Oracle® Identity Manager

Connector Guide for Database User Management

Release 9.0.4

E10154-01

May 2007

ORACLE®

Oracle Identity Manager Connector Guide for Database User Management, Release 9.0.4

E10154-01

Primary Author: Shiladitya Guha

Contributing Authors: Deepa Aswani, Debapriya Datta, Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Guide for Database User Management provides information about setting up Oracle Identity Manager for database user management.

Note: This is a transitional release following Oracle's acquisition of Thor Technologies. 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 deploy the Oracle Identity Manager connector for database user management.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

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 User Management?

This chapter provides an overview of the updates made to the software and documentation for the Database User Management connector in release 9.0.4 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.3 release of this guide for information about updates that were new for the 9.0.3 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.

Trusted Source Reconciliation

This release of the connector supports trusted source reconciliation. The required information has been included at appropriate places in the guide.

Separate Scheduled Tasks for Trusted and Nontrusted Source Reconciliation

In this release of the connector, there are separate user reconciliation scheduled tasks for trusted and nontrusted source reconciliation. In the "Configuring the Reconciliation Scheduled Tasks" section on page 3-3, the attributes of these scheduled tasks are described.

Timeout Support

This release of the connector provides timeout support for provisioning and reconciliation. In the "Defining IT Resources" section on page 2-11, the IT resource parameters that are used to implement this feature are described.

Partial Reconciliation

You can customize the reconciliation process by specifying the subset of added or modified target system records that must be reconciled. This feature is discussed in the following section:

- Partial Reconciliation on page 3-1

Specifying the Number of Records to Be Reconciled

In this release, you can specify the number of records to be reconciled by using the Record Size user reconciliation scheduled task attribute. This is described in the "Specifying the Number of Records to Be Reconciled" section on page 3-2.

Enabling Logging

By following the instructions in the "Enabling Logging" section on page 2-7, you can configure the generation of log information that is specific to the target system.

Secure Connection to the Oracle Database

In this release of the connector, you can set up a secure JDBC connection between Oracle Identity Manager and the Oracle Database only. This feature is not available for the other target systems. This is achieved by using the `isSecure` parameter, which is described in the "Defining IT Resources" section on page 2-11.

Testing Utility

The testing utility has been added in this release of the connector. The required information has been added in the following sections:

- Files and Directories That Comprise the Connector on page 1-10
- Step 3: Copying the Connector Files and External Code Files on page 2-3
- Chapter 4, "Testing Connector Functionality" on page 4-1

Documentation-Specific Updates

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

- Instructions in the "Determining the Release Number of the Connector" section on page 1-11 have been revised.
- Instructions to enable logging for this connector are given in the "Enabling Logging" section on page 2-7.
- Some of the content from the Chapter 2 of the earlier release of this guide has been moved to Chapter 3.

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. The connector for Database User Management is used to integrate Oracle Identity Manager with various databases.

> **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

Reconciliation involves duplicating in Oracle Identity Manager additions 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 following table lists the target system attributes whose values are read from the database during reconciliation.

Field	IBM DB2 UDB	Microsoft SQL Server	Oracle Database	Sybase
Login	Yes	Yes	Yes	Yes
userType	Yes	-	-	-

Field	IBM DB2 UDB	Microsoft SQL Server	Oracle Database	Sybase
Full Name	-	-	-	Yes
DefaultTablespace	-	-	Yes	-
dbName	Yes	-	-	-
Roles	-	Yes	Yes	Yes
schemaName	Yes	-	-	-
tableSpaceName	Yes	-	-	-
User	-	Yes	-	Yes
Group	-	-	-	Yes
Database	-	Yes	-	Yes

Reconciled Xellerate 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

Provisioning Module

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

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

For this target system, the provisioning module is divided into the following sections:

- Database Access Entity: Login Provisioning
- Database Access Entity: User Provisioning

Database Access Entity: Login Provisioning

The following fields are provisioned.

Field	IBM DB2 UDB	Microsoft SQL Server	Oracle Database	Sybase
Login	Yes	Yes	Yes	Yes
Password	Yes	Yes	Yes	Yes

Field	IBM DB2 UDB	Microsoft SQL Server	Oracle Database	Sybase
Default DB	-	-	-	Yes
Default Language	-	Yes	-	Yes
Full Name	-	-	-	Yes
Authentication Type	Yes	-	-	-
Tablespace	-	-	Yes	-
Datafile Size (in MB)	-	-	Yes	-
Default Role	-	-	-	Yes
DB2 Database	Yes	-	-	-
DB2 User Type	Yes	-	-	-
Role	-	-	Yes	Yes
Tablespace Name	Yes	-	-	-
Schema Name	Yes	-	-	-

Database Access Entity: User Provisioning

The following fields are provisioned.

Field	IBM DB2 UDB	Microsoft SQL Server	Oracle Database	Sybase
DB User	-	Yes	-	Yes
DB Name	-	Yes	-	Yes
DB Group	-	-	-	Yes
DB Parent Login	-	Yes	-	Yes
Authentication Type	-	Yes	-	-
Role	-	-	-	Yes

Supported Functionality

In Microsoft SQL Server and Sybase, database access entities can be divided into the following types:

- Login (parent)
- User (child)

Because the connector must provide user provisioning features in both these RDBMSs, each database access entity is handled using separate provisioning and reconciliation functions.

However, for Oracle Database and IBM DB2 UDB, the Create Login function is sufficient to create accounts for users. Therefore, the Create User function is not used for these RDBMSs.

