Oracle® Identity Manager

Connector Guide for JD Edwards EnterpriseOne User Management

Release 9.0.4

E10453-09

September 2013

ORACLE

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

E10453-09

Primary Author: Gauhar Khan

Contributing Authors: Gowri.G.R, Prakash Hulikere, Sridhar Machani, Alankrita Prakash

Contents

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

5 Known Issues

Index

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with JD Edwards EnterpriseOne 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/oim.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 JD Edwards EnterpriseOne User Management?

This chapter provides an overview of the updates made to the software and documentation for the JD Edwards EnterpriseOne User Management connector in release 9.0.4.12.

Note: Release 9.0.4.12 of the connector comes after release 9.0.4.3. Release numbers from 9.0.4.4 through 9.0.4.11 have not been used.

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 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.12

Software Updates in Release 9.0.4.1

The following are software updates in release 9.0.4.1:

- Separate JAR Files for Provisioning and Reconciliation
- New Connector XML Files

Separate JAR Files for Provisioning and Reconciliation

The `JDEConnector.jar` file has been split into two files, `JDEConnectorProv.jar` and `JDEConnectorRecon.jar`. Corresponding changes have been made in the following sections:

- "Files and Directories on the Installation Media" on page 2-1
- "Determining the Release Number of the Connector" on page 2-3
- "Copying the Connector Files" on page 2-14

New Connector XML Files

The connector XML file for target resource reconciliation has been changed from `JDEResourceObject.xml` to `JDEConnectorResourceObject.xml`.

The connector XML file for trusted source reconciliation has been changed from `JDEXLResourceObject.xml` to `JDEConnectorXLResourceObject.xml`.

See "Files and Directories on the Installation Media" on page 2-1 for more information.

Software Updates in Release 9.0.4.2

The following are the software update in release 9.0.4.2:

- Using the Connector Installer
- Support for New Target System

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.x or Release 11.1.1" on page 2-11 for details.

Support for New Target System

From this release onward, the connector adds support for JD Edwards EnterpriseOne Tools 8.98 and Application 8.12 as a target system.

This target system has been mentioned in the "Verifying Deployment Requirements" section.

Software Updates in Release 9.0.4.3

The following is a software update in release 9.0.4.3:

Support for Mapping New Attributes for Reconciliation and Provisioning

From this release onward, the connector enables you to map new target system attributes with Oracle Identity Manager attributes for reconciliation and provisioning.

To enable support for mapping new attributes for reconciliation and provisioning operations, the `Configuration Lookup` parameter has been added to the IT resource definition. You use this parameter to specify the name of the lookup definition that stores configuration information used during connector operations.

See the following sections for more information:

- Adding New Attributes for Target Resource Reconciliation
- Adding New Attributes for Provisioning

- Configuring the IT Resource
- Importing the Connector XML File

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See Section 3.5.2, "Request-Based Provisioning" for more information.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 9.0.4.2
- Documentation-Specific Updates in Release 9.0.4.3
- Documentation-Specific Updates in Release 9.0.4.12

Documentation-Specific Updates in Release 9.0.4.2

The following are the documentation-specific updates in release 9.0.4.2:

- In the "Verifying Deployment Requirements" section, changes have been made in the "Target system" row.
- The "Configuring the Connector for Multiple Installations of the Target System" section has been removed from the "Deploying the Connector" chapter. The connector does not directly support this feature.
- In the "Provisioning Module" section, the fields that are provisioned have been added.
- In the "Verifying Deployment Requirements" section, minor changes have been made in the "Target system" row.
- In the "Using External Code Files" section:
  - JAR files that have to be copied to Oracle Identity Manager have been added.
  - The path to the directory containing the template files has been modified.
- In the "Setting the Classpath on Oracle WebLogic Server Running on Microsoft Windows" section, one of the commands that is used for setting the classpath has been modified.

- In the "Setting the Classpath on Oracle Application Server" section, information about creating a shared library has been added.

Documentation-Specific Updates in Release 9.0.4.3

The following is a documentation-specific updates in release 9.0.4.3:

- The `Configuration Lookup` IT resource parameter has been added in the following sections:
  - Configuring the IT Resource
  - Importing the Connector XML File
  - User Reconciliation Scheduled Task
- 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 9.0.4.12

The following are documentation-specific updates in release 9.0.4.12:

- In the "Role Attributes for Target Resource Reconciliation and Provisioning" table, changes have been made to the "Effective Start Date" and "End Date" rows.
- From row "Target system user account" of Table 1–1, " Certified Components", the PKGBLD right has been removed.
- In the "Configuring Trusted Source Reconciliation" section, information about the file location for importing the XML files has been updated.
- In the "Using External Code Files" section, information about the destination directory for copying JAR files on Oracle Identity Manager release 11.1.1 has been updated.
- In the "Importing the Connector XML File" section, a note for the User, Password, ProxyUser, and ProxyUserPassword parameters has been added.

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 external, identity-aware applications. This guide discusses the connector that enables you to use JD Edwards EnterpriseOne either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

> **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, JD Edwards EnterpriseOne has been referred to as the **target system.**

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

This chapter contains the following sections:

1.1 Certified Components

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

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager release 9.0.1 through 9.0.3.2 ■ Oracle Identity Manager release 9.1.0.1 or later **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 will support. ■ Oracle Identity Manager 11*g* release 1 (11.1.1) **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1). The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at `http://www.oracle.com/technetwork/documentation/oim1014-097544.html`
Target system	The target system can be any one of the following: ■ JD Edwards EnterpriseOne Tools 8.96 and Application 8.12 ■ JD Edwards EnterpriseOne Tools 8.98 and Application 8.12
Target system user account	JD Edwards EnterpriseOne user account to which the `SYSADMIN` right has been assigned. You provide the credentials of this user account while configuring the IT resource. The procedure is described later in this guide. If this user account was not assigned the required rights, then a connection error would be thrown when Oracle Identity Manager tries to communicate with the target system.
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.2, use JDK 1.4.2 or a later release in the 1.4.2 series. ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or a later release in the 1.5 series. ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.

1.2 Certified Languages

The connector supports the following languages:

- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean

- Portuguese (Brazilian)
- Spanish

See Also: For information about supported special characters supported by Oracle Identity Manager, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*:

  Oracle Identity Manager Globalization Guide

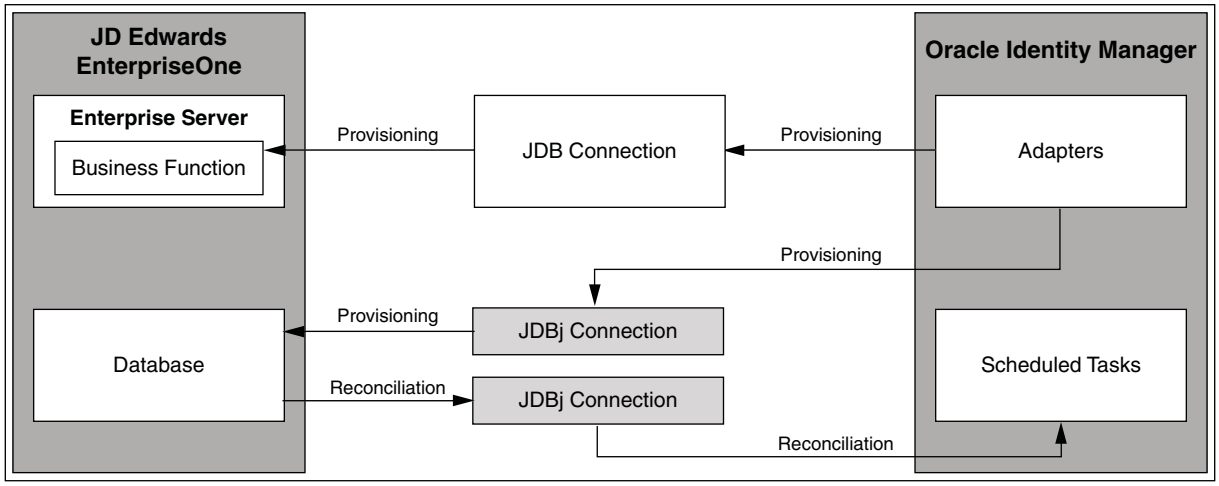
- For Oracle Identity Manager release 11.1.1:

  Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager

1.3 Connector Architecture

Figure 1–1 shows the connector integrating JD Edwards EnterpriseOne with Oracle Identity Manager.

