Oracle® Identity Manager

Connector Guide for JD Edwards EnterpriseOne User Management

Release 11.1.1
E37672-12
July 2022

ORACLE

Oracle Identity Manager Connector Guide for JD Edwards EnterpriseOne User Management, Release 11.1.1

E37672-12

Primary Author: Gowri.G.R

Contributing Authors: Alankrita Prakash

Contents

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

5 Known Issues and Limitations

Index

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with JD Edwards EnterpriseOne.

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 that have purchased support 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, visit the following Oracle Help Center page: http://docs.oracle.com/cd/E52734_01/index.html

For information about Oracle Identity Manager Connectors documentation, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E22999_01/index.htm

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?

This chapter provides an overview of the updates made to the software and documentation for release 11.1.1.6.0 of the JD Edwards EnterpriseOne connector.

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 the software updates:

- Software Updates in Release 11.1.1.6.0
- Software Updates in Release 11.1.1.5.0

Software Updates in Release 11.1.1.6.0

The following are issues resolved in release 11.1.1.6.0:

Bug Number	Issue	Resolution
15920223	After re-installing the connector, job history of scheduled jobs that were run during the earlier installation were displayed.	This issue has been resolved. Job history of scheduled jobs that were run during an earlier installation are no longer displayed.
16053666	If you were using Oracle Identity Manager 11*g* Release 2 BP01, then you might have encountered a SQL exception error while running the scheduled job for user data reconciliation in the target system mode.	The minimum Oracle Identity Manager 11*g* Release 2 requirement for installting and using this connector is 11.1.2.0.4. Therefore, you no longer encounter this error.
16088723	The User ID attribute was missing while updating the request dataset.	This issue has been resolved.
16490410	The IT Resource Type field was incorrectly tagged as ITResource=JDE.	This issue has been resolved. The IT Resource Type field is now correctly tagged as ITResource=true.
16489930	When you created an access policy with the DLNA flag, the connector did not work as expected.	This issue has been resolved.

Software Updates in Release 11.1.1.5.0

The following are software updates in release 11.1.1.5.0:

- Support for Identity Connector Framework
- Support for Deployment Using Connector Server
- Connection Pooling
- Independent Scheduled Jobs for User Records and Deleted User Records Reconciliation, and Lookup Field Synchronization
- Transformation and Validation of Account Data
- Support for Configuring the Connector for Multiple Target System Versions

Support for Identity Connector Framework

The Oracle Identity Manager Connector for JD Edwards EnterpriseOne is an ICF-based connector.

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager and Oracle Waveset connectors require. The ICF also uses classpath isolation, which allows the JD Edwards EnterpriseOne connector to co-exist with legacy versions of the connector.

See Connector Architecture for more information.

Support for Deployment Using Connector Server

In the earlier releases, the JD Edwards EnterpriseOne connector could be deployed in the machine on which Oracle Identity Manager was running. This release onward, you can deploy this connector either locally in Oracle Identity Manager or remotely in the Connector Server.

See the following sections for more information:

- Installing the Connector on Oracle Identity Manager
- Deploying the Connector in a Connector Server

Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools will be created, one for each target system installation.

See Setting up the Lookup.JDE.Configuration Lookup Definition for Connection Pooling for more information.

Independent Scheduled Jobs for User Records and Deleted User Records Reconciliation, and Lookup Field Synchronization

In the earlier releases, you had one scheduled task for configuring your connector for user record and deleted user record reconciliation in both the target resource and trusted source mode. Similarly, you had one scheduled task for running lookup field synchronization.

From this release onward, you have independent scheduled jobs as follows:

- JDE User Target Reconciliation
- JDE User Trusted Reconciliation
- JDE User Target Delete Reconciliation
- JDE User Trusted Delete Reconciliation
- JDE Date Format Lookup Reconciliation
- JDE Date Separation Character Lookup Reconciliation
- JDE Decimal Format Characters Lookup Reconciliation
- JDE Languages Lookup Reconciliation
- JDE Localization Country Code Lookup Reconciliation
- JDE Roles Lookup Reconciliation
- JDE Time Format Lookup Reconciliation
- JDE Universal Time Lookup Reconciliation

See the following sections for more information about each of the scheduled jobs:

- Reconciliation Scheduled Jobs
- Scheduled Job for Lookup Field Synchronization

Transformation and Validation of Account Data

You can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. In addition, you can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. See the following sections for more information:

- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During Reconciliation

Support for Configuring the Connector for Multiple Target System Versions

From this release onward, you can configure the connector for target system installations of different versions. See Configuring the Connector for Multiple Installations of the Target System for more information.

Documentation-Specific Updates

The following sections discuss the documentation-specific updates:

Documentation-Specific Updates in Release 11.1.1.6.0

The following is a documentation-specific update in revision "11" of release 11.1.1.6.0:

The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance 12.2.1.3.0.

The following is a documentation-specific update in revision "10" of release 11.1.1.6.0:

A Known Issue about disable or enable account operation has been added to Known Issues and Limitations.

The following is a documentation-specific update in revision "9" of release 11.1.1.6.0:

The "Oracle Identity Manager" row of Table 1-1 has been renamed to "Oracle Identity Governance or Oracle Identity Manager" and also updated to include support for Oracle Identity Governance 12*c* (12.2.1.4.0).

The following are documentation-specific updates in revision "8" of release 11.1.1.6.0:

- The "Target system" row of Table 1-1 have been updated to inlcude support for JD Edwards EnterpriseOne Tools 9.2.1.4 and Application 9.2.
- A Note has been added to the "Connector Server JDK" row of Table 1-1 for information regarding JDK requirement.
- Steps 2 and 3 of Copying External Code Files have been modified.
- JDK requirement for JD Edwards EnterprisesOne Tools 9.2 and Application 9.2 has been added.
- Steps 5 and 6 of Installing the Connector on the Connector Server have been modified.

The following are documentation-specific updates in revision "7" of release 11.1.1.6.0:

- Step 2 of Copying External Code Files has been modified.
- Step 5 of Installing the Connector on the Connector Server has been modified.

The following are documentation-specific updates in revision "6" of release 11.1.1.6.0:

- The "Target system" row of Table 1-1 has been updated.
- The "JDK" row of Table 1-1 has been renamed to "Connector Server JDK".

The following are documentation-specific updates in revision "5" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of Table 1-1 has been updated.
- Information specific to Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) has been added to Usage Recommendation.

The following is a documentation-specific update in revision "4" of release 11.1.1.6.0:

A "Note" regarding lookup queries has been added at the beginning of Extending the Functionality of the Connector.

The following is a documentation-specific update in revision "3" of release 11.1.1.6.0:

Information about limited reconciliation has been modified in Limited Reconciliation.

The following are documentation-specific updates in revision "2" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row in Table 1-1 has been modified.
- A note has been added in the "xml/JDE-Datasets.xml" row of Table 2-1.
- The following sections have been added:
  - Usage Recommendation
  - Configuring Oracle Identity Manager 11.1.2 or Later
  - Localizing Field Labels in UI Forms
  - Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added in the following sections:
  - Postupgrade Steps
  - Adding New Attributes for Target Resource Reconciliation
  - Adding New Attributes for Provisioning
- The issues tracked by the following bug numbers have been removed from Known Issues and Limitations as they have been resolved:
  - 15920223
  - 16053666
  - 16088723

Documentation-Specific Updates in Release 11.1.1.5.0

There are no documentation-specific updates in this release of the connector.

1

About the Connector

Oracle Identity Manager automates access rights management, and the security of resources to various target systems. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with target 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, 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:

Certified Components

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

Table 1-1 Certified Components

Item	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) • Oracle Identity Manager 11*g* Release 2 (11.1.2.0.4) and any later BP in this release track • Oracle Identity Manager 11*g* Release 1 (11.1.1.5.6) BP06 (with patch 15971939) and any later BP in this release track
Target system	The target system can be any one of the following: • JD Edwards EnterpriseOne Tools 8.98 and Application 8.12 • JD Edwards EnterpriseOne Tools 9.1.2 and Application 9.0.2 • JD Edwards EnterpriseOne Tools 9.1.2 and Application 9.1 • JD Edwards EnterpriseOne Tools 9.1.4.2 and Application 9.1 • JD Edwards EnterpriseOne Tools 9.2.1.4 and Application 9.2 • JD Edwards Enterprise One Tools 9.2.2.5 and Application 9.2 **Note:** If you are using JDE Tools 9.2.*x*, download and apply JDE Connector 11.1.1.6.0A Patch 27009976 as reconciliation operations may throw NullPointerException error. You can download the patch from the Patches and Updates page at: https://support.oracle.com/
Connector Server	11.1.1.5.0
Connector Server JDK	JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later **Note:** If you are using JD Edwards EnterpriseOne Tools 9.2 and Application 9.2, see JDK requirement for JD Edwards EnterprisesOne Tools 9.2 and Application 9.2 for information related to JDK requirement.

Usage Recommendation

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

- If you are using an Oracle Identity Manager release that is earlier than Oracle Identity Manager 11g Release 1 (11.1.1), then you must use the 9.0.4.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) or later (such as Oracle Identity Manager 11*g* Release 1 (11.1.1.5.6) BP06), or Oracle Identity Manager 11*g* Release 2 (11.1.2) or later, or Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.*x* version of this connector.
- If you are using JD Edwards EnterpriseOne Tools 8.96 and Application 8.12 as the target system, then you must use the 9.0.4.*x* version of this connector, irrespective of the Oracle Identity Manager release you are using.

Certified Languages

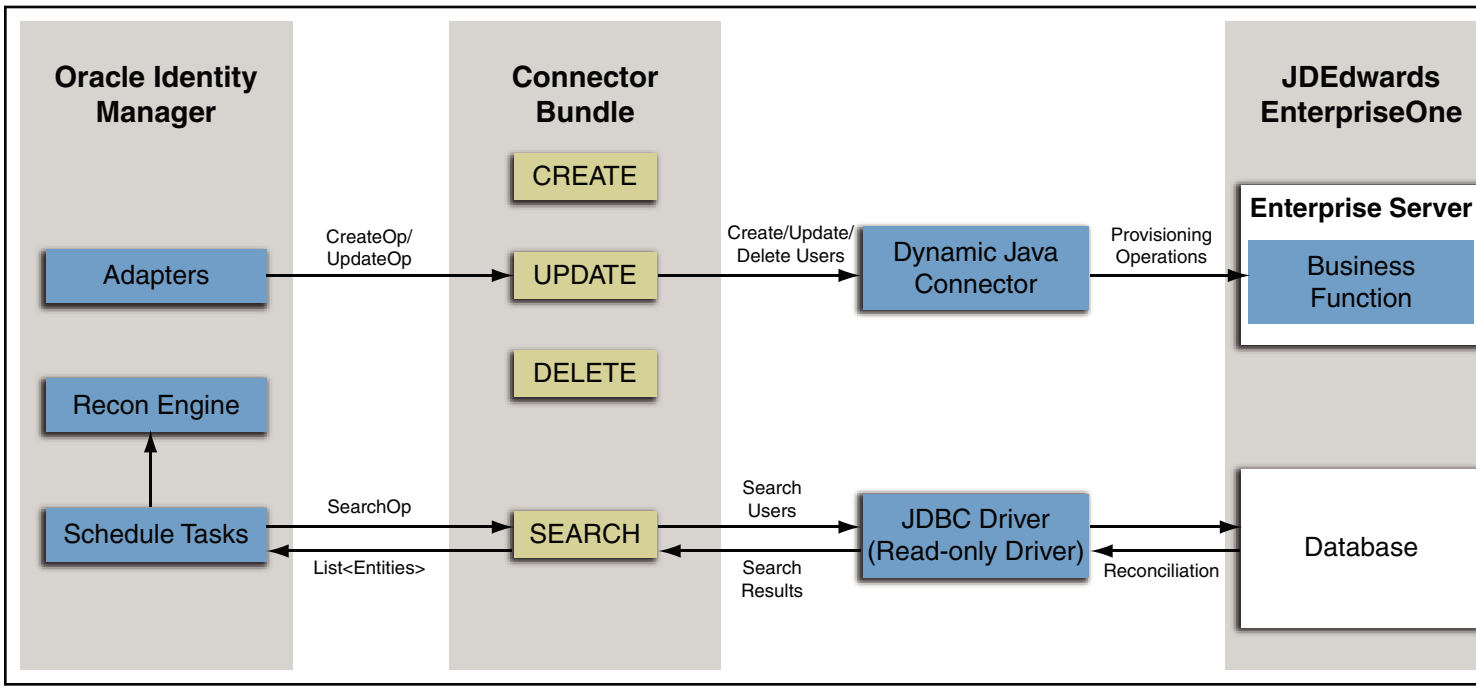
The connector supports the following languages:

- Arabic

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English (U.S.)
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

Connector Architecture

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



The JD Edwards EnterpriseOne User Management connector is implemented by using the Identity Connector Framework (ICF). The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Manager connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. The ICF is shipped along with Oracle Identity Manager. Therefore, you need not configure or modify the ICF.

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.

For provisioning operations such as Create, Update, and Delete, and reconciliation operations such as Search, Oracle Identity Manager makes SPI calls to ICF. In other words, Oracle Identity Manager invokes the connector bundle.

During provisioning, adapters carry provisioning data submitted through the process form to the target system. The adapters establish a connection with the connector bundle which inturn establishes a connection with a BSFN (for performing the required provisioning operation) in the target system by using the Dynamic Java Connector.

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

> **Note:**
>
> See *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about scheduled jobs.

During reconciliation, a schedule task is run which calls the SearchOp operation of the connector bundle. The connector bundle establishes a connection with the database by using the JDBC driver and retrieves all records that match the reconciliation criteria. This result is then passed to Oracle Identity Manager.

Features of the Connector

The following are features of the connector:

- Support for Both Target Resource and Trusted Source Reconciliation
- Full and Incremental Reconciliation
- Limited (Filtered) Reconciliation
- Support for Adding New Attributes for Reconciliation and Provisioning
- Reconciliation of Deleted User Records
- Transformation and Validation of Account Data
- Support for Connector Server
- Connection Pooling

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 Configuring Reconciliation for more information.

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. In incremental reconciliation, user accounts that have been added or modified since the last reconciliation run are fetched into Oracle Identity Manager.

You can perform a full reconciliation run at any time. See Performing Full Reconciliation for more information.

Limited (Filtered) Reconciliation

You can set a reconciliation filter as the value of the Filter attribute of the scheduled jobs. This filter specifies the subset of newly added and modified target system records that must be reconciled.

See Limited Reconciliation for more information.

Support for Adding New Attributes for Reconciliation and Provisioning

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

Reconciliation of Deleted User Records

You can reconcile data about user records that have been deleted on the target system that has been configured as a trusted source or target resource.

In target resource mode, if a user record is deleted on the target system, then the corresponding JDE User resource is revoked from the OIM User. In trusted source mode, if a user record is deleted on the target system, then the corresponding OIM User is deleted.

See Scheduled Job for Reconciliation of Deleted Users Records for more information about scheduled jobs used for reconciling data about deleted user records.

Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:

- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During Reconciliation

Support for Connector Server

Connector Server is a component provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles. In other words, a connector server enables remote execution of an Oracle Identity Manager connector.

A Java connector server is useful when you do not wish to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements.

Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools will be created, one for each target system installation.

Setting up the Lookup.JDE.Configuration Lookup Definition for Connection Pooling provides information about connection pooling.

