Oracle® Identity Manager

Connector Guide for JD Edwards EnterpriseOne

Release 9.0.4

E10182-01

May 2007

ORACLE®

Oracle Identity Manager Connector Guide for JD Edwards EnterpriseOne, Release 9.0.4

E10182-01

Contents

3   Configuring the Connector

4   Testing the Connector

5   Known Issues

A   Attribute Mappings Between Oracle Identity Manager and JD Edwards

Index

Preface

Oracle Identity Manager Connector Guide for JD Edwards EnterpriseOne provides information about integrating Oracle Identity Manager with JD Edwards EnterpriseOne.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for JD Edwards EnterpriseOne.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Release Notes*

- *Oracle Identity Manager Installation Guide for JBoss*

- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*

- *Oracle Identity Manager Installation Guide for WebLogic*

- *Oracle Identity Manager Installation Guide for WebSphere*

- *Oracle Identity Manager Administrative and User Console Guide*

- *Oracle Identity Manager Administrative and User Console Customization Guide*

- *Oracle Identity Manager Design Console Guide*

- *Oracle Identity Manager Tools Reference Guide*

- *Oracle Identity Manager Audit Report Developer Guide*

- *Oracle Identity Manager Best Practices Guide*

- *Oracle Identity Manager Globalization Guide*

- *Oracle Identity Manager Glossary of Terms*

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

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack Release 9.0.4 documentation library, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

What's New in the Oracle Identity Manager Connector for JD Edwards EnterpriseOne?

This chapter provides an overview of the updates made to the software and documentation for the JD Edwards EnterpriseOne connector in release 9.0.4 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.3.1 release of this guide for information about updates that were new for the 9.0.3.1 release

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

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

Software Updates

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

Enabling Logging

By following the instructions in the "Enabling Logging" section on page 2-8, you can configure the generation of log information that is specific to the target system.

Changes in the Supported Target Systems List

In the "Step 1: Verifying Deployment Requirements" section on page 2-1, the information on supported target system host platform has been modified. This release of the connector is not dependent on any target system host platform.

Documentation-Specific Updates

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

- In the "Multilanguage Support" section on page 1-4, Brazilian Portuguese has been added to the list of supported languages. From the Known Issues list in Chapter 4, the point stating that this language is not supported has been removed.

- In the "Step 1: Verifying Deployment Requirements" section on page 2-1, information about the user account required to connect to the target system has been added.

- Instructions in the "Determining the Release Number of the Connector" section on page 1-5 have been revised.

- Some of the content from the Chapter 2 of the earlier release of this guide has been moved to Chapter 3.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and Provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The JD Edwards EnterpriseOne Connector is used to integrate Oracle Identity Manager with JD Edwards EnterpriseOne.

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

This chapter contains the following sections:

- Reconciliation Module

- Provisioning Module

- Supported Functionality

- Multilanguage Support

- Files and Directories That Comprise the Connector

- Determining the Release Number of the Connector

> **Note:** At some places in this guide, JD Edwards EnterpriseOne has been referred to as the *target system*.

Reconciliation Module

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

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

This section discusses the elements that the reconciliation module extracts from the target system to construct reconciliation event records. The following are features of these records:

- The default data elements of each reconciliation event record are Organization, User Type, and Employee Type.

■ The default labels for the data elements in each reconciliation event record are:

  – `Event Linked` (for successful reconciliation)

  – `No Match Found` (for failed reconciliation)

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

■ Lookup Fields Reconciliation

■ User Reconciliation

Lookup Fields Reconciliation

For user reconciliation to work, the following lookup definitions must be available and the lookup values must be reconciled:

■ Lookup.JDE.DateSeparationCharacter

■ Lookup.JDE.Language

■ Lookup.JDE.Roles

■ Lookup.JDE.LocalizationCountryCode

■ Lookup.JDE.DateFormat

■ Lookup.JDE.FastPathCreate

■ Lookup.JDE.UniversalTime

■ Lookup.JDE.TimeFormat

■ Lookup.JDE.DecimalFormatCharector

User Reconciliation

User reconciliation can be divided into the following:

