Oracle® Identity Manager

Connector Guide for PeopleSoft User Management

Release 11.1.1
E25371-25
April 2022

ORACLE

Oracle Identity Manager Connector Guide for PeopleSoft User Management, Release 11.1.1

E25371-25

Primary Author: Gowri.G.R

Contributing Authors: Alankrita Prakash

Contents

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

C Changing Default Message Versions

Index

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

Related Documents

For information about installing and using Oracle Identity Manager, visit the following Oracle Help Center page: http://docs.oracle.com/cd/E52734_01/index.html

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

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

Conventions

The following text conventions are used in this document:

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

What's New in 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 11.1.1.6.0 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 11.1.1.6.0
- Software Updates in Release 11.1.1.5.0

Software Updates in Release 11.1.1.6.0

The following are issues resolved in this release:

Bug Number	Issue	Resolution
16395344	When you create an access policy with DNLA flags for the connector, the policy did not work as expected.	This issue has been resolved.
14697872	In Oracle Identity Manager 11.1.2, entitlement, Account Name, and Account ID tagging were missing in the process form fields.	This issue has been resolved.
16474937	In Oracle Identity Manager release 11.1.2, IT resource tagging was missing in the process form fields.	This issue has been resolved.
16482125	In Oracle Identity Manager Release 2 BP04 (11.1.2.0.4), provisioning of child table or entitlement failed.	This issue has been resolved.

Bug Number	Issue	Resolution
16091682	Testing scripts shipped with the connector failed with JRF PortabilityLayerException due to new dependencies introduced in Oracle Identity Manager release 11.1.2.	This issue has been resolved by updating the classpath in the scripts.
15873239	Reconciliation failed in a multithreaded environment with FWK005 parse error.	This issue has been resolved.
15868053	Roles that were added directly in PeopleSoft target system were deleted on running the Delete Role Recon scheduled task.	This issue has been resolved.
13939959	Reconciliation of users containing secondary emails failed.	This issue has been resolved.

Software Updates in Release 11.1.1.5.0

This is the first release of the Oracle Identity Manager Connector for PeopleSoft User Management based on Identity Connector Framework (ICF). The following software updates have been made in release 11.1.1.5.0:

- ICF Based Connector
- Simplified PeopleSoft Listener Deployment
- Support for Addition of Custom Attributes and ID Types
- Support for Custom Component Interfaces
- Support for Configuring the Connector for Multiple Target System Versions
- Support for Segregation of Duties (SoD)
- Support for Connection Pooling
- New Lookup Definitions
- Deployment Using Connector Server
- Enhanced Logging
- Resolved Issues

ICF Based Connector

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager connectors require.

The Oracle Identity Manager Connector for PeopleSoft User Management is an ICF-based connector. The ICF uses classpath isolation, which allows the connector to co-exist with legacy versions of the connector.

For more information about the ICF, see Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

Simplified PeopleSoft Listener Deployment

This release of the connector has a simplified process to deploy the PeopleSoft Listener compared to previous releases. The deployment is simplified using a new deployment tool. See Deploying the PeopleSoft Listener for more information.

Support for Addition of Custom Attributes and ID Types

The PeopleSoft User Management connector supports the addition of custom attributes and ID types for provisioning and reconciliation. See the following sections for more information:

- Adding New Attributes for Provisioning
- Adding New Attributes for Reconciliation
- Adding New ID Types for Provisioning
- Adding New ID Types for Reconciliation

Support for Custom Component Interfaces

The PeopleSoft User Management connector supports the addition of custom component interfaces. Component interface definitions are assigned in the PeopleSoft Component Interface configuration objects. You can modify or add custom definitions by editing a copy of the `PeopleSoftComponentInterfaces.xml` file located in the xml directory of the connector package.

See Connector Component Interfaces for the PeopleSoft User Management for more information.

Support for Configuring the Connector for Multiple Target System Versions

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

Support for Segregation of Duties (SoD)

The PeopleSoft user profile has roles that can be treated as entitlements. In such cases, the segregation of duties (SoD) features supported by Oracle Identity Manager can be used. See Configuring SoD on Oracle Identity Manager for more information.

Support for Connection Pooling

This release of the connector supports the connection pooling feature based on the ICF. In earlier releases, a connection with the target system was established at the start of a reconciliation run and closed at the end of the reconciliation run. With the introduction of connection pooling, multiple connections are established by the ICF and held in reserve for use by the connector.