Lookup Definitions Used During Connector Operations

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

- Lookup Definitions Synchronized with the Target System
- Preconfigured Lookup Definitions

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 jobs for lookup field synchronization:

> **See Also:**
>
> Scheduled Job for Lookup Field Synchronization for information about these scheduled tasks

- JDE Date Separation Character Lookup Reconciliation
- JDE Date Format Lookup Reconciliation
- JDE Decimal Format Characters Lookup Reconciliation
- JDE Languages Lookup Reconciliation
- JDE Localization Country Code Lookup Reconciliation
- JDE Roles Lookup Reconciliation
- JDE Time Format Lookup Reconciliation
- JDE Universal Time Lookup Reconciliation

Preconfigured Lookup Definitions

This section discusses 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. The other lookup definitions are as follows:

- Lookup.JDE.Configuration
- Lookup.JDE.Configuration.Trusted
- Lookup.JDE.UM.Configuration
- Lookup.JDE.UM.Configuration.Trusted
- Lookup.JDE.UM.ProvAttrMap
- Lookup.JDE.UM.ReconAttrMap
- Lookup.JDE.UM.ReconAttrMap.Trusted
- Lookup.JDE.UM.ReconDefaults.Trusted
- Lookup.JDE.FastPathCreate

Lookup.JDE.Configuration

The Lookup.JDE.Configuration lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

Table 1-2 lists the default entries in this lookup definition.

Table 1-2 Entries in the Lookup.JDE.Configuration Lookup Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.jde	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle class. Do *not* modify this entry.
Connector Name	org.identityconnectors.jde.JDEConnector	This entry holds the name of the connector class. Do *not* modify this entry.
preferredLanguage	E	This entry holds the preferred language in which the target system is installed and used internally by the connector to fetch appropriate lookup values based on the value of the field. Depending on the language that you want to set, the decode value of this entry 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`
User Configuration Lookup	Lookup.JDE.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.

Lookup.JDE.Configuration.Trusted

The Lookup.JDE.Configuration.Trusted lookup definition holds connector configuration entries that are used during trusted source reconciliation.

Table 1-3 lists the default entries in this lookup definition.

Table 1-3 Entries in the Lookup.JDE.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.jde	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle class. Do *not* modify this entry.
Connector Name	org.identityconnectors.jde.JDEConnector	This entry holds the name of the connector class. Do *not* modify this entry.
User Configuration Lookup	Lookup.JDE.UM.Configuration.Trusted	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.

Lookup.JDE.UM.Configuration

The Lookup.JDE.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a target resource.

Table 1-4 lists the default entries in this lookup definition.

Table 1-4 Entries in the Lookup.JDE.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.JDE.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.JDE.UM.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.JDE.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.JDE.UM.ReconAttrMap for more information about this lookup definition.

Lookup.JDE.UM.Configuration.Trusted

The Lookup.JDE.UM.Configuration.Trusted lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a trusted source.

Table 1-5 lists the default entries in this lookup definition.

Table 1-5 Entries in the Lookup.JDE.UM.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Recon Attribute Defaults	Lookup.JDE.UM.ReconDefaults.Trusted	This entry holds the name of the lookup definition that maps reconciliation fields and their default values. See Lookup.JDE.UM.ReconDefaults.Trusted for more information about this lookup definition.

Table 1-5 (Cont.) Entries in the Lookup.JDE.UM.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Recon Attribute Map	Lookup.JDE.UM.ReconAttrMap.Trusted	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.JDE.UM.ReconAttrMap.Trusted for more information about this lookup definition.

Lookup.JDE.UM.ProvAttrMap

The Lookup.JDE.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definitions is used during provisioning. This lookup definition is preconfigured. Table 1-11 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

Lookup.JDE.UM.ReconAttrMap

The Lookup.JDE.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured. Table 1-8 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Connector for more information.

Lookup.JDE.UM.ReconAttrMap.Trusted

The Lookup.JDE.UM.ReconAttrMap.Trusted lookup definition holds mappings between resource object fields and target system attributes. This lookup definitions is used during trusted source user reconciliation runs. This lookup definition is preconfigured. Table 1-12 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Connector for more information.

Lookup.JDE.UM.ReconDefaults.Trusted

The Lookup.JDE.UM.ReconDefaults.Trusted lookup definition holds mappings between reconciliation fields and their default values. This lookup definition is used when there is a mandatory field on the OIM User form, but no corresponding field in the target system from which values can be fetched during trusted source reconciliation.

Table 1-6 lists the default entries in this lookup definition.

Table 1-6 Entries in the Lookup.JDE.UM.ReconDefaults.Trusted Lookup Definition

Code Key	Decode
Employee Type	Full-Time
Organization	Xellerate Users
User Type	End-User

You add entries to this lookup definition in the following format, if required:

- **Code Key:** Name of the reconciliation field of the JDE User resource object
- **Decode:** Corresponding default value to be displayed

For example, assume a field named Preferred Language is a mandatory field on the OIM User form. Suppose the target system contains no field that stores information about the preferred language of communication for a user account. During reconciliation, no value for the Preferred Language field is fetched from the target system. However, as the Preferred Language field cannot be left empty, you must specify a value for this field. Therefore, create an entry in this lookup definition with the Code Key value set to Preferred Language and Decode value set to English. This implies that the value of the Preferred Language field on the OIM User form displays English for all user accounts reconciled from the target system.

Lookup.JDE.FastPathCreate

The Lookup.JDE.FastPathCreate lookup definition maps possible values for the Fast Path Create attribute of the target system with the corresponding values to be displayed in the Fast Path Create field of the OIM User form.

Table 1-7 lists the default entries in this lookup definition.

Table 1-7 Entries in the Lookup.JDE.FastPathCreate Lookup Definition

Code Key	Decode
N	No
Y	Yes

Connector Objects Used During Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified accounts on the target system and using this data to add or modify resources assigned to OIM Users.

The JDE User Target Reconciliation scheduled job is used to initiate a target resource reconciliation run. This scheduled job is discussed in Scheduled Jobs for Reconciliation of User Records.

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for conceptual information about reconciliation

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

- User Fields for Target Resource Reconciliation
- Reconciliation Rule for Target Resource Reconciliation
- Reconciliation Action Rules for Target Resource Reconciliation

User Fields for Target Resource Reconciliation

The Lookup.JDE.UM.ReconAttrMap lookup definition maps resource object fields and target system attributes. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, entries are in the following format:

- **Code Key:** Reconciliation field of the resource object
- **Decode:** Name of the target system attribute, prefixed with the table name. The following is the format in which you must enter the Decode value:

  TABLE_NAME.ATTR_NAME

  In this format, *TABLE_NAME* is the name of the table in the target system database in which the attribute is present. *ATTR_NAME* is the name of the attribute in the target system.

Table 1-8 provides information about user attribute mappings for target resource reconciliation.

Table 1-8 User Attributes for Target Resource Reconciliation

Resource Object Field	Target System Field
Date Format[LOOKUP]	F00921.FRMT
Date Separation Character[LOOKUP]	F00921.DSEP
Decimal Format Character[LOOKUP]	F00921.DECF
Fast Path Create	F0092.FSTP
Language[LOOKUP]	F00921.LNGP
Localization Country Code[LOOKUP]	F00921.CTR
ReturnValue	__UID__
Roles~Effective Date[DATE]	roles~JDERole~F95921.EFFDATE
Roles~Expiration Date[DATE]	roles~JDERole~F95921.EXPIRDATE
Roles~Include in ALL	roles~JDERole~F95921.FUROLE1
Roles~Role[LOOKUP]	roles~JDERole~F95921.FRROLE
Status	__ENABLE__

Table 1-8 (Cont.) User Attributes for Target Resource Reconciliation

Resource Object Field	Target System Field
Time Format[LOOKUP]	F00921.TIMEFORM
Universal Time[LOOKUP]	F00921.UTCTIME
User ID	__NAME__

Reconciliation Rule for Target Resource Reconciliation

This section contains the following topics:

- About Reconciliation Rule for Target Resource Reconciliation
- Viewing the Reconciliation Rule for Target Resource Reconciliation

> **See Also:**
>
> Creating Reconciliation Metadata in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about reconciliation matching and action rules

About Reconciliation Rule for Target Resource Reconciliation

The following is the process-matching rule:

Rule name: JDE Target Recon Rule

Rule element: User Login Equals UserID

In this rule:

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

Viewing the Reconciliation Rule for Target Resource Reconciliation

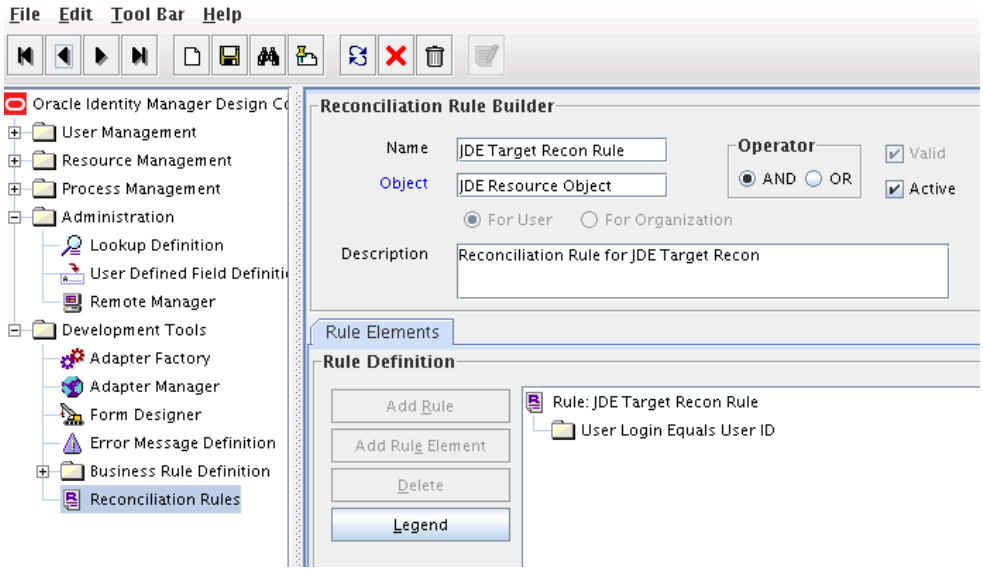
After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

> **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 1-1 shows the reconciliation rule for target resource reconciliation.

Figure 1-1 Reconciliation Rule for Target Resource Reconciliation



Reconciliation Action Rules for Target Resource Reconciliation

This section contains the following topics:

- About Action Rules for Target Resource Reconciliation
- Viewing the Action Rules for Target Resource Reconciliation

About Action Rules for Target Resource Reconciliation

Table 1-9 lists the action rules for target resource reconciliation.

Table 1-9 Action Rules for Target Resource Reconciliation

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

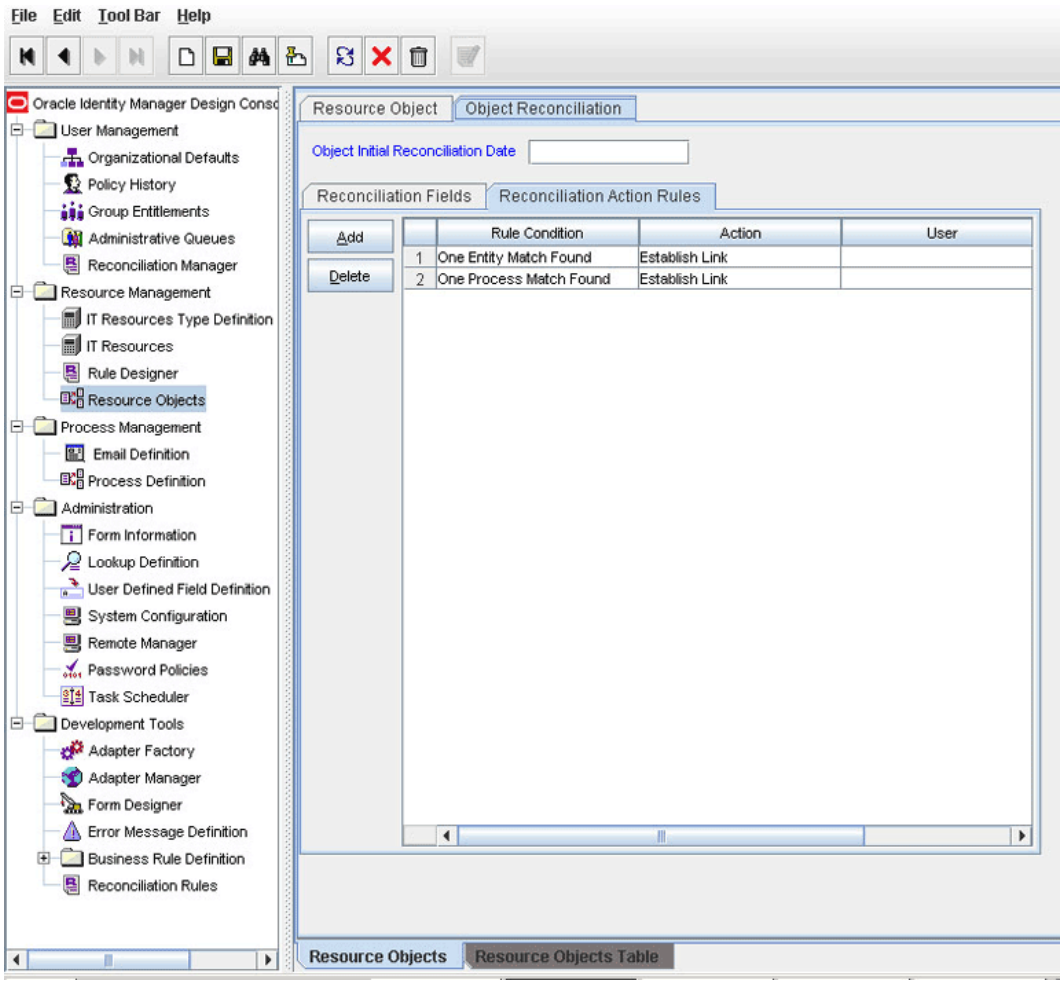
> **Note:**
>
> No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see Setting a Reconciliation Action Rule in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

Viewing the Action Rules for Target Resource Reconciliation

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 1-2 shows the reconciliation action rule for target resource reconciliation.

Figure 1-2 Reconciliation Action Rules for Target Resource Reconciliation



Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

> **See Also:**
>
> Managing Provisioning Tasks in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for conceptual information about provisioning

This section discusses the following topics:

- Provisioning Functions
- User Fields for Provisioning

Provisioning Functions

Table 1-10 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 1-10 Provisioning Functions

Function	Adapter
Create User	adpJDEUSERCREATE
Update User	adpJDEUPDATEUSER
Enable User	adpJDEENABLEUSER
Disable User	adpJDEDISABLEUSER
Delete User	adpJDEUSERDELETE
Add User Role	adpJDEADDROLETOUSER
Update User Role	adpJDEUPDATEROLE
Remove User Role	adpJDEREMOVEUSERROLE
Update a multiple attributes (for example, Date Format, Time Format, and Localization) together	adpJDEMULTIUPDATE

User Fields for Provisioning

The Lookup.JDE.UM.ProvAttrMap lookup definition maps process form fields with target system attributes. This lookup definition is used for performing user provisioning operations.