The following sections provide information about the provisioning and reconciliation functions supported by the connector for each database access entity type:

- Database Access Entity: Login

- Database Access Entity: User

Database Access Entity: Login

The following table lists the connector functions corresponding to the login database access entity type.

Note: Most of these functions are supported on all four RDBMSs: IBM DB2 UDB, Microsoft SQL Server, Oracle Database, and Sybase.

Function	Type	Description	Supported on
Create Login	Provisioning	Creates a login in the database **Note:** Running this function on Oracle Database would result in the creation of a user, but would not grant any privileges to the user. To provide the required privileges, run the Add Role or Grant function with the values CONNECT, RESOURCE, and SELECT ANY TABLE. For more information, refer to the description of the Add Role or Grant function.	All
Delete Login	Provisioning	Deletes a provisioned login	All
Enable Login	Provisioning	Enables a disabled login	IBM DB2 UDB
Disable Login	Provisioning	Disables a login	IBM DB2 UDB
Default DB Updated	Provisioning	Updates the properties of a login in the database according to a change in the Default DB Updated attribute You must add appropriate lookup codes (corresponding to valid database names) in the following lookup definitions: ■ **UD_Lookup.DB_Dbnames-sql:** For example, if a database named `model` exists on the target Microsoft SQL Server, then the following entry must be added as the lookup code: **Code Key:** `model` **Decode:** `model` **Lang:** `en` **Country:** `US` ■ **UD_Lookup.DB_Dbnames:** For example, if a database named `master` exists on the target Sybase installation, then the following entry must be added as the lookup code: **Code Key:** `master` **Decode:** `master` **Lang:** `en` **Country:** `US`	Microsoft SQL Server and Sybase
Full Name Updated	Provisioning	Updates the properties of a login in the database according to a change in the Full Name attribute	Sybase

Function	Type	Description	Supported on
Default Role Updated	Provisioning	Updates the properties of a login in the database according to a change in the Default Role attribute This function works only if the relevant role is already assigned to the Sybase login. You must add appropriate lookup codes (corresponding to valid roles) in the following lookup definition: **Lookup.DB Role:** For example, if a role named `oper_role` exists on the target Sybase database, then the following entry must be added as the lookup code: ■ **Code Key:** `oper_role` ■ **Decode:** `oper_role` ■ **Lang:** `en` ■ **Country:** `US`	Sybase
Default Language Updated	Provisioning	Updates the properties of a login in the database according to a change in the Default Language attribute You must add appropriate lookup codes (corresponding to valid roles) in the following lookup definition: **UD_Lookup.Def_Lang:** For example, if a language named `us_English` exists on the target Sybase or Microsoft SQL Server database, then the following entry must be added as the lookup code: ■ **Code Key:** `us_english` ■ **Decode:** `us_english` ■ **Lang:** `en` ■ **Country:** `US`	Microsoft SQL Server and Sybase
Password Updated	Provisioning	Updates the properties of a login in the database according to a change in the Password Updated attribute This function is run when the password in a process form is changed. **For Sybase:** ■ The password must contain at least 6 characters. ■ If no input is provided in the Password field of the process form, then the provisioned user is assigned a password with the same value as the user login.	Microsoft SQL Server, Oracle Database, and Sybase

Function	Type	Description	Supported on
Add Role or Grant	Provisioning	Adds a role to an existing login in the database The required role must be defined and valid in the target system. You must add appropriate lookup codes (corresponding to valid role names) in the following lookup definitions: ▪ **Lookup.DB Role:** For example, if a role named `oper_role` exists on the target Sybase database, then the following entry must be added as the lookup code: **Code Key:** `oper_role` **Decode:** `oper_role` **Lang:** `en` **Country:** `US` ▪ **Lookup.DB Role-Oracle:** For example, if a role named `DBA` exists on the target Oracle Database, then the following entry must be added as the lookup code: **Code Key:** `DBA` **Decode:** `DBA` **Lang:** `en` **Country:** `US`	Oracle Database and Sybase
Revoke Role	Provisioning	Revokes a role from an existing login in the database	Oracle Database and Sybase
Add Tablespace	Provisioning	Adds a tablespace to an existing login in the database The required tablespace must be defined and valid in the target system. You must add appropriate lookup codes (corresponding to valid tablespaces) in the following lookup definition: **UD_Lookup.DB_Tablespacenames:** For example, if a tablespace named `tb_xel` exists on the target IBM DB2 UDB database, then the following entry must be added as the lookup code: **Code Key:** `tb_xel` **Decode:** `tb_xel` **Lang:** `en` **Country:** `US`	IBM DB2 UDB
Delete Tablespace	Provisioning	Revokes a tablespace from an existing login in the database	IBM DB2 UDB

