Oracle® Identity Manager

Connector Guide for PeopleSoft User Management

Release 9.1.1

E11206-14

September 2013

ORACLE®

Oracle Identity Manager Connector Guide for PeopleSoft User Management, Release 9.1.1

E11206-14

Primary Author: Gauhar Khan

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

Contributor: Sanjay Rallapalli

Contents

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

List of Figures

List of Tables

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

For generic information about connectors, see *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

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

http://docs.oracle.com/cd/E14571_01/im.htm

Documentation Updates

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

http://docs.oracle.com/cd/E11223_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 the Oracle Identity Manager Connector for PeopleSoft User Management?

This chapter provides an overview of the updates made to the software and documentation for release 9.1.1.6 of the PeopleSoft User Management connector.

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

- Software Updates

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

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

Software Updates

The following sections discuss the software updates:

- Software Updates in Release 9.1.0
- Software Updates in Release 9.1.0.1
- Software Updates in Release 9.1.0.2
- Software Updates in Release 9.1.1
- Software Updates in Release 9.1.1.4
- Software Updates in Release 9.1.1.5
- Software Updates in Release 9.1.1.6

Software Updates in Release 9.1.0

The following software updates have been made in release 9.1.0:

- From this release onward, PeopleTools 8.22, 8.45, 8.46, 8.47, and 8.48 are not supported. Information specific to these releases has been removed from the guide. The modified target system requirements information is documented in Section 1.1, "Certified Components."
- The Remote Manager has been added to the connector to support provisioning operations for multiple target systems. Information specific to the connector with

the Remote Manager have been added to the relevant sections in this guide. The architecture of the connector with the Remote Manager is described in Section 1.3.3, "Architecture of the Connector with the Remote Manager."

- New files have been added to the installation media directory for the connector with the Remote Manager. These files are listed in Section 2.1.1.1, "Files and Directories on the Installation Media."
- From this release onward, the connector is installed through the Connector Installer feature of the Oracle Identity Manager Administrative and User Console. Instructions to perform the installation are provided in Section 2.2.1.1, "Running the Connector Installer."
- The Delete Reconciliation scheduled task has been added to the connector. Through this scheduled task, the data of deleted users is reconciled into Oracle Identity Manager. See Section 3.6, "Configuring Scheduled Tasks" for more information about this scheduled task and its attributes.
- You can configure SSL connectivity between Oracle Identity Manager and the target system for this release of the connector. However, SSL is not supported for Oracle Application Server. For instructions to configure SSL, see Section 2.3, "Postinstallation."
- Information about the files in which you set the log levels has changed. This information is available in Section 2.3.1.2, "Enabling Logging."

Software Updates in Release 9.1.0.1

The following software update has been made in release 9.1.0.1:

- Support for Oracle Identity Manager Release 9.1.0.1

Support for Oracle Identity Manager Release 9.1.0.1

From this release onward, the connector can be deployed on Oracle Identity Manager release 9.1.0.1.

Software Updates in Release 9.1.0.2

The following table lists the issues resolved in release 9.1.0.2:

Bug Number	Issue	Resolution
8271640	The connector could not be installed in an environment in which the PIA and JOLT servers were hosted on separate computers.	This issue has been resolved. The connector can be installed in an environment in which the PIA and JOLT servers are hosted on separate computers.

Software Updates in Release 9.1.1

The following software updates have been made in release 9.1.1:

- Support for Standard PeopleSoft Messages
- Enhanced Set of Lookup Definitions
- Support for New ID Types
- Support for Multiple Versions of the Target System
- Support for Resending Messages That Are Not Processed
- Enhanced Set of Default Attribute Mappings
- Support for Connection Pooling

- Support for Validation and Transformation of Account Data
- Support for Creating Copies of Connector Objects
- Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations
- Resolved Issues in Release 9.1.1

Support for Standard PeopleSoft Messages

In earlier releases, the connector made use of custom PeopleCode in PeopleSoft Enterprise Applications for full reconciliation and incremental reconciliation. From this release onward, the connector will use the following standard PeopleSoft messages that are delivered as part of the PeopleSoft installation:

- USER_PROFILE
- DELETE_USER_PROFILE

See Section 1.4.2, "Support for Standard PeopleSoft Messages" for more information.

Enhanced Set of Lookup Definitions

Lookup definitions have been added to support reconciliation based on standard message types.

See Section 1.5, "Lookup Definitions Used During Connector Operations" for a complete listing of the lookup definitions.

Support for New ID Types

The connector now supports the following ID Types in addition to the Employee (EMP) ID Type:

- Customer (CST)
- Vendor (VND)

The connector is now enhanced to support additional ID Types.

See Section 1.4.9, "Adding New ID Types" for more information.

Support for Multiple Versions of the Target System

From this release onward, the Remote Manager mode of the connector has been deprecated. Information specific to the connector with the Remote Manager has been removed from the corresponding sections in this guide. The connector can now be used for multiple versions of the target system without deploying the Remote Manager.

The connector can be configured to work with different versions of the target system at the same time. For example, you can use a single instance of the connector to integrate Oracle Identity Manager with a PeopleTools 8.48 installation and a PeopleTools 8.49 installation.

See Section 2.2.1.4, "Configuring the Connector to Support Multiple Versions of the Target System" for more information.

Support for Resending Messages That Are Not Processed

Standard messages provided by PeopleSoft are asynchronous. In other words, if a message is not delivered successfully, then the PeopleSoft Integration Broker marks that message as not delivered. The message can then be resent manually.

See Section 3.4, "Resending Messages That Are Not Received by the PeopleSoft Listener" for details.

Enhanced Set of Default Attribute Mappings

The default set of attribute mappings for reconciliation and provisioning has been enhanced. See the following sections for a full listing of the attribute mappings:

- Section 1.6.1, "User Attributes for Reconciliation"
- Section 1.7.2, "User Attributes for Provisioning"

Support for Connection Pooling

The connector supports the connection pooling feature introduced in Oracle Identity Manager release 9.1.0.2. In earlier releases, a connection with the target system was established at the start of a reconciliation run and closed after the reconciliation run. With the introduction of connection pooling, multiple connections are established by Oracle Identity Manager and held in reserve for use by the connector.

See Section 1.4.7, "Connection Pooling" for more information.

Support for Validation and Transformation 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.

See the following sections for more information:

- Section 4.7, "Configuring Validation of Data During Reconciliation"
- Section 4.8, "Configuring Transformation of Data During Reconciliation"

Support for Creating Copies of Connector Objects

To meet the requirements of specific use cases, you might need to create multiple copies of the Oracle Identity Manager objects that constitute the connector. The connector can work with multiple instances of these objects.

See Section 4.11, "Configuring the Connector for Multiple Installations of the Target System" for more information.

Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations

From this release onward, you can specify a list of accounts who must be excluded from all reconciliation and provisioning operations.

See Section 1.5.2.3.4, "Lookup.PSFT.UM.ExclusionList" for more information.

Resolved Issues in Release 9.1.1

The following issues are resolved in release 9.1.1:

Bug Number	Issue	Resolution
7526893	The connector supported the linking of user profile with employee ID type only. Other ID types, such as vendor and customer, were not supported.	This issue has been resolved. The connector now supports the linking of user profile with any ID type supported by the target system.

Bug Number	Issue	Resolution
8351580 and 8718471	The connector supported a single PeopleSoft implementation for a single Oracle Identity Manager. The connector did not allow the reuse of the adapters with multiple objects, processes, and form names required for different implementations.	This issue has been resolved. The connector now makes use of the configuration lookup definitions. The Oracle Identity Manager object references can now be configured. The Remote Manager approach to support multiple versions of the target system is deprecated. It is replaced by a class loader solution. See Section 2.2.1.4, "Configuring the Connector to Support Multiple Versions of the Target System" for more information.
8239326	The connector used to log the password.	This issue has been resolved. The connector does not log the password now.

Software Updates in Release 9.1.1.4

The following software updates have been made in release 9.1.1.4:

- Support for New Target Systems
- Resolved Issues in Release 9.1.1.4

Support for New Target Systems

From this release onward, the following target systems have been added to the list of target systems certified for the connector:

- PeopleTools 8.50 with HRMS 9.0
- PeopleTools 8.50 with HRMS 9.1

See Section 1.1, "Certified Components" for more information.

Resolved Issues in Release 9.1.1.4

The following issues are resolved in release 9.1.1.4:

Bug Number	Issue	Resolution
9341621	The lookup reconciliation failed if the Code Key value had a space.	This issue has been resolved. Code Key values with spaces are now reconciled during lookup field synchronization.

Software Updates in Release 9.1.1.5

The following software updates have been made in release 9.1.1.5:

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

Support for New Oracle Identity Manager Release

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

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

Support for Request-Based Provisioning

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

See Section 3.5.2, "Request-Based Provisioning in Oracle Identity Manager" for more information.

Software Updates in Release 9.1.1.6

The following software updates have been made in release 9.1.1.6:

- Support for New Oracle Identity Manager Release
- Support for New Target Systems
- Support for SoD Validation of Entitlement Provisioning on Oracle Identity Manager 11g
- Resolved Issues in Release 9.1.1.6

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager release 11.1.1.3 BP02.

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

Support for New Target Systems

From this release onward, the connector supports the following target systems:

- PeopleSoft HRMS 9.1 with PeopleTools 8.51
- PeopleSoft HRMS 8.9 with PeopleTools 8.50

See Section 1.1, "Certified Components" for the full list of certified target systems.

Support for SoD Validation of Entitlement Provisioning on Oracle Identity Manager 11g

From this release onward, the connector supports the Segregation of Duties (SoD) feature in Oracle Identity Manager release 11.1.1.3 BP02. Requests for PeopleSoft role entitlements can be validated with Oracle Application Access Controls Governor. Entitlements are provisioned on PeopleSoft only if the request passes the SoD validation process. This preventive simulation approach helps identify and correct potentially conflicting assignment of entitlements to a user, before the requested entitlements are granted to users.

Note: The connector does not support the SoD feature in Oracle Identity Manager release 9.1.0.2 and later releases in the 9.1.0.2 series.

See Section 1.4.5, "SoD Validation of Entitlement Provisioning" for information about SoD feature in Oracle Identity Manager release 11.1.1.3 BPO2.

See Section 2.3.1.8, "Configuring SoD" for the detailed procedures on configuring SoD on Oracle Identity Manager release 11.1.1.3 BP02.

See Section 5.2 "Upgrading from Release 9.1.1.5 to This Release" in the connector readme for upgrade information.

Resolved Issues in Release 9.1.1.6

The following issues are resolved in release 9.1.1.6:

Bug Number	Issue	Resolution
10223341	OIM_UM_DELETE project file contains no objects	This issue has been resolved. The OIM_UM_DELELE.xml file now contains objects required for removing the PeopleSoft project file and all its objects from the target system.
10306259	Role update failed in PeopleSoft provisioning	This issue has been resolved. Role update (Role update in process form) is now correctly working.
10358959	Value too large for column "UD_PSFT_BAS_SODCHECKRESULT" when tried PeopleSoft SOD	This issue has been resolved. Value too large for column "UD_PSFT_BAS_SODCHECKRESULT" error will not occur with SoD Configuration.
10355388	Modified e-mails are not processed properly in Oracle Identity Manager during incremental target reconciliation	This issue has been resolved. Modified e-mails are now processed properly during incremental target reconciliation.
10190939	PeopleSoft User Management connector displays FWKOO5 error	This issue has been resolved. PeopleSoft User Management connector will not display FWK005 error, when multiple messages are sent simultaneously from target system.
10117408	PeopleSoft message getting assigned to wrong user in Oracle Identity Manager	This issue has been resolved. The message that is sent to Oracle Identity Manager from PeopleSoft is now getting assigned to the correct user during incremental reconciliation.
10094460	Oracle Identity Manager not processing all PeopleSoft user profile messages	This issue has been resolved. PeopleSoft User Management connector is now reconciling all PeopleSoft user profile messages.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

Documentation-Specific Updates in Release 9.1.0

The following are the documentation-specific updates in release 9.1.0:

- Information about connector deployment has been modified in this document based on the different stages of connector deployment. This information is provided in Chapter 2, "Deploying the Connector."
- The extended functionality of the connector is described in Chapter 4, "Extending the Functionality of the Connector."

- The architecture of the connector has been included in this guide. This information is provided in Section 1.3, "Connector Architecture."
- The field mappings between the target system and Oracle Identity Manager have been moved from the appendix to the first chapter. The field mappings for lookup field synchronization, target resource reconciliation, and provisioning are described in the following sections, respectively:
  - "Lookup Definitions Used During Connector Operations" on page 1-11
  - "User Attributes for Reconciliation" on page 1-26
- The reconciliation matching and action rules for target resource reconciliation have been added to the guide. This information is available at the following section:
  - "Connector Objects Used During Reconciliation" on page 1-26

Documentation-Specific Updates in Release 9.1.0.1

The following is a documentation-specific update in release 9.1.0.1:

- In Section 2.2.1.5, "Deploying the PeopleSoft Listener," the steps to redeploy the PeopleSoftOIMListener.war file into the deployment directory of Oracle WebLogic Server have been modified.

Documentation-Specific Updates in Release 9.1.0.2

The following are the documentation-specific updates in release 9.1.0.2:

- In Section 2.2.1.3, "Configuring the IT Resource" and Section 2.3.3.1, "Configuring the IT Resource for the Connector with the Remote Manager":
  - The definition of the `ServerName` IT resource parameter has been modified
  - The `PIAServerName` IT resource parameter has been added.
- A note in Section 2.2.1.5, "Deploying the PeopleSoft Listener" section has been modified.

Documentation-Specific Updates in Release 9.1.1

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

Documentation-Specific Updates in Release 9.1.1.4

The following are documentation-specific updates in release 9.1.1.4:

- Section 2.2.2.3.3, "Preventing Transmission of Unwanted Fields During Incremental Reconciliation" has been added in the guide.
- Appendix B, "Setting Up SSL on Oracle WebLogic Server" has been added in the guide.

Documentation-Specific Updates in Release 9.1.1.5

There are no documentation-specific updates in release 9.1.1.5.

Documentation-Specific Updates in Release 9.1.1.6

The following are documentation-specific updates in release 9.1.1.6:

- From this release onward, the connector supports the OC4J configuration. The following sections have been updated for OC4J configuration.
  - Section 2.2.1.5.1, "Deploying the PeopleSoft Listener on Oracle Identity Manager Release 9.1.0.x"
  - Section 2.2.1.6, "Removing the PeopleSoft Listener"
  - Section 2.2.2.4, "Configuring the Target System for Provisioning"
  - Section 2.3.1.2.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"
- A note in the ninth step of Section 2.2.1.4, "Configuring the Connector to Support Multiple Versions of the Target System" has been added.
- Steps to configure Oracle Identity Manager server as a non-proxy host on PeopleSoft server has been added in this release. See Section 2.2.2.5, "Configuring Oracle Identity Manager Server as a Non-Proxy Host on PeopleSoft Server" for details.
- In Section 1.1, "Certified Components," PeopleTools 8.52 has been added as a newly certified target system.
- In Section 1.5.2.3.5, "Lookup.PSFT.UM.AttrMap.IDTypes," a note has been added.
- Section 2.3.1.6, "Setting Up the Lookup.PSFT.UM.AttrMap.IDTypes Lookup Definition" has been added.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning 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 PeopleSoft Enterprise Applications as a managed (target) source of user profile data for Oracle Identity Manager.

> **Note:** In this guide, the term **Oracle Identity Manager server** refers to the computer on which Oracle Identity Manager is installed.
>
> At some places in this guide, PeopleSoft Enterprise Applications has been referred to as the **target system.**

The PeopleSoft User Management connector helps you to manage PeopleTools-based PSOPRDEFN user profile records in PeopleSoft applications including Role and Permission List assignments to these records. This is done through target resource reconciliation and provisioning.

In the target resource configuration, information about user accounts 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.

> **Note:** See *Oracle Identity Manager Connector Concepts* for detailed information about connector deployment configurations.

This chapter contains the following sections:

1.1 Certified Components

Table 1–1 lists the components certified for use with the connector.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager release 9.1.0.2 BP05 or later **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.2 BP05 and future releases in the 9.1.0.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* release 1 (11.1.1) and 11.1.1.3 BP02 **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1), 11.1.1.3 BP02, and future releases in the 11.1.1 series that the connector will support.
Target systems	PeopleTools 8.48, PeopleTools 8.49, PeopleTools 8.50, PeopleTools 8.51, and PeopleTools 8.52. Note: When publishing data during certain connector operations, some data fields are blank. This issue has been fixed and the fix is available in the PeopleTools 8.51.13 release.
	Ensure that the following components are installed and configured in the target system environment: ■ Tuxedo and Jolt (the application server) ■ PeopleSoft Internet Architecture ■ PeopleSoft Application Designer (2-tier mode) The following standard PeopleSoft messages are available: ■ USER_PROFILE ■ DELETE_USER_PROFILE
SoD engine	If you want to enable and use the Segregation of Duties (SoD) feature of Oracle Identity Manager release 11.1.1.3 BP02 with this target system, then install Oracle Applications Access Controls Governor release 8.5.1. See Section 1.4.5, "SoD Validation of Entitlement Provisioning" for more information about the SoD feature.
JDK	The JDK requirement is as follows: ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or later ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 or later, or JRockit 1.6 or later

Determining the Version of PeopleTools and the Target System

Before you deploy the connector, you might want to determine the version of PeopleTools and the target system you are using to check whether you are using the combination supported by this connector. To do so, perform the following steps:

1. Open a Web browser and enter the URL of PeopleSoft Internet Architecture. The URL of PeopleSoft Internet Architecture is in the following format:

   ```
   http://IPADDRESS:PORT/psp/ps/?cmd=login
   ```

   For example:

   ```
   http://172.21.109.69:9080/psp/ps/?cmd=login
   ```

2. Click **Change My Password.** On the page that is displayed, press **Ctrl+J.** The versions of PeopleTools and the target system that you are using are displayed.

1.2 Certified Languages

The connector supports the following languages:

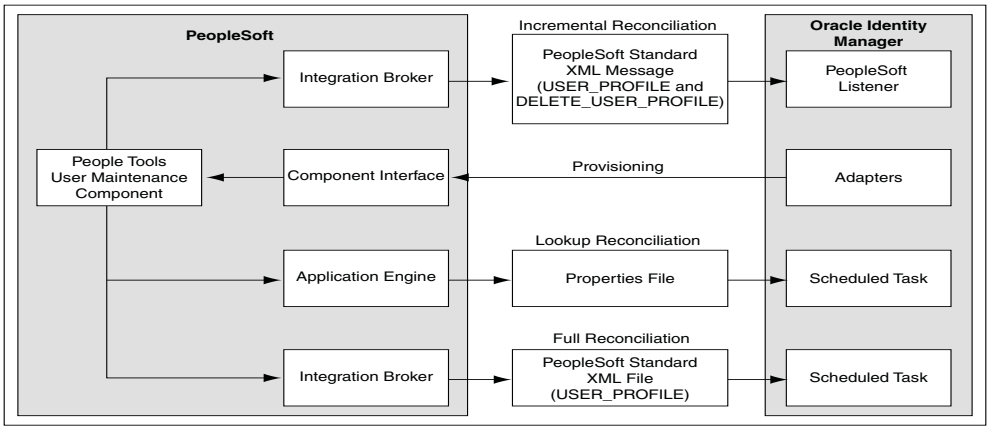
- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

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

1.3 Connector Architecture

Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of the Connector



The architecture of the connector can be explained in terms of the connector operations it supports. They are listed as follows:

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

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

- Section 1.3.1, "Reconciliation"
- Section 1.3.2, "Provisioning"
- Section 1.3.3, "Deployment Options"

1.3.1 Reconciliation

PeopleSoft Enterprise Application is configured as a target resource of Oracle Identity Manager. Through reconciliation, account data that is created and updated on the target system is fetched into Oracle Identity Manager and stored against the corresponding OIM Users.

Standard PeopleSoft XML files and messages are the medium of data interchange between PeopleSoft Enterprise Applications and Oracle Identity Manager.

The method by which account data is sent to Oracle Identity Manager depends on the type of reconciliation that you configure as follows:

- Section 1.3.1.1, "Lookup Reconciliation"
- Section 1.3.1.2, "Full Reconciliation"
- Section 1.3.1.3, "Incremental Reconciliation"

1.3.1.1 Lookup Reconciliation

A lookup reconciliation run fetches the records of Email Types, Currency Codes, Language Codes, Permission Lists, and Roles from the target system. Running PeopleSoft's Application Engine process generates these properties files at a specified location. Lookup reconciliation stores the information from these properties files into Oracle Identity Manager as reference data for subsequent use in provisioning.

You must run lookup reconciliation at periodic intervals to ensure that all the lookup data is reconciled into Oracle Identity Manager. See Section 3.3.1, "Performing Lookup Reconciliation" for instructions to perform Lookup reconciliation.

1.3.1.2 Full Reconciliation

Note: To reconcile all existing target system records into Oracle Identity Manager, you must run full reconciliation the first time you perform a reconciliation run after deploying the connector. This is to ensure that the target system and Oracle Identity Manager contain the same data.

PeopleSoft uses its standard message format USER_PROFILE to send user profile data to external applications such as Oracle Identity Manager. Full reconciliation fetches all

of these records from the target system to reconcile records in Oracle Identity Manager. Full reconciliation within Oracle Identity Manager is implemented using the USER_PROFILE XML file that PeopleSoft generates. See Section 1.4.2, "Support for Standard PeopleSoft Messages" for more information about the message.

Full reconciliation involves the following steps:

See Section 3.3.2, "Performing Full Reconciliation" for instructions to perform full reconciliation.

1. The PeopleSoft Integration Broker populates the XML files for the USER_PROFILE message with all the user profile data.
2. Copy these XML files to a directory on the Oracle Identity Manager host computer.
3. Configure the PeopleSoft User Management Target Reconciliation scheduled task. The XML files are read by this scheduled task to generate reconciliation events.

1.3.1.3 Incremental Reconciliation

Incremental reconciliation involves real-time reconciliation of newly created or modified user data. It is achieved by PeopleSoft standard messages, such as USER_PROFILE and DELETE_USER_PROFILE. See Section 1.4.2, "Support for Standard PeopleSoft Messages" for more information about these messages. You use incremental reconciliation to reconcile individual data changes after an initial, full reconciliation run has been performed. Incremental reconciliation is performed using PeopleSoft application messaging.

Incremental reconciliation involves the following steps:

See Section 3.3.3, "Performing Incremental Reconciliation" for instructions to perform incremental reconciliation.

1. When user data is added, updated, or deleted in the target system, a PeopleCode event is activated.
2. The Integration Broker generates an XML message, such as USER_PROFILE or DELETE_USER_PROFILE, which contains the modified or deleted user data and sends it in real time to the PeopleSoft listener over HTTP. The PeopleSoft listener is a Web application that is deployed on the Oracle Identity Manager host computer. If SSL is configured, then the message is sent to the PeopleSoft listener over HTTPS.
3. The PeopleSoft listener parses the XML message and creates a reconciliation event in Oracle Identity Manager.

Note: During connector deployment:

- On Oracle Identity Manager release 9.1.0.*x*, the PeopleSoft listener is deployed as a WAR file.
- On Oracle Identity Manager release 11.1.1, the PeopleSoft listener is deployed as an EAR file.

1.3.2 Provisioning

PeopleSoft Enterprise Application is configured as a target resource of Oracle Identity Manager. Through provisioning operations performed on Oracle Identity Manager, accounts are created and updated on the target system for OIM Users.

During a provisioning operation, the adapters pass on to PeopleSoft Enterprise Applications user data that are created, modified or deleted in Oracle Identity Manager.

The connector, by default, supports Customer and Vendor ID types in addition to the Employee ID type. The connector is enhanced to support new ID types depending on the PeopleSoft application module being provisioned. The new ID type can then be linked to a user profile for provisioning. See Section 1.4.9, "Adding New ID Types" for more information.

See *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning.

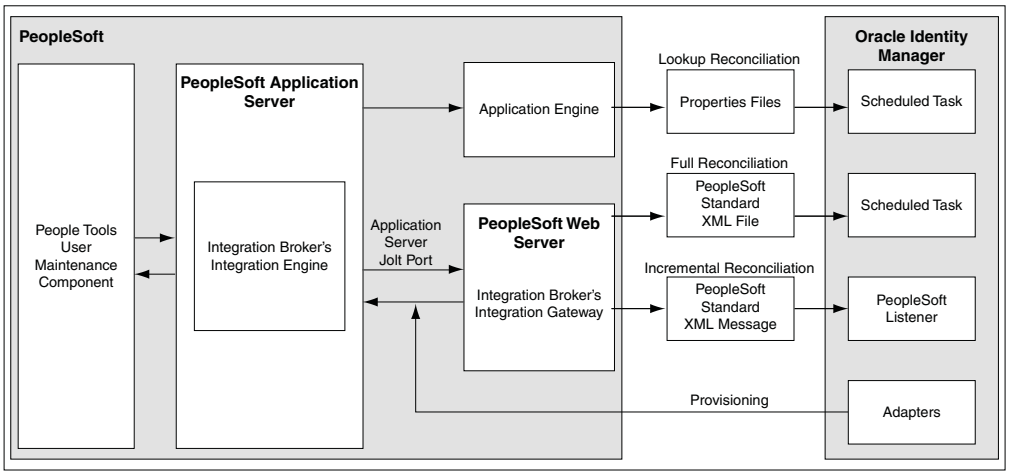
See Section 1.4.5, "SoD Validation of Entitlement Provisioning" for information about the process followed for provisioning of role entitlements in an SoD-enabled environment.

1.3.3 Deployment Options

The PeopleSoft Internet Architecture is flexible; this means that you have many options to consider for deploying PeopleSoft across your enterprise. The following section describes a split-deployment scenario where the Jolt listener resides on a different computer than the Integration Broker.

Figure 1–2 shows the architecture of the connector that supports a split-deployment scenario.

Figure 1–2 Architecture of the Connector for a Split-Deployment Scenario



In this configuration:

1. The Application Engine is run to generate the properties files for lookup reconciliation at a user-specified location on PeopleSoft Application Server. These files are then fed to the respective scheduled tasks in Oracle Identity Manager for lookup reconciliation. See Section 3.2, "Configuring the Scheduled Tasks for Lookup Field Synchronization" for more information.
2. Similarly, the Integration Broker creates PeopleSoft standard XML files at a user specified location on PeopleSoft Application Server for full reconciliation. These XML files are read by PeopleSoft User Management Target Reconciliation scheduled task to generate reconciliation events.

3. Incremental reconciliation is achieved by sending in real time standard PeopleSoft XML messages directly from PeopleSoft Integration Broker to the PeopleSoft listener over HTTP. The PeopleSoft listener is a Web application that is deployed on the Oracle Identity Manager host computer.
4. Provisioning of PeopleSoft user accounts is implemented from Oracle Identity Manager through the PeopleSoft Component Interface-based Java APIs. These APIs connect to the Application Server Jolt port through a limited rights user who has the privilege to add, update, and delete PeopleSoft user accounts.

1.4 Features of the Connector

The following are the features of the connector:

1.4.1 Full and Incremental Reconciliation

The connector supports reconciliation in two ways:

In a full reconciliation run, all records are fetched from the target system to Oracle Identity Manager in the form of XML files. In incremental reconciliation, records that are added, modified, or deleted are directly sent to the listener deployed on the Oracle Identity Manager host computer. The listener parses the records and sends reconciliation events to Oracle Identity Manager.

1.4.2 Support for Standard PeopleSoft Messages

PeopleSoft provides standard messages to synchronize user profiles with external applications, such as Oracle Identity Manager. The connector uses these standard PeopleSoft messages that are delivered as part of PeopleSoft installation to achieve full reconciliation and incremental reconciliation. They are listed as follows:

- USER_PROFILE
- DELETE_USER_PROFILE

  The USER_PROFILE message contains information about user accounts that are created or modified. The DELETE_USER_PROFILE message contains information about user accounts that are deleted.

Fetching all the records present in PeopleSoft to Oracle Identity Manager is implemented by running the USER_PROFILE message. Similarly, when a user profile is updated in PeopleSoft, the USER_PROFILE message is triggered. Oracle Identity Manager uses this message for incremental reconciliation. Similarly, when a user profile is deleted in PeopleSoft, the DELETE_USER_PROFILE message is triggered from PeopleSoft to delete the corresponding provisioned resource in Oracle Identity Manager. The DELETE_USER_PROFILE is supported through incremental reconciliation.

To distinguish between the full and incremental reconciliation USER_PROFILE XML messages, you must identify the number of transaction nodes in the message. In case of full reconciliation, the USER_PROFILE message has multiple transaction nodes. But, in incremental reconciliation, the USER_PROFILE message has a single transaction node for a particular user.

1.4.3 Support for Resending Messages That Are Not Processed

Standard messages provided by PeopleSoft are asynchronous. In other words, if a message is not delivered successfully, the PeopleSoft Integration Broker marks that message as not delivered. The message can then be retried manually.

If the connector is not able to process the message successfully, it sends an error code and PeopleSoft Integration Broker marks that message as Failed. A message marked as Failed can be resent to the listener. See Section 3.4, "Resending Messages That Are Not Received by the PeopleSoft Listener" for details.

> **See Also:** *Resubmitting and Canceling Service Operations for Processing* topic in the PeopleBook *Enterprise PeopleTools 8.49 PeopleBook: PeopleSoft Integration Broker* available on Oracle Technology Network:
>
> `http://download.oracle.com/docs/cd/E13292_01/pt849pbr0/eng/psbooks/tibr/book.htm`

1.4.4 Target Authentication

Target authentication is done to validate whether Oracle Identity Manager should accept messages from the target system or not. Target authentication is done by passing the name of the IT resource in the Integration Broker node. You must ensure that the correct value of the IT resource name is specified in the node. See Section 2.2.2.3.1, "Configuring PeopleSoft Integration Broker" for setting up the node. In addition, the flag IsActive is used to verify whether the IT resource is active or not. The value of this flag is `Yes`, by default. When this value is Yes, target authentication is carried out. Target authentication fails if it is set to `No`.

1.4.5 SoD Validation of Entitlement Provisioning

This connector supports the SoD feature in Oracle Identity Manager release 11.1.1.3 BP02.

> **Note:** The connector does not support the SoD feature in Oracle Identity Manager release 9.1.0.2 and later releases in the 9.1.0.2 series.

The following are the focal points of this feature:

- The SoD Invocation Library (SIL) is bundled with Oracle Identity Manager release. The SIL acts as a pluggable integration interface with any SoD engine.

- The connector is preconfigured to work with Oracle Applications Access Controls Governor as the SoD engine. To enable this, changes have been made in the provisioning workflows of the connector.
- The SoD engine processes role entitlement requests that are sent through the connector. Potential conflicts in role assignments can be automatically detected.

See Also:

Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager 11g Release 1 (11.1.1) for detailed information about the SoD feature

Section 2.3.1.8, "Configuring SoD" in this guide

SoD Validation Process

When you enable SoD, an entitlement is provisioned only after the SoD validation clears the request for the entitlement. Users can create entitlement requests for themselves. Alternatively, administrators can submit entitlement requests on behalf of users.

Note:

The connector supports the scenario in which a single request is created for multiple roles and a single approver is assigned the entire request.

the SoD validation process is asynchronous. The response from the SoD engine must be brought to Oracle Identity Manager by a scheduled task.

Request-based provisioning of roles involves the following steps:

1. A request for a role is created.

   Section 3.7, "Provisioning Operations Performed in an SoD-Enabled Environment" describes the procedure to create the request.

2. After the standard approval process, the SoD Checker process task is triggered. This process task is completed by running the GetSODCheckResultApproval scheduled task from the task scheduler.

   Note: The approver should not approve/deny this task manually while approving the request.

   After the SoD Checker process task is run and the SoD Check result is passed, the Human Approval task (if it has been defined) is triggered.

3. If the approval process clears the request, then the request data is sent to the process form. When this data reaches the target system, the role is assigned to the user.

   Note: If SoD is not enabled or if the provisioning operation does not include entitlement provisioning, then the SODCheckStatus field remains in the `SODCheckNotInitiated` state.

If the approval process does not clear the request, then the status of the request is set to Denied.

1.4.6 Validation and Transformation 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.

- Section 4.7, "Configuring Validation of Data During Reconciliation" provides information about setting up the validation feature.
- Section 4.8, "Configuring Transformation of Data During Reconciliation" provides information about setting up the transformation feature.

1.4.7 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 such as 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 are created, one for each target system installation.

The configuration properties of the connection pool are part of the IT resource definition. Section 2.2.1.3, "Configuring the IT Resource" provides information about setting up the connection pool.

Note: The connector does not support connection pooling for provisioning multiple versions of the target system. In other words, connection pooling is supported only when provisioning is done for one version of the target system. In this case, the Multiple Version Support parameter is set to `No` in the Lookup.PSFT.Configuration lookup definition.

1.4.8 Durable Entitlements

The connector now supports the capability to retrieve data from two servers that exist in the same Lookup definition. This has been made possible by placing IT resource in the lookup Code Key.

1.4.9 Adding New ID Types

You can configure the connector to support additional ID types effortlessly. The connector by default supports the following ID types other than the Employee (EMP) ID type:

- Customer (CST)
- Vendor (VND)

The following additional attributes are provided in the Oracle Identity Manager process form to support these ID types:

For Customer:

Set ID

Customer ID

For Vendor:

Set ID

Vendor ID

The Section 4.4, "Adding New ID Types for Provisioning" describes the procedure to add ID types.

1.4.10 Deleting User Accounts

When a user profile is deleted from PeopleSoft, a DELETE_USER_PROFILE message is triggered from PeopleSoft that deletes the corresponding provisioned resource in Oracle Identity Manager.

1.4.11 Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations

You can specify a list of accounts that must be excluded from all reconciliation and provisioning operations. Accounts whose user IDs you specify in the exclusion list are not affected by reconciliation and provisioning operations. See Section 1.5.2.3.4, "Lookup.PSFT.UM.ExclusionList" for more information.

1.4.12 Support for Multiple Versions of the Target System

Note: The connector only supports the PeopleTools 8.48 and PeopleTools 8.49 versions of the target system in the release. See Section 1.1, "Certified Components" for more information about certification. If you are using a PeopleTools version that is not supported, then you are likely to encounter issues that might be difficult to resolve.

The connector can be configured to work with different versions of the target system at the same time. For example, you can use a single instance of the connector to integrate Oracle Identity Manager with a PeopleTools 8.48 installation and a PeopleTools 8.49 installation.

See Section 2.2.1.4, "Configuring the Connector to Support Multiple Versions of the Target System" for more information.

1.5 Lookup Definitions Used During Connector Operations

Lookup definitions used during connector operations can be categorized as follows:

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

1.5.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field to specify a single value from a set of values. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are 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.

Note: As an implementation best practice, lookup fields should be synchronized before you perform reconciliation or provisioning operations.

Table 1–2 lists the lookup fields that are synchronized with their corresponding lookup definitions in Oracle Identity Manager.

Table 1–2 Lookup Fields That Are Synchronized

Lookup Definition	Target System Lookup Field	Synchronization Method
Lookup.PSFT.UM.LanguageCode	Language Code	You use the Language Code Lookup Reconciliation scheduled task to synchronize this lookup definition.
Lookup.PSFT.UM.CurrencyCode	Currency Code	You use the Currency Code Lookup Reconciliation scheduled task to synchronize this lookup definition.
Lookup.PSFT.UM.PermissionList	Permission Lists	You use the Permission List Lookup Reconciliation scheduled task to synchronize this lookup definition.
Lookup.PSFT.UM.EmailType	Email Type	You use the Email Type Lookup Reconciliation scheduled task to synchronize this lookup definition.
Lookup.PSFT.UM.Roles	Role Name	You use the Roles Lookup Reconciliation scheduled task to synchronize this lookup definition.

1.5.2 Preconfigured Lookup Definitions

This section describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. Either lookup definitions are prepopulated with values or values must be manually entered in them after the connector is deployed.

The predefined lookup definitions can be categorized as follows:

- Section 1.5.2.1, "Lookup Definitions Used to Process USER_PROFILE Messages"
- Section 1.5.2.2, "Lookup Definitions Used to Process DELETE_USER_PROFILE Messages"
- Section 1.5.2.3, "Other Lookup Definitions"

1.5.2.1 Lookup Definitions Used to Process USER_PROFILE Messages

The following lookup definitions are used to process the USER_PROFILE messages:

1.5.2.1.1 Lookup.PSFT.Message.UserProfile.Configuration The Lookup.PSFT.Message.UserProfile.Configuration lookup definition provides configuration-related information for the USER_PROFILE message.

The Lookup.PSFT.Message.UserProfile.Configuration lookup definition has the following entries:

Code Key	Decode	Description
Attribute Mapping Lookup	Lookup.PSFT.UM.UserProfile.AttributeMapping	Name of the lookup definition that maps Oracle Identity Manager attributes with the attributes in the USER_PROFILE message See Section 1.5.2.1.2, "Lookup.PSFT.UM.UserProfile.AttributeMapping" for more information about this lookup definition.
Child Table Lookup Definition	Lookup.PSFT.UM.UserProfile.ChildTables	Name of the lookup definition that maps resource object fields and multivalued target system attributes
Custom Query	Enter a Value	If you want to implement limited reconciliation, then enter the query condition that you create by following the instructions given in Section 3.3.4, "Limited Reconciliation."
Data Node Name	Transaction	Name of the node in the XML files to run a transaction Default value: `Transaction` You must not change the default value.
IT Resource Name	PSFT Server	Name of the IT resource
Message Handler Class	oracle.iam.connectors.psft.common.handler.impl.PSFTUserProfileReconMessageHandlerImpl	Name of the Java class that accepts the XML payload, configuration information, and a handle to Oracle Identity Manager. Depending on the message type, it retrieves the appropriate configuration from Oracle Identity Manager and processes the message. To parse a specific message type, it relies on a Message Parser factory. If you want a customized implementation of the message, then you must extend the `MessageHandler.java` class.

Code Key	Decode	Description
Message Parser	oracle.iam.connectors.psft.common.parser.impl.UserMessageParser	Name of the parser implementation class that contains the logic for message parsing If you want a customized implementation of the message, then you must extend the `MessageParser.java` class.
Recon Lookup Definition	Lookup.PSFT.UM.UserProfile.Recon	Name of the lookup definition that maps the Oracle Identity Manager attributes with the Resource Object attributes
Resource Object	Peoplesoft User	Name of the resource object
Transformation Lookup Definition	Lookup.PSFT.UM.UserProfile.Transformation	Name of the transformation lookup definition See Section 4.8, "Configuring Transformation of Data During Reconciliation" for more information about adding entries in this lookup definition.
User Status Lookup	Lookup.PSFT.UM.UserProfile.UserStatus	Name of the lookup definition that provides the user status See Section 1.5.2.1.4, "Lookup.PSFT.UM.UserProfile.UserStatus" for more information about this lookup definition.
Use Transformation	No	Use this parameter to perform transformation.
Use Validation	No	Use this parameter to perform validation.
Validation Lookup Definition	Lookup.PSFT.UM.UserProfile.Validation	Name of the validation lookup definition See Section 4.7, "Configuring Validation of Data During Reconciliation" for more information about adding entries in this lookup definition.

1.5.2.1.2 Lookup.PSFT.UM.UserProfile.AttributeMapping

The Lookup.PSFT.UM.UserProfile.AttributeMapping lookup definition maps OIM User attributes with the attributes defined in the USER_PROFILE message XML. The following is the format of the values stored in this lookup definition:

Code Key	Decode
Currency Code	CURRENCY_CD~PSOPRDEFN
Customer ID	CUST_ID~PSOPRALIAS~OPRALIASTYPE=CST
Customer Set ID	SETID~PSOPRALIAS~OPRALIASTYPE=CST
Email ID	EMAILID~PSUSEREMAIL~PRIMARY_EMAIL=N~None~CHILD=Email IDs
Email Type	EMAILTYPE~PSUSEREMAIL~PRIMARY_EMAIL=N~None~CHILD=Email IDs

Code Key	Decode
Employee ID	EMPLID~PSOPRALIAS~OPRALIASTYPE=EMP
Language Code	LANGUAGE_CD~PSOPRDEFN
Multi Language Code	MULTILANG~PSOPRDEFN
Navigator Home Permission List	DEFAULTNAVHP~PSOPRDEFN
Primary Email ID	EMAILID~PSUSEREMAIL~PRIMARY_EMAIL=Y
Primary Email Type	EMAILTYPE~PSUSEREMAIL~PRIMARY_EMAIL=Y
Primary Permission List	OPRCLASS~PSOPRDEFN
Process Profile Permission List	PRCSPRFLCLS~PSOPRDEFN
Role	ROLENAME~PSROLEUSER_VW~None~None~CHILD=Roles
Row Security Permission List	ROWSECCLASS~PSOPRDEFN
Symbolic ID	SYMBOLICID~PSOPRDEFN
User Description	OPRDEFNDESC~PSOPRDEFN
User ID	OPRID~PSOPRDEFN~None~None~PRIMARY
User ID Alias	USERIDALIAS~PSOPRDEFN
User Status	ACCTLOCK~PSOPRDEFN
Vendor ID	VENDOR_ID~PSOPRALIAS~OPRALIASTYPE=VND
Vendor Set ID	SETID~PSOPRALIAS~OPRALIASTYPE=VND

Code Key: Name of the OIM User field

Decode: Combination of the following elements separated by the tilde (~) character:

NODE~PARENT NODE~TYPE NODE=Value~EFFECTIVE DATED NODE~PRIMARY or CHILD=Multivalued Child Table RO Field

In this format:

`NODE`: Name of the node in the USER_PROFILE message XML from which the value is read. You must specify the name of the NODE in the lookup definition. It is a mandatory field.

`PARENT NODE`: Name of the parent node for the NODE. You must specify the name of the parent node in the lookup definition. It is a mandatory field.

`TYPE NODE=Value`: Type of the node associated with the Node value. Value defines the type of the Node.

`EFFECTIVE DATED NODE`: Effective-dated node for the NODE element, if any.

PeopleSoft supports effective-dated events. The value refers to the name of the node that provides information about the date on which the event becomes effective.

The USER_PROFILE message does not support effective-dated information. Therefore, the value of this parameter in the preceding syntax is `None`.

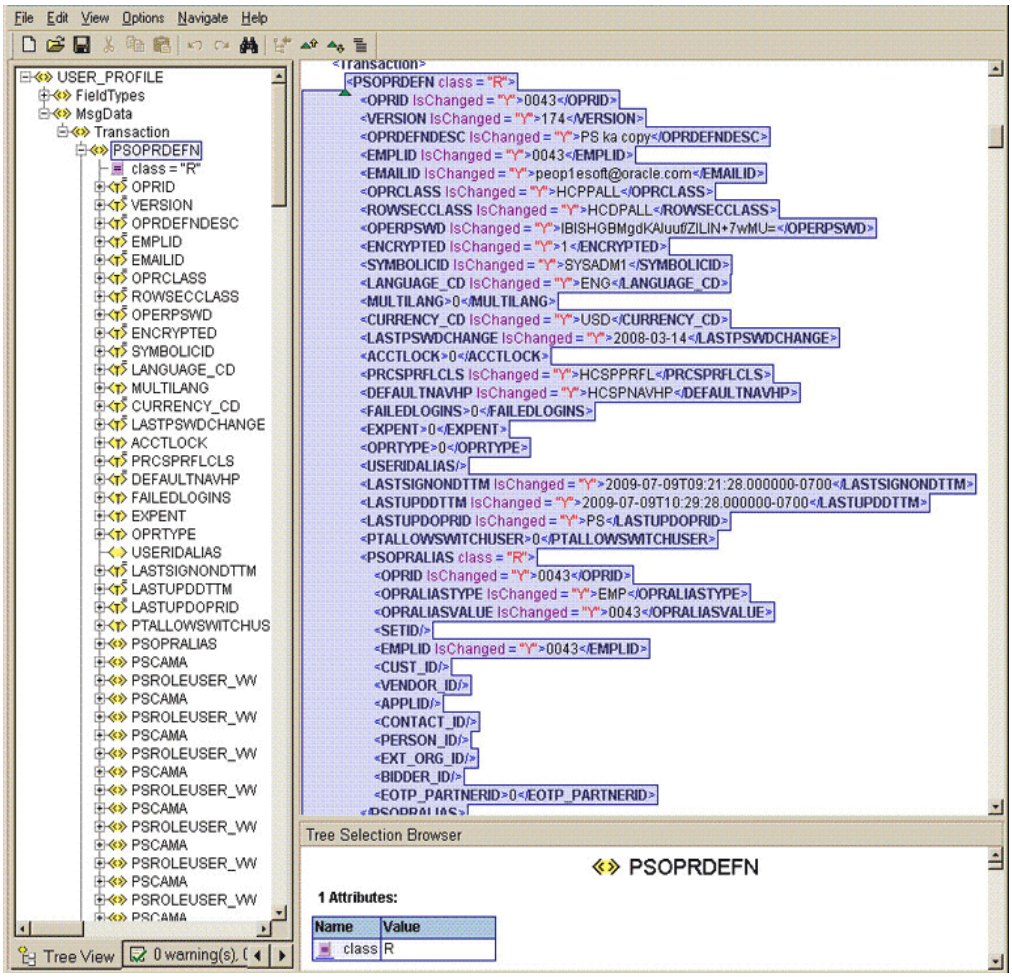
`PRIMARY or Child=Multivalued Child Table RO Field`: Specifies whether the node is a mandatory field or a multivalued attribute on Oracle Identity Manager.

In case of multivalued attribute data, CHILD specifies that this is a Child data followed by the name of the table defined in the resource object to which the data corresponds.

The following scenario illustrates how to map the entries in the lookup definition.

You want to retrieve the value for the Email Type Code Key that is defined as a multivalued attribute in Oracle Identity Manager. In PeopleSoft, the PSUSEREMAIL rowset lists the e-mail IDs assigned to a user. The NODE will be EMAILTYPE as depicted in the XML file. See the sample XML file in Figure 1–3 for more information about each node in the USER_PROFILE message.

Figure 1–3 Sample XML File for USER_PROFILE Message



Sample XML File for USER_PROFILE Message

****

The parent node for the EMAILTYPE node will be PSUSEREMAIL. Now suppose, you have a scenario where want to retrieve the e-mail IDs that are not defined as Primary. In this case, you must identify the TYPE NODE value for the parent node that has the value N. In this example, the type node is PRIMARY_EMAIL with the value N.

The effective-dated node will be None, because the USER_PROFILE message does not provide this information.

The Multivalued Child Table RO Field in this scenario is Email IDs. It is the name of the table defined in the Resource Object for the Email ID child attribute.

If you do not want to provide any element in the Decode column, then you must specify `None`. This is implemented for the User ID attribute.

Now, you can concatenate the various elements of the syntax by using a tilde (~) to create the Decode entry for Email Type, as follows:

NODE: EMAILTYPE

PARENT NODE: PSUSEREMAIL

TYPE NODE=Value: PRIMARY_EMAIL=N

EFFECTIVE DATED NODE: None

Child=Multivalued Child Table RO Field: CHILD=Email IDs

So, the Decode column for Email Type is as follows:

```
EMAILTYPE~PSUSEREMAIL~PRIMARY_EMAIL=N~None~CHILD=Email IDs
```

1.5.2.1.3 Lookup.PSFT.UM.UserProfile.Recon The Lookup.PSFT.UM.UserProfile.Recon lookup definition maps the resource object field name with the value fetched from the Lookup.PSFT.UM.UserProfile.AttributeMapping lookup.

The Lookup.PSFT.UM.UserProfile.Recon lookup definition has the following entries:

Code Key	Decode
Currency Code	Currency Code~None~LKF
Customer ID	Customer ID
Customer Set ID	Customer Set ID
Email Address	Email ID~None~None~Child
Email Type	Email Type~None~LKF~Child
Employee ID	Employee ID
ITResource Name	IT Resource Name
Language Code	Language Code~None~LKF
MultiLanguage code	Multi Language Code
Navigator Home Page	Navigator Home Permission List~None~LKF
Primary Email Address	Primary Email ID
Primary Email Type	Primary Email Type~None~LKF
Primary Permission	Primary Permission List~None~LKF
Process Profile	Process Profile Permission List~None~LKF
Role Name	Role~None~LKF~Child
Row Security	Row Security Permission List~None~LKF
Symbolic ID	Symbolic ID
User Description	User Description
User ID	User ID
User ID Alias	User ID Alias
User Status	User Status~User Status Lookup
Vendor ID	Vendor ID
Vendor Set ID	Vendor Set ID

Code Key: Name of the resource object field in Oracle Identity Manager

Decode: Combination of the following elements separated by a tilde (~) character:

ATTRIBUTE ~ LOOKUP DEF ~LKF

In this format:

ATTRIBUTE: Refers to the Code Key of the Lookup.PSFT.UM.UserProfile.AttributeMapping lookup definition

LOOKUP DEF: Name of the lookup definition, if the value of the attribute is retrieved from a lookup. This lookup is specified in the message-specific configuration lookup.

LKF: Specifies that the attribute is a lookup field on the process form.

Consider the scenario discussed in Section 1.5.2.1.2, "Lookup.PSFT.UM.UserProfile.AttributeMapping." In that example, you fetched the Email Type in the Code Key column from the EMAILTYPE node of the XML file.

Now, you must map this Email Type defined in the Lookup.PSFT.UM.UserProfile.AttributeMapping lookup definition with the resource object attribute Email Type defined in the Lookup.PSFT.UM.UserProfile.Recon lookup definition Code Key.

For example, if the name of the Code Key column in the Lookup.PSFT.UM.UserProfile.AttributeMapping lookup definition is E_Type then you define the mapping in the Lookup.PSFT.UM.UserProfile.Recon lookup definition as follows:

Code Key: Email Type

Decode: E_Type~None~LKF

In other words, this implies that the value for Email Type in the Lookup.PSFT.UM.UserProfile.Recon lookup definition is fetched from E_Type defined in the attribute mapping lookup definition.

The same process holds true for other attributes defined in the lookup.

However, to fetch the value of the User Status resource object field, you must consider the User Status lookup definition. `User Status` is defined in the message-specific attribute lookup, Lookup.PSFT.UM.UserProfile.AttributeMapping, which has a value `0` that is fetched from the `ACCTLOCK` node in the XML.

Now, the User Status Lookup lookup definition is defined in the message-specific configuration, Lookup.PSFT.Message.UserProfile.Configuration lookup definition. The mapping is as follows:

Code Key: User Status Lookup

Decode: Lookup.PSFT.UM.UserProfile.UserStatus

In other words, you must search for the value `0` in the Lookup.PSFT.UM.UserProfile.UserStatus lookup definition. The mapping in Lookup.PSFT.UM.UserProfile.UserStatus lookup definition is defined as follows:

Code Key: 0

Decode: Enabled

The resource is updated with the user status as **Enabled.**

1.5.2.1.4 Lookup.PSFT.UM.UserProfile.UserStatus

The Lookup.PSFT.UM.UserProfile.UserStatus lookup definition maps the value of the

ACCTLOCK node in the USER_PROFILE message XML with the status to be shown in Oracle Identity Manager for the user.

The Lookup.PSFT.UM.UserProfile.UserStatus lookup definition has the following entries:

Code Key	Decode
0	Enabled
1	Disabled

Section 2.3.1.4, "Setting Up the Lookup.PSFT.UM.UserProfile.UserStatus Lookup Definition" describes the procedure to modify the Decode values in this lookup definition.

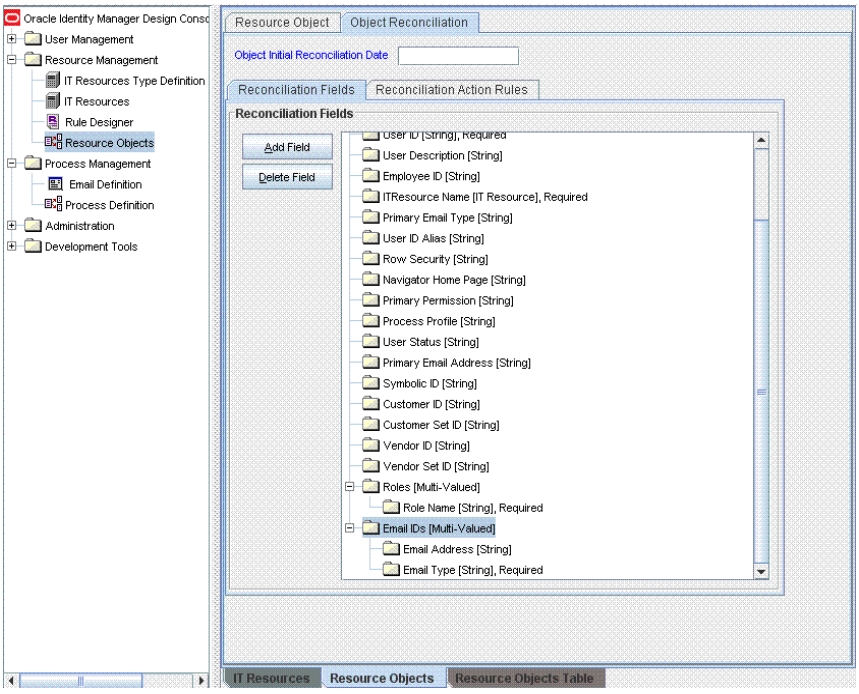
1.5.2.1.5 Lookup.PSFT.UM.UserProfile.ChildTables

The Lookup.PSFT.UM.UserProfile.ChildTables lookup definition maps the resource object fields with the multivalued target system attributes.

Code Key: Multivalued Child Table resource object field

Decode: Child Table attributes defined in the resource object separated by the tilde (~) character

The following screenshot displays the link between the table and the resource object attribute:



The Lookup.PSFT.UM.UserProfile.ChildTables lookup definition has the following entries:

Code Key	Decode
Email IDs	Email Address~Email Type
Roles	Role Name

1.5.2.1.6 Lookup.PSFT.UM.UserProfile.Validation

The Lookup.PSFT.UM.UserProfile.Validation lookup definition is used to store the mapping between the attribute for which validation has to be applied and the validation implementation class.

The Lookup.PSFT.UM.UserProfile.Validation lookup definition is empty, by default.

See Section 4.7, "Configuring Validation of Data During Reconciliation" for more information about adding entries in this lookup definition.

1.5.2.1.7 Lookup.PSFT.UM.UserProfile.Transformation

The Lookup.PSFT.UM.UserProfile.Transformation lookup definition is used to store the mapping between the attribute for which transformation has to be applied and the transformation implementation class.

The Lookup.PSFT.UM.UserProfile.Transformation lookup definition is empty, by default.

See Section 4.8, "Configuring Transformation of Data During Reconciliation" for more information about adding entries in this lookup definition.

1.5.2.2 Lookup Definitions Used to Process DELETE_USER_PROFILE Messages

The following lookup definitions are used to process DELETE_USER_PROFILE messages:

1.5.2.2.1 Lookup.PSFT.Message.DeleteUserProfile.Configuration

The Lookup.PSFT.Message.DeleteUserProfile.Configuration lookup definition provides configuration-related information for the DELETE_PROFILE message.

The Lookup.PSFT.Message.DeleteUserProfile.Configuration lookup definition has the following entries:

Code Key	Decode	Description
Attribute Mapping Lookup	Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping	Name of the lookup definition that maps Oracle Identity Manager attributes with attributes in the DELETE_PROFILE message See Section 1.5.2.2.2, "Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping" for more information about this lookup definition.
Data Node Name	Transaction	Name of the node in the XML files to run a transaction Default value: `Transaction` You must not change the default value.
IT Resource Name	PSFT Server	Name of the IT resource

Code Key	Decode	Description
Message Handler Class	oracle.iam.connectors.psft.common.handler.impl.PSFTDeleteUserReconMessageHandlerImpl	Name of the Java class that accepts the XML payload, configuration information, and a handle to Oracle Identity Manager. Depending on the message type, it retrieves the appropriate configuration from Oracle Identity Manager and processes the message. To parse a specific message type, it relies on a Message Parser factory. If you want a customized implementation of the message, then you must extend the `MessageHandler.java` class.
Message Parser	oracle.iam.connectors.psft.common.parser.impl.DeleteUserMessageParser	Name of the parser implementation class that contains the logic for message parsing If you want a customized implementation of the message, then you must extend the `MessageParser.java` class.
Recon Lookup Definition	Lookup.PSFT.UM.DeleteUserProfile.Recon	Name of the lookup definition that maps the Oracle Identity Manager attributes with the Resource Object attributes See Section 1.5.2.2.3, "Lookup.PSFT.UM.DeleteUserProfile.Recon" for more information about this lookup definition.
Resource Object	Peoplesoft User	Name of the resource object

1.5.2.2.2 Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping

The Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping lookup definition maps OIM User attributes with the attributes defined in the DELETE_PROFILE message XML.

The following is the format of the values stored in this lookup definition:

Code Key	Decode
User ID	`OPRID~PRG_USR_PROFILE~None~None~PRIMARY`

Code Key: Name of the OIM User field

Decode: Combination of the following elements separated by a tilde (~) character:

`NODE~PARENT NODE~TYPE NODE=Value~EFFECTIVE DATED NODE~PRIMARY`

For more information about the preceding syntax, see Section 1.5.2.1.2, "Lookup.PSFT.UM.UserProfile.AttributeMapping."

1.5.2.2.3 Lookup.PSFT.UM.DeleteUserProfile.Recon

The Lookup.PSFT.UM.DeleteUserProfile.Recon lookup definition maps the resource object field name with the value fetched from the Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping lookup definition.

The following is the format of the values stored in this table:

Code Key	Decode
User ID	User ID
ITResource Name	IT Resource Name

1.5.2.3 Other Lookup Definitions

The following are the predefined generic lookup definitions:

1.5.2.3.1 Lookup.PSFT.Configuration The Lookup.PSFT.Configuration lookup definition is used to store configuration information that is used by the connector. See Section 2.2.1.3, "Configuring the IT Resource" for information about the entries in this lookup definition.

> **Note:** This lookup definition is common to both, Employee Reconciliation and User Management connectors. Therefore, it has entries for both connector features.

The Lookup.PSFT.Configuration lookup definition has the following entries:

Code Key	Decode	Description
Constants Lookup	Lookup.PSFT.UM.Constants	Name of the lookup definition that is used to store constants used by the connector
DELETE_USER_PROFILE	Lookup.PSFT.Message.DeleteUserProfile.Configuration	Name of the lookup definition for the DELETE_USER_PROFILE message
Delete User Profile Component Interface Name	DELETE_USER_PROFILE	Component interface that deletes user data in PeopleSoft Enterprise Applications
HRMS Resource Exclusion List Lookup	Lookup.PSFT.HRMS.ExclusionList	Name of the Resource Exclusion lookup for PeopleSoft Employee Reconciliation This is used for the Employee Reconciliation functionality, and is not applicable in this context.
ID Types Attribute Map Lookup	Lookup.PSFT.UM.AttrMap.IDTypes	Name of the lookup definition for ID type attributes You must not change this value. See Section 1.5.2.3.5, "Lookup.PSFT.UM.AttrMap.IDTypes" for more information about this lookup definition.

Code Key	Decode	Description
Ignore Root Audit Action	No	Use this value if the Root PSCAMA audit action is required to be considered while parsing the XML message. Use `Yes` if PSCAMA Audit Action is not taken into account. Here, the Root Audit Action is considered as a Change event. Use `No` if PSCAMA Audit Action is taken into account. If Root PSCAMA Audit Action is NULL or Empty, then the Root Audit Action is considered as an ADD event. **See Also:** Appendix A, "Determining the Root Audit Action Details"
Multiple Version Support	No	Use this parameter to provision multiple versions of the target system. If the connector is used for provisioning multiple versions of the target system, then the value of this parameter is set to `Yes`, else `No`. See Section 2.2.1.4, "Configuring the Connector to Support Multiple Versions of the Target System" for details.
PERSON_BASIC_FULLSYNC	Lookup.PSFT.Message.PersonBasicSync.Configuration	Name of the lookup definition for the PERSON_BASIC_FULLSYNC message This is used for the Employee Reconciliation functionality, and is not applicable in this context.
PERSON_BASIC_SYNC	Lookup.PSFT.Message.PersonBasicSync.Configuration	Name of the lookup definition for the PERSON_BASIC_SYNC message This is used for the Employee Reconciliation functionality, and is not applicable in this context.
Provisioning Attribute Map Lookup	Lookup.PSFT.UM.Attr.Map.Prov	Name of the lookup definition that contains provisioning information

Code Key	Decode	Description
Target Date Format	yyyy-MM-dd	Data format of the Date type data in the XML file and messages You must not change this value.
UM Resource Exclusion List Lookup	Lookup.PSFT.UM.ExclusionList	Name of the Resource Exclusion lookup for User Management operations See Section 2.3.1.3, "Setting Up the Lookup.PSFT.UM.Exclusion List Lookup Definition" for more information about this lookup definition.
USER_PROFILE	Lookup.PSFT.Message.UserProfile.Configuration	Name of the lookup definition for the USER_PROFILE message See Section 1.5.2.1.1, "Lookup.PSFT.Message.User Profile.Configuration" for more information about this lookup definition.
User Profile Component Interface Name	USER_PROFILE	Component interface that loads user data in PeopleSoft Enterprise Applications
User Profile illegal Characters	,~;~ ~:~&~(~)~\~[~]~/~PPLSOFT	List of characters or strings that are not supported by PeopleSoft in the value specified for any user profile field
Use Validation For Prov	No	Validation flag for User Management provisioning
Validation Lookup For Prov	Lookup.PSFT.UM.Validation	Name of the lookup definition required for performing validation while provisioning
WORKFORCE_FULLSYNC	Lookup.PSFT.Message.WorkForceSync.Configuration	Name of the lookup definition for the WORKFORCE_FULLSYNC message This is used for the Employee Reconciliation functionality, and is not applicable in this context.
WORKFORCE_SYNC	Lookup.PSFT.Message.WorkForceSync.Configuration	Name of the lookup definition for the WORKFORCE_SYNC message This is used for the Employee Reconciliation functionality, and is not applicable in this context.

You can configure the message names, such as USER_PROFILE and DELETE_USER_PROFILE defined in this lookup definition. See Section 2.3.1.5,

"Setting Up the Lookup.PSFT.Configuration Lookup Definition" for instructions on configuring these message names in the lookup definition.

