Oracle® Identity Manager

Connector Guide for Database User Management

Release 9.0.4

E10425-10

September 2014

ORACLE

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

E10425-10

Primary Author: Gowri.G.R

Contributing Authors: Debapriya Datta, Alankrita Prakash, Deena Purushothaman

Contents

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Database User Management.

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

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

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

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

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

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in 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 9.0.4.5.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

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

Software Updates

The following sections discuss software updates:

- Software Updates in Release 9.0.4.1
- Software Updates in Release 9.0.4.1_6728658
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.5

Software Updates in Release 9.0.4.1

The following are software updates in release 9.0.4.1:

- Trusted Source Reconciliation
- Separate Scheduled Tasks for Trusted Source and Target Resource Reconciliation
- Timeout Support
- Partial Reconciliation
- Specifying the Number of Records to Be Reconciled
- Enabling Logging
- Secure Connection to the Oracle Database
- Testing Utility

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 Source and Target Resource Reconciliation

In this release of the connector, there are separate user reconciliation scheduled tasks for trusted source and target resource 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 "IT Resources" section on page 2-10, 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 "Partial Reconciliation" section 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 2-18, 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 "IT Resources" section on page 2-10.

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 on the Installation Media
- Copying the Connector Files
- Chapter 4, "Testing Connector Functionality"

Software Updates in Release 9.0.4.1_6728658

The following table describes issues resolved in release 9.0.4.1_6728658:

Bug Number	Issue	Resolution
6974826	On the Oracle Database target system, a Create User provisioning operation failed if the target system did not contain a temporary tablespace named TEMP. The "The task was rejected by ORA - 959" error message was displayed as the outcome of the provisioning operation.	You can now perform a Create User provisioning operation on the Oracle Database target system even if there is no temporary tablespace named `TEMP` on the target system. The default temporary tablespace of the target system is used to provision the user.
6371580 and 6488890	On Oracle Database, the minimum permissions to be assigned to the target system user account for performing connector operations was not known. You had to create and use an administrator-level user account for connector operations.	For this target system, a script to create the target system user account has been shipped along with the connector installation package. When you run the script, the target system user account is created and the minimum required permissions are automatically assigned to the user account. See "Configuring Oracle Database" for information about this script.
6438096	For the Microsoft SQL Server target system, the UD_Lookup.DB_Dbnames-sql lookup definition had to be manually updated with names of databases on the target system installation.	The DBAccessLookupReconTask lookup reconciliation scheduled task has been provided to automate updating of the database names in the UD_Lookup.DB_SQL_DBNames lookup definition. You can use the Exclusion List attribute of this scheduled task to specify the database names that must not be included in the reconciliation process.
6468961	Logging conventions were not consistent across target systems.	The logging functionality has been enhanced and made consistent.
6603690	There was a requirement for enhancement in the organization of process forms used for User and Login accounts.	See the information given after this table about changes made in the connector.
6617547	The status of the Create User process task remained at Rejected when the user could not be created on the target system. This is expected behavior. However, you could perform an Update Password provisioning operation on the user.	This has been resolved. If the user is not created on the target system, then you cannot perform Update User provisioning operations on the user through Oracle Identity Manager.
6624875	On Oracle Database, users in the Locked state could not be detected during a reconciliation run.	This issue has been resolved. You can now use the ReconcileLockedUser scheduled task attribute to specify whether or not you want target system user who are in the Locked state to be reconciled during a reconciliation run.
6639559	During a target resource reconciliation run, the resource object remained in the Provisioning state even after the reconciliation event was successfully linked.	In the provisioning processes, the response mapping for the Reconciliation Update Received task has been modified. For the "Event Processed" response code, the "C" (Completed) status code has been mapped to the "Provisioned" object status.
5496483	During a target resource reconciliation run on Microsoft SQL Server or Sybase, multiple user IDs were generated for users who belonged to two or more databases on the target system installation.	In the process definition for Microsoft SQL Server Users and Sybase Users, the "Database Name" field has been made a key field along with Parent Login Name and Username. That is, a composite key field is used.

Bug Number	Issue	Resolution
5505785	The Authentication Type field is a required parameter for creating a login account. However, this field was not a mandatory field on the process form. Provisioning failed if you did not enter a value in this field on the process form.	This issue has been resolved. See the information given after this table about changes made in the connector.
5582717	If you tried to change the login or user name through a provisioning operation, then the operation would always fail.	The Update Login and Update User provisioning operations are not supported. If you try to perform these operations, then an appropriate message is displayed.
6279025	If the max_retry IT resource parameter was left blank, then the `numberformatexception` exception was thrown during reconciliation and provisioning.	This issue has been resolved. If you do not specify values for the `max_retry` and `delay_retry` parameters while configuring the IT resource, then default values are used for these parameters during reconciliation and provisioning.
6455965	Microsoft SQL Server, Oracle Database, and Sybase do not support Enable/Disable User operations. If you performed the Enable or Disable provisioning operation on any of these target systems, the state of the resource in Oracle Identity Manager remained at "Provisioning."	The Enable/Disable User provisioning operation is supported only for IBM DB2 UDB. If you try to perform these provisioning operations on any of the other target systems, then a message stating that the operation is not supported is displayed.

The following resource objects replace the resource objects used in release 9.0.4.1:

- Database Access Oracle User RO: This resource object is equivalent to the login account on the target system.
- Database Access DB2UDB User RO: This resource object is equivalent to the login account on the target system.
- Database Access SQLServer Login RO: This resource object is equivalent to the login account on the target system.
- Database Access SQLServer User RO: This resource object is equivalent to the user account on the target system. A Microsoft SQL Server login can have one user account for each database. The number of users for a login depends on the number of databases on which the users are created.
- Database Access Sybase Login RO: This resource object is equivalent to the login account on the target system.
- Database Access Sybase User RO: This resource object is equivalent to the user account on the target system. A Sybase login can have one user account for each database. The number of users for a login depends on the number of databases on which the users are created.

Note: On Microsoft SQL Server and Sybase, user accounts are child elements of login accounts. However, Oracle Identity Manager does not maintain this relationship between the login and user account for the same user. In other words, Oracle Identity Manager treats the login and user resource as independent resources.