New Lookup Definitions

This release of the connector has new lookup definitions. See Lookup Definitions Used During Connector Operations for more information.

Deployment Using Connector Server

This release of the connector can be deployed using the Connector Server, which is included with the ICF. See Installation on Oracle Identity Manager for more information.

Enhanced Logging

This release of the connector uses the logging feature included in the ICF. See Enabling Logging for more information.

Resolved Issues

The following table lists issues resolved in this release of the connector:

Bug Number	Issue	Resolution
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 were not reconciled.	This issue has been resolved. The deleted roles in the child form data are now reconciled.
10402459	If you remove a secondary e-mail of a user profile, all other secondary e-mails were removed from the Oracle Identity Manager form.	This issue has been resolved. Removing a secondary e-mail does not impact other secondary e-mails on the Oracle Identity Manager form.
10402370	If you update a primary e-mail of a user profile, the secondary e-mails were removed from the Oracle Identity Manager form.	This issue has been resolved. Removing a primary e-mail does not impact other secondary e-mails on the Oracle Identity Manager form.
10402323	During incremental reconciliation of user profiles, roles were not updated correctly.	This issue has been resolved. Roles are now updated correctly during incremental reconciliation of user profiles.

Documentation-Specific Updates

The following sections discuss the documentation-specific updates:

- Documentation-Specific Updates in Release 11.1.1.6.0
- Documentation-Specific Updates in Release 11.1.1.5.0

Documentation-Specific Updates in Release 11.1.1.6.0

The following documentation-specific update has been made in revision "24" of release 11.1.1.6.0:

The "Target System" row of Table 1-1 has been updated to include support for PeopleTools 8.59.

The following documentation-specific update has been made in revision "23" of release 11.1.1.6.0:

The "Target System" row of Table 1-1 has been updated to include support for PeopleTools 8.58.

The following documentation-specific update has been made in revision "22" of release 11.1.1.6.0:

The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance release 12*c* PS4 (12.2.1.4.0).

The following documentation-specific updates have been made in revision "21" of release 11.1.1.6.0:

- The "Target System" and "Connector Server JDK" rows of Table 1-1 have been updated to include support for PeopleTools 8.57.
- JDK Requirement for PeopleTools 8.56 and PeopleTools 8.57 has been updated.
- PeopleTools 8.57 related update has been made to several sections across the guide.

The following is a documentation-specific update that has been made in revision "20" of release 11.1.1.6.0:

The "Oracle Identity Manager" row of Table 1-1 has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and also updated for Oracle Identity Governance 12c (12.2.1.3.0) certification.

The following documentation-specific updates have been made in revision "19" of release 11.1.1.6.0:

- The "Target System" and "Connector Server JDK" rows of Table 1-1 have been updated to include support for PeopleTools 8.56.
- JDK Requirement for PeopleTools 8.56 and PeopleTools 8.57 has been added.
- PeopleTools 8.56 update has been made to the following sections:
  - Creating a Permission List
  - Creating a Role for a Limited Rights User
  - Assigning the Required Privileges to the Target System Account
  - Installing and Configuring the Connector Server
  - Running the Connector Installer
  - Configuring the Connector to Support Multiple Versions of the Target System
  - Activating the Full Data Publish Rule
  - About Configuring the PeopleSoft Integration Broker
  - Configuring the PeopleSoft Integration Broker Gateway
  - Creating the Remote Node
  - Setting the CopyRowsetDelta Option
  - Activating the USER_PROFILE Service Operation
  - Configuring PeopleSoft Integration Broker
- The description of the *ORACLE_COMMON* environment variable in Deploying the PeopleSoft Listener has been modified.

The following documentation-specific updates have been made in revision "18" of release 11.1.1.6.0:

- The "Target System" and "Connector Server JDK" rows of Table 1-1 have been updated to include support for PeopleTools 8.55.
- Information regarding PeopleTools 8.55 has been added to the following sections:
  - JDK Requirement for PeopleTools 8.53, PeopleTools 8.54, and PeopleTools 8.55
  - Creating a Permission List
  - Creating a Role for a Limited Rights User
  - Assigning the Required Privileges to the Target System Account
  - Installing and Configuring the Connector Server
  - Running the Connector Installer
  - Configuring the Connector to Support Multiple Versions of the Target System
- The patch number to be applied for retesting the provisioning operation has been updated in Troubleshooting.
- Oracle Identity Manager interface names have been corrected throughout the document.