■ Reconciled JD Edwards EnterpriseOne Object Fields

■ Reconciled Xellerate User Fields

Reconciled JD Edwards EnterpriseOne Object Fields

The following fields are reconciled:

■ User ID

■ Password

■ Language

■ Date Format

■ Date Separation Character

■ Localization Country Code

■ Universal Time

■ Time Format

■ Decimal Format Character

■ Fast Path Create

■ Disable User

- Roles

Reconciled Xellerate User Fields

If trusted source reconciliation is implemented, then the following additional fields are reconciled:

- User ID

- First Name

- Last Name

- Organization

- User Type

- Employee Type

Provisioning Module

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

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

For this target system, the following fields are provisioned:

- User ID

- Password

> **Note:** If you create a user in Oracle Identity Manager and do not assign a role to the user, then the user would not be able to log in to the JD Edwards system.

Supported Functionality

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

Function	Type	Description
Create User	Provisioning	Creates a user in the JD Edwards system
Update User	Provisioning	Updates a user in the JD Edwards system
Reset Password	Provisioning	Updates the user password in the JD Edwards system
Enable User	Provisioning	Enables a user in the JD Edwards system
Disable User	Provisioning	Disables a user in the JD Edwards system
Delete User	Provisioning	Deletes a user from the JD Edwards system
Add User Role	Provisioning	Adds a role to a user in the JD Edwards system
Remove User Role	Provisioning	Removes the Role from a user in the JD Edwards system

Function	Type	Description
List Roles of User	Provisioning	Lists the roles of a user in the JD Edwards system
List All Roles	Provisioning	Lists all the roles present in the JD Edwards system
Reconciliation Insert Received	Reconciliation	Inserts information in Oracle Identity Manager about a user that is created in the JD Edwards system
Reconciliation Update Received	Reconciliation	Updates Oracle Identity Manager with information about a user that is updated in the JD Edwards system
Reconciliation Delete Received	Reconciliation	Deletes information in Oracle Identity Manager about a user that is deleted from the JD Edwards system

Multilanguage Support

This release of the connector supports the following languages:

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

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

Files and Directories That Comprise the Connector

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

```
Enterprise Applications/JDEdwards/JDE
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`xml/JDEResourceObject.xml`	This XML file contains definitions for the following components of the connector: ■ IT resource definition ■ JD Edwards User form ■ Lookup definitions ■ Adapters ■ Resource object ■ Process definition ■ Reconciliation scheduled tasks
`xml/JDEXLResourceObject.xml`	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.
`lib/JDEConnector.jar`	This is the connector code JAR file. This file contains all the classes and definitions required for provisioning and reconciliation.
Files in the `resources` directory	This directory contains files for locale-specific information that is used by the connector. **Note**: In this release, the JD Edwards connector supports only the English language.
`test/TroubleShootUtility.class`	This utility is used to test connector functionality.
`test/global.properties`	This file is used to specify the parameters and settings required to connect to the target system by using the `Troubleshoot` utility.
`test/log.properties`	This file is used to specify the log level and the directory in which the log file is to be created when you run the `Troubleshoot` utility.

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

The "Step 2: Copying the Connector Files and External Code Files" section on page 2-1 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

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

Before Deployment

To determine the release number of a connector:

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

    `Enterprise Applications/JDEdwards/JDE/lib`

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

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

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

After Deployment

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

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

1. Open the Oracle Identity Manager Design Console.

2. In the Form Designer, open the process form. The release number of the connector is the value of the **Version** field.

2

Deploying the Connector

Deploying the connector involves the following steps:

- Step 1: Verifying Deployment Requirements
- Step 2: Copying the Connector Files and External Code Files
- Step 3: Configuring the Oracle Identity Manager Server
- Step 4: Importing the Connector XML File

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target system	JD Edwards EnterpriseOne Tools release 8.9
Target system user account	JD Edwards EnterpriseOne user account to which the SYSADMIN and PKGBLD rights have been assigned.
	You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-11.
	If this user account were not assigned the required rights, then a connection error would be thrown when Oracle Identity Manager tries to communicate with the target system.

Step 2: Copying the Connector Files and External Code Files

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

File in the Installation Media Directory	Destination Directory
Files in the xml directory	*OIM_home*/Xellerate/JDE/xml
Files in the resources directory	*OIM_home*/xellerate/connectorResources
Files in the lib directory	*OIM_home*/Xellerate/JDE/lib *OIM_home*/Xellerate/JavaTasks

File in the Installation Media Directory	Destination Directory
Files in the test directory	*OIM_home*/Xellerate/JDE/test

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

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

File on the Target System Server	Destination Directory
The following JAR files from the *JDE_installation_dir*/E812/DDP/system/classes directory on the JD Edwards EnterpriseOne server:	*OIM_home*/Xellerate/JavaTasks

- ApplicationAPIs_JAR.jar
- Base_JAR.jar
- BizLogicContainer_JAR.jar
- BizLogicContainerClient_JAR.jar
- BusinessLogicServices_JAR.jar
- castor.jar
- Connector.jar
- Generator_JAR.jar
- JdbjBase_JAR.jar
- JdbjInterfaces_JAR.jar
- JdeNet_JAR.jar
- log4j.jar
- Metadata.jar
- MetadataInterface.jar
- PMApi_JAR.jar
- Spec_JAR.jar
- System_JAR.jar
- xalan.jar
- xerces.jar
- xml-apis.jar

File on the Target System Server	Destination Directory
Extract the following template files from the *JDE_installation_dir*/E812/DDP/system/classes/ConnectorSamples.zip file: ■ `jdbj.ini.templ` ■ `jdeinterop.ini.templ` ■ `jdelog.properties` Rename `jdbj.ini.templ` to `jdbj.ini`, and rename `jdeinterop.ini.templ` to `jdeinterop.ini`. Then, copy all three files to the specified destination directory.	*OIM_home*/Xellerate/JDE/Properties
If the EnterpriseOne server is running on Oracle Database, then copy the `tnsnames.ora` file to the specified destination directory.	*OIM_home*/Xellerate/JDE/Properties

> **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 JAR files listed in this table to the corresponding directories on each node of the cluster.

Changes to Be Made in the Property Files

You must modify the following property files to suit your deployment requirements:

■ jdbj.ini

■ jdeinterop.ini

■ jdelog.properties

> **Note:** The lists of configuration properties included in the following subsections are not comprehensive and include only those properties that are essential for the functioning of the connector. The files allow further customization of the connector functionality with other optional properties. Explicit descriptions and instructions to use the other configuration properties are included in the configuration files.

jdbj.ini

You need to modify the `jdbj.ini` file based on you requirements. This file contains configuration information for JDBj, which provides general database access capabilities for JD Edwards EnterpriseOne.

> **Note:** All property values in this file are case-sensitive.

In the `[JDBj-BOOTSTRAP SESSION]` section of this file, specify values for the parameters described in the following table:

Property	Sample Value	Description
user	user=JDE	User ID to connect to the target system
		This is an optional parameter.
password	password=jDPass	Password of the user
		This is an optional parameter.
environment	environment=PY812	Environment in which the user connects to the JD Edwards EnterpriseOne server
		The is a required parameter and *must* be specified in the jdbj.ini file.
		JD Edwards EnterpriseOne provides the following environments in which a user can access the system:
		■ Development Environment (DV812)
		■ Production Environment (PD812)
		■ Prototype Environment (PY812)
		■ Pristine Environment (PS812)
		To access the system in a particular environment, the user needs privileges for that environment.
role	role=*ALL	Role of the connecting user
		This is an optional parameter.

In the [JDBj-BOOTSTRAP DATA SOURCE] section of this file, specify values for the properties specified in the following table.

Property	Description
name	Name of the data source
	This property is not important for bootstrap connections. However, it shows up in error messages and logs.
	Sample value: name=System - 812
databaseType	Type of database used by the target system
	This value depends on the database used by the system. It can be any of the following:
	■ I = AS/400
	■ O = Oracle
	■ S = SQL Server
	■ W = UDB
	■ M = MSDE
	Sample value: databaseType=O
server	Name of the EnterpriseOne host server.
	Applicable for IBM AS/400 and SQL Server.
	Sample value: server=ibm1
serverPort	EnterpriseOne host server port number.
	Applicable only for Microsoft SQL Server

Property	Description
database	Database instance name
	Applicable only for Oracle Database and IBM DB2 UDB
	Sample value: database=ora10g
physicalDatabase	The physical database (used as library qualifier for IBM AS/400).
	This is applicable for Microsoft SQL Server and IBM AS/400
owner	Owner of the data source
	This is applicable for Oracle Database, Microsoft SQL Server, and IBM DB2 UDB.
	Sample value: owner=SY812
lob	Boolean value that indicates support for LOBs.
	This is applicable for Oracle Database and IBM AS/400.
	Sample value: lob=Y
unicode	Boolean value that indicates support for Unicode conversion is supported.
	This is applicable for Microsoft SQL Server.
	Sample value: unicode=N

> **Note:** A client of the EnterpriseOne server, also known as the Fat Client, has settings that correspond with the settings in the [JDBj-BOOTSTRAP DATA SOURCE] section in the jdbj.ini file. The values in this file must match those specified on the Fat Client. On the Fat Client, these settings are in the [DB SYSTEM SETTINGS] section of the jde.ini file.

In the [JDBj-JDBC DRIVERS] section of this file, specify the JDBC driver to connect to EnterpriseOne server. To do this, uncomment the line that specifies the driver for the database you are using. For example, if you are using Oracle Database, uncomment the line that specifies the driver for Oracle Database.