Figure 1–1 Connector Architecture



The target system, JD Edwards EnterpriseOne, is based on a client-server architecture. The JD Edwards EnterpriseOne User Management connector leverages this architecture to perform connector operations by calling business functions (BSFNs) within the JD Edwards Enterprise server or connecting to the JD Edwards Database, as required.

During provisioning, adapters carry provisioning data submitted through the process form to the target system. The adapters establish a connection with the target system in one of the following ways:

- If a BSFN for performing the required provisioning operation is available on the target system, then the adapter establishes a connection with the JD Edwards Enterprise Server by using JDB.
- If there is no BSFN on the target system that can perform the required provisioning operation, then the adapter establishes a connection with the JD Edwards Database by using JDBj.

After the adapters establish a connection with the target system, the required provisioning operation is performed, and then the response from the target system is returned to the adapters.

Note: In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

During reconciliation, a scheduled task establishes a connection with the JD Edwards Database by using JDBj. After the connection with the database is established, the user records that match the reconciliation criteria are retrieved, and passed on to the scheduled task, which brings the records to Oracle Identity Manager.

1.4 Features of the Connector

The following are features of the connector:

- Section 1.4.1, "Support for Both Target Resource and Trusted Source Reconciliation"
- Section 1.4.2, "Support for Both Full and Incremental Reconciliation"
- Section 1.4.3, "Support for Adding New Attributes for Reconciliation and Provisioning"

1.4.1 Support for Both Target Resource and Trusted Source Reconciliation

You can use the connector to configure JD Edwards EnterpriseOne as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.3, "Configuring Reconciliation" for more information.

1.4.2 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time. See Section 3.3.1, "Full Reconciliation" for more information.

1.4.3 Support for Adding New Attributes for Reconciliation and Provisioning

If you want to add to the standard set of single-valued attributes for reconciliation and provisioning, then perform the procedures described in Chapter 4, "Extending the Functionality of the Connector."

1.5 Lookup Definitions Used During Connector Operations

Lookup definitions used during connector operations can be divided into the following categories:

- Section 1.5.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.5.2, "Other Lookup Definitions"

1.5.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Date Format lookup field to select a date format from the list of supported date formats. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are automatically created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

The following lookup definitions are populated with values fetched from the target system by the scheduled tasks for lookup field synchronization:

> **See Also:** Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about these scheduled tasks

- Lookup.JDE.DateSeparationCharacter
- Lookup.JDE.Language
- Lookup.JDE.Roles
- Lookup.JDE.LocalizationCountryCode
- Lookup.JDE.DateFormat
- Lookup.JDE.UniversalTime
- Lookup.JDE.TimeFormat
- Lookup.JDE.DecimalFormatCharacter

1.5.2 Other Lookup Definitions

Table 1–2 describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

Table 1–2 Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.JDE.Configuration	This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.	This lookup definition is preconfigured. You cannot add or modify entries in this lookup definition.
Lookup.JDEReconciliation.FieldMap	This lookup definition holds mappings between the JDE User resource object fields and target system attributes.	This lookup definition is preconfigured. Table 1–3 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for user reconciliation. Chapter 4, "Extending the Functionality of the Connector" provides more information.
Lookup.JDE.FastPathCreate	This lookup definition enables you to set the JD Edwards FASTPATH feature for users.	This lookup definition is preconfigured. You need not add entries in this lookup definition.

1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning

The following sections provide information about connector objects used during target resource reconciliation and provisioning:

> **See Also:** The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about reconciliation

The following sections provide information about connector objects used during reconciliation:

- Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.2, "Role Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.3, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.4, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.5, "Provisioning Functions"

1.6.1 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–3 provides information about user attribute mappings for target resource reconciliation and provisioning.

Table 1–3 User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Attribute	Description
User ID	USER	Login ID
Language	LNGP	Language preference
Date Format	FRMT	Date format
Date Separation Character	DSEP	Date separation character

Table 1–3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Attribute	Description
Localization Country Code	CTR	Country Code
Universal Time	UTCTIME	Time zone
Time Format	TIMEFORM	Time format
Decimal Format Character	DECF	Decimal format character
Fast Path Create	FSTP	Fast redirect codes to navigate to frequently used JD Edwards applications such as Batch Versions and Automatic Accounting
Disable User	NA	This is a check box to specify whether you want to enable or disable a user. Select the **Disable User** check box to disable a user.

1.6.2 Role Attributes for Target Resource Reconciliation and Provisioning

Table 1–4 provides information about role attribute mappings for target resource reconciliation and provisioning.

Table 1–4 Role Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Role Attribute	Description
Role	szRole	Role name
Include in *ALL	cIncludedInALL	Specifies whether the search must be performed in all environments or only a particular environment
Effective Start Date	jdEffectiveDate	Date from which the role is effective for the user
End Date	jdExpirationDate	Date from which the role is no longer valid for the user

1.6.3 Reconciliation Rule for Target Resource Reconciliation

See Also: *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

The following is the process-matching rule:

Rule name: JDE Recon Rule

Rule element: User Login equals UserID

In this rule:

- User Login is one of the following:
  - For Oracle Identity Manager release 9.0.1 through 9.0.3.2:

    User ID attribute on the Xellerate User form.
  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.1:

    User ID attribute on the OIM User form.
- User ID is the User field of JD Edwards.

This rule supports the following scenarios:

- You can provision multiple JD Edwards resources to the same OIM User, either on Oracle Identity Manager or directly on the target system.
- You can change the user ID of a user on the target system.

This is illustrated by the following use cases:

- Use case 1: You provision a JD Edwards account for an OIM User, and you also create an account for the user directly on the target system.

  When the first rule condition is applied, no match is found. Then, the second rule condition is applied and it is determined that a second account has been given to the user on the target system. The second account is linked with the OIM User at the end of the reconciliation run.
- Use case 2: An OIM User has a JD Edwards account. You then change the user ID of the user on the target system.

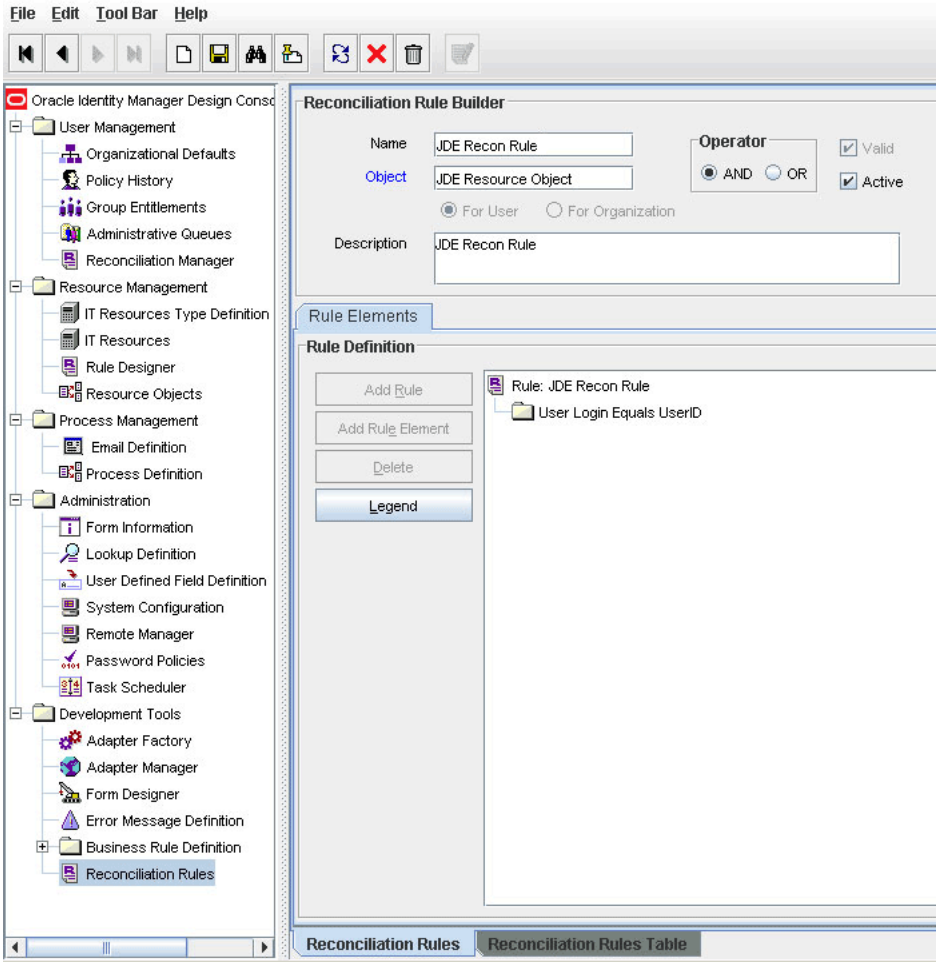
  During the next reconciliation run, application of the first rule condition helps match the resource with the record.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **JDE Recon Rule**. Figure 1–2 shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



1.6.4 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–5 lists the action rules for target resource reconciliation.