The following documentation-specific updates have been made in revision "17" of release 11.1.1.6.0:

- The "Connector Server" row has been added to Table 1-1.
- The "JDK" row of Table 1-1 has been renamed to "Connector Server JDK".

The following documentation-specific updates have been made in revision "16" of release 11.1.1.6.0:

- The "Target systems" row of Table 1-1 has been updated.
- A "Note" regarding full reconciliation has been added to the "Target systems" row of Table 1-1.
- Step 2 of Running the Connector Installer and Step 4 of Configuring the Connector to Support Multiple Versions of the Target System have been modified to include information specific to the psmanagement.jar file.

  A "Note" has also been added regarding the same.
- Troubleshooting has been updated.

The following documentation-specific updates have been made in revision "15" of release 11.1.1.6.0:

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

The following documentation-specific update has been made in revision "14" of release 11.1.1.6.0:

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

The following documentation-specific updates have been made in the revision "13" of release 11.1.1.6.0:

- Modified Configuring the Target System for Provisioning.

- Removed Section 2.2.2.4.2, "Creating APIs for the Component Interface".

The following documentation-specific updates have been made in the revision "12" of release 11.1.1.6.0:

- A "Note" has been added to Step 5.c of Creating a Role for a Limited Rights User.
- A "Note" has been added to Step 6.e of Assigning the Required Privileges to the Target System Account.

The following documentation-specific updates have been made in the revision "11" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of Table 1-1 has been modified to include Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0).
- Information specific to Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) has been added to Step 5 of Localizing Field Labels in UI Forms.

The following documentation-specific updates have been made in the earlier revisions of release 11.1.1.6.0:

- The "Oracle Identity Manager" row in Table 1-1 has been modified.
- A note has been added in the "Files in the dataset directory" row of Table 2-1.
- The following sections have been added:
  - Configuring Oracle Identity Manager 11.1.2 or Later
  - Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later
  - Localizing Field Labels in UI Forms
  - Upgrade the Connector from Release 11.1.1.5.0
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added in the following sections:
  - Running the Connector Installer
  - Configuring the IT Resource
  - Configuring Scheduled Jobs
- Information about including the jrf.jar, jrf-api.jar, and jrf-client.jar files for Oracle Identity Manager release 11.1.2.*x* has been added as step 2 in the following sections:
  - Testing Reconciliation
  - Testing Provisioning
- PeopleSoft HRMS 9.2 with PeopleTools 8.53 has been added as a supported target system for this connector. This information has been added in the "Target System" row of Table 1-1.
- Information about PeopleTools 8.53 has been added to the "JDK" row of Table 1-1.
- JDK Requirement for PeopleTools 8.53, PeopleTools 8.54, and PeopleTools 8.55 has been added.
- The first point to the note has been added in Displaying the EI Repository Folder.
- A note has been added to Activating the USER_PROFILE Messages.
- HRMS 9.2 related information has been added to the note in the procedure Activating the USER_PROFILE Service Operation of Setting the CopyRowsetDelta Option.
- Troubleshooting has been updated with information about provisioning operation failure.

- The name of the "Known Issues" chapter has been changed to "Known Issues and Workarounds." In addition, Known Issues and Workarounds has been restructured.

Documentation-Specific Updates in Release 11.1.1.5.0

The following documentation-specific update has been made in the revision "4" of the release 11.1.1.5.0:

- In Certified Components, the Oracle Identity Manager version has been updated to Release 11.1.1.5 BP02.

The following documentation-specific update has been made in the revision "5" of the release 11.1.1.5.0:

- Installation includes connector installation scenarios depending on where you want to run the connector code (bundle), either locally in Oracle Identity Manager or remotely in a Connector Server.

The following documentation-specific update has been made in the revision "6" of the release 11.1.1.5.0:

- In Certified Components the PeopleTools 8.52 has been added as a newly certified target system.

The following documentation-specific updates have been made in the revision "7" of the release 11.1.1.5.0:

- Updated Installing and Configuring the Connector Server and Running the Connector Server to indicate that these procedures are optional, to be performed if you want to run the connector code (bundle) remotely in a Connector Server.
- Added Deploying the PeopleSoft Listener on WebSphere Application Server.
- Added bug 13497967 to Known Issues and Workarounds.

1

About the Connector

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 chapter contains the following sections:

Introduction to the PeopleSoft User Management 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.