Function	Type	Description	Supported on
Add Schema	Provisioning	Adds a schema to an existing login in the database The required schema must be defined and valid in the target system. You must add appropriate lookup codes (corresponding to valid schema names) in the following lookup definition: **UD_Lookup.DB_Schemas:** For example, if a schema named `xeltest` exists on the target IBM DB2 UDB database, then the following entry must be added as the lookup code: **Code Key:** `xeltest` **Decode:** `xeltest` **Lang:** `en` **Country:** `US`	IBM DB2 UDB
Delete Schema	Provisioning	Revokes a schema from an existing login in the database	IBM DB2 UDB
Trusted Reconciliation for Login	Reconciliation	Creates login accounts in Oracle Identity Manager corresponding to reconciled logins from the database	All
Create Login	Reconciliation	Reconciles logins	All
Update Login	Reconciliation	Reconciles attributes of logins existing in Oracle Identity Manager	Microsoft SQL Server and Sybase
Default DB Updated	Reconciliation	Reconciles changes in the Default DB attribute of logins existing in Oracle Identity Manager	Microsoft SQL Server and Sybase
Full Name Updated	Reconciliation	Reconciles changes in the Full Name attribute of logins existing in Oracle Identity Manager	Sybase
Default Role Updated	Reconciliation	Reconciles changes in the Default Role attribute of logins existing in Oracle Identity Manager	Microsoft SQL Server and Sybase
Default Language Updated	Reconciliation	Reconciles changes in the Default Language attribute of logins existing in Oracle Identity Manager	Microsoft SQL Server and Sybase
Add Role or Grant	Reconciliation	Reconciles newly added roles of logins existing in Oracle Identity Manager	Oracle Database and Sybase
Add Tablespace	Reconciliation	Reconciles newly added tablespaces of logins existing in Oracle Identity Manager	IBM DB2 UDB
Add Schema	Reconciliation	Reconciles newly added schemas of logins existing in Oracle Identity Manager	IBM DB2 UDB

Database Access Entity: User

The following table lists the connector functions corresponding to the user database access entity type.

Note: These functions are supported on only Microsoft SQL Server and Sybase.

Function	Type	Description	Supported on
Create User	Provisioning	Creates a user corresponding to an existing login in the database While running this function, you must provide the required value in the DB Name field. The required schema must be defined and valid in the target system. You must add appropriate lookup codes (corresponding to valid schema names) in the following lookup definitions: ■ **UD_Lookup.DB_Dbnames:** For example, if a database named `master` exists on the target Sybase installation, then the following entry must be added as the lookup code: **Code Key:** `master` **Decode:** `master` **Lang:** `en` **Country:** `US` ■ **UD_Lookup.DB_Dbnames-sql:** For example, if a database named `model` exists on the target Microsoft SQL Server installation, then the following entry must be added as the lookup code: **Code Key:** `model` **Decode:** `model` **Lang:** `en` **Country:** `US`	Both
Delete User	Provisioning	Deletes a provisioned user corresponding to an existing login in the database This function can be run by running the Revoke Request function using the Request form in Oracle Identity Manager.	Both
Disable User	Provisioning	Disables an existing user in the database This function revokes access to all tables for the specified user.	Sybase
Enable User	Provisioning	Enables a disabled existing user in the database The provisioned account has default access to only a particular set of tables. This function grants all types of access privileges to the account for all system- and user-defined tables in the specified database.	Sybase

Function	Type	Description	Supported on
DB Group Updated	Provisioning	Updates the configuration of a user in the database according to a change in the DB Group attribute If no input is provided in the User Group field of the process form, then the provisioned user is added to the default group, `public`, in the Sybase database. The required group must be defined and valid in the Sybase database. You must add appropriate lookup codes (corresponding to valid group names) in the following lookup definition: **UD_Lookup.DB_Group:** For example, if a group named `Managers` exists on the target Sybase database, then the following entry must be added as the lookup code: ■ **Code Key:** `Managers` ■ **Decode:** `Managers` ■ **Lang:** `en` ■ **Country:** `US`	Sybase
Add Role	Provisioning	Adds a role to an existing user in the database The required role must be defined and valid on the target Microsoft SQL Server database. You must add appropriate lookup codes (corresponding to valid role names) in the following lookup definition: **Lookup.DB Role-MSSQL:** For example, if a role named `db_datawriter` exists on the target Sybase database, then the following entry must be added as the lookup code: ■ **Code Key:** `db_datawriter` ■ **Decode:** `db_datawriter` ■ **Lang:** `en` ■ **Country:** `US`	Microsoft SQL Server
Revoke Role	Provisioning	Revokes a role from an existing user in the database	Microsoft SQL Server
Create User	Reconciliation	Reconciles users that are created in the database	Both
DB Group Updated	Reconciliation	Reconciles the updated DB Group attribute of existing users in Oracle Identity Manager	Sybase
Add Role	Reconciliation	Reconciles newly added roles of existing logins in Oracle Identity Manager	Microsoft SQL Server

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 User Management
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`lib/xliDatabaseAccess.jar`	This file contains the class files required for performing provisioning and reconciliation.
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. There are two resource bundle files for a particular language, one for each database access entity (Login and User). **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/procGrantAllToUser.sql`	This file contains the code for the stored procedure that implements the Enable User function.
`scripts/procRevokeAllFromUser.sql`	This file contains the code for the stored procedure that implements the Disable User function.
`test/config/config.properties`	This file contains the attributes for Oracle Identity Manager to connect to the target system and perform provisioning operations.
`test/config/log.properties`	This file is used to store logging messages.
`test/scripts/DBAccess.bat` `test/scripts/DBAccess.sh`	This file is used to start the testing utility.
`xml/xliDBAccessLogin_DM Nontrusted.xml`	This XML file contains definitions for the connector components related to Database Access (Login) provisioning. These components include: ■ Database Access (Login) IT resource type ■ Custom Process form ■ Process task and adapters (along with their mappings) ■ Login resource object ■ Provisioning process ■ Pre-populate rules

File in the Installation Media Directory	Description
xml/xliDBAccessUser_DM Nontrusted.xml	This XML file contains definitions for the connector components related to Database Access (User) provisioning. These components include: ■ Database Access (User) IT resource type ■ Custom process form ■ Process task and adapters (along with their mappings) ■ User resource object ■ Provisioning process ■ Pre-populate rules
xml/xelluserDbAcess 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.