Table 1–5 Action Rules for Target Resource Reconciliation

Rule Condition	Action
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

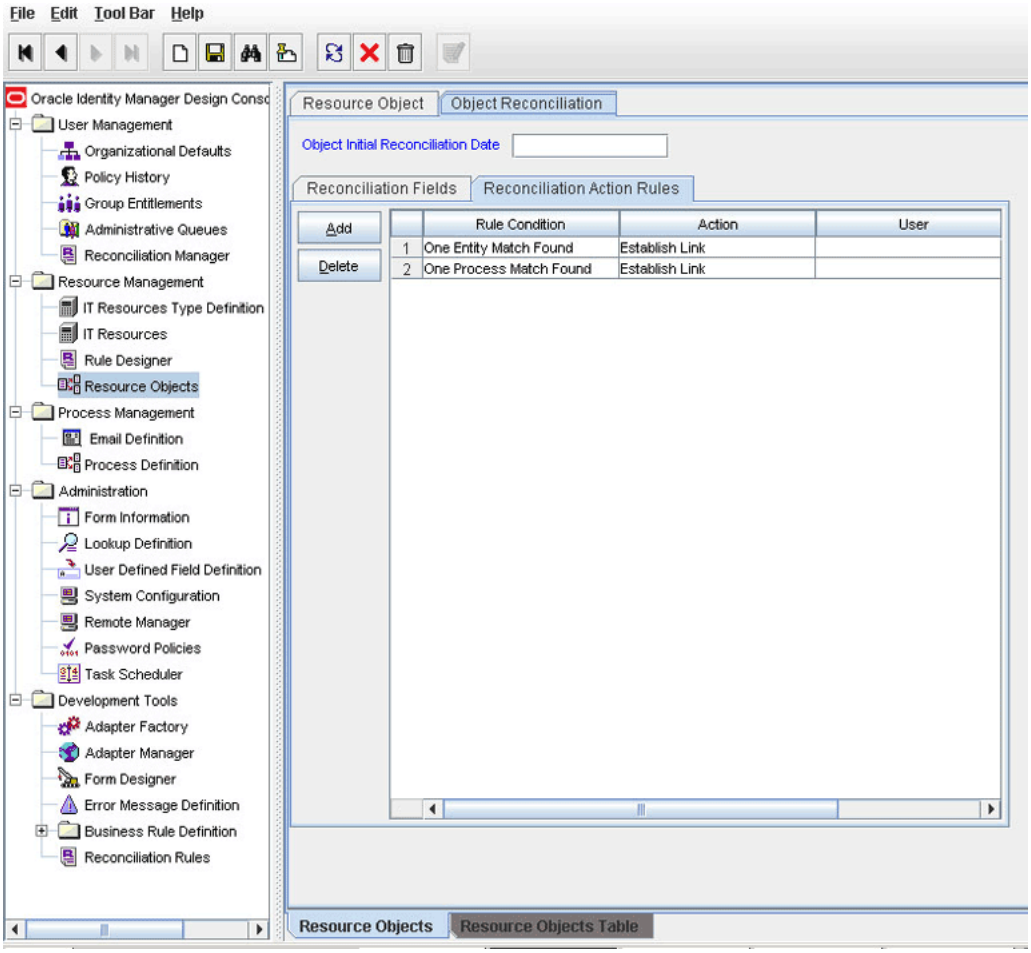
Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **JDE Resource Object** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rule for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules for Target Resource Reconciliation



1.6.5 Provisioning Functions

Table 1–6 lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

Table 1–6 Provisioning Functions

Function	Adapter
Create User	JDE Create User
Update User	JDE Modify User
Reset Password	Modify Password
Enable User	Enable and Disable User
Disable User	Enable and Disable User
Delete User	JDE Delete User
Add User Role	JDE Add Role
Remove User Role	JDE Remove Role

1.7 Connector Objects Used During Trusted Source Reconciliation

The following sections provide information about connector objects used during trusted source reconciliation:

- Section 1.7.1, "User Attributes for Trusted Source Reconciliation"
- Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"
- Section 1.7.3, "Reconciliation Action Rules for Trusted Source Reconciliation"

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–7 lists user attributes for trusted source reconciliation.

Table 1–7 User Attributes for Trusted Source Reconciliation

OIM User Form Field	Target System Attribute	Description
User ID	USER	Login ID
First Name	USER	Login ID
Last Name	USER	Login ID
Employee Type	NA	Default value: `Consultant`
User Type	NA	Default value: `End-User Administrator`
Organization	NA	Default value: `Xellerate Users`

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

See Also: *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

The following is the process matching rule:

Rule name: Trusted Source recon Rule

Rule element: User Login equals User ID

In this rule element:

- User Login is one of the following:
  - For Oracle Identity Manager Release 9.0.1 through 9.0.3.*x*:

User ID attribute on the Xellerate User form.

– For Oracle Identity Manager release 9.1.0.*x* or release 11.1.1:

User ID attribute on the OIM User form.

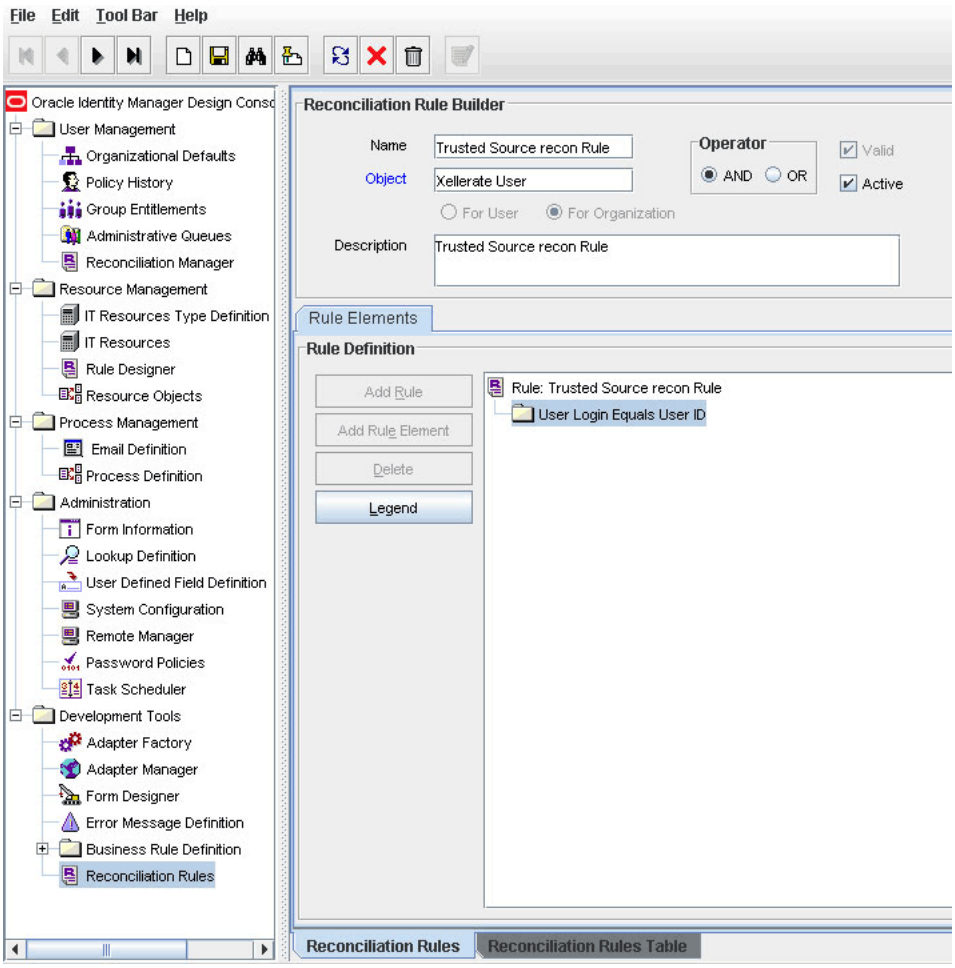
- User ID is the User field of JD Edwards.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **Trusted Source recon Rule**. Figure 1–4 shows the reconciliation rule for trusted source reconciliation.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–8 lists the action rules for target resource reconciliation.