> **See Also:**
>
> Installing Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about connector deployment configurations

Certified Components

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

Table 1-1 Certified Components

Item	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) • Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) • Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) and any later BP in this release track • Oracle Identity Manager 11*g* Release 1 BP06 (11.1.1.5.6) and any later BP in this release track
Target systems	The target system can be any one of the following: • PeopleTools 8.48 • PeopleTools 8.49 • PeopleTools 8.50 • PeopleTools 8.51 • PeopleTools 8.52 • PeopleTools 8.53 • PeopleTools 8.54 • PeopleTools 8.55 • PeopleTools 8.56 • PeopleTools 8.57 • PeopleTools 8.58 • PeopleTools 8.59 or later **Note:** If you are using PeopleTools 8.54, full reconciliation operation may not work as expected. Apply PeopleSoft Patch 21109998 using the following URL for this operation to work successfully: https://support.oracle.com/
Connector Server	11.1.2.1.0

Table 1-1 (Cont.) Certified Components

Item	Requirement
Connector Server JDK	JDK 1.6 Update 24 or later, or JRockit 1.6 or later If you are using PeopleTools 8.53, PeopleTools 8.54, or PeopleTools 8.55, see JDK Requirement for PeopleTools 8.53, PeopleTools 8.54, and PeopleTools 8.55, for information related to JDK requirement. If you are using PeopleTools 8.56 or PeopleTools 8.57, see JDK Requirement for PeopleTools 8.56 and PeopleTools 8.57, for information related to JDK requirement.
Other Software	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 11.1.1.5 BP01 with this target system, then install Oracle Applications Access Controls Governor (OAACG) release 8.6. See SoD Validation of Entitlement Provisioning for more information about the SoD feature.

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 determine the version of PeopleTools and the target system you are using:

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.

Usage Recommendation

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

- If you are using an Oracle Identity Manager release 9.1.0.2 BP05 or later and earlier than Oracle Identity Manager 11*g* Release 1 BP06 (11.1.1.5.6), then you must use the 9.1.1 version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 BP06 (11.1.1.5.6) or later, Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) or later, or Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.*x* version of this connector.

Certified Languages

The connector supports the following languages:

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

Connector Architecture

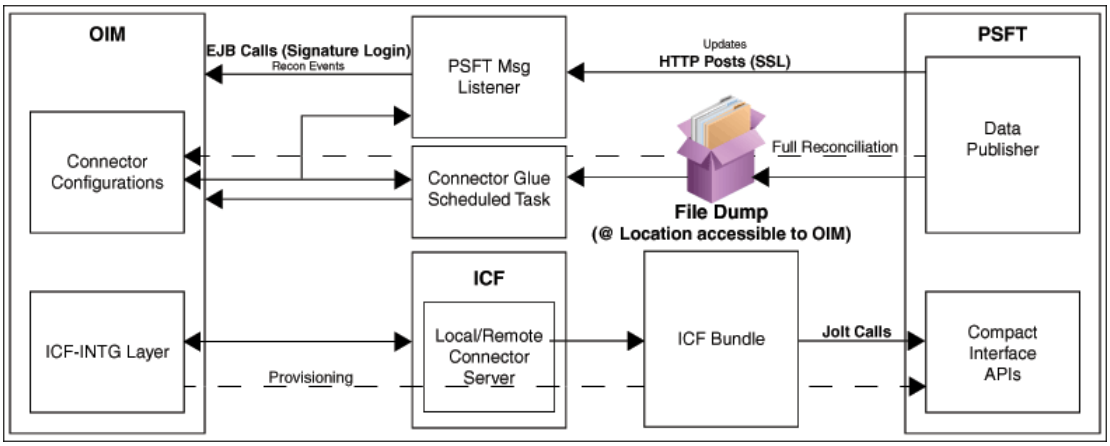
The architecture of the connector can be explained in terms of the connector operations it supports.

This section contains the following topics:

About the Connector Architecture

Figure 1-1 shows the architecture of the connector.

Figure 1-1 Architecture of the Connector



The target system is configured as a trusted source of identity data for Oracle Identity Manager. In other words, identity data that is created and updated on the target system is fetched into Oracle Identity Manager and used to create and update OIM Users.

The connector is implemented using the Identity Connector Framework (ICF). The ICF provides a container that separates the connector bundle from the application. The ICF also provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering.