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

The "Step 3: Copying the Connector Files and External Code Files" section on page 2-3 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 `xliDatabaseAccess.jar` file. This file is in the following directory on the installation media:

   `Database Servers/Database User Management/lib`

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

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 Files

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: ■ Oracle8i Database ■ Oracle9i Database ■ Oracle Database 10*g* ■ Oracle Real Application Clusters 10*g* ■ Microsoft SQL Server 2000 ■ Microsoft SQL Server 2005 ■ Sybase Adaptive Server Enterprise 12.5 ■ IBM DB2 UDB 8.1, IBM DB2 UDB 9.1
External code	The external code consists of the following files: ■ `classes12.zip` (Oracle8*i* Database, Oracle9i Database, and Oracle Database 10*g*) ■ `msbase.jar`, `mssqlserver.jar`, and `msutil.jar` (Microsoft SQL Server 2000) ■ `sqljdbc.jar` (Microsoft SQL Server 2005) ■ `jconn2.jar` (Sybase Adaptive Server Enterprise 12.5) ■ `db2java.zip` (IBM DB2 UDB) **Note:** These ZIP and JAR files are available in the corresponding database installation directories.

Item	Requirement
Target system user account	Depending on the target system, the required user account is one of the following: ■ For Oracle Database: sys, sysdba, or system ■ For Microsoft SQL Server: sa (administrator) ■ For Sybase: sa (administrator) ■ For IBM DB2 UDB: Host operating system administrator account If IBM DB2 UDB DB2 is installed on an Active Directory domain controller, then a Microsoft Windows 2000/2003 Server (Domain Controller) Administrator account must be used. If you do not provide the required rights to this user account, then the following exception is thrown: `ORA-01031: insufficient privileges` You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-11.

Step 2: Configuring the Target System

The following sections provide configuration instructions that are specific to the target system database:

- Configuring IBM DB2 UDB
- Configuring Microsoft SQL Server
- Configuring Oracle Database
- Configuring Sybase

Configuring IBM DB2 UDB

You configure IBM DB2 UDB by ensuring that:

- Authentication on IBM DB2 UDB is done through the operating system. Therefore, the user that you want to provision must exist in the security system of the operating system.

  For example, if you want to provision the domain, then the target (IBM DB2 UDB server) must exist on the domain server and the user that you want to provision must exist in the domain.

- For databases or services that you want to provision, you must enter the relevant lookup codes, corresponding to the databases or services that already exist on the target system, in the `UD_Lookup.DB_Dbnames` lookup definition.

- For tablespaces that you want to provision, you must enter the relevant lookup codes, corresponding to the tablespaces that already exist on the target system, in the `UD_Lookup.DB_Tablespacenames` lookup definition.

- For schemas that you want to provision, you must enter the relevant lookup codes, corresponding to the schemas that already exist on the target system, in the `UD_Lookup.DB_Schemas` lookup definition.

After you configure the IBM DB2 UDB installation, proceed to the "Step 3: Copying the Connector Files and External Code Files" section on page 2-3.

Configuring Microsoft SQL Server

You configure Microsoft SQL Server by ensuring that:

- The target database in which users are to be created exists in the target Microsoft SQL Server installation.
- The Microsoft SQL Server user account that is used to create users has DBA privileges. For example, `sa/sa`.
- For Microsoft SQL Server 2005, the TCP/IP connection configuration is enabled.

  To enable the TCP/IP connection configuration:

  1. Open the Microsoft SQL Server Configuration Manager.
  2. Click **SQL Server 2005 Network Configuration**.
  3. Click **Protocols for MSSQLSERVER**.
  4. In the right frame, right-click **TCP/IP** and then click **Enable**.

After you configure the Microsoft SQL Server installation, proceed to the "Step 3: Copying the Connector Files and External Code Files" section on page 2-3.

Configuring Oracle Database

You configure Oracle Database by ensuring that:

- The service name that is used to create users exists in the target Oracle Database installation.
- There is sufficient space in the database to store provisioned users.
- The Oracle Database user account that is used to create users has DBA privileges. For example, `sys` as `sysdba/sys` or `system/manager`.

After you configure the Oracle Database installation, proceed to the "Step 3: Copying the Connector Files and External Code Files" section on page 2-3.

Configuring Sybase

You configure Sybase by ensuring that:

- The target database in which users are to be created exists in the target Sybase ASE installation.
- The following scripts are run on the target Sybase database:
  - `procGrantAllToUser.sql`
  - `procRevokeAllFromUser.sql`

  Refer to the "Step 3: Copying the Connector Files and External Code Files" section on page 2-3 for instructions to copy these files from the installation media ZIP file to the *`OIM_home`*`/xellerate/XLIntegrations/DatabaseAccess/scripts` directory.

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 User Management`

Refer to the "Files and Directories That Comprise the Connector" section on page 1-10 for more information about these files.

File in the Installation Media Directory	Destination Directory
`lib/xliDatabaseAccess.jar`	*OIM_home*`/xellerate/JavaTasks` *OIM_home*`/xellerate/ScheduleTask`
Files in the `resources` directory	*OIM_home*`/xellerate/connectorResources`
Files in the `scripts` directory	*OIM_home*`/xellerate/XLIntegrations/DatabaseAccess/scripts`
Files in the `test/config` directory	*OIM_home*`/xellerate/XLIntegrations/test/config`
Files in the `test/scripts` directory	*OIM_home*`/xellerate/XLIntegrations/test/scripts`
Files in the `xml` directory	*OIM_home*`/xellerate/XLIntegrations/DatabaseAccess/xml`

Depending on the target system, perform the steps given in one of the following sections to copy external code files:

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 `connectorResources` directory and the JAR files to the corresponding directories on each node of the cluster.