```
ORACLE=oracle.jdbc.driver.OracleDriver
```

In the [JDBj-ORACLE] section of this file, specify the location of the tnsnames.ora that you copy from the EnterpriseOne server. The following setting is required only when you use Oracle Database:

```
tns=OIM_home/Xellerate/JDE/Properties/tnsnames.ora
```

jdeinterop.ini

The jdeinterop.ini file is a configuration file that is used by the JD Edwards connector to enable interoperability between the Oracle Identity Manager and JD Edwards system.

Modify the jdeinterop.ini file and specify values for the properties described in the following table:

Section in the File	Property/Sample Value	Description
[OCM]	OCMEnabled=false	Boolean value that specifies whether the connector uses Object Configuration Mapping (OCM) to find the EnterpriseOne server
[JDENET]	serviceNameConnect =6014	Port number to connect to EnterpriseOne server from Oracle Identity Manager
[SERVER]	glossaryTextServer =ibm1:6014	Name and port number to connect to glossary Text server
	codePage=1252	Code page number for a particular language
[SECURITY]	SecurityServer=ibm 1	Name of the security server
		Note: The security server is the same as the EnterpriseOne server.
[INTEROP]	enterpriseServer=i bm1	Name of the EnterpriseOne server
	port=6014	Port number to connect to EnterpriseOne server

jdelog.properties

You can customize this file to enable logging at different levels. To enable logging, you need to specify the properties described in the following table:

Property	Description	Sample Value
FILE	Location of the log file	FILE=//jderoot.log
LEVEL	Logging level You can specify any of the following values: ■ SEVERE ■ WARN ■ APPS ■ DEBUG These values are in decreasing order of priority.	LEVEL=WARN
FORMAT	Logging format This property can be set to: ■ APPS ■ TOOLS ■ TOOLS_THREAD In a production environment, this must be set to APPS.	FORMAT=APPS
MAXFILESIZE	Maximum size of the log file in MB	MAXFILESIZE=10MB
MAXBACKUPINDEX	Maximum number of log file backups to be maintained	MAXBACKUPINDEX=20
COMPONENTS	Components for which events are logged in the log file You can specify other components as well. A list of all the components is specified in the template for this file.	COMPONENT=RUNTIME| JAS|JDBJ

Property	Description	Sample Value
APPEND	Boolean value that specifies that log entries must be appended at the end of the file The value can be TRUE or FALSE.	APPEND=TRUE

Step 3: Configuring the Oracle Identity Manager Server

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

Configuring the Oracle Identity Manager server involves performing the following procedures:

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache\
- Enabling Logging

Changing to the Required Input Locale

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

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

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Step 2: Copying the Connector Files and External Code Files" section on page 2-1, you copy files from the resources directory on the installation media into the OIM_home/xellerate/connectorResources directory. Whenever you add a new resource bundle in the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, change to the OIM_home/xellerate/bin directory.

    > **Note:** You must perform Step 1 before you perform Step 2. If you run the command described in Step 2 as follows, then an exception is thrown:
    >
    > OIM_home/xellerate/bin/batch_file_name

2. Enter one of the following commands:

    - On Microsoft Windows:

        PurgeCache.bat ConnectorResourceBundle

    - On UNIX:

        PurgeCache.sh ConnectorResourceBundle

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

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

OIM_home/xellerate/config/xlConfig.xml

Enabling Logging

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

- ALL

  This level enables logging for all events.

- DEBUG

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

- INFO

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

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

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

- FATAL

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

- OFF

  This level disables logging for all events.

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

- **BEA WebLogic**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.JDECONNECTOR=log_level
     ```

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

     For example:

```
log4j.logger.XELLERATE=INFO
log4j.logger.XL_INTG.JDECONNECTOR=INFO
```

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

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

- **IBM WebSphere**

    To enable logging:

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

        ```
        log4j.logger.XELLERATE=log_level
        log4j.logger.XL_INTG.JDECONNECTOR=log_level
        ```

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

        For example:

        ```
        log4j.logger.XELLERATE=INFO
        log4j.logger.XL_INTG.JDECONNECTOR=INFO
        ```

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

    WebSphere_home/AppServer/logs/*server_name*/startServer.log

- **JBoss Application Server**

    To enable logging:

    1. In the *JBoss_home*/server/default/conf/log4j.xml file, locate or add the following lines:

        ```
        <category name="XELLERATE">
           <priority value="log_level"/>
        </category>

        <category name="XL_INTG.JDECONNECTOR">
           <priority value="log_level"/>
        </category>
        ```

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

        ```
        <category name="XELLERATE">
           <priority value="INFO"/>
        </category>

        <category name="XL_INTG.JDECONNECTOR">
           <priority value="INFO"/>
        </category>
        ```

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

    JBoss_home/server/default/log/server.log

- **OC4J**

    To enable logging:

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

```
log4j.logger.XELLERATE=log_level
log4j.logger.XL_INTG.JDECONNECTOR=log_level
```

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

For example:

```
log4j.logger.XELLERATE=INFO
log4j.logger.XL_INTG.JDECONNECTOR=INFO
```

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

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

Step 4: Importing the Connector XML File

As mentioned in the "Files and Directories That Comprise the Connector" section on page 1-4, the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.

2. Click the **Deployment Management** link on the left navigation bar.

3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.

4. Locate and open the JDEResourceObject.xml file, which is in the *OIM_home*/Xellerate/JDE/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 JDE IT Resource IT resource is displayed.

8. Specify values for the parameters of the JDE IT Resource IT resource. Refer to the table in the "Defining IT Resources" section on page 2-11 for information about the values to be specified.

9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the JDE IT Resource type is displayed.

10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

11. Click **View Selections**.

The contents of the XML file are displayed on the Import page. You *may* see a cross-shaped icon along with some nodes. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.

12. Click **Import**. The connector XML file is imported into Oracle Identity Manager.

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

Defining IT Resources

You must specify values for the `JDE IT Resource` IT resource parameters listed in the following table:

Parameter	Description
User	User ID of the user connecting to EnterpriseOne server
Password	Password of the user connecting to EnterpriseOne Server
Environment	Environment of the connecting user Sample value: DV812
Role	Role of the user connecting to EnterpriseOne Server Sample value: *ALL
ProxyUser	User ID of the system user in EnterpriseOne server
ProxyUserPassword	Password of the system user in EnterpriseOne server
TimeStamp	Timestamp for the first reconciliation run, the timestamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of reconciliation was completed is stored in this parameter. The following is sample timestamp value: Jun 01, 2006 at 10:00:00 GMT+05:30

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

3

Configuring the Connector

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

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

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

> **Note:** This chapter provides 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

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

- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks

Configuring Trusted Source Reconciliation

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

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

Enabling trusted source reconciliation involves the following steps:

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

2. Set the `isTrustedSource` scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which 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 locating files is displayed.

4. Locate and open the `JDEConnectorXLResourceObject.xml` file, which is in the *OIM_home*`/Xellerate/JDE/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**.

After you import the XML file for trusted source reconciliation, you must set the value of the `isTrustedSource` reconciliation scheduled task attribute to `True`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-2.

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Step 4: Importing the Connector XML File" section on page 2-10, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

1. Open the Oracle Identity Manager Design Console.

2. Expand the `Xellerate Administration` folder.

3. Select **Task Scheduler.**

4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.

5. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `ERROR` status to the task.

6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.

7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.

8. In the Interval region, set the following schedule parameters:

   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option. If you select the **Recurring Intervals**

option, then you must also specify the time interval at which you want the task to run on a recurring basis.

- ■ To set the task to run only once, select the **Once** option.

9. Provide values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 3-3 for information about the values to be specified.

10. Click **Save**. The scheduled task is created. The INACTIVE status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.

11. Repeat Steps 5 through 10 to create the second scheduled task.

Specifying Values for the Scheduled Task Attributes

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

- ■ Lookup Fields Reconciliation Scheduled Task
- ■ User Reconciliation Scheduled Task

Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the JDE LookUp Recon lookup fields reconciliation scheduled task.

Note:

- ■ Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

- ■ Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Attribute	Description	Sample Value
Language	Code of the language to be used in the lookup reconciliation	en
Country	Code of the country to be used in the lookup reconciliation	us
IT Resource	Name of the IT resource for setting up a connection to JD Edwards	JDE IT Resource
isRoleLookup	Specifies whether or not to perform a lookup for the Role value during reconciliation The value can be true or false.	true
isDateSeparation CharacterLookup	Specifies whether or not to perform a lookup for the Date Separation Character value during reconciliation The value can be true or false.	true
isLanguageLookup	Specifies whether or not to perform a lookup for the Language value during reconciliation The value can be true or false.	true

Attribute	Description	Sample Value
isLocalizationCo untryCodeLookup	Specifies whether or not to perform a lookup for the Localization Country Code value during reconciliation The value can be true or false.	true
isDateFormatLook up	Specifies whether or not to perform a lookup for the Date Format value during reconciliation The value can be true or false.	true
isUniversalTimeL ookup	Specifies whether or not to perform a lookup for the Universal Time value during reconciliation The value can be true or false.	true
isDecimalFormatC haracterLookup	Specifies whether or not to perform a lookup for the Decimal Format Character value during reconciliation The value can be true or false.	true
isTimeFormatLook up	Specifies whether or not to perform a lookup for the Time Format value during reconciliation The value can be true or false.	true
LanguagePreferen ceForLookup	Specifies the language setting for lookup field entries	You can specify one of the following values: ■ For English: E ■ For French: F ■ For German: G ■ For Italian: I ■ For Japanese: J ■ For Korean: KO ■ For Simplified Chinese: CS ■ For Spanish: S ■ For Traditional Chinese: CT

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

User Reconciliation Scheduled Task You must specify values for the following attributes of the JDE User Recon user reconciliation scheduled task.

