.encryption_
           client" value ="REQUESTED"/>
          <encryption_algorithm impl_class_name="oracle.net.encryption_
          client" value="DES40"/>
          <crypto_seed impl_class_name="oracle.net.crypto_seed"
          value="xelsysadmin_seed"/>
          <crypto_checksum_level
          impl_class_name="oracle.net.crypto_checksum_client"
          value="REQUIRED"/>
          <crypto_checksum_client
          impl_class_name="oracle.net.crypto_checksum_types_client"
          value="MD5"/>
    </properties>
    </database
</target_database>
```

This configuration contains the security properties to be provided to the JDBC driver for establishing a secure connection to Oracle Database. Note that if these parameters are not provided, then a nonsecure JDBC connection is established to the target database.

The following are the permitted values for each configuration parameter mentioned in the configuration XML code listed earlier.

Configuration Parameter	Permitted Value
`encryption_nego_level`	`REJECTED`, `ACCEPTED`, `REQUESTED`, or `REQUIRED`
`encryption_algorithm`	`RC4_256`, `RC4_128`, `RC4_56`, `RC4_40`, `AES256`, `AES192`, `AES128`, `3DES168`, `3DES112`, `DES`, or `DES40`
`crypto_seed`	`xelsysadmin_seed`
`crypto_checksum_level`	`REJECTED`, `ACCEPTED`, `REQUESTED`, or `REQUIRED`
`crypto_checksum_client`	`MD5` or `SHA1`

In addition to the changes in the configuration XML file, you must add the following parameters in the `sqlnet.ora` file:

```
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER= (MD5)
SQLNET.AUTHENTICATION_SERVICES= (NTS)
SQLNET.ENCRYPTION_TYPES_SERVER= (DES40)
SQLNET.CRYPTO_SEED = xelsysadmin_seed
```

Depending on the Oracle Database release that you are using, this file is in a directory whose path is similar to the following:

oracle_home\ora92\network\admin

Secure JDBC Connectivity Configuration for Sybase

In the configuration XML file, the following is the security configuration for Sybase:

```
<target_database>
<database name="Sybase">
    <properties>
        <cipher_suites impl_class_name="CIPHER_SUITES_1"
        value="SSL_DH_anon_EXPORT_WITH_RC4_40_MD5"/>
    </properties>
</database>
</target_database>
```

In this XML code, you can assign any one of the following values to cipher suite:

- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA

Disabling Secure JDBC Connectivity

If you do not want to implement secure JDBC connectivity, then in the configuration XML file, put the child tags of the <database> tag in a comment.

This is shown in the following example:

```
<target_database>
 <database name="Oracle">
  <!--<properties>
   <encryption_nego_level impl_class_name="oracle.net.encryption_client" value
="REQUESTED"/>
   <encryption_algorithm impl_class_name="oracle.net.encryption_client"
value="DES40"/>
   <crypto_seed impl_class_name="oracle.net.crypto_seed"value="xelsysadmin_seed"/>
   <crypto_checksum_levelimpl_class_name="oracle.net.crypto_checksum_client"
value="REQUIRED"/>
<crypto_checksum_clientimpl_class_name="oracle.net.crypto_checksum_types_client"va
lue="MD5"/>
  </properties>-->
 </database>
</target_database>
```

Password Encryption and Decryption

You can implement third-party encryption and decryption algorithms when you use this connector. The connector exposes the EncryptionSupportIntf interface, which you must implement and make available in the CLASSPATH environment variable.

While configuring the encryption for a column, the fully qualified class name must be provided. Before updating the data in the database, the connector encrypts the data. If reconciliation of the encrypted password is possible, then the decryption method is used to retrieve the actual password and to reconcile the password in Oracle Identity Manager.

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:

- Testing the Connector
- Troubleshooting

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 the *`OIM_home`*`/xellerate/XLIntegrations/DBAppTables/config` directory.

   See Also: The "Defining IT Resources" section on page 2-7 for information about the parameters in the `config.properties` file

2. Run one of the following files:

   For UNIX:

   ```
   OIM_home/xellerate/XLIntegrations/DBAppTables/scripts/DBTable.sh
   ```

   For Microsoft Windows

   ```
   OIM_home\xellerate\XLIntegrations\DBAppTables\scripts\DBTable.bat
   ```

Troubleshooting

The following table provides solutions to some commonly encountered issues associated with this connector.

Problem Description	Returned Error Code	Solution
Oracle Identity Manager cannot establish a connection with the target database.	DATABASE CONNECTION FAILED	■ Ensure that the drivers of the database are specified in the `CLASSPATH` environment variable of the Oracle Identity Manager server. ■ 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.
	DATABASE DRIVER NOT LOADED	Ensure that the database driver is available in the CLASSPATH environment variable of the Oracle Identity Manager server.
A provisioning operation fails with an error code other than those described in the following rows.	CONFIGURATION ERROR	■ Ensure that the configuration XML file given in the IT resource definition exists at the specified file system path. ■ Ensure that the XML schema file exists at the location specified in the configuration XML file. ■ Ensure that the configuration XML file adheres to the XML schema specified inside the file itself.
	DATA SIZE MISMATCH	Ensure that the data size of the user profile attributes in the configuration XML file adheres to the process form limitations.
	MANDATORY FIELD MISSING	■ Ensure that values are provided for all user attributes specified as `required` in the configuration XML file. This error is thrown even if a blank string is provided. ■ Ensure that the process form includes the fields marked as `required` in the configuration XML file.
	DATABASE OPERATION FAILED	■ Ensure that the maximum size of user profile attributes given in the configuration XML file matches the size defined in the actual database schema. ■ Ensure that all the mandatory fields of the database table are marked as `required` in the configuration XML file.
Create User provisioning operation fails	USER ALREADY EXISTS	Check if the target database table already has a record with the same user ID (or a combination of whichever primary key fields exist for the table).

Problem Description	Returned Error Code	Solution
Create User or Reset Password provisioning operation fails	`ENCRYPTION INTERFACE MISSING`	■ Check if password encryption is set to `true` in the configuration XML file. ■ Ensure that the encryption interface implementation class is available in the CLASSPATH environment variable of the Oracle Identity Manager server.
	`ENCRYPT/DECRYPT ERROR`	This error occurs if an exception is thrown from the encryption implementation class. ■ Check if the encryption implementation class is working correctly. ■ Check the logs for a description of the error and stack trace.
Update Any User Profile Attribute, Delete a User, or Revoke a Provisioned Resource Object from a User provisioning operation fails	`USER DOES NOT EXIST`	Check if the record for the user exists in the target database tables.

5

Known Issues

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

- This connector cannot be used in a scenario in which user attributes are stored in more than two database tables.
- The directory path that you specify as the value of the `Configuration XML Path` IT resource parameter must not contain spaces.
- 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 were using the Japanese language and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.
- Secure JDBC connection is not supported in Microsoft SQL Server and IBM DB2 UDB.

Index