1.5.2.3.2 Lookup.PSFT.UM.Attr.Map.Prov The Lookup.PSFT.UM.Attr.Map.Prov lookup definition maps the process form fields with the target system APIs. The Code Key holds the names of process form fields. The Decode column holds the setApi name and the Data type separated by a comma (,).

The Lookup.PSFT.UM.Attr.Map.Prov lookup definition has the following entries:

Code Key	Decode
UD_PSFT_BAS_NAVIGATORHOMELIST	setNavigatorHomePermissionList,String
UD_PSFT_BAS_LANGUAGE_CD	setLanguageCode,String
UD_PSFT_BAS_CURRENCYCODE	setCurrencyCode,String
UD_PSFT_BAS_OPERPSWD	setPassword,String
UD_PSFT_BAS_USERIDALIAS	setUserIDAlias,String
UD_PSFT_BAS_MULTILANG_CD	setMultiLanguageEnabled,BigDecimal
UD_PSFT_BAS_SYMBOLICID	setSymbolicID,String
UD_PSFT_BAS_ROWPERMISSIONLIST	setRowSecurityPermissionList,String
UD_PSFT_BAS_OPRDEFNDESC	setUserDescription,String
UD_PSFT_BAS_PRPERMISSIONLIST	setPrimaryPermissionList,String
UD_PSFT_BAS_PROCESSPROFILELIST	setProcessProfilePermissionList,String

1.5.2.3.3 Lookup.PSFT.UM.Validation The Lookup.PSFT.UM.Validation lookup definition stores the mapping between the process form column name for which validation has to be applied and the validation implementation class.

The Lookup.PSFT.UM.Validation lookup definition is empty, by default.

For example, to perform validation on the User ID attribute, you must update the Lookup.PSFT.UM.Validation lookup definition with the following values:

Code Key	Decode
UD_PSFT_BAS_OPRID	Complete Package Name of the Implementation Class

See Section 4.7, "Configuring Validation of Data During Reconciliation" for more information.

1.5.2.3.4 Lookup.PSFT.UM.ExclusionList The Lookup.PSFT.UM.ExclusionList lookup definition holds user IDs of target system accounts for which you do not want to perform reconciliation and provisioning.

The following is the format of the values stored in this table:

Code Key: User ID resource object field name

Decode: List of user IDs separated by the tilde character (~)

Section 2.3.1.3, "Setting Up the Lookup.PSFT.UM.ExclusionList Lookup Definition" describes the procedure to add entries in this lookup definition.

1.5.2.3.5 Lookup.PSFT.UM.AttrMap.IDTypes The Lookup.PSFT.UM.AttrMap.IDTypes lookup definition maps the process form fields with target system attributes. The mapping is as follows:

Code Key: Name of process form fields

Decode: *ID TYPE ~ ATTRIBUTE NAME* where tilde (~) is used as a separator between the ID type and the attribute name

The format that you must use is as follows:

FORM COLUMN NAME=IDTYPE~ATTRIBUTENAME

Section 4.4, "Adding New ID Types for Provisioning" describes the procedure to add ID Types.

The Lookup.PSFT.UM.AttrMap.IDTypes lookup definition has the following entries by default:

Note: The default entries in this lookup definition are applicable for PeopleTools 8.48 and PeopleTools 8.49. If you are using PeopleTools 8.5*x*, then you must modify some of the entries in this lookup definition. See Section 2.3.1.6, "Setting Up the Lookup.PSFT.UM.AttrMap.IDTypes Lookup Definition" for more infomation.

Code Key	Decode
UD_PSFT_BAS_EMPLID	EMP~EMPLID
UD_PSFT_BAS_CUSTSETID	CST~SetID#1
UD_PSFT_BAS_CUSTID	CST~Customer ID#2
UD_PSFT_BAS_VNDSETID	VND~SetID#1
UD_PSFT_BAS_VNDID	VND~Vendor ID#2

1.6 Connector Objects Used During Reconciliation

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

See Also: "Target Resource Reconciliation" in *Oracle Identity Manager Connector Concepts* for conceptual information about target resource reconciliation

This section discusses the following topics:

- Section 1.6.1, "User Attributes for Reconciliation"
- Section 1.6.2, "Reconciliation Rules"
- Section 1.6.3, "Reconciliation Action Rules"

1.6.1 User Attributes for Reconciliation

Table 1–3 lists the target system attributes whose values are fetched during a target resource reconciliation run.

Table 1–3 Attributes Used for Reconciliation

Resource Object Field	Target System Attribute	Description
Single-Valued Fields		
User Id	PSOPRDEFN.OPRID	Login ID of the user profile This is a mandatory field.
Employee Id	PSOPRDEFN.EMPLID	Employee ID of the employee linked with the user profile
User Description	PSOPRDEFN.OPRDEFNDESC	Description of the user profile
Multi Language Code	PSOPRDEFN.MULTILANG	Multilanguage code
Language Code	PSOPRDEFN.LANGUAGE_CD	Language code
Currency Code	PSOPRDEFN.CURRENCY_CD	Currency code
User Id Alias	PSOPRDEFN.USERIDALIAS	Alias of user login ID
Row Security Permission List	PSOPRDEFN.ROWSECCLASS	Row security parameter
Process Profile Permission List	PSOPRDEFN.PRCSPRFLCLS	Process profile parameter
Navigator Home Permission List	PSOPRDEFN.DEFAULTNAVHP	Navigator home page address
Primary Permission List	PSOPRDEFN.OPRCLASS	Primary permission list
Primary Email Address	PSUSEREMAIL.EMAILID	E-mail address (primary e-mail account)
Primary Email Type	PSUSEREMAIL.EMAILTYPE	Email type (primary e-mail account)
Multivalued Fields		
RoleName	PSROLEUSER_VW.ROLENAME	The role name that is assigned to the user profile
Email Address	PSUSEREMAIL.EMAILID	E-mail address
Email Type **Note:** To specify the e-mail address for an account, you must also specify the e-mail type of that e-mail address.	PSUSEREMAIL.EMAILTYPE	E-mail type
User Profile Type **Note:** PeopleSoft stores values corresponding to a user profile type, such as Employee ID, Customer ID, and Vendor ID in the `PSOPRALIAS.OPRALIASVALUE` target system field.	PSOPRALIAS.OPRALIASTYPE	A user profile can be attached to several user profile types, such as Employee (EMP), Customer (CST), and Vendor (VND)

1.6.2 Reconciliation Rules

The following sections provide information about the reconciliation rules for this connector:

- Section 1.6.2.1, "Overview of the Reconciliation Rule"
- Section 1.6.2.2, "Viewing the Reconciliation Rules in the Design Console"

1.6.2.1 Overview of the Reconciliation Rule

The following reconciliation rule is used for target resource reconciliation:

Rule Name: PSFT UM Target Recon Rule

Rule Element: User Login Equals User ID

In this rule:

- User Login represents the User ID field on the OIM User form.
- User ID represents the OPRID field of the user on the target system.

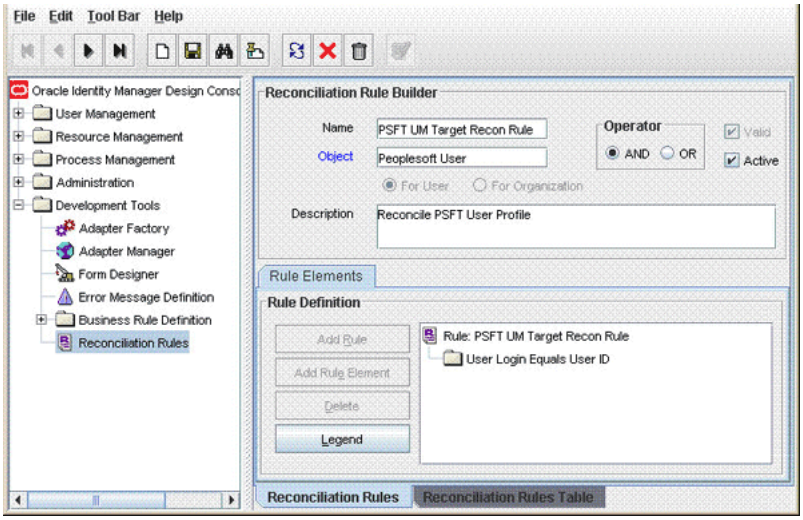
1.6.2.2 Viewing the Reconciliation Rules in the Design Console

After you deploy the connector, you can view the reconciliation rule 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 and open **PSFT UM Target Recon Rule.** Figure 1–4 shows this reconciliation rule.

Figure 1–4 Reconciliation Rule



See Also: *Oracle Identity Manager Design Console Guide* for information about modifying reconciliation rules

1.6.3 Reconciliation Action Rules

Application of the matching rule on reconciliation events would result in one of multiple possible outcomes. The action rules for reconciliation define the actions to be taken for these outcomes.

Note: For any rule condition that is not predefined for this connector, no action is performed and no error message is logged.

The following sections provide information about the reconciliation action rules for this connector:

- Section 1.6.3.1, "Overview of the Reconciliation Action Rules"
- Section 1.6.3.2, "Viewing the Reconciliation Action Rules in the Design Console"

1.6.3.1 Overview of the Reconciliation Action Rules

Table 1–4 lists the reconciliation action rules for this connector.

Table 1–4 Action Rules for Target Resource Reconciliation

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.6.3.2 Viewing the Reconciliation Action Rules in the Design Console

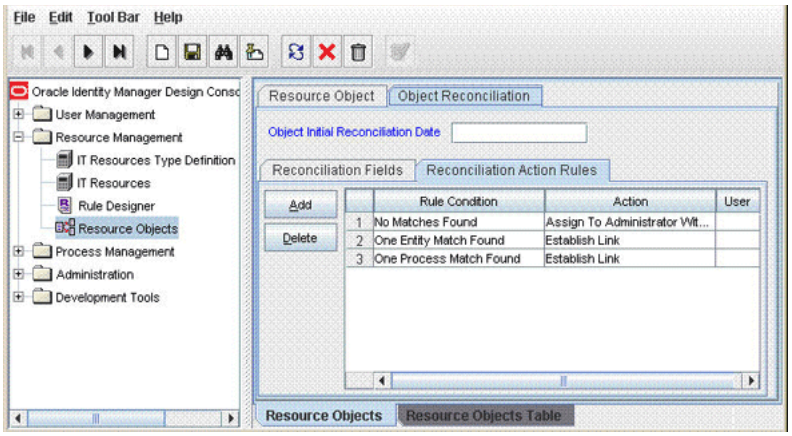
After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

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

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

   Figure 1–5 shows these reconciliation action rules.

Figure 1–5 Reconciliation Action Rules



See Also: *Oracle Identity Manager Design Console Guide* for information about modifying reconciliation action rules

1.7 Connector Objects Used During Provisioning

Provisioning involves creating, modifying, or deleting a user's account information on the target system through Oracle Identity Manager.

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

This section discusses the following topics:

- Section 1.7.1, "User Provisioning Functions"
- Section 1.7.2, "User Attributes for Provisioning"

1.7.1 User Provisioning Functions

Table 1–5 lists the supported user provisioning functions and the adapters that perform these functions. The functions listed in the table correspond to either a single or a multiple process tasks.

See Also: *Oracle Identity Manager Connector Concepts* for generic information about process tasks and adapters

Table 1–5 User Provisioning Functions Supported by the Connector

Function	Adapter
Create a user	PSFT UM Create User
Update the password of a user	PSFT UM Update Password
Update the description of a user	PSFT UM Update User
Update the multilanguage code of a user	PSFT UM UpdateUser
Update the primary e-mail address of a user	PSFT UM Update Primary Email

Table 1–5 (Cont.) User Provisioning Functions Supported by the Connector

Function	Adapter
Update the primary e-mail address type of a user	PSFT UM Update Primary Email
Update the language code of a user	PSFT UM Update User
Update the currency code of a user	PSFT UM UpdateUser
Update the Id type of a user	PSFT UM Update ID Types
Update the Primary Permission list of a user	PSFT UM UpdateUser
Update the Process Profile Permission list of a user	PSFT UM UpdateUser
Update the Navigator Home Permission list of a user	PSFT UM UpdateUser
Update the Row Security Permission list of a user	PSFT UM UpdateUser
Update the User Id alias of a user	PSFT UM UpdateUser
Add a role to a user	PSFT UM Modify User Role
Delete a role from a user	PSFT UM Modify User Role
Add an e-mail address to a user	PSFT UM Modify Email Address
Delete the e-mail address of a user	PSFT UM Modify Email Address
Unlock a user	PSFT UM Modify Lock Unlock User
Lock a user	PSFT UM Modify Lock Unlock User
Delete a user at the target system	PSFT UM Delete User
Prepopulate the User Id on the process form with the User Id of the OIM User **Note:** If the PeopleSoft Employee Reconciliation and the PeopleSoft User Management connectors are deployed on a single Oracle Identity Manager installation, then the User Id field of the OIM User is populated with the value of the Employee ID of the employee reconciled from PeopleSoft.	PSFT UM Prepopulate UserID
Prepopulate the Employee ID on the process form with the User Id of the OIM User **Note:** The Employee ID is used to link a user profile to the employee.	PSFT UM Prepopulate EmployeeID

1.7.2 User Attributes for Provisioning

Table 1–6 lists the user attributes for which you can specify or modify values during provisioning operations.

Table 1–6 User Attributes for Provisioning

OIM PeopleSoft UM Resources Process Form Field	Target System Attribute	Description	Adapter
Single-Valued Fields			
User ID	PSOPRDEFN.OPRID	Login Id of the user profile	PSFT UM Create User
User Description	PSOPRDEFN.OPRDEFNDESC	Description of the user profile	PSFT UM Create User
Employee ID	PSOPRDEFN.EMPLID	Employee Id of the employee to which the user profile is assigned	PSFT UM Create User
Symbolic ID	PSOPRDEFN.SYMBOLICID	Symbolic ID of the target system	PSFT UM Create User
Multi Language Code	PSOPRDEFN.MULTILANG	Multilanguage code	PSFT UM Create User
Language Code	PSOPRDEFN.LANGUAGE_CD	Language code	PSFT UM Create User
Currency Code	PSOPRDEFN.CURRENCY_CD	Currency code	PSFT UM Create User
User Id Alias	PSOPRDEFN.USERIDALIAS	Alias of user login Id	PSFT UM Create User
Row Security Permission List	PSOPRDEFN.ROWSECCLASS	Row security parameter	PSFT UM Create User
Process Profile Permission List	PSOPRDEFN.PRCSPRFLCLS	Process profile parameter	PSFT UM Create User
Navigator Home Permission List	PSOPRDEFN.DEFAULTNAVHP	Navigator home page address	PSFT UM Create User
Primary Permission List	PSOPRDEFN.OPRCLASS	Primary permission list	PSFT UM Create User
Primary Email Address	PSUSEREMAIL.EMAILID	E-mail address (primary e-mail account)	PSFT UM Create User
Primary Email Type	PSUSEREMAIL.EMAILTYPE	E-mail type (primary e-mail account)	PSFT UM Create User
Customer ID	PSOPRALIAS.CUST_ID	Customer ID **Note:** A user profile can be attached to several ID types, such as None (NON), Employee (EMP), Customer (CST), and Vendor (VND).	PSFT UM Create User
Customer Set ID	PSOPRALIAS.SETID	Customer's SetID	PSFT UM Create User
Vendor ID	PSOPRALIAS.VENDOR_ID	Vendor ID	PSFT UM Create User

Table 1–6 (Cont.) User Attributes for Provisioning

OIM PeopleSoft UM Resources Process Form Field	Target System Attribute	Description	Adapter
Vendor Set ID	PSOPRALIAS.SETID	Vendor's Set ID	PSFT UM Create User
Multivalued Fields			
Role Name	PSROLEUSER_VW.ROLENAME	The role name that is assigned to the user profile	PSFT UM Modify User Role
Email Address	PSUSEREMAIL.EMAILID	E-mail address (e-mail account)	PSFT UM Modify Email Address
Email Type	PSUSEREMAIL.EMAILTYPE	Email type (e-mail account)	PSFT UM Modify Email Address

Note: The name of the process form in the first column of the preceding table is UD_PSFT_BAS.

1.8 Roadmap for Deploying and Using the Connector

The following shows how information is organized in the rest of the guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform to extend the functionality of the connector.
- Chapter 5, "Testing and Troubleshooting" describes the procedure to use the connector testing utility for testing the connector.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.
- Appendix A, "Determining the Root Audit Action Details" provides information about root audit action.
- Appendix B, "Setting Up SSL on Oracle WebLogic Server" describes how to configure SSL on Oracle WebLogic Server for PeopleTools 8.50.

2

Deploying the Connector

Deploying the connector involves the following steps:

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- Section 2.1.1, "Preinstallation on Oracle Identity Manager"
- Section 2.1.2, "Preinstallation on the Target System"

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Section 2.1.1.1, "Files and Directories on the Installation Media"
- Section 2.1.1.2, "Determining the Release Number of the Connector"
- Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File"

2.1.1.1 Files and Directories on the Installation Media

Table 2–1 lists 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
configuration/Peoplesoft_User-Management-CI.xml	This XML file contains configuration information that is used during connector installation.
lib/PSFTUM.jar	This JAR file contains the class files that are specific to PeopleSoft reconciliation and provisioning. During connector deployment, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
lib/Common.jar	This JAR file contains the class files that are common to all connectors. During connector deployment, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
lib/PSFTCommon.jar	This JAR file contains PeopleSoft-specific files common to both Employee Reconciliation and User Management versions of the connector. During connector deployment, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
lib/CustomClassLoader.jar	This JAR file contains the class files that are needed to load the target system-specific JAR files at run time, for example psjoa.jar.
lib/PeopleSoftOIMListener.war lib/PeopleSoftOIMListener.ear	This Web Archive (WAR) file contains the classes and configuration files required to implement incremental reconciliation. This Enterprise Archive (EAR) file contains one or more entries representing the modules of the Web application to be deployed onto an application server. During connector deployment: ■ On Oracle Identity Manager release 9.1.0.*x*, the PeopleSoft listener is deployed as a WAR file. ■ On Oracle Identity Manager release 11.1.1, the PeopleSoft listener is deployed as an EAR file.

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

File in the Installation Media Directory	Description
The following files in the peoplecode directory: CurrencyCode.txt EmailType.txt LanguageCode.txt PermissionList.txt UserRoles.txt The following project files in the peoplecode directory: OIM_UM OIM_UM_DELETE	These files contain the PeopleCode for the steps that you define for the Application Engine program. This is explained in "Creating the Application Engine Program" on page 2-31. The project files contain the PeopleCode for the steps that you define for importing a Project from Application Designer. This is explained in Section 2.1.2.1, "Importing a Project from Application Designer." Each project file contains two files with .ini and .xml extension that has the same name as the project. They are listed as follows: ■ OIM_UM.ini ■ OIM_UM.xml ■ OIM_UM_DELETE.ini ■ OIM_UM_DELETE.xml
test/scripts/InvokeListener.bat test/scripts/InvokeListener.sh	This BAT file and the UNIX shell script call the testing utility for reconciliation.
test/scripts/PeoplesoftTestingUtility.bat test/scripts/PeoplesoftTestingUtility.sh	This BAT file and the UNIX shell script call the testing utility for provisioning.
test/config/reconConfig.properties test/config/log.properties	These files are used by theInvokeListener.bat file. The reconConfig.properties file contains configuration information for running the InvokeListener.bat file. The log.properties file contains logger information.
test/config/config.properties	This file is used to specify the parameters and settings required to connect, create, update, and delete users in the target system by using the testing utility for provisioning.

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

File in the Installation Media Directory	Description
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/ConnectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
xml/PeoplesoftUserManagement-ConnectorConfig.xml	This XML file contains definitions for the connector components: ■ IT resource type ■ Scheduled tasks ■ IT resource ■ Resource objects (This file contains the configurations of the resource objects for the target resource.) ■ Process definition ■ Process tasks ■ Adapters ■ Process form
JavaDoc	This directory contains information about the Java APIs used by the connector.

2.1.1.2 Determining the Release Number of the Connector

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

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

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

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

   OIM_HOME/xellerate/JavaTasks/PSFTUM.jar

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

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

2.1.1.3 Creating a Backup of the Existing Common.jar File

The Common.jar file is in the deployment package of each 9.1.*x* release of the connector. With each new release, code corresponding to that particular release is

added to the existing code in this file. For example, the Common.jar file shipped with Connector Y on 12-July contains:

- Code specific to Connector Y
- Code included in the Common.jar files shipped with all other 9.1.*x* release of the connectors that were released before 12-July

If you have installed a release 9.1.*x* connector that was released after the current release of the PeopleSoft User Management connector, back up the existing Common.jar file, install the PeopleSoft User Management connector, and then restore the Common.jar file. The steps to perform this procedure are as follows:

Caution: If you do not perform this procedure, then your release 9.1.*x* connectors might not work.

1. Determine the release date of your existing release 9.1.*x* connector as follows:
   a. Extract the contents of the following file in a temporary directory:

      OIM_HOME/xellerate/JavaTasks/Common.jar

      Note: On Oracle Identity Manager release 11.1.1, use either DownloadJars.sh or DownloadJars.bat to download the common.jar file from the database, and then extract the contents of this file into a temporary directory. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for instructions about using the Download JARs utility.

   b. Open the Manifest.mf file in a text editor.
   c. Note down the Build Date and Build Version values.
2. Determine the Build Date and Build Version values of the current release of the PeopleSoft User Management connector as follows:
   a. On the installation media for the connector, extract the contents of the lib/Common.jar and then open the Manifest.mf file in a text editor.
   b. Note down the Build Date and Build Version values.
3. If the Build Date and Build Version values for the PeopleSoft User Management connector are less than the Build Date and Build Version values for the connector that is installed, then:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. Copy the *OIM_HOME*/xellerate/JavaTasks/Common.jar to a temporary location.
     b. After you perform the procedure described in Section 2.2, "Installation" overwrite the new Common.jar file in the *OIM_HOME*/xellerate/JavaTasks directory with the Common.jar file that you backed up in the preceding step.
   - If you are using Oracle Identity Manager release 11.1.1, then run the Oracle Identity Manager Upload JARs utility to post the Common.jar file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

Note: Before you use the 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.

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility

2.1.2 Preinstallation on the Target System

Permission lists, roles, and user profiles are building blocks of PeopleSoft security. Each user of the system has an individual user profile, which in turn is linked to one or more roles. To each role, you can add one or more permission lists, which defines what a user can access. So, a user inherits permissions through the role that is attached to a user profile.

You must create limited rights users who have restricted rights to access resources in the production environment to perform PeopleSoft-specific installation or maintenance operations. A limited rights user has the privilege to invoke PeopleSoft User Profile Component Interface Java APIs for provisioning.

The preinstallation steps consist of creating a user account with limited rights. Permission lists may contain any number of accesses, such as the Web libraries permission, Web services permissions, page permissions, and so on. You attach this permission list to a role, which in turn is linked to a user profile.

This section describes the following procedures, which have to be performed on the target system to create a user account with limited rights:

- Section 2.1.2.1, "Importing a Project from Application Designer"
- Section 2.1.2.2, "Creating a Target System User Account for Connector Operations"

2.1.2.1 Importing a Project from Application Designer

A PeopleSoft Application Designer project is an efficient way to configure your application.

You can import the OIM_UM project created in Application Designer to automate the steps for creating a permission list. You can also create a permission list by manually performing the steps described in Section 2.1.2.2.1, "Creating a Permission List." If you import the OIM_UM project, then you need not perform the steps mentioned in this section. You must perform a separate set of instructions for creating an Application Engine program if you have imported the project. See "Creating the Application Engine Program" on page 2-31 for details.

Note: If you install, uninstall, or upgrade the same project repeatedly, the earlier project definition will be overwritten in the database.

To import a project from Application Designer:

Note: You can access the project files from the following directory:

For Oracle Identity Manager release 9.1.0.*x*:

OIM_HOME/xellerate/XLIntegrations/PSFTUM/peoplecode/OIM_UM

OIM_HOME/xellerate/XLIntegrations/PSFTUM/peoplecode/OIM_UM_DELETE

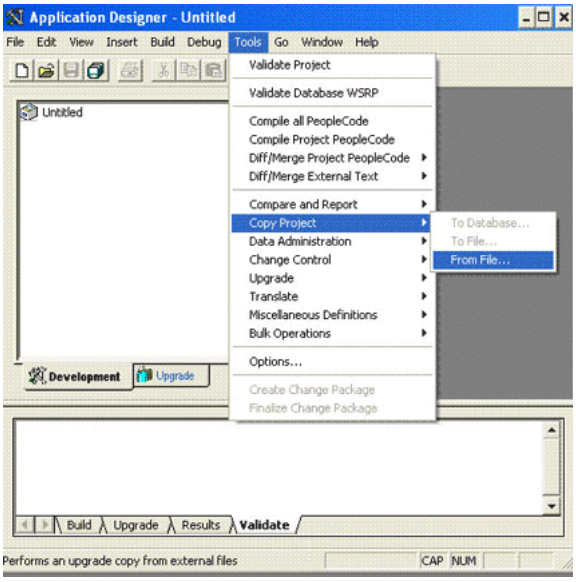
For Oracle Identity Manager release 11.1.1:

OIM_HOME/server/XLIntegrations/PSFTUM/peoplecode/OIM_UM

OIM_HOME/server/XLIntegrations/PSFTUM/peoplecode/OIM_UM_DELETE

Copy these files to a directory on your computer from where you can access Application Designer.

1. To open Application Designer in 2-tier mode, click **Start, Programs, Peoplesoft8.x,** and then **Application Designer.**
2. From the **Tools** menu, click **Copy Project** and then **From File.**



The Copy From File : Select Project dialog box appears.

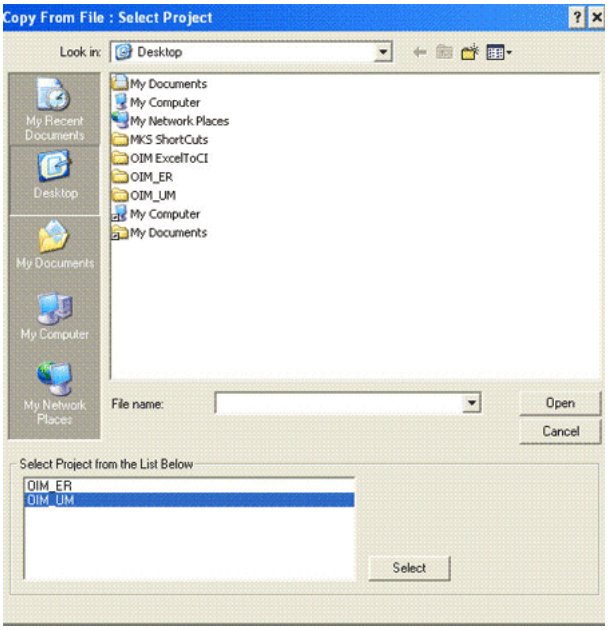
3. Navigate to the directory in which the PeopleSoft project file is placed.

   The project files are present in the `/peoplecode` directory of the installation media. Place these files in a new folder so that is accessible by the Application

Designer program. Ensure that the folder name is the same as that of the project you are importing.

For example, place the OIM_UM.ini and OIM_UM.xml in OIM_UM folder.

4. Select the project from the **Select Project from the List Below** region. The name of the project file is **OIM_UM.**



5. Click **Select.**
6. Click **Copy.**

Note: You can remove the PeopleSoft project file and all its objects from the target system if needed. To do so, repeat the steps described in the preceding procedure. When you reach Step 4, select **OIM_UM_DELETE** from the **Select Project from the List Below** region.

2.1.2.2 Creating a Target System User Account for Connector Operations

You must create a target system account with privileges required for connector operations. The user account created on the target system has the permission to perform all the configurations required for connector operations. This includes configuring the PeopleSoft Integration Broker for full reconciliation and incremental reconciliation. This account does not have access to pages or components that are not required by the connector.

The following section describes the procedures to create a target system account:

Note: For creating the target system account, you must log in to PeopleSoft Internet Architecture with administrator credentials.

- Section 2.1.2.2.1, "Creating a Permission List"
- Section 2.1.2.2.2, "Creating a Role for a Limited Rights User"

- Section 2.1.2.2.3, "Assigning the Required Privileges to the Target System Account"

2.1.2.2.1 Creating a Permission List

To create a permission list:

> **Note:** You can skip this section if you have imported a project from Application Designer. See Section 2.1.2.1, "Importing a Project from Application Designer" for more information.

1. Open a Web browser and enter the URL for PeopleSoft Internet Architecture. The URL is in the following format:

   `http://IPADDRESS:PORT/psp/ps/?cmd=login`

   For example:

   `http://172.21.109.69:9080/psp/ps/?cmd=login`

2. In the PeopleSoft Internet Architecture window, click **PeopleTools, Security, Permissions & Roles,** and then click **Permission Lists.**
3. Click **Add a new Value.** On the Add a New Value tab, enter the permission list name, for example, `OIMUM` and then click **Add.**
4. On the General tab, enter a description for the permission list in the **Description** field.
5. On the Component Interfaces tab, click the search icon for the **Name** field and perform the following:
   a. In the Name lookup, enter `USER_PROFILE` and then click **Lookup.** From the list, select **USER_PROFILE.** The application returns to the Component Interfaces tab. Click **Edit.**
   b. On the Component Interface Permissions page, click **Full Access(All).**
   c. Click **OK** and then click **Save.**
   d. Click the plus sign (+) to add a row for the **Name** field and repeat Steps a through c for the DELETE_USER_PROFILE component interface.
6. On the Pages tab, click the search icon for Menu Name and perform the following:
   a. In the Menu Name lookup, enter `APPLICATION_ENGINE` and then click **Lookup.** From the list, select **APPLICATION_ENGINE.** The application returns to the Pages tab. Click **Edit Components.**
   b. On the Component Permissions page, click **Edit Pages** for the AE_REQUEST component name.
   c. Click **Select All,** and then click **OK.** Click **OK** on the Components Permissions page.
   d. On the Pages tab, click the plus sign (+) to add a row for **Menu Name.** Click the search icon for Menu Name. In the Menu Name lookup, enter `IB_PROFILE` and then click **Lookup.** From the list, select **IB_PROFILE.** The application returns to the Pages tab. Click **Edit Components.**
   e. On the Component Permissions page, click **Edit Pages** for each of the following component names:

      IB_GATEWAY

IB_MESSAGE_BUILDER

IB_MONITOR_QUEUES

IB_NODE

IB_OPERATION

IB_QUEUEDEFN

IB_ROUTINGDEFN

IB_SERVICE

IB_SERVICEDEFN

IB_MONITOR

f. Click **Select All,** and then click **OK** for each of the components. Click **OK** on the Components Permissions page.

g. On the Pages tab, click the plus sign (+) to add another row for **Menu Name.**

h. In the Menu Name lookup, enter `PROCESSMONITOR` and then click **Lookup.** From the list, select **PROCESSMONITOR.** The application returns to the Pages tab. Click **Edit Components.**

i. On the Component Permissions page, click **Edit Pages** for the PROCESSMONITOR component name.

j. Click **Select All,** and then click **OK.** Click **OK** on the Components Permissions page.

k. On the Pages tab, click the plus sign (+) to add another row for **Menu Name.**

l. In the Menu Name lookup, enter `PROCESS_SCHEDULER` and then click **Lookup.** From the list, select **PROCESS_SCHEDULER.** The application returns to the Pages tab. Click **Edit Components.**

m. On the Component Permissions page, click **Edit Pages** for the PRCSDEFN component name.

n. Click **Select All,** and then click **OK.** Click **OK** on the Components Permissions page.

7. On the People Tools tab, select the **Application Designer Access** check box and click the **Definition Permissions** link. The Definition Permissions page is displayed.

8. On this page, grant full access to the following object types by selecting **Full Access** from the Access list:

   - App Engine Program
   - Message
   - Component Interface
   - Project
   - Application Package

9. Click **OK.**

10. Click the **Tools Permissions** link. The Tools Permissions page is displayed. On this page, grant full access to the SQL Editor tool by selecting **Full Access** from the Access list.

11. Click **OK.** The application returns to the People Tools tab.

12. On the Web Libraries tab, click the search icon for the Web Library Name field and perform the following:
    a. In the Web Library Name lookup, enter `WEBLIB_PORTAL` and then click **Lookup.** From the list, select **WEBLIB_PORTAL.** The application returns to the Web Libraries tab. Click the **Edit** link.
    b. On the WebLib Permissions page, click **Full Access(All).**
    c. Click **OK** and then click **Save.**
    d. Click the plus sign (+) to add a row for the **Web Library Name** field and repeat Steps a through c for the WEBLIB_PT_NAV library.
    e. Click **Save** to save all the settings specified for the permission list.
13. On the Process tab, click the **Process Group Permissions** link. The Process Group Permission page is displayed.
14. In the Process Group lookup, click the search icon. From the list, select **TLSALL.** The application returns to the Process Group Permission page.
15. Click the plus sign (+) to add another row for **Process Group.**
16. In the Process Group lookup, click the search icon. From the list, select **STALL.** The application returns to the Process Group Permission page.
17. Click **OK.**
18. Click **Save.**

2.1.2.2.2 Creating a Role for a Limited Rights User

To create a role for a limited rights user:

1. Open a Web browser and enter the URL for PeopleSoft Internet Architecture. The URL is in the following format:

   `http://`*`IPADDRESS:PORT`*`/psp/ps/?cmd=login`

   For example:

   `http://172.21.109.69:9080/psp/ps/?cmd=login`

2. In the PeopleSoft Internet Architecture window, click **PeopleTools, Security, Permissions & Roles,** and then click **Roles.**
3. Click **Add a new Value.** On the Add a New Value tab, enter the role name, for example, `OIMUM`, and then click **Add.**
4. On the General tab, enter a description for the role in the **Description** field.
5. On the Permission Lists tab, click the search icon and perform the following:
    a. In the Permission Lists lookup, enter `OIMUM` and then click **Lookup.** From the list, select **OIMUM.**
    b. Click the plus sign (+) to add another row.
    c. In the Permission Lists lookup, enter `EOEI9000` and then click **Lookup.** From the list, select **EOEI9000.**
    d. Click the plus sign (+) to add another row.
    e. In the Permission Lists lookup, enter `EOCO9000` and then click **Lookup.** From the list, select **EOCO9000.**
    f. Click **Save.**

2.1.2.2.3 Assigning the Required Privileges to the Target System Account

To assign the required privileges to a user:

1. Open a Web browser and enter the URL for PeopleSoft Internet Architecture. The URL is in the following format:

   `http://IPADDRESS:PORT/psp/ps/?cmd=login`

   For example:

   `http://172.21.109.69:9080/psp/ps/?cmd=login`

2. In the PeopleSoft Internet Architecture window, click **PeopleTools, Security, User Profiles,** and then click **User Profiles.**
3. Click **Add a new Value.** On the Add a New Value tab, enter the user profile name, for example, `OIMUM`, and then click **Add.**
4. On the General tab, perform the following:
   a. From the Symbolic ID list, select the value that is displayed, for example, SYSADM1.
   b. Enter valid values for the **Password** and **Confirm Password** fields.
   c. Click the search icon for the Process Profile permission list.
   d. In the Process Profile lookup, enter `OIMUM` and then click **Lookup.** From the list, select **OIMUM.** The application returns to the General tab.
5. On the ID tab, select **none** as the value of the ID type.
6. On the Roles tab, click the search icon and perform the following:
   a. In the Roles lookup, enter `OIMUM` and then click **Lookup.** From the list, select **OIMUM.**
   b. Click the plus sign (+) to add another row.
   c. In the Roles lookup, enter `ProcessSchedulerAdmin` and then click **Lookup.** From the list, select **ProcessSchedulerAdmin.**
   d. Click the plus sign (+) to add another row.
   e. In the Roles lookup, enter `EIR Administrator` and then click **Lookup.** From the list, select **EIR Administrator.**
   f. Click **Save** to save this user profile.

      Oracle Identity Manager uses this profile for the **Admin** user parameter in IT resource to enable the connector to perform provisioning operations. This profile is also used for a user with limited rights in PeopleSoft for performing all reconciliation-related configurations.

2.2 Installation

Installation information is divided across the following sections:

- Section 2.2.1, "Installation on Oracle Identity Manager"
- Section 2.2.2, "Installation on the Target System"

2.2.1 Installation on Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

2.2.1.1 Running the Connector Installer

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

Direct provisioning is automatically enabled after you run the Connector Installer. If required, you can enable request-based provisioning in the connector. Direct provisioning is automatically disabled when you enable request-based provisioning. See Section 2.3.1.9, "Enabling Request-Based Provisioning" if you want to use the request-based provisioning feature for this target system.

To run the Connector Installer:

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

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

   - For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/ConnectorDefaultDirectory
   - For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/ConnectorDefaultDirectory
2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console Guide*.
3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.*x*:

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

     On the Welcome to Identity Manager Advanced Administration page, under the System Management section, click **Install Connector**.
4. From the Connector List list, select **PeopleSoft User Management 9.1.1**. 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 **PeopleSoft User Management 9.1.1**.

5. Click **Load**.

6. To start the installation process, click **Continue**.

   The following tasks are performed, in sequence:

   a. Configuration of connector libraries

   b. Import of the connector XML files (by using the Deployment Manager)

   c. Compilation of adapters

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

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of steps that you must perform after the installation is displayed. These steps are as follows:

   Note: At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.1.1, "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.

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

   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

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

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

Table 2–2 Files Copied to Oracle Identity Manager

File in the Installation Media Directory	Destination for Oracle Identity Manager Release 9.1.0.x	Destination for Oracle Identity Manager Release 11.1.1
lib/Common.jar	*OIM_HOME*/xellerate/JavaTasks	Oracle Identity Manager database
lib/PSFTCommon.jar	*OIM_HOME*/xellerate/JavaTasks	Oracle Identity Manager database
lib/PSFTUM.jar	*OIM_HOME*/xellerate/JavaTasks	Oracle Identity Manager database
lib/CustomClassLoader.jar	*OIM_HOME*/xellerate/JavaTasks	Oracle Identity Manager database
lib/PesopleSoftOIMListener.war lib/PesopleSoftOIMListener.ear	To be deployed on the application server To deploy the application on Oracle Identity Manager release 9.1.0.*x*, see Section 2.2.1.5.1, "Deploying the PeopleSoft Listener on Oracle Identity Manager Release 9.1.0.x."	To be deployed on the application server To deploy the application on Oracle Identity Manager release 11.1.1, see Section 2.2.1.5.2, "Deploying the PeopleSoft Listener on Oracle Identity Manager Release 11.1.1."

Installing the Connector in an Oracle Identity Manager Cluster

While installing the connector in a cluster, you must copy all the JAR files and the contents of the resources directory into the destination directories on each node of the cluster. Then, restart each node. See Section 2.1.1.2, "Determining the Release Number of the Connector" for information about the files that you must copy and their destination locations on the Oracle Identity Manager host computer.

Restoring the Common.jar File

If required, restore the Common.jar file that you had backed up by following the procedure described in Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File."

2.2.1.2 Copying the Connector Files and External Code Files

Table 2–3 lists all the files that you must copy manually and the directories on the Oracle Identity Manager host computer to which you must copy them.

Note:

- While installing Oracle Identity Manager in a cluster, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the contents of the connectorResources directory and the JAR files to the corresponding directories on each node of the cluster.
- The directory paths given in the first column of this table correspond to the location of the connector files on the installation media. See Section 2.1.1.1, "Files and Directories on the Installation Media" for more information about these files.
- If a particular destination directory does not exist on the Oracle Identity Manager host computer, then create it.

Table 2–3 Files to Be Copied to the Oracle Identity Manager Host Computer

File in the Installation Media Directory	Destination for Oracle Identity Manager Release 9.1.0.*x*	Destination for Oracle Identity Manager Release 11.1.1
lib/PeopleSoftOIMListener.war lib/PeopleSoftOIMListener.ear	*OIM_HOME*/xellerate/XLIntegrations/PSFTUM/WAR	*OIM_HOME*/server/XLIntegrations/PSFTUM/EAR
Files in the peoplecode directory	*OIM_HOME*/xellerate/XLIntegrations/PSFTUM/peoplecode	*OIM_HOME*/server/XLIntegrations/PSFTUM/peoplecode
Files in the test/scripts directory	*OIM_HOME*/xellerate/XLIntegrations/PSFTUM/scripts	*OIM_HOME*/server/XLIntegrations/PSFTUM/scripts
Files in the test/config directory	*OIM_HOME*/xellerate/XLIntegrations/PSFTUM/config	*OIM_HOME*/server/XLIntegrations/PSFTUM/config

After you copy the connector files, copy the following files from the *PEOPLESOFT_HOME*/web/psjoa directory on the target system computer into the *OIM_HOME*/xellerate/ThirdParty directory.

Note: These files should be copied only if one version of the target system is supported, and the Multiple Version Support parameter in Lookup.PSFT.Configuration is set to `No`.

- psjoa.jar

  This JAR file contains the compiled Java classes required by Oracle Identity Manager to remotely connect to the target system.

- peoplesoft.jar

  This JAR file contains APIs for the USER_PROFILE and DELETE_USER_PROFILE component interfaces.

  The Section 2.2.2.4, "Configuring the Target System for Provisioning" provides information about the procedure to generate this file for the specific release of PeopleTools (8.49) that you are using.

Note: The supported JDK and JRE versions are linked to the PeopleTools version you are using. For PeopleTools 8.49, the supported JDK version is 1.5.0.

2.2.1.3 Configuring the IT Resource

The IT resource for the target system contains connection information about the target system. Oracle Identity Manager uses this information during provisioning and reconciliation.

When you run the Connector Installer, the `PSFT Server` IT resource is automatically created in Oracle Identity Manager. You must specify values for the parameters of this IT resource as follows:

1. Log in to the Administrative and User Console.
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource.**

- If you are using Oracle Identity Manager release 11.1.1, then:
  a. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced.**
  b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the **Configuration** region, click **Manage IT Resource.**

3. In the IT Resource Name field on the Manage IT Resource page, enter `PSFT UM Server` and then click **Search.**
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters.**
6. Specify values for the parameters of the IT resource. Table 2–4 describes each parameter.

Table 2–4 IT Resource Parameters

Parameter	Description
Admin	Enter the user name of the target system account to be used for connector operations. You create this account by performing the procedure described in the Section 2.1.2.2, "Creating a Target System User Account for Connector Operations" section. Sample value: `PS`
AdminCredentials	Enter the password of the target system account specified by the Admin ID parameter.
Configuration Lookup	This parameter holds the name of the lookup definition that contains configuration information. Default value: `Lookup.PSFT.Configuration` **Note:** You must not change the value of this parameter. However, if you create a copy of all the connector objects, then you can specify the unique name of the copy of this lookup definition as the value of the Configuration Lookup Name parameter in the copy of the IT resource.
IsActive	This parameter is used to specify whether the specified IT Resource is in use or not. When `Yes`, the message from PeopleSoft is validated against this parameter apart from the IT Resource name. If it is `No`, then the message from the PeopleSoft target is rejected and is not parsed. Default value: `Yes`
JAR File Location	Location of JAR files to support multiple PeopleSoft versions. Sample value: `C:\psft849Jars` **Note:** The connector reads the value of this attribute when the **Multiple Version Support** parameter in the Lookup.PSFT.Configuration lookup definition is set to `Yes`. See Section 2.2.1.4, "Configuring the Connector to Support Multiple Versions of the Target System" for more information.

Table 2–4 (Cont.) IT Resource Parameters

Parameter	Description
Jolt URL	URL of the computer hosting the PeopleSoft application server. Format: *TARGET COMPUTER IPADDRESS or HOSTNAME:PORT* Sample value: `172.21.109.65:9070` See "Determining the Jolt Listener Port" on page 2-19 for instructions to locate the Jolt Listener port. **Note:** If you have implemented high availability for PeopleSoft Application Servers, then you need not perform any additional step on Oracle Identity Manager for provisioning to work. You have to provide the correct Jolt URL according to your high availability set up for PeopleSoft Application Servers. For more information about high availability, see *Red Paper on Clustering and High Availability for Enterprise Tools 8.4x* on Oracle Support and *Working with Jolt Configuration Options* in the PeopleBook *Enterprise PeopleTools 8.49 PeopleBook: System and Server Administration*.
TopologyName	If you have installed the OAACG SIL provider, then enter `oaacgpsft`. Default value: `None` See Section 2.3.1.8.2, "Specifying a Value for the TopologyName IT Resource Parameter" for more information.
Connection Pooling Parameters	
Abandoned connection timeout	Time (in seconds) after which a connection must be automatically closed if it is not returned to the pool **Note:** You must set this parameter to a value that is high enough to accommodate processes that take a long time to complete (for example, full reconciliation). Default value: `600`
Connection wait timeout	Maximum time (in seconds) for which the connector must wait for a connection to be available Default value: `60`
DelayBetweenRetries	Use this parameter to specify the time difference between consecutive retries (in milliseconds). Default value: `20000`
Inactive connection timeout	Time (in seconds) of inactivity after which a connection must be dropped and replaced by a new connection in the pool Default value: `600`
Initial pool size	Number of connections that must be established when the connection pool is initialized The pool is initialized when it receives the first connection request from a connector. Default value: `1` Sample value: `3`
Max pool size	Maximum number of connections that must be established in the pool at any point of time This number includes the connections that have been borrowed from the pool. Default value: 100 Sample value: `30`

Table 2–4 (Cont.) IT Resource Parameters

Parameter	Description
Min pool size	Minimum number of connections that must be in the pool at any point of time This number includes the connections that have been borrowed from the pool. Default value: `5`
Validate connection on borrow	Specifies whether a connection must be validated before it is lent by the pool The value can be `true` or `false`. It is recommended that you set the value to `true`. Default value: `true`
Timeout check interval	Time interval (in seconds) at which the timeouts specified by the other parameters must be checked Default value: `30`
Pool preference	Preferred connection pooling implementation Value: `Default` **Note:** Do not change the value of this parameter.
Connection pooling supported	Enter `true` to enable connection pooling for this target system installation. Otherwise, enter `False`. Default value: `False`
Target supports only one connection	Indicates whether the target system can support one or more connections at a time Value: `false` **Note:** Do not change the value of this parameter.
ResourceConnection class definition	Implementation of the ResourceConnection class Default value: `oracle.iam.connectors.psft.usermgmt.integration.PSFTResourceConnectionImpl` **Note:** Do not change the value of this parameter.
Native connection pool class definition	Wrapper to the native pool mechanism that implements the GenericPool **Note:** Do not specify a value for this parameter.
NumberOfRetries	Use this parameter to specify the number of times Oracle Identity Manager must try connecting to the target system. Default value: `2` **Note:** The timeout feature is enabled only for full reconciliation.
Pool excluded fields	Comma-separated list of IT parameters whose change should not trigger a refresh of the connector pool Default value: `Is Active,Configuration Lookup` **Note:** You must not change the value of this parameter.

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

Determining the Jolt Listener Port

You can obtain the Jolt Listener port number from the PeopleSoft Application Server configuration file, psappsrv.cfg.

To locate the Jolt Listener Port:

1. Log in to the computer where you have deployed the Application Server.

2. Navigate to the folder where you have deployed PeopleTools, for example, the PT8.49 folder for PeopleTools 8.49.
3. Navigate to the appserv folder.
4. Navigate to the folder that corresponds to the name of your application server.
5. Open the psappsrv.cfg file using WordPad.

   The following is an example location for the file:

   ```
   C:\PT8.49\appserv\HR8DMO\psappsrv.cfg
   ```

   Note: You must not modify the contents of the file.

6. Search for the following text in the file:

   ```
   [JOLT Listener]
   ;============================================================================
   ; Settings for JOLT Listener
   ;============================================================================
   ```

   Search for the string Port. This provides you the value for the Jolt Listener port.

2.2.1.4 Configuring the Connector to Support Multiple Versions of the Target System

You might want to configure the connector for different versions of the target system simultaneously. For example, you can use the connector to perform provisioning operations on both PeopleTools 8.48 and PeopleTools 8.49 simultaneously. The following example illustrates this requirement:

To meet the requirement posed by such a scenario:

The London and New York offices of Example Multinational Inc. have their own installations of the target system. The London office has PeopleTools 8.48 installation, while the New York office has PeopleTools 8.49 installation. You have to provision resources on both installations of PeopleTools simultaneously.

Now, with this release, you can configure a single version of the connector to simultaneously provision the resources on both the versions of the target system. The connector uses a class loading mechanism, which toggles between the different versions of the installation. You only need to place the target system-specific JAR files on the computer that hosts Oracle Identity Manager.

To configure the connector to support multiple versions of the target system:

1. Copy lib/PSFTUM.jar in a temporary directory, and extract the following class from the JAR file:

   `PSFTUMUserProxyProvisonManager.class`

   Sample temporary directory: `c:\temp`

2. Run the following command to extract the class file from the JAR file:

   ```
   jar -xvf PSFTUM.jar
   ```

Note: You can also run the WinZip or WinRAR utility to extract the contents from the JAR file.

3. Copy PSFTUMUserProxyProvisonManager.class to another location.

   For example:

   c:\temp1\oracle\iam\connectors\psft\usermgmt\integration

4. Create a new JAR file, PeopleSoftProxy.jar that contains the extracted PSFTUMUserProxyProvisonManager.class file present in the directory defined in Step 3 as follows:

   a. Open the command prompt and navigate to the following directory:

      `c:\temp1`

   b. Run the following command:

      ```
      Jar -cvf PeopleSoftProxy.jar oracle .
      ```

5. Create a new JAR file, PSFTUM.jar, which contains the manifest file as follows:

   a. Open the command prompt and navigate to the following directory:

      `c:\temp`

   b. Run the following command:

      ```
      jar -cMvf PSFTUM.jar manifest-inclusion-file ./META-INF/MANIFEST.MF
      ./oracle
      ```

      Note: You must ensure that the PSFTUM.jar file does not contain the PSFTUMUserProxyProvisonManager.class file.

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

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then copy the PSFTUM.jar file to *OIM_HOME*/xellerate/JavaTasks.
   - If you are using Oracle Identity Manager release 11.1.1, then run the Upload JARs utility to post the Common.jar file to the Oracle Identity Manager database. This utility is copied to 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.

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility

7. Create a directory, for example PSFT849, which is accessible from Oracle Identity Manager.

   Note: Ensure that the directory resides outside the Oracle Identity Manager classpath. In other words, the directory should be created outside the Oracle Identity Manager installation directory.

8. Copy the following JAR files in the directory created in Step 5:
   - PeopleSoftProxy.jar
   - lib/common.jar
   - lib/PSFTCommon.jar
   - psjoa.jar (target specific)
   - peoplesoft.jar (target specific)
9. Provide the full path of the directory created in Step 5 in the IT resource attribute, **Jar File Location,** of the ITResource instance for PeopleSoft 8.49.

   Repeat the preceding procedure for the other version of the target system, PeopleSoft 8.48 with the following information:
   - When you reach Step 5, create a directory with the following name: PSFT848.
   - You can reuse the PeopleSoftProxy.jar, lib/common.jar, and lib/PSFTCommon.jar files. In addition, copy the target-specific psjoa.jar and peoplesoft.jar files in the directory created in Step 5.

     Note:
     - Each target system directory should contain the same version of the following JAR files:
       - PeopleSoftProxy.jar
       - common.jar
       - PSFTCommon.jar
     - For validation and transformation in case of multiple versions of the target system, you must not put these jar files in the java task, but you must place them in the jar location provided in IT resource.
10. Set the **Multiple Version Support** parameter in the Lookup.PSFT.Configuration lookup definition to **Yes.**

Note: Ensure that the following JAR files are not present in *OIM_HOME*/xellerate/ThirdParty for Oracle Identity Manager release 9.1.0.*x* and *OIM_HOME*/server/ThirdParty for Oracle Identity Manager release 11.1.1 or in any other directory inside the Oracle Identity Manager installation directory:

- psjoa.jar
- peoplesoft.jar

2.2.1.5 Deploying the PeopleSoft Listener

The PeopleSoft listener is a Web application that is deployed on an Oracle Identity Manager host computer. The PeopleSoft listener parses the XML message and creates a reconciliation event in Oracle Identity Manager.

This section is classified based on the Oracle Identity Manager releases. Perform the procedure described in one of the following sections:

- Section 2.2.1.5.1, "Deploying the PeopleSoft Listener on Oracle Identity Manager Release 9.1.0.x"
- Section 2.2.1.5.2, "Deploying the PeopleSoft Listener on Oracle Identity Manager Release 11.1.1"

2.2.1.5.1 Deploying the PeopleSoft Listener on Oracle Identity Manager Release 9.1.0.*x*

To deploy the PeopleSoft listener on Oracle Identity Manager release 9.1.0.*x*:

1. Copy the *OIM_HOME*/xellerate/XLIntegrations/PSFTUM/WAR/PeopleSoftOIMListener.war file into a temporary folder. Enter the following command to extract the contents of the PeopleSoftOIMListener.war file.

   ```
   jar -xvf PeopleSoftOIMListener.war
   ```

   Note: All the files mentioned in the remaining steps of this procedure are extracted from the PeopleSoftOIMListener.war file.

2. Copy the following files from the *OIM_HOME*/xellerate/lib directory to the WEB-INF/lib directory in the temporary folder:

   Note:

   - Before you copy these files from the *OIM_HOME*/xellerate/lib directory, check whether these files exist in the WEB-INF/lib directory of the temporary folder. If these files exist, then first delete them from the WEB-INF/lib directory.
   - If the lib folder does not exist in WEB-INF directory, then you must create it.

   - xlAPI.jar
   - xlAuthentication.jar
   - xlCache.jar

- xlCrypto.jar
- xlLogger.jar
- xlVO.jar
- xlDataObjectBeans.jar (For IBM WebSphere Application Server, copy this file from the *OIM_CLIENT*/xlclient/lib directory.)
- xlUtils.jar (For Oracle Application Server)

3. Copy Common.jar from the /lib directory on the installation media to the WEB-INF/lib directory in the temporary folder.
4. Edit the web.xml file as follows:
   a. Locate the **Login Name of the OIM Admin User** details.

      ```
      <param-value>OIM_ADMIN_USER</param-value>
      ```

      Replace OIM_ADMIN_USER with the Oracle Identity Manager administrator credentials.

      For example, if the administrative account on Oracle Identity Manager is xelsysadm, then update the line as follows:

      ```
      <param-value>xelsysadm</param-value>
      ```

   b. Locate the **XL Home Dir** details, and replace *OIM_HOME* with the Oracle Identity Manager Home location.

   c. Locate the **java security policy** details.

      ```
      <param-name>java.security.policy</param-name>
      <param-value>OIM_HOME/config/xl.policy</param-value>
      ```

      Here, java.security.policy property is used to specify the fully qualified file name of the policy file. Typically, this file is located in the *OIM_HOME*/designconsole/config directory.

      Replace OIM_HOME with the path to the design console directory as specified in Step 4 b.

      ```
      <param-value>E:/OIM11g_Installations/MAY1202010/Middleware/OIM_HOME/designc
      onsole/config/xl.policy</param-value>
      ```

   d. Locate the **java security login config** details.

      ```
      <param-name>java.security.auth.login.config</param-name>
      <param-value>OIM_HOME/xellerate/config/auth(ws/wl/oc4j).conf</param-value>
      ```

      Here, the java.security.auth.login.config property is used to specify the fully qualified file name of the authentication configuration file. Typically, this file is located in the *OIM_HOME*/xellerate/config directory.

      Each application server uses a different authentication configuration file:

      IBM WebSphere Application Server: authws.conf

      JBoss Application Server: auth.conf

      Oracle WebLogic Server: authwl.conf

      Oracle Application Server: authoc4j.conf

      You must edit the **auth(ws/wl/oc4j).conf** value in the preceding line to the application server-specific configuration file.

e. Locate the **Message Handler Impl classes** details.

```
<param-name>IT_RESOURCE_NAME</param-name>
```

Replace IT_RESOURCE_NAME with the name of the IT resource.

For example, if the name of the IT resource is PSFT Server, then update the line as follows:

```
<param-name>PSFT Server</param-name>
```

f. Locate the following line:

```
<param-value>MESSAGE~IMPLEMENTATION_CLASS;MESSAGE~IMPLEMENTATION_CLASS;MESS
AGE~IMPLEMENTATION_CLASS</param-value>
```

In this format, the message name and its implementation class must be separated by a tilde (~). For multiple messages, each pair must be separated by a semicolon (;). For default implementation, you must modify the line as follows:

```
<param-value>PERSON_BASIC_SYNC~oracle.iam.connectors.psft.common.handler.im
pl.PSFTPersonSyncReconMessageHandlerImpl;USER_PROFILE~oracle.iam.connectors
.psft.common.handler.impl.PSFTUserProfileReconMessageHandlerImpl;WORKFORCE_
SYNC~oracle.iam.connectors.psft.common.handler.impl.PSFTWorkForceSyncReconM
essageHandlerImpl;DELETE_USER_PROFILE~oracle.iam.connectors.psft.common.han
dler.impl.PSFTDeleteUserReconMessageHandlerImpl</param-value>
```

If PeopleSoft is sending the USER_PROFILE.VERSION_84 message instead of USER_PROFILE, then modify the line as follows:

```
<param-value>PERSON_BASIC_SYNC~oracle.iam.connectors.psft.common.handler.im
pl.PSFTPersonSyncReconMessageHandlerImpl;USER_PROFILE.VERSION_84~oracle.iam
.connectors.psft.common.handler.impl.PSFTUserProfileReconMessageHandlerImpl
;WORKFORCE_SYNC~oracle.iam.connectors.psft.common.handler.impl.PSFTWorkForc
eSyncReconMessageHandlerImpl;DELETE_USER_PROFILE~oracle.iam.connectors.psft
.common.handler.impl.PSFTDeleteUserReconMessageHandlerImpl</param-value>
```

g. Locate the **java provider** details.

```
<param-name>java.naming.provider.url</param-name>
<param-value>For valid value Check xlConfig.xml</param-value>
```

Typically, the xlConfig.xml file is located in the *OIM_HOME*/designconsole/config directory.

Replace For valid value Check xlConfig.xml with the value obtained from the XML file.

For example, is the value for Java provider in the XML file is t3://172.21.109.102:8003/oim, then update the line as follows:

```
<param-value>t3://172.21.109.102:8003/oim</param-value>
```

5. Delete the PeopleSoftOIMListener.war file from the temporary directory into which you extracted it, and then use the following command to re-create the file:

```
jar -cvf PeopleSoftOIMListener.war .
```

6. Ensure that the old version of the PeopleSoftOIMListener.war file is deleted from the application server deployment directory.

7. Deploy the newly created PeopleSoftOIMListener.war file in the deployment directory of the application server as follows:

For IBM WebSphere Application Server:

a. Log in to the WebSphere Admin console.

b. Expand **Applications.**

c. Click **Install New Application.**

d. Click the **Browse** button to locate the WAR file.

e. In the Context root field, enter `PeopleSoftOIMListener`.

f. Click **Next.**

g. In the Select installation options field, enter `PeopleSoftOIMListener` as the application name and click **Next.**

h. On the Map modules to servers page, select **PeopleSoftOIMListener.war** and click **Next.**

i. On the Map virtual hosts page, select **PeopleSoftOIMListener.war** and click **Next.**

j. Click **Finish.**

k. Click **Save** to save all the configurations to the master configuration in IBM WebSphere Application Server.

l. Click **Enterprise Applications.**

m. On the Enterprise Applications page, select **PeopleSoftOIMListener** and then click **Start** to restart the application.

For JBoss Application Server:

a. Copy the modified WAR file to the *JBOSS_HOME*/server/default/deploy directory.

   In a JBoss cluster, copy the modified WAR file to the *JBOSS_HOME*/server/all/deploy directory.

b. Restart JBoss Application Server.

For Oracle WebLogic Server:

a. Log in to the Oracle WebLogic admin console.

b. From the Domain Structure list, select **OIM_DOMAIN.**

   Where **OIM_DOMAIN** is the domain on which Oracle Identity Manager is installed.

c. Click the **Deployments** tab.

d. On Microsoft Windows, in the Change Centre window, click **Lock & Edit.** This enables the Install button of the Monitoring tab in the Summary Of Deployments section.

e. Click **Install.**

f. In the Install Application Assistant, enter the full path of the directory in which the WAR file is placed. Then, click **Next.**

g. Select the WAR file to install.

h. Click **Next.**

i. Select the **Install this deployment as an application** option, and then click **Next.**

j. In the **Name of deployment** field, enter `PeopleSoftOIMListener`.

k. In the Security section, select the **DD Only: Use only roles and policies that are defined in the deployment descriptors** option.

l. In the Source accessibility window, select the **Use the defaults defined by the deployments targets** option.

m. Click **Finish.**

On Microsoft Windows, the "The deployment has been successfully installed" message is displayed.

n. On UNIX platforms, click **Save.** The following messages are displayed:

Success All changes have been activated. No restarts are necessary.

Success Settings updated successfully.

o. On Microsoft Windows, to activate the changes that you have made up to this point:

i. Select the check box corresponding to the newly installed application.

ii. In the Change centre window, click **Activate Changes.**

p. On Microsoft Windows, select the check box for the newly installed application, select the **Servicing all requests** option from the Start list, and then click **Yes.**

For Oracle Application Server

a. Log in to the Oracle Application Server Control.

b. Click on OC4J instance where Oracle Identity Manager is deployed and running.

c. Click **Applications**, **Deploy**. The Select Archive step is displayed.

d. Enter PeopleSoftOIMListener.war file location and click **Next**.

e. In the Application Name field, enter PeopleSoftOIMListener and click **Next**.

f. Click **Deploy**.

g. Click **Return** when the application "PeopleSoftOIMListener" has been successfully deployed.