The following is a summary of the changes that have been made in the connector object definitions:

Connector Object	IBM DB2 UDB	Microsoft SQL Server	Oracle Database	Sybase
Resource objects	Database Access DB2UDB User RO	Database Access SQLServer Login RO	Database Access Oracle User RO	Database Access Sybase Login RO
		Database Access SQLServer User RO		Database Access Sybase User RO
Process forms	UD_DB_DB2_U (parent form for User entity)	UD_DB_SQL_L (parent form for Login entity)	UD_DB_ORA_U (parent form for User entity)	UD_DB_SYB_L (parent form for Login entity)
	UD_DB_DB2_S (child form for schema)	UD_DB_SQL_U (parent form for User entity)	UD_DB_ ORA _R (child form for role)	UD_DB_SYB_R (child form for role)
	UD_DB_DB2_T (child form for tablespace)	UD_DB_SQL_R (child form for role)	UD_DB_ ORA _P (child form for privilege)	UD_DB_SYB_U (parent form for User entity)
Provisioning processes	Database Access DB2UDB User	Database Access MSSQL Login	Database Access Oracle User	Database Access Sybase Login
		Database Access MSSQL User		Database Access Sybase User

The following connector objects are the same for all the target systems:

- Adapters
- IT resource type
- Definition of the user reconciliation scheduled task
- Definition of the lookup reconciliation scheduled task

Definitions of the connector objects are in the following XML files:

- For IBM DB2 UDB, the connector object definitions are in the `xliDBAccessLogin_DM Nontrusted.xml` file.
- For Microsoft SQL Server, the connector object definitions are in the `xliDBAccessLogin_DM Nontrusted.xml` and `xliDBAccessUser_DM Nontrusted.xml` files.
- For Oracle Database, the connector object definitions are in the `xliDBAccessLogin_DM Nontrusted.xml` file.
- For Sybase, the connector object definitions are in the `xliDBAccessLogin_DM Nontrusted.xml` and `xliDBAccessUser_DM Nontrusted.xml` files.

Software Updates in Release 9.0.4.2

The following software updates have been made in release 9.0.4.2:

- Using the Connector Installer
- Resolved Issues

Using the Connector Installer

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

See "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-6 for details.

Resolved Issues

The following are issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
7355039	The change in the Oracle Identity Manager objects delivered through patch number 9.0.4.1_6728658 were not reflected in the resource bundle of the connector.	This issue has been resolved. The resource bundle keys for both English and Non-English languages have been modified based on the new user configurations.

Software Updates in Release 9.0.4.3

The following is an issue resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
8206597	If the target system was Microsoft SQL Server 2000, then the following error was encountered during reconciliation: `Column index 7 is out of range`	This issue has been resolved. The error is not encountered during reconciliation with a Microsoft SQL Server 2000 database.

Software Updates in Release 9.0.4.4

The following are software updates in release 9.0.4.4:

Sybase Adaptive Server Enterprise 15.x Added to the List of Certified Target Systems

From this release onward, Sybase Adaptive Server Enterprise 15.x has been added to the list of certified target systems. This has been mentioned in the Verifying Deployment Requirements section.

Resolved Issues in Release 9.0.4.4

The following is an issue resolved in release 9.0.4.4:

Bug Number	Issue	Resolution
8211696	Reconciliation failed on Sybase.	This issue has been resolved. Reconciliation can be performed with a Sybase database.

Software Updates in Release 9.0.4.5

The following are software updates in release 9.0.4.5:

Support for the Update Tablespace Provisioning Operation

The Update Tablespace provisioning operation is supported from this release onward.

Resolved Issues in Release 9.0.4.5

The following is an issue resolved in release 9.0.4.5:

Bug Number	Issue	Resolution
7346730	Suppose a user with a single role assigned was reconciled from the target system. If this role was revoked from the user on the target system, then the role was not revoked from the user on Oracle Identity Manager during the next reconciliation run.	This issue has been resolved. The role is now revoked at the end of the next reconciliation run.
7233670	The following issue was observed during target resource reconciliation of login accounts: Even when you specified a database name as the value of the DBName attribute of the scheduled task, reconciliation was run on all databases.	This issue has been resolved. The DBName attribute is automatically applied during reconciliation.
8274800	If the target system was Microsoft SQL Server, then the Login Name and Record Size attributes of the scheduled task did not work correctly.	This issue has been resolved. The Login Name and Record Size attributes work on all certified target systems.
8284824	The following issue was observed on Oracle Database target systems: If you entered a value in the Username field in lowercase or mixed case characters, then the user had to use the following format to log in to the target system: `sqlplus "username"/password`	This issue has been resolved. The user can use the usual `sqlplus username/password` format, regardless of the case in which the Username value is specified.
7716122	The ReconcileLockedUser attribute of the scheduled task could not be used to reconcile users whose status was `EXPIRED & LOCKED`.	This issue has been resolved. The ReconcileLockedUser attribute can be used to reconcile users whose status is `LOCKED` or `EXPIRED & LOCKED`.
8274794	The Update Group provisioning operation did not work correctly.	This issue has been resolved. The Update Group provisioning operation works as expected.
7409831	The status of a resource was changed to `Provisioning` even after a task was rejected.	For all tasks other than the Create User task, the status of a provisioned resource does not change to `Provisioning` even if a task is rejected.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

Documentation-Specific Updates in Release 9.0.4.5

The following is a documentation-specific update in revision "10" of release 9.0.4.5:

- Section 2.1, "Verifying Deployment Requirements" has been removed and all the contents of this section have been moved to Section 1.1, "Certified Components" in order to make it consistent with other connector guides.

The following is a documentation-specific update in revision "09" of release 9.0.4.5:

- The "Usage Recommendation" section has been added.

The following are documentation-specific updates in earlier revisions of release 9.0.4.5:

- The following changes have been made to the list of supported functions in the "Database Access Entity: Login Provisioning" section:
  - The Account Status Updated provisioning function has been removed.
  - The Default Tablespace Updated provisioning function has been added.
  - The Account Status reconciliation event has been added.
- In the table given in "Testing Connector Functionality" chapter, the value of the Authentication_Type attribute has been changed from `isSqlAuth` to `SQL_SERVER_AUTHENTICATION`.
- The following item has been removed from the "Known Issues" chapter:
  - Bug 7300590

    On Microsoft SQL Server, you cannot use the testing utility to test the Delete User provisioning operation.
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target Systems" row.
- Oracle8*i* Database is no longer a supported target system version. All occurrences of "Oracle8*i* Database" have been removed from this guide.
- From this release onward:

  The minimum certified release of Oracle Identity Manager is release 9.1.0.1.

  The minimum certified release of JDK is release 1.4.2.

  See "Verifying Deployment Requirements" section for the complete listing of certified components.

Documentation-Specific Updates in Release 9.0.4.4

The following are documentation-specific updates in release 9.0.4.4:

- The Default Role attribute is not provisioned or reconciled. This attribute has been removed from the following sections:

  Database Access Entity: Login Provisioning

  Database Access Entity: Login Provisioning
- Bug 8424404 has been added in the "Known Issues" chapter.