Table 1-11 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-11 Entries in the Lookup.JDE.UM.ProvAttrMap lookup definition

Process Form Field	Target System Field
Date Format[LOOKUP]	szDateformat
Date Separation Character[LOOKUP]	cDateSeparator
Decimal Format Character[LOOKUP]	cDecimalFormat
Fast Path Create	cFastPathCreate
Language[LOOKUP]	szLanguagePreference
Localization Country Code[LOOKUP]	szCountry
Password	__PASSWORD__
ReturnValue	__UID__
Time Format[LOOKUP]	szTimeFormat
UD_JDEROL~Effective Date[DATE]	roles~JDERole~jdEffectiveDate
UD_JDEROL~Expiration Date[DATE]	roles~JDERole~jdExpirationDate
UD_JDEROL~Include in *ALL	roles~JDERole~cIncludedInALL
UD_JDEROL~Role[LOOKUP]	roles~JDERole~szRole
Universal Time[LOOKUP]	szUniversalTime
User ID	__NAME__

Connector Objects Used During Trusted Source Reconciliation

Trusted source reconciliation involves fetching data about newly created or modified accounts on the target system and using that data to create or update OIM Users.

> **See Also:**
>
> Trusted Source Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for conceptual information about trusted source reconciliation

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

- User Fields for Trusted Source Reconciliation
- Reconciliation Rule for Trusted Source Reconciliation
- Reconciliation Action Rules for Trusted Source Reconciliation

User Fields for Trusted Source Reconciliation

The Lookup.JDE.UM.ReconAttrMap.Trusted lookup definition maps user fields of the OIM User form with corresponding field names in the target system. This lookup definition is used for performing trusted source reconciliation runs.

Table 1-12 lists user attributes for trusted source reconciliation.

Table 1-12 Entries in the Lookup.JDE.UM.ReconAttrMap.Trusted Lookup Definition

OIM User Form Field	Target System Field
Last Name	__NAME__
Status[TRUSTED]	__ENABLE__
User ID	__NAME__

Reconciliation Rule for Trusted Source Reconciliation

This section contains the following topics:

- About Reconciliation Rule for Trusted Source Reconciliation
- Viewing the Reconciliation Rule for Trusted Resource Reconciliation

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for generic information about reconciliation matching and action rules

About Reconciliation Rule for Trusted Source Reconciliation

The following is the process matching rule:

Rule name: JDE Trusted Recon Rule

Rule element: User Login Equals User ID

In this rule element:

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

Viewing the Reconciliation Rule for Trusted Resource Reconciliation

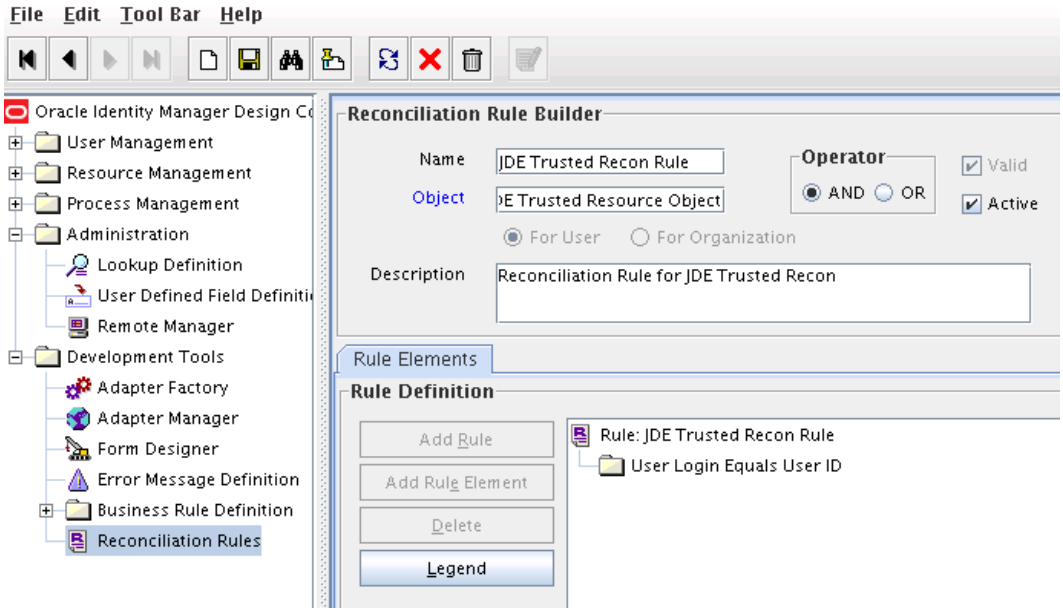
After you deploy the connector, you can view the reconciliation rule for trusted source reconciliation by performing the following steps:

> **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 1-3 shows the reconciliation rule for trusted source reconciliation.

Figure 1-3 Reconciliation Rule for Trusted Source Reconciliation



Reconciliation Action Rules for Trusted Source Reconciliation

This section contains the following topics:

- About Action Rules for Trusted Source Reconciliation
- Viewing the Actions Rules for Trusted Source Reconciliation

About Action Rules for Trusted Source Reconciliation

Table 1-13 lists the action rules for target resource reconciliation.

Table 1-13 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

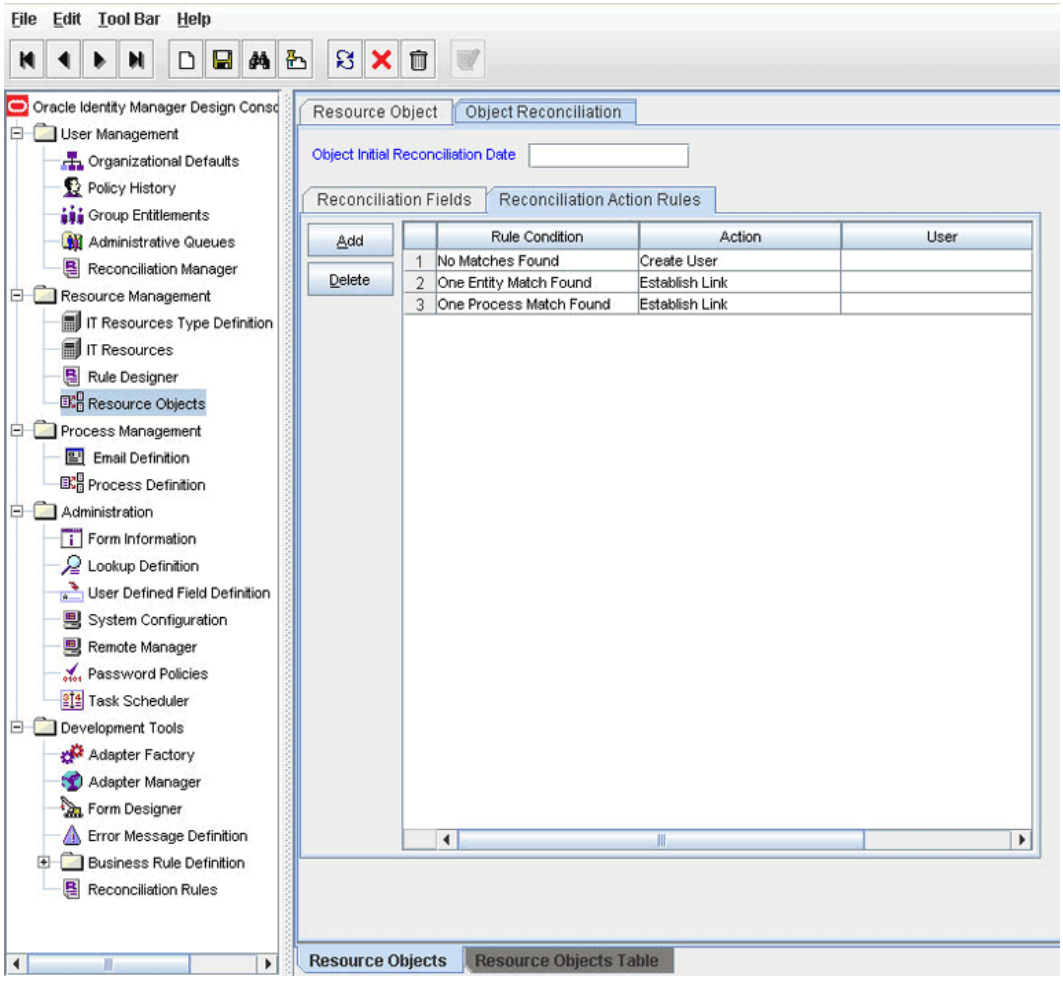
> **Note:**
>
> No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See Setting a Reconciliation Action Rule in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about modifying or creating reconciliation action rules.

Viewing the Actions Rules for Trusted Source Reconciliation

After you deploy the connector, you can view the reconciliation action rules for trusted source 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 Trusted 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 1-4 shows the reconciliation action rules for trusted source reconciliation.

Figure 1-4 Reconciliation Action Rules for Trusted Source Reconciliation



Roadmap for Deploying and Using the Connector

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

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

2
Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- Preinstallation
- Installation
- Postinstallation
- Upgrading the Connector
- Postcloning Steps

Preinstallation

Preinstallation information is divided across the following sections:

- Preinstallation on Oracle Identity Manager
- Preinstallation on the Target System

Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Files and Directories on the Installation Media
- Copying External Code Files
- Configuring the JDE Property Files
- Files and Property Values
- JDK requirement for JD Edwards EnterprisesOne Tools 9.2 and Application 9.2

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 Installation Media

File in the Installation Media Directory	Description
bundle/org.identityconnectors.jde-1.0.1115.jar	This JAR file contains the connector bundle.
configuration/JDE-CI.xml	This XML file contains configuration information that is used during the connector installation process.
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 Oracle Identity Manager database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages.

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

File in the Installation Media Directory	Description
upgrade/PostUpgradeScript.sql	This file is used during connector upgrade procedure.
xml/JDE-ConnectorConfig.xml	This XML file contains definitions for the following components of the connector: • Resource objects • IT resource types • IT resource instance • Process forms • Process tasks and adapters • Process definition • Prepopulate rules • Lookup definitions • Reconciliation rules • Scheduled jobs
xml/JDE-Datasets.xml	This XML file contains dataset related definitions for the create and modify user provisioning operations. This file is used if you want to enable request-based provisioning. You import this XML file into Oracle Identity Manager by using the Deployment Manager. **Note:** This dataset must *not* be imported if you are using Oracle Identity Manager release 11.1.2.*x* or later.

Copying External Code Files

You must copy the external code files as follows:

1. Create a directory named JDE-***RELEASE_NUMBER*** under the following directory:

   OIM_HOME/server/ConnectorDefaultDirectory/targetsystems-lib/

2. Copy the following JAR files from the *JDE_INSTALLATION_DIR*/E812/DDP/system/classes directory on the JD Edwards EnterpriseOne server to the *OIM_HOME*/server/ConnectorDefaultDirectory/targetsystems-lib/JDE-***RELEASE_NUMBER*** directory:

   > **Note:**
   >
   > If you are using JD Edwards EnterpriseOne Tools 8.98 and you want to configure SSL communication between Oracle Identity Manager and the target system, then obtain the JAR files listed in this step from the *JDE_INSTALLATION_DIR*/E812/DDP/system/classes directory of the JD Edwards EnterpriseOne Tools 8.98.4.11 or later versions.

   - ApplicationAPIs_JAR.jar
   - Base_JAR.jar
   - BizLogicContainerClient_JAR.jar
   - BizLogicContainer_JAR.jar

- castor.jar
- commons-codec.jar

  If you are using JD Edwards EnterpriseOne Tools 8.98, then copy the commons-codec-1.3.jar instead.
- httpclient.jar

  If you are using JD Edwards EnterpriseOne Tools 8.98, then copy the commons-httpclient-3.0.jar instead.
- commons-logging.jar

  If you are using JD Edwards EnterpriseOne Tools 8.98, then copy the commons-logging-1.1.jar instead.
- Connector.jar
- JdbjBase_JAR.jar
- JdbjInterfaces_JAR.jar
- JdeNet_JAR.jar
- jmxremote_optional.jar
- Metadata.jar
- MetadataInterface.jar
- PMApi_JAR.jar
- Spec_JAR.jar
- System_JAR.jar
- xerces.jar
- ManagementAgent_JAR.jar
- SystemInterfaces_JAR.jar
- If you are using JD Edwards EnterpriseOne Tools 9.2, then copy the following JAR files:
  - httpcore.jar
  - xml-apis.jar
  - commons-lang-2.6.jar

3. Raise a proof of concept (POC) request with the JD Edwards EnterpriseOne team to obtain the e1dadriver.jar file for the corresponding JDE target version.

   If you are using JDE 9.2.*x* target, raise a POC request for bug 27064458 with the JD Edwards EnterpriseOne team to obtain the e1dadriver.jar file.
4. Copy the e1dadriver.jar file to the *OIM_HOME*/server/ConnectorDefaultDirectory/targetsystems-lib/JDE-***RELEASE_NUMBER*** directory.

Configuring the JDE Property Files

You must modify the jdbj.ini, jdeinterop.ini, and jdelog.properties files to suit your deployment requirements. To do so:

1. Extract the following template files from the *JDE_INSTALLATION_DIR*/system/classes/samples/ConnectorSamples.zip file:

- jdbj.ini.templ
- jdeinterop.ini.templ
- jdelog.properties

2. Rename the jdbj.ini.templ file to jdbj.ini, and rename the jdeinterop.ini.templ file to jdeinterop.ini.
3. Modify the jdbj.ini, jdeinterop.ini, and jdelog.properties files to suit your deployment requirements. The values to be specified for the properties in each of these files is discussed later in this section. Alternatively, you can specify values for the properties in the jdbj.ini and jdeinterop.ini files by copying values from the *JDE_HTML_SERVER_HOME*/config/jas.ini file.
4. Save the changes made to the files.