8. Restart Oracle Identity Manager and the Design Console.

2.2.1.5.2 Deploying the PeopleSoft Listener on Oracle Identity Manager Release 11.1.1

To deploy the PeopleSoft listener on Oracle Identity Manager release 11.1.1:

1. Copy the *OIM_HOME*/server/XLIntegrations/PSFTER/EAR/PeopleSoftOIMListener.ear folder into a temporary folder, for example `temp`.
2. Copy the Common.jar file from the /lib directory on the installation media to the temp/PeopleSoftOIMListener.ear/PeopleSoftOIMListener.war/WEB-INF/lib folder.
3. Copy the following files from the *OIM_HOME*/server/client to the WEB-INF/lib folder in the temporary folder:
   - oimclient.jar

4. Copy the following files from the *OIM_HOME*/server/platform folders to the WEB-INF/lib folder in the temporary folder:
   - iam-platform-auth-client.jar
   - iam-platform-utils.jar
5. Edit the web.xml file present in temp/PeopleSoftOIMListener.ear/PeopleSoftOIMListener.war/WEB-INF folder as follows:
   a. Locate the **Login Name of the OIM Admin User** details.

      ```
      <param-name>oimLoginUserName</param-name>
      <param-value>OIM_ADMIN_USER</param-value>
      ```

      Replace OIM_ADMIN_USER with Oracle Identity Manager administrator credentials.

      For example, if the administrative account on Oracle Identity Manager is **xelsysadm,** then update the line as follows:

      ```
      <param-value>xelsysadm</param-value>
      ```

   b. Locate the **Message Handler Impl classes** details.

      ```
      <param-name>IT_RESOURCE_NAME</param-name>
      ```

      Replace IT_RESOURCE_NAME with the name of the IT resource.

      For example, if the name of IT resource is **PSFT Server,** then update the line as follows:

      ```
      <param-name>PSFT Server</param-name>
      ```

   c. Locate the following line:

      ```
      <param-value>MESSAGE~IMPLEMENTATION_CLASS;MESSAGE~IMPLEMENTATION_CLASS;MESS
      AGE~IMPLEMENTATION_CLASS</param-value>
      ```

      In this format, the message name and its implementation class must be separated by a tilde (~). For multiple messages, each pair must be separated by a semicolon (;). For default implementation, you must modify the line as follows:

      ```
      <param-value>PERSON_BASIC_SYNC~oracle.iam.connectors.psft.common.handler.im
      pl.PSFTPersonSyncReconMessageHandlerImpl;USER_PROFILE~oracle.iam.connectors
      .psft.common.handler.impl.PSFTUserProfileReconMessageHandlerImpl;WORKFORCE_
      SYNC~oracle.iam.connectors.psft.common.handler.impl.PSFTWorkForceSyncReconM
      essageHandlerImpl;DELETE_USER_PROFILE~oracle.iam.connectors.psft.common.han
      dler.impl.PSFTDeleteUserReconMessageHandlerImpl</param-value>
      ```

      If PeopleSoft is sending the USER_PROFILE.VERSION_84 message for USER_PROFILE, then modify the line as follows:

      ```
      <param-value>PERSON_BASIC_SYNC~oracle.iam.connectors.psft.common.handler.im
      pl.PSFTPersonSyncReconMessageHandlerImpl;USER_PROFILE.VERSION_84~oracle.iam
      .connectors.psft.common.handler.impl.PSFTUserProfileReconMessageHandlerImpl
      ;WORKFORCE_SYNC~oracle.iam.connectors.psft.common.handler.impl.PSFTWorkForc
      eSyncReconMessageHandlerImpl;DELETE_USER_PROFILE~oracle.iam.connectors.psft
      .common.handler.impl.PSFTDeleteUserReconMessageHandlerImpl</param-value>
      ```

6. Ensure that the old version of the PeopleSoftOIMListener.ear file is deleted from the application server deployment directory.

7. Deploy the newly created PeopleSoftOIMListener.ear file in the deployment directory of the application server as follows:

   a. Log in to the Oracle WebLogic admin console.

   b. On the left navigation pane, expand **Domain Structure,** and then click **Deployments.**

   c. Click **Lock & Edit.** It enables the Install button of the Monitoring tab in the Summary Of Deployments section.

   d. Click **Install.**

   e. On the Install Application Assistant page, in the **Path** field, enter the full path of the directory in which the EAR file is placed. Then, click **Next.**

   f. Select the **Install this deployment as an application** option, and then click **Next.**

   g. From the **Servers** list, select the server on which Oracle Identity Manager is deployed, for example `oim_server1` and then click **Next.**

   h. On the Optional Settings page, select **I will make the deployment accessible from the following location,** and then click **Next.**

   i. Review your choices, and then click **Finish.**

   j. Click **Activate Changes.**

      On Microsoft Windows, a message that reads "All changes have been activated. No restarts are necessary" is displayed.

8. Edit the *$DOMAIN_HOME*`/config/fmwconfig/system-jazn-data.xml` file as follows:

   a. Add the following block in the file:

```
      <grant>
            <grantee>
                <codesource>

<url>file:{samplelocation}/PeopleSoftOIMListener.ear/PeopleSoftOIMListener.
war/WEB-INF/lib/-</url>
                </codesource>
            </grantee>
                  <permissions>
                <permission>

<class>oracle.security.jps.service.credstore.CredentialAccessPermission</cl
ass>
                    <name>context=SYSTEM,mapName=oim,keyName=*</name>
                    <actions>read,write,delete</actions>
                </permission>
        </permissions>
            <permission-set-refs>
            </permission-set-refs>
        </grant>
```

   b. Locate the sample location details, and replace it with the path of the PeopleSoftOIMListener.ear file location.

      For example, if the EAR file is placed in the /temp folder, then replace **{samplelocation}** in the preceding block as follows:

```
<url>file:/temp/PeopleSoftOIMListener.ear/PeopleSoftOIMListener.war/WEB-INF
```

```
/lib/-</url>
```

9. Restart Oracle Identity Manager and the Admin Server.

2.2.1.6 Removing the PeopleSoft Listener

Note: This section is not a part of installation on Oracle Identity Manager. You might need this procedure to extend the connector.

To remove the PeopleSoft listener:

For IBM WebSphere Application Server:

1. Log in to the WebSphere Admin console.
2. Expand **Applications.**
3. Select **Enterprise Applications** from the list.

   A list of deployed applications is shown on the right pane.
4. Select the **PeopleSoftOIMListener.war** check box.
5. Specify the Context root as `PeopleSoftOIMListener.`
6. Click **Uninstall.**

   An Uninstall Application confirmation screen appears with the name of the application to be uninstalled. In this scenario, the application would be PeopleSoftOIMListener.
7. Click **OK.**

For JBoss Application Server:

1. Delete the WAR file from the *JBOSS_HOME*/server/default/deploy directory.

   In a JBoss cluster, delete the WAR file from the *JBOSS_HOME*/server/all/deploy directory.
2. Restart JBoss Application Server.

For Oracle WebLogic Server:

1. Log in to the Oracle WebLogic admin console.
2. From the Domain Structure list, select **OIM_DOMAIN.**

   Where **OIM_DOMAIN** is the domain on which Oracle Identity Manager is installed.
3. Click the **Deployments** tab.
4. On Microsoft Windows, in the Change Centre window, click **Lock & Edit.**
5. Select **PeopleSoftOIMListener.war** or **PeopleSoftOIMListener.ear** depending on Oracle Identity Manager release. This enables the Delete button of the Control tab in the Summary Of Deployments region.
6. Click **Stop.** A list appears.
7. Select **Force Stop Now.**

   The Force Stop Application confirmation screen appears.
8. Click **Yes.**

9. On the Control tab in the Summary Of Deployments region, select **PeopleSoftOIMListener.war** or **PeopleSoftOIMListener.ear** depending on Oracle Identity Manager release.
10. Click **Delete.**

    A confirmation message appears on successful deletion of the WAR file.
11. On the left pane, click the **Active Changes** button.

For Oracle Application Server

1. Log in to the Oracle Application Server Control.
2. Click on OC4J instance where Oracle Identity Manager is deployed and running.
3. Click **Applications**.
4. Select the PeopleSoftOIMListener application and click **Undeploy**. You will be prompted to confirm the removal of PeopleSoftOIMListener application.
5. Click **Yes**. A message confirming the removal of PeopleSoftOIMListener application will be displayed.
6. Click **Return**.

2.2.2 Installation on the Target System

During this stage, you configure the target system to enable it for reconciliation and provisioning operations. This information is provided in the following sections:

- Section 2.2.2.1, "Configuring the Target System for Lookup Reconciliation"
- Section 2.2.2.2, "Configuring the Target System for Full Reconciliation"
- Section 2.2.2.3, "Configuring the Target System for Incremental Reconciliation"
- Section 2.2.2.4, "Configuring the Target System for Provisioning"
- Section 2.2.2.5, "Configuring Oracle Identity Manager Server as a Non-Proxy Host on PeopleSoft Server"

2.2.2.1 Configuring the Target System for Lookup Reconciliation

Lookup reconciliation is used to reconcile lookup definitions for currency codes, languages, roles, permissions, and e-mail types corresponding to the lookup fields on the target system created into Oracle Identity Manager.

Configuring the target system for lookup reconciliation involves creating the properties file by performing the procedure described in the following section:

Creating the Application Engine Program

The Application Engine program populates the .properties file with lookup data that is required for look up reconciliation. This is a one-time procedure.

You can create the Application Engine program based on whether you have imported the PeopleSoft Application Designer project. Perform the procedure described in one of the following sections:

- Creating the Application Engine Program If PeopleSoft Application Designer Project Is Not Imported
- Creating the Application Engine Program If PeopleSoft Application Designer Project Is Imported

Creating the Application Engine Program If PeopleSoft Application Designer Project Is Not Imported

To create the Application Engine program if you have not imported the PeopleSoft Application Designer Project as described in Section 2.1.2.1, "Importing a Project from Application Designer," you must perform the following tasks:

1. To open Application Designer in 2-tier mode, click **Start, Programs, Peoplesoft8.x,** and then **Application Designer.**

   Note: To open Application Designer in 2-tier mode, the database client (client of the database that PeopleSoft is using) must be installed on the server. In addition, you must select the appropriate database type from the **Connection Type** field (for example, Oracle Database) while providing sign-on information in the PeopleSoft Application Designer Signon window.

2. From the File menu, click **New.**
3. In the New Definition dialog box, select **App Engine Program** from the **Definition** list.
4. On the App Engine Program page, a plus sign (+) is displayed besides the MAIN section. The MAIN section may contain multiple steps. Expand **MAIN.** A step named Step01 is added to MAIN.
5. Rename Step01 to `Language`.
6. Click **Action** in the **Insert** menu. An action is added to the Language step.
7. Select **PeopleCode** from the list for the new action.
8. Click **Save** in the **File** menu, and save the Application Engine program as LOOKUP_RECON.
9. Double-click the **PeopleCode** action. A new PeopleCode window is displayed.
10. Copy the code from the *OIM_HOME*/xellerate/XLIntegrations/PSFTUM/peoplecode/languageCode.txt file into the PeopleCode window.
11. Change the path to a directory location on the PeopleSoft server as follows:

```
&DataFile = GetFile("absolute path where you want to generate the DataFile",
"w", %FilePath_Absolute);
&LOGFile = GetFile("absolute path where you want to generate the LogFile", "w",
"a", %FilePath_Absolute);
```

    For example:

```
&DataFile = GetFile("C:\PSFT_849_LOOKUPS\language.properties", "w",
%FilePath_Absolute);
&LOGFile = GetFile("C:\PSFT_849_LOOKUPS\language.log", "w", "a",
%FilePath_Absolute);
```

    Note: Ensure that the name of the file ends in `.properties`, for example, language.properties.

12. Save the PeopleCode action, and close the window.

13. On the App Engine Program page, select the **language** step and then select **Step/Action** from the **Insert** menu.
14. Repeat Steps 5 through 12 to create the remaining steps, which are listed in the following table:

Step Name	File Containing the Required PeopleCode
`Currency`	CurrencyCode.txt
`userrole`	UserRoles.txt
`permiss`	PermissionList.txt
`EmailType`	EmailType.txt

15. Save the Application Engine program.

Creating the Application Engine Program If PeopleSoft Application Designer Project Is Imported

To create the Application Engine program if you have imported the PeopleSoft Application Designer Project as described in Section 2.1.2.1, "Importing a Project from Application Designer," you must perform the following tasks:

1. To open Application Designer in 2-tier mode, click **Start, Programs, Peoplesoft8.x,** and then **Application Designer.**
2. From the File menu, select **Open** and then select **Project.** Search for and open the project **OIM_UM.**

   The Open Definition dialog box appears.
3. In the Name field, enter `OIM_UM` as the project name and then click **Open.**

   The project appears on the left pane.
4. Click the plus sign (+) below Application Engine Programs.
5. Double-click **LOOKUP_RECON** on the left pane.

   The LOOKUP_RECON (App Engine Program) window appears on the right pane.
6. Double-click the PeopleCode action associated with Step01 - "Currency Code". A new PeopleCode window is displayed.
7. Change the path to a directory location on the PeopleSoft server as follows:

```
&DataFile = GetFile("absolute path where you want to generate the DataFile",
"w", %FilePath_Absolute);
&LOGFile = GetFile("absolute path where you want to generate the LogFile", "w",
"a", %FilePath_Absolute);
```

   For example:

```
&DataFile = GetFile("C:\PSFT_849_LOOKUPS\currencycodes.properties", "w",
%FilePath_Absolute);
&LOGFile = GetFile("C:\PSFT_849_LOOKUPS\lcurrencycodes.log", "w", "a",
%FilePath_Absolute);
```

Note: Ensure that the name of the file ends in `.properties`, for example, language.properties.

8. Save the PeopleCode action, and close the window.
9. Repeat Steps 6 through 8 for the remaining steps, such as Email Types, Language Codes, Permission Lists, and Roles.
10. Save the Application Engine program.

2.2.2.2 Configuring the Target System for Full Reconciliation

Configuring the target system for full reconciliation involves configuring the USER_PROFILE message by performing the following procedures:

Note: The procedure remains the same for PeopleTools 8.49 and for PeopleTools 8.50. The screenshots are taken on PeopleTools 8.49 version.

- Section 2.2.2.2.1, "Displaying the EI Repository Folder"
- Section 2.2.2.2.2, "Activating the USER_PROFILE Messages"
- Section 2.2.2.2.3, "Activating the Full Data Publish Rule"
- Section 2.2.2.2.4, "Configuring the PeopleSoft Integration Broker"
- Section 2.2.2.2.5, "Configuring the USER_PROFILE Service Operation"

2.2.2.2.1 Displaying the EI Repository Folder

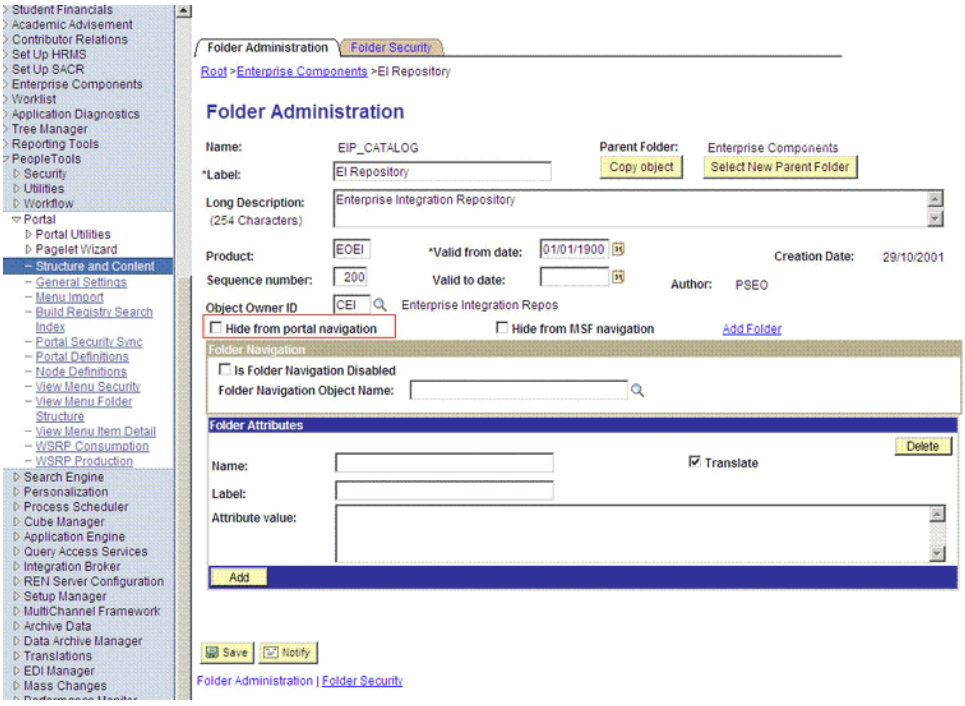
EI Repository is a hidden folder in PeopleSoft. Therefore, you must display this folder.

To display the EI Repository folder:

Note: Perform this procedure using the PeopleSoft administrator credentials.

1. In the PeopleSoft Internet Architecture, expand **People Tools, Portal,** and then **Structure and Content.**
2. Click the **Enterprise Components** link.
3. Click the **Edit** link for EI Repository, and then uncheck **Hide from portal navigation.**

   The Hide from portal navigation check box is shown in the following screenshot:



4. Click **Save.**
5. Log out, and then log in.

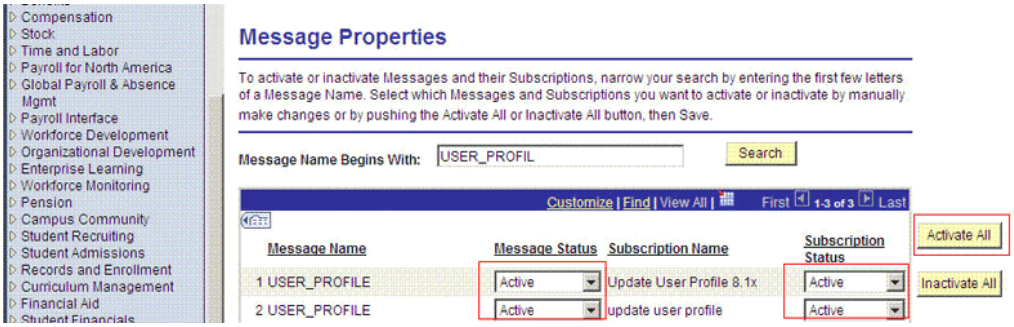
2.2.2.2.2 Activating the USER_PROFILE Messages

You must activate the USER_PROFILE message so that it can be processed.

To activate the USER_PROFILE messages:

1. In the PeopleSoft Internet Architecture, expand **Enterprise Components, EI Repository,** and then click **Message Properties.**
2. Search for and open the **USER_PROFILE** message.
3. Click **Activate All.**

   The message to be activated is shown in the following screenshot:



4. Click the **Subscription** tab, and activate the Subscription PeopleCode if it exists.

> **Note:** To perform this step, your user profile must have the EIR Administrator role consisting of **EOEI9000** and **EOCO9000** permission lists.

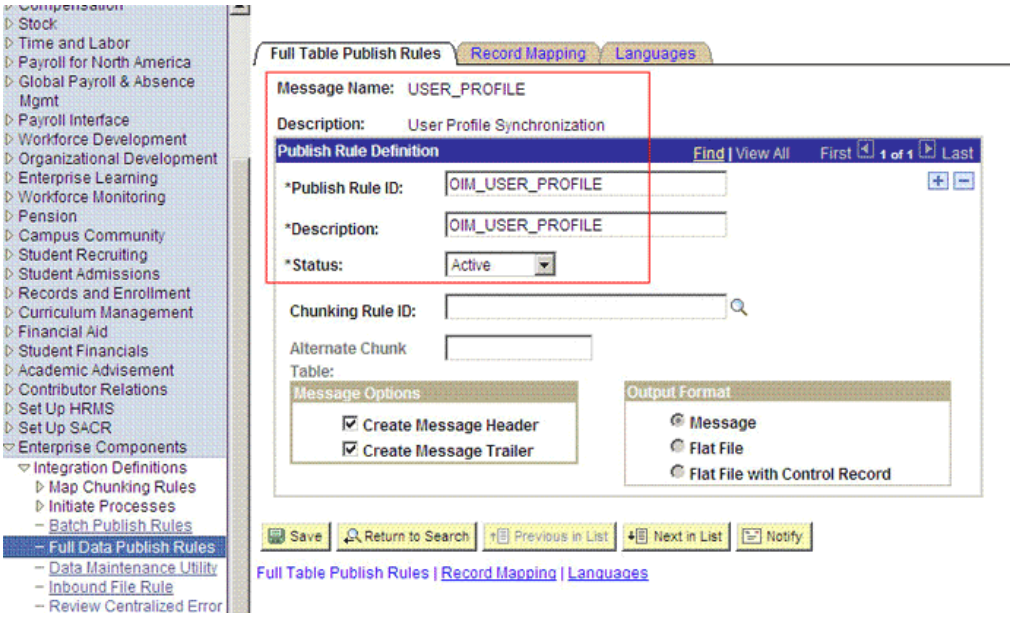
2.2.2.2.3 Activating the Full Data Publish Rule

You must define and activate this rule, because it acts as a catalyst for the Full Reconciliation process. This rule provides the Full Reconciliation process the desired information to initiate reconciliation.

To activate the full data publish rule:

1. In the PeopleSoft Internet Architecture, expand **Enterprise Components, Integration Definitions,** and then click **Full Data Publish Rules.**
2. Search for and open the **USER_PROFILE** message.
3. In the Publish Rule Definition region:
   a. In the Publish Rule ID field, enter `OIM_USER_PROFILE`.
   b. In the Description field, enter `OIM_USER_PROFILE`.
   c. From the Status list, select **Active.**

   The following screenshot displays the preceding steps:



4. Click **Save.**

2.2.2.2.4 Configuring the PeopleSoft Integration Broker

The following sections explain the procedures to configure the PeopleSoft Integration Broker:

Configuring the PeopleSoft Integration Broker Gateway

PeopleSoft Integration Broker is installed as part of the PeopleTools installation process. The Integration Broker Gateway is a component of PeopleSoft Integration Broker, which runs on the PeopleSoft Web Server. It is the physical hub between PeopleSoft and the third-party system. The integration gateway manages the receipt and delivery of messages passed among systems through PeopleSoft Integration Broker.

To configure the PeopleSoft Integration Broker gateway:

1. Open a Web browser and enter the URL for PeopleSoft Internet Architecture.

   The URL for PeopleSoft Internet Architecture is in the following format:

```
http://IPADDRESS:PORT/psp/ps/?cmd=login
```

For example:

```
http://172.21.109.69:9080/psp/ps/?cmd=login
```

2. To display the Gateway component details, expand **PeopleTools, Integration Broker, Configuration,** and then **Gateways.** The Gateway component details are displayed.
3. In the Integration Gateway ID field, enter `LOCAL` and then click **Search**. The LOCAL gateway is a default gateway that is created when you install PeopleSoft Internet Architecture.
4. Ensure that the IP address and host name specified in the URL of the PeopleSoft listener are those on which the target system is installed. The URL of the PeopleSoft listener is in one of the following formats:

```
http://HOSTNAME_of_the_PeopleSoft_Web_Server or
IP_address:port/PSIGW/PeopleSoftListeningConnector
```

For example:

```
http://10.121.16.42:80/PSIGW/PeopleSoftListeningConnector
```

5. To load all target connectors that are registered with the LOCAL gateway, click **Load Gateway Connectors.** A window is displayed mentioning that the loading process is successful. Click **OK.**
6. Click **Save.**
7. Click **Ping Gateway** to check whether the gateway component is active. The PeopleTools version and the status of the PeopleSoft listener are displayed. The status should be **ACTIVE.**

Configuring PeopleSoft Integration Broker

PeopleSoft Integration Broker provides a mechanism for communicating with the outside world using XML files. Communication can take place between different PeopleSoft applications or between PeopleSoft and third-party systems. To subscribe to data, third-party applications can accept and process XML messages posted by PeopleSoft by using the available PeopleSoft connectors. The Integration Broker routes messages to and from PeopleSoft.

A remote node that you create within the Integration Broker acts as the receiver for XML messages from PeopleSoft. This remote node accepts XML messages and posts them as XML files to a folder that you specify. During a reconciliation run, a scheduled task running on Oracle Identity Manager uses the data in these XML files to Oracle Identity Manager.

To create the remote node:

1. While creating the remote node, you use the value of the ig.fileconnector.password property in the integrationGateway.properties file. Determine the value of this property as follows:
   a. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Configuration,** and then click **Gateways.**
   b. In the Integration Gateway ID field, enter `LOCAL` and then click **Search.**
   c. Click the **Gateway Setup Properties** link.

d. Enter the user ID and password for accessing the integrationGateway.properties file, and then click **OK**.

e. On the PeopleSoft Node Configuration page, click **Advanced Properties Page**.

   The contents of the integrationGateway.properties file are displayed.

f. Search for **ig.fileconnector.properties** in the file contents. The line displayed in the file may be similar to the following sample line:

```
ig.fileconnector.password={V1.1}%5GhbfJ89bvNT1HzF98==
```

g. Copy the text after (that is, to the right of) the equal sign of the property. For example, copy `{V1.1}%5GhbfJ89bvNT1HzF98==` from the line given in the preceding sample.

   This is the password that you specify while creating the remote node. The sample password given here is encrypted. If the password displayed on your PeopleSoft installation is not encrypted, then you can encrypt it by following the steps given later in this section.

2. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Nodes.**
3. On the Add a New Value tab, enter the node name, for example, `OIM_FILE_NODE`, and then click **Add.**
4. On the Node Definition tab, provide the following values:

   In the Description field, enter a description for the node.

   In the Default User ID field, enter `PS`.
5. Make this node a remote node by deselecting the **Local Node** check box and selecting the **Active Node** check box.
6. Make the Node Type as **PIA.**
7. On the Connectors tab, search for the following information by clicking the Lookup icon:

   Gateway ID: LOCAL

   Connector ID: FILEOUTPUT
8. On the Properties page in the Connectors tab, enter the following information:

   Property ID: HEADER

   Property Name: sendUncompressed

   Required value: Y

   Property ID: PROPERTY

   Property Name: Method

   Required value: PUT

   Property ID: PROPERTY

   Property Name: FilePath

   Required value: Enter the full path of any folder on which the Integration Broker has Write permissions. The remote node will post XML files to this folder.

   Property ID: PROPERTY

   Property Name: Password

Required value: Enter the value of the ig.fileconnector.password property in the integrationGateway.properties file. This is the password that you determine by performing Step 1. If the password is not already encrypted, that you can encrypt it as follows:

a. In the Password Encrypting Utility region, enter the value of the ig.fileconnector.password property in the **Password** and **Confirm Password** fields.

b. Click **Encrypt**.

c. From the **Encrypted Password** field, copy the encrypted password to the Value field for the Password property.

9. Click **Save.**

10. Click **Ping Node** to check whether a connection is established with the specified IP address.

2.2.2.2.5 Configuring the USER_PROFILE Service Operation To configure the USER_PROFILE service operation perform the following procedures:

Note: The procedure remains the same for PeopleTools 8.49 and for PeopleTools 8.50. The screenshots are taken on PeopleTools 8.49 version.

- Activating the USER_PROFILE Service Operation
- Verifying the Queue Status for the USER_PROFILE Service Operation
- Setting Up the Security for the USER_PROFILE Service Operation
- Defining the Routing for the USER_PROFILE Service Operation

Activating the USER_PROFILE Service Operation

The service operation is a mechanism to trigger, receive, transform, and route messages that provide information about updates in the PeopleSoft or an external application. You must activate the service operation for successful transmission and receipt of messages.

To activate the USER_PROFILE service operation:

1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**

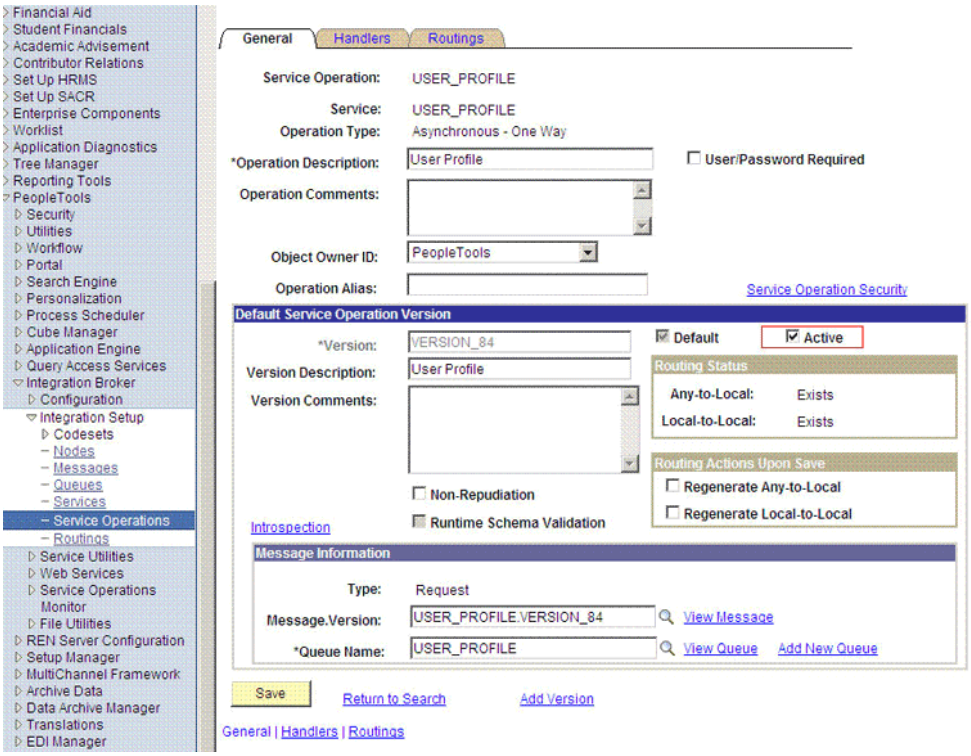
2. On the Find Service Operation tab, enter `USER_PROFILE` in the **Service** field, and then click **Search.**

3. Click the **USER_PROFILE** link.

Note: In PeopleSoft HRMS, there are two versions of the message associated with this service operation. But, when you integrate PeopleSoft HRMS 9.0 and Oracle Identity Manager, you must send `version_84`. So, you must use the default version, `VERSION_84`, for HRMS 9.0.

---

4. In the Default Service Operation Version region, click **Active.** The following screenshot displays the default version of the USER_PROFILE service operation:



5. Click **Save.**

Verifying the Queue Status for the USER_PROFILE Service Operation

All messages in PeopleSoft are sent through a queue. This is done to ensure that the messages are delivered in the correct sequence. Therefore, you must ensure that the queue is in the Run status.

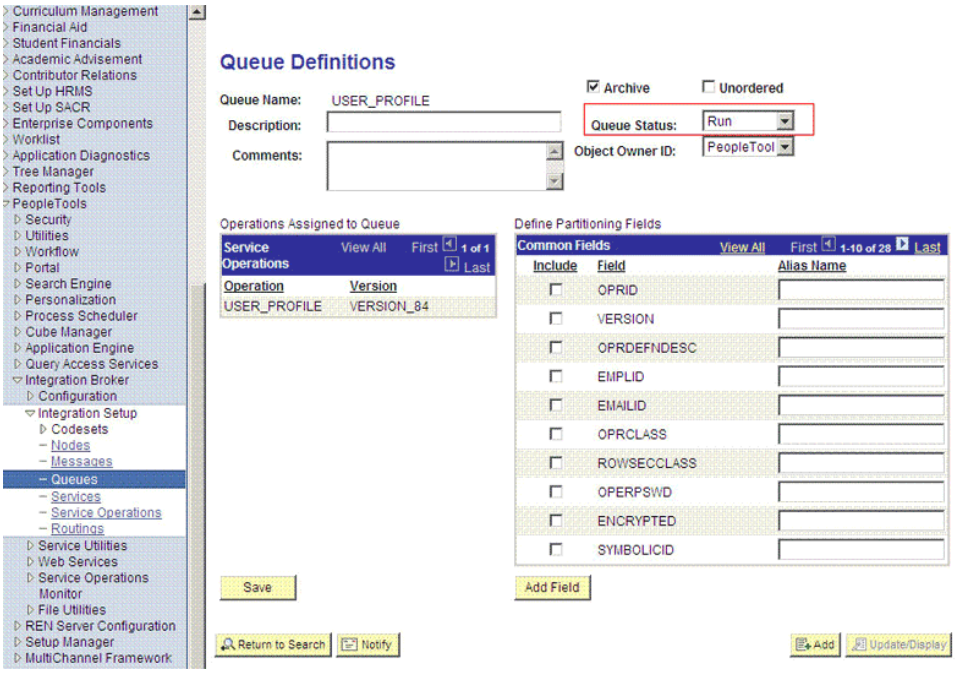
To ensure that the status of the queue for the USER_PROFILE service operation is Run:

1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Queues.**
2. Search for the **USER_PROFILE** queue.
3. In the Queue Status list, ensure that **Run** is selected.

Note: If the queue status is not Run:

1. From the Queue Status list, select **Run.**
2. Click **Save.**

The queue status is shown in the following screenshot:



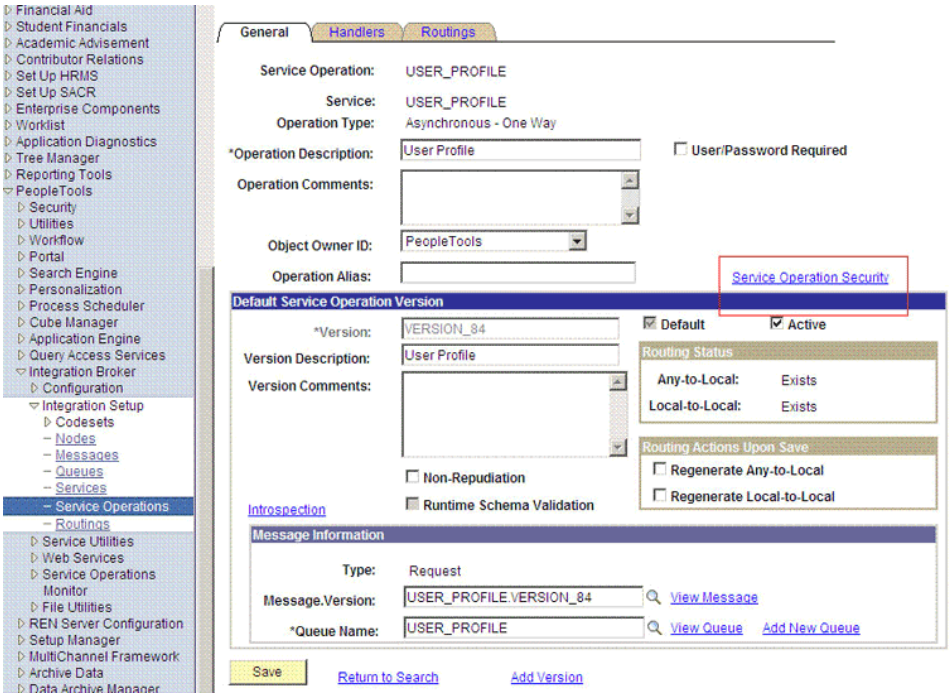
4. Click **Return to Search.**

Setting Up the Security for the USER_PROFILE Service Operation

The target system user who has the permission to modify, add, or delete personal or job information of an employee might not have access to send messages regarding these updates. Therefore, it is imperative to explicitly grant security to enable operations.

To set up the security for the USER_PROFILE service operation:

1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
2. Search for and open the **USER_PROFILE** service operation.
3. On the General tab, click the **Service Operation Security** link. The link is shown in the following screenshot:



4. Attach the permission list **OIMUM** to the USER_PROFILE service operation. This list is created in Step 3 of the preinstallation procedure discussed in Section 2.1.2.2.1, "Creating a Permission List."

   To attach the permission list:

   Note: This procedure describes how to grant access to the OIMUM permission list. The OIMUM permission list is used as an example. However, to implement this procedure you must use the permission list (attached through a role) to the user profile of the actual user who maintains the user profile information or the user who performs full reconciliation.

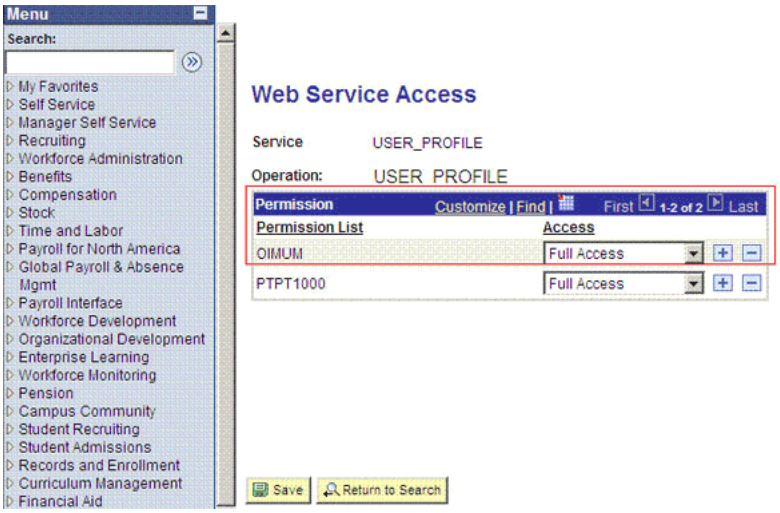
   a. Click the plus sign (+) to add a row to the Permission List field.

   b. In the Permission List field, enter **OIM** and then click the Look up Permission List icon.

      The **OIMUM** permission list appears.

   c. From the Access list, select **Full Access.**

      The following screenshot displays the Access list with Full Access:



d. Click **Save.**

e. Click **Return to Search.**

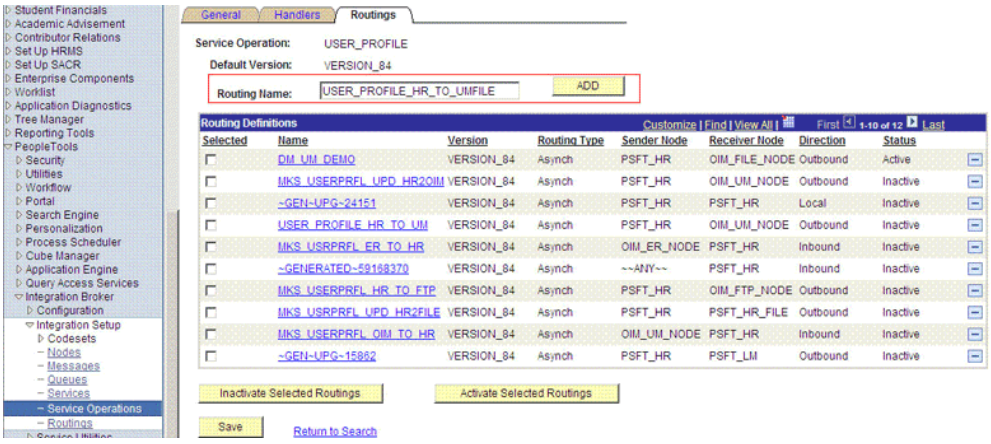
Defining the Routing for the USER_PROFILE Service Operation

Routing is defined to inform PeopleSoft about the origin and the intended recipient of the message. You might have to transform the message being sent or received according to the business rules.

To define the routing for the USER_PROFILE service operation:

1. On the Routing tab, enter `USER_PROFILE_HR_TO_UMFILE` as the routing name and then click **Add.**

The following screenshot displays the Routing Name field:



2. On the Routing Definition tab, enter the following:

Sender Node: `PSFT_HR`

Note: The Sender Node is the default active local node. To locate the sender node:

1. Click the Lookup icon.
2. Click **Default** to sort the results in descending order.

   The default active local node should meet the following criteria:

   Local Node: **1**

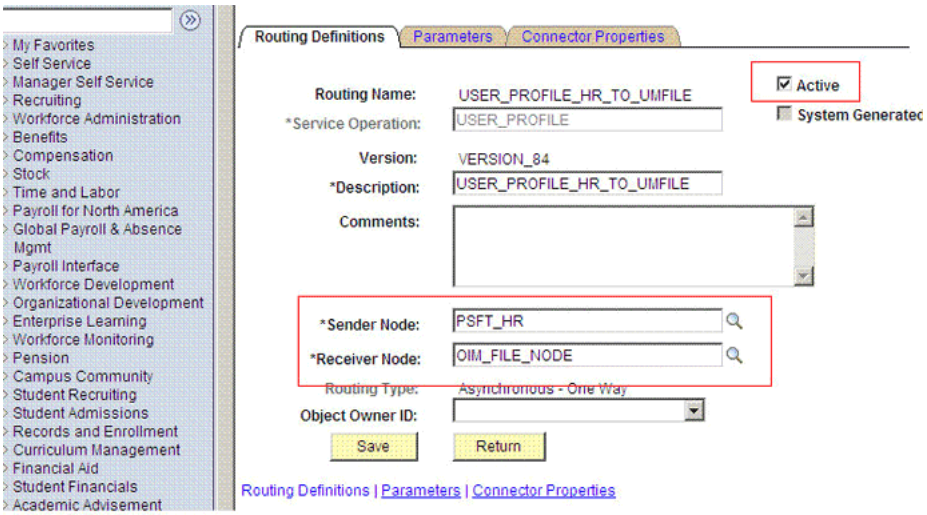
   Default Local Node: **Y**

   Node Type: **PIA**

   Only one node can meet all the above conditions at a time.
3. Select the node.
4. Click **Save.**

Receiver Node: `OIM_FILE_NODE`

The following screenshot displays the Sender and Receiver nodes:



3. Click **Save.**
4. Click **Return** to go back to the Routings tab of the Service Operation, and verify whether your routing is active.

2.2.2.3 Configuring the Target System for Incremental Reconciliation

Configuring the target system for incremental reconciliation involves configuration of USER_PROFILE and DELETE_USER_PROFILE service operations, nodes, and routing to send messages from PeopleSoft Integration Broker to other systems, and configuring PeopleSoft Integration Broker.

The USER_PROFILE message contains information about user accounts that are created or modified. The DELETE_USER_PROFILE message contains information about user accounts that have been deleted.

A message is the physical container for the XML data that is sent from the target system. Message definitions provide the physical description of data that is sent from the target system. This data includes fields, field types, and field lengths. A queue is

used to carry messages. It is a mechanism for structuring data into logical groups. A message can belong to only one queue.

Setting the PeopleSoft Integration Broker gateway is mandatory when you configure PeopleSoft Integration Broker. To subscribe to XML data, Oracle Identity Manager can accept and process XML messages posted by PeopleSoft by using PeopleSoft connectors located in the PeopleSoft Integration Broker gateway. These connectors are Java programs that are controlled by the Integration Broker gateway.

This gateway is a program that runs on the PeopleSoft Web server. It acts as a physical hub between PeopleSoft and PeopleSoft applications (or third-party systems, such as Oracle Identity Manager). The gateway manages the receipt and delivery of messages passed among systems through PeopleSoft Integration Broker.

To configure the target system for incremental reconciliation, perform the following procedures:

Note: You must use an administrator account to perform the following procedures.

- Section 2.2.2.3.1, "Configuring PeopleSoft Integration Broker"
- Section 2.2.2.3.2, "Configuring the Service Operations"
- Section 2.2.2.3.3, "Preventing Transmission of Unwanted Fields During Incremental Reconciliation"

2.2.2.3.1 Configuring PeopleSoft Integration Broker

The following sections explain the procedures to configure PeopleSoft Integration Broker:

Configuring the PeopleSoft Integration Broker Gateway

The Integration Broker Gateway is a component of PeopleSoft Integration Broker (a messaging system), which is deployed at the PeopleSoft Web server. The Integration Broker Gateway is used for sending messages from PeopleSoft and for receiving messages for PeopleSoft. The "Configuring the PeopleSoft Integration Broker Gateway" on page 2-36 describes the procedure to configure the PeopleSoft Integration Broker gateway.

Configuring PeopleSoft Integration Broker

Integration Broker is the inherent messaging system of PeopleSoft. You must configure Integration Broker to send and receive messages from and to PeopleSoft.

To configure PeopleSoft Integration Broker:

1. Create a remote node by performing the following steps:
   a. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Nodes.**
   b. On the Add a New Value tab, enter the node name, for example, `OIM_NODE`, and then click **Add.**
   c. On the Node Definition tab, enter a description for the node in the **Description** field. In addition, enter `PS` in the **Default User ID** field.
   d. Make this node a remote node by deselecting the **Local Node** check box and selecting the **Active Node** check box.
   e. Make the Node Type as **PIA.**

f. On the **Connectors** tab, search for the following information by clicking the Lookup icon:

Gateway ID: LOCAL

Connector ID: HTTPTARGET

g. On the **Properties** page in the Connectors tab, enter the following information:

Property ID: HEADER

Property Name: sendUncompressed

Required value: Y

Property ID: HTTP PROPERTY

Property Name: Method

Required value: POST

Property ID: HEADER

Property Name: Host

Required value: Enter the value of the IT resource name as configured for the target system.

Sample value: PSFT Server

Property ID: PRIMARYURL

Property Name: URL

Required value: Enter the URL of the PeopleSoft listener that is configured to receive XML messages. This URL must be in the following format:

`http://`*`HOSTNAME_of_OIM_SERVER or IPADDRESS:PORT`*`/PeopleSoftOIMListener`

The URL depends on the application server that you are using. For an environment on which SSL is not enabled, the URL must be in the following format:

For IBM WebSphere Application Server:

`http://10.121.16.42:9080/PeopleSoftOIMListener`

For JBoss Application Server:

`http://10.121.16.42:8080/PeopleSoftOIMListener`

For Oracle WebLogic Server:

`http://10.121.16.42:7001/PeopleSoftOIMListener`

For Oracle Application Server:

`http://10.121.16.42:7200/PeopleSoftOIMListener/`

For an environment on which SSL is enabled, the URL must be in the following format:

`https://`*`COMMON_NAME`*`:`*`PORT`*`/PeopleSoftOIMListener`

For IBM WebSphere Application Server:

`https://example088196:9443/PeopleSoftOIMListener`

For JBoss Application Server:

```
https://example088196:8443/PeopleSoftOIMListener
```

For Oracle WebLogic Server:

```
https://example088196:7002/PeopleSoftOIMListener
```

For Oracle Application Server

```
https://example088916:7200/PeopleSoftOIMListener/
```

h. Click **Save** to save the changes.

i. Click **Ping Node** to check whether a connection is established with the specified IP address.

Note: You might encounter the following error when you send a message from PeopleSoft Integration Broker over HTTP PeopleTools 8.50 target system:

```
HttpTargetConnector:PSHttpFactory init or
setCertificate failed
```

This happens because the Integration Broker Gateway Web server tries to access the keystore even if SSL is not enabled using the parameters defined in the integrationgateway.properties file as follows:

```
secureFileKeystorePath=<path to pskey>

secureFileKeystorePasswd=password
```

If either the <path to pskey> or the password (unencrypted) is incorrect, you will receive the preceding error message. Perform the following steps to resolve the error:

1. Verify if `secureFileKeystorePath` in the integrationgateway.properties file is correct.
2. Verify if `secureFileKeystorePasswd` in the integrationgateway.properties file is correct.
3. Access the pskeymanager to check the accuracy of the path and the password. You can access pskeymanager from the following location:

   <PIA_HOME>\webserv\peoplesoft\bin

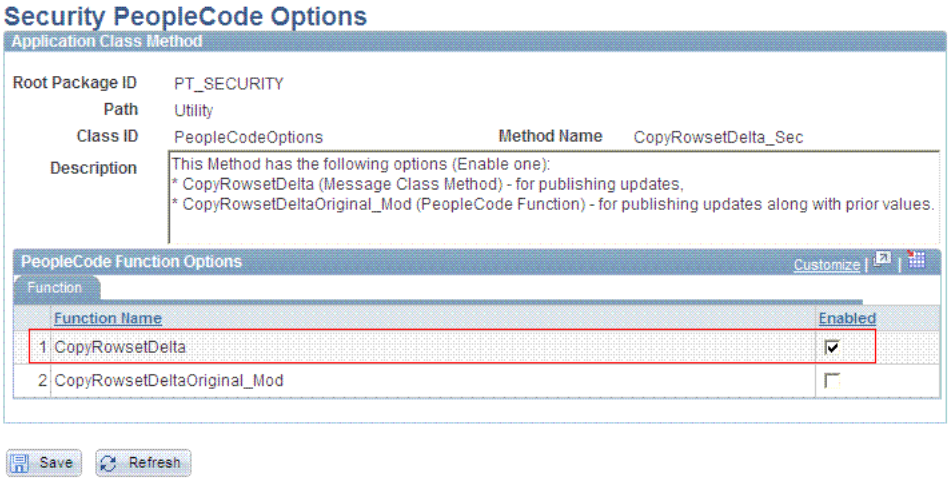
Usually, a new PeopleTools 8.50 instance throws the preceding error when you message over the HTTP target connector. The reason is that the default password is not in the encrypted format in the integrationgateway.properties file.

2.2.2.3.2 Configuring the Service Operations Perform the following procedures to configure the service operations:

- Configuring the USER_PROFILE Service Operation
- Configuring the DELETE_USER_PROFILE Service Operation

Before configuring the service operations for PeopleTools 8.50, ensure that the following setting is enabled:

1. In PeopleSoft Internet Architecture, expand **PeopleTools, Security, Security Objects,** and then click **Security PeopleCode Options.**
2. Select **CopyRowsetDelta** check box.



Configuring the USER_PROFILE Service Operation

> **Note:** The procedure remains the same for PeopleTools 8.49 and for PeopleTools 8.50. The screenshots are taken on PeopleTools 8.49 version.

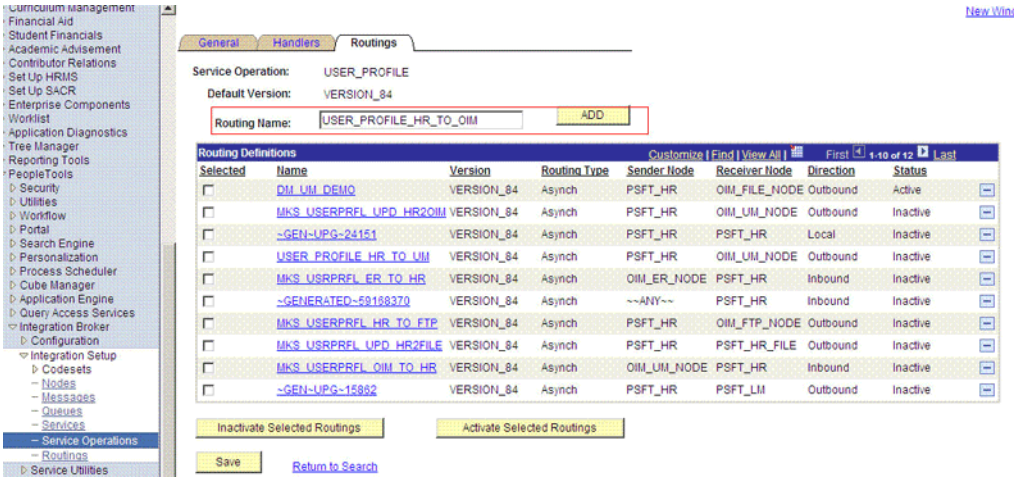
The USER_PROFILE message contains information about user accounts that are created or modified.

To configure the USER_PROFILE service operation:

> **Note:** See Section 2.2.2.2.5, "Configuring the USER_PROFILE Service Operation" for performing the initial configuration steps. This section describes the additional steps required for configuration.

1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
2. Search for and open the **USER_PROFILE** service operation.
3. On the Routing tab, enter `USER_PROFILE_HR_TO_OIM` as the routing name and then click **Add.**

   The following screenshot displays the Routing Name field:



4. On the Routing Definition tab, enter the following:

   Sender Node: `PSFT_HR`

   Note: The sender node is the default active local node. To locate the sender node:

   1. Click the Look up icon.
   2. Click **Default** to sort the results in descending order.

      The default active local node should meet the following criteria:

      Local Node: **1**

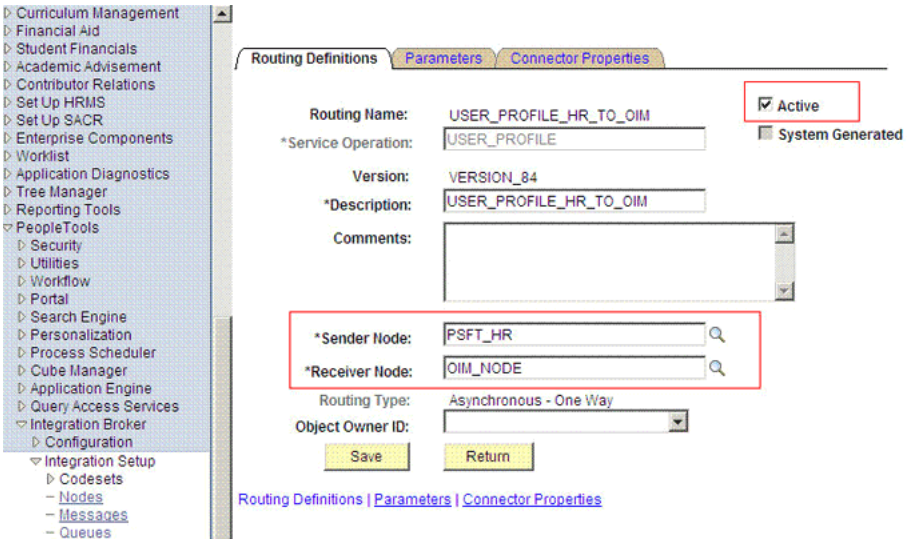
      Default Local Node: **Y**

      Node Type: **PIA**

      Only one node can meet all the above conditions at a time.
   3. Select the node.
   4. Click **Save.**

   Receiver Node: `OIM_NODE`

   The following screenshot displays the Sender and Receiver nodes:



5. Click **Save.**
6. Click **Return** to go back to the Routings tab of the Service Operation and verify whether your routing is active.

Configuring the DELETE_USER_PROFILE Service Operation

The DELETE_USER_PROFILE message contains information about user accounts that have been deleted. To configure the DELETE_USER_PROFILE service operation perform the following procedures:

> **Note:** The procedure remains the same for PeopleTools 8.49 and for PeopleTools 8.50. The screenshots are taken on PeopleTools 8.49 version.

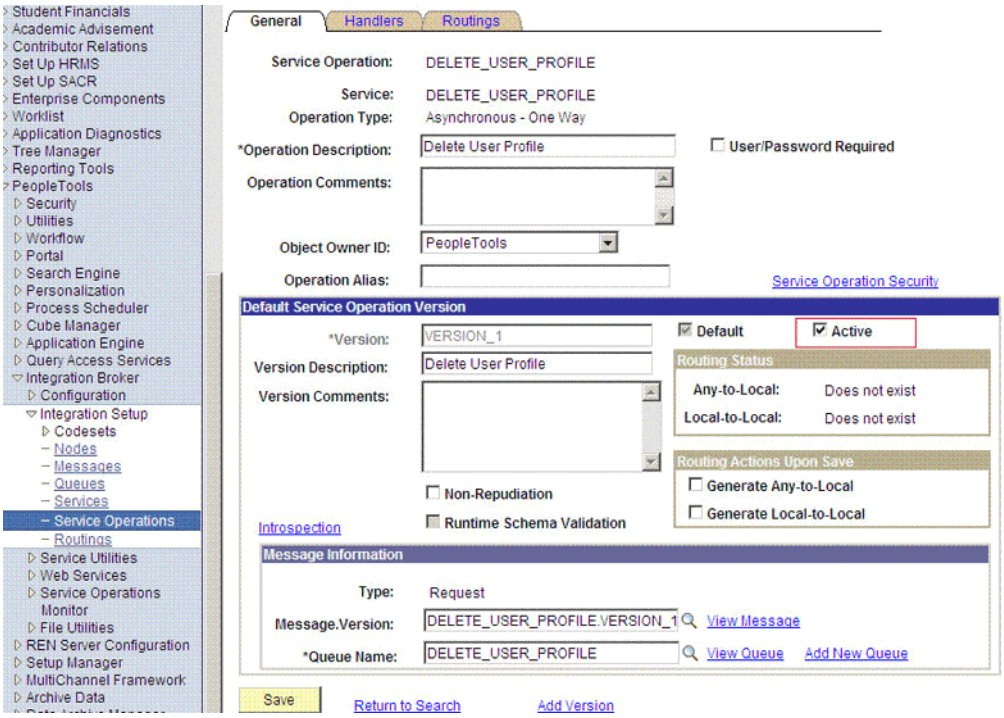
- Activating the DELETE_USER_PROFILE Service Operation
- Verifying the Queue Status for the DELETE_USER_PROFILE Service Operation
- Setting Up the Security for the DELETE_USER_PROFILE Service Operation
- Defining the Routing for the DELETE_USER_PROFILE Service Operation

Activating the DELETE_USER_PROFILE Service Operation

To activate the DELETE_USER_PROFILE service operation:

1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
2. On the Find Service Operation tab, enter `DELETE_USER_PROFILE` in the **Service** field, and then click **Search.**
3. Click the **DELETE_USER_PROFILE** link.
4. In the Default Service Operation Version region, click **Active.**

   The following screenshot displays the Active check box:



5. Click **Save.**

Verifying the Queue Status for the DELETE_USER_PROFILE Service Operation

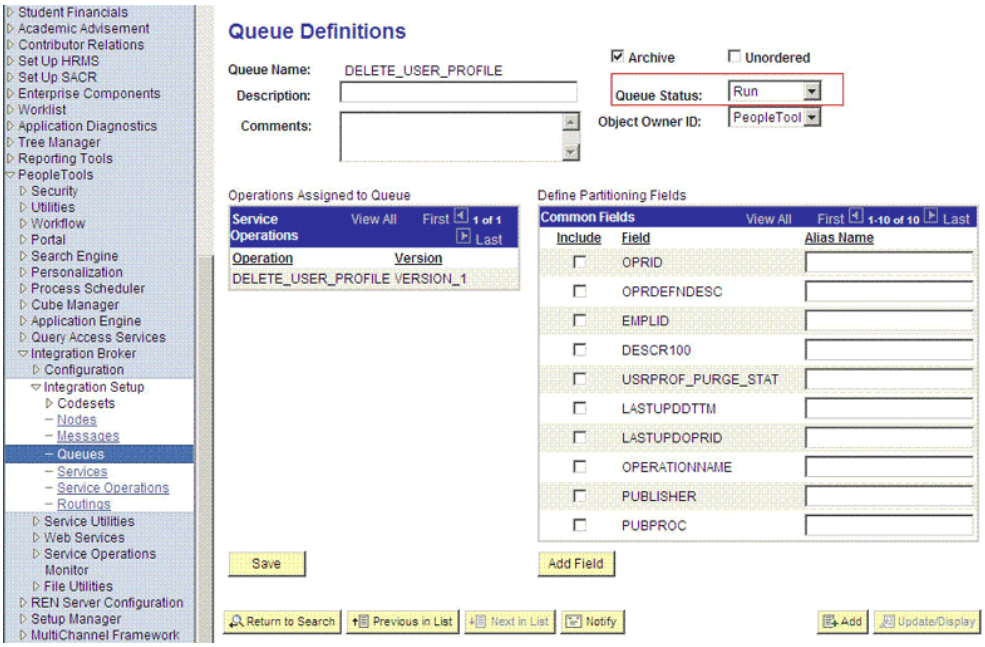
To ensure that the status of the queue for the DELETE_USER_PROFILE service operation is Run:

1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Queues.**
2. Search for the **DELETE_USER_PROFILE** queue.
3. In the Queue Status List, ensure that **Run** is selected.

Note: If the queue status is not Run:

1. From the Queue Status list, select **Run.**
2. Click **Save.**

The following screenshot displays the queue status:



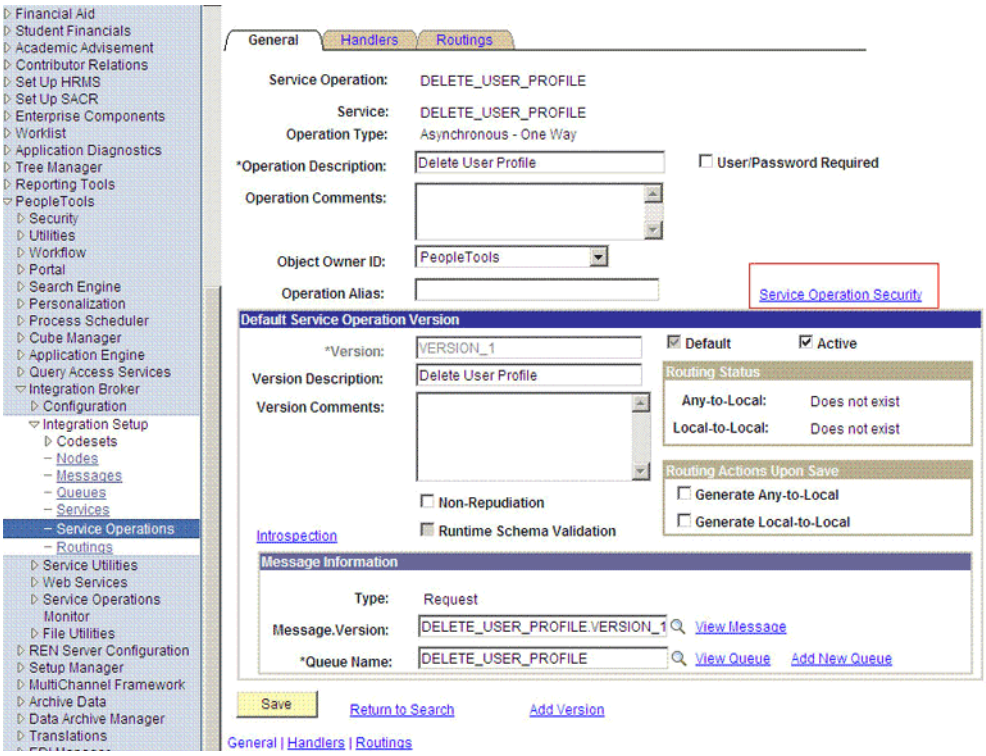
4. Click **Return to Search.**

Setting Up the Security for the DELETE_USER_PROFILE Service Operation

To set up the security for the DELETE_USER_PROFILE service operation:

1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
2. Search for and open the **DELETE_USER_PROFILE** service operation.
3. On the General tab, click the **Service Operation Security** link.

   The link is shown in the following screenshot:



4. Attach the permission list **OIMUM,** created as a part of the preinstalltion, in Step 3, (See Section 2.1.2.2.1, "Creating a Permission List") to the USER_PROFILE service operation.