- Copying External Code Files on IBM DB2 UDB
- Copying External Code Files on Microsoft SQL Server
- Copying External Code Files on Oracle Database
- Copying External Code Files on Sybase

Copying External Code Files on IBM DB2 UDB

For connectors used with IBM DB2 UDB, copy the `db2java.zip` file from the *DB2_HOME*`/IBM/SQLLIB/java` directory into the *OIM_home*`/xellerate/ThirdParty` directory.

After you copy the external code file, proceed to the "Step 5: Importing the Connector XML Files" section on page 2-10.

Copying External Code Files on Microsoft SQL Server

For connectors used with Microsoft SQL Server 2000, the required external JAR files are the JDBC driver files: `mssqlserver.jar`, `msbase.jar`, and `msutil.jar`.

To obtain these files, first download Microsoft SQL Server 2000 Driver for JDBC Service Pack 3 from the Microsoft Web site.

For connectors used with Microsoft SQL Server 2005, the required external JAR file is the `sqljdbc.jar` JDBC driver file. This file can be downloaded from the Microsoft Web site.

You must copy the required JAR files into the following directory:

OIM_home`/xellerate/ThirdParty`

Copying External Code Files on Oracle Database

If the connector is used with Oracle8*i* Database, Oracle9*i* Database, or Oracle Database 10*g*, then the required external code file is `classes12.zip`.

The `classes12.zip` file is available in the Oracle Database installation at, for example, the following path:

oracle_home`/ora92/jdbc/lib/`

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

You must copy the `classes12.zip` file into the *OIM_home*`/xellerate/ThirdParty` directory.

After you copy the external code file, proceed to the "Step 5: Importing the Connector XML Files" section on page 2-10.

Copying External Code Files on Sybase

For connectors used with Sybase ASE, copy the `jconn2.jar` file from the *SYBASE_HOME*`/jConnect-5_5/classes` directory into the *OIM_home*`/xellerate/ThirdParty` directory.

Step 4: Configuring the Oracle Identity Manager Server

This section discusses the following topics:

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

- Deploying the Microsoft Active Directory Connector If IBM DB2 UDB Is Used
- Changing to the Required Input Locale
- Modifying the SVP Table
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

Deploying the Microsoft Active Directory Connector If IBM DB2 UDB Is Used

> **Note:** Perform this step only if the target system is IBM DB2 UDB.

IBM DB2 UDB installed on a Microsoft Windows server does not support the creation of user accounts. Instead, it uses operating system users. It assigns the required privileges to a Microsoft Windows user to convert the user into a complete IBM DB2

UDB user. After a user account is created in Microsoft Windows, it can be assigned the relevant privileges in IBM DB2 UDB.

Therefore, if you want to use the Database User Management connector to provision accounts in IBM DB2 UDB, then you must first deploy the connector for Microsoft Active Directory in the following directory:

OIM_home/xellerate/XLIntegrations/ActiveDirectory

See Also: *Oracle Identity Manager Connector Guide for Microsoft Active Directory*

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.

Modifying the SVP Table

Change the length of the SVP_FIELD_VALUE column in the SVP table to 2000 as follows:

1. Log in to the Oracle Identity Manager database by using the Oracle Identity Manager database user credentials.
2. Enter the following command at the SQL prompt:

   For Oracle Database:

   ```
   ALTER TABLE SVP MODIFY SVP_FIELD_VALUE VARCHAR2(2000);
   ```

   For Microsoft SQL Server:

   ```
   ALTER TABLE SVP ALTER COLUMN SVP_FIELD_VALUE VARCHAR(2000);
   ```

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 2-3, 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. If you run the command described in Step 2 as follows, then an exception is thrown:

   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 and the log file path depend 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.`*`DB_Adapter=log_level`*

2. In this line, replace *DB_Adapter* with the name if the adapter for the database that is in use and *log_level* with the log level that you want to set.

   For example:

   – IBM DB2 UDB

   ```
   log4j.logger.Adapter.DB2UDB=INFO
   ```

   – Microsoft SQL Server

   ```
   log4j.logger.Adapter.MSSQL=INFO
   ```

   – Oracle Database

   ```
   log4j.logger.Adapter.ORACLE=INFO
   ```

   – Sybase

   ```
   log4j.logger.Adapter.DatabaseAccess=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.*DB_Adapter*=*log_level*

  2. In this line, replace *DB_Adapter* with the name if the adapter for the database that is in use and *log_level* with the log level that you want to set.

     For example:

     – IBM DB2 UDB

     ```
     log4j.logger.Adapter.DB2UDB=INFO
     ```

     – Microsoft SQL Server

     ```
     log4j.logger.Adapter.MSSQL=INFO
     ```

     – Oracle Database

     ```
     log4j.logger.Adapter.ORACLE=INFO
     ```

     – Sybase

     ```
     log4j.logger.Adapter.DatabaseAccess=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="DB_Adapter">
   <priority value="log_level"/>
</category>
```

2. In the second XML code line, replace *DB_Adapter* with the name if the adapter for the database that is in use and *log_level* with the log level that you want to set.

