Oracle® Identity Manager

Connector Guide for Database Access

Release 9.0.1

B31114-01

June 2006

ORACLE®

Oracle Identity Manager Connector Guide for Database Access, Release 9.0.1

B31114-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Guide for Database Access provides information about setting up Oracle Identity Manager for database access.

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 access.

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 set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade 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 Connector Framework Guide*
- *Oracle Identity Manager Connector Guide for Microsoft Active Directory*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.1 connector documentation set, 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.

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 access 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:

Supported Functionality

This section discusses the functionality supported by the connector.

Function	Type	Description
Provisioning process 1: Database Access (Login)		
Create Login	Provisioning	Creates a login in the database
Delete Login	Provisioning	Deletes a provisioned login
Enable Login	Provisioning	Enables a disabled login
Disable Login	Provisioning	Disables a login

Function	Type	Description
Default DB Updated	Provisioning	Updates the configuration of a login in the database according to a change in the Default DB Updated attribute This function is available only on: ■ Sybase ■ Microsoft SQL Server You must add appropriate lookup codes (corresponding to valid database names) in the following lookup definitions: ■ **UD_Lookup.DB_Dbnames:** For example, if a database named `master` exists on the target Sybase server, 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, then the following entry must be added as the lookup code: **Code Key:** `model` **Decode:** `model` **Lang:** `en` **Country:** `US`
Full Name Updated	Provisioning	Updates the configuration of a login in the database according to a change in the Full Name attribute This function is available only on: ■ Sybase ■ Microsoft SQL Server
Default Role Updated	Provisioning	Updates the configuration of a login in the database according to a change in the Default Role attribute This function is available only on Sybase. This function works 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`

Function	Type	Description
Default Language Updated	Provisioning	Updates the configuration of a login in the database according to a change in the Default Language attribute This function is available only on: ■ Sybase ■ Microsoft SQL Server 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`
Password Updated	Provisioning	Updates the configuration 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.

Function	Type	Description
Add Role	Provisioning	Adds a role to an existing login in the database This function is available only on: ■ Sybase ■ Oracle Database The required role must be defined and valid on 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`
Revoke Role	Provisioning	Revokes a role from an existing login in the database This function is available only on: ■ Sybase ■ Oracle
Add Tablespace	Provisioning	Adds a tablespace to an existing login in the database This function is available only on IBM DB2 UDB. The required tablespace must be defined and valid on 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`

Function	Type	Description
Delete Tablespace	Provisioning	Revokes a tablespace from an existing login in the database This function is available only on IBM DB2 UDB.
Add Schema	Provisioning	Adds a schema to an existing login in the database This function is available only on IBM DB2 UDB. The required schema must be defined and valid on 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`
Delete Schema	Provisioning	Revokes a schema from an existing login in the database This function is available only on IBM DB2 UDB.
Trusted Reconciliation for Login	Reconciliation	Creates Xellerate Login accounts with respect to the reconciled logins from the database
Create Login	Reconciliation	Reconciles logins from the database This function is available only on: ■ Sybase ■ Microsoft SQL Server
Update Login	Reconciliation	Reconciles attributes of logins existing in Xellerate, from the database This function is available only on: ■ Sybase ■ Microsoft SQL Server
Default DB Updated	Reconciliation	This function is available only on: ■ Sybase ■ Microsoft SQL Server
Full Name Updated	Reconciliation	This function is available only on: ■ Sybase ■ Microsoft SQL Server
Default Role Updated	Reconciliation	This function is available only on: ■ Sybase ■ Microsoft SQL Server