   To attach the permission list:

   Note: This procedure describes how to grant access to the OIMUM permission list. The OIMUM permission list is used as an example. However, to implement this procedure, you must use the permission list (attached through a role) to the user profile of the actual user who maintains the user profile information.

   a. Click the plus sign (+) to add a row for the Permission List field.

   b. In the Permission List field, enter **OIM** and then click the Look up Permission List icon.

      The **OIMUM** permission list appears.

   c. From the Access list, select **Full Access.**

      The following screenshot displays the Access list:

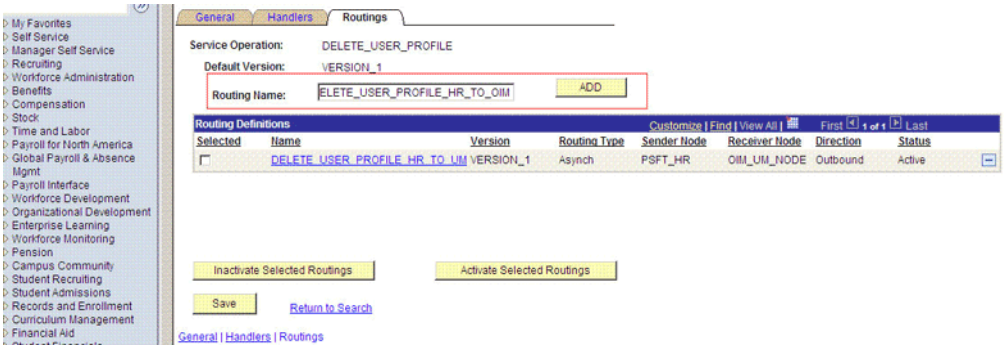
d. Click **Save.**

e. Click **Return to Search.**

Defining the Routing for the DELETE_USER_PROFILE Service Operation

To define the routing for the DELETE_USER_PROFILE service operation:

1. On the Routing tab, enter `DELETE_USER_PROFILE_HR_TO_OIM` as the routing name and then click **Add.** The following screenshot displays the routing information:



2. On the Routing Definition tab, enter the following:

   Sender Node: `PSFT_HR`

   Note: The sender node is the default active local node. To locate the sender node:

   1. Click the Look up icon.
   2. Click **Default** to sort the results in descending order.

      The default active local node should meet the following criteria:

      Local Node: **1**

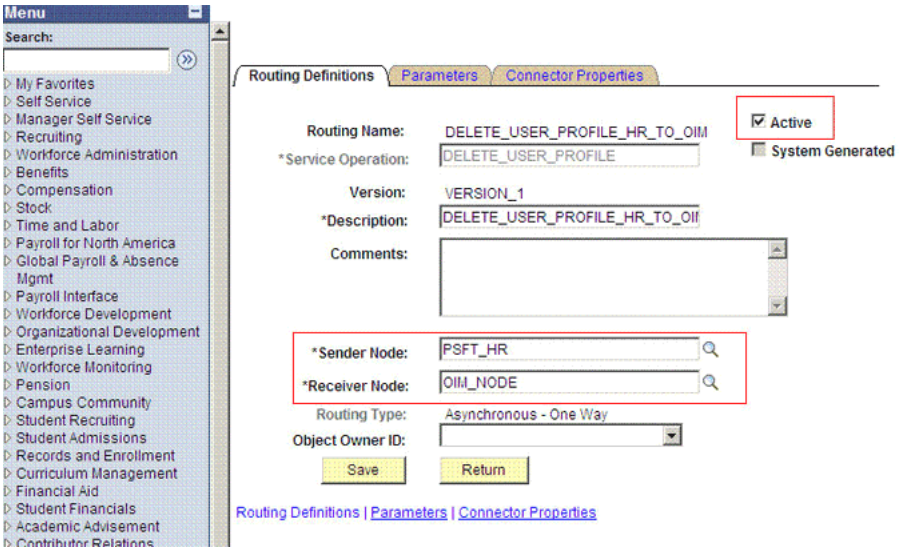
      Default Local Node: **Y**

      Node Type: **PIA**

      Only one node can meet all the above conditions at a time.
   3. Select the node.
   4. Click **Save**.

   Receiver Node: `OIM_NODE`

   The following screenshot displays the Sender and Receiver nodes:



3. Click **Save.**
4. Click **Return** to go back to the Routings tab of the Service Operation, and verify whether your routing is active.

2.2.2.3.3 Preventing Transmission of Unwanted Fields During Incremental Reconciliation

By default, Peoplesoft messages contain fields that are not needed in Oracle Identity Manager. If there is a strong use case that these fields should not be published to Oracle Identity Manager, then do the following:

Locate if there are any local-to-local or local-to-third party PeopleSoft active routings for the service operations using the message under study.

- If none, then you can safely remove the unwanted fields at message level. See "Removing Unwanted Fields at Message Level" section for more information.
- If active routings exist, analyze the subscription or handler code of the routing to determine the fields they are utilizing and the ones not needed in Oracle Identity Manager. If so, remove the unwanted fields at message level. See "Removing Unwanted Fields at Message Level" section for more information.
- Lastly, if there are active routings that use these sensitive fields that you do not want to transmit to Oracle Identity Manager, then you need to write a transformation.

  For more information about implementing transformation, refer to Chapter 21 of Integration Broker PeopleBook on Oracle Technology Network at the following location

  `http://download.oracle.com/docs/cd/E13292_01/pt849pbr0/eng/psbooks/tibr/book.htm`

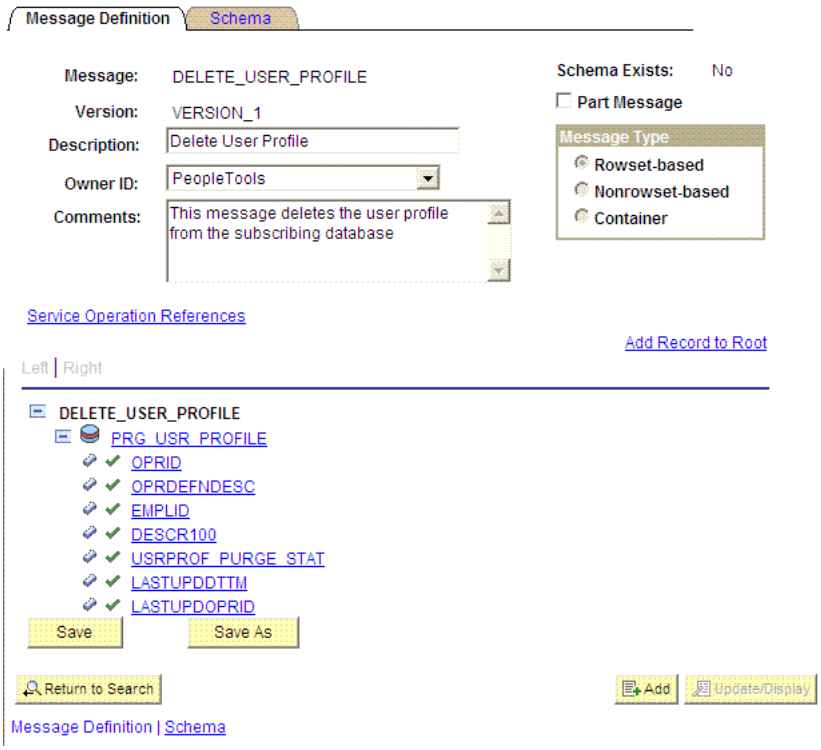
  In addition, refer to Chapter 43 of PeopleCode API Reference PeopleBook on Oracle Technology Network at the following location

  `http://download.oracle.com/docs/cd/E13292_01/pt849pbr0/eng/psbooks/tpcr/book.htm`

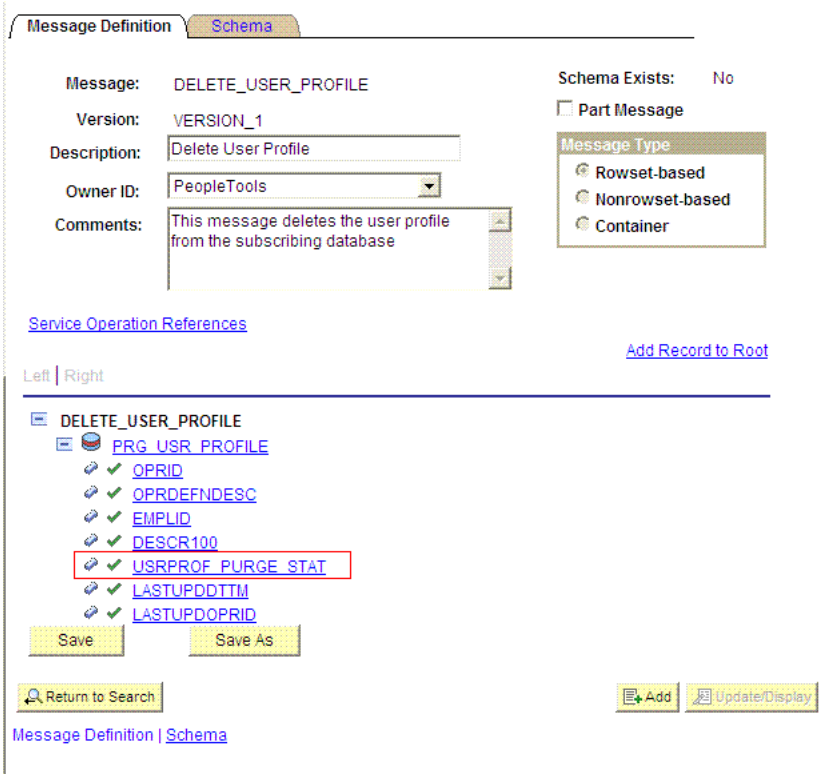
Removing Unwanted Fields at Message Level

1. Expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Messages.**

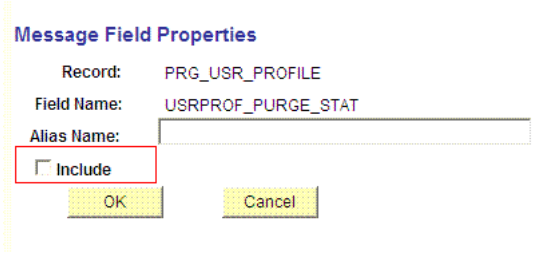
2. Search for and open the desired message, for example, DELETE_USER_PROFILE.VERSION_1 used for incremental reconciliation.
3. Expand the message.



4. Navigate to the field that you do not want to transmit to Oracle Identity Manager, for example, USRPROF_PRG_STAT.



5. Click the field and clear the **Include** check box.



6. Click **OK,** return and save the message.

2.2.2.4 Configuring the Target System for Provisioning

To configure the target system for provisioning, create the APIs for the component interface as follows:

1. To open the Application Designer, click **Start** and then select **Programs, Peoplesoft8.*x***, and **Application Designer.**
2. On the Application Designer page, click **Open** from the **File** menu.
3. In the Open Definition dialog box, select **Component Interface** from the **Definition** list.
4. Enter `USER_PROFILE` in the **Name** field, and then press **Enter.**

   All the component interfaces with names that start with `USER_PROFILE` are displayed in the Open Definition dialog box.
5. Double-click the **USER_PROFILE** entry.

If you are not authorized to perform any action on the USER_PROFILE component interface:

a. Log in to Application Designer with administrator credentials.

b. From the **Go** menu, select **Definition Security.**

   A new console, PS Definition Security appears.

c. From the **File** menu, select **Open,** and then select **Group.**

   The Definition Security Open dialog box appears.

d. From the Group ID list, select **PEOPLETOOLS,** and then click **OK.**

   The PS Definition Security - Group ID : PEOPLETOOLS window appears.

e. From the list, select **Component Interfaces.**

f. From the **Component Interfaces** list, select **USER_PROFILE** and **DELETE_USER_PROFILE.** Click the right arrow to move these to the **Excluded Component Interfaces:** list.

g. From the File menu, select **Save.**

6. From the File menu, select **Open.**

   The Open Definition window appears.

7. In the Name field, enter `USER_PROFILE`, and then click **Open.**

   The properties of the `USER_PROFILE` component interface are displayed in the **Definition matching selection criteria:** region.

8. Double-click the **USER_PROFILE** entry.

9. From the Build menu, select **PeopleSoft APIs.** The Build PeopleSoft API Bindings dialog box is displayed.

10. In the Java Classes region of the Build PeopleSoft API Bindings dialog box, select the **Build** check box.

    Note: Ensure that the other check boxes are unchecked.

11. From the **Select APIs to Build** list, select the following APIs:

    - CompIntfc.CompIntfcPropertyInfo
    - CompIntfc.CompIntfcPropertyInfoCollection
    - PeopleSoft.CompintfcCollection
    - PeopleSoft.Property
    - PeopleSoft.PropertyList
    - PeopleSoft.PSMessage
    - PeopleSoft.PSMessageCollection
    - PeopleSoft.RegionalSettings
    - PeopleSoft.Session
    - PeopleSoft.TraceSettings
    - CompIntfc.DELETE_USER_PROFILE

- CompIntfc.DELETE_USER_PROFILECollection
- APIs with names that start with CompIntfc.USER_PROFILE

12. In the **Target Directory** field, enter the path for the directory where you want to create the Java API classes, and then click **OK.**
13. Ensure that the psjoa.jar file is included in the CLASSPATH environment variable. This file is located in the *PEOPLESOFT_HOME*/web/psjoa directory.
14. Compile the APIs from the target directory specified in Step 11. To do so:
    a. Specify the JAVA_HOME environment variable.
    b. In the command prompt, run the following command in the directory that you specified in Step 10 of this procedure:

```
%JAVA_HOME%\bin\javac PeopleSoft\Generated\CompIntfc\*.java
```

> **Note:** You must ensure that the OC4J JDK version and Oracle Identity Manager JDK version are same, for example, create a peoplesoft.jar with JAVA_HOME set to JDK 1.5 as used in OC4J.

15. Bundle the compiled class files into a JAR file named peoplesoft.jar, as follows:
    a. Copy all the .class files into the following directory:

    temp\PeopleSoft\Generated\CompIntfc

> **Note:** This directory should contain only .class files.

    b. Run the following command from the temp directory:

```
jar -cvf peoplesoft.jar *.*
```

2.2.2.5 Configuring Oracle Identity Manager Server as a Non-Proxy Host on PeopleSoft Server

To configure Oracle Identity Manager server as a non-proxy host on PeopleSoft server:

1. Update PT_HOME/webserv/INSTANCE_NAME/bin/setEnv.sh file with OIM server value for the following parameter:

```
HTTP_PROXY_NONPROXY_HOSTS=OIM_SERVER_HOST_NAME
```

2. Update integrationGateway.properties, for example, /slot/ems1725/appmgr/pt850/webserv/h91c306/applications/peoplesoft/PSIGW.war/WEB-INF file with the following parameter:

```
ig.nonProxyHosts=OIM_SERVER_HOST_NAME
```

2.3 Postinstallation

Postinstallation information is divided across the following sections:

- Section 2.3.1, "Postinstallation on Oracle Identity Manager"
- Section 2.3.2, "Postinstallation on the Target System"

2.3.1 Postinstallation on Oracle Identity Manager

Postinstallation on Oracle Identity Manager consists of the following procedures:

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

- Section 2.3.1.1, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.1.2, "Enabling Logging"
- Section 2.3.1.3, "Setting Up the Lookup.PSFT.UM.ExclusionList Lookup Definition"
- Section 2.3.1.4, "Setting Up the Lookup.PSFT.UM.UserProfile.UserStatus Lookup Definition"
- Section 2.3.1.5, "Setting Up the Lookup.PSFT.Configuration Lookup Definition"
- Section 2.3.1.6, "Setting Up the Lookup.PSFT.UM.AttrMap.IDTypes Lookup Definition"
- Section 2.3.1.7, "Configuring SSL"
- Section 2.3.1.9, "Enabling Request-Based Provisioning"

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

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager release 9.1.0.*x* and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/bin directory.

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

For Oracle Identity Manager release 9.1.0.*x*:

OIM_HOME/xellerate/bin/*SCRIPT_FILE_NAME*

For Oracle Identity Manager release 11.1.1:

OIM_HOME/server/bin/*SCRIPT_FILE_NAME*

2. Enter one of the following commands:

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

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

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

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

  On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`

  On UNIX: `PurgeCache.sh ConnectorResourceBundle`

  Note: You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

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

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

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

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

  In this format:

- Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

  Sample value: `t3://localhost:8003`

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

2.3.1.2 Enabling Logging

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

- Section 2.3.1.2.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"
- Section 2.3.1.2.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.3.1.2.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.*x*

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

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

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

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

The file in which you set the log level depends on the application server that you use:

- **IBM WebSphere Application Server**

To enable logging:

1. Make the following changes in the *OIM_HOME*/xellerate/config/log.properties:
   - Search for the following line:

     ```
     log4j.rootLogger=WARN,stdout
     ```

     Make this line a comment and remove the comment from the line preceding this line.
   - Locate and remove the comment from following lines:

     ```
     #log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
     #log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
     #log4j.appender.logfile.File=DIRECTORY_PATH/xel.log
     #log4j.appender.logfile.MaxBackupIndex=20
     #log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
     #log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
     ```

2. Specify the name and the location of the file to which the preceding logs have to be written. You can do this by changing the value of the following line:

   ```
   log4j.appender.logfile.File=c:/oracle/xellerate/logs/xel.log
   ```

   Replace `c:/oracle/xellerate/logs` with a valid directory location.
3. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

   ```
   log4j.logger.OIMCP.PSFTUM=log_level
   log4j.logger.OIMCP.PSFTCOMMON=LOG_LEVEL
   ```

4. In this line, replace *log_level* with the log level to set.

   For example:

   ```
   log4j.logger.OIMCP.PSFTUM=DEBUG
   log4j.logger.OIMCP.PSFTCOMMON=DEBUG
   ```

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

DIRECTORY_PATH/xel.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/jboss-log4j.xml file, add the following lines:

     ```
     <category name="OIMCP.PSFTUM">
        <priority value="log_level"/>
     </category>
     <category name="OIMCP.PSFTCOMMON">
        <priority value="LOG_LEVEL"/>
     </category>
     ```

     In an Oracle Identity Manager cluster, make the changes in the following file:

     ```
     JBOSS_HOME/server/all/conf/jboss-log4j.xml
     ```

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

```
<category name="OIMCP.PSFTUM">
   <priority value="DEBUG"/>
</category>
<category name="OIMCP.PSFTCOMMON">
   <priority value="DEBUG"/>
</category>
```

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

```
JBOSS_HOME\server\default\log\server.log
```

In an Oracle Identity Manager cluster, the log information is written to the following file:

```
JBOSS_HOME\server\all\log\server.log
```

- **Oracle WebLogic Server**

  To enable logging:

  1. Make the following changes in the *OIM_HOME*/xellerate/config/log.properties:
     - Search for the following line:

       ```
       log4j.rootLogger=WARN,stdout
       ```

       Make this line a comment and remove the comment from the line preceding this line.
     - Locate and remove the comment from the following lines:

       ```
       #log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
       #log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
       #log4j.appender.logfile.File=DIRECTORY_PATH/xel.log
       #log4j.appender.logfile.MaxBackupIndex=20
       #log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
       #log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
       ```

  2. Specify the name and the location of the file to which the preceding logs have to be written. You can do this by changing the value of the following line:

     ```
     log4j.appender.logfile.File=c:/oracle/xellerate/logs/xel.log
     ```

     Replace `c:/oracle/xellerate/logs` with a valid directory location.
  3. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.OIMCP.PSFTUM=log_level
     ```

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

     For example:

     ```
     log4j.logger.OIMCP.PSFTUM=DEBUG
     ```

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

  ```
  DIRECTORY_PATH/xel.log
  ```

- **Oracle Application Server**

  To enable logging:

1. Make the following changes in the *OIM_HOME*/xellerate/config/log.properties:
   - Search for the following line:

     ```
     log4j.rootLogger=WARN,stdout
     ```

     Make this line a comment and remove the comment from the line preceding this line.
   - Locate and remove the comment from following lines:

     ```
     #log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
     #log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
     #log4j.appender.logfile.File=DIRECTORY_PATH/xel.log
     #log4j.appender.logfile.MaxBackupIndex=20
     #log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
     #log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
     ```

2. Specify the name and the location of the file to which the preceding logs have to be written. You can do this by changing the value of the following line:

   ```
   log4j.appender.logfile.File=c:/oracle/xellerate/logs/xel.log
   ```

   Replace `c:/oracle/xellerate/logs` with a valid directory location.
3. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

   ```
   log4j.logger.OIMCP.PSFTUM=log_level
   log4j.logger.OIMCP.PSFTCOMMON=LOG_LEVEL
   ```

4. In this line, replace *log_level* with the log level to set.

   For example:

   ```
   log4j.logger.OIMCP.PSFTUM=DEBUG
   log4j.logger.OIMCP.PSFTCOMMON=DEBUG
   ```

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

DIRECTORY_PATH/xel.log

2.3.1.2.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

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

Oracle Identity Manager release 11.1.1 uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.
- SEVERE

  This level enables logging of information about errors that may 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 message types are mapped to ODL message type and level combinations as shown in Table 2–5.

Table 2–5 Log Levels and ODL Message Type:Level Combinations

Java 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_SEVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

```
<log_handler name='psft-um-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="OIMCP.PSFTCOMMON" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="psft-um-handler"/>
```

```
    <handler name="console-handler"/>
  </logger>

<logger name="OIMCP.PSFTUM" level="[LOG_LEVEL]" useParentHandlers="false">
<handler name="psft-um-handler"/>
<handler name="console-handler"/>
</logger>
```

b. Replace all occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–5 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='psft-um-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\o
im_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="OIMCP.PSFTCOMMON" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="psft-um-handler"/>
     <handler name="console-handler"/>
   </logger>

<logger name="OIMCP.PSFTUM" level="NOTIFICATION:1"
useParentHandlers="false">
<handler name="psft-um-handler"/>
<handler name="console-handler"/>
</logger>
```

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

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

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

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

4. Restart the application server.

2.3.1.3 Setting Up the Lookup.PSFT.UM.ExclusionList Lookup Definition

In the Lookup.PSFT.UM.ExclusionList lookup definition, enter the user IDs of target system accounts for which you do not want to perform reconciliation and provisioning. See Section 1.5.2.3.4, "Lookup.PSFT.UM.ExclusionList" for more information about this lookup definition.

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the **Lookup.PSFT.UM.ExclusionList** lookup definition.
3. Click **Add.**

> **Note:** The Code Key represents the resource object field name on which the exclusion list is applied during reconciliation. In provisioning, the exclusion list is applied to User Id (OPRID), by default.

4. In the Code Key and Decode columns, enter the first user ID to exclude.
5. Repeat Steps 3 and 4 for all the user IDs to exclude.

   For example, if you do not want to provision users with user ID 's User001, User002, and User088 then you must populate the lookup definition with the following values:

Code Key	Decode
User ID	User001~User002~User088

6. Click the Save icon.

2.3.1.4 Setting Up the Lookup.PSFT.UM.UserProfile.UserStatus Lookup Definition

The lookup provides the mapping between the ACCTLOCK node in the USER_PROFILE message XML and the status to be shown on Oracle Identity Manager for the employee. See Section 1.5.2.1.4, "Lookup.PSFT.UM.UserProfile.UserStatus" for more information about this lookup definition.

You can change the Decode value in this lookup definition for the Code Key value to modify the status of the provisioned resource. For example, you can change the Decode value from `Enabled` to `Provisioned` for the Code Key value, `0` defined in this lookup definition. This enables you to modify the status of the provisioned resource from enabled to provisioned.

To modify or set the Decode value in this lookup definition:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the Lookup.PSFT.UM.UserProfile.UserStatus lookup definition.
3. Click **Add.**
4. In the Decode column for the Code Key, enter the following value.

   Code Key: 0

Decode: Provisioned

5. Click the Save icon.

2.3.1.5 Setting Up the Lookup.PSFT.Configuration Lookup Definition

Every standard PeopleSoft message has a message-specific configuration defined in the Lookup.PSFT.Configuration lookup definition. See Section 1.5.2.3.1, "Lookup.PSFT.Configuration" for more information about this lookup definition.

For example, the mapping for the USER_PROFILE message in this lookup definition is defined as follows:

Code Key: USER_PROFILE

Decode: Lookup.PSFT.Message.UserProfile.Configuration

You can configure the message names, such as USER_PROFILE and DELETE_USER_PROFILE, defined in this lookup definition.

Consider a scenario in which the target system sends the USER_PROFILE.VERSION_3 message. You must change the Code Key value in this lookup definition to implement the message sent by the target system.

To modify or set the Code Key value:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the **Lookup.PSFT.Configuration** lookup definition.
3. Click **Add.**
4. In the Code Key column, enter the name of the message you want to modify. In this scenario, define the mapping as follows:

   Code Key: USER_PROFILE.VERSION_3

   Decode: Lookup.PSFT.Message.UserProfile.Configuration
5. Repeat Steps 3 and 4 to rename the DELETE_USER_PROFILE message name.
6. Click the Save icon.

2.3.1.6 Setting Up the Lookup.PSFT.UM.AttrMap.IDTypes Lookup Definition

If you are using PeopleTools 8.5*x* as the target system, then you must modify the decode values for the Employee ID, Customer Set ID, and Vendor Set ID attribute names in the Lookup.PSFT.UM.AttrMap.IDTypes lookup definition as follows:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the **Lookup.PSFT.UM.AttrMap.IDTypes** lookup definition.
3. Search for the **UD_PSFT_BAS_EmplID** code key and change its decode value to `Empl ID.`
4. Search for the **UD_PSFT_BAS_CUSTSetID** code key and change its decode value to `Set ID.`
5. Search for the **UD_PSFT_BAS_VNDSetID** code key and change its decode value to `Set ID.`
6. Click the Save icon.

2.3.1.7 Configuring SSL

The following sections describe the procedure to configure SSL connectivity between Oracle Identity Manager and the target system:

- Section 2.3.1.7.1, "Configuring SSL on IBM WebSphere Application Server"
- Section 2.3.1.7.2, "Configuring SSL on JBoss Application Server"
- Section 2.3.1.7.3, "Configuring SSL on Oracle WebLogic Server"
- Section 2.3.1.7.4, "Configuring SSL on Oracle Application Server"

2.3.1.7.1 Configuring SSL on IBM WebSphere Application Server You can configure SSL connectivity on IBM WebSphere Application Server with either a self-signed certificate or a CA certificate. The following sections describe this:

- Configuring SSL on IBM WebSphere Application Server with a Self-Signed Certificate
- Configuring SSL on IBM WebSphere Application Server with a CA Certificate

Configuring SSL on IBM WebSphere Application Server with a Self-Signed Certificate

To configure SSL connectivity between Oracle Identity Manager on IBM WebSphere Application Server and the target system with a self-signed certificate, you must perform the following tasks:

1. Log in to the WebSphere Integrated Solutions Console. The URL may be similar to the following:

   `https://localhost:9043/ibm/console/logon.jsp`

2. Click **Security, SSL certificate and key management, Related items, Key stores and certificates, NodeDefaultKeyStore,** and then click **Personal certificates.**
3. Click **Create a self-signed certificate.**
4. In the **Alias** field, enter an alias name. You specify the alias name to identify the certificate request in the keystore.
5. In the CN field, enter a value for common name. The common name must be the fully-qualified DNS host name or the name of the computer. The CN of the certificate must match the domain name or the name of the computer. For example, if the name of your domain is us.example.com, then the CN of the SSL certificate that you create for your domain must also be us.example.com.
6. In the **Organization** field, enter an organization name.
7. In the **Organization unit** field, specify the organization unit.
8. In the **Locality** field, enter the locality.
9. In the **State or Province** field, enter the state.
10. In the **Zip Code** field, enter the zip code.
11. From the **Country or region** list, select the country code.
12. Click **Apply** and then **Save.**
13. Click **Security, SSL certificate and key management, Related items, Key stores and certificates, NodeDefaultKeyStore,** and then click **Personal certificates.**
14. Select the check box for the new alias name.

15. Click **Extract.**
16. Specify the absolute file path where you want to extract the certificate under the certificate file name, for example, C:\SSLCerts\sslcert.cer.
17. Click **Apply** and then click **OK.**

Configuring SSL on IBM WebSphere Application Server with a CA Certificate

To configure SSL connectivity between Oracle Identity Manager on IBM WebSphere Application Server and the target system with a CA certificate, you must perform the following tasks:

1. Log in to the WebSphere Integrated Solutions Console. The URL may be similar to the following:

   ```
   https://localhost:9043/ibm/console/logon.jsp
   ```

2. Click **Security, SSL certificate and key management, Related items, Key stores and certificates, NodeDefaultKeyStore.**
3. On the Additional Properties tab, click **Personal certificate requests.**
4. Click **New.**
5. In the File for certificate request field, enter the full path where the certificate request is to be stored, and a file name, for example, `c:\servercertreq.arm` (for a computer running on Microsoft Windows).
6. In the **Key label** field, enter an alias name. You specify the alias name to identify the certificate request in the keystore.
7. In the CN field, enter a value for common name. The common name must be the fully-qualified DNS host name or the name of the computer. The CN of the certificate must match the domain name of your community. For example, if the name of your domain is us.example.com, then the CN of the SSL certificate that you create for your community must also be us.example.com.
8. In the **Organization** field, enter an organization name.
9. In the **Organization unit** field, specify the organization unit.
10. In the **Locality** field, enter the locality.
11. In the **State or Province** field, enter the state.
12. In the **Zip Code** field, enter the zip code.
13. From the **Country or region** list, select the country code.
14. Click **Apply** and then **Save.** The certificate request is created in the specified file location in the keystore. This request functions as a temporary placeholder for the signed certificate until you manually receive the certificate in the keystore.

    Note: Keystore tools such as iKeyman and keyTool cannot receive signed certificates that are generated by certificate requests from IBM WebSphere Application Server. Similarly, IBM WebSphere Application Server cannot accept certificates that are generated by certificate requests from other keystore utilities.

15. Send the certification request arm file to a CA for signing.

16. Create a backup of your keystore file. You must create this backup before receiving the CA-signed certificate into the keystore. The default password for the keystore is WebAS. The Integrated Solutions Console contains the path information for the location of the keystore. The path to the NodeDefaultKeyStore is listed in the Integrated Solutions Console as:

    was_profile_root\config\cells\cell_name\nodes\node_name\key.p12

    Now, you can receive the CA-signed certificate into the keystore to complete the process of generating a signed certificate for IBM WebSphere Application Server.

To receive a signed certificate issued by a CA, perform the following tasks:

1. In the WebSphere Integrated Solutions Console, click **Security, SSL certificate and key management, Related items, Key stores and certificates, NodeDefaultKeyStore,** and then click **Personal Certificates.**
2. Click **Receive a certificate from a certificate authority.**
3. Enter the full path and name of the certificate file.
4. Select the default data type from the list.
5. Click **Apply** and then **Save.**

The keystore contains a new personal certificate that is issued by a CA. The SSL configuration is ready to use the new CA-signed personal certificate.

2.3.1.7.2 Configuring SSL on JBoss Application Server Before configuring SSL on JBoss Application Server, ensure the following:

- JBoss Application Server is installed on the Oracle Identity Manager host computer
- Java Runtime Environment is installed on the JBoss Application Server host

You can configure SSL connectivity on JBoss Application Server with either a self-signed certificate or a CA certificate. The following sections describe this. If you are configuring SSL on JBoss Application Server with a self-signed certificate, then perform the following tasks:

- Creating a Self-Signed Certificate
- Moving the Keystore
- Updating the Configuration File

If you are configuring SSL on JBoss Application Server with a CA certificate, then perform the following tasks:

- Importing a CA Certificate
- Moving the Keystore
- Updating the Configuration File

Creating a Self-Signed Certificate

To create a self-signed certificate, see "Generating Keystore" on page 2-75.

Importing a CA Certificate

To import a CA certificate, perform the following tasks:

1. Run the following command:

```
keytool -genkey -alias ALIAS_NAME -keystore ABSOLUTE_KEYSTORE_PATH -keyalg
```

```
KEY_ALGORITHM -storepass KEYSTORE_PASSWORD -keypass PRIVATE_KEY_PASS
```

For example:

```
keytool -genkey -alias example088196 -keystore c:\temp\keys\custom.keystore
-keyalg RSA -storepass example1234 -keypass example1234
```

Note:

- The keystore password and the private key password must be the same.
- Typically, the alias is the name or the IP address of the computer on which you are configuring SSL.
- The alias used in the various commands of this procedure must be the same.

2. When prompted, enter information about the certificate, such as company and contact name. This information is displayed to employees attempting to access a secure page in the application. This is illustrated in the following example:

```
What is your first and last name?
  [Unknown]:  Must be the name or IP address of the computer
What is the name of your organizational unit?
  [Unknown]:  example
What is the name of your organization?
  [Unknown]:  example
What is the name of your City or Locality?
  [Unknown]:  New York
What is the name of your State or Province?
  [Unknown]:  New York
What is the two-letter country code for this unit?
  [Unknown]:  US
Is <CN=Name or IP address of the computer, OU=example, O=example, L=New York,
ST=New York, C=US> correct?
  [no]:  yes
```

When you enter yes in the last line of the preceding example, the custom keystore file is created in the c:\temp\keys\ directory.

3. Generate the certificate signing request by running the following command:

```
keytool -certreq -alias ALIAS_NAME -file ABSOLUTE_CSR_PATH  -keystore
ABSOLUTE_KEYSTORE_PATH
```

For example:

```
keytool -certreq -alias example088196 -file c:\temp\keys\certReq.csr -keystore
c:\temp\keys\custom.keystore
```

4. Submit the certReq.csr file on a CA Web site for downloading the CA certificate.

Ensure that your %JAVA_HOME%\jre\lib\security\cacerts has the root certificate of the CA that has generated the CA certificate.

To check all the root certificates that %JAVA_HOME%\jre\lib\security\cacerts contains, run the following command:

```
keytool -list -keystore %JAVA_HOME%\jre\lib\security\cacerts -storepass
cacerts_store_password
```

For example:

```
%JAVA_HOME%\jre\bin\keytool -list -keystore
%JAVA_HOME%\jre\lib\security\cacerts -storepass changeit
```

If the %JAVA_HOME%\jre\lib\security\cacerts keystore does not contain the root certificate of CA that has generated the CA certificate, then you must import the root certificate of CA into %JAVA_HOME%\jre\lib\security\cacerts.

Run the following command to import the root certificate of CA:

```
keytool -import  -alias <cacerts_key_entry_alias> -file <CARootCertificate.cer>
-keystore %JAVA_HOME%\jre\lib\security\cacerts  -storepass
cacerts_store_password
```

For example:

```
keytool -import -alias cakey -file "C:\temp\Thawte Test Root.cer" -keystore
%JAVA_HOME%\jre\lib\security\cacerts -storepass changeit
```

The certificate is added to the keystore.

5. Import the CA certificate by running the following command:

```
keytool -import -alias ALIAS_NAME -keystore ABSOLUTE_KEYSTORE_PATH
-trustcacerts -file ABSOLUTE_CACERT_PATH
```

ABSOLUTE_CACERT_PATH represents the path in which you have stored the certificate downloaded from CA.

For example:

```
keytool -import -alias example088196 -keystore c:\temp\keys\custom.keystore
 -trustcacerts -file c:\temp\keys\CACert.cer
```

When you run this command, you are prompted for the keystore password, as shown:

```
Enter keystore password:  example1234 [Enter]
Owner: CN=Thawte Test CA Root, OU=TEST TEST TEST, O=Thawte Certification,
ST=FOR TESTING PURPOSES ONLY, C=ZA
Issuer: CN=Thawte Test CA Root, OU=TEST TEST TEST, O=Thawte Certification,
ST=FOR TESTING PURPOSES ONLY, C=ZA
Serial number: 0
Valid from: Thu Aug 01 05:30:00 GMT+05:30 1996 until: Fri Jan 01 03:29:59
GMT+05:30 2021
Certificate fingerprints:
         MD5:  5E:E0:0E:1D:17:B7:CA:A5:7D:36:D6:02:DF:4D:26:A4
         SHA1: 39:C6:9D:27:AF:DC:EB:47:D6:33:36:6A:B2:05:F1:47:A9:B4:DA:EA
Trust this certificate? [no]:  yes [Enter]
```

In this example, the instances when you can press Enter are shown in bold.

Moving the Keystore

To move the certificate to a JBoss Application Server directory, copy the generated keystore to the conf directory of your JBoss installation. For example, the directory can be C:\Program Files\jboss-4.0.3\server\default\conf\.

Updating the Configuration File

Before updating the configuration file, shut down JBoss Application Server. The *JBOSS_HOME*/server/default/deploy/jbossweb-tomcat55.sar/server.xml file

contains information about what Web features to enable when the server starts. Inside this file, there is a part that looks similar to the following:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore
<Connector port="8443" address="${jboss.bind.address}"
  maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
  emptySessionPath="true"
  scheme="https" secure="true" clientAuth="false"
  keystoreFile="${jboss.server.home.dir}/conf/chap08.keystore"
  keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
```

In the code, make the following changes:

- Remove the comment from the block of code.
- Change the value of `Connector port` to `443` (default SSL port).
- Change the value of `keystoreFile` to the absolute path of the keystore generated in "Generating Keystore" on page 2-75.
- Change the value of `keystorePass` to the password of the keystore.

After the changes are made, the code block looks similar to the following:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="443" address="${jboss.bind.address}"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/ custom.keystore"
keystorePass=" example1234 " sslProtocol = "TLS" />
<!-- -->
```

SSL is now enabled. You can restart JBoss Application Server and browse to the following URL to verify whether SSL is enabled:

```
https://localhost:443
```

2.3.1.7.3 Configuring SSL on Oracle WebLogic Server You can configure SSL connectivity on Oracle WebLogic Server with either a self-signed certificate or a CA certificate. The following sections describe the procedures:

See Also: Appendix B, "Setting Up SSL on Oracle WebLogic Server"

- Configuring SSL on Oracle WebLogic Server with a Self-Signed Certificate
- Configuring SSL on Oracle WebLogic Server with a CA Certificate

Configuring SSL on Oracle WebLogic Server with a Self-Signed Certificate

To configure SSL connectivity between Oracle Identity Manager on Oracle WebLogic Server and the target system with a self-signed certificate, you must perform the following tasks:

- Generating Keystore
- Configuring Oracle WebLogic Server

Generating Keystore

To generate the keystore:

1. Run the following command:

   ```
   keytool -genkey -keystore ABSOLUTE_KEYSTORE_PATH -alias ALIAS_NAME -keyalg
   KEY_ALGORITHM -storepass KEYSTORE_PASSWORD -keypass PRIVATE_KEY_PASSWORD
   ```

   For example:

   ```
   keytool -genkey -keystore c:\temp\keys\keystore.jks -alias example088196
   -keyalg RSA -storepass example1234 -keypass example1234
   ```

   Note:

   - The keystore password and the private key password must be the same.
   - Typically, the alias is the name or the IP address of the computer on which you are configuring SSL.
   - The alias used in the various commands of this procedure must be the same.

2. When prompted, enter information about the certificate. This information is displayed to users attempting to access a secure page in the application. This is illustrated in the following example:

   ```
   keytool -genkey -keystore c:\temp\keys\keystore.jks -alias example088196
   -keyalg RSA -storepass example1234 -keypass example1234
   What is your first and last name?
     [Unknown]: Must be the name or IP address of the computer
   What is the name of your organizational unit?
     [Unknown]:  example
   What is the name of your organization?
     [Unknown]:  example
   What is the name of your City or Locality?
     [Unknown]:  New York
   What is the name of your State or Province?
     [Unknown]:  New York
   What is the two-letter country code for this unit?
     [Unknown]:  US
   Is <CN=Name or IP address of the computer
   , OU=example, O=example, L=New York, ST=New York, C=US> correct?
     [no]:  yes
   ```

   When you enter yes in the last line of the preceding example, the keystore.jks file is created in the c:\temp\keys\directory.

3. Export the keystore to a certificate file by running the following command:

   ```
   keytool -export -alias ALIAS_NAME -keystore ABSOLUTE_KEYSTORE_PATH -file
   CERTIFICATE_FILE_ABSOLUTE_PATH
   ```

   For example:

   ```
   keytool -export -alias example088196 -keystore c:\temp\keys\keystore.jks -file
   c:\temp\keys\keystore.cert
   ```

4. When prompted for the private key password, enter the same password used for the keystore, for example, `example1234`.

5. Import the keystore by running the following command:

```
keytool -import -alias ALIAS_NAME -keystore NEW_KEYSTORE_ABSOLUTE_PATH -file
CERTIFICATE_FILE_ABSOLUTE_PATH
```

For example:

```
keytool -import -alias example088196 -keystore c:\temp\keys\new.jks -file
c:\temp\keys\keystore.cert
```

When you run this command, it prompts for the keystore password, as shown in the following example:

```
Enter keystore password:  example1234 [Enter]
Trust this certificate? [no]:  yes [Enter]
Certificate was added to keystore
```

In this example, the instances when you can press Enter are shown in bold.

Configuring Oracle WebLogic Server

After generating and importing the keystore, start Oracle WebLogic Server. To configure Oracle WebLogic Server:

1. Log in to the Oracle WebLogic Server console at `http://localhost:7001/console` and perform the following:
   a. Expand the servers node and select the **oim** server instance.
   b. Select the **General** tab.
   c. Select the **SSL Listen Port Enabled** option.
   d. Ensure that a valid port is specified in the SSL Listen Port field. The default port is 7002.
   e. Click **Apply** to save your changes.
2. Click the **Keystore & SSL** tab, and then click **Change.**
3. From the Keystores list, select **Custom identity And Java Standard Trust,** and then click **Continue.**
4. Configure the keystore properties. To do so:
   a. In the Custom Identity Key Store File Name column, specify the full path of the keystore generated in Step 1 of "Generating Keystore" on page 2-75, for example, `c:\temp\keys\keystore.jks`. In the Custom Identity Key Store Type column, specify the type of keystore, for example, `JKS`. In the Custom Identity Key Store Pass Phrase and Confirm Custom Identity Key Store Pass Phrase columns, specify the keystore password.
   b. Provide the Java standard trust keystore pass phrase and the Confirm Java standard trust keystore pass phrase. The default password is `changeit`.
   c. Click **Continue.**
5. Specify the private key alias, pass phrase and the confirm pass phrase as the keystore password. Click **Continue.**
6. Click **Finish.**
7. Restart Oracle WebLogic Server. If the server starts successfully with the SSL configuration, then lines similar to the following are recorded in the startup log:

```
<Apr 21, 2008 2:35:43 PM GMT+05:30> <Notice> <WebLogicServer> <BEA-000355>
<Thread "ListenThread.Default" listening on port 7001, ip address *.*>
<Apr 21, 2008 2:35:43 PM GMT+05:30> <Notice> <WebLogicServer> <BEA-000355>
```

```
<Thread "SSLListenThread.Default" listening on port 7002, ip address *.*>
```

Note: The default SSL port for Oracle WebLogic Server is 7002.

Configuring SSL on Oracle WebLogic Server with a CA Certificate

To configure SSL connectivity between Oracle Identity Manager on Oracle WebLogic Server and the target system with a CA certificate, you must perform the following tasks:

Note: Although this is an optional step in the deployment procedure, Oracle strongly recommends that you configure SSL communication between the target system and Oracle Identity Manager.

- Generating Keystore
- Configuring Oracle WebLogic Server

Generating Keystore

The connector requires Certificate Services to be running on the host computer. To generate the keystore:

1. Run the following command:

   ```
   keytool -genkey -keystore ABSOLUTE_KEYSTORE_PATH -alias ALIAS_NAME -keyalg
   KEY_ALGORITHM -storepass KEYSTORE_PASSWORD -keypass PRIVATE_KEY_PASSWORD
   ```

   For example:

   ```
   keytool -genkey -keystore c:\temp\keys\keystore.jks -alias example088196
   -keyalg RSA -storepass example1234 -keypass example1234
   ```

   Note:

   - The keystore password and the private key password must be the same.
   - Typically, the alias name is the name or the IP address of the computer on which you are configuring SSL.

2. When prompted, enter information about the certificate. This information is displayed to users attempting to access a secure page in the application. This is illustrated in the following example:

   ```
   keytool -genkey -keystore c:\temp\keys\keystore.jks -alias example088196
   -keyalg RSA -storepass example1234 -keypass example1234
   What is your first and last name?
     [Unknown]:  Must be the name or IP address of the computer
   What is the name of your organizational unit?
     [Unknown]:  example
   What is the name of your organization?
     [Unknown]:  example
   What is the name of your City or Locality?
     [Unknown]:  New York
   ```

```
What is the name of your State or Province?
  [Unknown]:  New York
What is the two-letter country code for this unit?
  [Unknown]:  US
Is <CN=Name or IP address of the computer, OU=example, O=example, L=New York,
ST=New York, C=US> correct?
  [no]:  yes
```

When you enter yes in the last line of the preceding example, the keystore.jks file is created in the c:\temp\keys\directory.

3. Generate the certificate signing request by running the following command:

   ```
   keytool -certreq -keystore ABSOLUTE_KEYSTORE_PATH -alias ALIAS_NAME -keyalg
   KEY_ALGORITHM -file CERTIFICATE_FILE_ABSOLUTE_PATH
   ```

   For example:

   ```
   keytool -certreq -keystore c:\temp\keys\keystore.jks -alias example088196
   -keyalg RSA -file c:\temp\keys\keystore.cert
   ```

   When prompted for the keystore password, enter the same password used for the keystore in Step 1, for example, `example1234`. This stores a certificate request in the file that you specified in the preceding command.

4. Get the certificate from a CA by using the certificate request generated in the previous step, and store the certificate in a file.

5. Export the keystore generated in Step 1 to a new certificate file, for example, myCert.cer, by running the following command:

   ```
   keytool –export –keystore ABSOLUTE_KEYSTORE_PATH -alias alias-name specified in
   step 1 -file CERTIFICATE_FILE_ABSOLUTE_PATH
   ```

   For example:

   ```
   keytool –export –keystore c:\temp\keys\keystore.jks -alias example088196 -file
   c:\temp\keys\myCert.cer
   ```

6. Import the CA certificate to a new keystore by running the following command:

   ```
   keytool -import -alias ALIAS_NAME -file CERTIFICATE_FILE_ABSOLUTE_PATH
   -keystore NEW_KEYSTORE_ABSOLUTE_PATH -storepass KEYSTORE_PASSWORD generated in
   Step 1
   ```

   For example:

   ```
   keytool -import -alias example088196 -file c:\temp\keys\rootCert.cert -keystore
   c:\temp\keys\rootkeystore.jks
   ```

   When you run this command, it prompts for the keystore password, as shown:

   ```
   Enter keystore password:  example1234 [Enter]
   Trust this certificate? [no]:  yes [Enter]
   Certificate was added to keystore
   ```

   In this example, the instances when you can press Enter are shown in bold.

Configuring Oracle WebLogic Server

After creating and importing the keystore to the system, start Oracle WebLogic Server. To configure Oracle WebLogic Server:

1. Log in to the Oracle WebLogic Server console (http://*localhost*:7001/console) and perform the following:
   a. Expand the server node and select the server instance.
   b. Select the **General** tab.
   c. Select the **SSL Port Enabled** option.
   d. Ensure that a valid port is specified in the SSL Listen Port field. The default port is 7002.
   e. Click **Apply** to save your changes.
2. Click the **Keystore & SSL** tab, and click the **Change** link.
3. From the Keystores list, select **Custom Identity And Custom Trust,** and then click **Continue.**
4. Configure the keystore properties. To do so:
   a. In the Custom Identity Key Store File Name column, specify the full path of the keystore generated in Step 1 of "Generating Keystore" on page 2-78, for example, `c:\temp\keys\keystore.jks`. In the Custom Identity Key Store Type column, specify the type of keystore, for example, `JKS`. In the Custom Identity Key Store Pass Phrase and Confirm Custom Identity Key Store Pass Phrase columns, specify the keystore password.
   b. In the Custom Trust and Custom Trust Key Store File Name column, specify the full path of the keystore generated in Step 1 of "Generating Keystore" on page 2-78, for example, `c:\temp\keys\rootkeystore.jks`. In the Custom Trust Key Store Type column, specify the type of keystore, for example, `JKS`. In the Custom Trust Key Store Pass Phrase and Confirm Custom Trust Key Store Pass Phrase columns, specify the keystore password.
   c. Provide the Java standard trust keystore password. The default password is `changeit`.
   d. Click **Continue.**
5. Specify the alias name and private key password. Click **Continue.**
6. Click **Finish.**
7. Restart Oracle WebLogic Server. If the server starts successfully with the SSL configuration, then lines similar to the following are recorded in the startup log:

```
<Apr 21, 2008 2:35:43 PM GMT+05:30> <Notice> <WebLogicServer> <BEA-000355>
<Thread "ListenThread.Default" listening on port 7001, ip address *.*>
<Apr 21, 2008 2:35:43 PM GMT+05:30> <Notice> <WebLogicServer> <BEA-000355>
<Thread "SSLListenThread.Default" listening on port 7002, ip address *.*>
```

Note: The default SSL port for Oracle WebLogic Server is 7002.

2.3.1.7.4 Configuring SSL on Oracle Application Server

See "Oracle Application Server Administrator's Guide" for information about Configuring SSL on Oracle Application server.

2.3.1.8 Configuring SoD

This section discusses the following procedures for configuring SoD on Oracle Identity Manager release 11.1.1.3 BP02:

- Section 2.3.1.8.1, "Configuring the Oracle Applications Access Controls Governor to Act As the SoD Engine"
- Section 2.3.1.8.2, "Specifying a Value for the TopologyName IT Resource Parameter"
- Section 2.3.1.8.3, "Registering PeopleSoft and Oracle Application Access Controls Governor Instance in Oracle Identity Manager"
- Section 2.3.1.8.4, "Updating OAACG IT Resource Instance"
- Section 2.3.1.8.5, "Disabling and Enabling SoD"

2.3.1.8.1 Configuring the Oracle Applications Access Controls Governor to Act As the SoD Engine See the "Configuring Oracle Application Access Controls Governor" section of the "Configuring SoD Validation" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about this procedure.

2.3.1.8.2 Specifying a Value for the TopologyName IT Resource Parameter The TopologyName IT resource parameter holds the name of the combination of the following elements that you want to use for SoD validation of entitlement provisioning operations:

- Oracle Identity Manager installation
- Oracle Applications Access Controls Governor installation
- PeopleSoft installation

The value that you specify for the TopologyName parameter must be the same as the value of the topologyName element in the SILConfig.xml file. For Oracle Identity Manager release 11.1.1, if you are using default SIL registration, then specify `oaacgpsft` as the value of the topologyName parameter.

For more information about this element, see the "Configuring SoD Validation" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

See Section 2.2.1.3, "Configuring the IT Resource" section for information about specifying values for parameters of the IT resource.

To specify a value for TopologyName in the IT resource:

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. Click **Configuration**, **Manage IT Resource**. The Manage IT Resource page is displayed.
4. Search for and edit "PSFT Server" IT resource or open any IT resource, which you have configured for PeopSoft User Management Connector.
5. In the Topology Name attribute, enter **oaacgpsft**.
6. Click **Save**.

2.3.1.8.3 Registering PeopleSoft and Oracle Application Access Controls Governor Instance in Oracle Identity Manager To register PeopleSoft and Oracle Application Access Controls Governor (OAACG) instance in Oracle Identity Manager:

1. Register a new PeopleSoft and OAACG instance using the command:

   $OIM_HOME/server/bin/registration.sh

   The following snippet shows the example commands for registration:

```
[JohnDoe@adc2190420 bin]$ ./registration.sh
Enter data related to login to OIM Server
[Enter the admin username:]xelsysadm
[Enter the admin password:]
[Enter the service url : (i.e.: t3://oimhostname:oimportno)]t3://adc2190420.us.oracle.com:8002
Do you want to proceed with registration? (y/n)
y
Register System Instance for type OIM ?(y/n)
n
Register System Instance for type EBS ?(y/n)
n
Register System Instance for type PSFT ?(y/n)
y
Provide instance name
PSFT
Register System Instance for type OAACG ?(y/n)
y
Provide instance name
PSFT-OAACG-ITRes
OIM ITResource Instance Name:
PSFT-OAACG-ITRes
Register System Instance for type SAP ?(y/n)
n
Register System Instance for type GRC ?(y/n)
n
Register System Instance for type OIM SDS ?(y/n)
n
Register System Instance for type OIA ?(y/n)
n
```

2. Print the registration IDs of the registered instances using the command:

   $OIM_HOME/server/bin/registration.sh

   The following snippet shows the example commands for printing registration IDs:

```
[JohnDoe@adc2190420 bin]$ ./registration.sh
[JohnDoe@adc2190420 bin]$ pwd
/scratch/JohnDoe/OIM/OIMGA/beahome2/Oracle_IDM1/server/bin
[JohnDoe@adc2190420 bin]$ ./registration.sh printRegistrationIds
Enter data related to login to OIM Server
[Enter the admin username:]xelsysadm
[Enter the admin password:]
[Enter the service url : (i.e.: t3://oimhostname:oimportno)]t3://adc2190420.us.oracle.com:8002
-----------------------------------------------
System Type     Instanace Name  Registration ID
-----------------------------------------------
PSFT            psftInstance            21
OAACG           oaacgInstancePSFT               22
PSFT            PSFT            41
OAACG           PSFT-OAACG-ITRes                42
OIM             oimInstance             1
EBS             ebsInstance             2
SAP             sapInstance             3
OAACG           oaacgInstance           4
GRC             grcInstance             5
[JohnDoe@adc2190420 bin]$
```

3. Update SILConfig.xml with registration IDs:

   a. Export the SILConfig.xml using the command:
   $OIM_HOME/server/bin/weblogicExportMetadata.sh

   File Name: metadata/iam-features-sil/db/SILConfig.xml

   b. Update the OAACGPSFT topology with PeopleSoft and OAACG details using the command:

```
<Topology>
<name> oaacgpsft</name>
<IdmId>1</IdmId>
<SodId>7</SodId>
<SDSId>6</SDSId>
```

```
</Topology>
```

c. Import the file back using weblogicImportMetadata.sh.

d. Purge the cache using the command "PurgeCache.sh All" in the same directory.

2.3.1.8.4 Updating OAACG IT Resource Instance To update OAACG IT Resource Instance:

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. Click **Configuration**, **Manage IT Resource**. The Manage IT Resource page is displayed.
4. Search for and open OAACG as the resource type. Select **PSFT-OAACG-ITRes** and edit this IT resource.
5. Provide the OAACG environment details that is configured for PeopleSoft. Table Table 2–6 shows the sample values.

Table 2–6 OAACG Environment Values

Field Name	Sample Value	Description
Source Datastore Name	PSFT 80	Name of the data source that you had specified during PeopleSoft ETL on OAACG server.
Port	8080	Port of the OAACG server.
dbuser	oaacg_850	Database user used to configure OAACG.
dbpassword	ooacg_850	Database user password used to configure OAACG
username	Admin	Username to log in to OAACG.
password	Password	Password to log in to OAACG.
server	10.1.6.82	Host machine where OAACG is running.
sodServerUrl	http://10.1.6.82/grcc/services/GrccService	SOD Server URL
sslEnable	False	True or false
jdbcURL	jdbc:oracle:thin:@172.21.104.74:1521:orcl	Jdbc url to connect to OAACG database.

6. Click **Save**.

2.3.1.8.5 Disabling and Enabling SoD This section describes the procedures to disable and enable SoD.

To disable SoD:

> **Note:** The SoD feature is disabled by default. Perform the following procedure only if the SoD feature is currently enabled and you want to disable it.

1. Log in to the Administrative and User Console.
2. Set the XL.SoDCheckRequired system property to `FALSE` as follows:

a. On the Welcome page, click **Advanced** in the upper-right corner of the page.

b. On the Welcome to Identity Manager Advanced Administration page, in the System Management section, click **Search System Properties**.

c. On the left pane, in the **Search System Configuration** field, enter `XL.SoDCheckRequired`, which is the name of the system property as the search criterion.

d. In the search results table on the left pane, click the XL.SoDCheckRequired system property in the Property Name column.

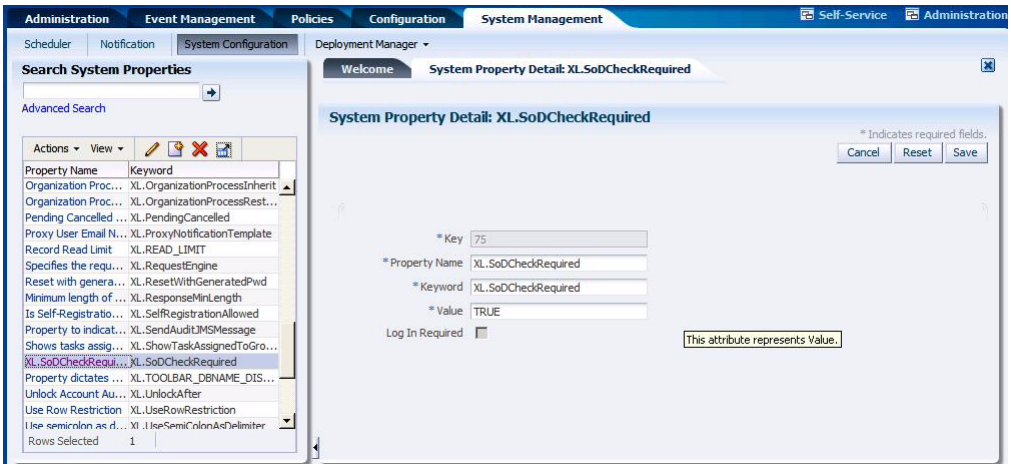
e. On the System Property Detail page, in the Value field, enter `FALSE`.

f. Click **Save** to save the changes made.

A message confirming that the system property has been modified is displayed.

3. Restart Oracle Identity Manager. Figure Figure 2–1 shows the details of disabling SoD.

Figure 2–1 Disable SoD



To enable SoD:

> **Note:** If you are enabling SoD for the first time, then see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information.

1. Log in to the Administrative and User Console.

2. Set the XL.SoDCheckRequired system property to `TRUE` as follows:

a. On the Welcome page, click **Advanced** in the upper-right corner of the page.

b. On the Welcome to Identity Manager Advanced Administration page, in the System Management section, click **Search System Properties**.

c. On the left pane, in the Search System Configuration field, enter `XL.SoDCheckRequired`, which is the name of the system property as the search criterion.

d. In the search results table on the left pane, click the XL.SoDCheckRequired system property in the Property Name column.

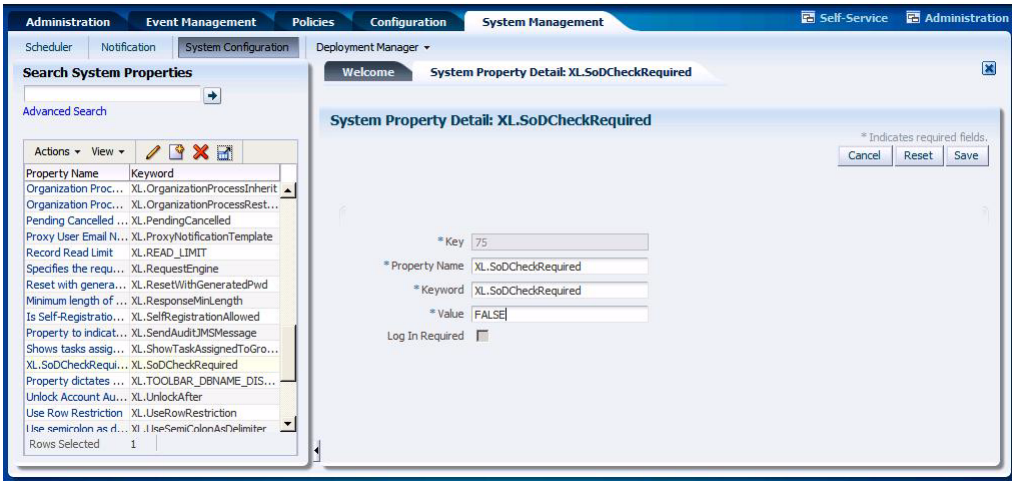
e. On the System Property Detail page, in the Value field, enter `TRUE`.

f. Click **Save** to save the changes made.

A message confirming that the system property has been modified is displayed.

3. Restart Oracle Identity Manager. Figure Figure 2–2 shows the details of enabling SoD.

Figure 2–2 Enable SoD



2.3.1.9 Enabling Request-Based Provisioning

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

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

Note: Do *not* enable request-based provisioning if you want to use the direct provisioning feature of the connector. See *Oracle Identity Manager Connector Concepts* for information about direct provisioning.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.
- Direct provisioning cannot be used if you enable request-based provisioning.

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

- Section 2.3.1.9.1, "Copying Predefined Request Datasets"
- Section 2.3.1.9.2, "Importing Request Datasets into MDS"
- Section 2.3.1.9.3, "Enabling the Auto Save Form Feature"

- Section 2.3.1.9.4, "Running the PurgeCache Utility"

2.3.1.9.1 Copying Predefined Request Datasets

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

The following is the list of predefined request datasets available in the DataSets directory on the installation media:

- ProvisionResource_PeoplesoftUser.xml
- ModifyProvisionedResource_PeoplesoftUser.xml

Copy the files from the DataSets directory on the installation media to the *OIM_HOME*/DataSet/file directory.

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

2.3.1.9.2 Importing Request Datasets into MDS

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

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

To import a request dataset definition into the MDS:

1. Ensure that you have set the environment variables for running the MDS Import utility. In the weblogic.properties file, set values for the wls_servername, application_name, and metadata_from_loc properties. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.
2. In a command window, change to the *OIM_HOME*/server/bin directory.
3. Run one of the following commands:
   - On Microsoft Windows:

     ```
     weblogicImportMetadata.bat
     ```

   - On UNIX:

     ```
     weblogicImportMetadata.sh
     ```

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

     Enter the username used to log in to the Oracle WebLogic Server

     Sample value: `WL_User`
   - `Please enter your password [weblogic]`

Enter the password used to log in to the WebLogic server

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

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

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

  In this format, replace:

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

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

The request dataset is imported into MDS.

2.3.1.9.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

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

2.3.1.9.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.1.1, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

2.3.2 Postinstallation on the Target System

Postinstallation on the target system consists of the following procedure:

Configuring SSL

To configure SSL on the target system:

1. Copy the certificate to the computer on which PeopleSoft Enterprise Applications is installed.

   Note: If you are using IBM WebSphere Application Server, then you must download the root certificate from a CA.

2. Run the following command:

   `PEOPLESOFT_HOME/webserv/peoplesoft/bin/pskeymanager.cmd -import`

3. When prompted, enter the current keystore password.
4. When prompted, enter the alias of the certificate that you imported while performing the application server specific procedures listed in Section 2.3.1.7, "Configuring SSL."

Note: The alias must be the same as the one created when the keystore was generated.

If you are using IBM WebSphere Application Server, then enter `root` as the alias.

5. When prompted, enter the full path and name of the certificate and press **Enter.**

Note: If you are using IBM WebSphere Application Server, then enter the path of the root certificate.

6. When prompted for the following:

```
Trust this certificate? [no]: yes
```

Select `yes` and press **Enter.**

7. Restart the Web server of the target system.

3

Using the Connector

This chapter contains the following sections:

3.1 Summary of Steps to Use the Connector

The following is a summary of the steps to use the connector for full reconciliation:

Note: It is assumed that you have performed all the procedures described in the preceding chapter.

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

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

---

1. Configure and run the scheduled task to synchronize the lookup fields. See Section 3.2, "Configuring the Scheduled Tasks for Lookup Field Synchronization" for more information.
2. Generate XML files for the USER_PROFILE message for all users. See Section 3.3.2, "Performing Full Reconciliation" for more information.
3. Copy these XML files to a directory on the Oracle Identity Manager host computer.

4. Configure and run the PeopleSoft User Management Target Reconciliation scheduled task for the USER_PROFILE message. The XML files are read by this scheduled task to generate reconciliation events. See "Configuring the Scheduled Task for User Data Reconciliation" on page 3-6 for more information.

Change from full reconciliation to incremental reconciliation. See Section 3.3.3, "Performing Incremental Reconciliation" for instructions.

3.2 Configuring the Scheduled Tasks for Lookup Field Synchronization

When you run the Connector Installer, the following scheduled tasks for lookup field synchronization are automatically created in Oracle Identity Manager:

- Currency Code Lookup Reconciliation
- Email Type Lookup Reconciliation
- Language Code Lookup Reconciliation
- Permission List Lookup Reconciliation
- Roles Lookup Reconciliation

These scheduled tasks are used to synchronize the values of the lookup fields between the target system and Oracle Identity Manager. Table 3–1 describes the attributes of this scheduled task. See Section 3.6, "Configuring Scheduled Tasks" for instructions on running the scheduled task.

Note: Default attribute values are predefined in the connector XML file that is imported during the installation of the connector. Specify values only for those attributes that you want to change.

Table 3–1 Scheduled Task Attributes for Lookup Field Synchronization

Attribute	Description
IT Resource Name	Enter the name of the IT resource. Default Value: `PSFT Server`
FilePath	Enter the full path of the file in which the lookup data to be reconciled is stored. The operating system of the computer on which Oracle Identity Manager is installed must be able to access this file path. The data extracted from this file is stored in the Lookup Definition Name attribute of the scheduled task. Default value: Enter a Value Sample value: `C:\PSFTUM\LookupRecon\Roles.properties`
Lookup Definition Name	Enter the name of the lookup definitions created in Oracle Identity Manager that corresponds to the lookup fields in the target system. The value can be any one of the following: ▪ `Lookup.PSFTUM.LanguageCode` ▪ `Lookup.PSFTUM.EmailType` ▪ `Lookup.PSFTUM.CurrencyCode` ▪ `Lookup.PSFTUM.PermissionList` ▪ `Lookup.PSFTUM.Roles`
Task Name	Enter the name of the scheduled task. Sample value: `Language Code Lookup Reconciliation`

Table 3–1 (Cont.) Scheduled Task Attributes for Lookup Field Synchronization

Attribute	Description
Ref Data Provider Impl	Enter the name of the lookup reconciliation implementation class. Default value: `oracle.iam.connectors.psft.usermgmt.tasks.PSFTUMLookupReconTask` **Note:** You must not change this value.
File Archival	Enter `Yes` if you want the lookup properties file used during lookup reconciliation to be archived. Enter `No` if you want the file to be deleted after data inside the files is reconciled. Default value: `No`
File Archival Folder	Enter the full path and name of the directory in which you want the lookup properties file used during lookup reconciliation to be archived. Default Value: Enter a Value **Note:** You must change this value if the File Archival attribute is set to `Yes`. Sample Value: `C:\ArchiveFolder`

3.3 Configuring Reconciliation

This section discusses the following topics related to configuring reconciliation:

- Section 3.3.1, "Performing Lookup Reconciliation"
- Section 3.3.2, "Performing Full Reconciliation"
- Section 3.3.3, "Performing Incremental Reconciliation"
- Section 3.3.4, "Limited Reconciliation"

3.3.1 Performing Lookup Reconciliation

This section describes the procedure to generate the properties file, which contains the lookup data to be consumed by the lookup reconciliation scheduled task.

Running the Application Engine Program

You can run the Application Engine program by using PeopleSoft Internet Architecture to perform Lookup Reconciliation as follows:

Note: You must run the Application Engine program periodically.

1. Open a Web browser and enter the URL for PeopleSoft Internet Architecture. The URL is in the following format:

   `http://`*`IPADDRESS:PORT`*`/psp/ps/?cmd=login`

   For example:

   `http://`*`172.21.109.69:9080`*`/psp/ps/?cmd=login`

2. Click **People Tools, Process Scheduler, Processes,** and then **Add a new Value.**
3. Select **Application Engine** as the process type, and enter `LOOKUP_RECON` as the process name.
4. Click **Add.**

5. In the Process Definition Options tab, enter the following values for **Component** and **Process Groups**, and click **Save:**

   Component: `AE_REQUEST`

   Process Groups: `TLSALL`, `STALL`

6. To make the Application Engine program run in PeopleSoft Internet Architecture, click **People Tools, Application Engine, Request AE,** and then click **Add a new Value.**

7. Enter values for the following and then click **Add:**

   User ID: Enter your User ID

   Run Control ID: Enter a unique run control value

   Program Name: Enter `LOOKUP_RECON`

8. Click **Run.**

9. From the list that is displayed, select the **LOOKUP_RECON** process, which you created in Step 3.

10. Click **OK.**

11. To determine the progress status of the Application Engine program, click **People Tools, Process Scheduler,** and then **Process Monitor.** Click **Refresh** until `Success` message is displayed as the status.

> **Note:** If Status is displayed as "Queued," then you must check the status of the process scheduler. To do so, click **People Tools, Process Scheduler,** and then **Process Monitor.** Click the **Server List** tab and check the status of the server. If the status is not displayed, then start the process scheduler.

3.3.2 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user profile records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

The following sections discuss the procedures involved in full reconciliation:

- Section 3.3.2.1, "Generating XML Files"
- Section 3.3.2.2, "Importing XML Files into Oracle Identity Manager"

3.3.2.1 Generating XML Files

You must generate XML files for all existing users in the target system.

> **Note:** Before performing the procedure to generate XML files, you must ensure that you have configured the USER_PROFILE message. See Section 2.2.2.2, "Configuring the Target System for Full Reconciliation" for more information.

To generate XML files for full reconciliation, perform the following procedure:

Note: If you are using PeopleTools 8.50 and HCM 9.0, then before running Full Data Publish, you must apply the patch that addresses Bug 824529. This patch can be downloaded from Oracle Metalink.

Running the USER_PROFILE (VERSION_84) Message for Full Data Publish

To configure the USER_PROFILE message, see Section 2.2.2.2.5, "Configuring the USER_PROFILE Service Operation."

Note: You must run the Application Engine program if you are performing the full reconciliation for the first time. See "Running the Application Engine Program" on page 3-3 for more information.

To run the USER_PROFILE message:

1. In PeopleSoft Internet Architecture, expand **Enterprise Components, Integration Definitions, Initiate Processes,** and then click **Full Data Publish.**
2. Click the **Add a New Value** tab.
3. In the Run Control ID field, enter a value and then click **ADD.**
4. In the **Process Request** region, provide the following values:

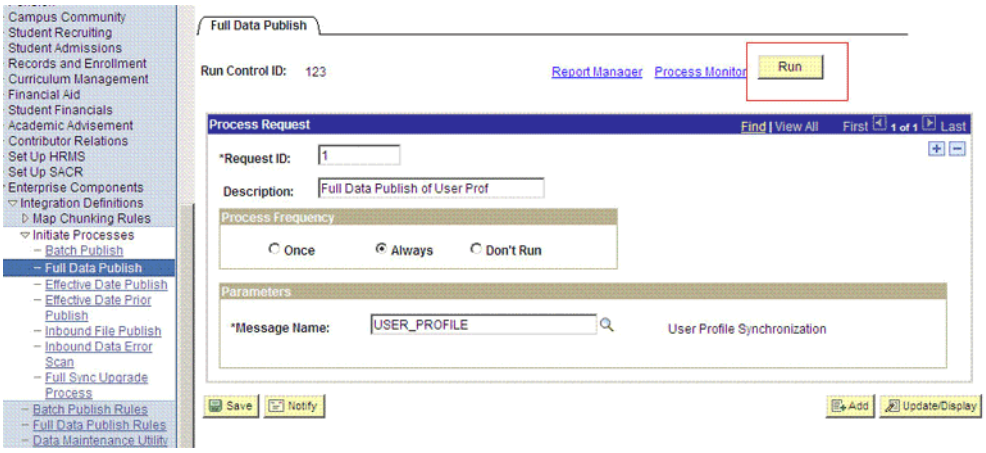
   Request ID: Enter a request ID.

   Description: Enter a description for the process request.

   Process Frequency: Select **Always.**

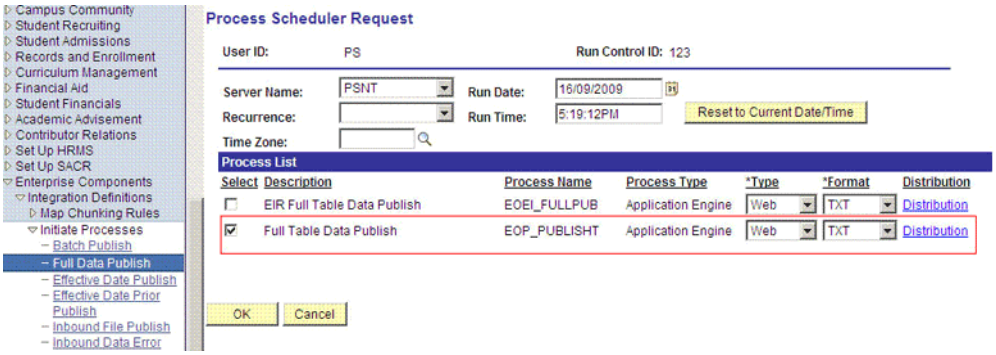
   Message Name: Enter `USER_PROFILE` as the message name.
5. Click **Save** to save the configuration.
6. Click **Run.**

   The following screenshot displays the preceding steps:



   The Process Scheduler Request page appears.
7. From the **Server Name** list, select the appropriate server.
8. Select **Full Table Data Publish** process list, and click **OK.**

   The following screenshot displays the Process Scheduler Request page:



9. Click **Process Monitor** to verify the status of EOP_PUBLISHT Application Engine. The **Run Status** is **Success** if the transaction is successfully completed.

   On successful completion of the transaction, XML files for the USER_PROFILE message are generated at a location that you specified in the FilePath property while creating the OIM_FILE_NODE node for PeopleSoft Web Server. See "Configuring PeopleSoft Integration Broker" on page 2-37 section for more information.

   You must copy these XML files to a directory on the Oracle Identity Manager host computer.

Note: After you have performed this procedure:

- Remove the permission list created in "Setting Up the Security for the USER_PROFILE Service Operation" on page 2-41 section. This is for security purposes.
- Disable the USER_PROFILE_HR_TO_UMFILE routing created in "Defining the Routing for the USER_PROFILE Service Operation" on page 2-43 section. To do so, clear the **Active** check box in Step 2 of the procedure.

3.3.2.2 Importing XML Files into Oracle Identity Manager

This section describes the procedure to import XML files into Oracle Identity Manager.

Configuring the Scheduled Task for User Data Reconciliation

When you run the Connector Installer, the PeopleSoft User Management Target Reconciliation scheduled task is automatically created in Oracle Identity Manager.

The PeopleSoft User Management Target Reconciliation scheduled task is used for target resource reconciliation. In addition, this same scheduled task is used to reconcile data of deleted users from a target resource into Oracle Identity Manager.

The scheduled task transfers data from the XML file to the parser. The parser then converts this data into reconciliation events. Table 3–2 describes the attributes of this scheduled task. See Section 3.6, "Configuring Scheduled Tasks" for instructions on configuring the scheduled task.

Table 3–2 Attributes of the Scheduled Task for Reconciliation of User Data

Attribute	Description
Archive Mode	Enter `yes` if you want XML files used during full reconciliation to be archived. After archival, the file is deleted from the original location. If `no`, then the XML file is not archived.
Archive Path	Enter the full path and name of the directory in which you want XML files used during full reconciliation to be archived. You must enter a value for the Archive Path attribute only if you specify `yes` as the value for the Archive Mode attribute. Sample value: `/usr/archive`
File Path	Enter the path of the directory on the Oracle Identity Manager host computer into which you copied the file containing XML data. Sample value: `/usr/data`
IT Resource Name	Enter the name of the IT resource that you create by performing the procedure described in the Section 2.2.1.3, "Configuring the IT Resource" section. Default value: `PSFT Server`

Message Implementation Class	Enter the name of the Implementation class for the message handler required to process the message. For example, the implementation class for the following messages are provided by default:
	For the USER_PROFILE message:
	`oracle.iam.connectors.psft.common.handler.impl.PSFTUserProfileReconMessageHandlerImpl`
	For the DELETE_USER_PROFILE message:
	`oracle.iam.connectors.psft.common.handler.impl.PSFTDeleteUserReconMessageHandlerImpl`

Message Name	Use this attribute to specify the name of the delivered message used for full reconciliation. Sample value: `USER_PROFILE`
Task Name	This attribute holds the name of the scheduled task. Default value: `PeopleSoft User Management Target Reconciliation`

3.3.3 Performing Incremental Reconciliation

You do not require additional configuration for incremental reconciliation.

It is assumed that you have deployed the PeopleSoft listener as described in Section 2.2.1.5, "Deploying the PeopleSoft Listener."

3.3.4 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current incremental reconciliation run. For full reconciliation, all target system records are fetched into Oracle Identity Manager.

You can configure limited reconciliation to specify the subset of target system records that must be fetched into Oracle Identity Manager.

You configure limited reconciliation by specifying a query condition as the value of the Custom Query attribute of the PeopleSoft User Management Target Reconciliation scheduled task.

You must use the following format to specify a value for the Custom Query attribute:

RESOURCE_OBJECT_ATTRIBUTE_NAME=VALUE

For example, suppose you specify the following as the value of the Custom Query attribute:

```
Currency Code=1~USD
```

With this query condition, only records for users with currency code as 1~USD are considered for reconciliation.

You can add multiple query conditions by using the ampersand (&) as the AND operator and the vertical bar (|) as the OR operator. For example, the following query condition is used to limit reconciliation to records of those users for whom the Currency Code is 1~USD and User ID is John01:

```
Currency Code=1~USD  & User ID=John01
```

To configure limited reconciliation:

1. Create the query condition. Apply the following guidelines when you create the query condition:
   - Use only the equal sign (=), the ampersand (&), and the vertical bar (|) in the query condition. Do not include any other special characters in the query condition. Any other character that is included is treated as part of the value that you specify.
   - Add a space before and after the ampersand and vertical bar signs used in the query condition. For example:

     ```
     Currency Code=1~USD  & User ID=John01
     ```

     ```
     Currency Code=1~USD  | User ID=John01
     ```

     This is to help the system distinguish between ampersands and vertical bars used in the query and the same characters included as part of attribute values specified in the query condition.
   - You must not include unnecessary blank spaces between operators and values in the query condition.

     A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

     ```
     Currency Code=1~USD  & User ID=John01
     ```

     ```
     Currency Code= 1~USD  & User ID= John01
     ```

     In the second query condition, the reconciliation engine would look for Currency Code and User ID values that contain a space at the start.
   - Ensure that attribute names that you use in the query condition are in the same case (uppercase or lowercase) as the case of the attribute defined in PeopleSoft User resource object. For example, the following query condition would fail:

     ```
     cUrReNcY Code= 1~USD
     ```
2. Configure the message-specific configuration lookup with the query condition as the value of the Custom Query attribute. For example, to specify the query condition for the USER_PROFILE message, search and open the

Lookup.PSFT.Message.UserProfile.Configuration lookup. Specify the query condition in the Decode column of the **Custom Query** attribute.

3.4 Resending Messages That Are Not Received by the PeopleSoft Listener

The messages are generated and sent to Oracle Identity Manager regardless of whether the WAR file is running. Reconciliation events are not created for the messages that are sent to Oracle Identity Manager while the WAR file is unavailable. To ensure that all the messages generated on the target system reach Oracle Identity Manager, perform the following procedure:

Manually Sending Messages

If Oracle Identity Manager is not running when a message is published, then the message is added to a queue. You can check the status of the message in the queue in the Message Instance tab. This tab lists all the published messages in a queue. When you check the details of the particular message, the status is listed as `Timeout` or `Error`.

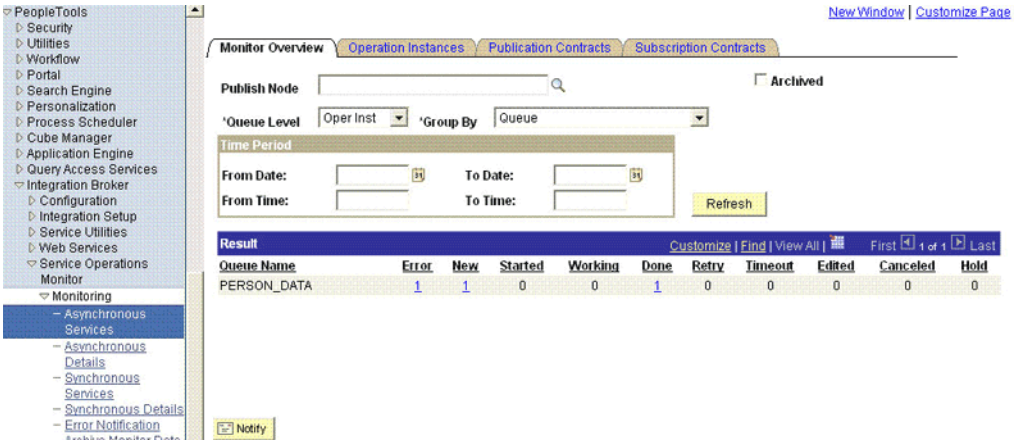
To publish a message in the queue to Oracle Identity Manager, resubmit the message when Oracle Identity Manager is running.

If the status of the message is `New` or `Started` and it does not change to `Timeout` or `Done`, then you must restart the PeopleSoft application server after you restart Oracle Identity Manager.

Note: PeopleSoft supports this functionality for a limited rights user described in Section 2.1.2.2.2, "Creating a Role for a Limited Rights User." But, you can specify users who have rights to perform this task based on the security policy of your organization.

To manually resend messages in Error or TimeOut status:

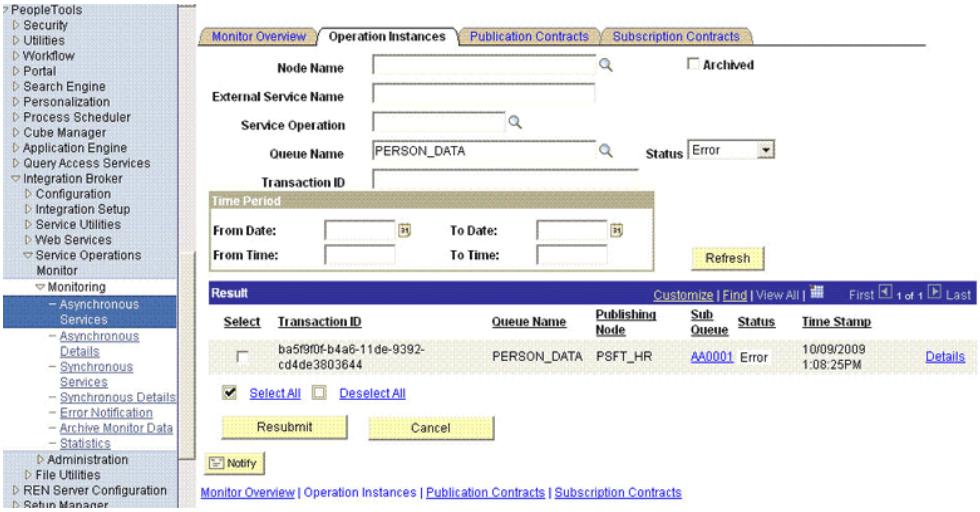
1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Service Operations Monitor, Monitoring,** and then click **Asynchronous Services.**
2. From the Group By list, select **Service Operation** or **Queue** to view the number of messages in Error, TimeOut, Done, and so on.



The number is in the form of a link, which when clicked displays the details of the message.

3. Click the link pertaining to the message to be resent, for example, the link under the Error or the TimeOut column.

   You are taken to the Operation Instance tab.



4. Click the **Details** link of the message to be resent. A new window appears.

5. Click the **Error Messages** link to check the error description.
6. Click **Resubmit** after you have resolved the issue.

3.5 Performing Provisioning Operations

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

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning

> **Note:** The "Unable to access pstools.properties" message might be recorded in the server logs during provisioning operations. You can safely ignore this message.

This section discusses the following topics:

- Section 3.5.1, "Direct Provisioning on Oracle Identity Manager"
- Section 3.5.2, "Request-Based Provisioning in Oracle Identity Manager"

3.5.1 Direct Provisioning on Oracle Identity Manager

This section describes the prerequisites and the procedure to perform direct provisioning. It contains the following sections:

- Section 3.5.1.1, "Prerequisites"
- Section 3.5.1.2, "Performing Direct Provisioning"

3.5.1.1 Prerequisites

Note: Perform the procedure in this section only in the following situations:

- The first time you perform direct provisioning.
- If you switch from request-based provisioning to direct provisioning.

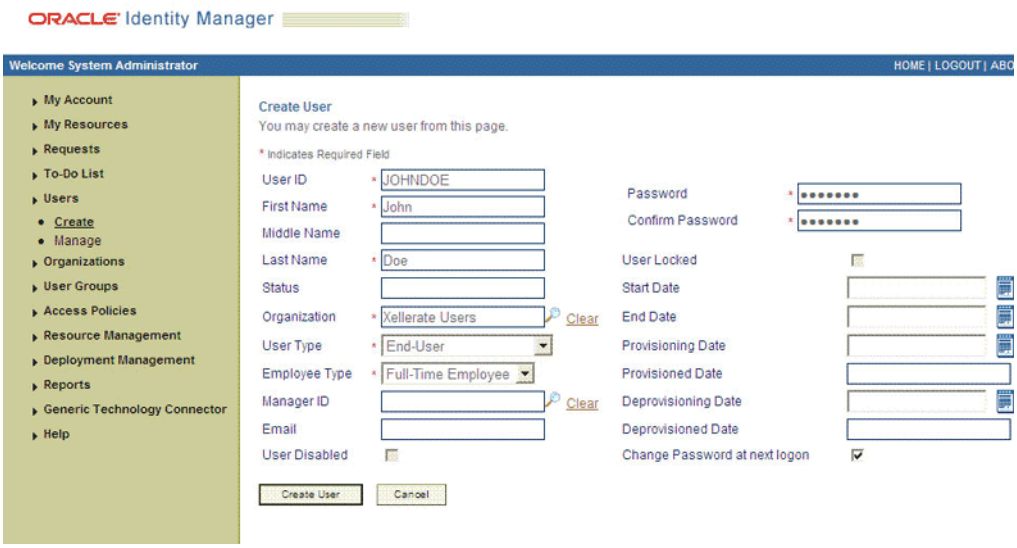
When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you configure the connector for request-based provisioning, then the process form is suppressed and 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 Section 3.8, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

3.5.1.2 Performing Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced.**
   b. Click the **Administration** tab.
3. If you want to first create the OIM User and then provision a resource:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. From the Users menu, select **Create.**
     b. On the Create User page, enter values for the OIM User fields and then click **Create User.**



- If you are using Oracle Identity Manager release 11.1.1, then:

  a. On the Welcome to Identity Administration page, in the Users region, click **Create User.**

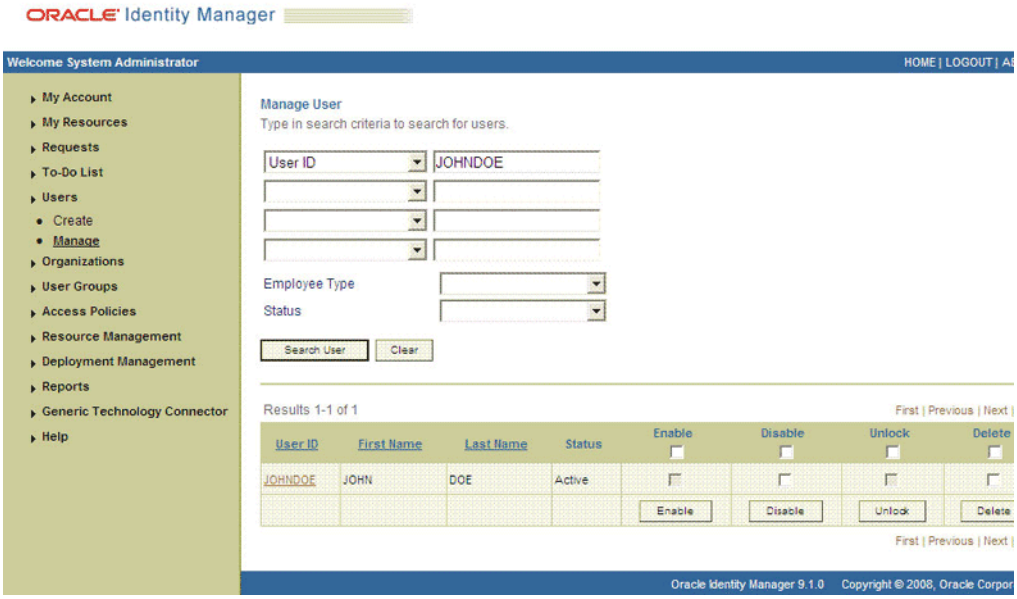
  b. On the Create User page, enter values for the OIM User fields, and then click **Save.**

4. If you want to provision a target system account to an existing OIM User, then:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:

     a. From the Users menu, select **Manage.**

     b. Search for the OIM User by using the Search feature, and then click the link for the OIM User from the list of users displayed in the search results table.



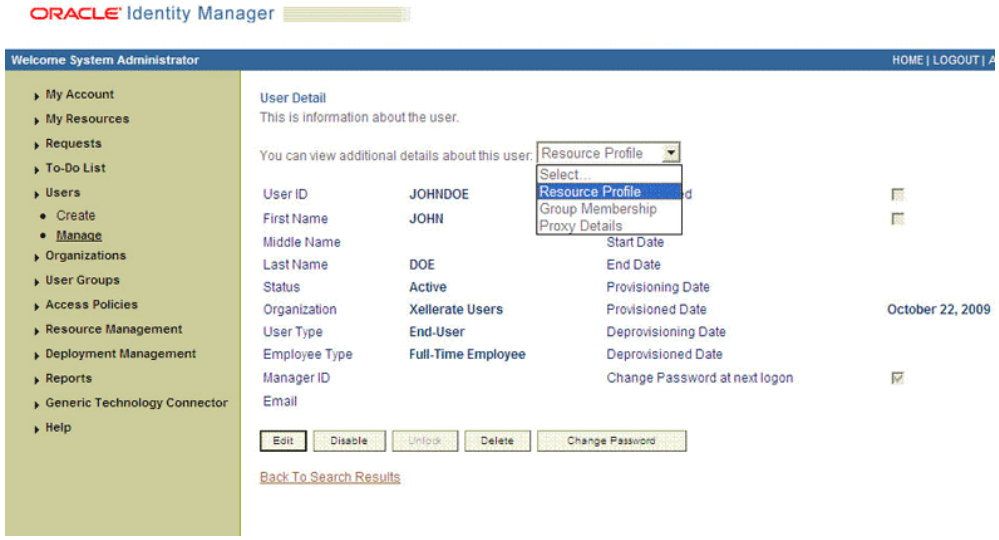
- If you are using Oracle Identity Manager release 11.1.1, then:

a. On the Welcome to Identity Administration page, in the Users region, click **Advanced Search - Users.**

b. Search for the OIM User by using the Search feature, and then click the link for the OIM User from the list of users displayed in the search results table.

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

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then on the User Detail page, select **Resource Profile** from the list at the top of the page.



   - If you are using Oracle Identity Manager release 11.1.1, then click the **Resources** tab.

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

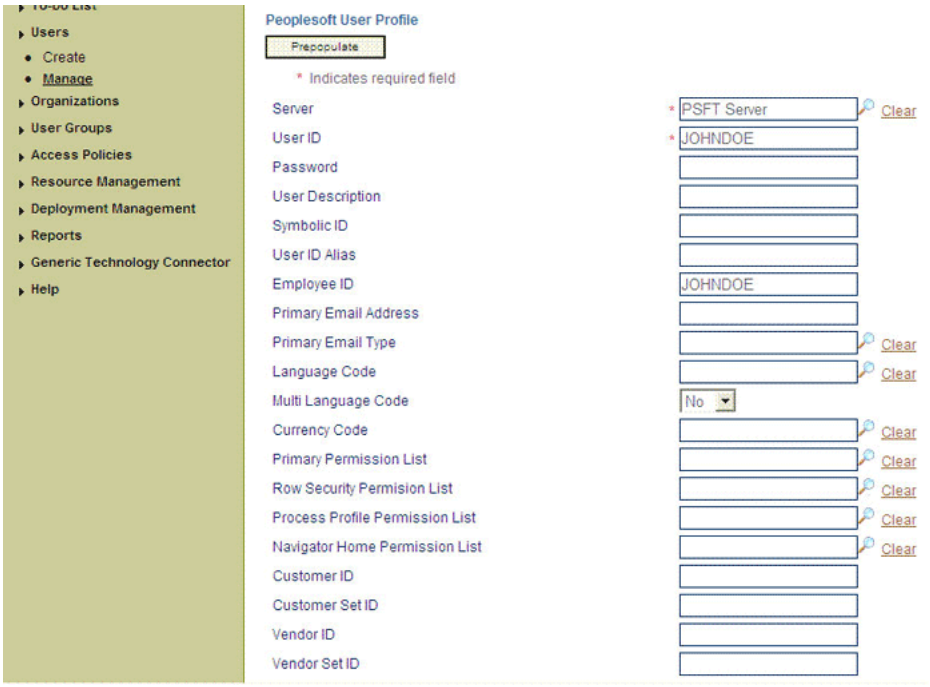
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Resource Profile page, click **Provision New Resource.**

- If you are using Oracle Identity Manager release 11.1.1, then click **Add.** The Provision Resource to User page is displayed in a new window.

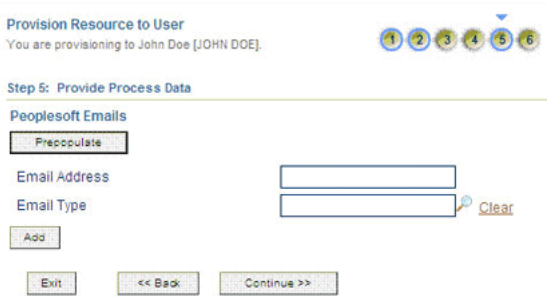
7. On the Select a Resource page, select **Peoplesoft User** from the list, and then click **Continue.**

8. On the Verify Resource Selection page, click **Continue.**

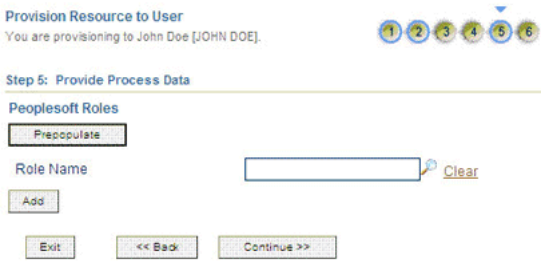
9. On Provide Process Data page, enter the details of the account that you want to create on the target system, and then click **Continue.**



10. On the Provide Process Data page for child data, search for and select the child data for the user on the target system. For instance, on the Provide Process Data page for e-mail data, specify the e-mail address and e-mail type for the account and then click **Add.** If you want to add more than one e-mail, repeat the process. Then, click **Continue.**



11. On the Provide Process Data page for role data, specify the role name, and then click **Add.** If you want to add more than one role, repeat the process. Then, click **Continue.**



12. On the Verify Process Data page, verify the data that you entered, and then click **Continue.**

    The account is created on the target system and provisioned as a resource to the OIM User.

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

    - If you are using Oracle Identity Manager release 9.1.0.*x*, then page that is displayed provides options to disable or revoke the resource from the OIM User.
    - If you are using Oracle Identity Manager release 11.1.1, the "Provisioning has been initiated" message is displayed. Close this window, and click **Refresh** to view details of the newly provisioned resource.

      See Also: Section 1.7, "Connector Objects Used During Provisioning" for more information about the provisioning functions supported by this connector and the process form fields used for provisioning

3.5.2 Request-Based Provisioning in Oracle Identity Manager

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

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

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

The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

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

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

3.5.2.1 End User's Role in Request-Based Provisioning

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

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 then 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 specified 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 the 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 **PeopleSoft User**, 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 is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.5.2.2 Approver's Role in Request-Based Provisioning

The approver in a request-based provisioning operation performs the following steps:

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 region, you can specify a search criterion for the request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

3.6 Configuring Scheduled Tasks

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

The following is a list of scheduled tasks that you must configure.

- Currency Code Lookup Reconciliation
- Email Type Lookup Reconciliation
- Language Code Lookup Reconciliation
- Permission List Lookup Reconciliation
- Roles Lookup Reconciliation
- PeopleSoft User Management Target Reconciliation

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced.**
     b. Click the **System Management** tab, and then click **Scheduler.**
     c. On the left pane, click **Advanced Search**.
3. On the page that is displayed, you can use any combination of the search options provided to locate a scheduled task. Click **Search** after you specify the search criteria.

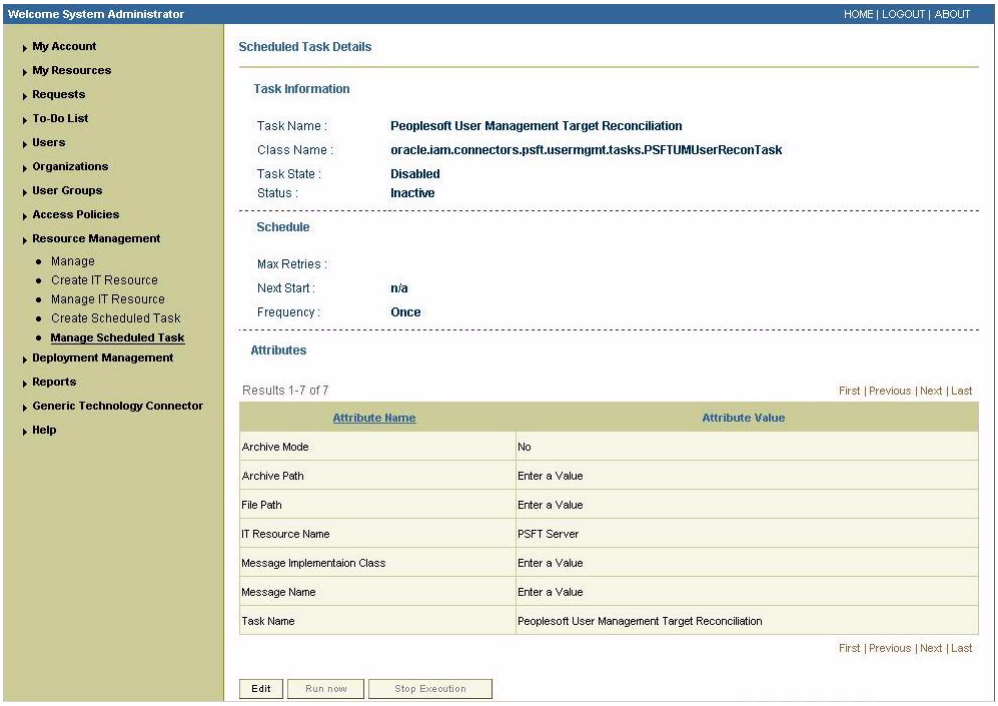
   The following screenshot shows the Scheduled Task Management page for Oracle Identity Manager release 9.1.0.*x*:

The list of scheduled tasks that match your search criteria is displayed in the search results table.

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

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then in the search results table, click the Edit icon in the Edit column for the scheduled task.

     The following screenshot shows the Scheduled Task Details page:



- If you are using Oracle Identity Manager release 11.1.1, then select the link for the scheduled task from the list of scheduled tasks displayed in the search results table.

5. Modify the details of the scheduled task. To do so:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Edit Scheduled Task Details page, you can modify the following parameters:

     - **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

     - **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.

     - **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

     - **Frequency:** Specify the frequency at which you want the task to run.

   - If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, you can modify the following parameters:

     - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

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

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

6. After modifying the values for the scheduled task details listed in the previous step, perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Continue.**
   - If you are using Oracle Identity Manager release 11.1.1, then perform the next step.

7. Specify values for the attributes of the scheduled task. To do so:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then select each attribute from the Attribute list, specify a value in the field provided, and then click **Update.** See Table 3–2 for more information about the attributes of the scheduled task.

     The following screenshot shows the Attributes page. The attributes of the scheduled task that you select for modification are displayed on this page.

- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, under the Parameters section, specify values for the attributes of the scheduled task. See Table 3–2 for more information about the attributes of the scheduled task.

  Note: Attribute values are predefined in the connector XML file that is imported during the installation of the connector. Specify values only for the attributes that you want to change.

8. After specifying the attributes, perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

     Note: The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

   - If you are using Oracle Identity Manager release 11.1.1, then 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 start, stop, or reinitialize the scheduler.

3.7 Provisioning Operations Performed in an SoD-Enabled Environment

Note: The information in this section applies only to Oracle Identity Manager 11.1.1.

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

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning of accounts
- Request-based provisioning of entitlements
- Provisioning triggered by policy changes

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

This section discusses the following topics:

- Section 3.7.1, "Overview of the Provisioning Process in an SoD-Enabled Environment"
- Section 3.7.2, "Direct Provisioning in an SoD-Enabled Environment"
- Section 3.7.3, "Request-Based Provisioning in an SoD-Enabled Environment"

3.7.1 Overview of the Provisioning Process in an SoD-Enabled Environment

The following is the sequence of steps that take places during a provisioning operation performed in an SoD-enabled environment:

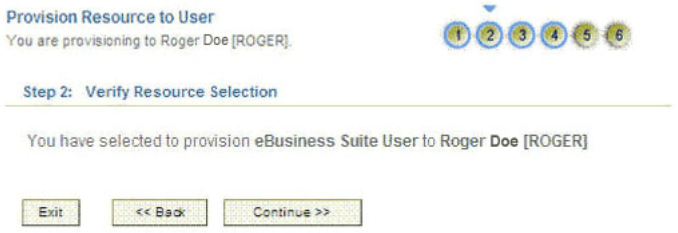
1. The provisioning operation triggers the appropriate adapter.
2. The adapter carries provisioning data to the corresponding BAPI on the target system.
3. If you select an account or entitlements to be provisioned to the OIM User, then the SoD check is initiated. The SoDChecker task submits the User Account and Entitlements details in a form of Duties list to Oracle Application Access Controls Governor. In other words, the SoD validation process takes place asynchronously.
4. The user runs either the Get SOD Check Results Provisioning or Get SOD Check Results Approval scheduled task.
5. The scheduled task passes the entitlement data to the Web service of Oracle Application Access Controls Governor.
6. After Oracle Application Access Controls Governor runs the SoD validation process on the entitlement data, the response from the process is returned to Oracle Identity Manager.
7. The status of the process task that received the response depends on the response itself. If the entitlement data clears the SoD validation process, then the status of the process task changes to Completed. This translates into the entitlement being granted to the user. If the SoD validation process returns the failure response, then status of the process task changes to Canceled.

3.7.2 Direct Provisioning in an SoD-Enabled Environment

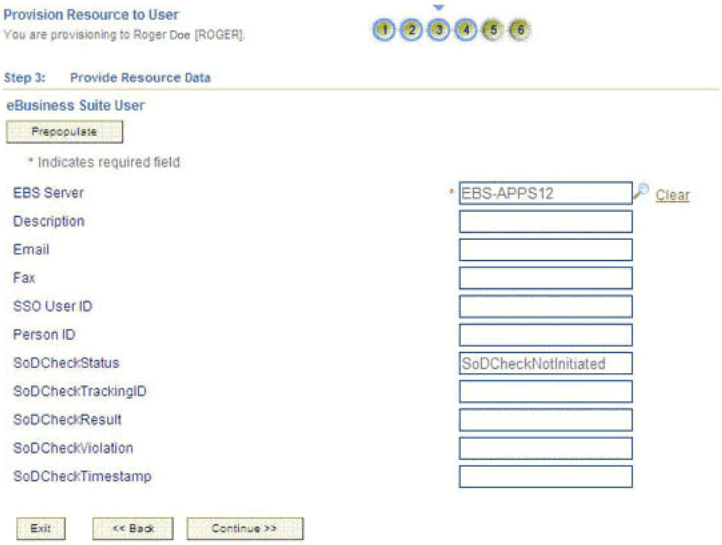
To provision a resource by using the direct provisioning approach:

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 Identity Manager - Self Service page, click **Administration**.
   b. On the Welcome to Identity Administration page, in the Users section, click **Create User.**
   c. 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 drop-down 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 the resource that you want to provision from the list and then click **Continue**. The following screenshot shows the Step 1: Select a Resource page:

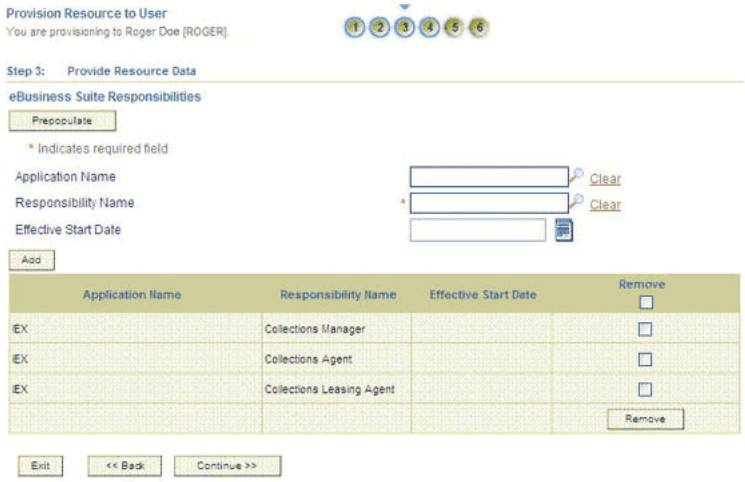
7. On the Step 2: Verify Resource Selection page, click **Continue**. The following screenshot shows the Step 2: Verify Resource Selection page:



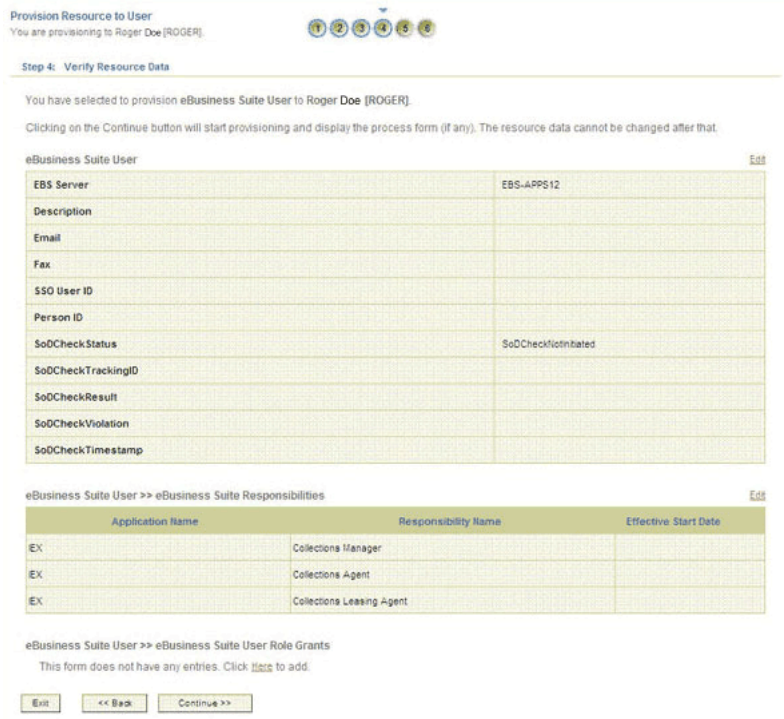
8. On the Step 3: Provide Resource Data page for process data, enter the details of the account that you want to create on the target system and then click **Continue**. The following screenshot shows the user details added:



9. On the Step 3: Provide Process Data page for role data, specify the role name for the account, and then click **Add**. If you want to add more than one role, repeat the process. Then, click **Continue**. The following screenshot shows this page:



10. On the Step 4: Verify Process Data page, verify the data that you have provided and then click **Continue**. The following screenshot shows Step 4: Verify Process Data page.



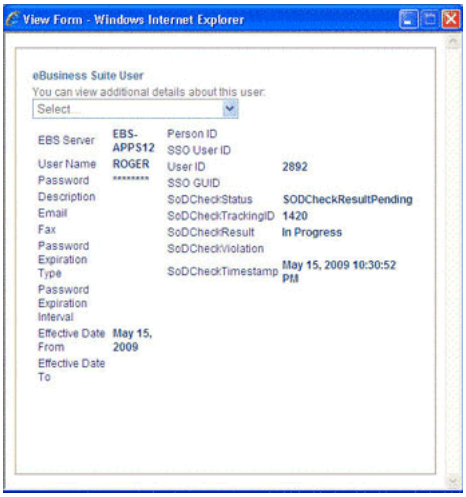
11. The "Provisioning has been initiated" message is displayed. To view the newly provisioned resource, perform one of the following steps:

    a. Close the window displaying the "Provisioning has been initiated" message.

    b. On the Resource tab of the user details page, click **Refresh** to view the newly provisioned resource.

12. To view the process form, on the Resources tab of the user details page, select the row displaying the newly provisioned resource, and then click **Open.** The Edit Form page is displayed.

    The following screenshot shows the page displaying the process form:



In this screenshot, the SODCheckStatus field shows SODCheckPending. The value in this field can be SoDCheckResultPending or SoDCheckCompleted.

Note: If Oracle Identity Manager is not SoD enabled, then SOD Check Status field shows SODCheckNotInitiated.

13. To view the Resource Provisioning Details page, which shows the details of the process tasks that were run, on the Resources tab of the user details page, from the Action menu, select **Resource History.**

    The following screenshot shows the Resource Provisioning Details page:

This page shows the details of the process tasks that were run. The Holder and SODChecker tasks are in the Pending state. These tasks will change state after the status of the SoD check is returned from the SoD engine. The Add Role to User task corresponds to the roles selected for assignment to this user.

Note: SoD validation by Oracle Application Access Controls Governor is asynchronous. The validation process returns a result as soon as it is completed.

14. After the Get SOD Check Results Provisioning scheduled task is run, the results of the SoD validation process are brought to Oracle Identity Manager. To view the process form, on the Resources tab of the User Details page, select the row displaying the newly provisioned resource, and then click **Open.** The Edit Form page is displayed.

    The following screenshot shows the page displaying this process form:

In this screenshot, the SOD Check Status field shows SoDCheckCompleted. Because a violation by the SoD engine in this particular example, the SoD Check Violation field shows the details of the violation.

In addition, the Resource Provisioning Details page shows the status of the SODChecker and Holder tasks as Completed.

The following screenshot shows this page:

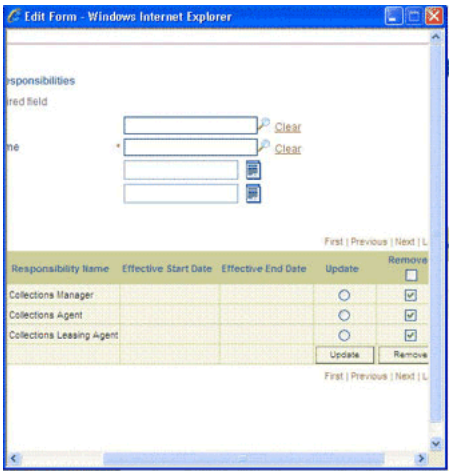
In this screenshot, the status of the Add User Role tasks is Canceled because the request failed the SoD validation process.

15. As the administrator assigning a resource to a user, you can either end the process when a violation is detected or modify the assignment data and then resend it. To modify the assignment data, on the Resource tab of the user details page, select the row containing the resource, and then click **Open.**

16. In the Edit Form window that is displayed, you can modify the role and profile data that you had selected earlier.

> **Note:** To modify a set of entitlements In the Edit Form window, you must first remove all entitlements and then add the ones that you want to use.

In the following screenshot, one of the roles selected earlier is marked for removal:



17. Rerun the Get SOD Check Results Provisioning scheduled task to initiate the SoD validation process.

18. After the Get SOD Check Results Provisioning scheduled task is run, the results of the SoD validation process are brought to Oracle Identity Manager. On the Resources tab of the user details page, select the row containing the resource, and then click **Open.** The process form is displayed.

    The following screenshot shows the page displaying the process form:

    In this screenshot, the SOD Check Status field shows SoDCheckCompleted. Because no violation was detected by the SoD engine, the SoDCheckResult field shows `Passed`.

    In addition, the Resource Provisioning Details page shows the status of the SODChecker and Holder tasks as Completed.

    The following screenshot shows this page:

On the Resource Provisioning Details page, the state of the Add Role to User task is completed.

3.7.3 Request-Based Provisioning in an SoD-Enabled Environment

See Also: Section 2.3.1.8, "Configuring SoD"

The request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The request-based provisioning process described in this section covers steps to be performed by both entities.

In the example used in this section, the end user creates a request for two roles on the target system. The request clears the SoD validation process and is approved by the approver.

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

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

See Also: The "Creating and Searching Requests" chapter of *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Advanced 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 specified 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 **PeopleSoft User**, 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. On the Resource tab of the Request Details page, click the View Details link in the row containing the resource for which the request was created. The Resource data page in displayed in a new window.

    One of the fields on this page is the SODCheckStatus field. The value in this field can be SoDCheckResultPending or SoDCheckCompleted. When the request is placed, the SODCheckStatus field contains the SoDCheckResultPending status.

    Note: If Oracle Identity Manager is not SoD enabled, then the SOD Check Status field shows SODCheckNotInitiated.

15. To view details of the approval, on the Request Details page, click the **Approval Tasks** tab.

    On this page, the status of the SODChecker task is pending.

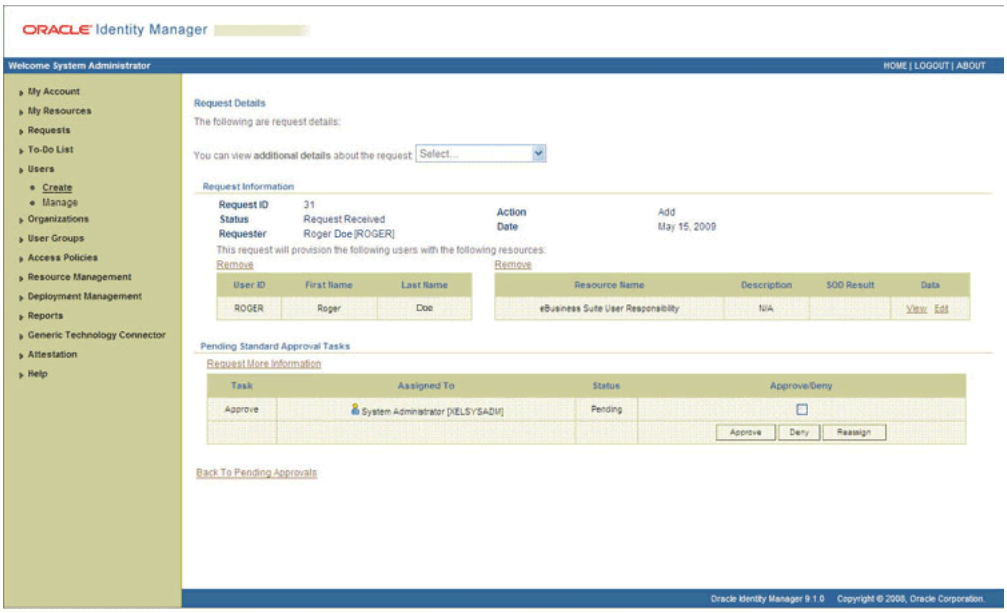
16. To initiate SoD validation of pending requests, the approver must run the Get SOD Check Results Approval scheduled task.

17. After the Get SOD Check Results Approval scheduled task is run, on the Request Details page, click the **Approval Tasks** tab. The status of the SODChecker task is Completed and the Approval task status is Pending. This page also shows details of the administrator who must now approve the request.

3.7.3.2 Approver's Role in Request-Based Provisioning

This section discusses the role of the approver in a request-based provisioning operation.

The approver to whom the request is assigned can use the Pending Approvals feature to view details of the request.



In addition, the approver can click the View link to view details of the SoD validation process.

The approver can decide whether to approve or deny the request, regardless of whether the SoD engine accepted or rejected the request. The approver can also modify entitlements in the request.

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.

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

> **Note:** It is assumed that you have performed the procedure described in Section 2.3.1.9, "Enabling Request-Based Provisioning."

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

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.

b. Search for and open the **Peoplesoft User Management** 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 **Peoplesoft User** resource object.

c. Deselect the **Self Request Allowed** check box.

d. Click the Save icon.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning 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 **Peoplesoft User Management** 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 **Peoplesoft User** resource object.

c. Select the **Self Request Allowed** check box.

d. Click the Save icon.

4

Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

4.1 Adding New Attributes for Provisioning

You can configure a new attribute for provisioning, in addition to those provided by default.

Note: If you do not want to add new attributes for provisioning, then you can ignore this section.

To add a new attribute for provisioning:

Note: Only those attributes that have their corresponding SET APIs in IUserProfile.class in the peoplesoft.jar file can be provisioned. For example, to provision the Worklist attribute, the peoplesoft.jar file must also contain the setWorklistUser (String s) API.

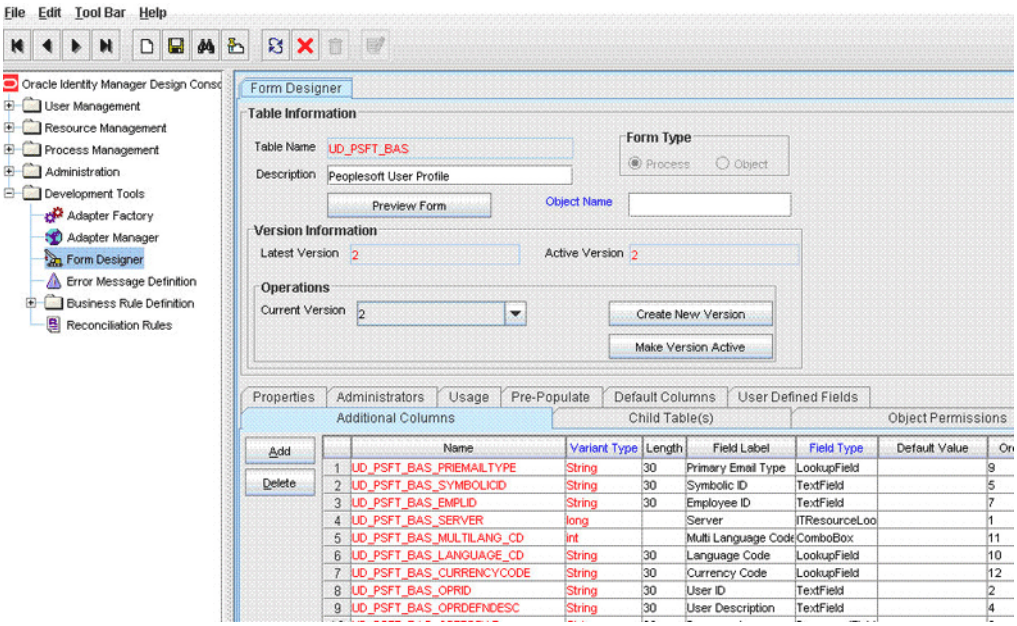
The data type of the argument in setWorklistUser (String s) must be the same or compatible with the data type of the corresponding Worklist field in Oracle Identity Manager.

1. Add a new column in the process form by performing the following:

   a. Log in to the Oracle Identity Manager Design Console.

   b. Expand **Development Tools** and then double-click **Form Designer.**

   c. Enter `UD_PSFT_BAS` in the Table Name field and click the **Query for records** button.



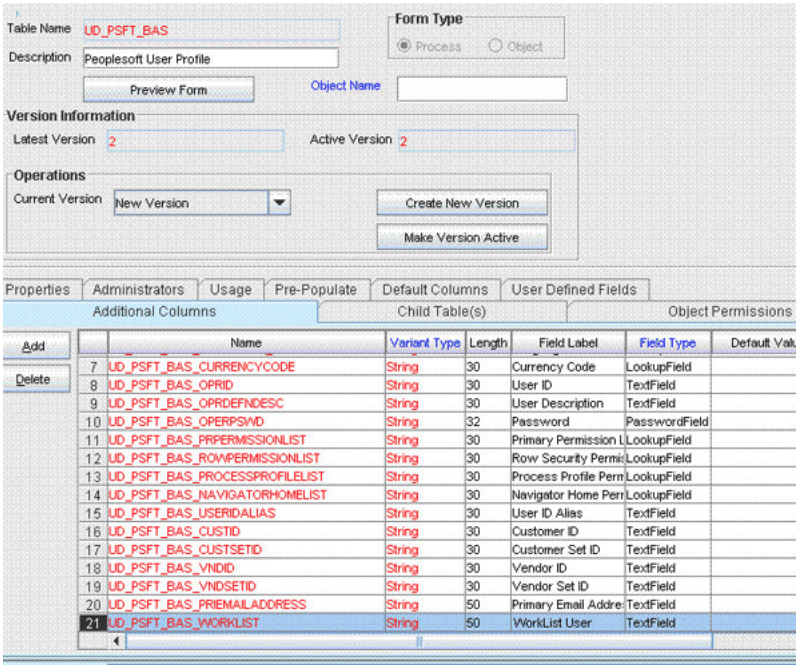
   d. Click **Create New Version.**

   e. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.

   f. From the **Current Version** list, select the newly created version.

   g. On the Additional Columns tab, click **Add.**

   h. Specify the new attribute name, for example, `UD_PSFT_BAS_WORKLIST` and other values.



See Also: *Oracle Identity Manager Design Console Guide* for more information about this step and the remaining steps of this procedure

i. Click the **Make Version Active** button.

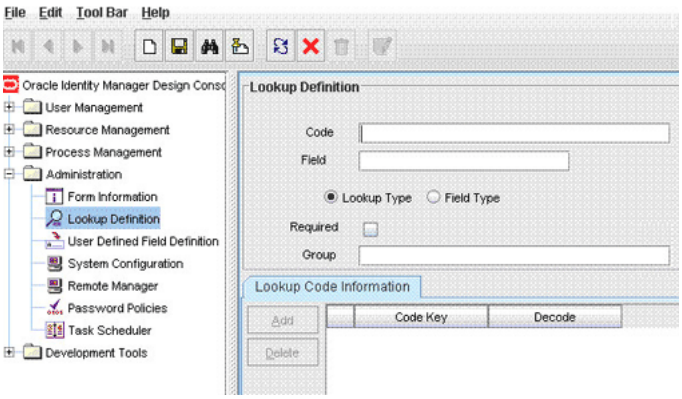
Note: To enable the new attributes perform the procedure described in Section 4.2, "Enabling Update on a New Attribute for Provisioning."

---

2. Add a mapping for the new attribute. To do so:

   a. Log in to the Oracle Identity Manager Design Console.

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



   c. Enter the Lookup.PSFT.UM.Attr.Map.Prov as the name of the lookup definition in the **Code** field and click the **Query for records** button.

   d. Modify the Lookup.PSFT.UM.Attr.Map.Prov lookup definition and add a new row with the form column name as `code` and target field name as `decode`.

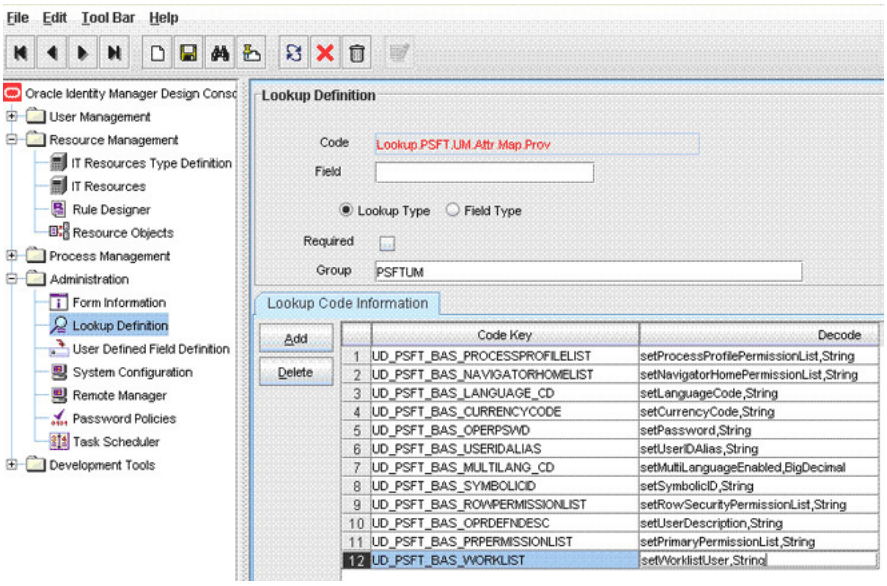
      The format that you must use is as follows:

FORM COLUMN NAME=TARGET API NAME

For example:

To add the Worklist field, you must add the following Code Key and Decode values in the Lookup.PSFT.UM.Attr.Map.Prov lookup definition:

Code Key	Decode
UD_PSFT_BAS_WORKLIST	setWorklistUser,String



Note: The peoplesoft.jar file must contain a setWorklistUser API for the attribute in the Decode column of the lookup. This Decode value is case sensitive.

The Decode value is a combination of APIName and DataType separated by a comma (,). The supported data types are String, Date, Boolean, and BigDecimal.

3. Update the request dataset.

   When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

   a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

   b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

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

      For example, while performing Step 1 of this procedure, if you added City as an attribute on the process form, then enter the following line:

      ```
      <AttributeReference
      ```

```
name = "City"
attr-ref = "City"
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_PSFT_BAS_CITY is the value in the Name column of the process form, then you must specify `CITY` is 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 while performing Step 1.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 1.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 1.
- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 1.
- For the available-in-bulk attribute, specify `true` if the data value is available for bulk modification. Otherwise specify `false`.