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

Attribute	Description	Sample Value
Organization	Default organization assigned to a new user	Xellerate Users
Xellerate Type	Default type assigned to a new user	End-User Administrator
Role	Default employee type assigned to a new user	Consultant
ITResource	Name of the IT Resource for setting up a connection with JD Edwards	JDE IT Resource
ResourceObject	Name of the resource object that is used for	JDE Resource Object
isTrustedSource	Specifies whether or not trusted source reconciliation is to be performed If it is set to true, then the target system is treated as a trusted source. If it is set to false, then the target system is treated as a nontrusted target. By default, the value is false.	false
XLDeleteUsersAllowed	Specifies whether or not users are to be deleted in Oracle Identity Manager during user reconciliation	false

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

Stopping Reconciliation

Suppose the User Reconciliation Scheduled Task for the connector is running and user records are being reconciled. If you want to stop the reconciliation process:

1. Perform Steps 1 through 4 of the procedure to configure reconciliation scheduled tasks.

2. Select the **Stop Execution** check box in the task scheduler.

3. Click **Save**.

Configuring Provisioning

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

> **Note:** You must perform this procedure if you want to use the provisioning features of Oracle Identity Manager for this target system.

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

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

- ■   `Enable and Disable User`

- ■   `JDE Delete User`

- ■   `Modify Password`

- ■   `PrePopulate JDE Form`

- ■   `JDE Remove Role`

- ■   `JDE Modify User`

- ■   `JDE Create User`

- ■   `JDE Add Role`

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

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.

2. To compile all the adapters that you import into the current database, select **Compile All**.

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

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

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.

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

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

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

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.

2. Double-click the row header of the adapter, or right-click the adapter.

3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

Configuring the Connector for Multiple Installations of the Target System

> **Note:**   Perform this procedure only if you want to configure the connector for multiple installations of JD Edwards EnterpriseOne.

You may want to configure the connector for multiple installations of JD Edwards EnterpriseOne. The following example illustrates this requirement:

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

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of JD Edwards EnterpriseOne.

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 resource object for each target system installation. The Resource Objects form is in the Resource Management folder. The `JDE Resource Object` resource object is created when you import the connector XML file. You can use this resource object as the template for creating the remaining resource objects.

2. Create and configure one IT resource for each resource object. The IT Resources form is in the Resource Management folder. The `JDE IT Resource` IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

3. Create and configure one process definition for each resource object.

   The Process Definition form is in the Process Management folder. The `JDE Process` process definition is created when you import the connector XML file. You can use this process definition as the template for creating the remaining process definitions. While creating each process definition, the following steps that you must perform are specific to this procedure:

   a. From the **Object Name** lookup field, select the resource object that you create in Step 1.

   b. While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list. Design one process form for each process definition.

4. The Form Designer form is in the Development Tools folder. The following process forms are created when you import the connector XML file:

   - `UD_JDE` (parent form)

   - `UD_JDEROL` (child form for multivalue attributes)

   You can use these process forms as templates for creating the remaining process forms. While creating the process forms, from the Object Name lookup field, select the resource object that you create in Step 1.

5. Configure reconciliation for each target system installation. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:

   - `ITResource`

   - `ResourceObject`

   - `isTrustedSource`

Set the `isTrustedSource` attribute to `True` for the JD Edwards installation that you want to designate as a trusted source.

6. 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 JD Edwards installation to which you want to provision the user.

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

4

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses procedure to test connector.

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system

To use the utility:

1. Specify the required values in the `global.properties` file. This file is in the *OIM_home*`/Xellerate/JDE 9.0.3/test` directory. The following table describes the sections of this file in which you must provide information for runing the tests.

Section	Description
Server Information	Connection parameters required to connect to the target system
Create User Parameter	Field information required to create or delete a user profile
Modify User Parameter	Field information required to modify a user profile
Password Reset	Field information required to reset a password for a user profile
Modify Enable / Disable User Parameters	Field information required to enable or disable a user profile
Add Role to User Parameters	Field information required add a role to a user profile
Remove Role from User Parameters	Field information required remove a role from a user profile
Reconcile Users	The From Date timestamp
	The To Date is set to the current date and time by default.

2. Add all the JAR files mentioned in the "Step 2: Copying the Connector Files and External Code Files" section on page 2-1 to the `CLASSPATH` environment variable.

   Add all the files in the *OIM_home*`/Xellerate/JDE/Properties` directory to the `CLASSPATH` environment variable.

3. In the `log.properties` file in the same directory:

   a. In the following parameter, set the path of the directory in which you want to create the log files:

      ```
      log4j.appender.logfile.File=log_file_path
      ```

Here, *log_file_path* is the path of the directory in which you want to create the log file.

    b. Specify any one of the following log levels:

      – DEBUG

      – INFO

      – WARN

      – ERROR

      – FATAL

For example, if the log level for DEBUG is to be enabled, then you must add the following entry file:

```
log4j.logger.ADAPTERS.ACTIVEDIRECTORY=DEBUG
```

4. Create an ASCII-format copy of the global.properties file as follows:

    a. In a command window, change to the following directory:

```
OIM_home/Xellerate/JDE/test
```

    b. Enter the following command:

```
native2ascii global.properties troubleshoot.properties
```

The troubleshoot.properties file is created when you run the native2ascii command. The contents of this file are an ASCII-format copy of the contents of the global.properties file.

5. Perform the following tests:

    ■ Enter the following command to create a user:

```
java -DTproperties=OIM_home/test/troubleShoot.properties
-Dlog4j.configuration=file:/OIM_home/test/log.properties
TroubleShootUtility C
```

    ■ Enter the following command to delete a user:

```
java -DTproperties=OIM_home/test/troubleShoot.properties
-Dlog4j.configuration=file:/OIM_home/test/log.properties
TroubleShootUtility D
```

    ■ Enter the following command to modify a user:

```
java -DTproperties=OIM_home/test/troubleShoot.properties
-Dlog4j.configuration=file:/OIM_home/test/log.properties
TroubleShootUtility M
```

    ■ Enter the following command to reset the password of a user:

```
java -DTproperties=OIM_home/test/troubleShoot.properties
-Dlog4j.configuration=file:/OIM_home/test/log.properties
TroubleShootUtility P
```

    ■ Enter the following command to enable and disable a user:

```
java -DTproperties=OIM_home/test/troubleShoot.properties
-Dlog4j.configuration=file:/OIM_home/test/log.properties
TroubleShootUtility ED
```

- Enter the following command to add a role to user:

```
java -DTproperties=OIM_home/test/troubleShoot.properties
-Dlog4j.configuration=file:/OIM_home/test/log.properties
TroubleShootUtility AUR
```

- Enter the following command to remove a role from user:

```
java -DTproperties=OIM_home/test/troubleShoot.properties
-Dlog4j.configuration=file:/OIM_home/test/log.properties
TroubleShootUtility RUR
```

- Enter the following command to test reconcile users:

```
java -DTproperties=OIM_home/test/troubleShoot.properties
-Dlog4j.configuration=file:/OIM_home/test/log.properties
TroubleShootUtility R
```

5

Known Issues

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

- The target system does not accept a user ID that is longer than 10 characters. During provisioning, if you specify a user ID that is longer than 10 characters, then the first 10 characters are used to create the user ID on the target system.

  This limitation also applies to the password that you specify for the new user.

- While reconciling users from the target system, the User ID value is used to populate the First Name and Last Name fields of the Xellerate User account in Oracle Identity Manager.

- This connector does not support secure connection between Oracle Identity Manager and the target system because the interoperability solution used in building the connector does not support this type of connection.

  The only way to secure communication between Oracle Identity Manager and the target system is to place both on a secure network.

- Linking in Oracle Identity Manager is asynchronous. If a user is first created and then disabled in the JD Edwards system, then that user might not be disabled in Oracle Identity Manager in the first reconciliation run. The user will be disabled in Oracle Identity Manager in the second reconciliation run.

- While creating a user in a provisioning operation, if you specify the login credentials in a multibyte language (for example, Japanese or Korean), then the user account may not be correctly created on the target system. The user will not be able to log in to the target system.

  The following sample scenario illustrates this problem:

  While installing the operating system on the target system server, suppose you had selected the English language for installation. Now, you are using a language pack for the Japanese language that you want to use on that server. As mentioned earlier, on this target system, the login credentials of newly created user accounts will not work.

  However, suppose you had selected the Japanese language while installing the operating system on the target system server. You do not need to use the Japanese language pack on this server. On a target system installed on this server, a user would be able to log in using user credentials created on Oracle Identity Manager.

A

Attribute Mappings Between Oracle Identity Manager and JD Edwards

The following table discusses attribute mappings between Oracle Identity Manager and JD Edwards.

Oracle Identity Manager Attribute	JD Edwards Attribute	Description
sUserId	USER	Login ID
sLanguagePreference	LNGP	Language preference
sDateFormat	FRMT	Date format character
sDateSeparator	DSEP	Date separation character
sDecimalFormat	DECF	Decimal format character
sCountry	CTR	Country
sUniversalTime	UTCTIME	Universal time
sTimeFormat	UTCTIME	Time format
sFastPath	FSTP	Fast path
EnabledUser	EUSER	Enable or disable user This is a Boolean value that toggles the enabling and disabling of the user.
RoleName	FRROLE	Name of the role
EffectiveDate	EFFDATE	Effective date of the role
ExpirationDate	EXPIRDATE	Expiration date of the role
IncludeAll	FUROLE1	Include a role or privilege in the *ALL role

Index