Documentation-Specific Updates in Release 9.0.4.3

In the "Known Issues" chapter:

- Items that are not related to limitations of the connector have been removed.
- Bug numbers have been added for the remaining items.
- Issues related to Bugs 8274794 and 8274800 have been added.

Documentation-Specific Updates in Release 9.0.4.2

There are no documentation-specific updates in release 9.0.4.2.

Documentation-Specific Updates in Release 9.0.4.1_6728658

There are no documentation-specific updates in release 9.0.4.1_6728658.

Documentation-Specific Updates in Release 9.0.4.1

Major changes have been made to the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of information provided by the guide.

1

About the Connector

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

This connector supports IBM DB2 UDB, Microsoft SQL Server, Oracle Database, and Sybase target systems.

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

- Login: A login entity is used for authentication purposes.
- User: A user entity is used for authorization or access control purposes.

Microsoft SQL Server and Sybase treat these entities as parent (Login) and child (User) elements. However, in Oracle Identity Manager, these entities are treated as separate, independent entities. In other words, the connector provides login provisioning as well as user provisioning features in both Microsoft SQL Server and Sybase.

In Oracle Database and IBM DB2 UDB, the Login and User entities are treated as a single entity. In this guide, that entity is referred to as the Login entity.

This chapter contains the following sections:

Note: In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.

At some places in this guide, Database User Management has been referred to as the *target system*.

1.1 Certified Components

Table 1–1 lists the certified components for this connector.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager Release 9.1.0.1 and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector supports.
Target systems	The target system can be any one of the following: ■ IBM DB2/UDB Version 8.1, 9.1 ■ Microsoft SQL Server 2000 with SP4 or later service packs In Microsoft SQL Server 2000 to which SP4 has not been applied, network access is denied even if the TCP/IP port is enabled. Therefore, if SP4 is not applied, then the connector will not be able to connect to the target system because the connector uses a TCP/IP port to connect. ■ Microsoft SQL Server 2005 ■ Oracle9*i* Database ■ Oracle Database 10*g* ■ Sybase Adaptive Server Enterprise 12.5, 15.x
External code	The external code consists of the following files: ■ `ojdbc14.jar` (Oracle9*i* 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 and 15.x) ■ `db2jcc.jar` and `db2jcc_license_cu.jar` (IBM DB2/UDB) **Note:** These JAR files are available in the corresponding database installation directories.
Target system user account	Depending on the target system, one of the following user account is required to configure the target system: ■ For Oracle Database: `sys` as `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 2003 Server (Domain Controller) Administrator account must be used.
JDK	JDK 1.4.2

1.2 Usage Recommendation

Depending on the Oracle Identity Manager version that you are using, you must deploy and use one of the following connectors:

- If you are using an Oracle Identity Manager release that is 9.1.0.1 or later and earlier than Oracle Identity Manager Release 9.1.0.2 BP08, then use the 9.0.4.*x* version of this connector.
- If you are using Oracle Identity Manager Release 9.1.0.2 BP08 or later and earlier than Oracle Identity Manager 11*g* Release 1 PS1 BP03 (11.1.1.5.3), then use the latest 9.1.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 PS1 BP03 (11.1.1.5.3) or later, or Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) or later, then use the latest 11.1.1.*x* version of this connector.

1.3 Reconciliation Module

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

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

The following table lists the target system Login entity attributes whose values are read from the database during target resource reconciliation:

Target System Login Attribute	IBM DB2 UDB	Microsoft SQL Server	Oracle Database	Sybase
Login Name (for Microsoft SQL Server and Sybase) Username (for Oracle Database and IBM DB2 UDB)	Yes	Yes	Yes	Yes
userType	Yes	-	-	-
Full Name	-	-	-	Yes
Default Tablespace	-	-	Yes	-
Temporary Tablespace	-	-	Yes	-
Account Status	-	-	Yes	-
Profile	-	-	Yes	-
dbName	Yes	-	-	-
Default Database	-	Yes	-	Yes
Default Language	-	Yes	-	Yes
Roles **Note:** This is a multivalued attribute.	-	-	Yes	Yes
Privileges **Note:** This is a multivalued attribute.	-	-	Yes	-

Target System Login Attribute	IBM DB2 UDB	Microsoft SQL Server	Oracle Database	Sybase
Schema Names **Note:** This is a multivalued attribute.	Yes	-	-	-
Tablespace Names **Note:** This is a multivalued attribute.	Yes	-	-	-

The following table lists the target system User entity attributes whose values are read from the database during target resource reconciliation:

Target System User Attribute	Microsoft SQL Server	Sybase
User	Yes	Yes
Group	-	Yes
Database	Yes	Yes
Roles **Note:** This is a multivalued attribute.	Yes	-

1.3.1 Reconciled Xellerate User (OIM User) Fields

The following Xellerate User (OIM User) fields are reconciled only if trusted source reconciliation is implemented:

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

1.4 Provisioning Module

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

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

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

> **See Also:** The "Supported Functionality" section on page 1-6 for information about the difference between these entities

- Database Access Entity: Login Provisioning

- Database Access Entity: User Provisioning

1.4.1 Database Access Entity: Login Provisioning

Note: Information in this section is applicable to all four supported target systems.

The following target system attributes are provisioned.

Target System Login/User Attribute	IBM DB2 UDB	Microsoft SQL Server	Oracle Database	Sybase
Login Name (for Microsoft SQL Server and Sybase) Username (for Oracle Database and IBM DB2 UDB)	Yes	Yes	Yes	Yes
Password	Yes	Yes	Yes	Yes
Default Database	-	Yes **Note:** If the target system is Microsoft SQL Server 2000, then you must select the default database during provisioning.	-	Yes
Default Language	-	Yes	-	Yes
Full Name	-	-	-	Yes
Authentication Type	-	Yes	-	-
Default Tablespace	-	-	Yes	-
Temporary Tablespace	-	-	Yes	-
Quota	-	-	Yes	-
Database	Yes	-	-	-
User Type	Yes	-	-	-
Profile	-	-	Yes	-
Account Status	-	-	Yes	-
Roles **Note:** This is a multivalued attribute.	-	-	Yes	Yes
Tablespace Names **Note:** This is a multivalued attribute.	Yes	-	-	-
Schema Names **Note:** This is a multivalued attribute.	Yes	-	-	-
Privileges **Note:** This is a multivalued attribute.	-	-	Yes	-

1.4.2 Database Access Entity: User Provisioning

Note: Information in this section is applicable to Microsoft SQL Server and Sybase target systems.

The following target system attributes are provisioned.