While performing Step 1, if you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

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

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

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

See Section 2.3.1.9.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

4.2 Enabling Update on a New Attribute for Provisioning

To enable the update of newly provisioned attributes:

Note:

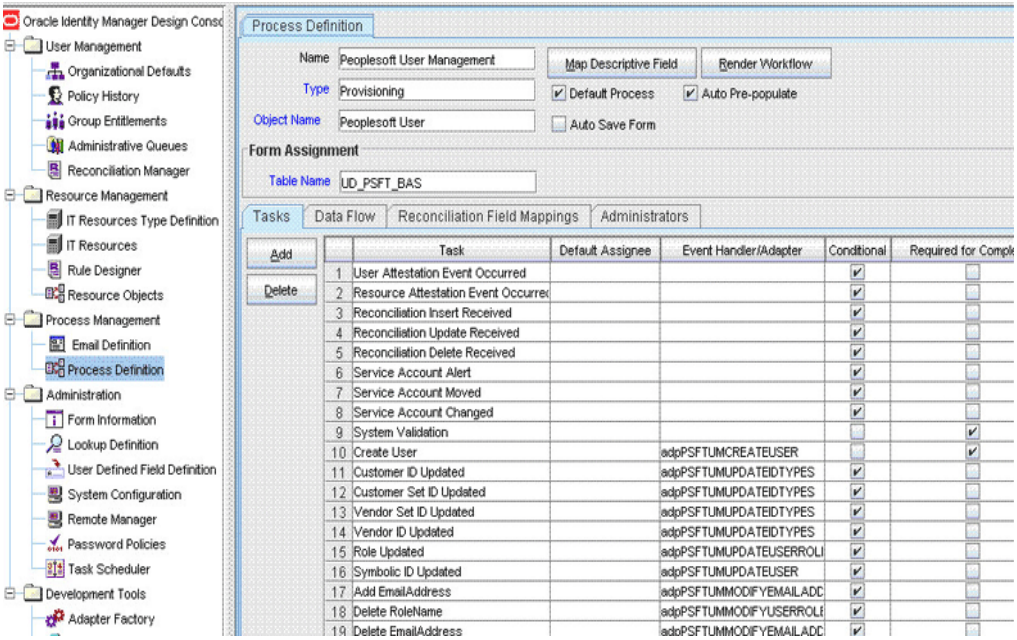
Some of the steps in the following procedure are specific to the values that have been used. If you use other values, then these steps must be performed differently.

To add new attributes for provisioning, see Section 4.1, "Adding New Attributes for Provisioning."

---

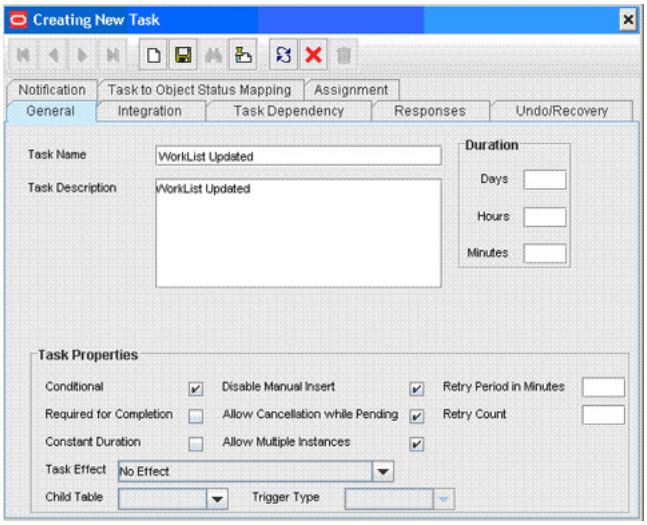
1. Log in to the Oracle Identity Manager Design Console.

2. Expand **Process Management** and then double-click **Process definition.**
3. In the Name field, enter `Peoplesoft User Management` and then click the **Query for records** button.

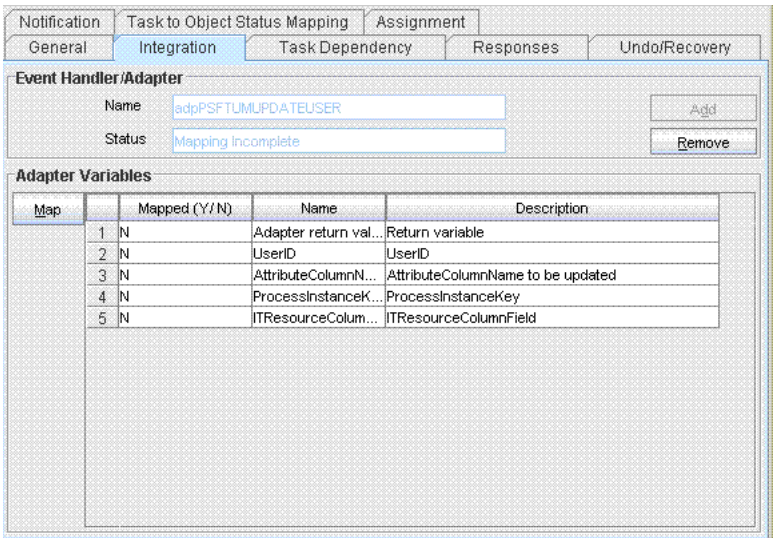


4. Add a new task, for example `WorkList User Updated` and save the task.

Note: While creating a new task, ensure that the task name is same as the name of the field in the process form.

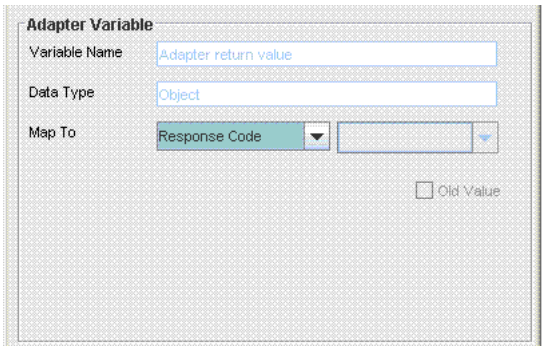


5. Click the **Integration** tab of the WorkList User Updated task, and then click **Add.**
6. Select **Adapter** as the handler type and then perform the following:
   a. Select **ADPPSFTUMUPDATEUSER** and click **Save.**



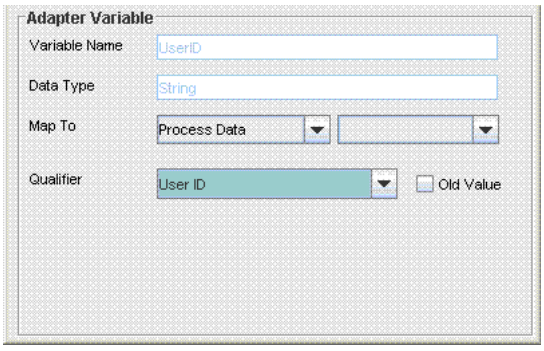
b. In the Adapter Variables region, double-click **Adapter return value**. A window is displayed for editing the data mapping for the variable.

c. From the Map To list, select **Response Code** and then click **Save.**



d. In the Adapter Variables region, double-click **UserID.** A window is displayed for editing the data mapping of the variable.

e. From the Map To list, select **Process Data** and from the Qualifier list, select **User ID** and then click **Save.**



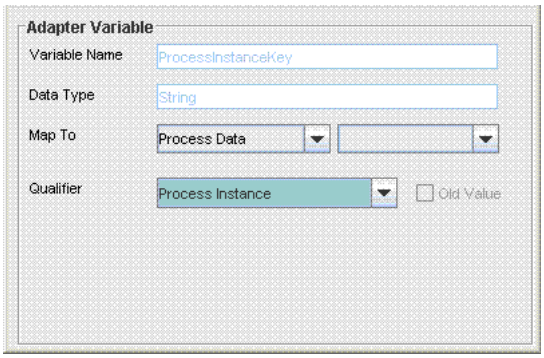
f. In the Adapter Variables region, double-click **AttributeColumnName.** A window is displayed for editing the data mapping of the variable.

g. From the Map To list, select **Literal.**

h. In the Literal Value field, enter `UD_PSFT_BAS_WORKLIST` as the column name for the new attribute that was added in the Lookup.PSFT.UM.Attr.Map.Prov lookup definition.

i. In the Adapter Variables region, double-click **ProcessInstanceKey.** A window is displayed for editing the data mapping of the variable.

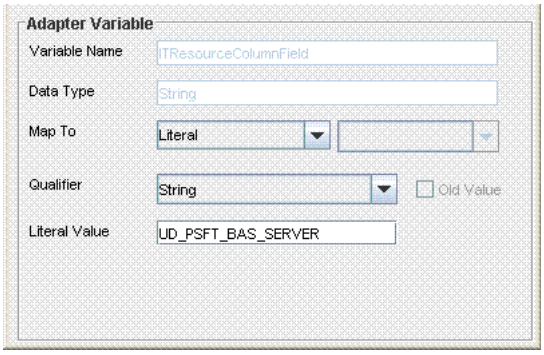
j. From the Map To list, select **Process Data** and from the Qualifier list, select **Process Instance** and then click **Save.**



k. In the Adapter Variables region, double-click **ITResourceColumnField.** A window is displayed for editing the data mapping of the variable.

l. From the Map To list, select **Literal.**

m. In the Literal Value field, enter `UD_PSFT_BAS_SERVER` as the column name of the ITResource field.



7. Perform the mappings and save the form.

8. Click the **Responses** tab of the Worklist Updated task. The `PSFT.USER_MODIFIED_SUCCESSFUL` response should be mapped to status **C** and all other responses to status **R.**

Note: You must enter `Y` or `N` in the WorklistUser field, because PeopleSoft accepts only these values.

4.3 Adding New Attributes for Reconciliation

You can modify the default field mappings between Oracle Identity Manager and the target system. For example, the Lookup.PSFT.UM.UserProfile.AttributeMapping lookup definition for the USER_PROFILE message holds the default attribute mappings. If required, you can add to this predefined set of attribute mappings.

To add a new attribute for reconciliation:

Note: If you do not want to add new attributes for reconciliation, then you need not perform this procedure.

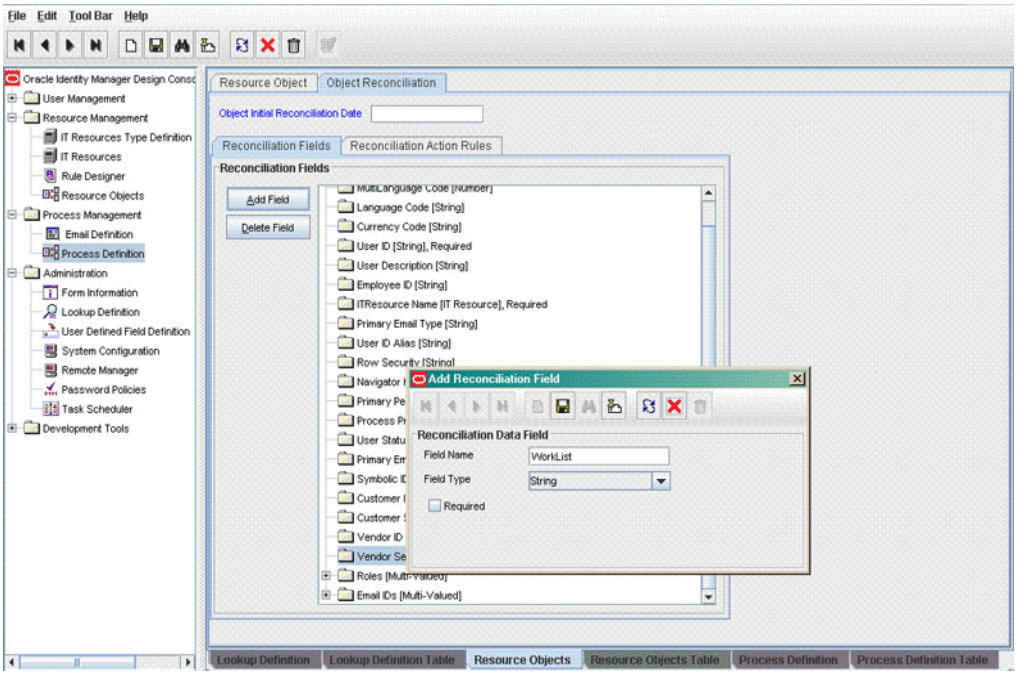
1. In the Oracle Identity Manager Design Console, make the required changes as follows:

   See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions on performing the following steps

   a. Add a new attribute on the process form. See Section 4.1, "Adding New Attributes for Provisioning" for more information.

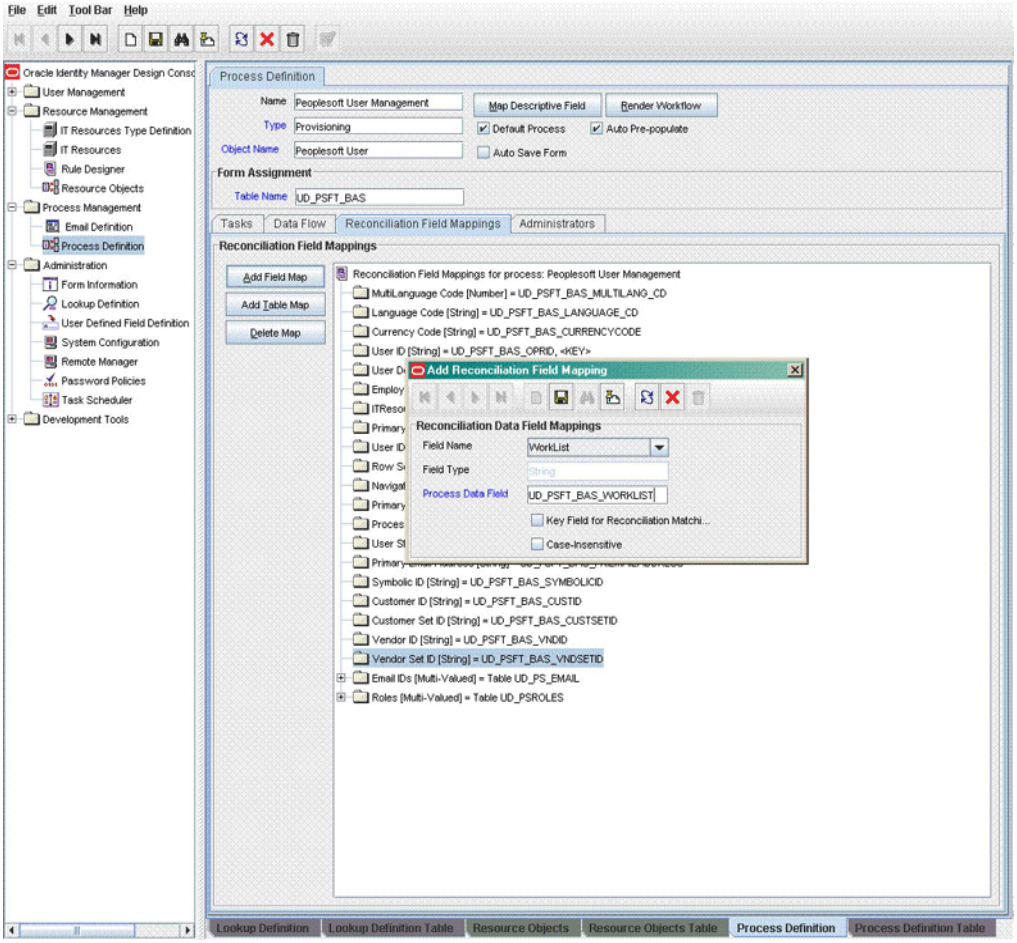
   b. If you are using Oracle Identity Manager release 11.1.1, then on the Object Reconciliation tab, click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

   c. Add a reconciliation field corresponding to the new attribute in the Peoplesoft User resource object. For example, you can add the WorkList reconciliation field.



   d. Modify the Peoplesoft User Management process definition to include the mapping between the newly added field and the corresponding reconciliation field.

      The mapping is shown in the following screenshot:



2. Add the new attribute in the message-specific attribute mapping lookup definition, for example, the Lookup.PSFT.UM.UserProfile.AttributeMapping lookup definition for the USER_PROFILE message.

   The following is the format of the values stored in this table:

Code Key	Decode
AttributeName	*NODE~PARENT NODE~NODE TYPE=Value~EFFECTIVE DATED NODE~PRIMARY or Child Table=Multivalued Child Table RO Field*

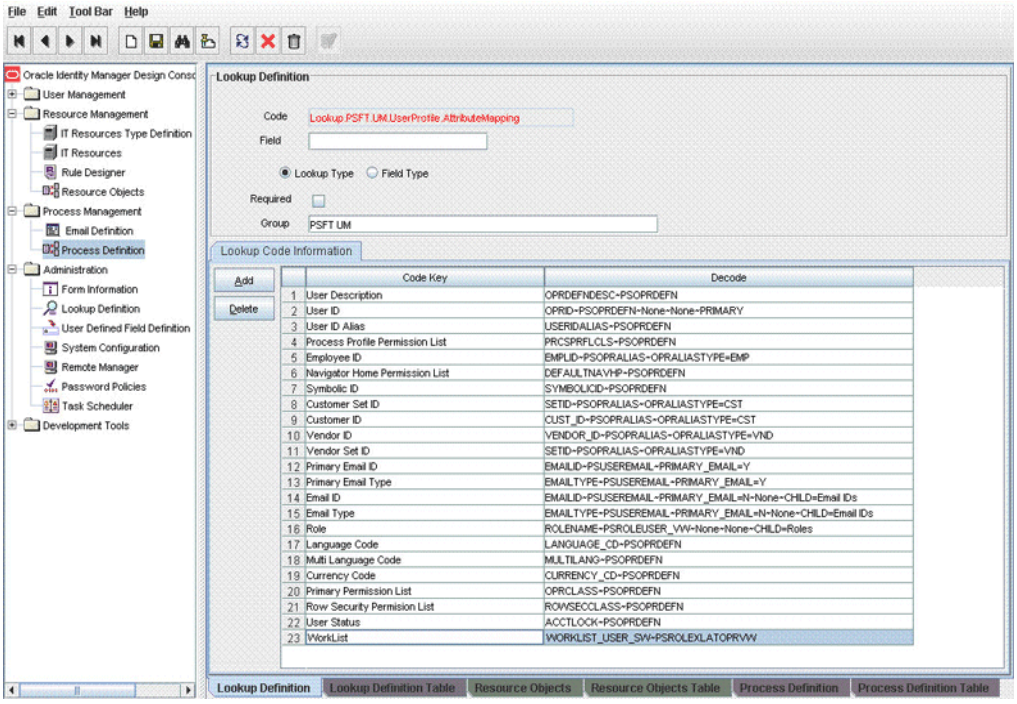
   For example:

   Code Key: WorkList

   Decode: WORKLIST_USER_SW~PSROLEXLATOPRVW

   In this example, WorkList is the reconciliation field, and its equivalent target system field is WORKLIST_USER_SW.

   The mapping is shown in the following screenshot:



3. Add the new attribute in the Resource Object attribute reconciliation lookup definition, for example, the Lookup.PSFT.UM.UserProfile.Recon lookup definition for the USER_PROFILE message.

The following is the format of the values stored in this table:

Code Key	Decode
RO Attribute	*ATTRIBUTE_NAME~LOOKUP_DEFINITION_NAME~LOOKUP_FIELD*

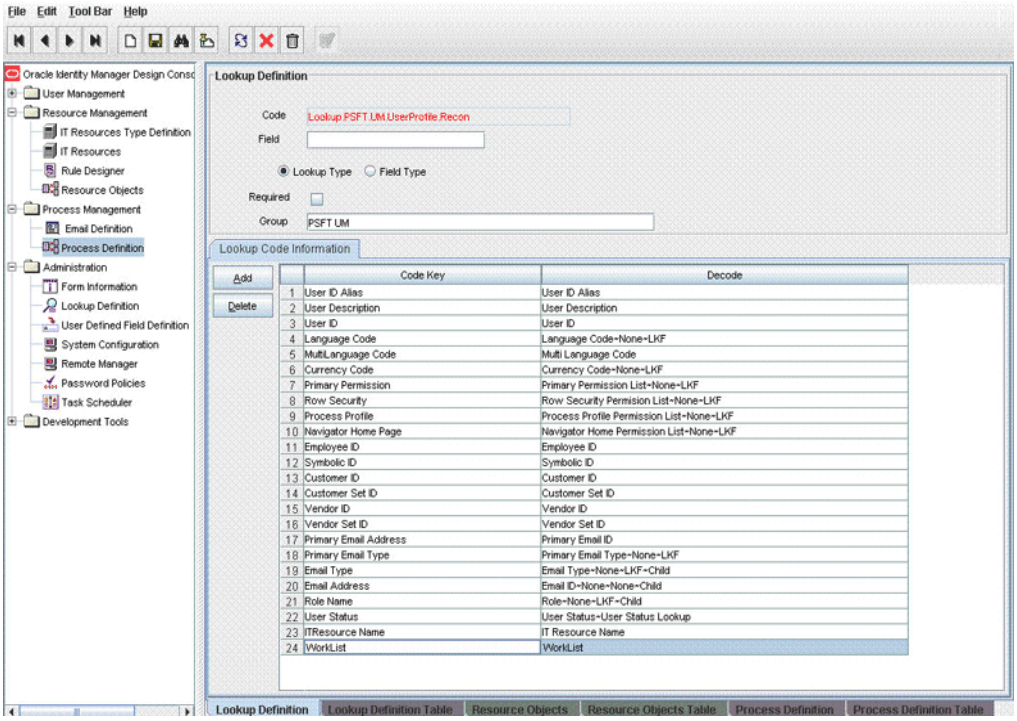
In this example, RO Attribute refers to the resource object attribute name added in the preceding steps. The Decode column refers to the Code Key value in the message-specific attribute mapping lookup definition.

For example:

Code Key: WorkList

Decode: WorkList

The following screenshot displays the mapping:



4.4 Adding New ID Types for Provisioning

A user profile describes a particular user of the PeopleSoft system. Each user of the system has an individual user profile, which in turn is linked to one or more roles. Typically, a user profile must be linked to at least one role to be a usable profile. To each role, you can add one or more permission lists, which control what a user can and cannot access. So, a user inherits permissions through the role.

You can categorize user profiles based on ID types. In addition, you can grant data access based on ID type, such as customer, employee, and so on.

The Human Resource system is designed to focus on employee user type. On the other hand, the financial system is designed to keep track of customer and supplier user types. The ID type enables you to link user types with records that are most relevant when a user interacts with the system. So, when a user logs in to the PeopleSoft application, they see information relevant to them.

The Attribute Value field is where you select the value associated with the attribute name for the ID type. For example, the value reflects the employee number, but it could be a customer number or a vendor number.

PeopleSoft supports Customer and Vendor ID types in addition to Employee ID type. You can also add new ID types depending on the PeopleSoft application module being provisioned. The new ID type can then be linked to a user profile for provisioning.

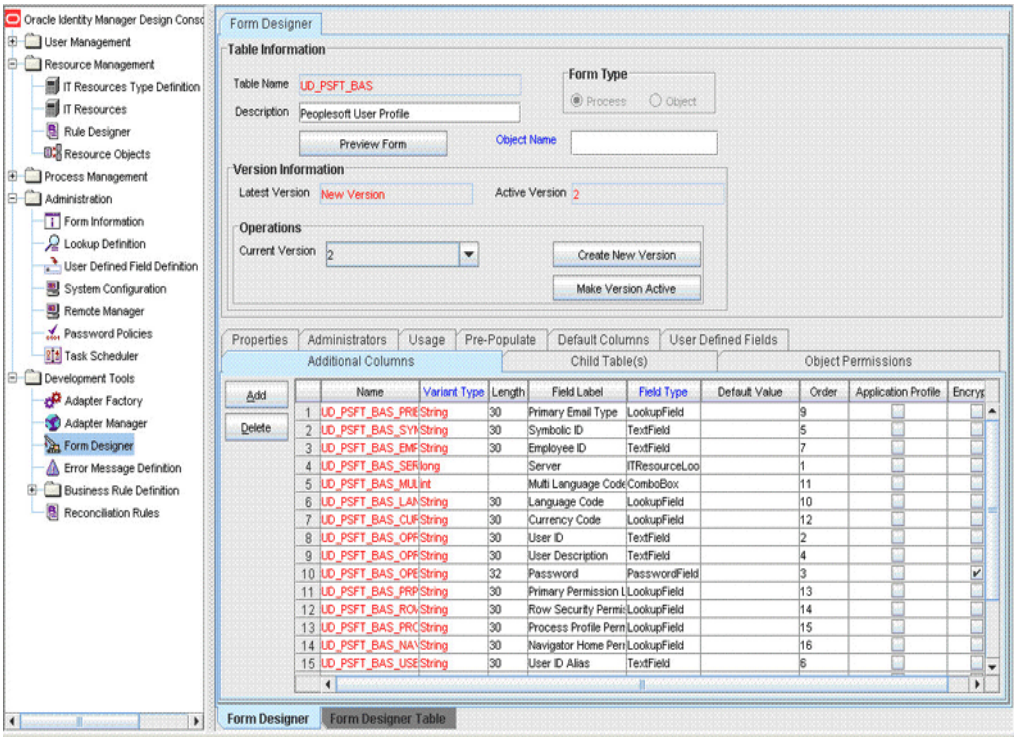
Note: The ID type and attributes discussed in the following procedure are sample values, and might differ from the values in the actual environment. Therefore, you must follow the same procedure with the values applicable in your present environment.

Suppose you want to add a new ID type Department with attributes SetID and Department. Perform the steps mentioned in the following procedure:

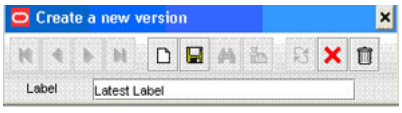
Note: The ID type attribute that you decide to use while configuring the new user profile ID type must map to a field in the PSOPRALIAS table.

To add a new ID type for provisioning:

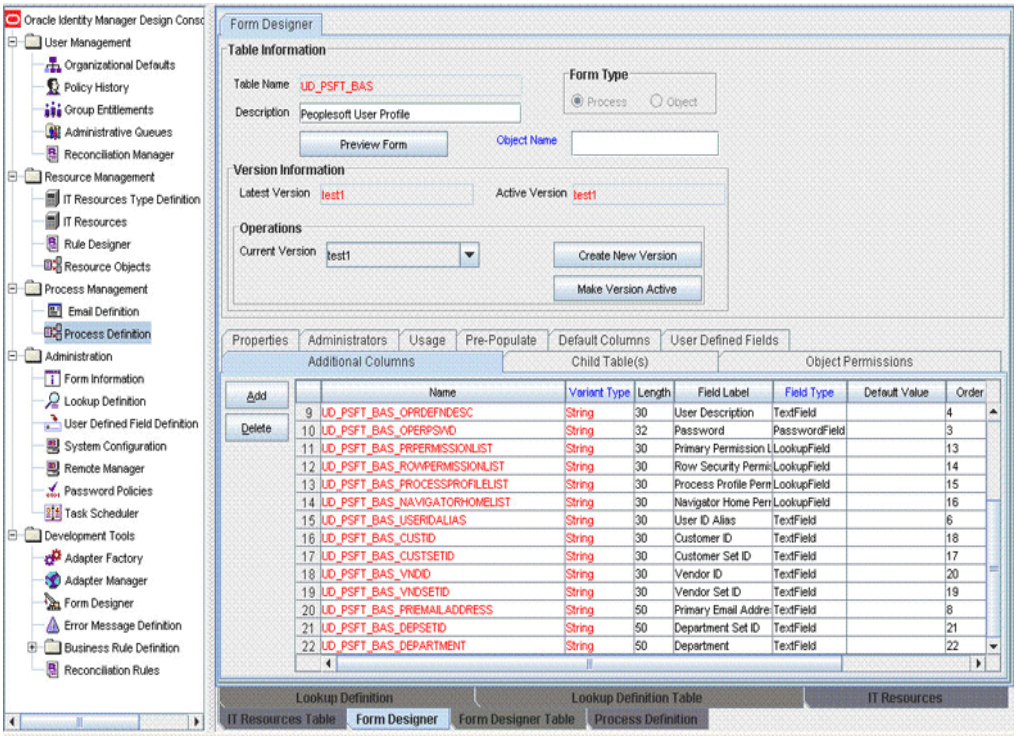
1. Add a new column to the process form by performing the following steps:
   a. Log in to the Oracle Identity Manager Design Console.
   b. Expand **Development Tools** and then double-click **Form Designer.**
   c. In the Table Name field, enter `UD_PSFT_BAS` and click the **Query for records** button.



   d. Click **Create New Version.**
   e. In the Create a new version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.



   f. From the **Current Version** list, select the newly created version.
   g. On the Additional Columns tab, click **Add.**
   h. Specify the new attribute name for the attribute Set ID, for example `UD_PSFT_BAS_DEPSETID`. In addition, enter other values, such as the field label as `Department Set ID`.



See Also: *Oracle Identity Manager Design Console Guide* for more information about this step and the remaining steps of this procedure

i. Click **Make Version Active.**

2. Add a mapping for the new ID type attribute. To do so:

   a. Log in to the Oracle Identity Manager Design Console.

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

   c. Enter `Lookup.PSFT.UM.AttrMap.IDTypes` as the name of the lookup definition in the Code field and click the **Query for records** button.

   d. Modify the Lookup.PSFT.UM.AttrMap.IDTypes lookup definition by adding a new row with the following values:

      Code Key: Column name of the form

      Decode: It is a combination of the following elements:

      ID TYPE~ATTRIBUTE NAME#EXECUTION ORDER NUMBER

      In this format, tilde (~) is used as a separator between ID type and the corresponding attribute. The number sign (#) is used as a separator to define the execution order.

      The format that you must use is as follows:

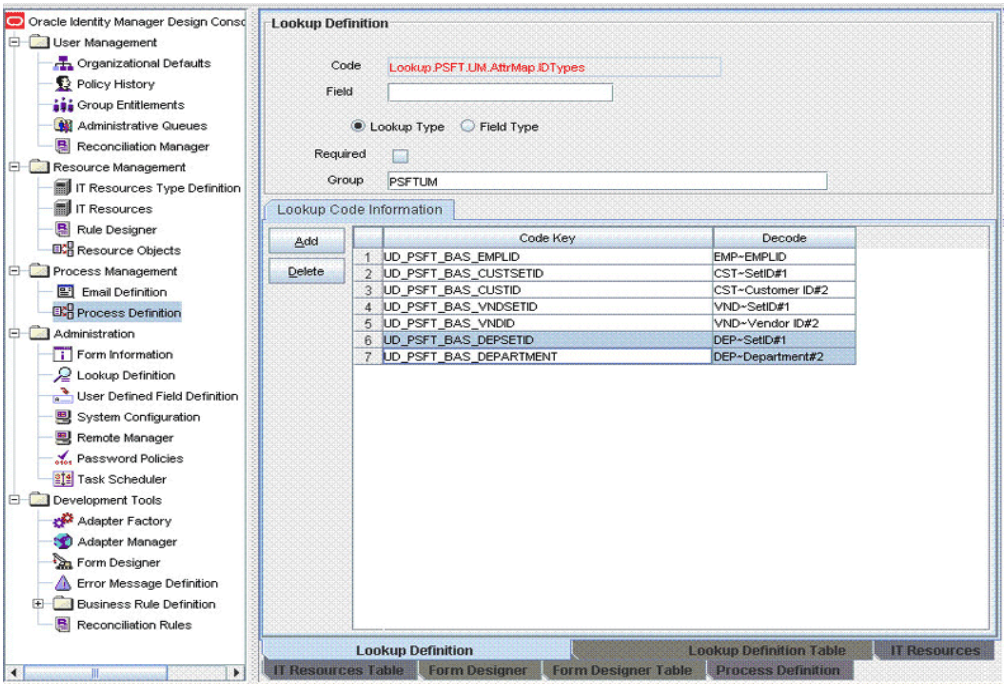
      FORM COLUMN NAME=ID TYPE~ATTRIBUTE NAME#EXECUTION ORDER NUMBER

      To add Department ID type with the ID type value Dep, and attribute names Set ID and Department, you must define the following mapping in the Lookup.PSFT.UM.AttrMap.IDTypes lookup definition:

Code Key	Decode
UD_PSFT_BAS_DEPSETID	DEP~SetID#1
UD_PSFT_BAS_DEPARTMENT	DEP~Department#2

In the preceding example, DEP is the User Profile ID type. SetID and Department are the attributes of DEP ID type, and the order of execution is 1 and 2 for the two attributes.

The mapping is shown in the following screenshot:

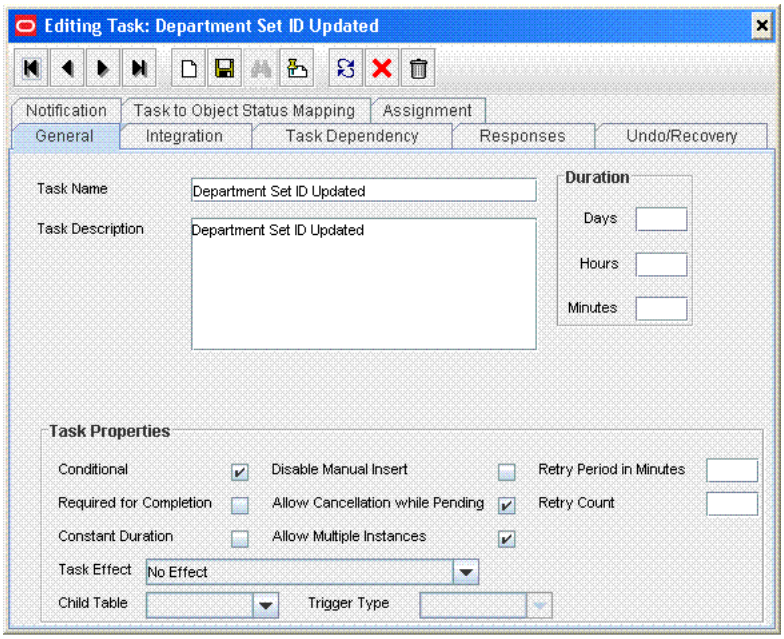


4.5 Enabling Update on a New ID Type for Provisioning

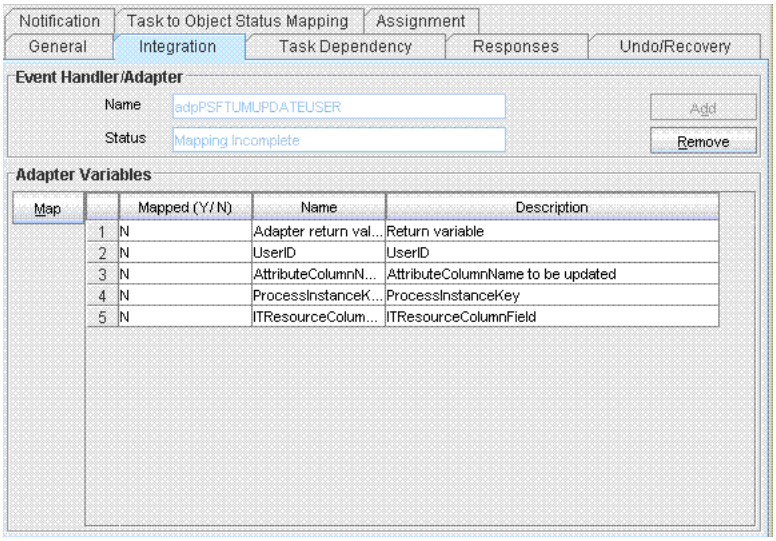
Suppose, you want to update the Department Set ID field as described in Section 4.4, "Adding New ID Types for Provisioning." Then, perform the following procedure:

To update the newly added ID type attributes:

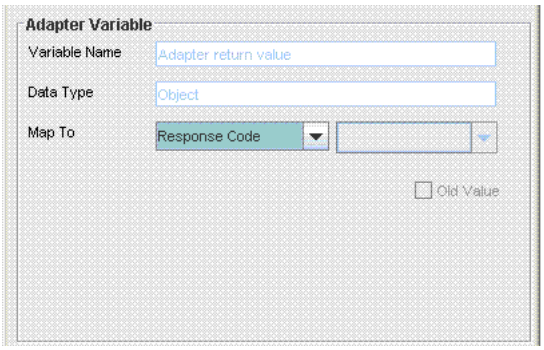
1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Process Management** and then double-click **Process definition.**
3. Enter `Peoplesoft User Management` in the Name field, and then click the **Query for records** button.
4. Add a new task, for example `Department Set ID Updated`, and save the task.



5. Click the **Integration** tab of the Department Set ID Updated task, and then click **Add.**
6. Select **Adapter** as the handler type and then perform the following:
   a. Select **ADPPSFTUMUPDATEIDTYPES** and click **Save.**



   b. In the Adapter Variables region, double-click **Adapter return value.** A window is displayed for editing the data mapping of the variable.



c. From the Map To list, select **Response Code** and then click **Save.**

d. In the Adapter Variables region, double-click **UserID.** A window is displayed for editing the data mapping of the variable.

e. From the Map To list, select **Process Data,** and from the Qualifier list, select **User ID** and then click **Save.**

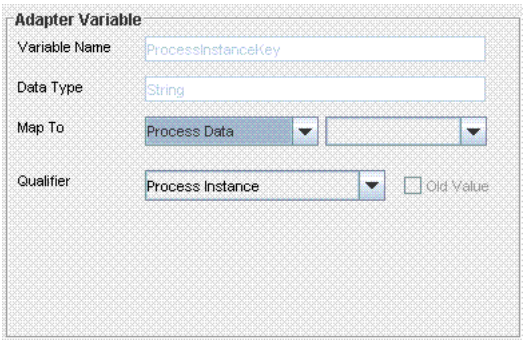
f. In the Adapter Variables region, double-click **IDTypesColumnName.** A window is displayed for editing the data mapping of the variable.

g. From the Map To list, select **Literal.**

h. In the Literal Value field, enter `UD_PSFT_BAS_DEPSETID` as the column name for the new attribute that was added in the Lookup.PSFT.UM.Attr.Map.Prov lookup definition.

i. In Adapter Variables region, double-click **ProcessInstanceKey.** A window is displayed for editing the data mapping of the variable.

j. From the Map To list, select **Process Data,** and from the Qualifier list, select **Process Instance** and then click **Save.**



k. In Adapter Variables region, double-click **ITResourceColumnField.** A window is displayed for editing the data mapping of the variable.

l. From the Map To list, select **Literal.**

m. In the Literal Value field, enter `UD_PSFT_BAS_SERVER` as the column name of the ITResource Field.

7. Perform the mappings and save the format.

8. Click the **Responses** tab of the Department Set ID Updated task. The PSFT.IDTYPES_MODIFIED_SUCCESSFUL response should be mapped with status **C** and all other responses with status **R**.

4.6 Adding New ID Type for Reconciliation

Suppose, you want to reconcile the Department Set ID field as described in Section 4.4, "Adding New ID Types for Provisioning," then perform the following procedure:

To add a new ID type for reconciliation:

1. In the Oracle Identity Manager Design Console, make the required changes as follows:

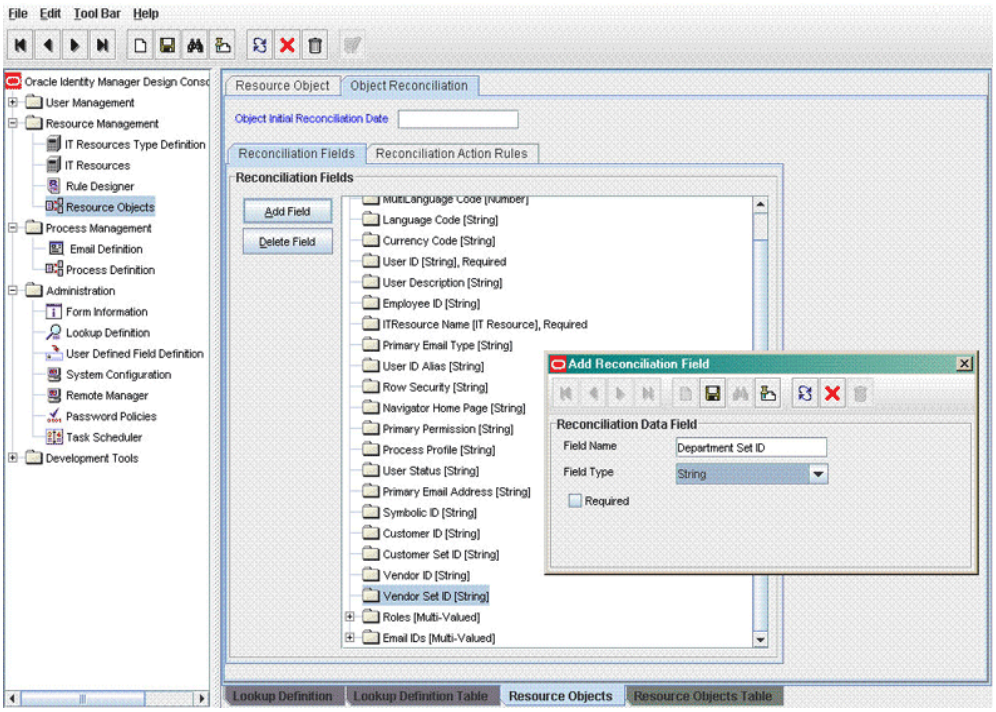
   See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions on performing the following steps

   a. Add new ID Type attribute on the process form. For the procedure to add a new ID Type attribute, see Section 4.4, "Adding New ID Types for Provisioning."

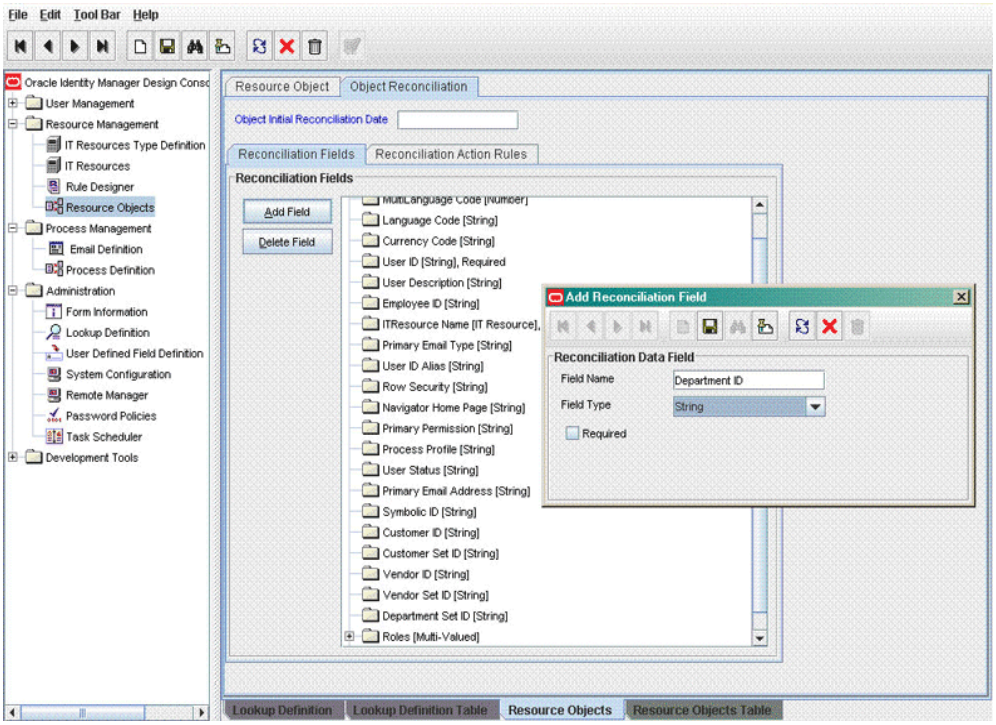
   b. If you are using Oracle Identity Manager release 11.1.1, then on the Object Reconciliation tab, click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

   c. Add a reconciliation field corresponding to the new attribute in the Peoplesoft User resource object.

      The Department Set ID reconciliation field is shown in the following screenshot:

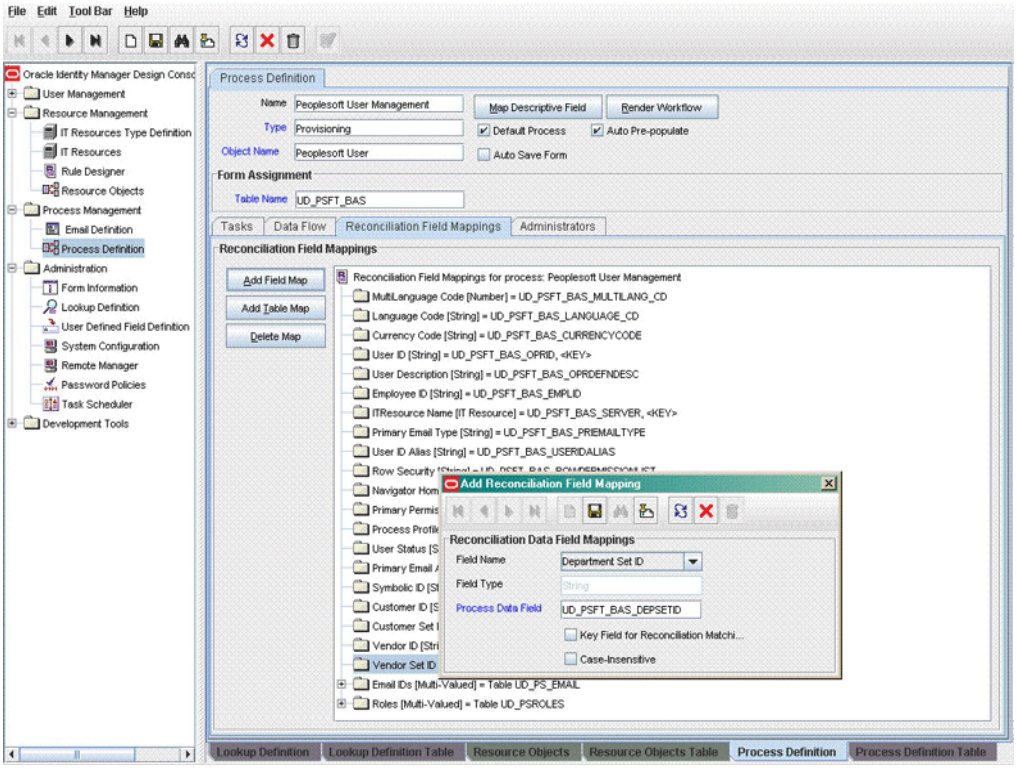


The Department ID reconciliation field is shown in the following screenshot:

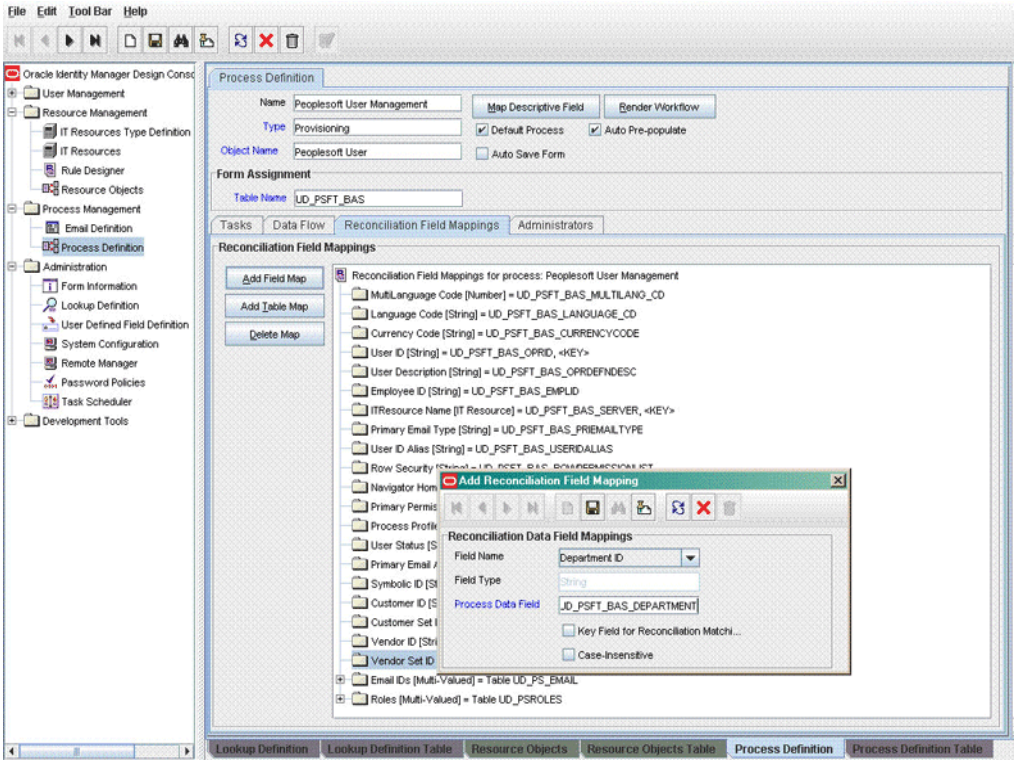


d. Modify the Peoplesoft User Management process definition to include the mapping between the newly added field and the corresponding reconciliation field.

The following screenshot shows the mapping for Department Set ID field:



The following screenshot shows the mapping for the Department ID field:



2. Add the new attribute in the message-specific attribute mapping lookup definition, for example, the Lookup.PSFT.UM.UserProfile.AttributeMapping lookup definition for the USER_PROFILE message.

   The following is the format of the values stored in this table:

Code Key	Decode
AttributeName	*NODE~PARENT NODE~NODE TYPE=Value~EFFECTIVE DATED NODE~PRIMARY or Child Table=Multivalued Child Table RO Field*

   For example:

   Code Key: Department

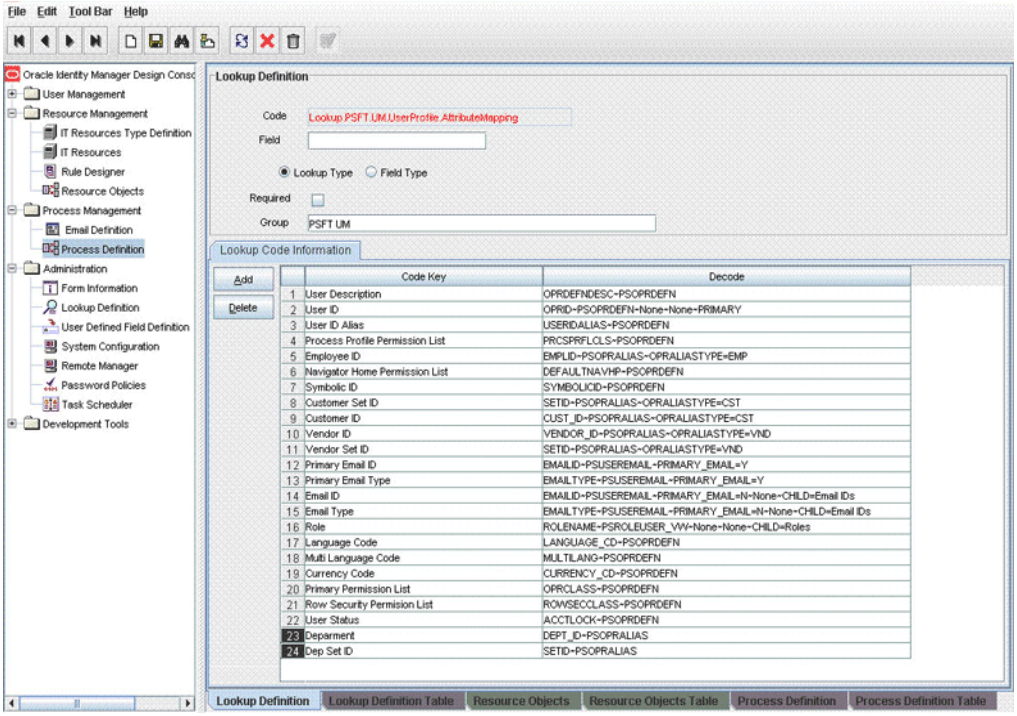
   Decode: DEPT_ID~PSOPRALIAS

   Code Key: Dep Set ID

   Decode: SETID~PSOPRALIAS

   In this example, `Department` is the reconciliation field and its equivalent target system field is Dept_ID. The equivalent target system field for Dep Set ID is SETID.

   The mapping is shown in the following screenshot:



3. Add the new attribute in the Resource Object attribute reconciliation lookup definition, for example, the Lookup.PSFT.UM.UserProfile.Recon lookup for the USER_PROFILE message.

   The following is the format of the values stored in this table:

Code Key	Decode
RO Attribute	*ATTRIBUTE FIELD~LOOKUP NAME~LOOKUP FIELD*

   In this example, the RO Attribute refers to the resource object attribute name added in the preceding steps. The Decode value is the Code Key value in the message-specific attribute mapping lookup definition.

   For example:

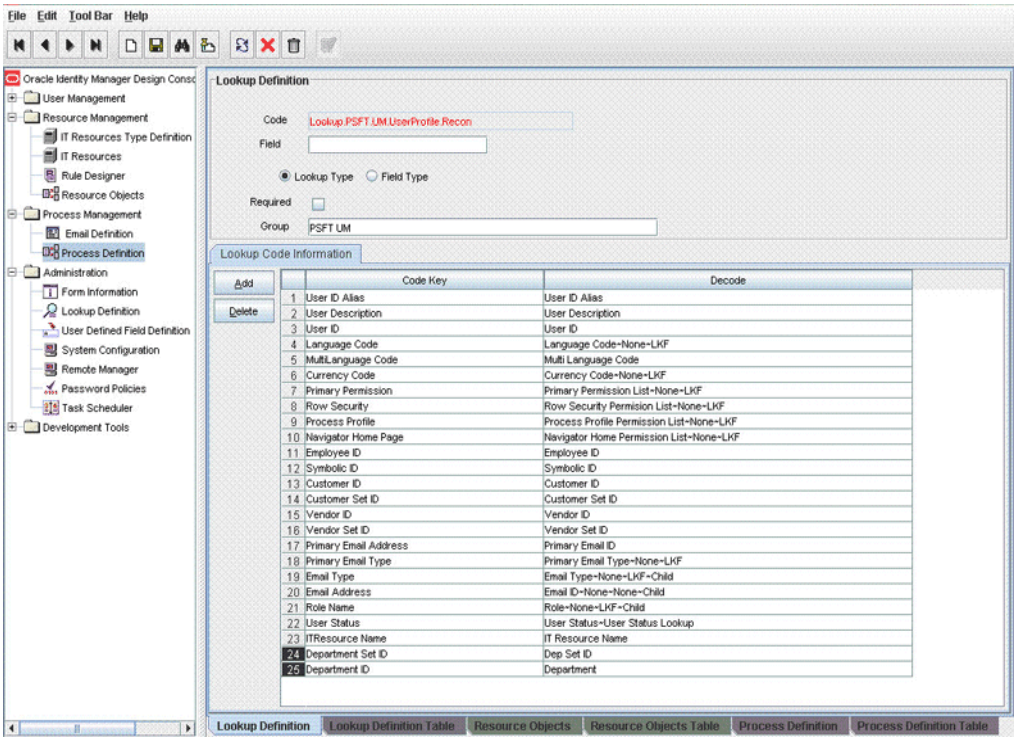
   Code Key: Department Set ID

   Decode: Dep Set ID

   Code Key: Department ID

   Decode: Department

   The following screenshot displays the mapping:



4.7 Configuring Validation of Data During Reconciliation

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data entered in the Currency Code field on the process form so that the number sign (#) is not sent to the Oracle Identity Manager during reconciliation operation.

For data that fails the validation check, the following message is displayed or recorded in the log file:

`Value returned for field` *`FIELD_NAME`* `is false.`

To configure validation of data:

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

   This validation class must implement the oracle.iam.connectors.common.validate.Validator interface and the validate method.

   > **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 Currency Code attribute contains the number sign (#):

```
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 sCurrencyCode=(String) hmUserDetails.get(field);
           for(int i=0;i<sCurrencyCode.length();i++){
             if (sCurrencyCode.charAt(i) == '#'){
                   valid=false;
                   break;
             }
           }
           return valid;
    }
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.

> **Note:** If you are using Oracle Identity Manager release 11.1.1, then see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for steps to import the contents of JavaTasks directory into the Oracle Identity Manager database.

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 message-specific configuration lookup definition, in this example, the **Lookup.PSFT.Message.UserProfile.Configuration** lookup definition for the USER_PROFILE message. See Section 1.5.2.1.1, "Lookup.PSFT.Message.UserProfile.Configuration" for information about this lookup definition. Check for the Validation Lookup Definition parameter in this lookup definition. The Decode value specifies the name of the validation lookup. In this example, the Decode value is Lookup.PSFT.UM.UserProfile.Validation.
   c. Search for and open the **Lookup.PSFT.UM.UserProfile.Validation** lookup definition.
   d. In the Code Key column, enter the resource object name. In the Decode column, enter the class name.

      For example, to perform validation on the Currency Code attribute, you must define the following mapping in the lookup definition:

      Code Key: Currency Code

      Decode: oracle.iam.connectors.recon.validation

      Here, the Code Key value specifies the name of the resource object attribute to validate and the Decode value is the complete package name of the Implementation class.
   e. Save the changes to the lookup definition.

f. Search for and open the message-specific configuration lookup definition, in this example, the Lookup.PSFT.Message.UserProfile.Configuration lookup definition.

g. Set the value of the **Use Validation** entry to `yes`.

h. Save the changes to the lookup definition.

5. Remove the PeopleSoftOIMListener.war file or PeopleSoftOIMListener.ear file depending on the Oracle Identity Manager release from the application server.

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

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:

     a. Copy the *OIM_HOME*/xellerate/XLIntegrations/PSFTUM/WAR/PeopleSoftOIMListener.war file into a temporary folder. Enter the following command to extract the contents of the PeopleSoftOIMListener.war file:

     ```
     jar -xvf PeopleSoftOIMListener.war
     ```

     b. Copy the validation JAR file created in Step 2 to the following directory of the extracted PeopleSoftOIMListener.war file:

     ```
     WEB-INF/lib
     ```

     c. Delete the PeopleSoftOIMListener.war file from the temporary directory into which you extracted its contents.

     d. Use the following command to re-create the file:

     ```
     jar -cvf PeoplesoftOIMListener.war .
     ```

   - If you are using Oracle Identity Manager release 11.1.1, copy the validation JAR file created in Step 2 to the following directory:

     PeoplSoftOIMListener.ear/PeoplSoftOIMListener.war/WEB-INF/lib

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

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then redeploy the PeopleSoftOIMListener.war file on the application server. See Section 2.2.1.5.1, "Deploying the PeopleSoft Listener on Oracle Identity Manager Release 9.1.0.x" for the procedure.

   - If you are using Oracle Identity Manager release 11.1.1, then redeploy the PeopleSoftOIMListener.ear file on the application server. See Section 2.2.1.5.2, "Deploying the PeopleSoft Listener on Oracle Identity Manager Release 11.1.1" for the procedure.

4.8 Configuring Transformation of Data During Reconciliation

You can configure the transformation of reconciled single-valued data according to your requirements. For example, you can use the Currency Code value to create a value for the Currency Code field in Oracle Identity Manager.

To configure the transformation of data:

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

This transformation class must implement the oracle.iam.connectors.common.transform.Transformation interface and the transform method.

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

The following sample transformation class modifies a value for the Currency Code attribute by prefixing a dollar sign ($) in the Currency Code value received from the target system:

```
package oracle.iam.connectors.common.transform;

import java.util.HashMap;

public class TransformAttribute1 implements Transformation {

      /*
      Description:Abstract method for transforming the attributes
      param hmUserDetails<String,Object>
      HashMap containing parent data details
      param hmEntitlementDetails <String,Object>
      HashMap containing child data details

      */
      public Object transform(HashMap hmUserDetails, HashMap
      hmEntitlementDetails,String sField) { {
      /*
       * 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.
       */
      System.out.println("sfield =" + sField);
      String sCurrencyCode= (String)hmUserDetails.get(sField);
      sCurrencyCode = "$"+sCurrencyCode;
      return sCurrencyCode;
      }
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.

> **Note:** If you are using Oracle Identity Manager release 11.1.1, then see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for steps to import the contents of JavaTasks directory into the Oracle Identity Manager database.

4. If you created the Java class for transforming a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Search for and open the message-specific configuration lookup definition, in this example, the Lookup.PSFT.Message.UserProfile.Configuration lookup definition for the USER_PROFILE message. See Section 1.5.2.1.1,

"Lookup.PSFT.Message.UserProfile.Configuration" for information about this lookup definition. Check for the Transformation Lookup Definition parameter in this lookup definition. The Decode value specifies the name of the transformation lookup. In this example, the Decode value is Lookup.PSFT.UM.UserProfile.Transformation.

c. Search for and open the **Lookup.PSFT.UM.UserProfile.Transformation** lookup definition.

d. In the Code Key column, enter the resource object field name. In the Decode column, enter the class name.

For example, to perform transformation on the Currency Code attribute, you must define the following mapping in the lookup definition:

Code Key: Currency Code

Decode: oracle.iam.connectors.common.transform.TransformAttribute1

Here, the Code Key value specifies the name of the resource object attribute on which you have applied transformation and the Decode value is the complete package name of the Implementation class.

e. Save the changes to the lookup definition.

f. Search for and open the message-specific configuration lookup definition, in this example, the Lookup.PSFT.Message.UserProfile.Configuration lookup definition.

g. Set the value of the **Use Transformation** entry to `yes`.

h. Save the changes to the lookup definition.