Table 1–8 Action Rules for Trusted Source Reconciliation

Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

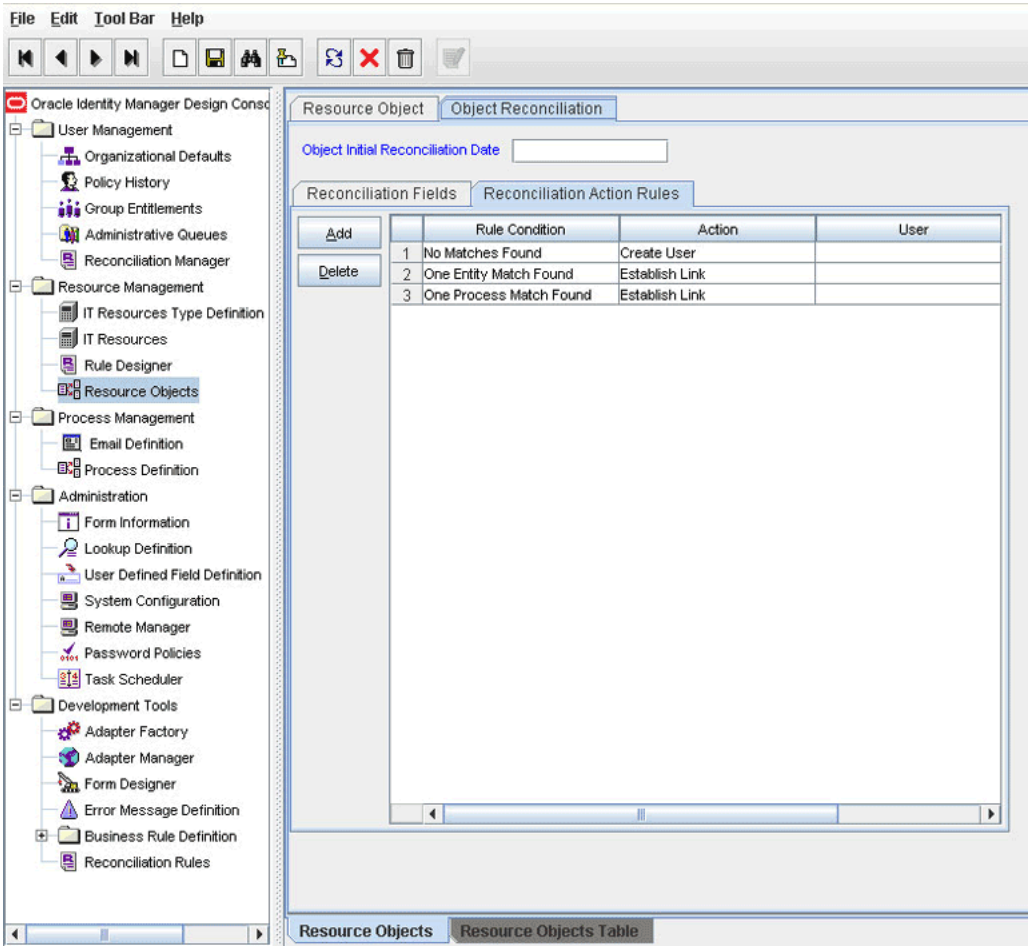
Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Xellerate User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–5 shows the reconciliation action rules for trusted source reconciliation.

Figure 1–5 Reconciliation Action Rules for Trusted Source Reconciliation



1.8 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform if you want to extend the functionality of the connector.
- Chapter 5, "Known Issues" lists known issues associated with this release of the connector.

2

Deploying the Connector

This chapter is divided into the following sections:

- Section 2.1, "Files and Directories on the Installation Media"
- Section 2.2, "Determining the Release Number of the Connector"
- Section 2.3, "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:
  - Section 2.4, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"
  - Section 2.5, "Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2"
- Section 2.6, "Configuring the Oracle Identity Manager Server"

2.1 Files and Directories on the Installation Media

Table 2–1 describes the files and directories on the installation media.

Table 2–1 Files and Directories On the Connector Installation Media

File in the Installation Media Directory	Description
configuration/JDEdwards-CI.xml	This XML file contains configuration information that is used during connector installation.
Files in the DataSets directory	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
lib/JDEConnectorProv.jar	This JAR file contains the class files required for provisioning. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
lib/JDEConnectorRecon.jar	This JAR file contains the class files required for reconciliation. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database

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

File in the Installation Media Directory	Description
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
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.
xml/JDEConnectorResourceObject.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 **Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1. See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.
xml/JDEConnectorXLResourceObject.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.

2.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.1, then skip this section.

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/JDEConnectorProv.jar

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

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

2.3 Using 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.

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: ■ 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 ■ jmxremote_optional.jar ■ ManagementAgent_JAR.jar ■ SystemInterfaces_JAR.jar ■ jmxri.jar	For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*: *OIM_HOME*/xellerate/ThirdParty For Oracle Identity Manager release 11.1.1: The JAR files on the JD Edwards Target System Server must be copied to the Oracle Identity Manager database. To copy these JAR files, run the Upload JARs utility from the temporary location to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager: **Note:** Before you run this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed. **For Microsoft Windows:** *OIM_HOME*/server/bin/UploadJars.bat **For UNIX:** *OIM_HOME*/server/bin/UploadJars.sh When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. To upload these JARs, specify 3 as the value of the JAR type.
Extract the following template files from the *JDE_INSTALLATION_DIR*/E812/DDP/system/classes/samples/ConnectorSamples.zip file: ■ jdbj.ini.templ ■ jdeinterop.ini.templ ■ jdelog.properties Rename the jdbj.ini.templ file to jdbj.ini, and rename the jdeinterop.ini.templ file to jdeinterop.ini. Then, copy all three files to the specified destination directory.	For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*: *OIM_HOME*/xellerate/JDE/Properties For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/JDE/Properties
If the EnterpriseOne server is running on Oracle Database, then copy the tnsnames.ora file to the specified destination directory.	For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*: *OIM_HOME*/xellerate/JDE/Properties For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/JDE/Properties

2.3.1 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.

2.3.1.1 jdbj.ini

You must modify the `jdbj.ini` file based on your 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=Password`	Password of the user This is an optional parameter.
`environment`	`environment=PY812`	Environment in which the user connects to the target system The is a required parameter and *must* be specified in the `jdbj.ini` file. The target system 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
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
```

2.3.1.2 jdeinterop.ini

The jdeinterop.ini file is a configuration file that is used by the 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

2.3.1.3 jdelog.properties

You can customize this file to enable logging at different levels. To enable logging, you must 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

Property	Description	Sample Value
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
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

After configuring the property files, you must add the directory in which the property files are present to the classpath environment variable. This variable is on the application server where Oracle Identity Manager is installed. The procedure to set the classpath depends on the application server on which Oracle Identity Manager is installed:

- Section 2.3.1.3.1, "Setting the Classpath on Oracle WebLogic Server Running on Microsoft Windows"
- Section 2.3.1.3.2, "Setting the Classpath on Oracle WebLogic Server Running on Linux"
- Section 2.3.1.3.3, "Setting the Classpath on IBM WebSphere Application Server on Microsoft Windows"
- Section 2.3.1.3.4, "Setting the Classpath on JBoss Application Server Running on Microsoft Windows"
- Section 2.3.1.3.5, "Setting the Classpath on JBoss Application Server Running on Linux"
- Section 2.3.1.3.6, "Setting the Classpath on Oracle Application Server"

2.3.1.3.1 Setting the Classpath on Oracle WebLogic Server Running on Microsoft Windows To add the directory into the classpath in the WebLogic Application Server on Windows:

1. In the WebLogic server installation directory, navigate to the domain name directory.
2. Open the startWebLogic.cmd file in a text editor.
3. Edit the following command:

```
set
CLASSPATH=%WEBLOGIC_CLASSPATH%;%POINTBASE_CLASSPATH%;%JAVA_HOME%\jre\lib\rt.jar
;%WL_HOME%\server\lib\webservices.jar;%CLASSPATH%
```

Add the JDE_CONFIG directory into the classpath that contains the property files as shown below:

```
set CLASSPATH=
JDE_CONFIG;JDBC_DRIVER_JAR_PATH;%WEBLOGIC_CLASSPATH%;%POINTBASE_CLASSPATH%;%JAV
A_HOME%\jre\lib\rt.jar;%WL_HOME%\server\lib\webservices.jar;%CLASSPATH%
```

In this command:

- Replace JDE_CONFIG with full path and name of the JDE_CONFIG directory. This directory contains the property files jdbj.ini, jdeinterop.ini, and jdelog.properties.

- Replace *JDBC_DRIVER_JAR_PATH* with the full path and name of the JDBC driver JAR.

2.3.1.3.2 Setting the Classpath on Oracle WebLogic Server Running on Linux To add the directory into the classpath in the WebLogic Application Server on Linux:

1. In the WebLogic server installation directory, navigate to the domain name directory.
2. Open the startWebLogic.sh file in a text editor.
3. Edit the following command:

```
CLASSPATH="${WEBLOGIC_CLASSPATH}:${POINTBASE_CLASSPATH}:${JAVA_HOME}/jre/lib/rt
.jar:${WL_HOME}/server/lib/webservices.jar:${CLASSPATH}"
```

Add the JDE_CONFIG directory into the classpath that contains the property files as shown below:

```
CLASSPATH=JDE_CONFIG:${WEBLOGIC_CLASSPATH}:${POINTBASE_CLASSPATH}:${JAVA_HOME}/
jre/lib/rt.jar:${WL_HOME}/server/lib/webservices.jar:${CLASSPATH}"
)
```

In this command, replace JDE_CONFIG with full path and name of the JDE_CONFIG directory. This directory contains the property files `jdbj.ini`, `jdeinterop.ini`, and `jdelog.properties`.

2.3.1.3.3 Setting the Classpath on IBM WebSphere Application Server on Microsoft Windows To add the directory into the classpath in the WebSphere Application Server on Windows:

1. In the WebSphere server installation directory, navigate to the bin directory.
2. Open startServer.bat in a text editor.
3. Edit the following command:

```
set CLASSPATH=%WAS_CLASSPATH%
```

Add the JDE_CONFIG directory into the classpath that contains the property files as shown below:

```
set CLASSPATH=JDE_CONFIG;%WAS_CLASSPATH%
```

In this command, replace JDE_CONFIG with full path and name of the JDE_CONFIG directory. This directory contains the property files `jdbj.ini`, `jdeinterop.ini`, and `jdelog.properties`.

2.3.1.3.4 Setting the Classpath on JBoss Application Server Running on Microsoft Windows To add the directory into the classpath in the JBoss Application Server on Windows:

1. In the JBoss installation directory, navigate to the bin directory.
2. Open the run.bat file in a text editor.
3. Edit the following command:

```
if "%JBOSS_CLASSPATH%" == "" (
set JBOSS_CLASSPATH=%JAVAC_JAR%;%RUNJAR%
) ELSE (
set JBOSS_CLASSPATH=%JBOSS_CLASSPATH%;%JAVAC_JAR%;%RUNJAR%
)
```

Add the JDE_CONFIG directory into the classpath that contains the property files as shown below:

```
if "%JBOSS_CLASSPATH%" == "" (
set JBOSS_CLASSPATH=JDE_CONFIG;%JAVAC_JAR%;%RUNJAR%
) ELSE (
set
JBOSS_CLASSPATH=JDE_CONFIG;%JBOSS_CLASSPATH%;%JAVAC_JAR%;%RUNJAR%
)
```

In this command, replace JDE_CONFIG with full path and name of the JDE_CONFIG directory. This directory contains the property files jdbj.ini, jdeinterop.ini, and jdelog.properties.

2.3.1.3.5 Setting the Classpath on JBoss Application Server Running on Linux To add the directory into the classpath in the JBoss Application Server on Linux:

1. In the JBoss installation directory, navigate to the bin directory.
2. Open the run.sh file in a text editor.
3. Edit the following command:

```
if [ "x$JBOSS_CLASSPATH" = "x" ]; then
JBOSS_CLASSPATH="$JBOSS_BOOT_CLASSPATH:$JAVAC_JAR"
ELSE JBOSS_CLASSPATH="$JBOSS_CLASSPATH:$JBOSS_BOOT_CLASSPATH:$JAVAC_JAR"
fi
```

Add the JDE_CONFIG directory into the classpath that contains the property files as shown below:

```
if [ "x$JBOSS_CLASSPATH" = "x" ]; then
JBOSS_CLASSPATH="$JBOSS_BOOT_CLASSPATH:$JAVAC_JAR"
ELSE
JBOSS_CLASSPATH="$JBOSS_CLASSPATH:$JBOSS_BOOT_CLASSPATH:$JAVAC_JAR"
fi
JBOSS_CLASSPATH=JDE_CONFIG:$JBOSS_CLASSPATH
```

In this command, replace JDE_CONFIG with the full path and name of the JD Edwards configuration directory. This directory contains the jdbj.ini, jdeinterop.ini, and jdelog.properties files.

2.3.1.3.6 Setting the Classpath on Oracle Application Server To set the classpath on Oracle Application Server, you must perform the following steps:

1. Add the directory into the classpath in the Oracle application server as follows:
   a. In the Oracle application server installation directory, navigate to the opmn directory.
   b. Open the opmn.xml file in a text editor.
   c. Edit the following command:

```
-Xbootclasspath^/p:D:\product\10.1.3.1\OracleAS_3\bpel\lib\orabpel-boot.jar
```

Add the JDE_CONFIG directory into the classpath that contains the property files as shown below:

```
-Xbootclasspath^/p:D:\product\10.1.3.1\OracleAS_3\bpel\lib\orabpel-boot.jar
; JDE_CONFIG
```

In this command, replace JDE_CONFIG with full path and name of the JDE_CONFIG directory. This directory contains the property files jdbj.ini, jdeinterop.ini, and jdelog.properties.

2. Create a shared library in Oracle Application Server as follows:

a. Login to the Oracle Application Server Enterprise Management Console, and select the application server.

b. From the Server Components list, select **home of OIM Instance**.

c. Click the **Administration** tab, select **Shared Libraries,** and then click **Go To Task**.

d. Click **Create**, and provide the name and version of the Shared Library, for example:

   – **Shared Library Name:** *SHARED_LIBRARY_NAME*

   – **Shared Library Version:** *SHARED_LIBRARY_VERSION_NUMBER*

e. Click **Next**, and then click **ADD** to display the list of third-party JAR files. Add these JAR files to the Shared Library created in Step d.

f. Click **Finish.**

g. Navigate and open the `application.xml` file from the Oracle Application Server installation directory, for example:

```
/product/10.1.3.1/OAS_DIRECTORY/j2ee/home/config
```

h. Add the `imported-shared-libraries` element for the Shared Library in the application.xml file as follows:

```
<imported-shared-libraries>
<import-shared-library name="SHARED_LIBRARY_NAME"/>
</imported-shared-libraries>
```

i. Save the `application.xml` file.

j. Restart Oracle Identity Manager.

   You can, for example, run the following command to restart Oracle Identity Manager:

```
pomnctl stopproc/startpoc process-type=OIM_INSTANCE_NAME
```

2.4 Installing the Connector on Oracle Identity Manager Release 9.1.0.*x* or Release 11.1.1

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.*x* or release 11.1.1 later involves the following procedures:

- Section 2.4.1, "Running the Connector Installer"
- Section 2.4.2, "Configuring the IT Resource"

2.4.1 Running the Connector Installer

To run the Connector Installer:

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

Note: In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

- For Oracle Identity Manager release 9.1.0.*x*:
  OIM_HOME/xellerate/ConnectorDefaultDirectory
- For Oracle Identity Manager release 11.1.1:
  OIM_HOME/server/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 the following guide:
   - For Oracle Identity Manager release 9.1.0.*x*:

     Oracle Identity Manager Administrative and User Console Guide
   - For Oracle Identity Manager release 11.1.1:

     Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager
3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.*x*:

     Click **Deployment Management**, and then click **Install Connector**.
   - For Oracle Identity Manager release 11.1.1:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.
4. From the Connector List list, select **JDEdwards *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

   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 **JDEdwards *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 XML files (by using the Deployment Manager)
   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 Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.6.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.

   There are no prerequisites for some predefined connectors.

   b. Configuring the 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 2–1.

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 Section 2.6.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.4.2 Configuring the IT Resource

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

1. Log in to the Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `JDE IT Resource` and then click **Search**.

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 `JDE IT Resource` IT resource. The following table describes each parameter:

Parameter	Description
User	User ID of the user account for connecting to the target system **Note:** The value for this parameter must be entered in uppercase.
Password	Password of the user account for connecting to the target system **Note:** The value for this parameter must be entered in uppercase.
Environment	Environment of the user account for connecting to the target system Sample value: `DV812`
Role	Role of the user account for connecting to the target system Sample value: `*ALL`
ProxyUser	User ID of the system user in the target system **Note:** The value for this parameter must be entered in uppercase.
ProxyUserPassword	Password of the system user in the target system **Note:** The value for this parameter must be entered in uppercase.
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`
Configuration Lookup	Name of the lookup definition that contains the configuration information used during connector operations. Default value: `Lookup.JDE.Configuration`

8. To save the values, click **Update**.

2.5 Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2

Installing the connector on any Oracle Identity Manager release between releases 9.0.1 and 9.0.3.2 involves the following procedures:

- Section 2.5.1, "Copying the Connector Files"
- Section 2.5.2, "Importing the Connector XML File"
- Section 2.5.3, "Compiling Adapters"

2.5.1 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: Section 2.1, "Files and Directories on the Installation Media" for more information about these files

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
lib/JDEConnectorProv.jar	*OIM_HOME*/xellerate/JDE/lib *OIM_HOME*/xellerate/JavaTasks
lib/JDEConnectorRecon.jar	*OIM_HOME*/xellerate/JDE/lib *OIM_HOME*/xellerate/ScheduleTask
Files in the test directory	*OIM_HOME*/xellerate/JDE/test

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.

2.5.2 Importing the Connector XML File

As mentioned in Section 2.1, "Files and Directories on the Installation Media," 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 opening files is displayed.
4. Locate and open the JDEConnectorResourceObject.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. See the following table for information about the values to be specified:

Parameter	Description
User	User ID of the user account for connecting to the target system **Note:** The User ID value must be entered in uppercase.
Password	Password of the user account for connecting to the target system **Note:** The Password value must be entered in uppercase.
Environment	Environment of the user account for connecting to the target system Sample value: `DV812`
Role	Role of the user account for connecting to the target system Sample value: `*ALL`

Parameter	Description
ProxyUser	User ID of the system user in the target system **Note:** The ProxyUser ID value must be entered in uppercase.
ProxyUserPassword	Password of the system user in the target system **Note:** The ProxyUserPassword value must be entered in uppercase.
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`
Configuration Lookup	Name of the lookup definition that contains the configuration information used during connector operations. Default value: `Lookup.JDE.Configuration`

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.

    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 XML file is imported into Oracle Identity Manager.

2.5.3 Compiling Adapters

Note: Skip this section if you do not 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: Section 1.6.5, "Provisioning Functions" 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.

2.6 Configuring the Oracle Identity Manager Server

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

- Section 2.6.1, "Changing to the Required Input Locale"
- Section 2.6.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.6.3, "Enabling Logging"
- Section 2.6.4, "Configuring Trusted Source Reconciliation"
- Section 2.6.5, "Configuring Oracle Identity Manager for Request-Based Provisioning"

2.6.1 Changing to the Required Input Locale

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster.

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.

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

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager release 9.0.3.2 and release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to 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, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/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:

   For Oracle Identity Manager release 9.0.3.2 or release 9.1.0.*x*:

   ```
   OIM_HOME/xellerate/bin/SCRIPT_FILE_NAME
   ```

   For Oracle Identity Manager release 11.1.1:

   ```
   OIM_HOME/server/bin/SCRIPT_FILE_NAME
   ```

2. Enter one of the following commands:

Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *`CATEGORY_NAME`* on Microsoft Windows or `PurgeCache.sh` *`CATEGORY_NAME`* on UNIX. The *`CATEGORY_NAME`* argument represents the name of the content category that must be purged.

For example, the following commands purge Metadata entries from the server cache:

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

- For Oracle Identity Manager release 9.0.3.2 or release 9.1.0.*x*:

  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. This exception is different from the one mentioned in Step 1.

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

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

  When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

  `t3://`*`OIM_HOST_NAME`*`:`*`OIM_PORT_NUMBER`*

  In this format:

  – Replace *`OIM_HOST_NAME`* with the host name or IP address of the Oracle Identity Manager host computer.

  – Replace *`OIM_PORT_NUMBER`* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.6.3 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform the procedure described in one of the following sections:

- Section 2.6.3.1, "Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.2 or Release 9.1.0.x"
- Section 2.6.3.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.6.3.1 Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.2 or Release 9.1.0.*x*

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

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 might 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:

- **IBM WebSphere Application Server**

  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, 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, locate or add the following lines if they are not already present in the file:

```
<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, 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 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, log information is written to the following file:

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

- **Oracle WebLogic Server**

  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, log information is displayed on the server console.

2.6.3.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

Oracle Identity Manager release 11.1.1 uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. 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:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

  This level enables logging of messages that highlight the progress of the application.

- CONFIG

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

- FINE, FINER, FINEST

  These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in Table 2–2.

Table 2–2 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

```
<log_handler name='JDECONNECTOR' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='[FILE_NAME]'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="XL_INTG.JDECONNECTOR" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="jdeconnector-handler"/>
     <handler name="console-handler"/>
   </logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–2 lists the supported message type and level combinations.

      Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

      The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]** :