Target System User Attribute	Microsoft SQL Server	Sybase
User	Yes	Yes
Database Name	Yes	Yes
Database Group	-	Yes
Parent Login	Yes	Yes
Authentication Type	Yes	-
Roles	Yes	-

Note: This is a multivalued attribute.

1.5 Supported Functionality

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 Provisioning
- Database Access Entity: User Provisioning

1.5.1 Database Access Entity: Login Provisioning

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

Note: Information in this section is applicable to all four supported target systems. The Supported on column of the table lists the target systems on which the functions are supported.

Function	Type	Description	Supported on
Create Login	Provisioning	Creates a login in the database **Note:** Running this provisioning operation on Oracle Database would result in the creation of a user, but would not grant any privileges to the user. In other words, the provisioned user would not be able to log in to the database. To provide the minimum required privileges to the provisioned user, run the Add Role or Grant Privilege provisioning operation with the values CONNECT, RESOURCE, and SELECT ANY TABLE. For more information, refer to the description of the Add Role or Grant function in this table.	All
Delete Login	Provisioning	Deletes a provisioned login	All

Function	Type	Description	Supported on
Enable Login	Provisioning	Enables a disabled login	IBM DB2 UDB and Oracle Database
Disable Login	Provisioning	Disables a login	IBM DB2 UDB and Oracle Database
Default Database Updated	Provisioning	Updates the properties of a login in the database according to a change in the Default Database attribute You must configure scheduled tasks to reconcile target system values for populating the following lookup definitions: ■ **UD_Lookup.DB_SQL_DBNames:** To fetch values from Microsoft SQL Server and copy them into this lookup definition, configure the `DBAccessLookupReconTask` scheduled task. See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information. ■ **UD_Lookup.DB_Sybase_Databases:** To populate this lookup definition, you must add lookup codes corresponding to database names in the target system.	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
Default Language Updated	Provisioning	Updates the properties of a login in the database according to a change in the Default Language attribute You must configure scheduled tasks to reconcile target system values for populating the following lookup definitions: ■ **UD_Lookup.DB_SQL_DefaultLang:** To fetch values from Microsoft SQL Server and copy them into this lookup definition, configure the `DBAccessLookupReconTask` scheduled task. See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information. ■ **UD_Lookup.DB_Sybase_DefaultLang:** To populate this lookup definition, you must add lookup codes corresponding to supported languages in the target system.	Microsoft SQL Server and Sybase
Password Updated	Provisioning	Updates the properties of a login in the database according to a change in the Password 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	Add roles to an existing login in the database The required role must be defined and valid in the target system. You must configure scheduled tasks to reconcile target system values for populating the following lookup definitions: ▪ **UD_Lookup.DB_ORA_Roles:** To fetch values from Oracle Database and copy them into this lookup definition, configure the `DBAccessLookupReconTask` scheduled task. See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information. ▪ **UD_Lookup.DB_Sybase_Roles:** To populate this lookup definition, you must add lookup codes corresponding to role names in the target system.	Oracle Database and Sybase
Revoke Role	Provisioning	Revokes a role from an existing login in the database	Oracle Database and Sybase
Add Tablespace	Provisioning	Add tablespaces to an existing login in the database To fetch values from IBM DB2 UDB and copy them into the `UD_Lookup.DB_DB2UDB_Tablespaces` lookup definition, configure the `DBAccessLookupReconTask` scheduled task. See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information.	IBM DB2 UDB
Delete Tablespace	Provisioning	Revokes a tablespace from an existing login in the database	IBM DB2 UDB
Add Schema	Provisioning	Add schemas to an existing login in the database To fetch values from IBM DB2 UDB and copy them into the `UD_Lookup.DB_DB2UDB_Schema` lookup definition, configure the `DBAccessLookupReconTask` scheduled task. See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information.	IBM DB2 UDB
Delete Schema	Provisioning	Revokes a schema from an existing login in the database	IBM DB2 UDB
Add Privileges	Provisioning	Adds or grants privileges to an existing login in the database To fetch values from Oracle Database and copy them into the `UD_Lookup.DB_ORA_Privileges` lookup definition, configure the `DBAccessLookupReconTask` scheduled task. See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information.	Oracle Database
Revoke Privilege	Provisioning	Revokes a privilege from an existing login in the database	Oracle Database
Profile Name Updated	Provisioning	Updates the properties of a login in the database according to a change in the profile name attribute To fetch values from Oracle Database and copy them into the `UD_Lookup.DB_ORA_Profiles` lookup definition, configure the `DBAccessLookupReconTask` scheduled task. See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information.	Oracle Database

Function	Type	Description	Supported on
Default Tablespace Updated	Provisioning	Updates the properties of a login in the database according to a change in the Default Tablespace attribute.	Oracle Database
Trusted Reconciliation for Login	Reconciliation	Creates Xellerate Users (OIM Users) corresponding to reconciled logins from the database	All
Target Resource Reconciliation for Login	Reconciliation	Reconciles login data from the target system to Oracle Identity Manager This data is used to create or update target system resources (accounts) assigned to OIM Users	All
Account Status	Reconciliation	Reconciles account status data from the target system to Oracle Identity Manager	Oracle Database

1.5.2 Database Access Entity: User Provisioning

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 creating a user, you must provide the required value in the Database Name field. You must configure scheduled tasks to reconcile target system values for populating the following lookup definitions: ■ **UD_Lookup.DB_SQL_DBNames:** To fetch values from Microsoft SQL Server and copy them into this lookup definition, configure the `DBAccessLookupReconTask` scheduled task. See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information. ■ **UD_Lookup.DB_Sybase_Databases:** To populate this lookup definition, you must add lookup codes corresponding to database names in the target system.	Both
Delete User	Provisioning	Deletes a provisioned user corresponding to an existing login in the database You can run this function (provisioning operation) 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

Function	Type	Description	Supported on
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
Database Group Updated	Provisioning	Updates the configuration of a user in the database according to a change in the Database Group attribute **Microsoft SQL Server** Groups in Oracle Identity Manager are the same as roles in Microsoft SQL Server. To fetch values from the Microsoft SQL Server lookup field and copy them into this lookup definition, configure the `DBAccessLookupReconTask` scheduled task. **Note:** In this release, the Update Database Group provisioning operation is not supported on Microsoft SQL Server. This point is also mentioned under Bug 8274794 in the "Known Issues" chapter. **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 `UD_Lookup.DB_Sybase_DBGroups` lookup definition. 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`	Both
Add Role	Provisioning	Add roles to an existing user in the database To fetch values from Microsoft SQL Server and copy them into the `UD_Lookup.DB_SQL_DBRoles` lookup definition, configure the `DBAccessLookupReconTask` scheduled task.	Microsoft SQL Server
Revoke Role	Provisioning	Revokes a role from an existing user in the database	Microsoft SQL Server
Target Resource Reconciliation for User	Reconciliation	Reconciles user data from the target system to Oracle Identity Manager This data is used to create or update target system resources provisioned to OIM Users. There is no separate scheduled task for user entity reconciliation. User entities are reconciled along with logins when the login reconciliation scheduled task for Microsoft SQL Server and Sybase is run. **Note:** Trusted source reconciliation is supported only for logins in Microsoft SQL Server and Sybase. Users in these target systems cannot be reconciled as OIM Users.	Both

1.6 Multilanguage Support

The connector supports the following languages:

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

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

1.7 Files and Directories on the Installation Media

The files and directories on the installation media are listed in Table 1–2.