Function	Type	Description
Default Language Updated	Reconciliation	This function is available only on: ■ Sybase ■ Microsoft SQL Server
Add Role	Reconciliation	Reconciles newly added roles of logins existing in Xellerate, from the database This function is available only on: ■ Sybase ■ Oracle
Add Tablespace	Reconciliation	Reconciles newly added tablespaces of existing logins in Xellerate, from the database This function is available only on IBM DB2 UDB.
Add Schema	Reconciliation	Reconciles newly added schemas of existing logins in Xellerate, from the database This function is available only on IBM DB2 UDB.
Provisioning process 2 : Database Access (User)		
Create User	Provisioning	Creates a user with respect to an existing login in the database This function is available only on: ■ Sybase ■ Microsoft SQL Server While running this function, you must provide the required entry in the DB Name field. The required schema must be defined and valid on 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 server, 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, then the following entry must be added as the lookup code: **Code Key:** `model` **Decode:** `model` **Lang:** `en` **Country:** `US`

Function	Type	Description
Delete User	Provisioning	Deletes a provisioned user with respect to an existing login in the database This function is available only on: ■ Sybase ■ Microsoft SQL Server This function can be run by running the Revoke Request function using the Request form in Oracle Identity Manager.
Disable User	Provisioning	Disables an existing user in the database This function is available only on Sybase. This function revokes access to all tables for the specified user.
Enable User	Provisioning	Enables a disabled existing user in the database This function is available only on Sybase. 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 that are there in the specified database.
DB Group Updated	Provisioning	Updates the configuration of a user in the database according to a change in the DB Group attribute This function is available only on Sybase. 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`

Function	Type	Description
Add Role	Provisioning	Adds a role to an existing user in the database This function is available only on Microsoft SQL Server. 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`
Revoke Role	Provisioning	Revokes a role from an existing user in the database This function is available only on Microsoft SQL Server.
Create User	Reconciliation	Reconciles users for a login, from the database This function is available only on: ■ Sybase ■ Microsoft SQL Server
DB Group Updated	Reconciliation	Reconciles updated DB Group attribute of existing user in Xellerate from the database This function is available only on Sybase.
Add Role	Reconciliation	Reconciles newly added roles of existing logins in Xellerate, from the database This function is available only on Microsoft SQL Server.

Reconciliation Module

The elements that the reconciliation module extracts from the target system in order to construct reconciliation event records are given in the following table.

Attribute Name	Oracle Database	IBM DB2 UDB	Sybase	Microsoft SQL Server
`Login`	Yes	Yes	Yes	Yes
`userType`	No	Yes	No	No
`Full Name`	No	No	Yes	No
`DefaultTablespace`	Yes	No	No	No
`dbName`	No	Yes	No	No
`Roles`	Yes	No	Yes	Yes
`schemaName`	No	Yes	No	No

Attribute Name	Oracle Database	IBM DB2 UDB	Sybase	Microsoft SQL Server
tableSpaceName	No	Yes	No	No
User	No	No	Yes	Yes
Group	No	No	Yes	No
Database	No	No	Yes	Yes

Provisioning Module

The provisioning module can be divided into the following types:

-

DB Login Provisioning

The following fields are provisioned:

- Login
- Password
- Default DB (Sybase)
- Default Language
- Full Name
- Authentication Type
- Tablespace
- Datafile size (MB)
- Default Role (Sybase)
- DB2 Database
- DB2 User Type
- Default DB (SQL Server)
- Role (Sybase)
- Role (Oracle)
- Tablespace Name
- Schema Name

DB User Provisioning

The following fields are provisioned:

- DB User
- DB Name (Sybase)
- DB Group
- DB Parent Login
- Authentication Type
- DB Name (SQL Server)

- Role (SQL Server)

Files and Directories That Comprise the Connector

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

`Database Servers\Database User Management\Database Rev 3.1.0.zip`

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`xml\xliDBAccessLogin_DM.xml`	This XML file contains the Oracle Identity Manager components of the connector 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
`xml\xliDBAccessUser_DM.xml`	This XML file contains the Oracle Identity Manager components of the connector 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\xliDBAccessScheduleTask_DM.xml`	This XML file contains the Oracle Identity Manager components of the connector related to Database Access reconciliation. These components include: ■ Reconciliation task ■ Reconciliation task attributes
`lib\xliDatabaseAccess.jar`	This file contains the class files required for performing provisioning and reconciliation.
`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.
`docs\B31114_01.pdf` `docs\html`	These are PDF and HTML versions of this guide, which provides instructions to deploy the connector.