```
<log_handler name='JDECONNECTOR' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="OIMCP.JDECONNECTOR" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="jdeconnector-handler"/>
     <handler name="console-handler"/>
   </logger>
```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the `NOTIFICATION:1` level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

   Replace ***FILENAME*** with the location and name of the file to which you want to redirect the output.
4. Restart the application server.

2.6.4 Configuring Trusted Source Reconciliation

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:** 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. If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation bar.

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

3. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.
4. Locate and open the JDEConnectorXLResourceObject.xml file located in the following directory:
   - For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

     OIM_HOME/xellerate/ConnectorDefaultDirectory/JDE_***RELEASE_NUMBER***/xml
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ConnectorDefaultDirectory/JDE_***RELEASE_NUMBER***/xml

   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 Section 3.4, "Configuring Scheduled Tasks."

2.6.5 Configuring Oracle Identity Manager for Request-Based Provisioning

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

  > **Note:** Direct provisioning allows the provisioning of multiple target system accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

2.6.5.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following predefined request datasets are available in the DataSets directory on the installation media:

- ProvisionResourceJDE User.xml
- ModifyResourceJDE User.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\JDE

Note: Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide* for Oracle Identity Manager for information on modifying request datasets.

2.6.5.2 Importing Request Datasets into MDS

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

Note: While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.6.5.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\JDE directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

2. In a command window, change to the *OIM_HOME*\server\bin directory.
3. Run one of the following commands:
   - On Microsoft Windows

     `weblogicImportMetadata.bat`

   - On UNIX

     `weblogicImportMetadata.sh`

4. When prompted, enter the following values:
   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

     Enter the password used to log in to the WebLogic server.

   - `Please enter your server URL [t3://localhost:7001]`

     Enter the URL of the application server in the following format:

     `t3://`*`HOST_NAME_IP_ADDRESS`*`:`*`PORT`*

     In this format, replace:

     – *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

     – *PORT* with the port on which Oracle Identity Manager is listening.

   The request dataset is imported into MDS.

2.6.5.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**
3. Search for and open the **JDE Process** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.6.5.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.6.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to configure request-based provisioning ends with this step.

3

Using the Connector

This chapter is divided into the following sections:

> **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.

3.1 Performing First-Time Reconciliation

First-time reconciliation involves synchronizing lookup definitions in Oracle Identity Manager with the lookup fields of the target system, and performing full reconciliation. In full reconciliation, all existing user records from the target system are brought into Oracle Identity Manager.

The following is the sequence of steps involved in reconciling all existing user records:

> **Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

1. Perform lookup field synchronization by running the scheduled tasks provided for this operation.

See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about the attributes of the scheduled tasks for lookup field synchronization.

See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

2. Perform user reconciliation by running the scheduled task for user reconciliation.

   See Section 3.3.2, "User Reconciliation Scheduled Task" for information about the attributes of this scheduled task.

   See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

After first-time reconciliation, depending on the mode in which you configure the connector, the TimeStamp parameter of the JDE IT Resource IT resource is automatically set to the time stamp at which the reconciliation run began.

See Also: Section 2.4.2, "Configuring the IT Resource" for information about the parameters of the IT resource

From the next reconciliation run onward, only target system user records that are added or modified after the time stamp stored in the IT resource are considered for incremental reconciliation. These records are brought to Oracle Identity Manager when you configure and run the user reconciliation scheduled task.

3.2 Scheduled Task for Lookup Field Synchronization

Note: In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

The JDE LookUp Recon scheduled task is used for lookup field synchronization. Table 3–1 describes the attributes of this scheduled task. See Section 3.4, "Configuring Scheduled Tasks" for information about configuring 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.

Table 3–1 Attributes of the JDE LookUp Recon Scheduled Task

Attribute	Description
Language	Enter the code of the language to be used in the lookup reconciliation. Default value: `en`
Country	Enter the code of the country to be used in the lookup reconciliation. Default value: `us`
ITResource	Enter the name of the IT resource for setting up a connection to JD Edwards. Default value: `JDE IT Resource`
isRoleLookup	Enter `true` if you want to synchronize the Lookup.JDE.Roles lookup definition in Oracle Identity Manager with the target system. Enter `false` if you do not want to synchronize the Lookup.JDE.Roles lookup definition in Oracle Identity Manager with the target system. Default Value: `true`
isDateSeparationCharacterLookup	Enter `true` if you want to synchronize the Lookup.JDE.DateSeparationCharacter lookup definition in Oracle Identity Manager with the target system. Enter `false` if you do not want to synchronize the Lookup.JDE.DateSeparationCharacter lookup definition in Oracle Identity Manager with the target system. Default Value: `true`
isLanguageLookup	Enter `true` if you want to synchronize the Lookup.JDE.Language lookup definition in Oracle Identity Manager with the target system. Enter `false` if you do not want to synchronize the Lookup.JDE.Language lookup definition in Oracle Identity Manager with the target system. Default Value: `true`
isLocalizationCountryCodeLookup	Enter `true` if you want to synchronize the Lookup.JDE.LocalizationCountryCode lookup definition in Oracle Identity Manager with the target system. Enter `false` if you do not want to synchronize the Lookup.JDE.LocalizationCountryCode lookup definition in Oracle Identity Manager with the target system. Default Value: `true`
isDateFormatLookup	Enter `true` if you want to synchronize the Lookup.JDE.DateFormat lookup definition in Oracle Identity Manager with the target system. Enter `false` if you do not want to synchronize the Lookup.JDE.DateFormat lookup definition in Oracle Identity Manager with the target system. Default Value: `true`
isUniversalTimeLookup	Enter `true` if you want to synchronize the Lookup.JDE.UniversalTime lookup definition in Oracle Identity Manager with the target system. Enter `false` if you do not want to synchronize the Lookup.JDE.UniversalTime lookup definition in Oracle Identity Manager with the target system. Default Value: `true`

Table 3–1 (Cont.) Attributes of the JDE LookUp Recon Scheduled Task

Attribute	Description
isDecimalFormatCharacterLookup	Enter `true` if you want to synchronize the Lookup.JDE.DecimalFormatCharacter lookup definition in Oracle Identity Manager with the target system. Enter `false` if you do not want to synchronize the Lookup.JDE.DecimalFormatCharacter lookup definition in Oracle Identity Manager with the target system. Default Value: `true`
isTimeFormatLookup	Enter `true` if you want to synchronize the Lookup.JDE.TimeFormat lookup definition in Oracle Identity Manager with the target system. Enter `false` if you do not want to synchronize the Lookup.JDE.TimeFormat lookup definition in Oracle Identity Manager with the target system. Default Value: `true`
LanguagePreferenceForLookup	Enter the language setting for the lookup field entries. Depending on the language that you want to set, the value can be one of the following: ■ 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` Default Value: `E`

3.3 Configuring Reconciliation

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:

- Section 3.3.1, "Full Reconciliation"
- Section 3.3.2, "User Reconciliation Scheduled Task"

3.3.1 Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Manager.

To perform a full reconciliation run, set the TimeStamp parameter of the JDE IT Resource IT resource to `0`. At the end of the reconciliation run, this parameter is automatically set to the time stamp at which the run started. From the next reconciliation run onward, only records created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

3.3.2 User Reconciliation Scheduled Task

When you run the Connector Installer or import the connector XML file, the JDE User Recon scheduled task is automatically created in Oracle Identity Manager. This scheduled task is used to reconcile user data from the target system.

You must specify values for the following attributes of the JDE User Recon user reconciliation scheduled task. Table 3–2 describes the attributes of this 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.

Table 3–2 Attributes of the User Reconciliation Scheduled Task

Attribute	Description
Organization	Enter the name of the Oracle Identity Manager organization in which reconciled users must be created. Default value: `Xellerate Users`
Xellerate Type	Enter the role that must be set for OIM Users created through reconciliation. You can enter one of the following values: ▪ `End-User` ▪ `End-User Administrator` Default value: `End-User Administrator`
Role	Enter the employee type that must be set for OIM Users created through reconciliation. You can enter one of the following values: ▪ `Full-Time Employee` ▪ `Part-Time Employee` ▪ `Temp` ▪ `Intern` ▪ `Consultant` Default value: `Consultant`
ITResource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `JDE IT Resource`
ResourceObject	Enter the name of the resource object that is used in reconciliation. Default value: `JDE Resource Object`

Table 3–2 (Cont.) Attributes of the User Reconciliation Scheduled Task

Attribute	Description
isTrustedSource	Enter `true` if you want to configure the connector for trusted source reconciliation. Enter `false` if you want to configure the connector for target resource reconciliation. Default value: `false`
XLDeleteUsersAllowed	Enter `true` if you want to allow users to be deleted in Oracle Identity Manager during user reconciliation. Enter `false` if you do not want to allow users to be deleted in Oracle Identity Manager during user reconciliation. Default value: `false`
Configuration Lookup	This attribute contains the name of the lookup definition that stores configuration information used during connector operations. Default value: `Lookup.JDE.Configuration` **Note:** You must not change the value of this attribute.

3.4 Configuring Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table 3–3 lists the scheduled tasks that you must configure.

Table 3–3 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
JDE LookUp Recon	This scheduled task is used for lookup field synchronization. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about this scheduled task.
JDE User Recon	This scheduled task is used for user reconciliation. See Section 3.3.2, "User Reconciliation Scheduled Task" for information about this scheduled task.

Depending on the Oracle Identity Manager release that you are using, perform the procedure described in one of the following sections:

- Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.2 or Release 9.1.0.x"
- Section 3.4.2, "Configuring Scheduled Tasks on Oracle Identity Manager Release 11.1.1"

3.4.1 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.2 or Release 9.1.0.*x*

To configure a scheduled task:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder, and then select **Task Scheduler**.
3. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.

4. 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 `FAILED` status to the task.
5. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
6. 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.
7. 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.
8. Provide values for the attributes of the scheduled task.
9. 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.