Table 1–2 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
`configuration/DatabaseAccess-CI.xml`	This XML file contains configuration information that is used during connector installation.
`lib/xliDatabaseAccess.jar`	This file contains the class files required for performing provisioning and reconciliation. During connector deployment, this file is copied into the following directories: *OIM_HOME*`/xellerate/JavaTasks` *OIM_HOME*`/xellerate/ScheduleTask`
Files in the `resources` directory	Each of these resource bundles contains language-specific information that is used by the connector. There are two resource bundles for a particular language, one for each database access entity (Login and User). During connector deployment, these resource bundles are copied into the following directory: *OIM_HOME*`/xellerate/connectorResources` **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
`scripts/procGrantAllToUser.sql`	This file contains the stored procedures that create and grant the required roles to the Sybase user for connector operations. See "Configuring Sybase" for information about using this file.

Table 1–2 (Cont.) Files and Directories On the Installation Media

File in the Installation Media Directory	Description
`scripts/procRevokeAllFromUser.sql`	This file contains the stored procedures that revoke the roles granted to the Sybase user for connector operations. See "Configuring Sybase" for information about using this file.
`scripts/OimUser.sql`	This file contains SQL commands to create an Oracle Database user for connector operations.
`scripts/OimUserGrants.sql`	This file contains SQL commands that grants the required roles to the Oracle Database user for connector operations.
`scripts/OIM.bat`	On Microsoft Windows platforms, this BAT file is to be used to create the IT resource user for Oracle Database. When you run this BAT file, it calls the `OimUser.sql` and `OimUserGrants.sql` files.
`scripts/OIM.sh`	On UNIX platforms, this script file is to be used to create the IT resource user for Oracle Database. When you run this script file, it calls the `OimUser.sql` and `OimUserGrants.sql` files.
`config/LookUpQuery.properties`	This file contains the lists of lookup fields that can be reconciled by using the `DBAccessLookupReconTask` scheduled task. Each lookup field has a SQL command associated with it. The scheduled task uses the SQL command to fetch values from the target system fields and populate the corresponding lookup definitions in Oracle Identity Manager.
`test/config/config.properties`	This testing-utility 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 that are generated when you run the testing utility.
`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: ■ Common IT resource type ■ Process form for each login entity ■ Adapters ■ Process tasks for each login entity ■ Resource objects for each login entity ■ Provisioning Processes for each login entity
`xml/xliDBAccessUser_DM Nontrusted.xml`	This XML file contains definitions for the connector components related to Database Access (User) provisioning. These components include: ■ Common IT resource type ■ Process form for each user entity ■ Adapters ■ Process tasks for each user entity ■ Resource objects for each user entity ■ Provisioning Processes for each login entity
`xml/xelluserDbAccess Trusted.xml`	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

File in the Installation Media Directory	Description
configuration/DatabaseAccess-CI.xml	This XML file contains configuration information that is used during connector installation.
lib/xliDatabaseAccess.jar	This file contains the class files required for performing provisioning and reconciliation. During connector deployment, this file is copied into the following directories: *OIM_HOME*/xellerate/JavaTasks *OIM_HOME*/xellerate/ScheduleTask
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. There are two resource bundles for a particular language, one for each database access entity (Login and User). During connector deployment, these resource bundles are copied into the following directory: *OIM_HOME*/xellerate/connectorResources **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
scripts/procGrantAllToUser.sql	This file contains the stored procedures that create and grant the required roles to the Sybase user for connector operations. See "Configuring Sybase" for information about using this file.
scripts/procRevokeAllFromUser.sql	This file contains the stored procedures that revoke the roles granted to the Sybase user for connector operations. See "Configuring Sybase" for information about using this file.
scripts/OimUser.sql	This file contains SQL commands to create an Oracle Database user for connector operations.
scripts/OimUserGrants.sql	This file contains SQL commands that grants the required roles to the Oracle Database user for connector operations.
scripts/OIM.bat	On Microsoft Windows platforms, this BAT file is to be used to create the IT resource user for Oracle Database. When you run this BAT file, it calls the OimUser.sql and OimUserGrants.sql files.
scripts/OIM.sh	On UNIX platforms, this script file is to be used to create the IT resource user for Oracle Database. When you run this script file, it calls the OimUser.sql and OimUserGrants.sql files.
config/LookUpQuery.properties	This file contains the lists of lookup fields that can be reconciled by using the DBAccessLookupReconTask scheduled task. Each lookup field has a SQL command associated with it. The scheduled task uses the SQL command to fetch values from the target system fields and populate the corresponding lookup definitions in Oracle Identity Manager.
test/config/config.properties	This testing-utility 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 that are generated when you run the testing utility.
test/scripts/DBAccess.bat test/scripts/DBAccess.sh	This file is used to start the testing utility.

File in the Installation Media Directory	Description
xml/xliDBAccessLogin_DM Nontrusted.xml	This XML file contains definitions for the connector components related to Database Access (Login) provisioning. These components include: ■ Common IT resource type ■ Process form for each login entity ■ Adapters ■ Process tasks for each login entity ■ Resource objects for each login entity ■ Provisioning Processes for each login entity
xml/xliDBAccessUser_DM Nontrusted.xml	This XML file contains definitions for the connector components related to Database Access (User) provisioning. These components include: ■ Common IT resource type ■ Process form for each user entity ■ Adapters ■ Process tasks for each user entity ■ Resource objects for each user entity ■ Provisioning Processes for each login entity
xml/xelluserDbAccess Trusted.xml	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

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

1.8 Determining the Release Number of the Connector

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

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

   OIM_HOME/xellerate/JavaTasks/xliDatabaseAccess.jar

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.

2

Deploying the Connector

Deploying the connector involves the following steps:

- Configuring the Target System
- Using External Code Files
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
  - Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later
  - Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.1
- IT Resources
- Configuring the Oracle Identity Manager Server

2.1 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

2.1.1 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 to a login entity, 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_DB2UDB_DBName` lookup definition in Oracle Identity Manager.