   For example:

   – IBM DB2 UDB

   ```
   <category name="Adapter.DB2UDB">
      <priority value="INFO"/>
   </category>
   ```

   – Microsoft SQL Server

   ```
   <category name="Adapter.MSSQL">
      <priority value="INFO"/>
   </category>
   ```

   – Oracle Database

   ```
   <category name="Adapter.ORACLE">
      <priority value="INFO"/>
   </category>
   ```

   – Sybase

   ```
   <category name="Adapter.DatabaseAccess">
      <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.*DB_Adapter*=*log_level*

  2. In this line, replace *DB_Adapter* with the name if the adapter for the database that is in use and *log_level* with the log level that you want to set.

     For example:

     – IBM DB2 UDB

     ```
     log4j.logger.Adapter.DB2UDB=INFO
     ```

     – Microsoft SQL Server

     ```
     log4j.logger.Adapter.MSSQL=INFO
     ```

     – Oracle Database

     ```
     log4j.logger.Adapter.ORACLE=INFO
     ```

     – Sybase

```
log4j.logger.Adapter.DatabaseAccess=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 Files

To import the connector XML files 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 locating files is displayed.
4. Locate and open the `xliDBAccessLogin_DM.xml` file, which is in the *OIM_home*`/xellerate/XLIntegrations/DatabaseAccess/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 `OracleITResource` IT resource is displayed. If this is the IT resource corresponding to the database that you are using, then perform the next step. Otherwise, click **Next** until the Provide IT Resource Instance Data page for the IT resource of the database that you are using is displayed.
8. Depending on the database that you are using, specify values for the parameters of the IT resource. Refer to the appropriate table in the "Defining IT Resources" section on page 2-14 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 a new 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.
13. Perform the same procedure to import the `xliDBAccessUser_DM.xml` and `xliDBAccessScheduleTask_DM.xml` files. These files are in the *OIM_home*`/xellerate/XLIntegrations/DatabaseAccess/xml` directory.

Note: Ensure that you import the connector XML files in the specified order.

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

Defining IT Resources

This section provides IT resource parameter values for the following databases:

- IT Resource Parameter Values for IBM DB2 UDB
- IT Resource Parameter Values for Microsoft SQL Server
- IT Resource Parameter Values for Oracle Database
- IT Resource Parameter Values for Sybase

IT Resource Parameter Values for IBM DB2 UDB

You must specify values for the `IBM DB2 UDB` IT resource parameters listed in the following table.

Parameter	Description
`DataBaseType`	Type of RDBMS Value: `DB2`
`DatabaseName`	Not required
`Driver`	JDBC driver class Value: `COM.ibm.db2.jdbc.net.DB2Driver`
`URL`	JDBC URL for the target database (**Note:** The URL that you specify must be less than 2000 characters long.) Value: `jdbc:db2://`*`Target_Host`*`:6789/`*`DatabaseName`* Sample value: `jdbc:db2://10.1.1.127:6789/TESTDB` **Note:** Use the IP address, not the computer name or host name.
`UserID`	User name of the DBA login that is used to create users Value: `sa`
`Password`	Not required
`Target Locale: Country`	Country code Default value: `US` **Note:** You must specify the value in uppercase.
`Target Locale: Language`	Language code Default value: `en` **Note:** You must specify the value in lowercase.
`isSecure`	Specifies whether or not a secure connection must be set up to the target system The value can be `Yes` or `No`. The default value is `Yes`. **Note:** This feature is supported only on for the Oracle Database.

Parameter	Description
max_retry	Number of times that the connector must retry connecting to the target server, if the connection fails Default value: 2
delay_retry	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, if the connection fails Default value: 10000

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

IT Resource Parameter Values for Microsoft SQL Server

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

Parameter	Description
DataBaseType	Type of RDBMS Value: MSSQL
DatabaseName	Name of the target database in which users are created Sample value: XELL
Driver	**For Microsoft SQL Server 2000** JDBC driver class: com.microsoft.jdbc.sqlserver.SQLServerDriver **For Microsoft SQL Server 2005** JDBC driver class: com.microsoft.sqlserver.jdbc.SQLServerDriver

Parameter	Description
URL	JDBC URL for the target database (**Note:** The URL that you specify must be less than 2000 characters long.) **For Microsoft SQL Server 2000** Value: jdbc:microsoft:sqlserver://*Target_Host*:1433;DatabaseName=*DatabaseName* Sample value: jdbc:microsoft:sqlserver://192.168.49.64:1433;DatabaseName=XELL **Note:** Use the IP address, not the computer name or host name in this URL. **For Microsoft SQL Server 2005** Value: jdbc:sqlserver://*serverName*;*instanceName*:*portNumber*;*property*=*value*[;*property*=*value*] Sample value: jdbc:sqlserver://123.12.23.321:1433;database=master **Note:** Use the IP address, not the computer name or host name in this URL.
UserID	User name of the DBA login that is used to create users Value: sa
Password	Password of the DBA login that is used to create users Value: sa
Target Locale: Country	Country code Default value: US **Note:** You must specify the value in uppercase.
Target Locale: Language	Language code Default value: en **Note:** You must specify the value in lowercase.
isSecure	Specifies whether or not a secure connection must be set up to the target system The value can be Yes or No. The default value is Yes. **Note:** This feature is supported only on for the Oracle Database.
max_retry	Number of times that the connector must retry connecting to the target server, if the connection fails Default value: 2
delay_retry	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, if the connection fails Default value: 10000

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

IT Resource Parameter Values for Oracle Database

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

Parameter	Description
`DataBaseType`	Type of database Value: `Oracle`
`DatabaseName`	Name of the target database in which users are created Sample value: `xeldb`
`Driver`	JDBC driver class Value: `oracle.jdbc.driver.OracleDriver`