Files and Property Values

This section discusses the following files and the values to be specified for the properties in each of these files:

- jdbj.ini
- jdeinterop.ini
- jdelog.properties

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

jdbj.ini

You 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

Property	Description
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=true`
unicode	Boolean value that indicates support for Unicode conversion is supported. This is applicable for Microsoft SQL Server. Sample value: `unicode=false`

> **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=tnsnames.ora
```

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

Section in the File	Property/Sample Value	Description
	codePage=1252	Code page number for a particular language
[SECURITY]	SecurityServer=ibm1	Name of the security server **Note:** The security server is the same as the EnterpriseOne server.
[INTEROP]	enterpriseServer=ibm1	Name of the EnterpriseOne server
	port=6014	Port number to connect to EnterpriseOne server

jdelog.properties

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

JDK requirement for JD Edwards EnterprisesOne Tools 9.2 and Application 9.2

The following are the JDK requirements if you are using JD Edwards EnterpriseOne Tools 9.2 and Application 9.2:

- If you are using a Connector Server, then it is mandatory to use JDK 1.7.0_40 as the minimum version in the Connector Server.

- If the you are not using a Connector Server and Oracle Identity Manager is not using JDK 1.7.0_40, then perform one of the following:
  - Refer to the Oracle Identity Manager certification matrix and upgrade the JDK version used by Oracle Identity Manager to JDK 1.7.0_40 if it is supported.
  - If JDK 1.7.0_40 is not supported for Oracle Identity Manager, then it is mandatory to use a Connector Server with minimum version JDK of 1.7.0_40. In addition, enter the name of this Connector Server as the value of the Connector Server name parameter of the IT resource.

Preinstallation on the Target System

Preinstallation on the target system involves performing the procedures described in the following sections:

- Applying a Patch for Revoking a User Account
- Creating a Target System User Account for Connector Operations

Applying a Patch for Revoking a User Account

For the connector to successfully revoke user accounts by using BSFNs, you must apply a patch on the target system. Contact JD Edwards support to obtain and apply the patch for bug 15836361 for your target system version.

Creating a Target System User Account for Connector Operations

Oracle Identity Manager requires a target system user account to access the target system during reconciliation and provisioning operations. You provide the credentials of this user account while performing the procedure described in Configuring the IT Resource.

To create this target system account with minimum rights, you must create user in the target system and assign the SYSADMIN role. The following steps describe this procedure:

1. Log in to Oracle JD Edwards EnterpriseOne user interface.
2. From the **Navigator** menu, select **EnterpriseOne Menus, EnterpriseOne Life Cycle Tools, System Administration Tools, User Management,** and then **User Profiles.**
3. Click the Add (+) icon and provide all user profile details such as User ID, Language, Date Format, and so on.
4. Click the Save icon to create the user profile.
5. From the **Navigator** menu, select **EnterpriseOne Menus, EnterpriseOne Life Cycle Tools, System Administration Tools, User Management,** and then **Role Relationships.**
6. In the Role Relationships page, search for the user created in Step 3.
7. Expand the **Available Roles** folder, and select the **SYSADMIN (JDE Install/ Upgrade Group)** role, and then move it to the Assigned Roles region.
8. Select the **Include *ALL** option.

9. From the **Navigator** menu, select **EnterpriseOne Menus, EnterpriseOne Life Cycle Tools, System Administration Tools, Security Maintenance,** and then **User Security.**
10. On the User Security page, click the Add (+) icon, and search for the user created in Step 3 as follows:
    a. On the User Security - Security Revisions page, click the lookup icon next to the User ID field. The User Search & Select dialog box is displayed.
    b. Search for and select the user, and then click the Select icon (the green check mark). The selected user is displayed in the User ID field.
11. On the User Security - Security Revisions page, specify values for the Data Source, System User, and Password fields.
12. In the User Status section, ensure that the Enabled option is selected.
13. Click the Save icon.

Installation

Depending on where you want to run the connector code (bundle), the connector provides the following installation options:

- To run the connector code locally in Oracle Identity Manager, perform the procedure described in Installing the Connector on Oracle Identity Manager.
- To run the connector code remotely in a Connector Server, perform the procedures described in Installing the Connector on Oracle Identity Manager and Deploying the Connector in a Connector Server.

Installing the Connector on Oracle Identity Manager

> **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 involves the following procedures:

- Running the Connector Installer
- Modifying the Connector Bundle
- Configuring the IT Resource
- IT Resource Parameters

Running the Connector Installer

To run the Connector Installer:

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

   OIM_HOME/server/ConnectorDefaultDirectory

2. If you have not already done so, create a directory in *OIM_HOME*/server/ConnectorDefaultDirectory/targetsystems-lib with the same name as the connector package. For the JD Edwards connector, this name is JDE-11.1.1.5.0. For example:

   OIM_HOME/server/ConnectorDefaultDirectory/targetsystems-lib/jde-11.1.1.5.0

   Copy the external JAR files to this directory. See Copying External Code Files for more information.

3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager release 11.1.1.*x*:

     a. Log in to the Administrative and User Console by using the user account described in Creating User Account for Installing Connectors of *Oracle Fusion Middleware Administering Oracle Identity Manager.*

     b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector.**

   - For Oracle Identity Manager release 11.1.2.*x* or later:

     a. Log in to Oracle Identity System Administration.

     b. In the left pane, under System Management, click **Manage Connector.**

4. In the Manage Connector page, click **Install.**

5. 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.***

6. Click **Load**.

7. 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.

8. 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 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 to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2-1.

Modifying the Connector Bundle

You must modify the connector bundle to include the jdbj.ini, jdeinterop, jdelog.properties and tnsnames.ora files. To do so:

1. Run the Oracle Identity Manager Download JARs utility to download the org.identityconnectors.jde-1.0.1115.jar file from the database. This utility is copied into the following location when you install Oracle Identity Manager:

> **Note:**
>
> Before you use 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/DownloadJars.bat

- **For UNIX:**

  OIM_HOME/server/bin/DownloadJars.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 downloaded, and the location to which the JAR file is to be downloaded. Specify `4` (ICFBundle) as the value of the JAR type.

2. Update the org.identityconnectors.jde-1.0.1115.jar file as follows:

a. Extract the contents of the org.identityconnectors.jde-1.0.1115.jar file into a temporary directory.

b. Copy the jdbj.ini, jdeinterop, jdelog.properties and tnsnames.ora files at the same level as the lib or org directory.

c. Re-create the org.identityconnectors.jde-1.0.1115.jar file by running the following command:

```
jar -cvfm org.identityconnectors.jde-1.0.1115.jar META-INF/MAINFEST.MF *
```

> **Note:**
>
> While re-creating the JAR file, ensure that META-INF\MANIFEST.MF file is unchanged.

3. Run the Oracle Identity Manager Upload JARs utility to upload the org.identityconnectors.jde-1.0.1115.jar file to the database. This utility is copied into the following location when you install Oracle Identity Manager:

> **Note:**
>
> Before you use 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. Specify `4` (ICFBundle) as the value of the JAR type.

4. Purge the cache to get the changes reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* for information on purging cache.

Configuring the IT Resource

> **Note:**
>
> If you have configured your target system as a trusted source, then create an IT resource of type **JDE.** For example, JDE Trusted. The parameters of this IT resource are the same as the parameters of the IT resources described in Table 2-2 of this section. See Creating IT Resources in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about creating an IT resource.

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

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.*x*:

     Log in to the Administrative and User Console
   - For Oracle Identity Manager release 11.1.2.*x* or later:

     Log in to Oracle Identity System Administration
2. If you are using Oracle Identity Manager release 11.1.1.*x,* 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 Configuration region, click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then in the left pane, under Configuration, click **IT Resource.**
4. In the IT Resource Name field on the Manage IT Resource page, enter `JDE IT Resource` and then click **Search**. Alternatively, from the IT Resource Type menu, select **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. Table 2-2 describes each parameter of the JDE IT Resource.
8. To save the values, click **Update**.

IT Resource Parameters

Table 2-2 describes each parameter of the JDE IT Resource.

Table 2-2 Parameters of the JDE IT Resource for the Target System

Parameter	Description
Configuration Lookup	Name of the lookup definition that contains the configuration information used during reconciliation and provisioning. If you have configured your target system as a target resource, then enter `Lookup.JDE.Configuration`. If you have configured your target system as a trusted source, then enter `Lookup.JDE.Configuration.Trusted`. Default value: `Lookup.JDE.Configuration`
Connector Server Name	Name of the IT resource of the type "Connector Server." You create an IT resource for the Connector Server in Creating the IT Resource for the Connector Server. **Note:** Enter a value for this parameter only if you have deployed the JD Edwards connector in the Connector Server. Sample value: `JDE Connector Server`
environment	Environment of the user account for connecting to the target system Sample value: `DV812`

Table 2-2 (Cont.) Parameters of the JDE IT Resource for the Target System

Parameter	Description
loginPassword	Enter the password of the user account that you created by performing the procedure described in Creating a Target System User Account for Connector Operations.
loginUser	Enter the User ID of the user account that you created by performing the procedure described in Creating a Target System User Account for Connector Operations.
proxyUser	User ID of the system user in the target system
proxyUserPassword	Password of the system user in the target system
Role	Role of the user account for connecting to the target system Sample value: `*ALL`

Deploying the Connector in a Connector Server

You can deploy the JD Edwards connector either locally in Oracle Identity Manager or remotely in the Connector Server. A **connector server** is an application that enables remote execution of an Identity Connector, such as the JD Edwards connector.

> **Note:**
>
> - To deploy the connector bundle remotely in a Connector Server, you must first deploy the connector in Oracle Identity Manager, as described in Installing the Connector on Oracle Identity Manager.
> - See Creating the IT Resource for the Connector Server for related information.

This procedure can be divided into the following stages:

- Installing and Configuring the Connector Server
- Running the Connector Server
- Installing the Connector on the Connector Server

Installing and Configuring the Connector Server

Connector servers are available in two implementations:

- As a .Net implementation that is used by Identity Connectors implemented in .Net
- As a Java Connector Server implementation that is used by Java-based Identity Connectors

The JD Edwards connector is implemented in Java, so you can deploy this connector to a Java Connector Server.

Use the following steps to install and configure the Java Connector Server:

> **Note:**
>
> Before you deploy the Java Connector Server, ensure that you install the JDK or JRE on the same computer where you are installing the Java Connector Server and that your *JAVA_HOME* or *JRE_HOME* environment variable points to this installation.

1. Create a new directory on the computer where you want to install the Java Connector Server.

   > **Note:**
   >
   > In this guide, *CONNECTOR_SERVER_HOME* represents this directory.

2. Unzip the Java Connector Server package in the new directory created in Step 1. You can download the Java Connector Server package from the Oracle Technology Network.
3. Open the ConnectorServer.properties file located in the `conf` directory. In the ConnectorServer.properties file, set the following properties, as required by your deployment.

Property	Description
connectorserver.port	Port on which the Java Connector Server listens for requests. Default is `8763`.
connectorserver.bundleDir	Directory where the connector bundles are deployed. Default is `bundles`.
connectorserver.libDir	Directory in which to place dependent libraries. Default is `lib`.
connectorserver.usessl	If set to **`true`**, the Java Connector Server uses SSL for secure communication. Default is `false`. If you specify **`true`**, use the following options on the command line when you start the Java Connector Server: • `-Djavax.net.ssl.keyStore` • `-Djavax.net.ssl.keyStoreType` (*optional*) • `-Djavax.net.ssl.keyStorePassword`
connectorserver.ifaddress	Bind address. To set this property, uncomment it in the file (if necessary). The bind address can be useful if there are more NICs installed on the computer.
connectorserver.key	Java Connector Server key.

4. Set the properties in the ConnectorServer.properties file, as follows:
   - To set the connectorserver.key, run the Java Connector Server with the `/setKey` option.

> **Note:**
>
> For more information, see Running the Connector Server.

- For all other properties, edit the ConnectorServer.properties file manually.

5. The conf directory also contains the logging.properties file, which you can edit if required by your deployment.

> **Note:**
>
> Oracle Identity Manager has no built-in support for connector servers, so you cannot test your configuration.

Running the Connector Server

To run the Java Connector Server, use the ConnectorServer.bat script for Windows and use the ConnectorServer.sh script for UNIX as follows:

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Installing and Configuring the Connector Server.
2. Change to the *CONNECTOR_SERVER_HOME*\bin directory and find the ConnectorServer.bat script.

   The ConnectorServer.bat supports the following options:

Option	Description
`/install [serviceName] ["-J java-option"]`	Installs the Java Connector Server as a Windows service. Optionally, you can specify a service name and Java options. If you do not specify a service name, the default name is `ConnectorServerJava`.
`/run ["-J java-option"]`	Runs the Java Connector Server from the console. Optionally, you can specify Java options. For example, to run the Java Connector Server with SSL: `ConnectorServer.bat /run "-J-Djavax.net.ssl.keyStore=mykeystore.jks" "-J-Djavax.net.ssl.keyStorePassword=password"`
`/setKey [key]`	Sets the Java Connector Server key. The `ConnectorServer.bat` script stores the hashed value of the key in the `connectorserver.key` property in the `ConnectorServer.properties` file.
`/uninstall [serviceName]`	Uninstalls the Java Connector Server. If you do not specify a service name, the script uninstalls the `ConnectorServerJava` service.

3. If you need to stop the Java Connector Server, stop the respective Windows service.

Installing the Connector on the Connector Server

> **See Also:**
>
> Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing and configuring connector server and running the connector server

If you need to deploy the JD Edwards connector into the Java Connector Server, then follow these steps:

1. Stop the Java Connector Server.

   > **Note:**
   >
   > - You can download the necessary Java Connector Server from the Oracle Technology Network web page.
   > - Ensure that you are using latest framework JARs of Oracle Identity Manager to keep the Connector Server consistent with your Oracle Identity Manager instance. To do so:
   >
   >   Copy the framework JAR files, connector-framework.jar and connector-framework-internal.jar, from the *OIM_HOME*/server/ext/internal directory to the *CONNECTOR_SERVER_HOME*/lib/framework directory.

2. Copy the connector bundle JAR file (org.identityconnectors.jde-1.0.1115.jar) from the installation media into the Java Connector Server *CONNECTOR_SERVER_HOME*/bundles directory.
3. Copy the following JAR files into the *CONNECTOR_SERVER_HOME*/lib directory:
   - *JDE_INSTALLATION_DIRECTORY*/system/classes/xmlparserv2.jar
   - *WL_HOME*/server/ext/jdbc/oracle/11g/ojdbc5.jar
4. Extract the contents of the org.identityconnectors.jde-1.0.1115.jar file into a temporary directory.
5. In the lib directory, copy the following third-party JAR files from the *JDE_INSTALLATION_DIR*/E812/DDP/system/classes directory on the JD Edwards EnterpriseOne server:
   - ApplicationAPIs_JAR.jar
   - Base_JAR.jar
   - BizLogicContainerClient_JAR.jar
   - BizLogicContainer_JAR.jar
   - castor.jar
   - commons-codec.jar

If you are using JD Edwards EnterpriseOne Tools 8.98, then copy the commons-codec-1.3.jar instead.

- httpclient.jar

  If you are using JD Edwards EnterpriseOne Tools 8.98, then copy the commons-httpclient-3.0.jar instead.

- commons-logging.jar

  If you are using JD Edwards EnterpriseOne Tools 8.98, then copy the commons-logging-1.1.jar instead.

- Connector.jar
- JdbjBase_JAR.jar
- JdbjInterfaces_JAR.jar
- JdeNet_JAR.jar
- jmxremote_optional.jar
- Metadata.jar
- MetadataInterface.jar
- PMApi_JAR.jar
- Spec_JAR.jar
- System_JAR.jar
- xerces.jar
- ManagementAgent_JAR.jar
- SystemInterfaces_JAR.jar
- If you are using JD Edwards EnterpriseOne Tools 9.2, then copy the following JAR files:
  - httpcore.jar
  - xml-apis.jar
  - commons-lang-2.6.jar

6. Raise a proof of concept (POC) request with the JD Edwards EnterpriseOne team to obtain the e1dadriver.jar file for the corresponding JDE target version.

   If you are using JDE 9.2.*x* target, raise a POC request for bug 27064458 with the JD Edwards EnterpriseOne team to obtain the e1dadriver.jar file.

7. Copy the e1dadriver.jar file to lib directory. The lib directory is obtained after extracting the contents of the org.identityconnectors.jde-1.0.1115.jar file in Step 4.
8. Copy the jdbj.ini, jdeinterop.ini, jdelog.properties and tnsnames.ora files at the same level as the lib directory.
9. Re-create the connector bundle by running the following command:

   ```
   jar -cvfm org.identityconnectors.jde-1.0.1115.jar META-INF/MANIFEST.MF *
   ```

   While re-creating the connector bundle, ensure that the META-INF/MANIFEST.MF file remains unchanged.

10. Start the Java Connector Server.

Postinstallation

The following sections discuss postinstallation procedures:

- Configuring Oracle Identity Manager
- Creating the IT Resource for the Connector Server
- Configuring SSL

Configuring Oracle Identity Manager

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

- Configuring Oracle Identity Manager 11.1.2 or Later
- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Modifying the Hosts File
- Setting up the Lookup.JDE.Configuration Lookup Definition for Connection Pooling
- Enabling Logging
- Configuring Oracle Identity Manager for Request-Based Provisioning
- Localizing Field Labels in UI Forms

Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2 or later, you must create additional metadata such as a UI form and an application instance. In addition, you must run entitlement and catalog synchronization jobs. These procedures are described in the following sections:

- Creating and Activating a Sandbox
- Creating a New UI Form
- Creating an Application Instance
- Publishing a Sandbox
- Harvesting Entitlements and Sync Catalog

Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see Managing Sandboxes in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

1. Log in to Oracle Identity System Administration.
2. In the upper right corner of the page, click the **Sandboxes** link.

   The Manage Sandboxes page is displayed.
3. On the toolbar, click **Create Sandbox.**
4. In the Create Sandbox dialog box, enter values for the following fields:
   - **Sandbox Name:** Enter a name for the sandbox.

- **Sandbox Description:** Enter a description of the sandbox.

5. Click **Save and Close.**
6. Click **OK** on the confirmation message that is displayed.

   The sandbox is created and displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
8. On the toolbar, click **Activate Sandbox.**

   The sandbox is activated.

Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see Managing Forms in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

1. In the left pane, under Configuration, click **Form Designer.** The Form Designer page is displayed.
2. From the Actions menu, select **Create.** Alternatively, click **Create** on the toolbar. The Create Form page is displayed.
3. On the Create Form page, enter values for the following UI fields:
   - **Resource Type:** Select the resource object that you want to associate the form with. For example, **JDE Resource Object.**
   - **Form Name:** Enter a name for the form.
4. Click **Create.**

   A message is displayed stating that the form is created.

Creating an Application Instance

Create an application instance as follows. For detailed instructions, see Managing Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

1. In the left pane of the System Administration console, under Configuration, click **Application Instances.** The Application Instances page is displayed.
2. From the Actions menu, select **Create.** Alternatively, click **Create** on the toolbar. The Create Application Instance page is displayed.
3. Specify values for the following fields:
   - **Name:** The name of the application instance.
   - **Display Name:** The display name of the application instance.
   - **Description:** A description of the application instance.
   - **Resource Object:** The resource object name. Click the search icon next to this field to search for and select **JDE Resource Object.**
   - **IT Resource Instance:** The IT resource instance name. Click the search icon next to this field to search for and select **JDE IT Resource.**

- **Form:** Select the form name (created in Creating a New UI Form).

4. Click Save. The application instance is created.
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users.
   a. On the Organizations tab of the Application Instance page, click **Assign.**
   b. In the Select Organizations dialog box, select the organization to which you want to publish the application instance.
   c. Select the **Apply to entitlements** checkbox.
   d. Click **OK.**

> **See Also:**
>
> Managing Organizations Associated With Application Instances in *Oracle Fusion Middleware for Administering Oracle Identity Manager* for detailed instructions.

Publishing a Sandbox

To publish the sandbox that you created in Creating and Activating a Sandbox:

1. Close all the open tabs and pages.
2. In the upper right corner of the page, click the **Sandboxes** link.

   The Manage Sandboxes page is displayed.
3. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Creating and Activating a Sandbox.
4. On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.
5. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Scheduled Job for Lookup Field Synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

Changing to the Required Input Locale

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

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

Clearing Content Related to Connector Resource Bundles from the Server Cache

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database. 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, 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:
   >
   > `OIM_HOME/server/bin/SCRIPT_FILE_NAME`

2. Enter 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
   > ```

   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 Administering Oracle Identity Manager* for more information about the PurgeCache utility.

Modifying the Hosts File

> **Note:**
>
> Perform the procedure described in this section only if the target system and the computer hosting Oracle Identity Manager are in different domains.

If the target system and computer hosting Oracle Identity Manager are in different domains, then during connector operations the hostname may not be resolved and an "Unknown Host" error is encountered. To avoid this issue, modify the Hosts file as follows:

Depending on the operating system on which Oracle Identity Manager is running, perform one of the following steps:

- **For Microsoft Windows:**

  Edit the hosts file located in the C:\WINDOWS\system32\drivers\etc directory to include an entry for the computer hosting the target system.

- **For UNIX:**

  Edit the /etc/hosts file to add an entry for the computer hosting the target system. Note that to edit the /etc/hosts file, the Super User privileges are required.

The following is the format in which you must add the entry:

IP_ADDRESS DOMAIN_NAME ALIAS1 ALIAS2 . . .ALIASn

In this format, replace:

- *IP_ADDRESS* with the IP address of the computer hosting the target system.
- *DOMAIN_NAME* with the domain name of the computer hosting the target system
- *ALIAS1* with the alias for the computer hosting the target system. Similarly, replace *ALIAS2 . . . ALIASn* accordingly. Note that the alias entries are optional.

The following is a sample entry:

```
172.20.55.120 mydomain123.example.com mydomain123 MYDOMAIN123
```

Setting up the Lookup.JDE.Configuration Lookup Definition for Connection Pooling

This section contains the following topics:

- Connection Pooling Properties

- Modifying the Connection Pooling Properties

Connection Pooling Properties

By default, this connector uses the ICF connection pooling. Table 2-3 lists the connection pooling properties, their descriptions, and default values set in ICF:

Table 2-3 Connection Pooling Properties

Property	Description
Pool Max Idle	Maximum number of idle objects in a pool. Default value: `10`
Pool Max Size	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`
Pool Min Evict Idle Time	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	Minimum number of idle objects in a pool. Default value: `1`

Modifying the Connection Pooling Properties

If you want to modify the connection pooling properties to use values that suit requirements in your environment, then:

1. Log in to the Design Console.
2. Expand **Administration,** and then double-click **Lookup Definition.**
3. Search for and open the **Lookup.JDE.Configuration** lookup definition.
4. On the Lookup Code Information tab, click **Add.**

   A new row is added.
5. In the **Code Key** column of the new row, enter `Pool Max Idle`.
6. In the **Decode** column of the new row, enter a value corresponding to the Pool Max Idle property.
7. Repeat Steps 4 through 6 for adding each of the connection pooling properties listed in Table 2-3.
8. Click the Save icon.

Enabling Logging

This section contains the following topics:

- Log Levels
- Enabling Logging on Oracle WebLogic Server

Log Levels

Oracle Identity Manager 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 2-4.

Table 2-4 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.

Enabling Logging on Oracle WebLogic Server

To enable logging on Oracle WebLogic Server:

1. Edit the logging.xml file as follows:
   a. Add the following blocks in the file:

```
<log_handler name='jde-handler' 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="org.identityconnectors.jde" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="jde-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 2-4 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='jde-handler' 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
\oim_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="org.identityconnectors.jde" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="jde-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.

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.*x*.

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:

- Importing Request Datasets
- Enabling the Auto Save Form Feature
- Running the PurgeCache Utility

Importing Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation.

There are two ways of importing request datasets:

- Importing Request Datasets Using MDS Import Utility

- Importing Request Datasets Using Deployment Manager

> **Note:**
>
> Request Datasets imported either into MDS or by using Deployment Manager are same.

Importing Request Datasets Using MDS Import Utility

To import a request dataset definition into the metadata store (MDS):

1. Copy the predefined request dataset from the installation media to any directory on the Oracle Identity Manager host computer. The predefined request dataset is available in the xml/JDE-Datasets.xml file on the installation media. 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 JDE-Datasets.xml file is the MDS location into which this file is imported after you run the Oracle Identity Manager MDS Import utility.

2. Ensure that you have set the environment for running the MDS Import utility. See Migrating User Modifiable Metadata Files in *Oracle Fusion Middleware Developing and Customizing Applications 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 Step 1 of this procedure, 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`.

3. In a command window, change to the *OIM_HOME*\server\bin directory.
4. Run one of the following commands:

- On Microsoft Windows

  `weblogicImportMetadata.bat`

- On UNIX

  `weblogicImportMetadata.sh`

5. 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 at the following location:

   /custom/connector/*RESOURCE_NAME*

Importing Request Datasets Using Deployment Manager

The request datasets (predefined or generated) can also be imported by using the Deployment Manager (DM). The predefined request datasets are stored in the xml/JDE-Datasets.xml on the installation media.

To import a request dataset definition by using the Deployment Manager:

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 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 JDE-Datasets.xml file, which is located in the xml directory of the installation media.

   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**.

The request datasets are imported into MDS.

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.

Running the PurgeCache Utility

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

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

Localizing Field Labels in UI Forms

> **Note:**
>
> Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.*x* or later and you want to localize UI form field labels.

To localize field label that is added to the UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open one of the following files in a text editor:
   - For Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
   - For releases prior to Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:
   a. Search for the following text:

```
<file source-language="en"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

b. Replace with the following text:

```
<file source-language="en" target-language="LANG_CODE"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

In this text, replace *LANG_CODE* with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

```
<file source-language="en" target-language="ja"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

c. Search for the application instance code. This procedure shows a sample edit for JDE application instance. The original code is:

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_JDE
_LANGUAGE__c_description']}">
<source>Language</source>
</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.JDE.entity.JDEEO.UD_JDE_LANGUAG
E__c_LABEL">
<source>Language</source>
</target>
</trans-unit>
```

d. Open the resource file from the connector package, for example JDEdwards_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_JDE_LANGUAGE__c_LABEL=\u8A00\u8A9E.

e. Replace the original code shown in Step 6.b with the following:

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_JDE
_LANGUAGE__c_description']}">
<source>Language</source>
<target>\u8A00\u8A9E</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.JDE.entity.JDEEO.UD_JDE_LANGUAG
E__c_LABEL">
<source>Language</source>
<target>\u8A00\u8A9E</target>
</trans-unit>
```

f. Repeat Steps 6.a through 6.d for all attributes of the process form.

g. Save the file as BizEditorBundle_*LANG_CODE*.xlf. In this file name, replace *LANG_CODE* with the code of the language to which you are localizing.

Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

> **See Also:**
>
> Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager,* for more information about exporting and importing metadata files

8. Log out of and log in to Oracle Identity Manager.

Creating the IT Resource for the Connector Server

> **Note:**
>
> Perform the procedure described in this section *only* if you have deployed the connector bundle remotely in a Connector Server.

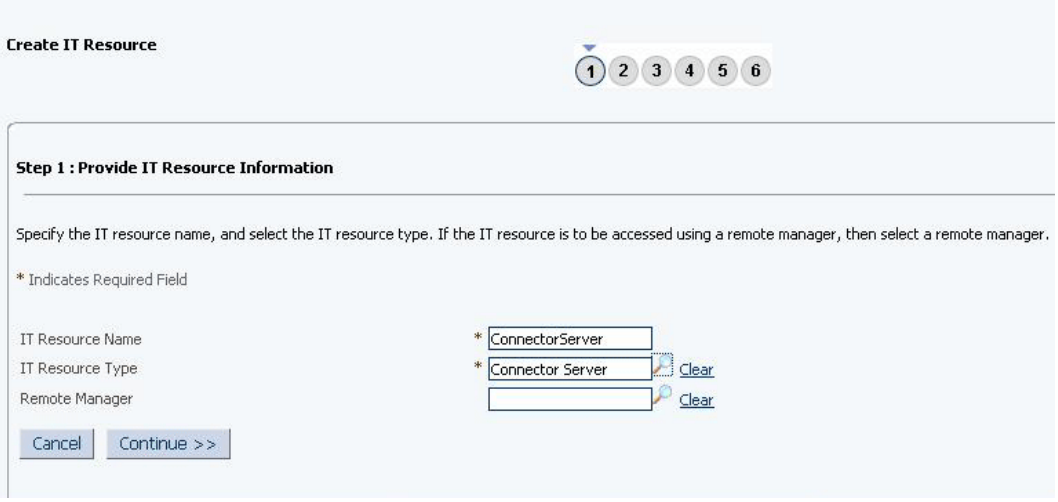
To create the IT resource for the Connector Server:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.*x:*

     Log in to the Administrative and User Console
   - For Oracle Identity Manager release 11.1.2.*x* or later:

     Log in to Oracle Identity System Administration
2. If you are using Oracle Identity Manager release 11.1.1.*x,* 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 Configuration region, click **Create IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:
   a. In the left pane, under Configuration, click **IT Resource.**
   b. In the Manage IT Resource page, click **Create IT Resource.**
4. On the Step 1: Provide IT Resource Information page, perform the following steps:
   - **IT Resource Name**: Enter a name for the IT resource.
   - **IT Resource Type**: Select **Connector Server** from the IT Resource Type list.
   - **Remote Manager**: Do not enter a value in this field.
5. Click **Continue**. Figure 2-1 shows the IT resource values added on the Create IT Resource page.

Figure 2-1 Step 1: Provide IT Resource Information



6. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. Figure 2-2 shows the Step 2: Specify IT Resource Parameter Values page.

Figure 2-2 Step 2: Specify IT Resource Parameter Values

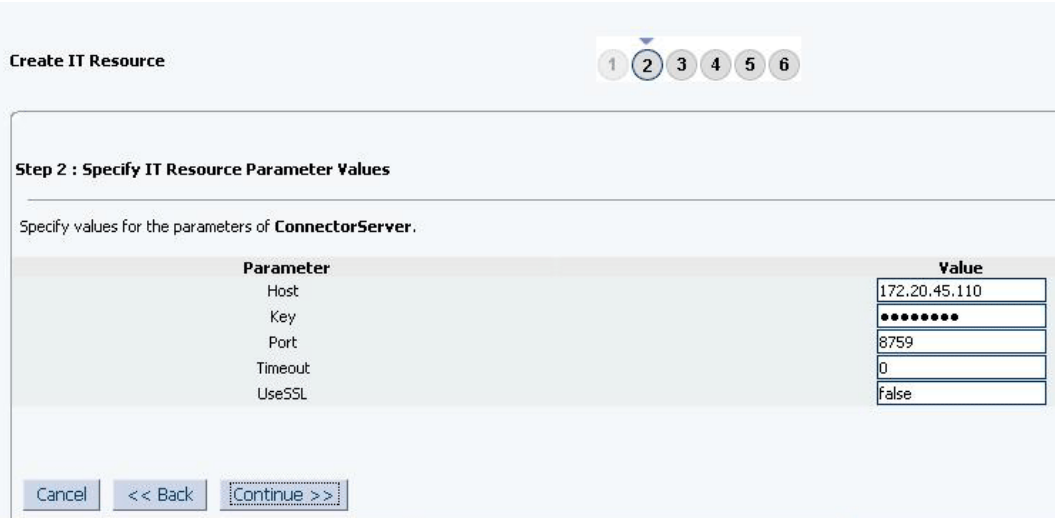


Table 2-5 provides information about the parameters of the IT resource.

Table 2-5 Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: `RManager`
Key	Enter the key for the Java connector server.

Table 2-5 (Cont.) Parameters of the IT Resource for the Connector Server

Parameter	Description
Port	Enter the number of the port at which the connector server is listening. Default value: `8759`
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: `300`
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter `false`. Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, run the connector server by using the /setKey [*key*] option. The value of this key must be specified as the value of the Key IT resource parameter of the connector server.

7. On the Step 3: Set Access Permission to IT Resource page, the `SYSTEM ADMINISTRATORS` group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.

> **Note:**
>
> This step is optional.

If you want to assign groups to the IT resource and set access permissions for the groups, then:

a. Click **Assign Group**.

b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

c. Click **Assign**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

> **Note:**
>
> - This step is optional.
> - You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

a. Click **Update Permissions**.

b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

c. Click **Update**.

9. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

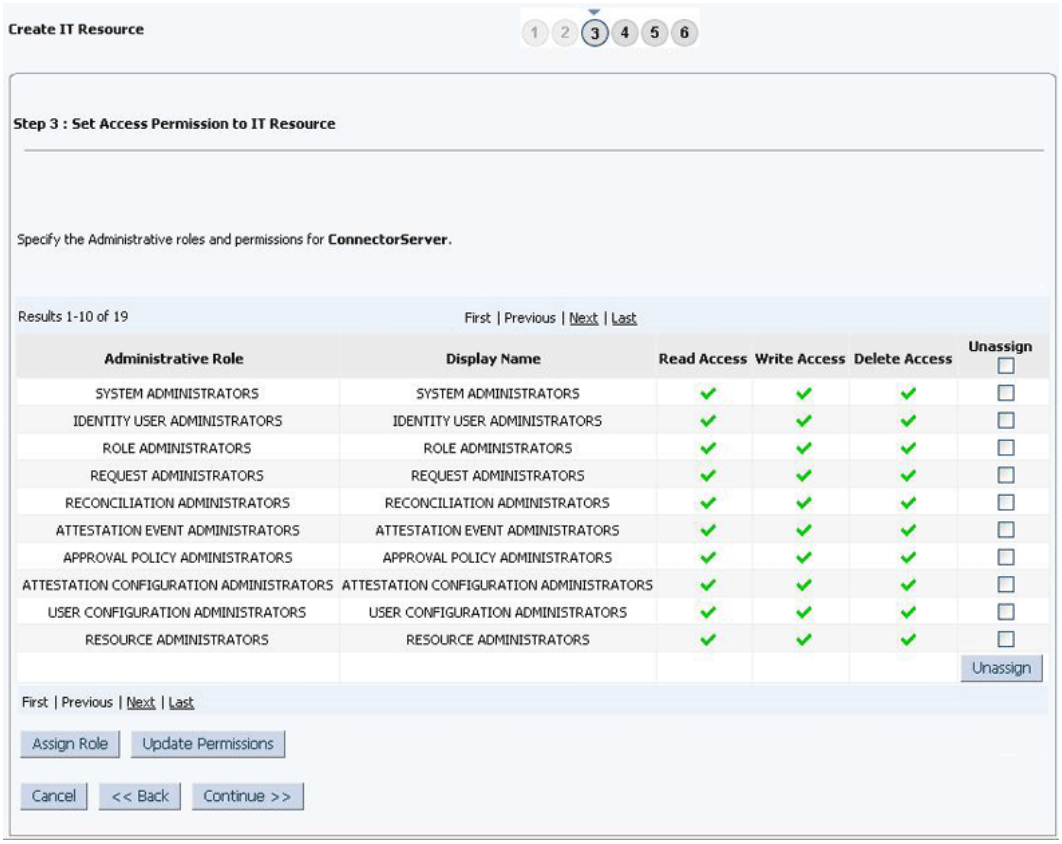
> **Note:**
>
> - This step is optional.
> - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

a. Select the **Unassign** check box for the group that you want to unassign.

b. Click **Unassign**.

10. Click **Continue**. Figure 2-3 shows the Step 3: Set Access Permission to IT Resource page.

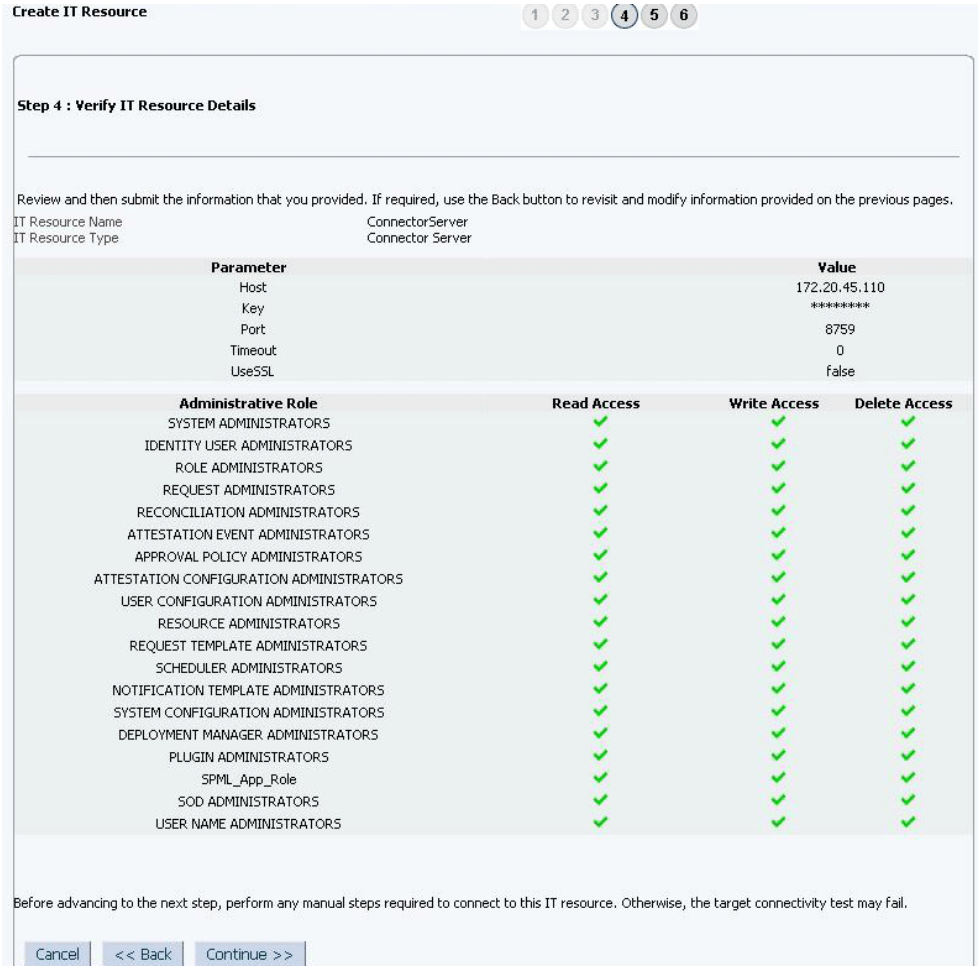
Figure 2-3 Step 3: Set Access Permission to IT Resource



11. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.

12. To proceed with the creation of the IT resource, click **Continue**. Figure 2-4 shows Step 4: Verify IT Resource Details page.

Figure 2-4 Step 4: Verify IT Resource Details

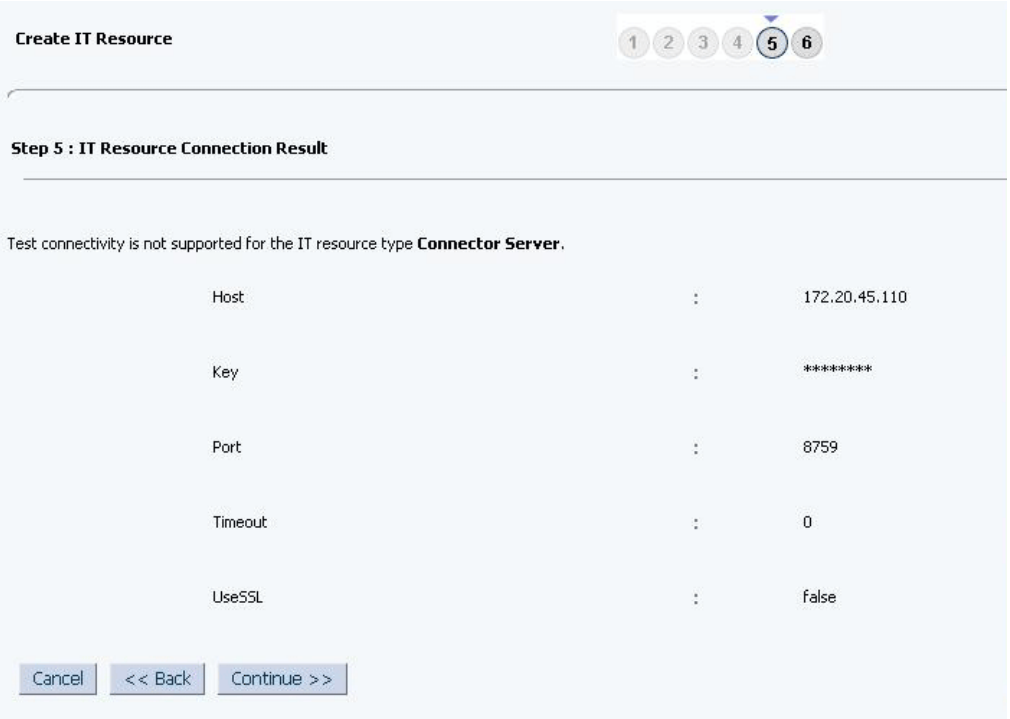


13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:

    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.

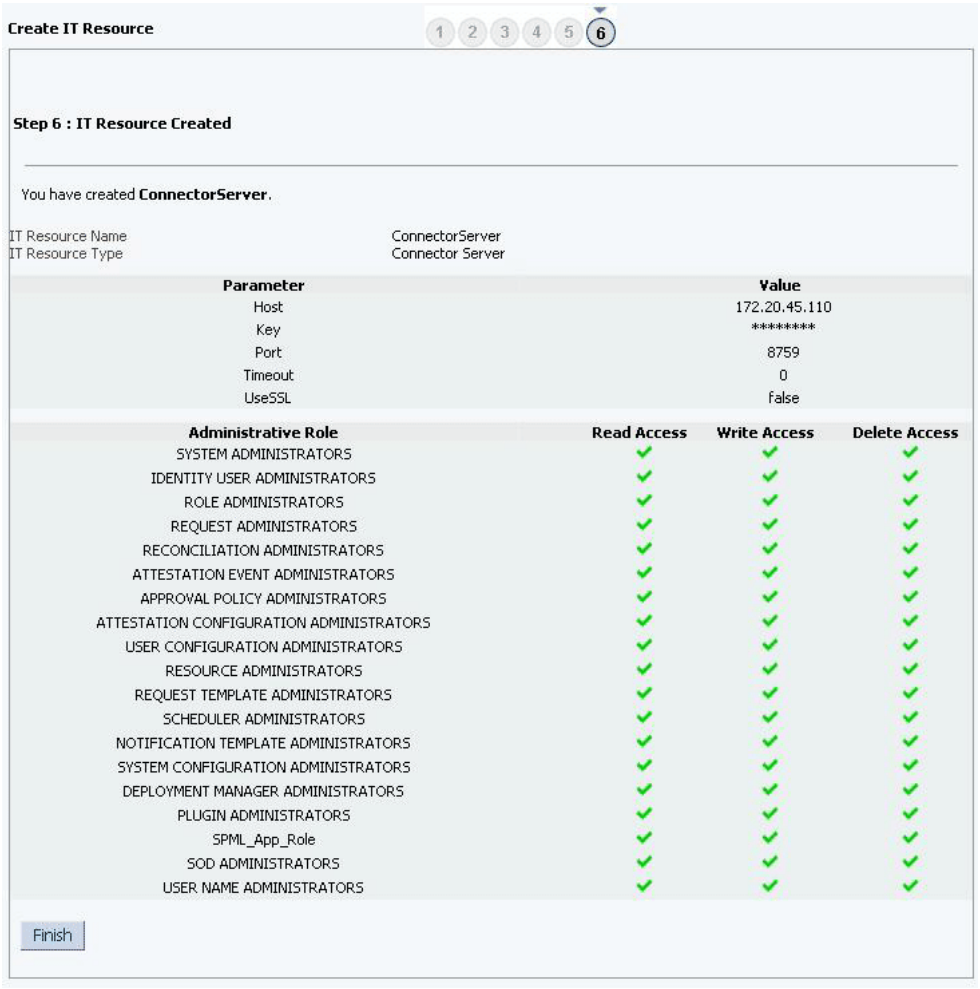
      Figure 2-5 shows the Step 5: IT Resource Connection Result page.

Figure 2-5 Step 5: IT Resource Connection Result



14. Click **Finish**. Figure 2-6 shows the IT Resource Created page.

Figure 2-6 Step 6: IT Resource Created



Configuring SSL

Note:

- Configuring SSL is supported only in the following versions of the target system:
  - JD Edwards EnterpriseOne Tools 8.98.4.11 or later versions
  - JD Edwards EnterpriseOne Tools 9.1.2.1 or later versions
- If you are using JD Edwards EnterpriseOne Tools 8.98 as the target system, ensure that you use third-party JAR files that have been obtained from JD Edwards EnterpriseOne Tools 8.98.4.11 or later versions. See Copying External Code Files for more information.

To configure SSL between Oracle Identity Manager and the target system, see Configuring SSL for JDENET (Release 9.1 Update 2.1) in *JD Edwards EnterpriseOne Tools Security Administration Guide.*

Upgrading the Connector

If you have already deployed an earlier release of this connector, then upgrade the connector to the current release.

> **Note:**
>
> Before you perform the upgrade procedure:
>
> - It is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
> - As a best practice, perform the upgrade procedure in a test environment initially.

> **See Also:**
>
> Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information of these steps

The following sections discuss the procedure to upgrade the connector:

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

Preupgrade Steps

Perform the following preupgrade steps:

1. Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
2. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector.
3. If required, create the connector XML file for a clone of the source connector.
4. Disable all the scheduled jobs.

Upgrade Steps

Depending on the environment in which you are upgrading the connector, perform one of the following steps:

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.
- Production Environment

Perform the upgrade procedure by using the silent mode.

Postupgrade Steps

Perform the following procedure:

1. Upload new connector jars:
   a. Use $*ORACLE_HOME*/bin/UploadJars.sh utility for uploading connector jars.
   b. Update the org.identityconnectors.jde-1.0.1115.jar file as follows:

      (i) Extract the contents of the org.identityconnectors.jde-1.0.1115.jar file into a temporary directory.

      (ii) Copy the jdbj.ini, jdeinterop.ini, jdelog.properties and tnsnames.ora files at the same level as the lib or org directory.

      (iii) Re-create the org.identityconnectors.jde-1.0.1115.jar file by running the following command:

      ```
      jar -cvfm org.identityconnectors.jde-1.0.1115.jar META-INF/MAINFEST.MF *
      ```

      > **Note:**
      >
      > While re-creating the JAR file, ensure that META-INF\MANIFEST.MF file is unchanged.

2. Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation. To do so:
   a. In a text editor, open the fvc.properties file located in the *OIM_DC_HOME* directory and include the following entries:

      ```
      ResourceObject;JDE Resource Object
      FormName;UD_JDE
      FromVersion;9.0.4.1
      ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_UPGRADE
      ```

   b. Run the FVC utility. This utility is copied into the following directory when you install the design console:

      For Microsoft Active Directory:

      OIM_DC_HOME/fvcutil.bat

      For UNIX:

      OIM_DC_HOME/fvcutil.sh

      When you run this utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, and the logger level and log file location.

> **See Also:**
>
> Using the Form Version Control Utility in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the FVC utility

3. Run the PostUpgradeScript.sql script as follows:
   a. Connect to the Oracle Identity Manager database by using the OIM User credentials.
   b. Run the PostUpgradeScript. This script is located in the Upgrade folder on the installation media.
4. Configure the upgraded IT resource of the source connector. See Configuring the IT Resource for information about configuring the IT resource.
5. Purge the cache to get the changes reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* for information on purging cache.
6. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:
   a. Log in to Oracle Identity System Administration.
   b. Create and active a sandbox. See Creating and Activating a Sandbox for more information.
   c. Create a new UI form to view the upgraded fields. See Creating a New UI Form for more information about creating a UI form.
   d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in Step 6.6.c), and then save the application instance.
   e. Publish the sandbox. See Publishing a Sandbox for more information.

After upgrading the connector, you can perform either full reconciliation or incremental reconciliation. This ensures that records created or modified since the last reconciliation run (the one that you performed in Preupgrade Steps) are fetched into Oracle Identity Manager. From the next reconciliation run onward, the reconciliation engine automatically enters a value for the Latest Token attribute.

See Configuring Reconciliation for more information about performing full or incremental reconciliation.

Postcloning Steps

You can clone this connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

> **Note:**
>
> During cloning, the column names in the process form must not exceed the maximum character length limit, which is 30.

> **See Also:**
>
> Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about cloning connectors and the steps mentioned in this section

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- IT Resource

  The cloned connector has its own set of IT resources. You must configure both the cloned connector IT resources and Connector Server IT resources, and provide the reference of the cloned Connector Server IT Resource in the cloned connector IT resource. Ensure you use the configuration lookup definition of the cloned connector.

- Scheduled Job

  The values of the Resource Object Name and IT Resource scheduled job attributes in the cloned connector refer to the values of the base connector. Therefore, these values (values of the Resource Object Name and IT resource scheduled job attributes that refer to the base connector) must be replaced with the new cloned connector artifacts.

- Lookup Definition

  The cloned lookup definition (for example, Lookup.JDEclone.ProvAttrMap) corresponding to the Lookup.JDE.UM.ProvAttrMap lookup definition has Code Key entries related to child form fields that still map to the old child form fields. You must change the values of these Code Key entries so that they map to the cloned child form fields.

  For example, consider UD_JD1ROL to be the cloned child form of the UD_JDEROL child form. After cloning, the Lookup.JDEclone.ProvAttrMap lookup definition contains Code Key entries that correspond to the fields of the old child form UD_JDEROL. To ensure that the Code Key entries point to the fields of the cloned child form (UD_JD1ROL), specify the following values in the corresponding Code Key columns:

  - UD_JD1ROL~Include in *ALL
  - UD_JD1ROL~Effective Date[DATE]
  - UD_JD1ROL~Expiration Date[DATE]
  - UD_JD1ROL~Role[LOOKUP]

After updating the values of the Code Key entries, check whether values for all other Code Key and Decode pair entries are consistent with the entries listed in Table 1-11 in User Fields for Provisioning. For example returnValue points to __UID__.

- Process Tasks

  You must update the adapter variable mappings of all event handlers attached to the process tasks with new names of the cloned artifacts.

  To do so:

  1. Log in to the Design Console.
  2. Expand **Process Management** and double-click **Process Definition.**
  3. Search for and open the cloned process definition. For example, JDE Process1.
  4. On the Tasks tab, double-click the first task. For example, Create User. The Editing Task: <*TASK_NAME*> dialog box is displayed.
  5. On the Integration tab, in the Adapter Variables region, double-click the first adapter variable.
  6. In the Editing Data Mapping Variable dialog box, ensure that the variable is mapped to the artifacts of the cloned connector. For example, for the Create User task, ensure that the itResourceFieldName adapter variable contains the correct literal value, as mentioned in the cloned form of UD_JDE.
  7. Repeat Steps 5 and 6 for the rest of the adapter variables listed on the Integration tab.
  8. Repeat Steps 4 through 7 for the rest of the process tasks listed on the Tasks tab.

- Localization Properties

  You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

  For example, the process form (UD_JDE) attributes are referenced in the Japanese properties file, JDE_ja.properties, as `global.udf.UD_JDE_USERNAME`. During cloning, if you change the process form name from `UD_JDECLONED` to `global.udf.UD_JDECLONED_USERNAME`, then you must add the process form attributes to `global.udf.UD_JDE_USERNAME`.

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.

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:

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

   See Scheduled Job for Lookup Field Synchronization for information about the attributes of the scheduled tasks for lookup field synchronization.

   See Configuring Scheduled Jobs for information about running scheduled tasks.

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

   See Reconciliation Scheduled Jobs for information about the attributes of this scheduled task.

   See Configuring Scheduled Jobs 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 is automatically set to the time stamp at which the reconciliation run began.

> **See Also:**
>
> Configuring Scheduled Jobs for information about attributes of the scheduled job

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.

Scheduled Job for Lookup Field Synchronization

The following scheduled jobs are used for lookup fields synchronization:

- JDE Date Format Lookup Reconciliation
- JDE Date Separation Character Lookup Reconciliation
- JDE Decimal Format Characters Lookup Reconciliation
- JDE Languages Lookup Reconciliation
- JDE Localization Country Code Lookup Reconciliation
- JDE Roles Lookup Reconciliation
- JDE Time Format Lookup Reconciliation
- JDE Universal Time Lookup Reconciliation

You must specify values for the attributes of these scheduled jobs. Table 3-1 describes the attributes of these scheduled jobs. Configuring Scheduled Jobs describes the procedure to configure scheduled jobs.

Table 3-1 Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
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`
Object Type	Enter the type of object you want to reconcile. Depending on the scheduled job that you are running, the default value is one of the following: • For JDE Date Format Lookup Reconciliation: `DATE_FORMAT` • For JDE Date Separation Character Lookup Reconciliation: `DATE_SEPARATION_CHAR` • For JDE Decimal Format Characters Lookup Reconciliation: `DECIMAL_FORMAT_CHARS` • For JDE Languages Lookup Reconciliation: `LANGUAGES` • For JDE Localization Country Code Lookup Reconciliation: `LOCALIZATION_COUNTRY_CODE` • For JDE Roles Lookup Reconciliation: `ROLES` • For JDE Time Format Lookup Reconciliation: `TIME_FORMAT` • For JDE Universal Time Lookup Reconciliation: `UNIVERSAL_TIME`

Table 3-1 (Cont.) Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Lookup Name	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Depending on the scheduled job that you are using, the default values are as follows: • For JDE Date Format Lookup Reconciliation: `Lookup.JDE.DateFormat` • For JDE Date Separation Character Lookup Reconciliation: `Lookup.JDE.DateSeparationCharacter` • For JDE Decimal Format Characters Lookup Reconciliation: `Lookup.JDE.DecimalFormatCharacters` • For JDE Languages Lookup Reconciliation: `Lookup.JDE.Languages` • For JDE Localization Country Code Lookup Reconciliation: `Lookup.JDE.LocalizationCountryCode` • For JDE Roles Lookup Reconciliation: `Lookup.JDE.Roles` • For JDE Time Format Lookup Reconciliation: `Lookup.JDE.TimeFormat` • For JDE Universal Time Lookup Reconciliation: `Lookup.JDE.UniversalTime`
Code Key Attribute	Enter the name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: `__UID__`
Decode Attribute	Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: `__NAME__`
Resource Object Name	Name of the resource object that is used for reconciliation. Default value: `JDE Resource Object`

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:

- Performing Full Reconciliation
- Limited Reconciliation
- Reconciliation Scheduled Jobs

Performing 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, ensure that no values are specified for the Latest Token and Filter attributes of the scheduled jobs for reconciling user records.

At the end of the reconciliation run, the Latest Token attribute of the scheduled job for user record reconciliation is automatically set to the time stamp at which the run ended. From the next reconciliation run onward, only records created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled.

The connector provides a Filter attribute that allows you to use any of the JDE resource attributes to filter the target system records.

You can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a Filter attribute (a scheduled task attribute) that allows you to use JDE resource attributes to filter the target system records.

For detailed information about ICF Filters, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

> **Note:**
>
> The __UID__ attribute name can only be used with the equalTo filter.

While deploying the connector, follow the instructions in Configuring Scheduled Jobs to specify attribute values.

Reconciliation Scheduled Jobs