Note:

- For tablespaces that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_DB2UDB_Tablespaces` lookup definition.
- For schemas that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_DB2UDB_Schema` lookup definition.

See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information.

2.1.2 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, the `sa/sa` account.
- For Microsoft SQL Server 2000 and 2005, ensure that:
  - The TCP/IP port is enabled. The default port is 1433.

    To enable the TCP/IP port:

    i. Open the Microsoft SQL Server Configuration Manager.

    ii. Click **SQL Server Network Configuration**.

    iii. Click **Protocols for MSSQLSERVER**.

    iv. In the right frame, right-click **TCP/IP** and then click **Enable**.
  - The TCP/IP port is not the only port enabled.
  - Mixed mode authentication is enabled.
  - The TCP/IP port is not blocked by a firewall.

Note:

- For a database that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_SQL_DBNames` lookup definition.
- For a language that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_SQL_DefaultLang` lookup definition.
- For a role that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_SQL_DBRoles` lookup definition.

See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information.

2.1.3 Configuring Oracle Database

To configure Oracle Database:

- Ensure that the service name used to create users exists in the target Oracle Database installation.
- Run one of the following scripts on the target system to create the target system user account for connector operations:
  - On Microsoft Windows platforms:

    OIM_HOME/XLIntegrations/DatabaseAccess/SQLScripts/OIM.bat

  - On UNIX platforms:

    OIM_HOME/XLIntegrations/DatabaseAccess/SQLScripts/OIM.sh

  When you run the script, the following privileges are granted to the user:

  - CREATE SESSION
  - CREATE USER
  - GRANT ANY PRIVILEGE
  - GRANT ANY ROLE
  - ALTER USER
  - DROP USER
  - SELECT ON DBA_ROLE_PRIVS
  - SELECT ON DBA_USERS
  - SELECT ON DBA_ROLES
  - SELECT ON DBA_TABLESPACES
  - SELECT ON DBA_PROFILES
  - SELECT ON DBA_PROFILES
  - SELECT ON DBA_SYS_PRIVS

– CREATE TABLE

You provide the credentials of this user account while configuring the IT resource. The procedure is described later in the guide.

Note:

- For a role that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_ORA_Roles` lookup definition.
- For a privilege that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_ORA_Privileges` lookup definition.
- For a profile that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_ORA_Profiles` lookup definition.
- For a default tablespace that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_ORA_Tablespaces` lookup definition.
- For a temporary tablespace that you want to provision to a user entity, configure the `DBAccessLookupReconTask` scheduled task in Oracle Identity Manager to populate the `UD_Lookup.DB_ORA_TempTablespaces` lookup definition.

See "Configuring the Reconciliation Scheduled Tasks for Lookup Fields" on page 3-6 for more information.

2.1.4 Configuring Sybase

You configure Sybase by ensuring that:

- The target database in which logins and users are to be created exists in the target Sybase ASE installation.
- The `procGrantAllToUser.sql` script is run on the target Sybase database. This file contains the stored procedures that create and grant the required roles to the Sybase user for connector operations.

  The `procRevokeAllFromUser.sql` script is run on the target Sybase database. This file contains the stored procedures that revoke roles from the Sybase user for connector operations.

  Refer to the "Copying the Connector Files" section on page 2-9 for instructions to copy these files from the connector installation package.

Note:

- For default databases that you want to provision to login entities, enter lookup codes corresponding to the databases that already exist on the target system in the `UD_Lookup.DB_Sybase_Databases` lookup definition.
- For default languages that you want to provision to login entities, enter lookup codes corresponding to the languages supported by the target system in the `UD_Lookup.DB_Sybase_DefaultLang` lookup definition.
- For roles that you want to provision to login entities, enter lookup codes corresponding to the roles defined on the target system in the `UD_Lookup.DB_Sybase_Roles` lookup definition.
- For database groups that you want to provision to user entities, enter lookup codes corresponding to the database groups on the target system in the `UD_Lookup.DB_Sybase_DBGroups` lookup definition.

See *Oracle Identity Manager Design Console Guide* for information about modifying lookup definitions.

2.2 Using External Code Files

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

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

2.2.1 Copying External Code Files for IBM DB2 UDB

For connectors used with IBM DB2 UDB, copy the `db2jcc.jar` and `db2jcc_license_cu.jar` files 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 "Importing the Connector XML Files" section on page 2-9.

2.2.2 Copying External Code Files for Microsoft SQL Server

For connectors used with Microsoft SQL Server 2000 target systems, 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 4 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 *OIM_HOME*`/xellerate/ThirdParty` directory.

2.2.3 Copying External Code Files for Oracle Database

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

If the connector is used with Oracle9*i* Database or Oracle Database 10*g*, then the required external code file is `ojdbc14.jar`.

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

ORACLE_HOME`/jdbc/lib`

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

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

Note: If you are using Oracle Identity Manager release 9.0.3.1 or later, then the `ojdbc14.jar` file is already present in the `ThirdParty` directory.

After you copy the external code file, proceed to the "Importing the Connector XML Files" section on page 2-9.

2.2.4 Copying External Code Files for 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.

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

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

Installing the connector on Oracle Identity Manager release 9.1.0 or later involves the following procedures:

- Running the Connector Installer
- Configuring the IT Resource

2.3.1 Running the Connector Installer

To run the Connector Installer:

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

   OIM_HOME/xellerate/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console*.
3. Click **Deployment Management**, and then click **Install Connector**.
4. From the Connector List list, select **Database Access *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

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

   a. In the **Alternative Directory** field, enter the full path and name of that directory.
   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
   c. From the Connector List list, select **Database Access *RELEASE_NUMBER***.
5. Click **Load**.
6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries
   b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see "Configuring the Target System As a Trusted Source" on page 3-2.
   c. Compilation of adapters

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

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.
7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

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

Note: At this stage, run the `PurgeCache` utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-17 for information about running the `PurgeCache` utility.

There are no prerequisites for some predefined connectors.

b. Configuring an IT resource for the connector

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

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

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

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 1–2.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the `connectorResources` directory into the corresponding directories on each node of the cluster. See Table 1–2 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.3.2 Configuring the IT Resource

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

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

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter the name of one of the following IT resources, and then click **Search**:
   - For IBM DB2 UDB, enter `DB2UDB`.
   - For Microsoft SQL Server, enter `MS SQL Server`.
   - For Oracle Database, enter `Oracle Database`.
   - For Sybase, enter `Sybase Server`.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.

7. Specify values for the parameters of the IT resource. Refer to "IT Resources" on page 2-10 for information about the parameters of the IT resource.
8. To save the values, click **Update**.