For more information about the ICF, see Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

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:

- Lookup Reconciliation
- Full Reconciliation
- Incremental Reconciliation

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 Performing Lookup Reconciliation for instructions to perform Lookup reconciliation.

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 Support for Standard PeopleSoft Messages for more information about the message.

Full reconciliation involves the following steps:

See 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 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.

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 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 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, the PeopleSoft listener is deployed as an EAR file.

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 Adding New ID Types for more information.

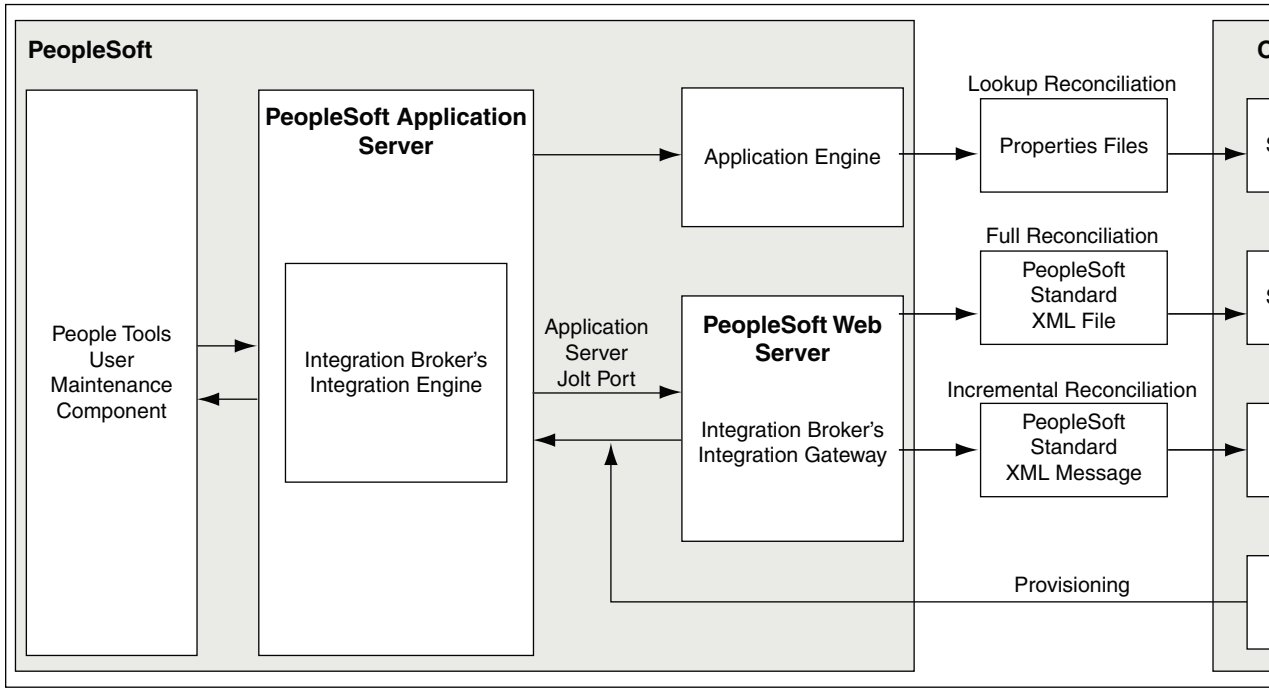
See SoD Validation of Entitlement Provisioning for information about the process followed for provisioning of role entitlements in an SoD-enabled environment.

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 Configuring the Scheduled Jobs 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.

Features of the Connector

The following are the features of the connector:

- Full and Incremental Reconciliation
- Support for Standard PeopleSoft Messages
- Support for Resending Messages That Are Not Processed

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.

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.

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 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`

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 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`.

Target authentication is also carried out during a ping request from the PeopleSoft node.

SoD Validation of Entitlement Provisioning

This connector supports the SoD feature in Oracle Identity Manager release 11.1.1.5 BP01.

This section contains the following topics:

- About SoD Validation of Entitlement Provisioning
- SoD Validation Process

About SoD Validation of Entitlement Provisioning

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:**
>
> Configuring SoD on Oracle Identity Manager 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.

   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.

Validation and Transformation of Account Data

You can configure validation and transformation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning.

- Lookup.PSFT.UM.ReconValidation and Configuring Validation of Data During Reconciliation provide information about setting up the validation feature during reconciliation.
- Configuring Transformation of Data During Reconciliation provides information about setting up the transformation feature.
- Lookup.PSFT.UM.ProvValidation and Configuring Validation of Data During Provisioning provide information about setting up the validation feature during provisioning.