10. Repeat Steps 4 through 9 to create the second scheduled task.

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 3 of the procedure to configure reconciliation scheduled tasks.
2. Select the **Stop Execution** check box in the task scheduler.
3. Click **Save**.

3.4.2 Configuring Scheduled Tasks on Oracle Identity Manager Release 11.1.1

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
   a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
   b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   c. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the following parameters:
   – **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

– **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

Note: See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

5. On the Job Details tab, in the Parameters region, specify values for the attributes of the 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 is left empty, then reconciliation is not performed.

6. Click **Apply** to save the changes.

Note: The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

3.5 Performing Provisioning Operations

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.6, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

See Also: *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- Section 3.5.1, "Direct Provisioning"

- Section 3.5.2, "Request-Based Provisioning"

3.5.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. From the Users menu, select **Create**.
     b. On the Create User page, enter values for the OIM User fields and then click **Create User**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
     b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM User, then:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. From the Users menu, select **Manage**.
     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.
     b. On the Resource Profile page, click **Provision New Resource**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the user details page, click the **Resources** tab.
     b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.
5. On the Step 1: Select a Resource page, select **JDE Resource Object** from the list and then click **Continue**.

6. On the Step 2: Verify Resource Selection page, click **Continue**.
7. On the Step 5: Provide Process Data for JDE User Details page, enter the details of the account that you want to create on the target system and then click **Continue**.
8. On the Step 5: Provide Process Data for User Role page, search for and select a role for the user on the target system and then click **Continue**.
9. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
10. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
    - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
    - If you are using Oracle Identity Manager release 11.1.1, then:
        a. Close the window displaying the "Provisioning has been initiated" message.
        b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.5.2 Request-Based Provisioning

Note: The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

Note: The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- Section 3.5.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.5.2.2, "Approver's Role in Request-Based Provisioning"

3.5.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.

3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account..

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **JDE Resource Object**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.5.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

3.6 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

Note: It is assumed that you have performed the procedure described in Section 2.6.5, "Configuring Oracle Identity Manager for Request-Based Provisioning."

On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **JDE Process** process definition.
   c. Deselect the **Auto Save Form** check box.
   d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **JDE Resource Object** resource object.
   c. Deselect the **Self Request Allowed** check box.
   d. Click the Save icon.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **JDE Process** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the Save icon.
3. If you want to enable end users to raise requests for themselves, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **JDE Resource Object** resource object.
   c. Select the **Self Request Allowed** check box.
   d. Click the Save icon.

4

Extending the Functionality of the Connector

The following section describes procedures that you can perform to extend the functionality of the connector for addressing your specific business requirements:

- Section 4.1, "Adding New Attributes for Target Resource Reconciliation"
- Section 4.2, "Adding New Attributes for Provisioning"

4.1 Adding New Attributes for Target Resource Reconciliation

Note: This section describes an optional procedure. You need not perform this procedure if you do not want to add new attributes for reconciliation.

By default, the attributes listed in Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning" are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation.

To add a new attribute for target resource reconciliation, perform the following procedure:

Note: You must ensure the new attributes that you add for reconciliation contain data in string-format only. Binary attributes must not be introduced into Oracle Identity Manager natively.

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the OIM User process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Search for and open the **UD_JDE** process form.
   d. Click **Create New Version**.
   e. In the **Label** field, enter the version name. For example, `version#1`.
   f. Click the Save icon.
   g. Select the current version created in Step e from the **Current Version** list.

h. Click **Add** to create a new attribute, and provide the values for that attribute.

For example, if you are adding the organization attribute, then enter the following values in the **Additional Columns** tab:

Field	Value
Name	AddressNumber
Variant Type	String
Length	100
Field Label	AddressNumber
Order	14

i. Click the Save icon.

j. Click **Make Version Active**.

3. Add the new attribute to the list of reconciliation fields in the resource object as follows:

a. Expand **Resource Management.**

b. Double-click **Resource Objects**.

c. Search for and open the **JDE Resource Object** resource object.

d. On the **Object Reconciliation** tab, click **Add Field**, and then enter the following values:

Field Name: `AddressNumber`

Field Type: `String`

e. Click the Save icon and then close the dialog box.

f. If you are using Oracle Identity Manager release 11.1.1, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

4. Create a reconciliation field mapping for the new attribute in the process definition form as follows:

a. Expand **Process Management.**

b. Double-click **Process Definition**.

c. Search for and open the **JDE Process** process definition.

d. On the **Reconciliation Field Mappings** tab, click **Add Field Map**, and then select the following values:

Field Name: `AddressNumber`

Field Type: `String`

Process Data Field: `AddressNumber`

e. Click the Save icon.

5. Create an entry for the attribute in the lookup definition for reconciliation as follows:

a. Expand **Administration**.

b. Double-click **Lookup Definition**.

c. Search for and open the **Lookup.JDEReconciliation.FieldMap** lookup definition.

d. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the attribute given in the resource object. The Decode value is the name of the attribute in the target system.

For example, enter `AN8` in the **Code Key** field and then enter `AddressNumber` in the **Decode** field.

e. Click the Save icon.

6. Add the new attribute to the **Lookup.JDE.Configuration** lookup definition as follows:

a. Expand **Administration**.

b. Double-click **Lookup Definition**.

c. Search for and open the **Lookup.JDE.Configuration** lookup definition.

d. Every attribute that you add belongs to a JDE database table. If the name of this JDE database table is already listed as the Code Key value, then enter the column name as Decode value.

Note: If you have more than one value in the Decode column, then each value must be separated by a comma (`,`).

---

e. If the name of this JDE database table is not listed as a Code Key value, then:

a. Click **Add.**

b. Enter the name of the JDE table as the **Code Key** value. For example, `TF0092`.

c. Enter the JDE table column name as the **Decode** value. For example, `Email`.

f. Click the Save icon.

4.2 Adding New Attributes for Provisioning

Note:

- This section describes an optional procedure. You need not perform this procedure if you do not want to add new attributes for provisioning.
- Before starting the following procedure, perform Steps 1 and 2 as described in Section 4.1, "Adding New Attributes for Target Resource Reconciliation." If these steps have been performed while adding new attributes for target resource reconciliation, then you need not repeat the steps.

By default, the attributes listed in Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning" are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a new attribute for provisioning:

1. Create an entry for the attribute in the lookup definition for provisioning as follows:
   a. Log in to the Oracle Identity Manager Design Console.
   b. Expand **Administration.**
   c. Double-click **Lookup Definition.**
   d. Search for and open the **Lookup.JDEProvisioning.FieldMap** lookup definition.
   e. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the attribute given in the resource object. The Decode value is the name of the attribute in the target system.

      For example, enter `UD_JDE_ADDRESSNUMBER` in the **Code Key** field and then enter `mnAddressNumber` in the Decode field.
   f. Click the Save icon.

   Note: Perform steps 2 through 4 only if you want to perform request-based provisioning.

2. Update the request dataset.

   When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:
   a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.
   b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

      See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

      For example, if you added Address Number as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Address Number"
attr-ref = "Address Number"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

      In this AttributeReference element:

      – For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

        For example, if UD_JDE_ADDRESS_NUMBER is the value in the Name column of the process form, then you must specify `Address Number` as the value of the name attribute in the AttributeReference element.

- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form.
- For the length attribute, enter the value that you entered in the Length column of the process form.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

3. Run the PurgeCache utility to clear content related to request datasets from the server cache.

   See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

4. Import into MDS the request dataset definitions in XML format.

   See Section 2.6.5.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

4.2.1 Enabling Update of New Attributes for Provisioning

After you add an attribute for provisioning, you must enable update operations on the attribute. If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of a new attribute for provisioning a user:

1. Expand **Process Management.**
2. Double-click **Process Definition** and open the **JDE Process** process definition.
3. In the process definition, add a new task for updating the field as follows:

   a. Click **Add** and enter the task name, for example, `AddressNumber Updated` and the task description.

   b. In the Task Properties section, select the following fields:

   - Conditional
   - Required for Completion
   - Allow Cancellation while Pending
   - Allow Multiple Instances

   c. Click on the Save icon.

4. On the Integration tab, click **Add,** and then click **Adapter.**
5. Select the **adpJDEMODIFYUSER** adapter, click **Save,** and then click **OK** in the message that is displayed.

6. To map the adapter variables listed in this table, select the adapter, click **Map,** and then specify the data given in the following table:

> **Note:** Some of the values in this table are specific to Address Number (`mnAddressNumber` value in the target system). These values must be replaced with values relevant to the attributes that you require.

Variable Name	Data Type	Map To	Qualifier	Literal Value
sPropertyName	String	Literal	String	mnAddressNumber
processKeyInstance	String	Process Data	Process Instance	NA
Adapter return value	Object	Response Code	NA	NA
JDEITResource	IT Resource	Process Data	IT Resource Type	NA
userID	String	Process Data	User ID	NA

7. Click the Save icon and then close the dialog box.

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 (OIM 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.

- The testing utility is not included from release 9.0.4.12 onward.

Index

R

S

T

X