2.4 Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.1

Installing the connector on any Oracle Identity Manager release between releases 8.5.3.1 and 9.0.3.1 involves the following procedures:

- Copying the Connector Files
- Importing the Connector XML Files

2.4.1 Copying the Connector Files

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

> **See Also:** "Files and Directories on the Installation Media" on page 1-11 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/SQLScripts`
Files in the `config` directory	*OIM_HOME*`/xellerate/XLIntegrations/DatabaseAccess/config`
Files in the `test/config` directory	*OIM_HOME*`/xellerate/XLIntegrations/DatabaseAccess/config`
Files in the `test/scripts` directory	*OIM_HOME*`/xellerate/XLIntegrations/DatabaseAccess/scripts`
Files in the `xml` directory	*OIM_HOME*`/xellerate/XLIntegrations/DatabaseAccess/xml`

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

2.4.2 Importing the Connector XML Files

Definitions of the connector objects are in the following XML files:

- For IBM DB2 UDB, the connector object definitions are in the `xliDBAccessLogin_DM Nontrusted.xml` file.
- For Microsoft SQL Server, the connector object definitions are in the `xliDBAccessLogin_DM Nontrusted.xml` and `xliDBAccessUser_DM Nontrusted.xml` files.
- For Oracle Database, the connector object definitions are in the `xliDBAccessLogin_DM Nontrusted.xml` file.
- For Sybase, the connector object definitions are in the `xliDBAccessLogin_DM Nontrusted.xml` and `xliDBAccessUser_DM Nontrusted.xml` files.

To import the required 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 opening files is displayed.
4. Locate and open the `xliDBAccessLogin_DM Nontrusted.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 `Oracle Database` 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 "IT Resources" section on page 2-13 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 Administrative and User Console Guide* for instructions.

11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You *may* see a cross-shaped icon along with some nodes. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.
12. Click **Import**. The connector file is imported into Oracle Identity Manager.
13. If you use Microsoft SQL Server or Sybase, then import the `xliDBAccessUser_DM Nontrusted.xml` file by performing Steps 3 through 12.

2.5 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

2.5.1 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`*`:`*`Port_Number`*`/`*`DatabaseName`* Sample value: `jdbc:db2://10.1.1.127:6789/TESTDB` **Note:** Use the IP address, not the computer name or host name. 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 database is installed. You cannot specify the host name of the computer as the value of the URL parameter.
`UserID`	User name of the DBA login that is used to create, update, and delete users Sample value: `db2admin`
`Password`	Password of the DBA login that is used to create, update, and delete users
`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 `No`. **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: `3`
`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.

2.5.2 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`

`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
	Format:
	`jdbc:microsoft:sqlserver://`*`Target_Host`*`:`*`Port_number`*`;DatabaseName=`*`DatabaseNam e`*
	
	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
	Format:
	`jdbc:sqlserver://`*`serverName`*`;`*`instanceName`*`:`*`portNumber`*`;`*`property=value`*`[;`*`propert y=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, update, and delete users Sample value: `sa`
`Password`	Password of the DBA login that is used to create users
`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.

Parameter	Description
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 No. **Note:** This feature is supported only on Oracle Database.
max_retry	Number of times that the connector must retry connecting to the target server, if the connection fails Default value: 3
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.

2.5.3 IT Resource Parameter Values for Oracle Database

You must specify values for the Oracle Database 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 (for Oracle Database 10*g* and later) URL value: `jdbc:oracle:thin:@//Oraclehost.domain:Oracleportnumber/Oracleservicename` Sample value: `jdbc:oracle:thin:@//host1.examplewidgets.com:1521/srvce1` ■ Multiple database instances support one service URL value: `jdbc:oracle:thin:@(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:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=host1.examplewidgets.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host2.examplewidgets.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host3.examplewidgets.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host4.examplewidgets.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.examplewidgets:1521:srvce1`
UserID	User name of the Oracle Database user account that is used to create, update, and delete users See "Configuring Oracle Database" on page 2-3 for information about creating this user account.
Password	Password of the Oracle Database user account that is used to create, update, and delete users
Target Locale: Country	Country code Default value: US **Note:** You must specify the value in uppercase.

Parameter	Description
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 No.
max_retry	Number of times that the connector must retry connecting to the target server, if the connection fails Default value: 3
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.

2.5.4 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.) Format: jdbc:sybase:Tds:*Target_Host*:*Port_Number*/*DatabaseName* Sample value: jdbc:sybase:Tds:integnt:5000/master
UserID	User name of the DBA login that is used to create, update, and delete users Sample value: OIMUser See "Configuring Sybase" for more information about this user account.
Password	Password of the DBA login that is used to create users
Target Locale: Country	Country code Default value: US **Note:** You must specify the value in uppercase.

Parameter	Description
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 No. **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: 3
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.

2.6 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

2.6.1 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.

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

2.6.2 Changing to the Required Input Locale

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

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

2.6.3 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);
   ```

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

While performing the instructions described in the "Copying the Connector Files" section on page 2-9, you copy files from the `resources` directory on the installation media into the *`OIM_HOME`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, change to the *`OIM_HOME`*`/xellerate/bin` directory.

   Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

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

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   Note: You can ignore the exception that is thrown when you perform Step 2.

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

OIM_HOME`/xellerate/config/xlConfig.xml`

2.6.5 Enabling Logging

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

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

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

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

- **Oracle WebLogic Server**

  To enable logging:

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

     `log4j.logger.OIMCP.DUTC=`*`log_level`*

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

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

- **IBM WebSphere Application Server**

  To enable logging:

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