The "Step 4: Copying the Connector Files" section on page 2-3 provides instructions to copy these files into the required directories.

2

Deploying the Connector

Deploying the connector involves the following steps:

Step 1: Verifying Installation Requirements

The following table lists the installation 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 ■ Microsoft SQL Server 2000 ■ Sybase Adaptive Server Enterprise 12.5 ■ IBM DB2 UDB 8.1
Target system host platforms	The platform can be any one of the following: ■ Microsoft Windows 2000 Server (Oracle Database, Microsoft SQL Server) ■ Microsoft Windows NT Server (Sybase) ■ Microsoft Windows 2003 Server (IBM DB2 UDB)

Item	Requirement
External code	The external code consists of the following files: ■ `classes12.zip` (Oracle8*i* Database and Oracle9i Database) ■ `msbase.jar`, `mssqlserver.jar`, and `msutil.jar` (Microsoft SQL Server 2000) ■ `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.

Step 2: Configuring the Target System

All of the required configuration information (such as tablespace name, default database, user name, and password) is provided in the form of parameters that are used by Oracle Identity Manager. This information is required to perform the procedure described in the "Defining Resource Assets" section on page 2-7.

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

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

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`.

Configuring Microsoft SQL Server

You configure Microsoft SQL Server by ensuring that:

- The target database in which users are supposed 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`.

Configuring Sybase

You configure Sybase by ensuring that:

- The target database in which users are supposed 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 4: Copying the Connector Files" section on page 2-3 for instructions to copy these files from the installation media ZIP file to the *xellerate_home*\xellerate\XLIntegrations\DatabaseAccess\scripts directory.

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 systems, 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 systems, 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 systems, in the UD_Lookup.DB_Schemas lookup definition.

Step 3: Configuring the Oracle Identity Manager Server

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 the users that are present in the operating system (Microsoft Windows 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 Access connector to provision accounts in IBM DB2 UDB, then you must first deploy the connector for Microsoft Active Directory in the following directory:

xellerate_home\xellerate\XLIntegrations\ActiveDirectory

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

Step 4: Copying the Connector Files

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

Note: The directory paths given in the first column of this table correspond to the location of the connector files in the following ZIP file on the installation media:

`Database Servers\Database User Management\Database Rev 3.1.0.zip`

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

File in the Installation Media Directory	Destination Directory
The following files in the `xml` directory: ■ `xliDBAccessLogin_DM.xml` ■ `xliDBAccessUser_DM.xml` ■ `xliDBAccessScheduleTask_DM.xml`	*`xellerate_home`*`\xellerate\XLIntegrations\DatabaseAccess\xml`
`lib\xliDatabaseAccess.jar`	*`xellerate_home`*`\xellerate\JavaTasks`
`lib\xliDatabaseAccess.jar`	*`xellerate_home`*`\xellerate\ScheduleTask`
The following files in the `scripts` directory: ■ `procGrantAllToUser.sql` ■ `procRevokeAllFromUser.sql`	*`xellerate_home`*`\xellerate\XLIntegrations\DatabaseAccess\scripts`

The following contents of the `docs` directory:
`B31114_01.pdf`
`html`
	`xellerate_home``\xellerate\XLIntegrations\DatabaseAccess\docs`

Step 5: Copying External Code

The location of the external code files depends on the database of the target database system. The following sections provide information that is specific to the target system database:

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

Copying External Code Files on Oracle Database

For connectors used with Oracle8*i* Database or Oracle9*i* Database, the required external JAR file required is `classes12.jar`.

The `classes12.jar` file is available in the Oracle9*i* Database installation at the following path:

`oracle_home``\ora92\jdbc\lib\`

In this directory path, *`oracle_home`* is the location where Oracle9*i* Database is installed. For example, `C:\Oracle`.