When you run the Connector Installer, the scheduled tasks corresponding to the following scheduled jobs are automatically created in Oracle Identity Manager:

- Scheduled Jobs for Reconciliation of User Records
- Scheduled Job for Reconciliation of Deleted Users Records

> **Note:**
>
> When you run the scheduled jobs for reconciliation, the following warning message is encountered, which can be ignored:
>
> ```
> ADP ClassLoader failed to load
> ```

Scheduled Jobs for Reconciliation of User Records

Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled jobs:

- JDE User Target Reconciliation

  This scheduled job is used to reconcile user data in the target resource (account management) mode of the connector.

- JDE User Trusted Reconciliation

  This scheduled job is used to reconcile user data in the trusted source (identity management) mode of the connector.

Table 3-2 describes the attributes of both scheduled jobs.

Table 3-2 Attributes of the Scheduled Jobs for Reconciliation of User Records

Attribute	Description

Filter	Expression for filtering records. Use the following syntax:
	`syntax = expression ( operator expression )*`
	`operator = 'and' | 'or'`
	`expression = ( 'not' )? filter`
	`filter = ('equalTo' | 'contains' | 'containsAllValues'`
	`| 'startsWith' | 'endsWith' | 'greaterThan' | 'greaterThanOrEqualTo'`
	`| 'lessThan' | 'lessThanOrEqualTo' ) '(' 'attributeName' ','`
	`attributeValue')'`
	`attributeValue = singleValue | multipleValues`
	`singleValue = 'value'`
	`multipleValues = '[' 'value_1' (',' 'value_n')* ']'`
	
	Default value: None

Incremental Recon Attribute	Name of the attribute that holds the time stamp value. Default value: `TIMESTAMP` **Note:** Do *not* change the value of this attribute.
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Sample value: `JDE`
Latest Token	This attribute holds the value for the TIMESTAMP variable that is specified for the Incremental Recon Attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty. **Note:** Do *not* enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: `1354753427000`
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. The default value of this attribute in the JDE User Target Reconciliation scheduled job is `JDE Resource Object.` The default value of this attribute in the JDE User Trusted Reconciliation scheduled job is `JDE Trusted Resource Object.`
Scheduled Task Name	Name of the scheduled task used for reconciliation. The default value of this attribute in the JDE User Target Reconciliation scheduled job is `JDE User Target Reconciliation.` The default value of this attribute in the JDE User Trusted Reconciliation scheduled job is `JDE User Trusted Reconciliation.`

Scheduled Job for Reconciliation of Deleted Users Records

Depending on whether you want to implement trusted source or target resource delete reconciliation, you must specify values for the attributes of one of the following scheduled jobs:

- JDE User Target Delete Reconciliation

  This scheduled job is used to reconcile data about deleted users in the target resource (account management) mode of the connector. During a reconciliation run, for each deleted user account on the target system, the JDE resource is revoked for the corresponding OIM User.

- JDE User Trusted Delete Reconciliation

  This scheduled job is used to reconcile data about deleted users in the trusted source (identity management) mode of the connector. During a reconciliation run, for each deleted target system user account, the corresponding OIM User is deleted.

Table 3-3 describes attributes of both scheduled jobs.

Table 3-3 Attributes of the Scheduled Job for Delete User Reconciliation

Attributes	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile user data. The default value of this attribute in the JDE User Target Delete Reconciliation scheduled job is `JDE IT Resource`. The default value of this attribute in the JDE User Trusted Delete Reconciliation scheduled job is the name of the IT resource instance that you create for trusted source reconciliation in Configuring the IT Resource.
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. The default value of this attribute in the JDE User Target Delete Reconciliation scheduled job is `JDE Resource Object`. The default value of this attribute in the JDE User Trusted Delete Reconciliation scheduled job is `JDE Trusted Resource Object`.

Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Table 3-4 lists the scheduled jobs that you must configure.

Table 3-4 Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
JDE Date Format Lookup Reconciliation	This scheduled job is used to synchronize values of the date format lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.

Table 3-4 (Cont.) Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
JDE Date Separation Character Lookup Reconciliation	This scheduled job is used to synchronize values of the date separation character lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
JDE Decimal Format Characters Lookup Reconciliation	This scheduled job is used to synchronize values of the decimal format characters lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
JDE Languages Lookup Reconciliation	This scheduled job is used to synchronize values of the language lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
JDE Localization Country Code Lookup Reconciliation	This scheduled job is used to synchronize values of the localization country code lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
JDE Roles Lookup Reconciliation	This scheduled job is used to synchronize values of the role lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
JDE Time Format Lookup Reconciliation	This scheduled job is used to synchronize values of the time format lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
JDE Universal Time Lookup Reconciliation	This scheduled job is used to synchronize values of the universal time lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
JDE User Target Reconciliation	This scheduled job is used to fetch user data during target resource reconciliation. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of User Records.
JDE User Target Delete Reconciliation	This scheduled task is used to fetch data about deleted users during target resource reconciliation. During a reconciliation run, for each deleted user account on the target system, the JDE resource is revoked for the corresponding OIM User. For information about this scheduled task and its attributes, see Scheduled Job for Reconciliation of Deleted Users Records.
JDE User Trusted Reconciliation	This scheduled job is used to fetch user data during trusted source reconciliation. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of User Records.
JDE User Trusted Delete Reconciliation	This scheduled job is used to fetch data about deleted users during trusted source reconciliation. During a reconciliation run, for each deleted target system account, the corresponding OIM User is deleted. For information about this scheduled task and its attributes, see Scheduled Job for Reconciliation of Deleted Users Records.

Configuring Scheduled Jobs

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

To configure a scheduled job:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

- For Oracle Identity Manager release 11.1.1:
  a. Log in to the Administrative and User Console.
  b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
  c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
- For Oracle Identity Manager release 11.1.2.*x*:
  a. Log in to Oracle Identity System Administration.
  b. In the left pane, under System Management, click **Scheduler.**

2. Search for and open the scheduled job as follows:
   a. 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.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
3. 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 Administering Oracle Identity Manager* for detailed information about schedule types.

   In addition to modifying the job details, you can enable or disable a job.
4. 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.

5. 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.

Guidelines on Using the Connector

The following is a guideline on using 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.

Performing Provisioning Operations in Oracle Identity Manager Release 11.1.1.*x*

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, 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 Switching Between Request-Based Provisioning and Direct Provisioning.

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning

> **See Also:**
>
> Manually Completing a Task in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for information about the types of provisioning

This section discusses the following topics:

> **Note:**
>
> The time required to complete a provisioning operation that you perform the first time by using this connector takes longer than usual.

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:
   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:
   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. On the user details page, click the **Resources** tab.
5. 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.
6. On the Step 1: Select a Resource page, select **JDE Resource Object** from the list and then click **Continue**.
7. On the Step 2: Verify Resource Selection page, click **Continue**.
8. 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**.
9. 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**.
10. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
11. Close the window displaying the "Provisioning has been initiated" message.
12. On the Resources tab, click **Refresh** to view the newly provisioned resource.

Request-Based Provisioning

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 this section 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.

- End User's Role in Request-Based Provisioning
- Approver's Role in Request-Based Provisioning

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 Performing Self Service Tasks 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.

Approver's Role in Request-Based Provisioning

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

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.

Switching Between Request-Based Provisioning and Direct Provisioning

> **Note:**
>
> It is assumed that you have performed the procedure described in Configuring Oracle Identity Manager for Request-Based Provisioning.

- 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.

- 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.

Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later

To perform provisioning operations in Oracle Identity Manager release 11.1.2 or later:

> **Note:**
>
> The time required to complete a provisioning operation that you perform the first time by using this connector takes longer than usual.

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See Managing Users in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance created in Step 3, and then click **Checkout.**
5. Specify value for fields in the application form and then click **Ready to Submit.**
6. Click **Submit.**
7. If you want to provision entitlements, then:
   a. On the Entitlements tab, click **Request Entitlements.**
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
   c. Click **Submit.**

Uninstalling the Connector

If you want to uninstall the connector for any reason, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4

Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

> **Note:**
>
> From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See Managing Lookups in *Oracle Fusion Middleware Administering Oracle Identity Manager* for information about managing lookups by using the Form Designer in the Oracle Identity Manager System Administration console.

- Adding New Attributes for Target Resource Reconciliation
- Adding New Attributes for Provisioning
- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During Reconciliation
- Configuring the Connector for Multiple Installations of the Target System

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 User Fields for Target Resource Reconciliation 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 procedures:

> **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.

- Adding the New Attribute on the OIM User Process Form
- Adding the New Attribute to the list of Reconciliation Fields

- Creating a Reconciliation Field Mapping for the New Attribute
- Creating an Entry for the Attribute in the Reconciliation Lookup Definition
- Enabling Update of New Attributes for Provisioning

Adding the New Attribute on the OIM User Process Form

To add the new attribute on the OIM User process form:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Form Designer**.
4. Search for and open the **UD_JDE** process form.
5. Click **Create New Version**.
6. In the **Label** field, enter the version name. For example, `version#1`.
7. Click the Save icon.
8. Select the current version created in Step e from the **Current Version** list.
9. Click **Add** to create a new attribute, and provide the values for that attribute.

   For example, if you are adding the address number 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

10. Click the Save icon.
11. Click **Make Version Active**.
12. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:
    a. Log in to Oracle Identity System Administration.
    b. Create and active a sandbox. See Creating and Activating a Sandbox for more information.
    c. Create a new UI form to view the newly added field along with the rest of the fields. See Creating a New UI Form for more information about creating a UI form.
    d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in Step 5.c), and then save the application instance.
    e. Publish the sandbox. See Publishing a Sandbox for more information.

Adding the New Attribute to the list of Reconciliation Fields

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

1. Expand **Resource Management.**
2. Double-click **Resource Objects**.
3. Search for and open the **JDE Resource Object** resource object.
4. On the **Object Reconciliation** tab, click **Add Field**, and then enter the following values:

   Field Name: `AddressNumber`

   Field Type: `String`
5. Click the Save icon and then close the dialog box.

Creating a Reconciliation Field Mapping for the New Attribute

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

1. Expand **Process Management.**
2. Double-click **Process Definition**.
3. Search for and open the **JDE Process** process definition.
4. 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`
5. Click the Save icon.
6. Click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

Creating an Entry for the Attribute in the Reconciliation Lookup Definition

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

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open the **Lookup.JDE.ReconAttrMap** lookup definition.
4. 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, prefixed with the table name. The following is the format in which you must enter the Decode value:

   TABLE_NAME.ATTR_NAME

   In this format, *TABLE_NAME* is the name of the table in the target system database in which the attribute is present. *ATTR_NAME* is the name of the attribute in the target system.

For example, enter `AddressNumber` in the **Code Key** field and then enter `F00921.AddressNumber` in the **Decode** field. Note that both Code Key and Decode values are the same.

5. Click the Save icon.

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.
> - You can add only attributes (for provisioning) that are declared in the data structure of the 'AddUserIDToProfileAndPreference' API of the target system.
> - Before starting the following procedure, perform Steps 1 through 12 as described in 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 User Fields for Target Resource Reconciliation 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, perform the following procedures:

- Creating an Entry for the Attribute in the Lookup Definition for Provisioning
- Updating the Request Dataset
- Enabling Update of New Attributes for Provisioning

Creating an Entry for the Attribute in the Lookup Definition for Provisioning

Create an entry for the attribute in the lookup definition for provisioning as follows:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Administration.**
3. Double-click **Lookup Definition.**
4. Search for and open the **Lookup.JDE.UM.ProvAttrMap** lookup definition.
5. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the value of the Field Label created in Step 9 in Adding the New Attribute on the OIM User Process Form. The Decode value is the name of the attribute in the target system.

   For example, enter `Address Number` in the **Code Key** field and then enter `mnAddressNumber` in the Decode field.
6. Click the Save icon.

Updating 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:

> **Note:**
>
> Perform the steps provided in this topic only if you want to perform request-based provisioning.

1. In a text editor, open the xml/JDE-Datasets.xml file located on the installation media for editing.
2. Add the AttributeReference element and specify values for the mandatory attributes of this element.

   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.
3. Save and close the XML file.
4. Run the PurgeCache utility to clear content related to request datasets from the server cache.

See *Oracle Fusion Middleware System Administering Oracle Identity Manager* for more information about the PurgeCache utility.

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

   See Importing Request Datasets for detailed information about the procedure.

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
      - 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 **adpJDEUPDATEUSER** 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
processKeyInstance	Long	Process Data	Process Instance	NA
Adapter return value	Object	Response Code	NA	NA
objectType	String	Literal	String	User
attrFieldName	String	Literal	String	mnAddressNumber
itResourceFieldName	String	Literal	String	UD_JDE_RESOURCETYPE

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

Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

> **See Also:**
>
> The Javadocs shipped with the connector for more information about this interface

The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