```
log4j.logger.OIMCP.DUTC=log_level
```

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

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

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

- **JBoss Application Server**

  To enable logging:

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

     ```
     <category name="OIMCP.DUTC">
        <priority value="log_level"/>
     </category>
     ```

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

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

  JBoss_home/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

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

     ```
     log4j.logger.OIMCP.DUTC=log_level
     ```

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

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

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

3

Configuring the Connector

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

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

- Configuring Reconciliation
- Configuring Provisioning
- Configuring the Connector for Multiple Installations of the Target System

3.1 Configuring Reconciliation

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

- Partial Reconciliation
- Specifying the Number of Records to Be Reconciled
- Configuring the Target System As a Trusted Source
- Configuring the Reconciliation Scheduled Tasks
- Configuring the Reconciliation Scheduled Tasks for Lookup Fields
- Enabling Reconciliation in Oracle Identity Manager Release 9.0.1

3.1.1 Partial Reconciliation

> **Note:** See Bug 8274800 in the "Known Issues" chapter for information about an issue related to this feature.

By default, all target system records are fetched into Oracle Identity Manager during a 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.

3.1.2 Specifying the Number of Records to Be Reconciled

Note: See Bug 8274800 in the "Known Issues" chapter for information about an issue related to this feature.

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.

Note: If you provide a value for the `Login Name` attribute, then the `Record Size` attribute is ignored.

3.1.3 Configuring the Target System As a Trusted Source

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

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

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

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

Note: 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:

1. Import the XML file for trusted source reconciliation, `xelluserDbAccess 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 `xelluserDbAccess 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 import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the `xelluserDbAccess 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**.

Note: After you import the XML file for trusted source reconciliation, you must configure the scheduled task for trusted source reconciliation. The procedure is described in this chapter.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Importing the Connector XML Files" section on page 2-9, the scheduled tasks for lookup fields, trusted source user, and target resource user reconciliations are automatically created in Oracle Identity Manager. To configure the trusted source or target resource reconciliation scheduled tasks:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Administration** folder.
3. Select **Task Scheduler.**

4. Use the **Find** option to search for either the `Database Reconciliation Task - Non Trusted` or `Database Reconciliation Task - Trusted` scheduled task. Select the task to display its details.
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 `FAILED` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following scheduled tasks:
   - `Database Reconciliation Task - Trusted` (Scheduled task for trusted source reconciliation)
   - `Database Reconciliation Task - Non Trusted` (Scheduled task for target resource reconciliation)

   The following table describes the attributes of both scheduled tasks.

Note:

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

Attribute	Description	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 target resource reconciliation, set the value of this attribute to `No`.

Attribute	Description	Sample Value
Target System Login Recon - Resource Object name	Name of the target system parent resource object	■ For Oracle Database: Database Access Oracle User RO ■ For IBM DB2 UDB: Database Access DB2UDB User RO ■ For Microsoft SQL Server: Database Access SQLServer Login RO ■ For Sybase: Database Access Sybase Login RO
Target System User Recon - Resource Object name	Name of the target system child resource object	■ For IBM DB2 UDB: nodata ■ For Microsoft SQL Server: Database Access SQLServer User RO ■ For Oracle Database: nodata ■ For Sybase: Database Access Sybase User RO
Trusted Source Recon - Resource Object name	Name of the trusted source resource object	For trusted source reconciliation: Xellerate User For target resource reconciliation: False
DBName	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, specify none as the value of 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. If you provide a value for the Login Name attribute, then the Record Size attribute is ignored. **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. **Note:** If you provide a value for the Login Name attribute, then the Record Size attribute is ignored.	The default value of this attribute is All.
ExcludeSystemUsers	Specifies the logins to be excluded from reconciliation You can use this attribute to specify system logins that you do not want to reconcile into Oracle Identity Manager.	A comma-separated list of logins.

Attribute	Description	Sample Value
ReconcileLockedUser	Specifies whether or not users who are in the Locked state in Oracle Database must be reconciled Enter yes as the value of this attribute if you want users that are in the Locked state on the target system to be reconciled during a reconciliation run. Otherwise, enter no.	The default value is yes.

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.

3.1.5 Configuring the Reconciliation Scheduled Tasks for Lookup Fields

To configure the lookup field reconciliation scheduled tasks:

1. Perform Steps 1 through 8 of the procedure described in "Configuring the Reconciliation Scheduled Tasks" on page 3-3. While performing Step 4, search for the DBAccessLookupReconTask scheduled task.
2. While performing Step 9, use the information given in the following table:

Attribute	Description	Sample Value
Server	Name of the IT resource	Oracle
LookupFieldName	Specifies the name of the lookup definition for which reconciliation must be performed The list of lookup definitions for which reconciliation is supported can be performed is given in the *OIM_HOME*\XLIntegrations\DatabaseAccess\config\LookUpQuery.properties file. You can specify the name of any one of the supported lookup definitions as the value of the LookupFieldName attribute.	UD_Lookup.DB_ORA_Roles.
Exclusion List	Specifies the target system attribute values that must not be reconciled into the corresponding lookup For example, if you specify UD_Lookup.DB_ORA_Roles as the value of the LookupFieldName attribute, then you can specify DBA as the value of the Exclusion List attribute. By doing this, you ensure that the DBA role will not be stored in the UD_Lookup.DB_ORA_Roles lookup definition.	Comma-separated list of target system property names

3. Perform Step 10 of the procedure to configure the reconciliation scheduled tasks.

3.1.6 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 provisioning process.

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**.

3.2 Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager.

> **Note:** You must perform the procedure described in this section if you want to use the provisioning features of Oracle Identity Manager for this target system.
>
> You need not perform the procedure to compile adapters if you have performed the procedure described in "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-6.

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 1-6 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
- DB2 Delete TableSpace
- DB Prepopulate UserLogin
- DB Update Group
- DB EnableSybaseUser
- DB DisableSybaseUser
- DB Delete User
- DB Create User
- DBPrepopulateUserFullName

- DB Add Privilege
- DB Revoke Privilege
- DBPreventModify
- DB2 Delete Schema

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

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you import into the current database, select **Compile All**.

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

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

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

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

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

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

3.3 Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of 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 Example 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. Copy the files in the `test/config` directory on the installation media to the *`OIM_HOME`*`/xellerate/XLIntegrations/DatabaseAccess/config` directory.

   Copy the files in the `test/scripts` directory on the installation media to the *`OIM_HOME`*`/xellerate/XLIntegrations/DatabaseAccess/scripts` directory.

2. Open the following file:

   `OIM_HOME``/xellerate/XLIntegrations/DatabaseAccess/config/config.properties`

3. 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

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`

Attribute	Description	Sample Value
FullName	Full name of the user associated with the login created	`FullName`
DefDBSql	Default database for Microsoft SQL Server	`MyDB`
Default_Language	Default language	`En`
Authentication_Type	Authentication type for Microsoft SQL Server	`SQL_SERVER_AUTHENTICATION` 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`

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

     OIM_HOME\xellerate\XLIntegrations\DatabaseAccess\scripts\DBAccess.bat

   - For UNIX, run the following file:

     OIM_HOME/xellerate/XLIntegrations/DatabaseAccess/scripts/DBAccess.sh

5. When you are prompted for a password, enter the password of the user account whose credentials you specify in the IT resource. See "IT Resources" on page 2-10 for more information.
6. 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:

- **Bug 6624849**

  Reconciliation of deleted logins or users is not supported.

- **Bug 8424404**

  Due to some reason, if two instances of the same resource are assigned (provisioned) to a user, then resource (process) matching during target resource reconciliation fails but shows "Processes Matched" as the status.

  The work around is to manually link the reconciliation event to the resource.

Index

S

T

V

X