Parameter	Description
URL	JDBC URL for the target database (**Note:** The URL that you specify must be less than 2000 characters long.) The URL value that you must specify depends on the number of database instances and the services they support: ■ One database instance supports multiple services URL value: jdbc:oracle:thin:@//*Oraclehost.domain*:*Oracleportnumber*/*Oracleservicename* Sample value: jdbc:oracle:thin:@//host1.acmewidgets.com:1521/srvce1 ■ Multiple database instances support one service URL value: jdbc:oracle:thin:*loginid*/*password*@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=*host1_name.domain*)(PORT=*port1_number*))(ADDRESS=(PROTOCOL=TCP)(HOST=*host2_name.domain*)(PORT=*port2_number*))(ADDRESS=(PROTOCOL=TCP)(HOST=*host3_name.domain*)(PORT=*port3_number*)) . . . (ADDRESS=(PROTOCOL=TCP)(HOST=*hostn_name.domain*)(PORT=*portn_number*))(CONNECT_DATA=(SERVICE_NAME=<*name_of_Oracle_service_that_connects_all_given_hosts*>))) Sample value: jdbc:oracle:thin:sys/welcome1@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=host1.acmewidgets.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host2.acmewidgets.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host3.acmewidgets.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host4.acmewidgets.com)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME= srvce1))) ■ One database instance supports one service URL value: jdbc:oracle:thin:@*host_name.domain*:*port_number*:*name_of_Oracle_Database_service* Sample value: jdbc:oracle:thin:@host1.acemwidgets:1521:srvce1
UserID	User name of the DBA login that is used to create users Value: `sys as sysdba` or `system`
Password	Password of the DBA login that is used to create users Value: `sys` or `manager`

Parameter	Description
Target Locale: Country	Country code Default value: US **Note:** You must specify the value in uppercase.
Target Locale: Language	Language code Default value: en **Note:** You must specify the value in lowercase.
isSecure	Specifies whether or not a secure connection must be set up to the target system The value can be Yes or No. The default value is Yes.
max_retry	Number of times that the connector must retry connecting to the target server, if the connection fails Default value: 2
delay_retry	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, if the connection fails Default value: 10000

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

IT Resource Parameter Values for Sybase

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

Parameter	Description
DataBaseType	Type of RDBMS Value: SYBASE
DatabaseName	Name of the target database in which users are created Sample value: master
Driver	JDBC driver class Value: com.sybase.jdbc2.jdbc.SybDriver
URL	JDBC URL for the target database (**Note:** The URL that you specify must be less than 2000 characters long.) Value: jdbc:sybase:Tds:*Target_Host*:5000/*DatabaseName* Sample value: jdbc:sybase:Tds:integnt:5000/master
UserID	User name of the DBA login that is used to create users Value: sa

Parameter	Description
Password	Password of the DBA login that is used to create users Value: sa
Target Locale: Country	Country code Default value: US **Note:** You must specify the value in uppercase.
Target Locale: Language	Language code Default value: en **Note:** You must specify the value in lowercase.
isSecure	Specifies whether or not a secure connection must be set up to the target system The value can be Yes or No. The default value is Yes. **Note:** This feature is supported only on for the Oracle Database.
max_retry	Number of times that the connector must retry connecting to the target server, if the connection fails Default value: 2
delay_retry	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, if the connection fails Default value: 10000

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

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
- Configuring the Connector for Multiple Installations of the Target System

Configuring Reconciliation

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

- Partial Reconciliation
- Specifying the Number of Records to Be Reconciled
- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks
- Enabling Reconciliation in Oracle Identity Manager Release 9.0.1

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 a filter for the reconciliation module.

Creating a filter involves specifying a value for the `Login Name` scheduled task attribute. This value is used in the query SELECT criteria to reconcile target system records for which the value of the `Login Name` field matches the value of the `Login Name` scheduled task attribute.

For example, if you specify `jdoe` as the value of the `Login Name` scheduled task attribute, then all new or updated target system records for which the login name is `jdoe` are reconciled.

While deploying the connector, follow the instructions in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-3 to specify values for the `Login Name` scheduled task attribute.

Specifying the Number of Records to Be Reconciled

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.

For a trial reconciliation run, you can specify the number of records to be reconciled by using the `Record Size` user reconciliation scheduled task attribute. The numeric value that you assign to this attribute represents the number of records that must be reconciled. The default value of the `Record Size` attribute is `All`, which signifies that all records are to be reconciled.

You can use this feature to perform a trial reconciliation run.

You specify a value for the `Record Size` attribute by following the instructions described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-3.

Configuring Trusted Source Reconciliation

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

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

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, `xelluserDbAcess 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 `xelluserDbAcess 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 `Database Reconciliation Task - Trusted` 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 locating files is displayed.
4. Locate and open the `xelluserDbAcess Trusted.xml` file, which is in the *`OIM_home`*`/xellerate/XLIntegrations/DatabaseAccess/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**.

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Step 5: Importing the Connector XML Files" section on page 2-10, the scheduled tasks for lookup fields, trusted source user, and nontrusted 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 **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. Depending on whether you want to implement trusted or nontrusted soured reconciliation, you must specify values for the attributes of one of the following scheduled tasks:
   - `Database Reconciliation Task - Trusted` (Scheduled task for trusted source reconciliation)
   - `Database Reconciliation Task - Non Trusted` (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	Sample Value
`Server`	Name of the IT resource	`Oracle`
`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`.
`Target System Login Recon - Resource Object name`	Name of the target system parent resource object	`Database Access (Login)`
`Target System User Recon - Resource Object name`	Name of the target system child resource object	`Database Access (User)`

`Trusted Source Recon - Resource Object name`	Name of the trusted source resource object	For trusted source reconciliation:
		`Xellerate User`
		For nontrusted source reconciliation:
		`False`

`DB2DBName`	For IBM DB2 UDB, Microsoft SQL Server, and Sybase, specify the name of the target database from where data is to be reconciled. For Oracle Database, do not specify any value for this attribute.	`TESTDB`
`Login Name`	This is a filter attribute. Use this attribute to specify the login name of the user whose records you want to reconcile. If you do not want to use then specify `Nodata.` **See Also:** The "Partial Reconciliation" section on page 3-1	`Jdoe`
`Record Size`	Specifies the number of records to be reconciled The value can be any integer greater than zero.	The default value of this attribute is `All.`

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.