5. Remove the PeopleSoftOIMListener.war file or PeopleSoftOIMListener.ear file depending on the Oracle Identity Manager release from the application server.

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

- If you are using Oracle Identity Manager release 9.1.0.*x*, then:

a. Copy the *OIM_HOME*/xellerate/XLIntegrations/PSFTUM/WAR/PeopleSoftOIMListener.war file into a temporary folder. Enter the following command to extract the contents of the PeopleSoftOIMListener.war file:

```
jar -xvf PeopleSoftOIMListener.war
```

b. Copy the transformation JAR file created in Step 2 to the following directory of the extracted PeopleSoftOIMListener.war file:

```
WEB-INF/lib
```

c. Delete the PeopleSoftOIMListener.war file from the temporary directory into which you extracted its contents.

d. Use the following command to re-create the file:

```
jar -cvf PeoplesoftOIMListener.war .
```

- If you are using Oracle Identity Manager release 11.1.1, copy the transformation JAR file created is Step 2 to the following directory:

PeoplSoftOIMListener.ear/PeoplSoftOIMListener.war/WEB-INF/lib

7. Depending on the Oracle Identity Manager release that you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then redeploy the PeopleSoftOIMListener.war file on the application server. See Section 2.2.1.5.1, "Deploying the PeopleSoft Listener on Oracle Identity Manager Release 9.1.0.x" for the procedure.
   - If you are using Oracle Identity Manager release 11.1.1, then redeploy the PeopleSoftOIMListener.ear file on the application server. See Section 2.2.1.5.2, "Deploying the PeopleSoft Listener on Oracle Identity Manager Release 11.1.1" for the procedure.

4.9 Configuring Validation of Data During Provisioning

You can configure the validation of provisioned single-valued data according to your requirements. For example, you can validate the user ID provisioned to ensure that it does not contain the number sign (#).

For data that fails the validation check, the following message is displayed or recorded in the log file:

`Value returned for field` *`FIELD_NAME`* `is false.`

In this format, *`FIELD_NAME`* is the name of the field on which you perform validation.

To configure validation of data:

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

   This validation class must implement the oracle.iam.connectors.common.validate.Validator interface and the validate method.

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

   The following sample validation class checks whether the value in the user ID attribute contains the number sign (#):

```
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 sUserID=(String) hmUserDetails.get(field);
            for(int i=0;i<sUserID.length();i++){
              if (sUserID.charAt(i) == '#'){
                    valid=false;
                    break;
```

```
            }
        }
        return valid;
    }
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.

> **Note:** If you are using Oracle Identity Manager release 11.1.1, then see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for steps to import the contents of JavaTasks directory into the Oracle Identity Manager database.

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.PSFT.UM.Validation** lookup definition.
   c. In the Code Key column, enter the column name of the process form field. In the Decode column, enter the class name.

      For example, to perform validation on the user ID attribute, you must define the following mapping in the Lookup.PSFT.UM.Validation lookup definition:

      Code Key: UD_PSFT_BAS_OPRID

      Decode: oracle.iam.connectors.prov.validation

      Here, the Code Key value specifies the column name of the field you want to validate and the Decode value is the complete package name of the Implementation class.
   d. Save the changes to the lookup definition.
5. Set the value of the **Use Validation For Prov** entry to `yes` in the Lookup.PSFT.Configuration lookup definition.
6. Save the changes to the lookup definition.

4.10 Modifying Field Lengths on the Process Form

You might want to modify the lengths of the fields (attributes) on the process form. For example, if you use a Japanese locale, then you might want to increase the lengths of the process form fields to accommodate multibyte data from the target system.

To modify the length of a field on the OIM User form:

1. Log in to the Design Console.
2. Expand **Administration,** and double-click **User Defined Field Definition.**
3. Search for and open the **Users** form.
4. Modify the length of the required field.
5. Click the Save icon.

4.11 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 wants to configure Oracle Identity Manager to link all the installations of the target system.

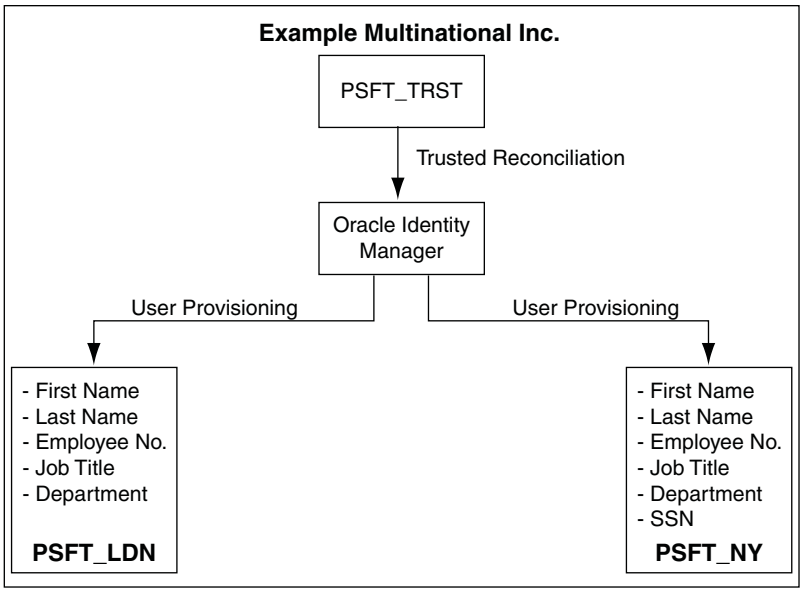
The company has a trusted (authoritative) source of identity data for Oracle Identity Manager, for example PSFT_TRST. The company uses the PeopleSoft Employee Reconciliation connector to reconcile person records, which in turn creates OIM Users.

The company now needs to provision resources on two different target systems, PSFT_LDN and PSFT_NY for London and New York offices, respectively, using the PeopleSoft User Management connector.

The resources in the London office have five mandatory fields to be provisioned. But, the New York office has an additional field to provision, for example the Social Security Number (SSN). In this scenario, you must create a clone of the User Management connector to provision PSFT_LDN and PSFT_NY target systems. The connector for the PSFT_NY target system has an additional SSN field to provision.

Figure 4–1 shows the architecture for multiple installations of the target system in Example Multinational Inc.

Figure 4–1 Architecture for Multiple 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, process form, process definition, 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.

All connector objects are linked. For example, a scheduled task holds the name of the IT resource. Similarly, the IT resource holds the name of the common configuration lookup definition, which is Lookup.PSFT.Configuration. If you create a copy of an object, then you must specify the name of the copy in other connector object. Table 4–1 lists the association between connector objects whose copies can be created and the other objects that reference these objects. When you create a copy of an object, use this information to change the associations of that object with other objects.

Table 4–1 Connector Objects and Their Associations

Connector Object	Name	Referenced By	Description
IT Resource	PSFT Server	■ Scheduled Task: PeopleSoft User Management Target Reconciliation ■ Resource Object: Peoplesoft User	You need to create a copy of IT Resource with a different name.
Resource Object	Peoplesoft User	Message-specific configuration lookup definitions: ■ Lookup.PSFT.Message.UserProfile.Configuration ■ Lookup.PSFT.Message.DeleteUserProfile.Configuration	It is optional to create a copy of a resource object. If you are reconciling the same set of attributes from the other target system, then you need not create a new resource object. **Note:** Create copies of this resource object only if there are differences in attributes between two installations of the target system.
Process Definition	Peoplesoft User Management	NA	It is optional to create a copy of a process definition. If you are reconciling or provisioning the same set of attributes, then you need not create a copy of this connector object. **Note:** Create copies of this process definition only if there are differences in attributes between two installations of the target system.
Process Form	UD_PSFT_BAS	NA	It is optional to create a copy of the process form. If you are provisioning different sets of attributes, then you need to create a copy of this connector object.

Table 4–1 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Description
Common Configuration Lookup Definition	Lookup.PSFT.Configuration	Message-specific configuration lookup definitions: ■ Lookup.PSFT.Message.UserProfile.Configuration ■ Lookup.PSFT.Message.DeleteUserProfile.Configuration	It is optional to create a copy of the common configuration lookup definition. **Note:** Create copies of this lookup definition only if there are differences in attributes between two installations of the target system.
Message-specific Configuration Lookup Definition	■ Lookup.PSFT.Message.UserProfile.Configuration ■ Lookup.PSFT.Message.DeleteUserProfile.Configuration	Attribute mapping lookup definitions: ■ Lookup.PSFT.UM.UserProfile.AttributeMapping ■ Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping	It is optional to create a copy of the message-specific lookup definitions. **Note:** Create copies of this lookup definition only if there are differences in attributes between two installations of the target system.
Attribute Mapping Lookup Definition	■ Lookup.PSFT.UM.UserProfile.AttributeMapping ■ Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping	NA	This lookup definition holds the information of the attributes reconciled from the XML message file from the target system. **Note:** Create copies of this lookup definition only if there are differences in attributes between two installations of the target system.
Recon Map Lookup Definition	■ Lookup.PSFT.UM.UserProfile.Recon ■ Lookup.PSFT.UM.DeleteUserProfile.Recon	NA	This lookup definition maps the resource object field with the data reconciled from the message. **Note:** Create copies of this lookup definition only if there are differences in attributes between two installations of the target system.

To create copies of the connector objects:

> **Note:** See the *Oracle Identity Manager Design Console Guide* for detailed information about the steps in this procedure.

1. Create a copy of the IT resource. See Section 2.2.1.3, "Configuring the IT Resource" for information about this IT resource.

   You can enable dependent lookups if you want to view data in the lookup fields of the process form for the selected IT resource. Section 4.12, "Enabling the Dependent Lookup Fields Feature" describes the procedure to configure the dependent lookups.

2. Create a copy of the Peoplesoft User resource object.

3. Create copy of the USER_PROFILE message-specific configuration lookup.
4. Create a copy of the Lookup.PSFT.Configuration lookup definition. See Section 1.5.2.3.1, "Lookup.PSFT.Configuration" for information about this lookup definition.
5. Create a copy of the message-specific attribute mapping and the Recon lookup definition, for example, Lookup.PSFT.UM.UserProfile.AttributeMapping and the Lookup.PSFT.UM.UserProfile.Recon for the USER_PROFILE message.
6. Create a copy of the PeopleSoft User Management Target Reconciliation scheduled task. See "Configuring the Scheduled Task for User Data Reconciliation" on page 3-6 for information about this scheduled task.
7. Remove the PeopleSoftOIMListener.war file as described in Section 2.2.1.6, "Removing the PeopleSoft Listener."
8. Extract the removed PeopleSoftOIMListener.war file to a temporary folder.
9. Edit the web.xml file as follows:
   a. Search for the </servlet> tag in the file.
   b. Edit the following lines above the </servlet> tag:

```
<init-param>
<!-- Specify Message Handler Impl classes -->
<param-name>IT_RESOURCE_NAME</param-name>
<param-value>MESSAGE~IMPLEMENTATION_CLASS;MESSAGE~IMPLEMENTATION_CLASS;MESS
AGE~IMPLEMENTATION_CLASS</param-value>
</init-param>
```

   Here, IT_RESOURCE_NAME refers to the new IT Resource name defined in Step 1 of this procedure.

   Modify the second line as described in Step 4 (e) of the procedure in Section 2.2.1.5, "Deploying the PeopleSoft Listener."
10. Deploy the PeopleSoftOIMListener.war file as described in Section 2.2.1.5, "Deploying the PeopleSoft Listener."

To reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the `ITResource` scheduled task attribute.

4.12 Enabling the Dependent Lookup Fields Feature

When you perform a provisioning operation, lookup fields on the Administrative and User Console allow you to select values from lists. Some of these lookup fields are populated with values copied from the target system.

In earlier releases of the connector, if you had multiple installations of the target system, then entries in the lookup field were linked to the target system installation from which the entries were copied. This allowed you to select lookup field values that were specific to the target system installation on which the provisioning operation was to be performed.

For release 9.1.1 of the connector, the Dependent Lookup Fields feature is disabled by default. You can enable this feature after you deploy the Oracle Identity Manager release 9.1.0.2 bundle patch BP05 or later.

To enable the Dependent Lookup Fields feature after you deploy the bundle patch BP05 or later, perform the following procedures:

Note: To provision a resource, you enter the required values in the process form with atleast one lookup value selected, for example, Currency Code and then click Continue. But, if you click the Back button now, the description of the Code Key on the process form changes to the Decode value. If you proceed with provisioning now, the following exception is thrown:

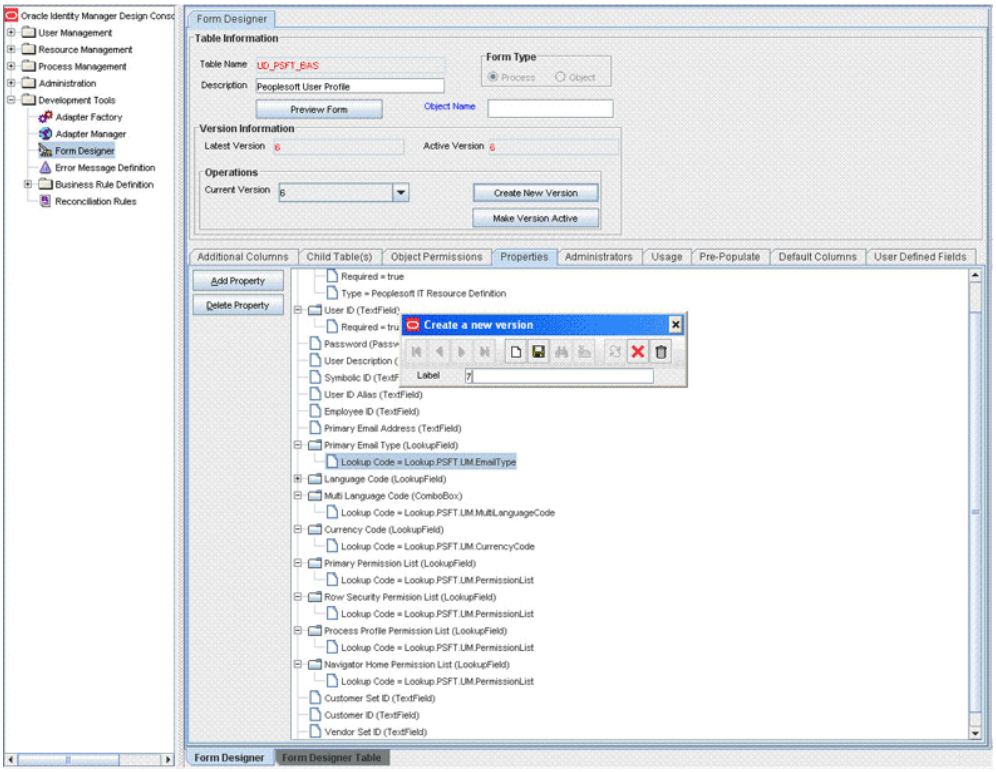
Column data length is too long

- Section 4.12.1, "Updating the UD_PSFT_BAS Form"
- Section 4.12.2, "Updating the UD_PS_EMAIL Form"
- Section 4.12.3, "Updating the UD_PSROLES Form"

4.12.1 Updating the UD_PSFT_BAS Form

Update the UD_PSFT_BAS form as follows:

1. On the Design Console, expand **Development Tools** and double-click **Form Designer.**
2. Search for and open the **UD_PSFT_BAS** form.
3. Click **Create New Version,** enter a new version number, and then save the version.



4. From the **Current Version** list, select the version that you created.
5. Open the **Properties** tab.
6. Add properties for the **Primary Email Type** lookup field as follows:

a. Select the **Lookup Code= Name of Lookup Definition** property, and then click **Delete Property.**

   For example:

   Lookup Code = Lookup.PSFT.UM.EmailType

b. Select **Primary Email Type,** and then click **Add Property.**

c. In the Add Property dialog box:

   From the Property Name list, select **Lookup Column Name.**

   In the **Property Value** field, enter `lkv_encoded`.

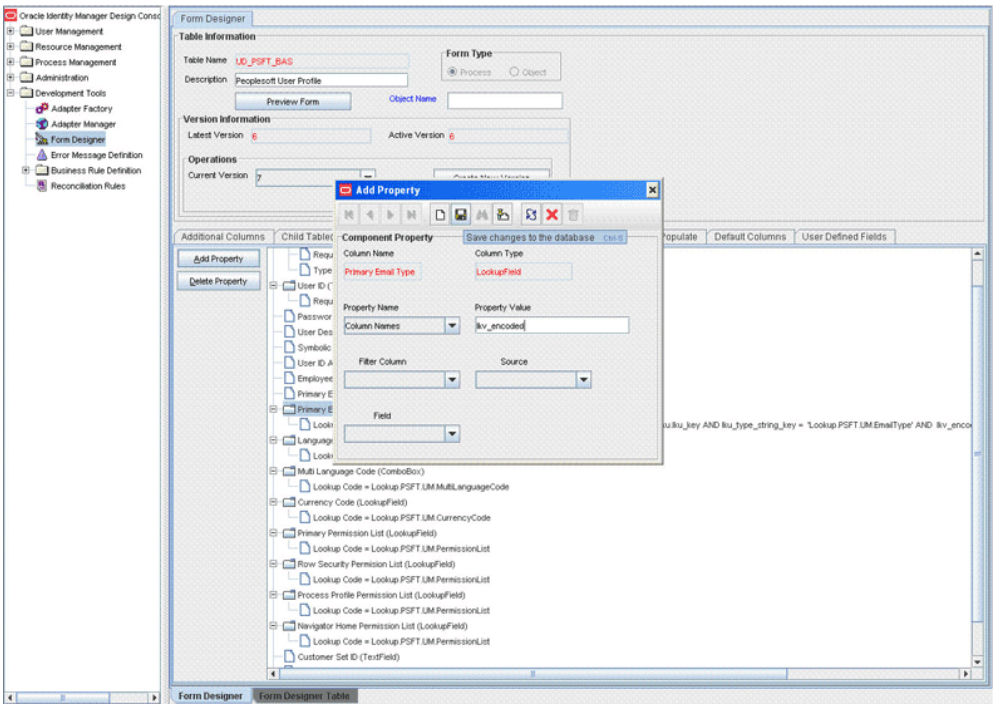
   Click the Save icon, and then close the dialog box.

d. Select **Primary Email Type,** and then click **Add Property.**

e. In the Add Property dialog box:

   From the Property Name list, select **Column Names.**

   In the **Property Value** field, enter `lkv_encoded`.



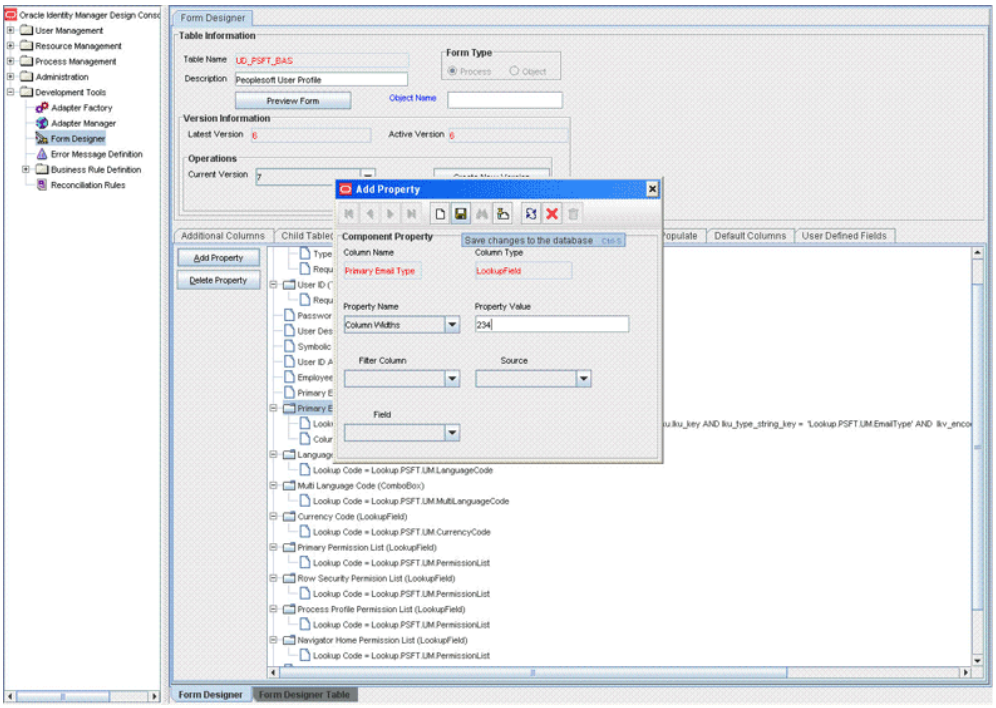
   Click the Save icon, and then close the dialog box.

f. Select **Primary Email Type,** and then click **Add Property.**

g. In the Add Property dialog box:

   From the Property Name list, select **Column Widths.**

   In the **Property Value** field, enter `234`.

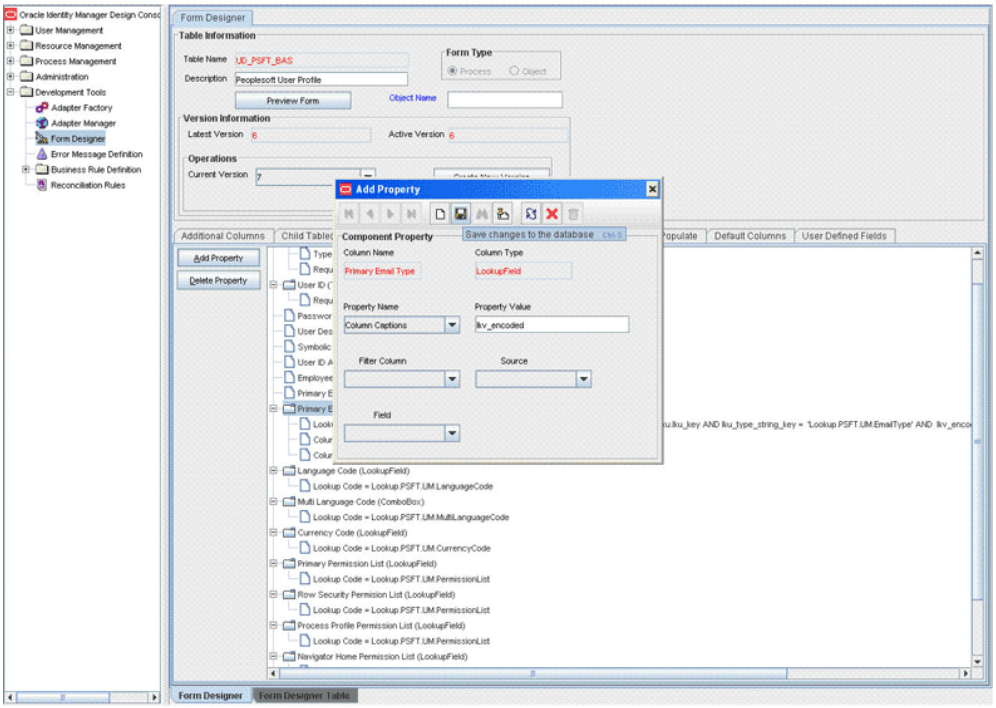


h. Select **Primary Email Type,** and then click **Add Property.**

i. In the Add Property dialog box:

From the Property Name list, select **Column Captions.**

In the **Property Value** field, enter `lkv_decoded`.



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

j. Select **Primary Email Type,** and then click **Add Property.**

k. In the Add Property dialog box:

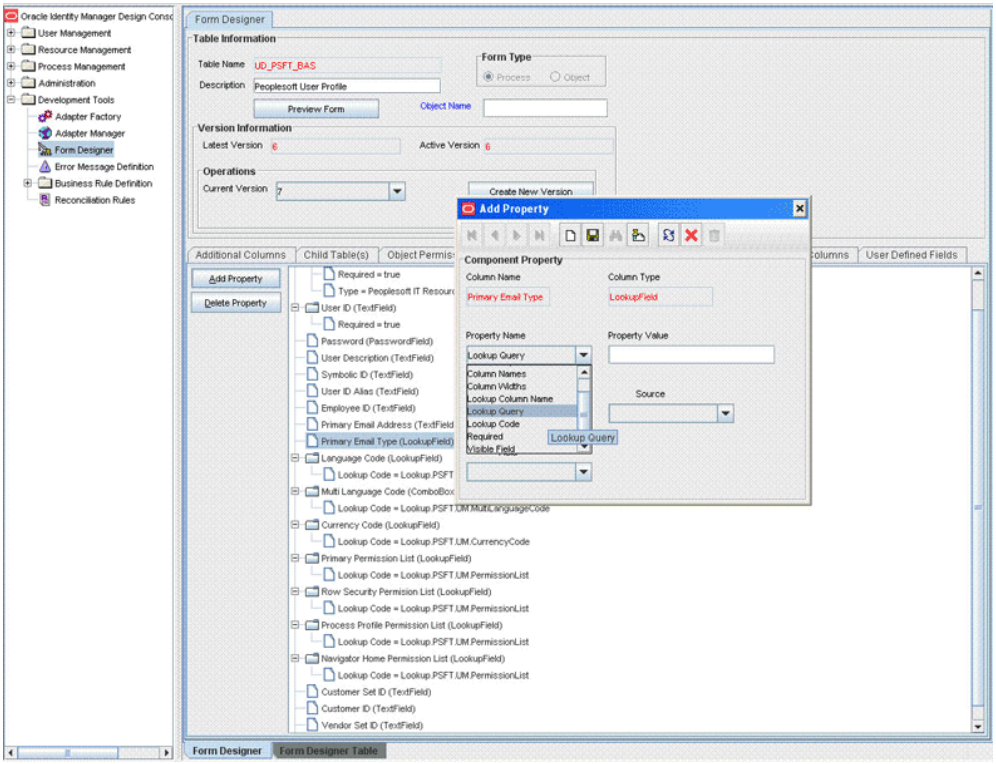
From the Property Name list, select **Lookup Query.**

In the Property Value field, enter the following if Oracle Identity Manager is running on Oracle:

```
SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key =
lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.EmailType' AND
lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$','~%')
```

In the Property Value field, enter the following if Oracle Identity Manager is running on Microsoft SQL Server:

```
SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key =
lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.EmailType'AND
lkv_encoded like '$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
```



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

7. Perform Steps 6.a through 6.j. Add the properties that you added for the Primary Email Type field on the UD_PSFT_BAS form.

8. When you perform Step 6.k, enter values in the Property Value field for the lookup query specified in Table 4–2 for the respective field, such as Language Code, Currency Code, Primary Permission List, Row Security Permission List, Process Profile Permission List, and Navigator Home Permission List.

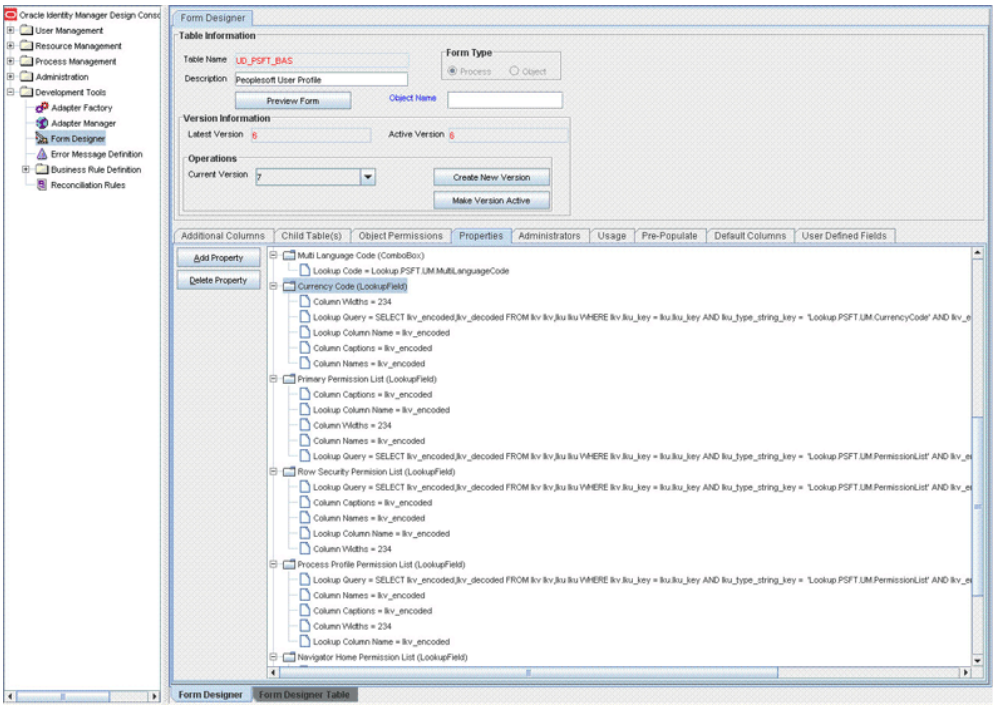


Table 4–2 lists the lookup queries.

Table 4–2 Queries for Lookup Fields

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
Field Name (UD_PSFT_BAS)		
Primary Email Type	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.EmailType' AND lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$', '~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.EmailType'AND lkv_encoded like '$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
Language Code	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.LanguageCode' AND lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$', '~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key ANDlku_type_string_key ='Lookup.PSFT.UM.LanguageCode' AND lkv_encoded like '$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
Currency Code	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.CurrencyCode' AND lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$', '~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key ANDlku_type_string_key = 'Lookup.PSFT.UM.CurrencyCode' AND lkv_encoded like'$Formdata.UD_PSFT_BAS_SERVER$' + '~%'

Table 4–2 (Cont.) Queries for Lookup Fields

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
Primary Permission List	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key ='Lookup.PSFT.UM.PermissionList' AND lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$', '~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key ANDlku_type_string_key = 'Lookup.PSFT.UM.PermissionList' AND lkv_encoded like'$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
Row Security Permission List	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key ='Lookup.PSFT.UM.PermissionList' AND lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$', '~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key ANDlku_type_string_key = 'Lookup.PSFT.UM.PermissionList' AND lkv_encoded like'$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
Process Profile Permission List	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.PermissionList' AND lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$', '~%'	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key ANDlku_type_string_key = 'Lookup.PSFT.UM.PermissionList' AND lkv_encoded like'$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
Navigator Home Permission List	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.PermissionList' AND lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$', '~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key ANDlku_type_string_key = 'Lookup.PSFT.UM.PermissionList' AND lkv_encoded like'$Formdata.UD_PSFT_BAS_SERVER$' + '~%'

9. Click the Save icon to save the changes to the form.
10. Click **Make Version Active.**

4.12.2 Updating the UD_PS_EMAIL Form

The procedure that you perform to update the UD_PS_EMAIL form is almost the same as the procedure described in Section 4.12.1, "Updating the UD_PSFT_BAS Form":

1. On the Design Console, expand **Development Tools** and double-click **Form Designer.**
2. Search for and open the **UD_PS_EMAIL** form.
3. Click **Create New Version,** enter a new version number, and then save the version.
4. From the **Current Version** list, select the version that you created.
5. Open the **Properties** tab.
6. Add properties for the Email Type lookup field as follows:

a. When you perform Step 6.b of the procedure described in Section 4.12.1, "Updating the UD_PSFT_BAS Form," select **Email Type** instead of Primary Email Type.

b. Perform Steps 6.c through 6.j. Add the properties that you added for the Primary Email Type field on the UD_PSFT_BAS form.

c. When you perform Step 6.k, enter the following in the Property Value field for the lookup query:

For Oracle:

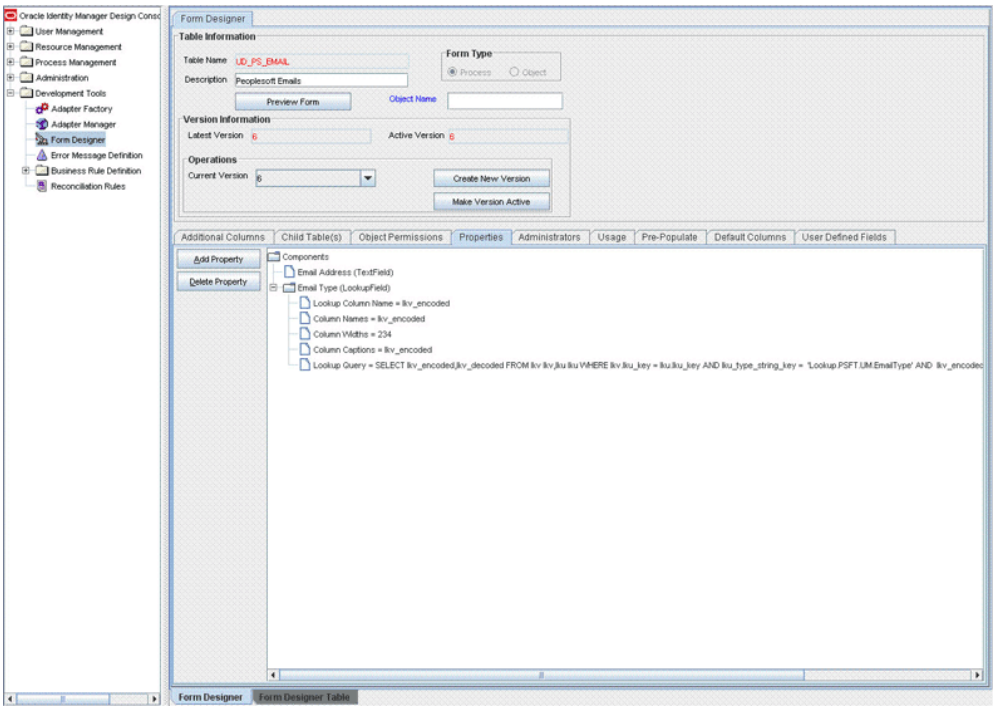
```
SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key =
lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.EmailType' AND
lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$',   '~%')
```

For Microsoft SQL Server:

```
SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE
lkv.lku_key=lku.lku_key
ANDlku_type_string_key='Lookup.PSFT.UM.EmailType'and lkv_encoded
like'$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
```

7. Click the Save icon to save the changes to the form.

8. Click **Make Version Active.**



4.12.3 Updating the UD_PSROLES Form

The procedure that you perform to update the UD_PSROLES form is almost the same as the procedure described in Section 4.12.1, "Updating the UD_PSFT_BAS Form":

1. On the Design Console, expand **Development Tools** and double-click **Form Designer.**

2. Search for and open the **UD_PSROLES** form.

3. Click **Create New Version,** enter a new version number, and then save the version.
4. From the **Current Version** list, select the version that you created.
5. Open the **Properties** tab.
6. Add properties for the Role Name lookup field as follows:
   a. When you perform Step 6.b of the procedure described in Section 4.12.1, "Updating the UD_PSFT_BAS Form," select **Role Name** instead of Primary Email Type.
   b. Perform Steps 6.c through 6.j. Add the properties that you added for the Primary Email Type field on the UD_PSFT_BAS form.
   c. When you perform Step 6.k, enter the following in the Property Value field for the lookup query:

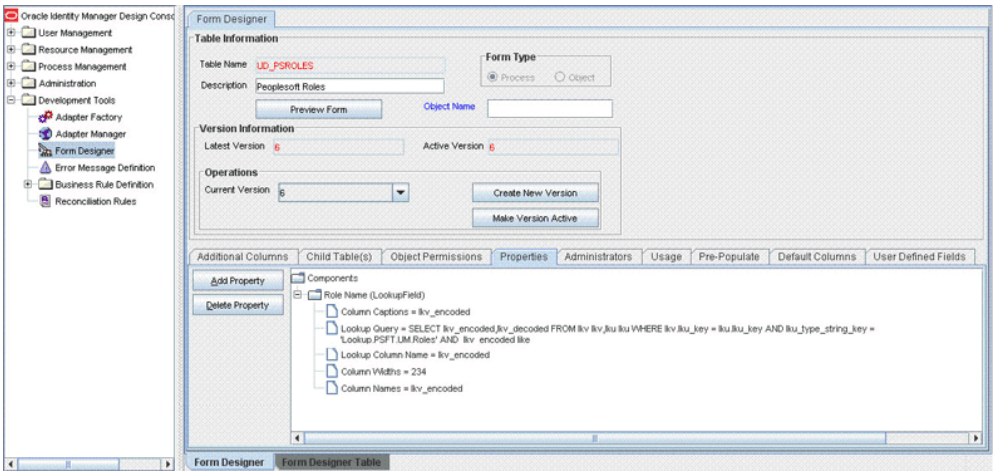
      For Oracle:

      ```
      SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key =
      lku.lku_key AND lku_type_string_key = 'Lookup.PSFT.UM.Roles' AND
      lkv_encoded like CONCAT('$Form data.UD_PSFT_BAS_SERVER$',   '~%')
      ```

      For Microsoft SQL Server:

      ```
      SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE
      lkv.lku_key=lku.lku_key ANDlku_type_string_key='Lookup.PSFT.UM.Roles' AND
      lkv_encoded like'$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
      ```

7. Click the Save icon to save the changes to the form.
8. Click **Make Version Active.**



5 Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- Section 5.1, "Testing Reconciliation"
- Section 5.2, "Testing Provisioning"
- Section 5.3, "Troubleshooting"

5.1 Testing Reconciliation

After you deploy the connector, you must test it to ensure that it functions as expected. The testing utility takes as input the XML file or message generated by the target system. It can be used for testing full and incremental reconciliation.

The testing utility is located in the test directory on the installation media. See Section 2.1.1.1, "Files and Directories on the Installation Media" for more information.

To run the testing utility:

1. Copy the testing utility files to the following directories:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:

     Copy files from the test/config directory on the installation media to the *OIM_HOME*/xellerate/XLIntegrations/PSFTUM/config directory.

     Copy files from the test/scripts directory on the installation media to the *OIM_HOME*/xellerate/XLIntegrations/PSFTUM/scripts directory.
   - If you are using Oracle Identity Manager release 11.1.1, then:

     Copy files from the test/config directory on the installation media to the *OIM_HOME*/server/XLIntegrations/PSFTUM/config directory.

     Copy files from the test/scripts directory on the installation media to the *OIM_HOME*/server/XLIntegrations/PSFTUM/scripts directory.

     Note: You must create the destination directories on the Oracle Identity Manager host computer if they are not present.
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then copy the log4j.jar file into the following directory:

OIM_HOME/xellerate/ThirdParty

- If you are using Oracle Identity Manager release 11.1.1, then copy the lib/PSFTCommon.jar and lib/Common.jar files from installation media into the following directory:

  OIM_HOME/server/JavaTasks

3. Modify the files that you copy into the config directory as follows:

   a. If you are using Oracle Identity Manager release 9.1.0.*x*, then modify the log.properties file as described in Section 2.3.1.2, "Enabling Logging."

   b. Open and edit the reconConfig.properties file as follows:

      i) Enter the PeopleSoftOIMListener servlet URL as the value of ListenerURL in following syntax:

      ```
      http://HOST_NAME:PORT/PeopleSoftOIMListener
      ```

      For example:

      ```
      ListenerURL=http://10.1.6.83:8080/PeopleSoftOIMListener
      ```

      ii) Enter the absolute XML message file path as the value of XMLFilePath as shown in the following example:

      ```
      XMLFilePath=c:/xmlmessages/user_profile.xml
      ```

      Note: Ensure that there is no blank or white-space character in the directory path and file name that you specify.

      iii) Enter a value for the MessageType. For a ping message, specify `Ping`, `None`, or `otherwise` as shown in the following example:

      ```
      MessageType=None
      ```

      iv) Enter a value for **ITResourceName.** This value must match the active IT resource in Oracle Identity Manager.

      For example:

      ```
      ITResourceName=PSFT Server
      ```

      v) Enter the name of the message for which you are run the testing utility.

      For example:

      ```
      MessageName=USER_PROFILE
      ```

   c. Open a command window, and navigate to the following directory:

      If you are using Oracle Identity Manager release 9.1.0.*x*, then:

      OIM_HOME/xellerate/XLIntegrations/PSFTUM/scripts

      If you are using Oracle Identity Manager release 11.1.1, then:

      OIM_HOME/server/XLIntegrations/PSFTUM/scripts

   d. Run the following script:

      For Microsoft Windows:

      ```
      InvokeListener.bat
      ```

For UNIX:

```
InvokeListener.sh
```

After the testing utility completes the run, it creates a reconciliation event. Verify that the reconciliation event is created in Oracle Identity Manager and that the event contains the data specified in the message-specific XML file.

5.2 Testing Provisioning

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

When you run the testing utility, it reads the connectivity information from the IT Resource, lookup definitions from Oracle Identity Manager, and process form data is read from the config.properties file.

While running the testing utility, you must ensure that Oracle Identity Manager is running.

Note: The testing utility might not work on Oracle Identity Manager release 9.1.0.*x* running on IBM WebSphere Application Server, Oracle WebLogic Server, or Oracle Application Server.

---

1. Depending on the Oracle Identity Manager release that you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager 9.1.0.*x*, then copy the following files to *OIM_HOME*/xellerate/ThirdParty directory:

     For IBM WebSphere Application Server:

     com.ibm.ws.admin.client_6.1.0.jar from *WAS_HOME*/AppServer/runtimes

     ibmorb.jar from *WAS_HOME*/AppServer/java/jre/lib

     xlDataObjectBeans.jar from *OIM_CLIENT*/xlclient/lib

     For JBoss Application Server:

     jbossall-client.jar from *OIM_CLIENT*/xlclient/ext

     log4j.jar from *JBOSS_HOME*/server/default/lib

     xlGenericUtils.jar from *OIM_HOME*/xellerate/lib

     For Oracle WebLogic Server:

     weblogic.jar from *BEA_HOME*/weblogic81/server/lib

   - If you are using Oracle Identity Manager 11.1.1, then:
     a. Create the wlfullclient.jar file by using the WebLogic JarBuilder Tool. See Oracle WebLogic Server documentation for more information.
     b. Copy the wlfullclient.jar file to the *OIM_HOME*/server/ThirdParty directory.
     c. Copy the lib/PSFTUM.jar, lib/PSFTCommon.jar, and lib/Common.jar files from installation media into the following directory:

        OIM_HOME/server/JavaTasks

2. Modify the attributes of the config.properties file using the values specified in the following table. This file is located in the config directory on the installation media. Table 5–1 describes each property:

Table 5–1 Properties of config.properties File

Property	Description	Default Value
ACTION	Specify the action that you want the testing utility to perform. You can enter one of the following values: `CONNECT,CREATE,DELETE,ENABLE, DISABLE,UPDATEUSER,UPDATEEMAIL, UPDATEROLE,ADDORDELETEEMAIL, ADDORDELETEROLE,UPDATEPASSWORD, UPDATEIDTYPE`	`CONNECT`
IT_RESOURCE_NAME	Enter the name of the IT resource that the testing utility must use.	`PSFT Server`

Table 5–1 (Cont.) Properties of config.properties File

Property	Description	Default Value
UD_PSFT_BAS_SYMBOLICID UD_PSFT_BAS_EMPLID UD_PSFT_BAS_SERVER UD_PSFT_BAS_MULTILANG_CD UD_PSFT_BAS_LANGUAGE_CD UD_PSFT_BAS_CURRENCYCODE UD_PSFT_BAS_OPRID UD_PSFT_BAS_OPRDEFNDESC UD_PSFT_BAS_PRIEMAILADDRESS UD_PSFT_BAS_PRIEMAILTYPE UD_PSFT_BAS_OPERPSWD UD_PSFT_BAS_PRPERMISSIONLIST UD_PSFT_BAS_ROWPERMISSIONLIST UD_PSFT_BAS_PROCESSPROFILELIST UD_PSFT_BAS_NAVIGATORHOMELIST UD_PSFT_BAS_USERIDALIAS UD_PSFT_BAS_CUSTID UD_PSFT_BAS_CUSTSETID UD_PSFT_BAS_VNDID UD_PSFT_BAS_VNDSETID	Enter Create User and Update User data that must be set during the test provisioning operation. The description of attributes for Create User and Update User operations used in the config.properties file is as follows: UD_PSFT_BAS_SYMBOLICID: Symbolic ID UD_PSFT_BAS_EMPLID: Employee ID UD_PSFT_BAS_SERVER: IT Resource Name UD_PSFT_BAS_MULTILANG_CD: Multi Language Code UD_PSFT_BAS_LANGUAGE_CD: Language Code UD_PSFT_BAS_CURRENCYCODE: Currency Code UD_PSFT_BAS_OPRID: User ID UD_PSFT_BAS_OPRDEFNDESC: User Description UD_PSFT_BAS_PRIEMAILADDRESS Primary Email Address UD_PSFT_BAS_PRIEMAILTYPE: Primary Email Type UD_PSFT_BAS_OPERPSWD: Password UD_PSFT_BAS_PRPERMISSIONLIST: Primary Permission List UD_PSFT_BAS_ROWPERMISSIONLIST: Row Security Permission List UD_PSFT_BAS_PROCESSPROFILELIST: Process Profile Permission List UD_PSFT_BAS_NAVIGATORHOMELIST: Navigator Home Permission List UD_PSFT_BAS_USERIDALIAS: User ID Alias UD_PSFT_BAS_CUSTID: Customer ID UD_PSFT_BAS_CUSTSETID: Customer Set ID UD_PSFT_BAS_VNDID: Vendor ID UD_PSFT_BAS_VNDSETID: Vendor Set ID	NA
DELETE_USER_ID	Specify the user ID to be deleted.	NA
ENABLE_USER_ID	Specify the user ID to be enabled.	NA
DISABLE_USER_ID	Specify the user ID to be disabled.	NA

Table 5–1 (Cont.) Properties of config.properties File

Property	Description	Default Value
MODIFY_EMAIL_USER_ID EMAIL_ACTION EMAIL_TYPE EMAIL_ADDRESS	These properties are used to add or delete an e-mail record. MODIFY_EMAIL_USER_ID: Specify the user ID whose e-mail record is to be modified. EMAIL_ACTION: This can be set to `ADD` or `DELETE`. EMAIL_TYPE: Specify the type of e-mail **Note:** EMAIL_TYPE must be specified in the 1~BB format. EMAIL_ADDRESS: Specify the e-mail address.	NA
MODIFY_ROLE_USER_ID ROLE_ACTION ROLE_NAME	These properties are used to add or delete a role. MODIFY_ROLE_USER_ID: Specify the user ID whose role is to be modified. ROLE_ACTION: This can be set to `ADD` or `DELETE`. ROLE_NAME: Specify the name of the role to be added or deleted. **Note:** ROLE_NAME must be provided in the 1~CE User format.	NA
UPDATE_PASSWORD_USER_ID	Specify the user ID of the user whose password is to be updated.	NA
UPDATE_ID_TYPE_USER_ID IDTYPE_COLUMNNAME_TO_BE_UPDATED	These properties are used to update the ID type associated with a user profile. UPDATE_ID_TYPE_USER_ID: Specify the User ID of the user whose ID Type is to be modified. IDTYPE_COLUMNNAME_TO_BE_UPDATED: Specify the column name of the ID Type attribute. For example, if employee ID is to be updated then specify UD_PSFT_BAS_EMPLID.	`UD_PSFT_BAS_EMPLID`
UPDATE_ROLE_USER_ID OLD_ROLE_NAME NEW_ROLE_NAME	These properties are used to update the role assigned to a user profile. UPDATE_ROLE_USER_ID: Specify the user ID of the user whose role is to be updated. OLD_ROLE_NAME: Specify the existing role name. NEW_ROLE_NAME: Specify the new role name ROLE NAME must be provided in the 1~Role Name format. For example, 1~CE User.	NA

Table 5–1 (Cont.) Properties of config.properties File

Property	Description	Default Value
UPDATE_EMAIL_USER_ID NEW_EMAIL_TYPE OLD_EMAIL_TYPE NEW_EMAIL_ADDRESS	These properties are used to update the e-mail messages assigned to a user profile. NEW_EMAIL_TYPE: Specify the new e-mail type to be updated. OLD_EMAIL_TYPE: Specify the existing e-mail type of the e-mail. NEW_EMAIL_ADDRESS: Specify the new e-mail address. **Note:** Ensure that the OLD_EMAIL_TYPE is already assigned to the user. **Note:** EMAIL TYPE must be provided in the 1~EMAILTYPE format. For example, 1~BB.	NA
UPDATE_USER_ID COLUMN_TO_BE_UPDATED	These properties are used to update user attributes. UPDATE_USER_ID: Specify the user ID of the user profile whose attribute is to be updated. COLUMN_TO_BE_UPDATED: Specify the column name of the attribute to be updated. **Note:** The updated data is fetched from create user and update user data.	NA

Table 5–1 (Cont.) Properties of config.properties File

Property	Description	Default Value
XL_HOME_DIR JAVA_SECURITY_AUTH_LOGIN_CONFIG JAVA_NAMING_PROVIDER_URL JAVA_NAMING_FACTORY_INITIAL	The following are system properties, which have to be set for a signature-based logging into Oracle Identity Manager. XL_HOME_DIR: Specify the path of the Oracle Identity Manager home directory, for example, path till the xellerate directory. For example: For Oracle Identity Manager 9.1.0.*x*: C:\OIM_JBOSS_9102\OimServer\xellerate For Oracle Identity Manager 11.1.1: E:\\OIM11g\\Middleware\\Oracle_IDM\\server JAVA_SECURITY_AUTH_LOGIN_CONFIG: Specify the path of the auth.conf file. It is present in the `config` directory. For Oracle Identity Manager 9.1.0.*x*: For JBoss Application Server: Specify the path of the aut.conf file. For Oracle WebLogic Server: Specify the path of the authwl.conf file. For IBM WebSphere Application Server: Specify the path of the authws.conf file. For Oracle Identity Manager 11.1.1: E:\\OIM11g\\Middleware\\Oracle_IDM\\server\\config\\authwl.conf JAVA_NAMING_PROVIDER_URL: Specify the value of the "java.naming.provider.url" attribute present in the Discovery settings in the following file: For Oracle Identity Manager 9.1.0.*x*: *OIM_HOME*/xellerate/config/xlconfig.xml For Oracle Identity Manager 11.1.1: *OIM_HOME*/designconsole/config/xlconfig.xml Sample value: t3://10.1.6.82:8003 JAVA_NAMING_FACTORY_INITIAL: Specify the value of the "java.naming.factory.initial" attribute present in the Discovery settings in the following file: For Oracle Identity Manager 9.1.0.*x*: *OIM_HOME*/xellerate/config/xlconfig.xml For Oracle Identity Manager 11.1.1: *OIM_HOME*/designconsole/config/xlconfig.xml	NA
OIM_LOGIN_USER_ID	OIM_LOGIN_USER_ID: Specify the User ID to log in to Oracle Identity Manager. Sample Value: `xelsysadm`	NA

3. After you specify values in the config.properties file, run the PeoplsoftTestingUtility.sh or PeoplsoftTestingUtility.bat file. This file is located in the scripts directory on the installation media.

5.3 Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the PeopleSoft User Management connector:

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with the PeopleSoft Enterprise Applications server.	■ Ensure that the PeopleSoft Enterprise Applications server is running. ■ Ensure that Oracle Identity Manager is running. ■ Ensure that all the adapters have been compiled. ■ Use the IT resources form to examine the Oracle Identity Manager record. Ensure that the IP address, admin ID, and admin password are correct. ■ Ensure that the correct Jolt URL has been specified. See Table 2–4, " IT Resource Parameters" for information about locating and determining a Jolt URL. ■ Ensure that the server on which Oracle Identity Manager is running can communicate with the Jolt listener over the Jolt URL.
Class loading error **Returned Error Message:** ERROR [STDERR] Caused by: java.lang.NoClassDefFoundError: psft/pt8/joa/JOAException	■ Check the value of the Multiple Version Support parameter in the Lookup.PSFT.Configuration lookup definition. If the value is set to `No`, then ensure that the *OIM_HOME*/xellerate/ThirdParty directory contains the target system specific JAR files (psjoa.jar and peoplesoft.jar). ■ If the value of the Multiple Version Support parameter in the lookup definition is set to `Yes`, then verify the directory path specified in the Jar File Location parameter of ITResource. It should contain target system specific JAR files (psjoa.jar and peoplesoft.jar).
Connection error **Returned Error Message:** Reason:NwHdlr: Cannot open socketINFO [STDOUT] Jolt Session Pool cannot provide a connection to the appsever. This appears to be because there is no available application server domain. ERROR [STDERR] [Thu Nov 12 19:36:16 IST 2009] bea.jolt.ServiceException: Invalid Session	Check the Jolt URL parameter defined in the ITResource. See Table 2–4, " IT Resource Parameters" for more information. It should contain the correct host name and port.

Problem Description	Solution
Class loading error **Returned Error Message:** ERROR [PSFTUM] Description : ADP ClassLoader failed to load: oracle.iam.connectors.psft.usermgmt.integration.PSFTUMUserProxyProvisionManagerERROR [PSFTUM] java.lang.ClassNotFoundException: ADP ClassLoader failed to load: oracle.iam.connectors.psft.usermgmt.integration.PSFTUMUserProxyProvisionManager	▪ Check the value of the Multiple Version Support parameter in the Lookup.PSFT.Configuration lookup definition. If the value is set to `No`, then ensure that the *OIM_HOME*/xellerate/JavaTasks directory contains the PSFTUM.jar file with the oracle.iam.connectors.psft.usermgmt.integration.PSFTUMUserProxyProvisionManager class. ▪ If the value of the Multiple Version Support parameter in the lookup definition is set to `Yes`, then verify the directory path specified in the Jar File Location parameter of ITResource. It should contain PeopleSoftProxy.jar with oracle.iam.connectors.psft.usermgmt.integration.PSFTUMUserProxyProvisionManager class.

You might receive the following error message while reconciling user profile data:
`ERROR [PSFTCOMMON]`
`==========`
`ERROR [PSFTCOMMON]`
`oracle.iam.connectors.psft.common.handler.HandlerFactory:`
`getMessageHandler:`
`No Lookup defined for message USER_PROFILE.VERSION_84`
`ERROR [PSFTCOMMON]`
`==========`
 	
`ERROR [PSFTCOMMON]`
`==========`
`ERROR [PSFTCOMMON]`
`oracle.iam.connectors.psft.common.listener.PeopleSoftOIMListener:`
`process : Message specific handler couldn'tbe initialized.`
`Please check if lookup definition has been`
`specified for the message "USER_PROFILE.VERSION_84".`
`ERROR [PSFTCOMMON]`
`==========`
 	
This indicates that the target system is sending the USER_PROFILE message with the name USER_PROFILE.VERSION_84.
	You must modify the Code Key value of the USER_PROFILE attribute in the Lookup.PSFT.Configuration lookup definition as follows:
	Code Key: USER_PROFILE.VERSION_84
	Decode: Lookup.PSFT.Message.UserProfile.Configuration

6

Known Issues

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

- **Bug 12677496**

  When publishing data during certain connector operations, some data fields are blank. This issue has been fixed and the fix is available in the PeopleTools 8.51.13 release.

- **Bug 12731681**

  After a full data publish operation for USER_PROFILE, no data is published for PSROLEXLATOPRVW in the generated XML file.

- **Bug 12720160**

  On Oracle Identity Manager 11*g* release 1 (11.1.1) BP05, during an incremental reconciliation operation, the deleted roles in the child form data are not reconciled.

- **Bug 9018313**

  Connection pooling is not supported when the connector is used for provisioning operation across multiple versions of the target system.

- **Bug 9113650**

  While updating an ID type, all the ID type attributes cannot be updated in a single process form update. For example, if you want to update the attributes of the Vendor ID type, such as Vendor ID and Vendor Set ID, then you must not update both the attributes to new values in a single process form update. Instead, you must update each of them separately.

- **Bug 9244759**

  PeopleTools 8.50 does not support user profile IM information.

- **Bug 9406473**

  The delete bulk attribute reconciliation API is not supported in Oracle Identity Manager release 11.1.1. Therefore, delete reconciliation of child tables throw an error on this release of Oracle Identity Manager.

- **Bug 10402459**

  Removing a secondary e-mail removes all other secondary e-mails from Oracle Identity Manager form.

- **Bug 10402370**

  Primary e-mail update is removing the secondary e-mail details from Oracle Identity Manager form.

- **Bug 10402323**

  Role update is not happening correctly for user profile incremental reconciliation.

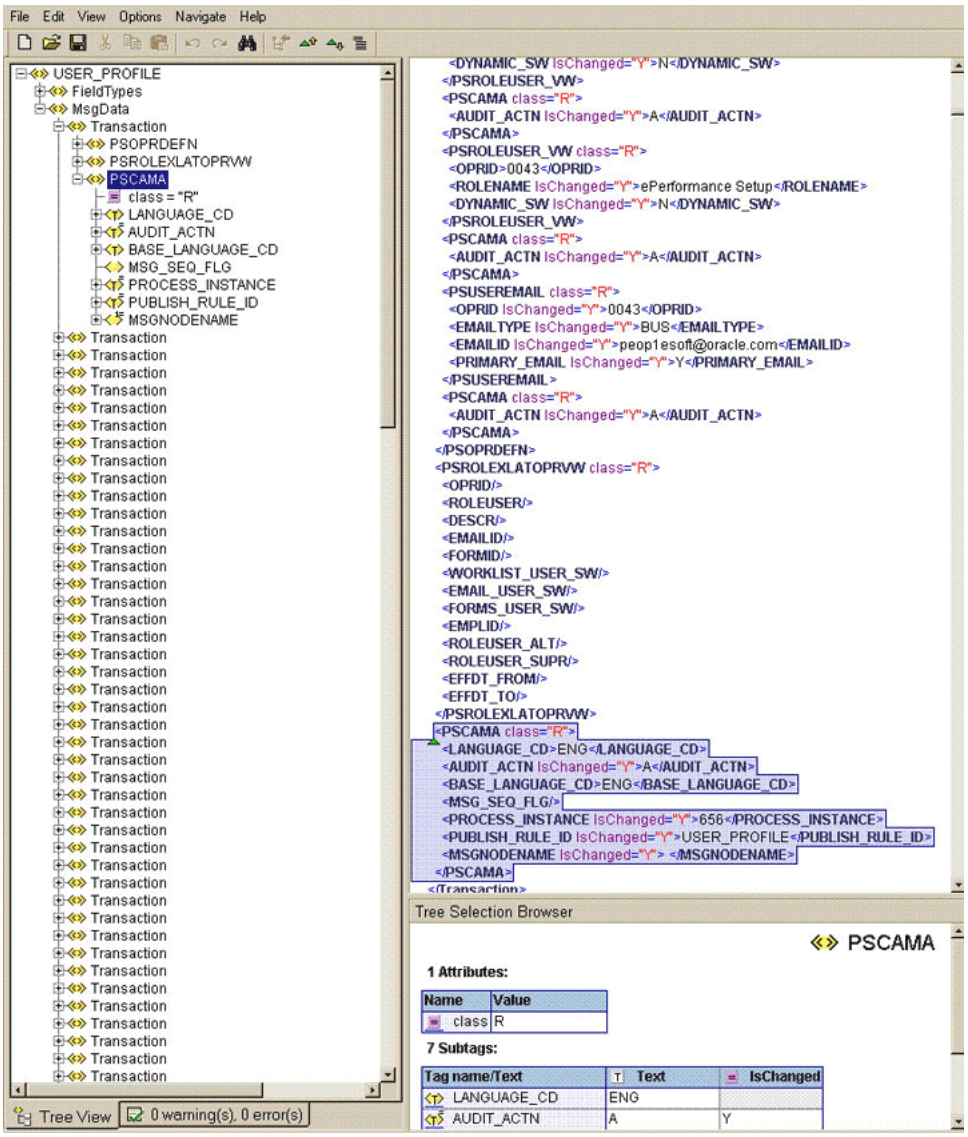
A

Determining the Root Audit Action Details

An XML message that is published by PeopleSoft contains a Transaction node. In case of full reconciliation, the XML file for USER_PROFILE message has multiple transaction nodes. However, in case of incremental reconciliation, the XML message has only one transaction node.

Every transaction node has a PeopleSoft Common Application Messaging Attributes (PSCAMA) subnode.

The following screenshot shows the PSCAMA node:



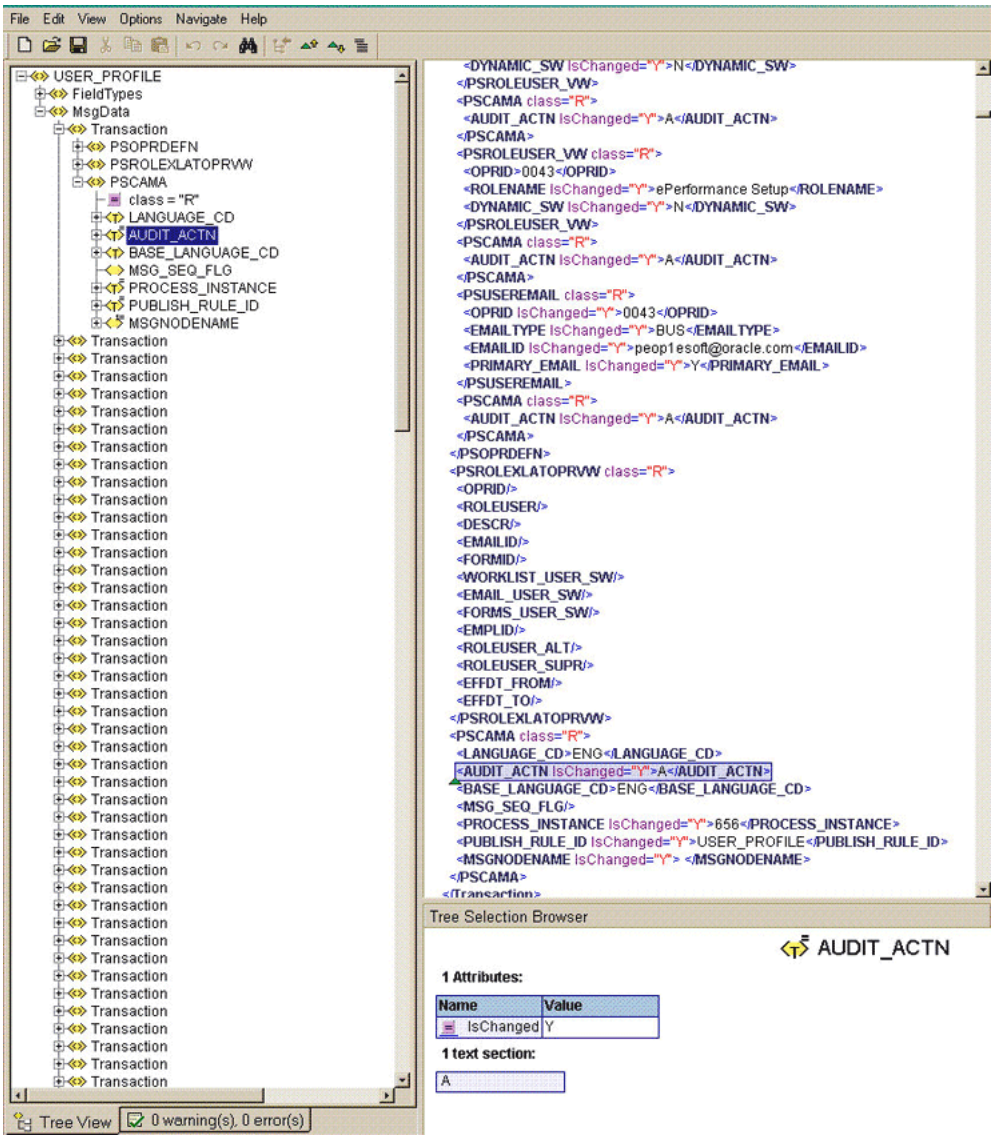
PSCAMA is an XML tag that contains fields common to all messages. The PSCAMA tag is repeated for each row in each level of the Transaction section of the message. PSCAMA provides the following information about the message data:

- Language in which the data is written
- Type of transaction the row represents, such as add, update, or delete

When receiving a message, PeopleCode inspects the PSCAMA node for this information and responds accordingly.

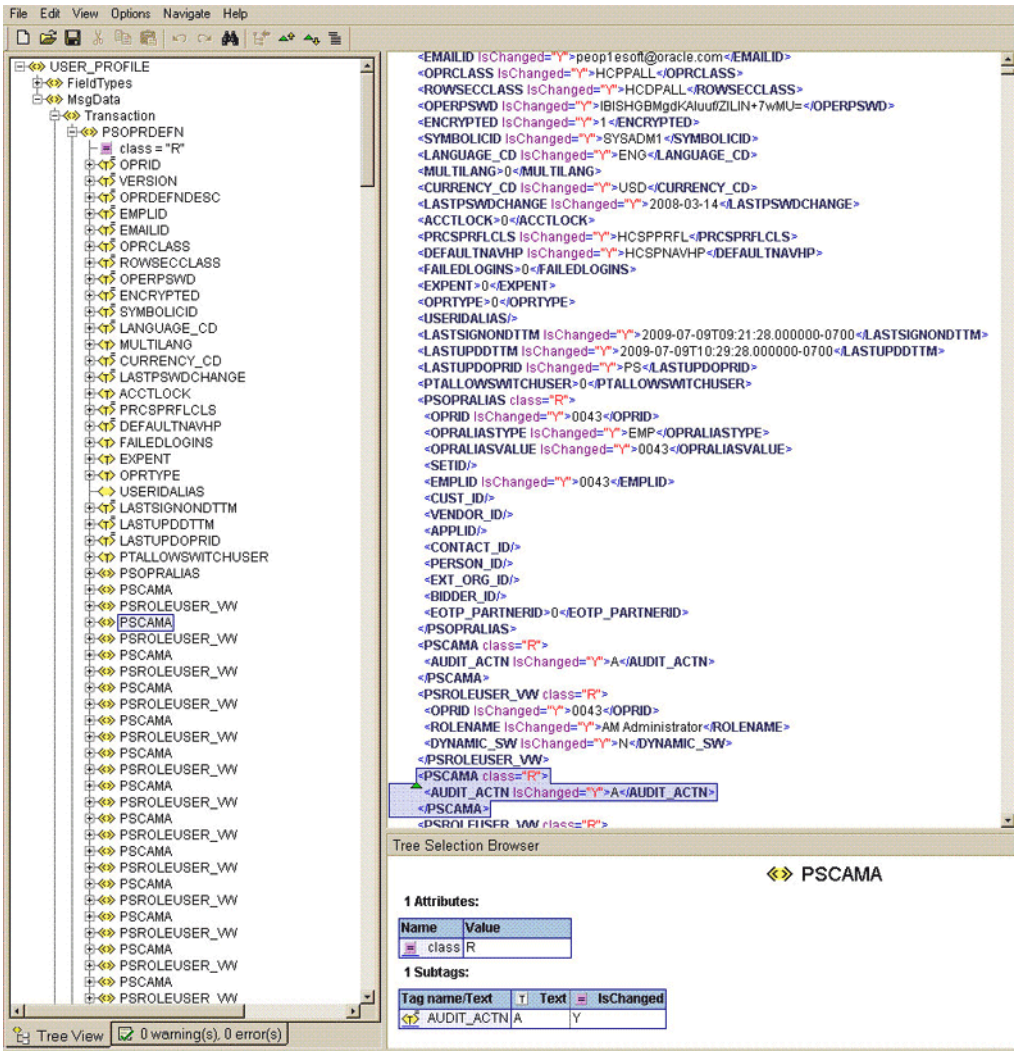
The AUDIT_ACTN subnode of PSCAMA, known as Root Audit Action, filters the data records in an XML message. It indicates the action taken against a user profile, such as Add, Change, or Delete in Oracle Identity Manager.

The AUDIT_ACTN node is shown in the following screenshot:



If the user profile information is changed on the target system, then the Root Audit Action value is C. If a new profile is added, the Root Audit Action is either A or empty.

The Add Root Audit Action is shown in the following screenshot:


File Edit View Options Navigate Help
USER_PROFILE
FieldTypes
MsgData
Transaction
PSOPRDEFN
class = "R"
OPRID
VERSION
OPRDEFNDESC
EMPLID
EMAILID
OPRCLASS
ROWSECCLASS
OPERPSWD
ENCRYPTED
SYMBOLICID
LANGUAGE_CD
MULTILANG
CURRENCY_CD
LASTPSWDCHANGE
ACCTLOCK
PRCSPRFLCLS
DEFAULTNAVHP
FAILEDLOGINS
EXPENT
OPRTYPE
USERIDALIAS
LASTSIGNONDTTM
LASTUPDDTTM
LASTUPDOPRID
PTALLOWSWITCHUSER
PSOPRALIAS
PSCAMA
PSROLEUSER_VW
Tree View
0 warning(s), 0 error(s)
<EMAILID IsChanged="Y">peop1esoft@oracle.com</EMAILID>
<OPRCLASS IsChanged="Y">HCPPALL</OPRCLASS>
<ROWSECCLASS IsChanged="Y">HCDPALL</ROWSECCLASS>
<OPERPSWD IsChanged="Y">IBISHGBMgdKAluufZILIN+7wMU=</OPERPSWD>
<ENCRYPTED IsChanged="Y">1</ENCRYPTED>
<SYMBOLICID IsChanged="Y">SYSADM1</SYMBOLICID>
<LANGUAGE_CD IsChanged="Y">ENG</LANGUAGE_CD>
<MULTILANG>0</MULTILANG>
<CURRENCY_CD IsChanged="Y">USD</CURRENCY_CD>
<LASTPSWDCHANGE IsChanged="Y">2008-03-14</LASTPSWDCHANGE>
<ACCTLOCK>0</ACCTLOCK>
<PRCSPRFLCLS IsChanged="Y">HCSPPRFL</PRCSPRFLCLS>
<DEFAULTNAVHP IsChanged="Y">HCSPNAVHP</DEFAULTNAVHP>
<FAILEDLOGINS>0</FAILEDLOGINS>
<EXPENT>0</EXPENT>
<OPRTYPE>0</OPRTYPE>
<USERIDALIAS/>
<LASTSIGNONDTTM IsChanged="Y">2009-07-09T09:21:28.000000-0700</LASTSIGNONDTTM>
<LASTUPDDTTM IsChanged="Y">2009-07-09T10:29:28.000000-0700</LASTUPDDTTM>
<LASTUPDOPRID IsChanged="Y">PS</LASTUPDOPRID>
<PTALLOWSWITCHUSER>0</PTALLOWSWITCHUSER>
<PSOPRALIAS class="R">
<OPRID IsChanged="Y">0043</OPRID>
<OPRALIASTYPE IsChanged="Y">EMP</OPRALIASTYPE>
<OPRALIASVALUE IsChanged="Y">0043</OPRALIASVALUE>
<SETID/>
<EMPLID IsChanged="Y">0043</EMPLID>
<CUST_ID/>
<VENDOR_ID/>
<APPLID/>
<CONTACT_ID/>
<PERSON_ID/>
<EXT_ORG_ID/>
<BIDDER_ID/>
<EOTP_PARTNERID>0</EOTP_PARTNERID>
</PSOPRALIAS>
<PSCAMA class="R">
<AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
</PSCAMA>
<PSROLEUSER_VW class="R">
<OPRID IsChanged="Y">0043</OPRID>
<ROLENAME IsChanged="Y">AM Administrator</ROLENAME>
<DYNAMIC_SW IsChanged="Y">N</DYNAMIC_SW>
</PSROLEUSER_VW>
<PSCAMA class="R">
<AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
</PSCAMA>
Tree Selection Browser
PSCAMA
1 Attributes:
Name
Value
class
R
1 Subtags:
Tag name/Text
Text
IsChanged
AUDIT_ACTN
A
Y

B

Setting Up SSL on Oracle WebLogic Server

This section describes how to configure SSL on Oracle WebLogic Server for PeopleTools 8.50.

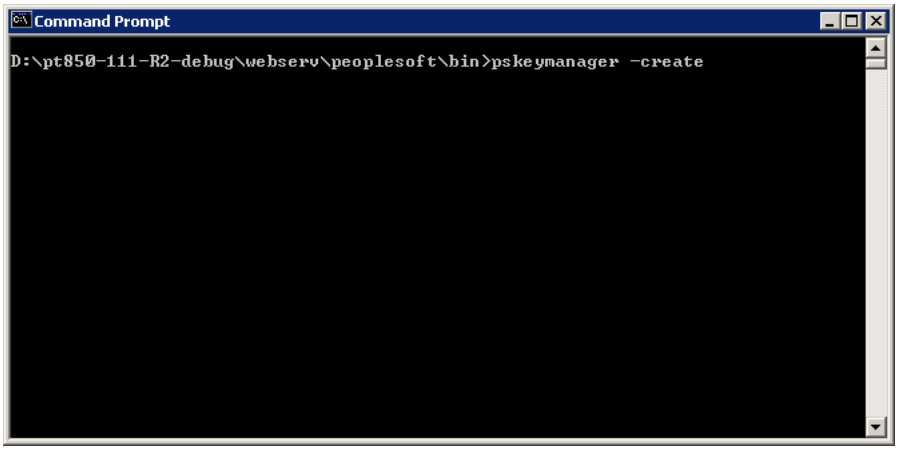
To set up SSL on Oracle WebLogic Server:

1. Generate signed public encryption key and certificate signing request (CSR).

    a. Start PSKeyManager by navigating to the appropriate directory on the MS-DOS command prompt.

    b. Enter the following at the command line:

    ```
    pskeymanager -create
    ```



    The PSKeyManager opens.

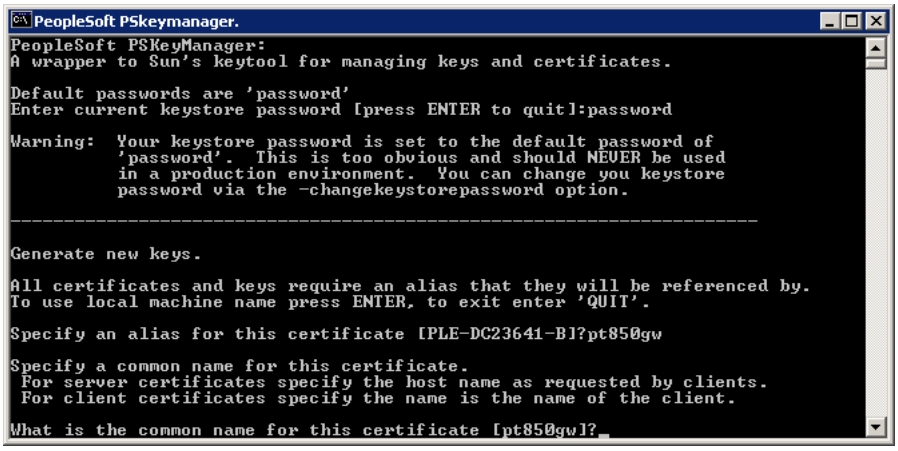
    c. Enter the following at the command line:

    At the `Enter current keystore password [press ENTER to quit]` command prompt, enter the password. The default password is `password`.

    At the `Specify an alias for this certificate <host_name>?` command prompt, enter the certificate alias and press **Enter.** The default certificate alias is the local machine name.

    At the `What is the common name for this certificate <host_name>?` command prompt, enter the host name for the certificate, for example <host_name>.corp.myorg.com.

    Press **Enter.**



Enter the appropriate information at the following command prompts:

Organization unit

Organization

City or Locality

State or Province

Country code

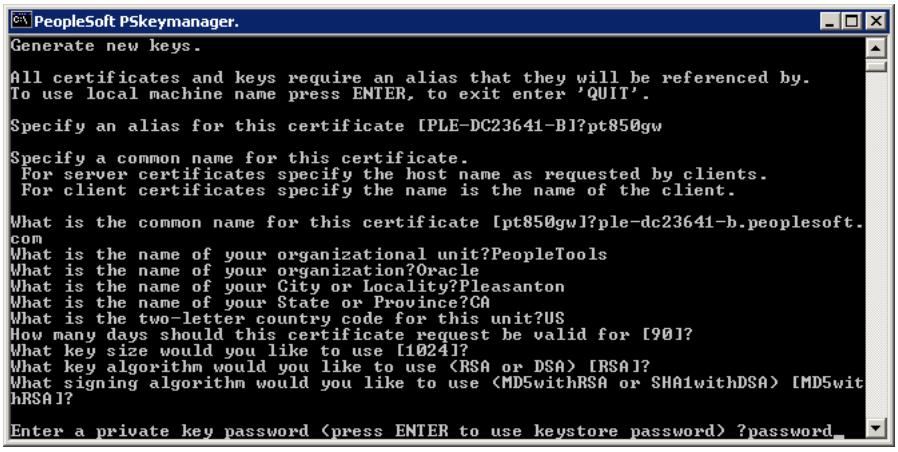
Number of days the certificate should be valid (Default is 90.)

Key size to use (Default is 1024.)

Key algorithm (Default is RSA.)

Signing algorithm (Default is MD5withRSA or SHA1withDSA.)

d. At the `Enter a private key password <press ENTER to use keystore password>` prompt, specify the password or press **Enter.**



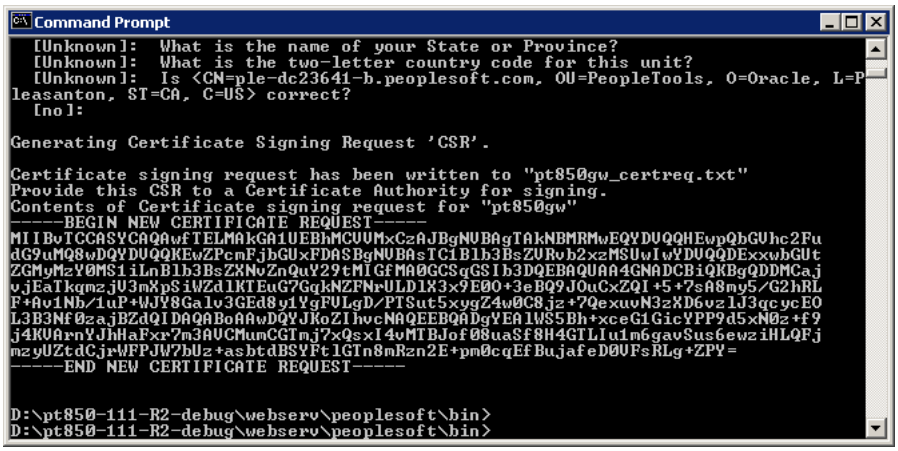
e. Verify that the values you entered are correct, and press **Enter.**

The PSKeyManager generates a public key and provides the CSR that you must submit to the Certificate Authority (CA) for signing.

The following example shows a sample CSR:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBtDCCAR0CAQAwdDELMAkGA1UEBhMCVVMxEDAOBgNVBAgTB0FyaXpvbmExEDAOBgNVBAcTB1B
```