You must ensure that the `classes12.jar` file is in the following directory:

xellerate_home\xellerate\ThirdParty

If the classes12.zip file is used instead of the classes12.jar file, then:

- For JBoss Application Server:

  Copy the classes12.zip file to the *JBOSS_HOME*\server\default\lib directory, and then restart the server. Here, *JBOSS_HOME* is the directory in which JBoss is installed.

- For BEA WebLogic:

  Copy the classes12.zip file into the *xellerate_home*\xellerate\ThirdParty directory. Make an entry for the classes12.zip file in the classpath mentioned in the *BEA_HOME*\user_projects\domains*domain_name*\xlStartWLS.bat file, and then restart the server. Here, *BEA_HOME* is the directory in which JBoss is installed.

- For IBM WebSphere:

  Copy the classes12.zip file to the *WEBSPHERE_HOME*\AppServer\lib directory, and then restart the server.

Copying External Code Files on Microsoft SQL Server

For connectors used with Microsoft SQL Server 2000, the external JAR files required 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. Then, copy these files into the following directory:

xellerate_home\xellerate\ThirdParty

Using JBoss Application Server with Microsoft SQL Server

Copy the JDBC driver files (mssqlserver.jar, msbase.jar, and msutil.jar) into the *JBOSS_HOME*\server\default\lib directory, and then restart the server. Here, *JBOSS_HOME* is the directory in which JBoss is installed.

Using BEA WebLogic with Microsoft SQL Server

If you are using BEA WebLogic as the application server, then edit the xlStartWLS.cmd file to specify the location of the JDBC driver files. To do this:

1. Open the xlStartWLS.cmd file in a text editor.

   This file is in the following directory:

   WEBLOGIC_HOME\user_projects\domains*DOMAIN*_NAME\

   In this directory path, *WEBLOGIC_HOME* is the BEA WebLogic home directory, and *DOMAIN_NAME* is the name of the domain.

2. Add the following lines in the xlStartWLS.cmd file:

   ```
   SET SQL_DB_ACCESS_INT_JARS=xellerate_home\xellerate\ThirdParty\mssqlserver.jar;
   xellerate_home\xellerate\ThirdParty\msbase.jar;
   xellerate_home\xellerate\ThirdParty\msutil.jar;
   ```

   Append the following text to the start of the set classpath command:

   ```
   %SQL_DB_ACCESS_INT_JARS%;
   ```

Using IBM WebSphere with Microsoft SQL Server

Copy the JDBC driver files (`mssqlserver.jar`, `msbase.jar`, and `msutil.jar`) to the *`WEBSPHERE_HOME`*`\AppServer\lib\ext` directory.

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 to the *`xellerate_home`*`\xellerate\ThirdParty\` directory.

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 to one of the following directories:

- For JBoss Application Server:

  Copy the `db2java.zip` file to the *`JBOSS_HOME`*`\server\default\lib` directory, and then restart the server. Here, *`JBOSS_HOME`* is the directory in which JBoss is installed.

- For BEA WebLogic:

  Copy the `db2java.zip` file into the *`xellerate_home`*`\xellerate\ThirdParty` directory. Make an entry for the `classes12.zip` file in the classpath mentioned in the *`BEA_HOME`*`\user_projects\domains\domain_name\xlStartWLS.bat` file, and then restart the server. Here, *`BEA_HOME`* is the directory in which JBoss is installed.

- For IBM WebSphere:

  Copy the `db2java.zip` file to the *`WEBSPHERE_HOME`*`\AppServer\lib` directory, and then restart the server.

Step 6: 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 *`xellerate_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 `Oracle` IT resource is displayed.
8. Specify values for the parameters of the `OracleITResource` IT resource. Refer to the table in the "IT Resource Parameter Values for Oracle Database" section on page 2-8 for information about the values to be specified.