Enabling Reconciliation in Oracle Identity Manager Release 9.0.1

If you are using Oracle Identity Manager release 9.0.1, then you must perform the following procedure to enable reconciliation:

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

1. Open the Process Definition form for the `Database Access (Login)` User. This form is in the Process Management folder.
2. Click the **Reconciliation Field Mappings** tab.
3. For each field that is of the IT resource type:
   a. Double-click the field to open the Edit Reconciliation Field Mapping window for that field.
   b. Deselect **Key Field for Reconciliation Matching**.
4. Repeat Steps 1 through 3 for the `Database Access (User)` user.

Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. Refer to the "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector.

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

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

> **See Also:** The "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector

- `DB Revoke Role`
- `DB Modify Password`
- `DB Modify Login`
- `DB Enable login`
- `DB Disable login`
- `DB Delete Login`
- `DB Create Login`
- `DB Add TableSpace`
- `DB Add Schema`
- `DB Add Role`

- DB Delete TableSpace
- DB Prepopulate UserLogin
- DB Update Group
- DB EnableSybaseUser
- DB DisableSybaseUser
- DB Delete User
- DB Create User
- DB Prepopulate UserLogin

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.

Changing the Default Language Assigned to Provisioned User Accounts

Note: The instructions given in this section are not part of the deployment procedure.

If you want to enable the option for changing the default language assigned to provisioned user accounts, then:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. Open the process form for Database Access (Login).
3. On the Tasks tab, select the **Default Language Updated** task.
4. Select **Allow Multiple Instances**.
5. Click **Save**.

Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of the target system.

You may want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Acme Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of the target system.

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

See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

1. Create and configure one IT resource for each target system installation.

   The IT Resources form is in the Resource Management folder. An IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same IT resource type.
2. Configure reconciliation for each target system installation. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that you only need to modify the attributes that are used to specify the IT resource and to specify whether or not the target system installation is to be set up as a trusted source.
3. If required, modify the fields to be reconciled for the Xellerate User resource object.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the target system installation to which you want to provision the user.

4

Testing Connector Functionality

You can use the testing utility to directly use the connector for identifying the cause of problems associated with connecting to the target system server and performing basic operations on the target system.

To use the testing utility:

1. Open the following file:

   OIM_home/xellerate/XLIntegrations/test/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	Provisioning action to be performed by the testing utility	CONNECT CREATE_LOGIN DELETE_LOGIN CHANGE_PASSWORD DISABLE_USER
Application_Name	Application name	DBAccess
Database_Driver	Database driver	Com.microsoft.jdbc.sqlserver.SQLServerDriver
Database_URL	Database URL	Jdbc:microsoft:sqlserver://172.21.109.73:1433;DatabaseName=sales
Database_User_ID	User ID for connecting to the database	jdoe
Database_Name	Database name	sales
Database_Type	Database type	MSSQL
LocaleLanguage	Locale language of the target system	En
LocaleCountry	Locale country of the target system	US
Login	Login to be created	loginname
Password	Password for the login	password
FullName	Full name of the user associated with the login created	FullName
DefDBSql	Default database for Microsoft SQL Server	MyDB

Attribute	Description	Sample Value
Default_Language	Default language	`En`
Authentication_Type	Authentication type for Microsoft SQL Server	`isSqlAuth` This is the actual value.
Tablespace	Any valid tablespace in Oracle Database	`Mytablespace`
Datafile_size	Datafile size in Oracle Database	`500`
Default_Role	Default role in Sybase	
DB2_Database	IBM DB2 UDB database name	`DBApp`
DB2_User_Type	IBM DB2 UDB user type (Group/User)	`Group`
Default_DB	Default database for IBM DB2 UDB	`SYSTOOLS`
Role	Role	`DBA`
Tablespace_Name	Valid tablespace name for IBM DB2 UDB	`Systool`
Schema_Name	Valid schema name for IBM DB2 UDB	`Systool`
Del_Login	Login name to be deleted	`Dellogin`
New_Password	New password for changing password	`Password`
Chg_Login	Login name of the user for whom changes are required	jdoe
User_Type	New user type	`User`
DIS_Login	Login to be disabled	`DISLogin`
DIS_User_Type	User type of the login to be disabled (Group/User)	`User`

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

     OIM_home\xellerate\XLIntegrations\test\scripts\DBAccess.bat

   - For UNIX, run the following file:

     OIM_home/xellerate/XLIntegrations/test/scripts/DBAccess.sh

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

5

Known Issues

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

- When the connector is used with Microsoft SQL Server 2000, Microsoft SQL Server 2005, or IBM DB2 UDB, the `URL` parameter of the IT resource accepts only the IP address of the target computer on which the Microsoft SQL Server 2000 server is installed. You cannot use the host name of the computer.
- 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.
- You may come across an error while trying to change the default language assigned to provisioned user accounts. To avoid this error, you must enable the option to change the default language. This procedure is described in the "Changing the Default Language Assigned to Provisioned User Accounts" section on page 3-6.

Index

R

S

T

V

X