ob2VuaXgxFDASBgNVBAoTC1Blb3BsZVRvb2xzMRMwEQYDVQQLEwpZW9wbGVzb2Z0MRYwFAYDVQQ
DEw1NREFXU09OMDUxNTAzMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC43lCZWxrsyxven5
QethAdsLIEEPhhhl7TjA0r8pxpO+ukD8LI7TlTntPOMU535qMGfk/jYtG0QbvpwHDYePyNMtVou
6wAs2yr1B+wJSp6Zm42m8PPihfMUXYLG9RiIqcmp2FzdIUi4M07J8ob8rf0W+Ni1bGW2dmXZ0jG
vBmNHQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAKx/ugTt0soNVmiH0YcI8FyW8b81FWGIR0f1
Cr2MeDiOQ2pty24dKKLUqIhogTZdFAN0ed6Ktc82/5xBoH1gv7YeqyPBJvAxW6ekMsgOEzLq9OU
3ESezZorYFdrQTzqsEXUp1A+cZdfo0eKwZTFmjNAsh1kis+HOLoQQwyjgaxYI=
-----END NEW CERTIFICATE REQUEST-----

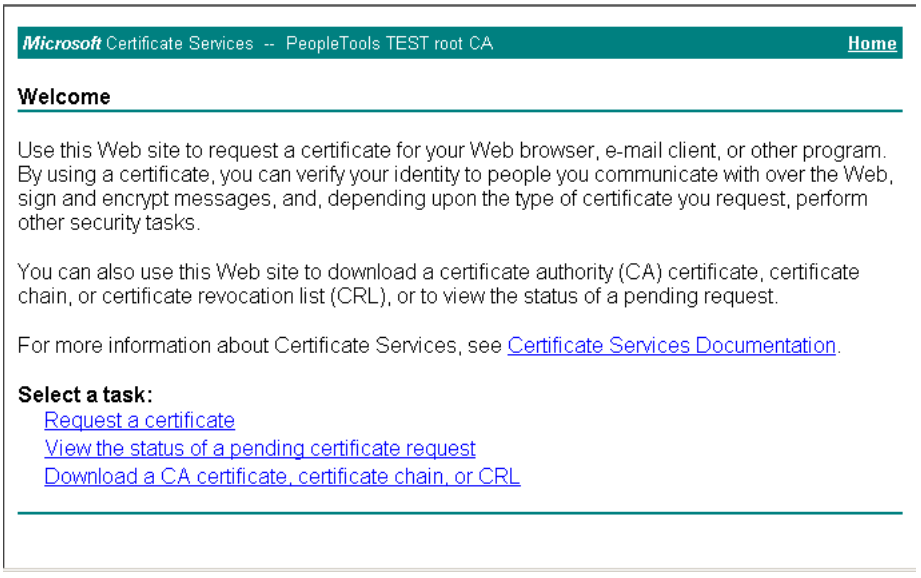


The CSR is a text file, and is written to the <*PSFT_HOME*>\webserv\peoplesoft directory. The file name is <host_name>_certreq.txt.

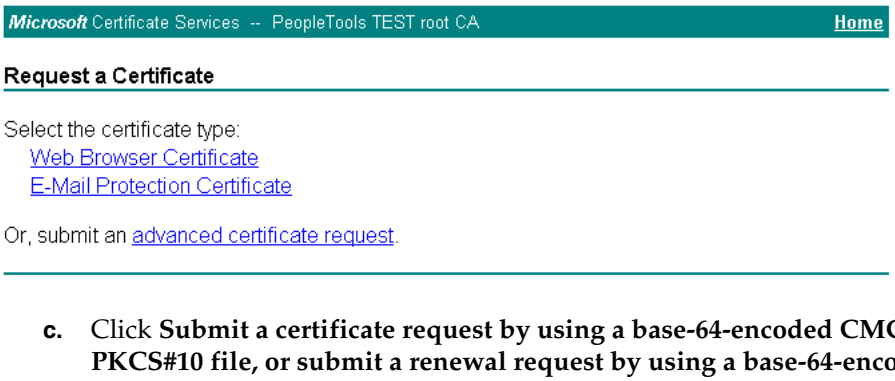
2. Submit CSRs to CAs for signing:

Note: The set of pages are different depending on what CA you plan on using.

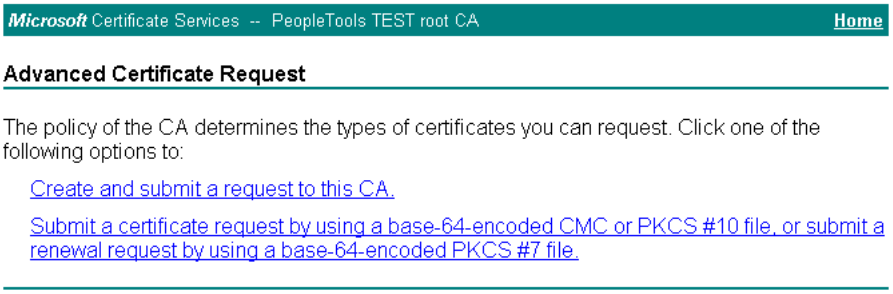
a. Click **Download a CA certificate, certificate chain, or CRL**.



b. Click **advanced certificate request.**

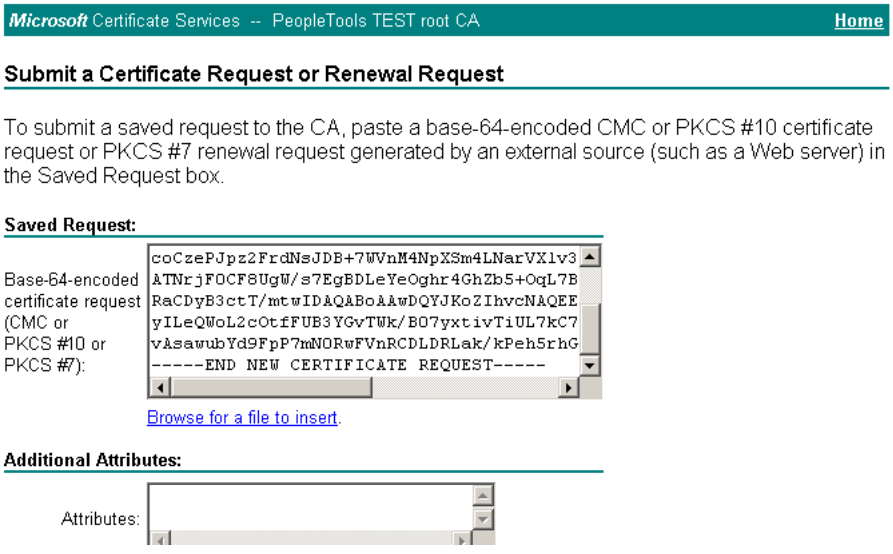


c. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.**



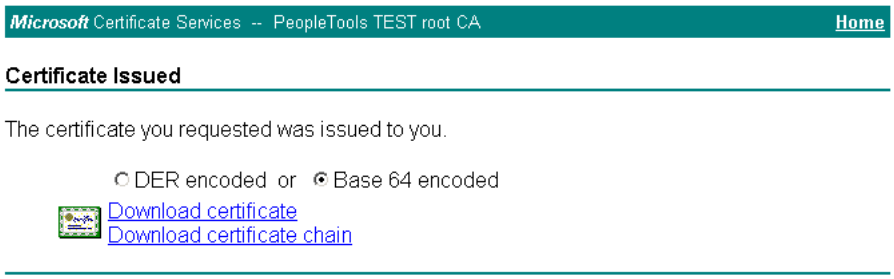
The Submit a Certificate Request or Renewal page appears.

d. Paste the content of the CSR in the **Saved Request** list box.



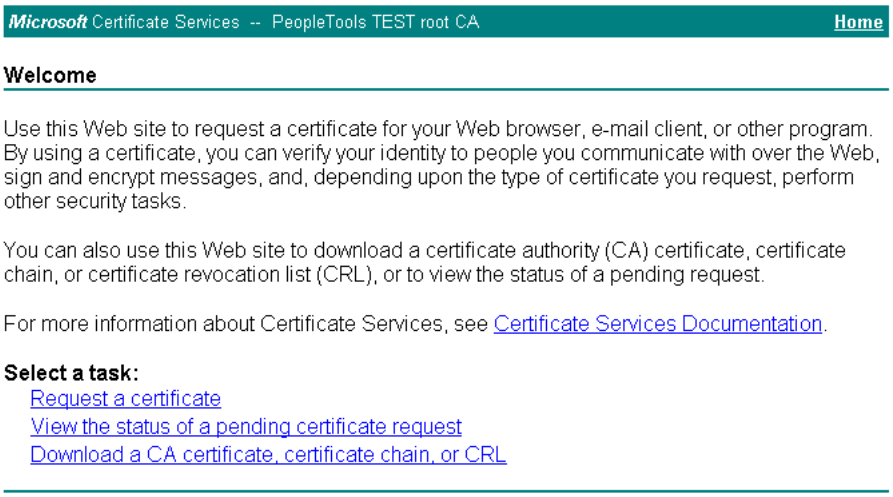
The CA may send the signed public key (root) certificate to you by e-mail or require you to download it from a specified web page.

e. Download and save the signed public key on your local drive.

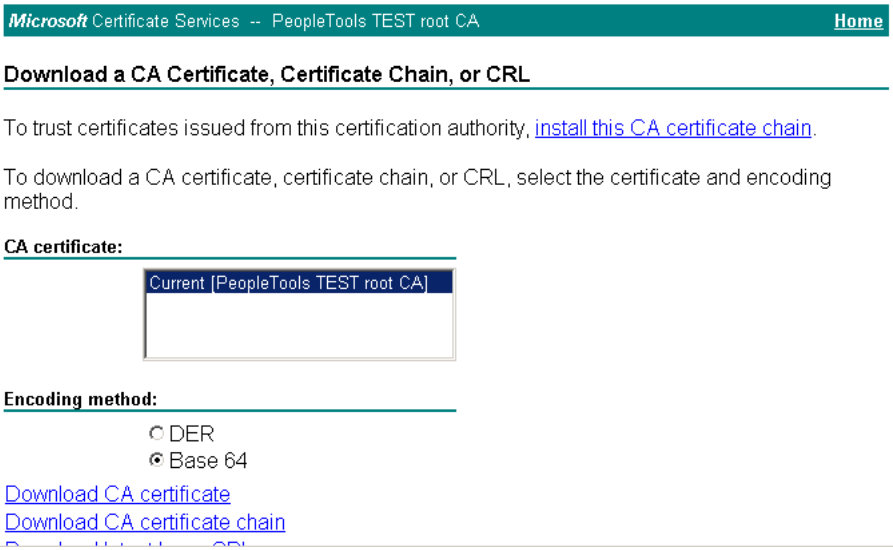


3. Download the root certificate.

   a. Click **Download a CA certificate, certificate chain, or CRL.**



   b. From the **CA certificate** list, select the certificate.



   c. Download and save the root certificate on your local drive.

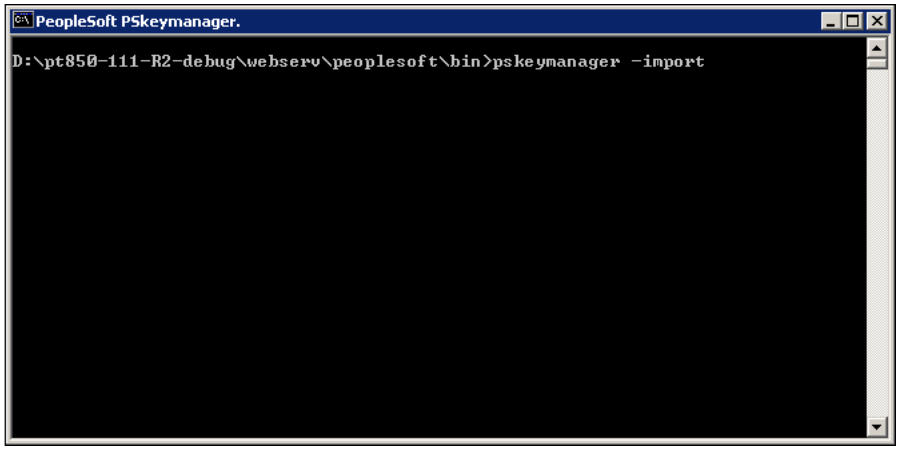
4. Import a server-side public key into a keystore.

   a. Open PSKeyManager.

   b. Navigate to the required directory on the MS-DOS command prompt.

c. Enter the following at the command line:

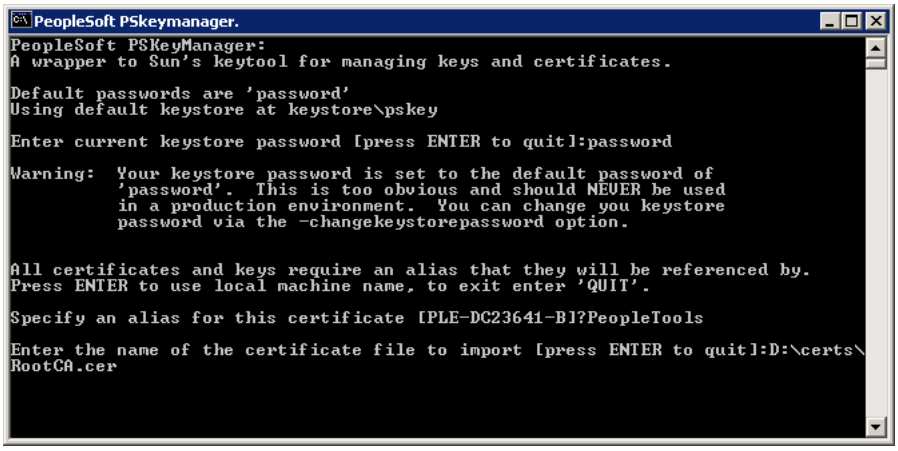
```
pskeymanager -import
```



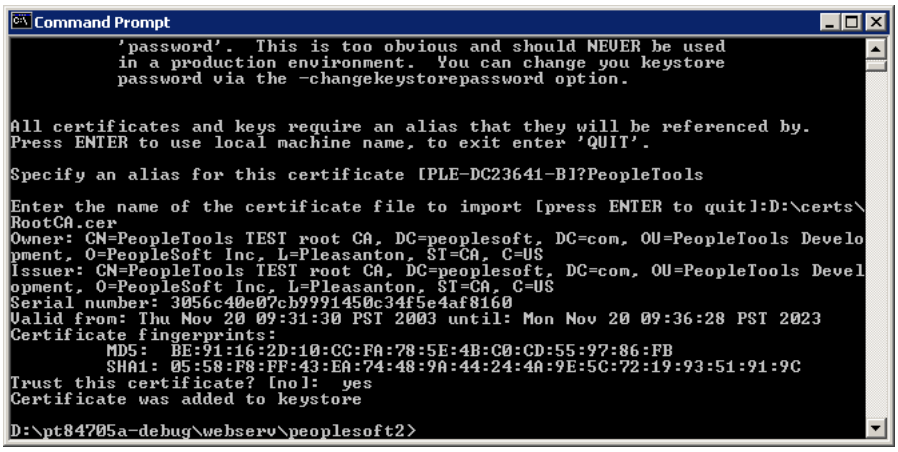
d. At the `Enter current keystore password` command prompt, enter the password and press **Enter.**

e. At the `Specify an alias for this certificate <host_name>?` command prompt, enter the certificate alias and press **Enter.**

f. At the `Enter the name of the certification file to import` command prompt, enter the path and name of the certificate to import.



g. At the `Trust this certificate` command prompt, enter **Yes** and press **Enter.**



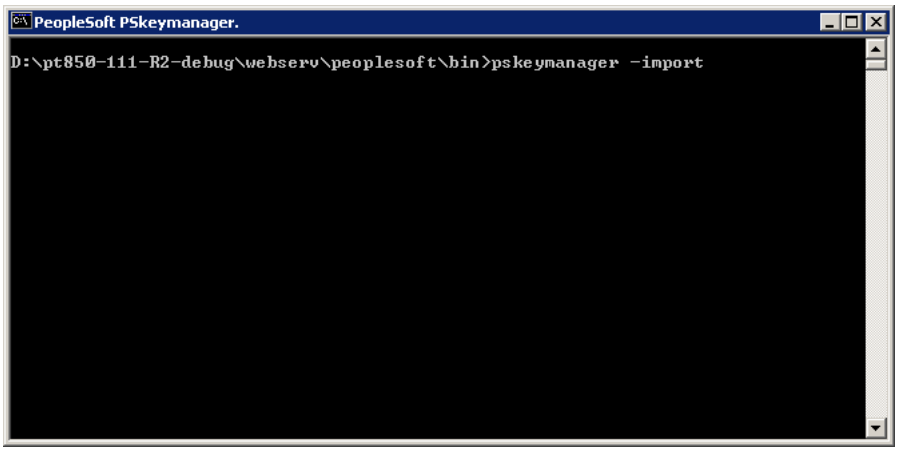
5. Generate and import public keys.

   a. Place the public key from your CA in the keystore. The location of the keystore is as follows:

      <*PSFT_HOME*>\webserv\peoplesoft\keystore

   b. Install the certificate for server authentication SSL on Oracle WebLogic Server using the following command:

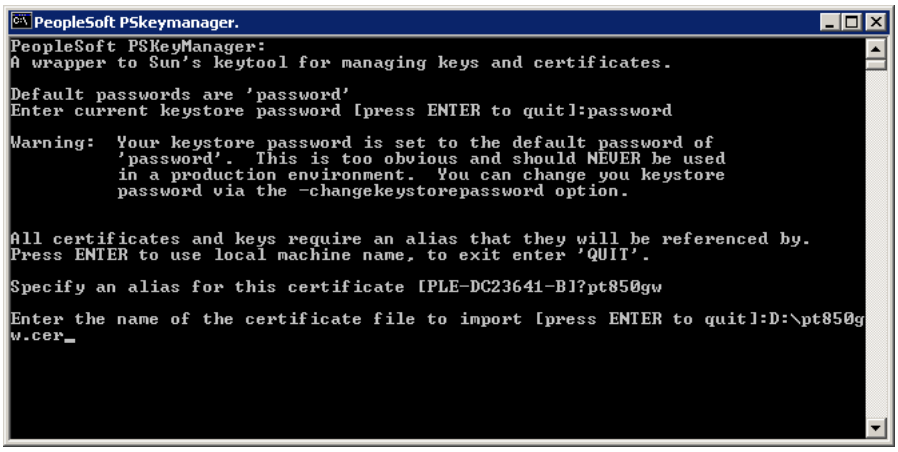
      ```
      pskeymanager -import
      ```



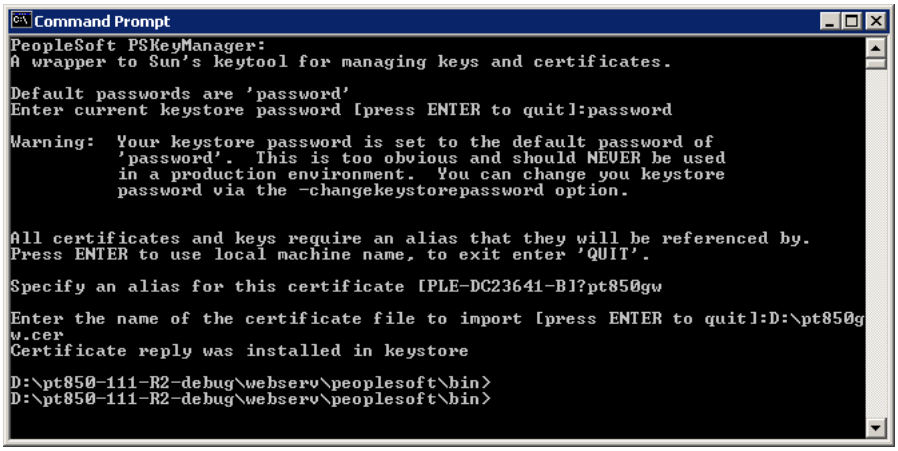
   c. At the `Enter current keystore password` command prompt, enter the password and press **Enter.**

   d. At the `Specify an alias for this certificate <host_name>?` command prompt, enter the certificate alias and press **Enter.**

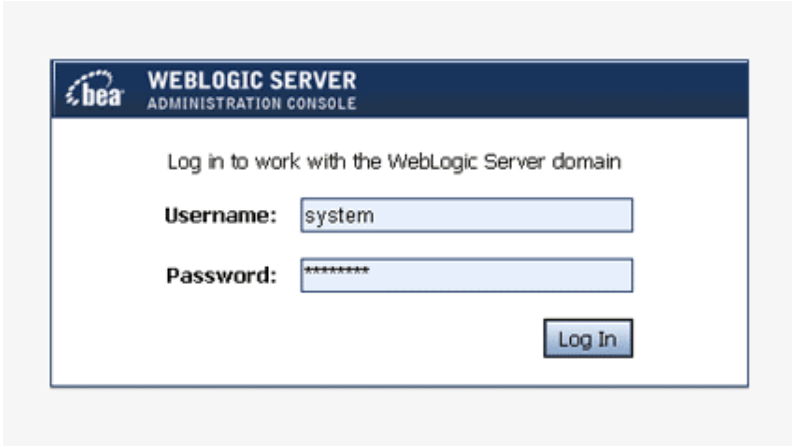
   e. At the `Enter the name of the certification file to import` command prompt, enter the path and name of the certificate to import.



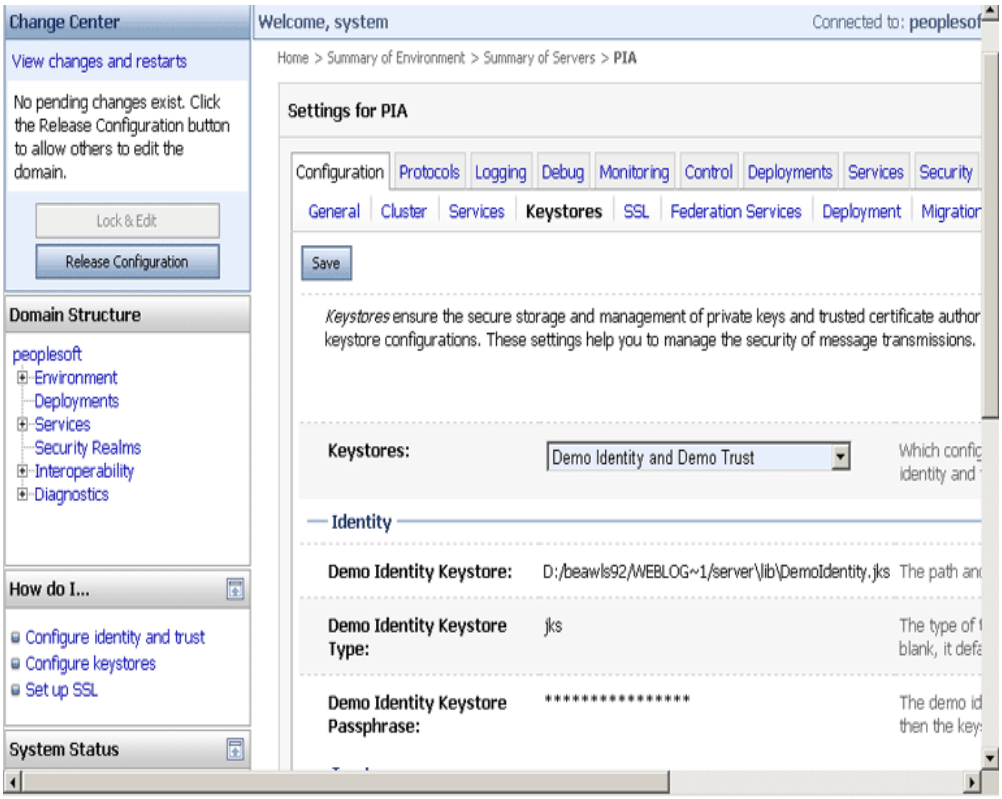
Certificate is successfully installed in the keystore.



6. Configuring the Oracle WebLogic Server to use the keystore.
   a. Log in to Oracle WebLogic Administration Console.



   b. Expand **PeopleSoft, Environment, Servers, PIA** to setup the SSL configuration for the PIA server.



c. Click the **Keystores** tab.

d. From the **Keystores** list, select **Custom Identity and Custom Trust.**

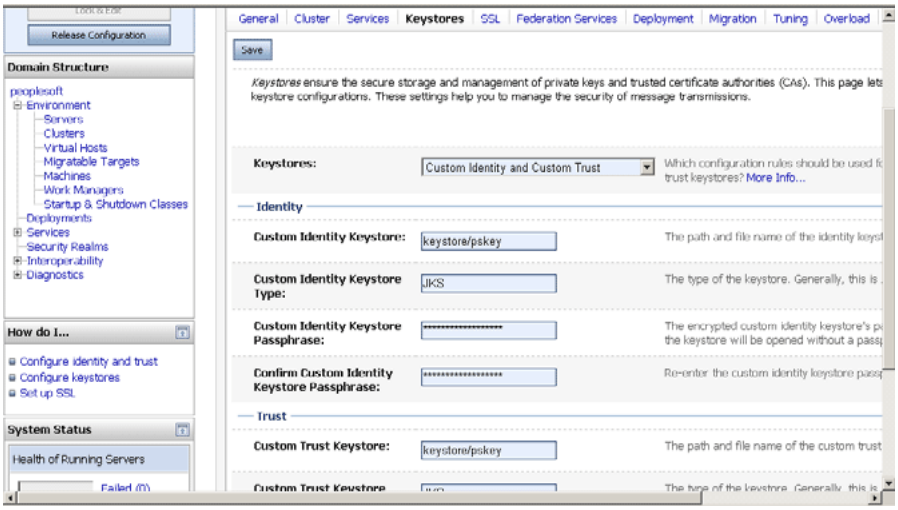
e. In the **Identity** region, complete the following fields:

- In the Custom Identity Keystore field, enter `keystore/pskey`.

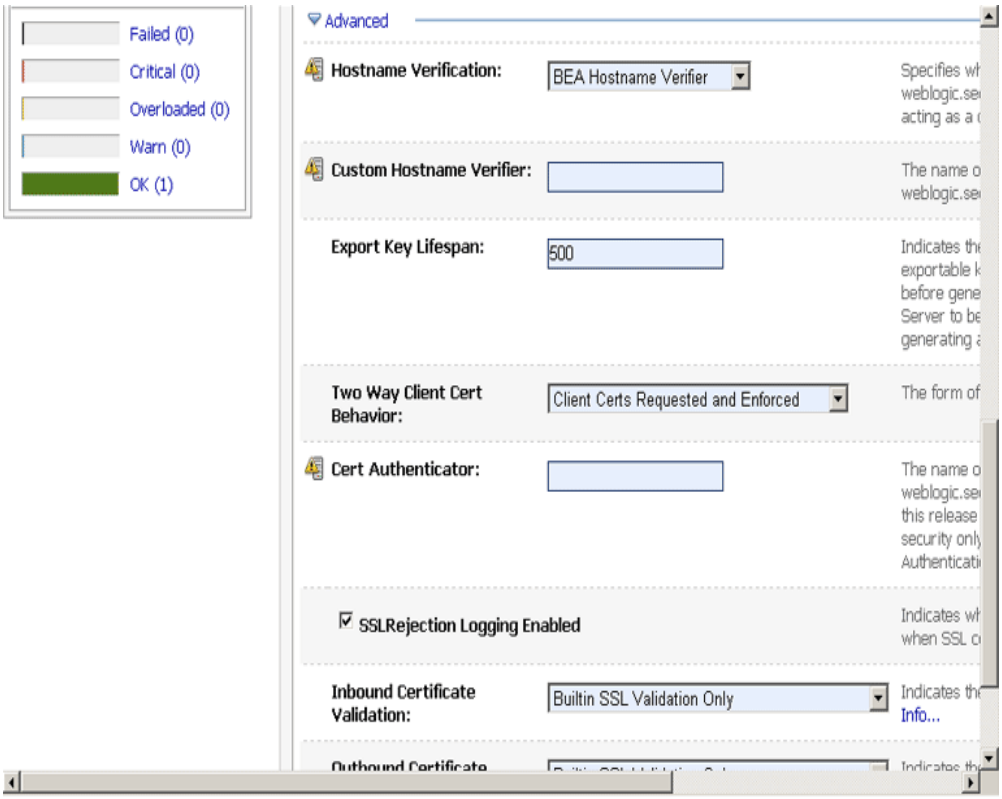
- In the Custom Identity Keystore Type field, enter `JKS`.

- In the Custom Identity Keystore Passphrase field, enter `password`.

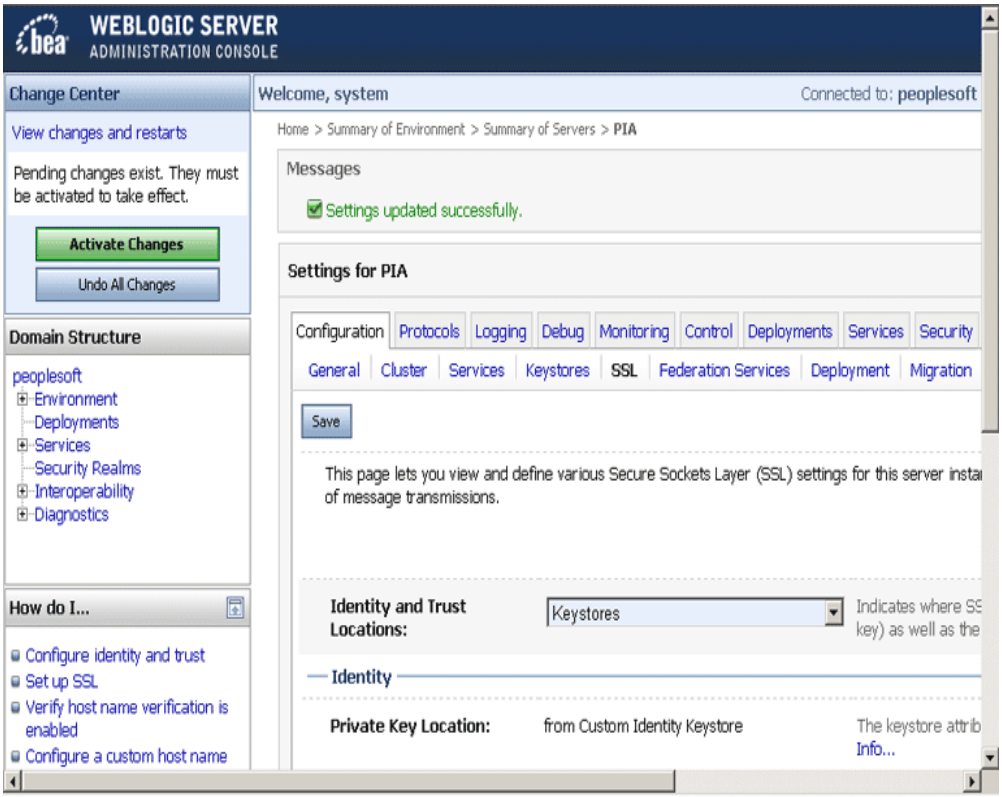
- In the Confirm Custom Identity Keystore Passphrase field, enter `password` again.



f. On the SSL tab, ensure that the parameter **Two Way Client Cert Behavior** is set to **Client Certs Requested and Enforced.**

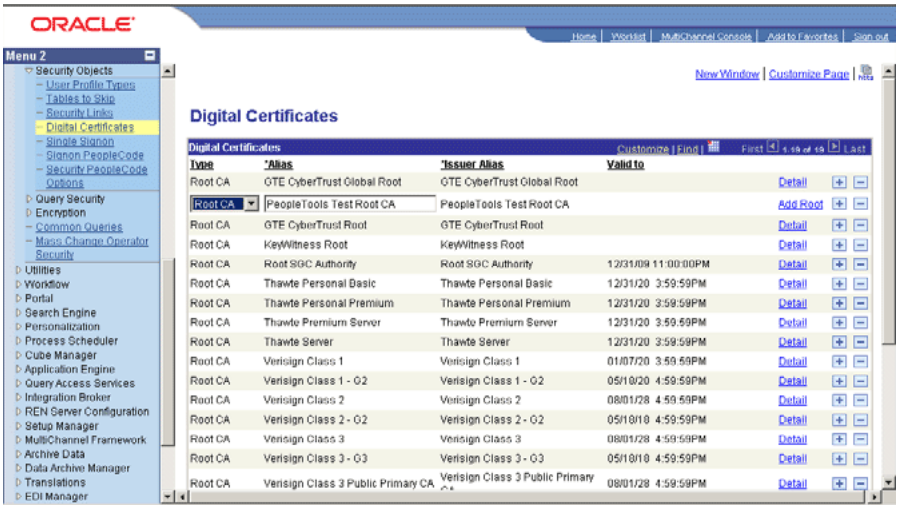


g. Click the **Activate Changes** button.



7. Add root certificate.

   a. Expand **Security, Security Objects,** and then click **Digital Certificates.**



   b. Click **Add Root.**

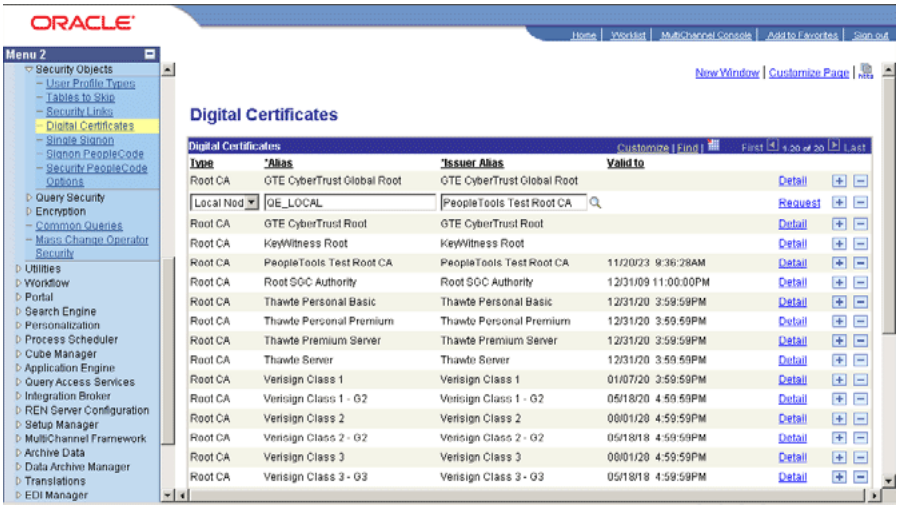
8. Configure the Peoplesoft certificates.

> **Note:** You can use the same root certificate generated in Step 2.

   a. Expand **Security, Security Objects,** and then click **Digital Certificates.**

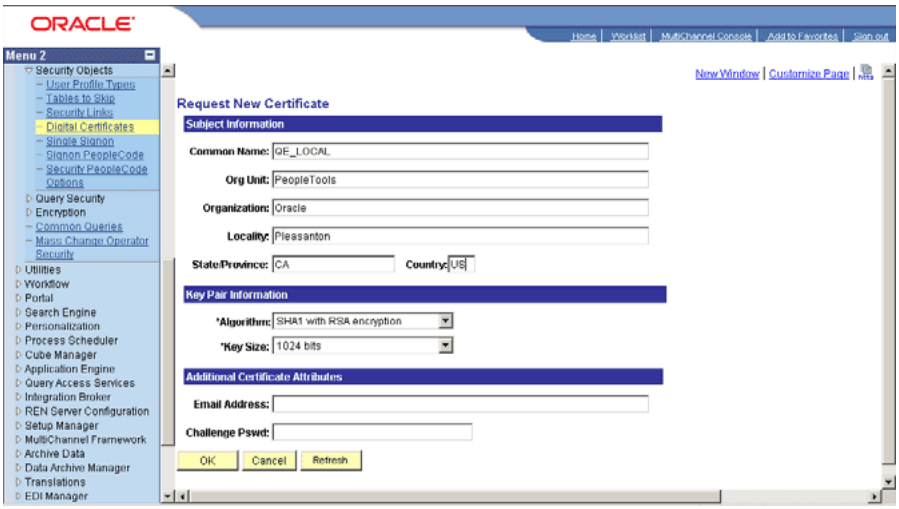
   b. Add a local node type certificate.

   c. Set **Alias** to the default local node.

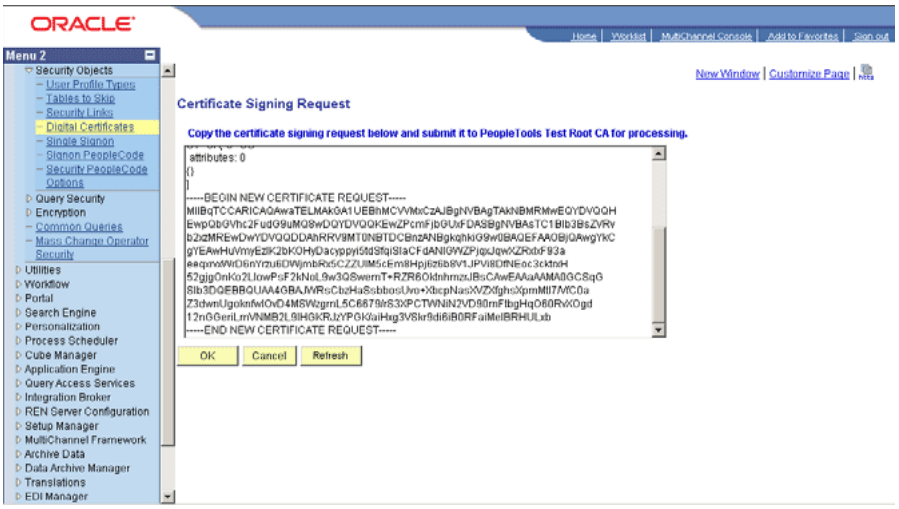


   d. Click **Request.**

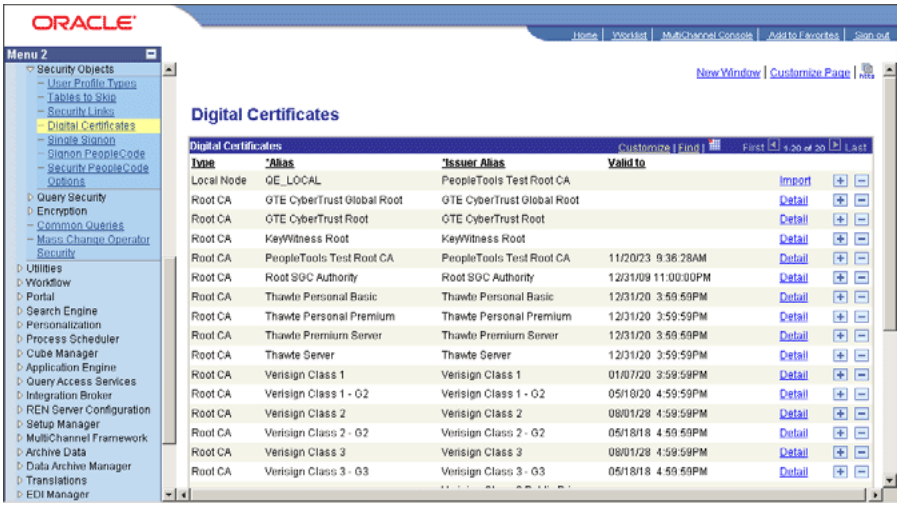
   e. Send this certificate request to the CA to get a new certificate.



f. Click **OK.**

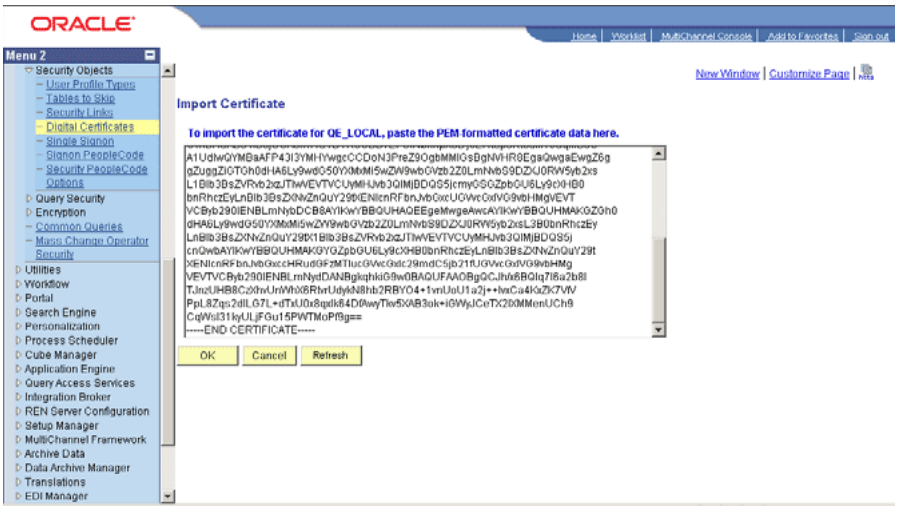


g. Ensure that the local node appears on the Digital Certificates list.

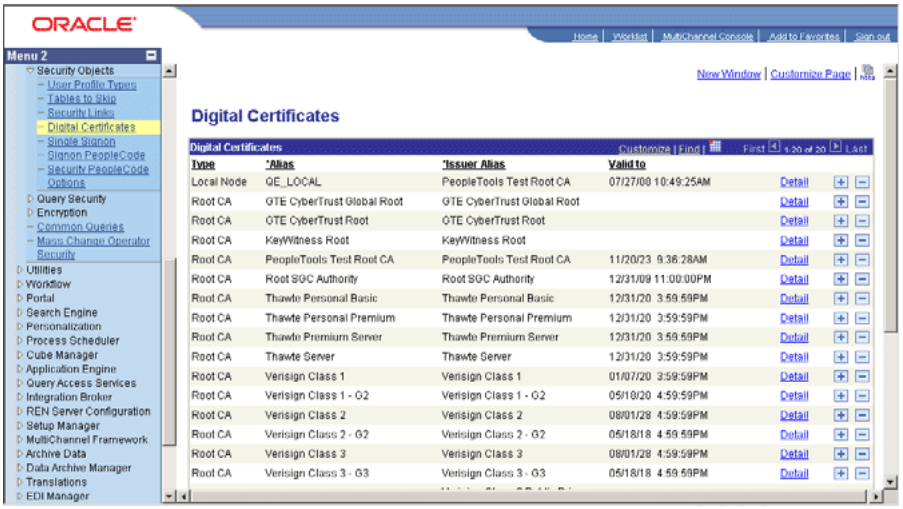


h. Click **Import.**

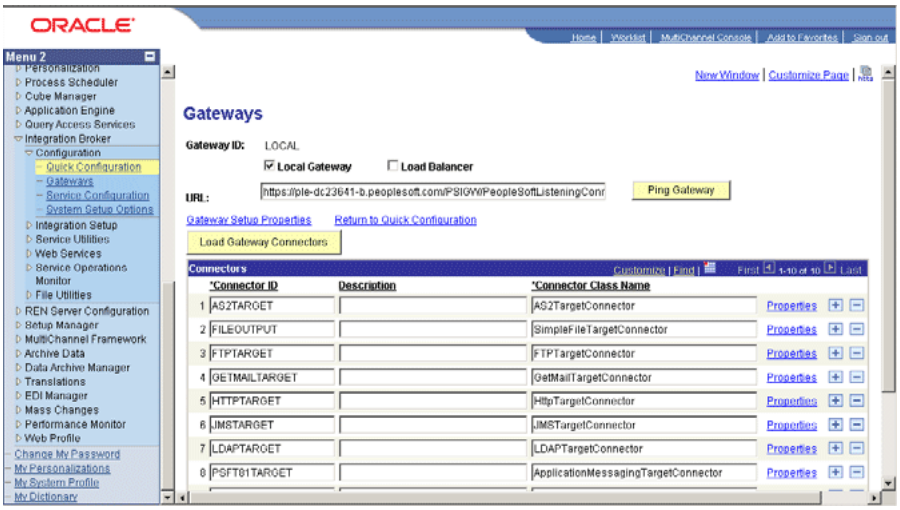
The Import Certificate page appears.



i. Click **OK.**



j. Click **Load Gateway Connectors.**

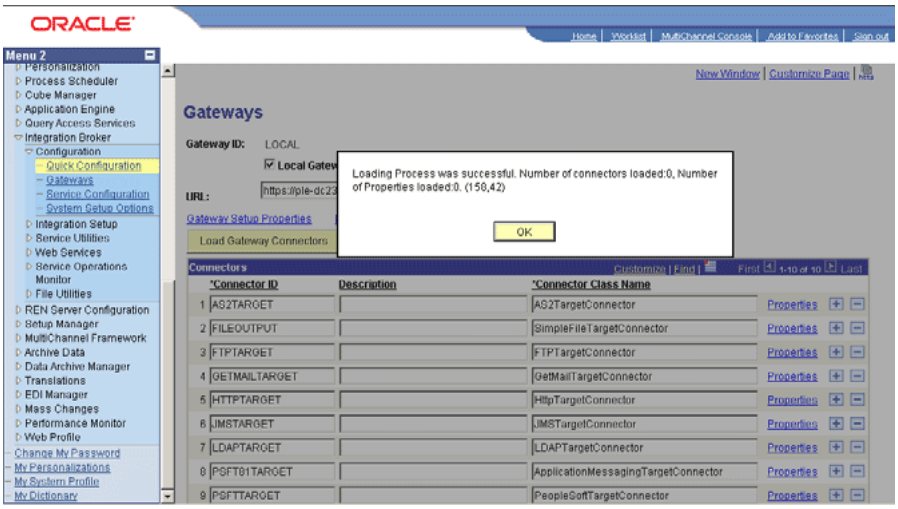


The following message appear:

```
Loading Process was successful. Number of connectors loaded:0. Number of
Properties loaded:0. (158,42)
```

Click **OK.**

k. Click **Ping Node** to ping your local node.



Index

M

P

R

S

T

V