9. Click **Next.** The Provide IT Resource Instance Data page for the `Microsoft SQL Server 2000` IT resource is displayed.
10. Specify values for the parameters of the `Microsoft SQL Server 2000` IT resource. Refer to the table in the "IT Resource Parameter Values for Microsoft SQL Server" section on page 2-8 for information about the values to be specified.
11. Click **Next.** The Provide IT Resource Instance Data page for the `Sybase Server` IT resource is displayed.
12. Specify values for the parameters of the `Sybase Server` IT resource. Refer to the table in the "IT Resource Parameter Values for Sybase" section on page 2-8 for information about the values to be specified.
13. Click **Next.** The Provide IT Resource Instance Data page for the `IBM DB2 UDB` IT resource is displayed.
14. Specify values for the parameters of the `IBM DB2 UDB` IT resource. Refer to the table in the "IT Resource Parameter Values for IBM DB2 UDB" section on page 2-8 for information about the values to be specified.
15. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `Database` IT resource type is displayed.
16. 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.

17. 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. You must remove these nodes. To do this, right-click each such node and then select **Remove.**
18. Click **Import**. The connector file is imported into Oracle Identity Manager.
19. Perform the same procedure to import the `xliDBAccessUser_DM.xml` file, which is in the *`xellerate_home`*`\xellerate\XLIntegrations\DatabaseAccess\xml\` directory.

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

20. Perform the same procedure to import the `xliDBAccessScheduleTask_DM.xml` file, which is in the *`xellerate_home`*`\xellerate\XLIntegrations\DatabaseAccess\xml\` directory.

Defining Resource Assets

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

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

- IT Resource Parameter Values for IBM DB2 UDB

IT Resource Parameter Values for Oracle Database

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

Parameter Name	Parameter Description
`DataBaseType`	Type of database Value: `Oracle`
`DatabaseName`	Name of the target database on which the users are created Sample value: `xeldb`
`Driver`	JDBC driver class Value: `oracle.jdbc.driver.OracleDriver`
`URL`	JDBC URL for the target database Value: `jdbc:oracle:thin:@host_IP:1521:Database_Name` Sample value: `jdbc:oracle:thin:@10.1.1.80:1521:xeltest`
`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`

IT Resource Parameter Values for Microsoft SQL Server

You must specify values for the `Microsoft SQL Server 2000` IT resource parameters listed in the following table.

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

Parameter Name	Parameter Description
URL	JDBC URL for the target database 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 the 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

IT Resource Parameter Values for Sybase

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

Parameter Name	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 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
Password	Password of the DBA login that is used to create users Value: sa

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 Name	Parameter Description
`DataBaseType`	Type of RDBMS Value: DB2
`DatabaseName`	Not required
`Driver`	JDBC driver class Value: `COM.ibm.db2.jdbc.net.DB2Driver`

`URL`	The JDBC URL for the target database
	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 the host name.

`UserID`	User name of the DB login used to create users Value: sa
`Password`	Not needed

Step 7: Configuring Reconciliation

Configuring reconciliation involves creating scheduled tasks for Lookup Fields and User reconciliations. To create 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 tasks are displayed on two different tabs.
5. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager should attempt to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.
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 appropriate table in 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.
11. Repeat Step 5 through 11 to create the second scheduled task.

After you create both scheduled tasks, proceed to the "Step 8: Compiling Adapters" section on page 2-11.

Specifying Values for the Scheduled Task Attributes

The following table describes the required attributes for the relevant scheduled task on the Task Scheduler form.

Attribute Name	Description	Sample Value
`Server`	Name of the IT resource	`OracleITResource`
`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	`Xellerate User`
`DB2DBName`	Name of the IBM DB2 UDB target database from where data is reconciled This attribute is required only for IBM DB2 UDB databases.	`TESTDB`

Step 8: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file. You must compile these adapters before you can use them to provision accounts on the target system.

- `DB Revoke Role`
- `DB Modify Password`
- `DB Modify Login`
- `DB Enable login`
- `DB Disable login`
- `adpDBDELETETABLESPACE`
- `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

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 the **Compile All** option.

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

   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 adapters that you specify.

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.

   Note: To compile multiple adapters simultaneously, use the Adapter Manager form. To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about how to use these forms.

3

Known Issues

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

When the connector is used with Microsoft SQL Server 2000 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.

Index