```
package com.validate;
import java.util.*;
public class MyValidation {

public boolean validate(HashMap hmUserDetails,
         HashMap hmEntitlementDetails, String field) {
            /*
         * You must write code to validate attributes. Parent
         * data values can be fetched by using hmUserDetails.get(field)
         * For child data values, loop through the
         * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
         * Depending on the outcome of the validation operation,
         * the code must return true or false.
         */
         /*
         * In this sample code, the value "false" is returned if the field
         * contains the number sign (#). Otherwise, the value "true" is
         * returned.
         */
            boolean valid=true;
            String sFirstName=(String) hmUserDetails.get(field);
            for(int i=0;i<sFirstName.length();i++){
              if (sFirstName.charAt(i) == '#'){
                    valid=false;
                    break;
              }
            }
            return valid;
        }
      } /* End */
```

2. Create a JAR file to hold the Java class.

3. Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 2 to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use 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. Specify 1 as the value of the JAR type.

4. If you created the Java class for validating a process form field for reconciliation, then:

   a. Log in to the Design Console.

   b. Search for and open the **Lookup.JDE.UM.ReconValidation** lookup definition.

      > **Note:**
      >
      > If you do not find this lookup definition, then create it.

   c. In the Code Key column, enter the resource object field name that you want to validate For example, `Username`. In the Decode column, enter the class name. For example, `org.identityconnectors.jde.extension.JDEValidator`.

   d. Save the changes to the lookup definition.

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

   f. In the Code Key column, enter `Recon Validation Lookup`. In the Decode column, enter `Lookup.JDE.UM.ReconValidation`.

   g. Save the changes to the lookup definition.

5. If you created the Java class for validating a process form field for provisioning, then:

   a. Log in to the Design Console.

   b. Search for and open the **Lookup.JDE.UM.ProvValidation** lookup definition.

   c. In the Code Key column, enter the process form field name. In the Decode column, enter the class name.

   d. Save the changes to the lookup definition.

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

f. In the Code Key column, enter `Provisioning Validation Lookup`. In the Decode column, enter `Lookup.JDE.UM.ProvValidation`.

g. Save the changes to the lookup definition.

6. Purge the cache to get the changes reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information.

Configuring Transformation of Data During Reconciliation

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to configure transformation of data during reconciliation.

You can configure the transformation of reconciled single-valued data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

To configure the transformation of data:

1. Write code that implements the required transformation logic in a Java class.

> **See Also:**
>
> The Javadocs shipped with the connector for more information about this interface

This transformation class must implement the transform method. The following sample transformation class modifies the Username attribute by using values fetched from the __NAME__ attribute of the target system:

```
package com.transformationexample;
import java.util.HashMap;
public class MyTransformer {
public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails, String sField) throws ConnectorException {
      /*
      * You must write code to transform the attributes.
      * Parent data attribute values can be fetched by using
hmUserDetails.get("Field Name").
      * To fetch child data values, loop through the
      * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
      * Return the transformed attribute.
      */
        String sUserName = (String) hmUserDetails.get("__NAME__");
        return sUserName + "@example.com";
        }
}
```

2. Create a JAR file to hold the Java class.

3. Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 2 to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

> **Note:**
>
> Before you use 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. Specify 1 as the value of the JAR type.

4. Create a new lookup definition by the name **Lookup.JDE.UM.ReconTransformations** and then add the following entry:

   a. Log in to the Design Console.

   b. Expand **Administration,** and then double-click **Lookup Definition.**

   c. In the Code field, enter `Lookup.JDE.UM.ReconTransformations` as the name of the lookup definition.

   d. In the Field field, enter the name of the table column of the Oracle Identity Manager or user-created form or tab, from which the text field, lookup field, or box field will be accessible.

   e. Select the **Lookup Type** option.

   f. On the Lookup Code Information tab, click **Add.**

   g. In the **Code Key** column, enter the name of the attribute on which you want to apply the transformation. For example: `FirstName`.

   h. In the **Decode** column, enter the name of the class file. For example: `oracle.iam.connectors.jde.Transformation`.

   i. Save the lookup definition.

5. Purge the cache to get the changes reflected in Oracle Identity Manager. See *Oracle Fusion Middleware Administering Oracle Identity Manager* for information on purging cache.

Configuring the Connector for Multiple Installations of the Target System

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

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

To meet the requirement posed by such a scenario, you can create copies of connector objects, such as the IT resource and resource object.

The decision to create a copy of a connector object is based on a requirement. For example, an IT resource can hold connection information for one target system installation. Therefore, it is mandatory to create a copy of the IT resource for each target system installation.

With some other connector objects, you do not need to create copies at all. For example, a single attribute-mapping lookup definition can be used for all installations of the target system.

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

1. Obtain the jdbj.ini, jdeinterop.ini, jdelog.properties and tnsnames.ora files for the second instance of the target system and configure it to suit your deployment requirements. See Configuring the JDE Property Files for more information.
2. Create a JDE connector bundle with a different version. To do so:
   a. Extract the contents of the bundle/org.identityconnectors.jde-1.0.1115.jar file on the installation media to a temporary directory.
   b. In a text editor, open the MANIFEST.MF file located in the META-INF directory for editing.
   c. Specify a new value for the ConnectorBundle-Version attribute. For example, specify `1.0.1117` as the new value.
   d. Save and close the file.
   e. Update the JAR file by performing the procedure described in Step 2 of Modifying the Connector Bundle.
   f. Rename the connector bundle to reflect the new version. For example, org.identityconnectors.jde-1.0.1117.jar.
3. Run the Oracle Identity Manager Upload JARs utility to upload the newly created JAR file (for example, org.identityconnectors.jde-1.0.1117.jar file) to the database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use 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. Specify `4` (ICFBundle) as the value of the JAR type.

> **See Also:**
>
> Migrating JARs and Resource Bundle in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Upload JARs utility

4. Create a configuration lookup definition for this instance of the target system. For example, create a lookup definition by the name **Lookup.JDE.Configuration1.**
5. Add the following entries to this lookup definition and specify the corresponding values in the Decode column:
   - Connector Name
   - Bundle Version
   - User Configuration Lookup
   - Bundle Name

> **Note:**
>
> Ensure that the Decode value of Bundle Version is the latest version specified in Step 2. For example, `1.0.1117`. For all entries other than Bundle Version, you can specify the same values as those present in the Lookup.JDE.Configuration lookup definition.

6. Create an IT resource of the JDE IT Resource type. Ensure that the value of the Configuration Lookup parameter in this newly created IT resource contains the name of the lookup definition created in Step 4.
7. If you are using the connector server, then repeat steps 1 through 7 of this section with the following difference:

   While performing Step 3 of this procedure, instead of uploading the new created JAR file to Oracle Identity Manager database, copy it to the *CONNECTOR_SERVER_DIR*/bundles directory.

5
Known Issues and Limitations

This section discusses the following topics:

Known Issues

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

- **Bug 31740167**

  When the JD Edwards target account is reconciled to Oracle Identity Manager, and you try to perform disable or enable account operation, it fails with the following error:

  "Must provide the password"

  This issue is encountered as the JD Edwards user password cannot be reconciled to Oracle Identity Manager, and the disable or enable operation needs the user password to execute the JD Edwards business function correctly in the target system.

  As a workaround, before performing a disable or enable account operation, perform a password reset operation in the Oracle Identity Manager account that was reconciled from JD Edwards target system. This ensures that the Oracle Identity Manager account contains the correct password attribute value for the JD Edwards user.

- **Bug 15853409**

  When you update one of the fields by performing an update provisioning operation, the bulk update task is initiated.

- **Bug 16033813**

  Translations for the DATE SEPARATION CHARACTER and DECIMAL FORMAT CHARACTER fields are not available.

  As a work around, perform the following procedure:

  1. Run the Oracle Identity Manager Download Resource Bundle utility to download the JDEdwards_*LOCALE*.properties file from the database. This utility is copied into the following location when you install Oracle Identity Manager:

     > **Note:**
     >
     > Before you use 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/DownloadResourceBundles.bat

     – **For UNIX:**

OIM_HOME/server/bin/DownloadResourceBundles.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 resource bundle file being downloaded, and the location to which the resource bundle file is to be downloaded. Specify `2` (Connector Resource) as the value of the resource bundle file type.

> **See Also:**
>
> Dowload Resource Bundle Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*

2. In a text editor, open the JDEdwards_*LOCALE*.properties file.
3. Search for and replace global.udf.UD_JDE_DATESEPARATIONCHARECTER with global.udf.UD_JDE_DATESEPARATIONCHARACTER.
4. Search for and replace global.udf.UD_JDE_DECIMALFORMATCHARATER with global.udf.UD_JDE_DECIMALFORMATCHARACTER.
5. Save and close the file.
6. Verify that values for the DATE SEPARATION CHARACTER and DECIMAL FORMAT CHARACTER fields are translated.

- **Bug 16033928**

  The connector does not support any operation with multibyte character sets.

- **Bug 16002973**

  After upgrading the connector, the process form version for the following user accounts does not get updated by the FVC utility:

  User accounts that were reconciled by using the older version of the connector and were not modified directly on Oracle Identity Manager.

  In addition, the update provisioning operation on such reconciled user accounts fails.

  As a workaround, update the value of the <*PROCESS_FORM_NAME*>_UPDATE column in the Oracle Identity Manager database with the value of the <*PROCESS_FORM_NAME*>_CREATE column.

- **Bug 16049841**

  The following issue is encountered if you are using Oracle Identity Manager 11*g* Release 2:

  An update provisioning operation on any of the fields of the child form (for example, Effective Date or Expiration Date) does not initiate the update process task. In addition, no error message is displayed.

Limitations

The following is a limitation associated with the target system:

Bug 15883381

When you clear the value of a lookup field on the process form, value from the corresponding lookup field on the target system is not cleared.

Index