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.

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

> **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.

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:

- Customer ID
- Customer Set ID

For Vendor:

- Vendor ID
- Vendor Set ID

The Adding New ID Types for Provisioning describes the procedure to add ID types.

Deleting User Accounts

The DELETE_USER_PROFILE component interface definition is used to delete user profile definitions. The delCompIntfcKey key is defined in the PeopleSoft Component Interface map definition file, PeopleSoftComponentInterfaces.xml.

The Lookup.PSFT.Configuration lookup definition contains a mapping for the delCompIntfcKey key to determine the user profile to be used for delete operations.

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.

Lookup Definitions for Exclusion Lists describes the lookup definitions where you specify the user IDs to be excluded during reconciliation and provisioning operations. Setting Up the Lookup Definitions for Exclusion Lists describes the procedure to add entries in these lookup definitions.

Support for Multiple Versions of the Target System

> **Note:**
>
> See Certified Components for information about the supported PeopleTools versions. 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 without any custom class loader. The connector uses the Identity Connector Framework (ICF) connector class loader for this feature. 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 Configuring the Connector to Support Multiple Versions of the Target System for more information.

Features Provided by the Identity Connector Framework

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

For more information, see Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

Support for the Connector Server

If required by your deployment, you can deploy the connector in the Connector Server. For more information, see Installing and Configuring the Connector Server.

Lookup Definitions Used During Connector Operations

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

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

Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field 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.

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:

- Lookup.PSFT.Configuration
- Lookup Definitions Used to Process USER_PROFILE Messages
- Lookup Definitions Used to Process DELETE_USER_PROFILE Messages
- Other Lookup Definitions

Lookup.PSFT.Configuration

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

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

Code Key	Decode	Description
Bundle Name	org.identityconnectors.peoplesoftintfc	Name of the connector bundle package. Do not modify this entry.
Bundle Version	1.0.5963	Version of the connector bundle class. Do not modify this entry.

Code Key	Decode	Description
Connector Name	org.identityconnectors.peoplesoft.compintfc.PeopleSoftCompIntfcConnector	Name of the connector class. Do not modify this entry.
Constants Lookup	Lookup.PSFT.UM.Constants	Name of the lookup definition that is used to store constants used by the connector.
delCompIntfcKey	DELETE_USER_PROFILE	Name of the component interface used for delete operations.
DELETE_USER_PROFILE	Lookup.PSFT.Message.DeleteUserProfile.Configuration	Name of the lookup definition for the DELETE_USER_PROFILE message.
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:** Determining the Root Audit Action Details
mappingFactoryClassName	org.identityconnectors.peoplesoft.common.mapping.idm.IDMSAXComponentInterfacesFactory	TBD
maxFindItems	300	TBD
Recon Exclusion List	Lookup.PSFT.UM.Recon.ExclusionList	Name of the lookup for specifying exclusions during reconciliation
rwCompIntfcKey	USER_PROFILE_8_4X **Note:** If you want to support a different component interface, you must change this value. See Connector Component Interfaces for the PeopleSoft User Management for more information.	Name of the component interface used for create and update operations.
Target Date Format	yyyy-MM-dd	Data format of the Date type data in the XML file and messages Do not modify this entry.

Code Key	Decode	Description
USER_PROFILE.VERSION_84	Lookup.PSFT.Message.UserProfile.Configuration	Name of the lookup definition for the USER_PROFILE message See Lookup.PSFT.Message.UserProfile.Configuration for more information about this lookup definition.
User Configuration Lookup	Lookup.PSFT.UM.Prov.Configuration	Name of the lookup definition that contains user-specific configuration properties for provisioning. Do not modify this entry.
xmlMapping[LOADFROMURL]	Enter the path to the PeopleSoft Component Interface map definition file. Sample value: `file://PATHTOXML/PeopleSoftComponentInterfaces.xml`	This file contains the definitions used by the connector for various operations. By default, the file is located in the /xml of the connector package. Note: See Connector Component Interfaces for the PeopleSoft User Management for more information about this definition file. If you deploy the connector on a cluster, you must copy this file to the same location on all the nodes.

The combination of the following fields form the Identity Connector Framework (ICF) connector key used for identifying the right connector bundle:

- Bundle Name
- Bundle Version
- Connector Name

You can configure the message names, such as USER_PROFILE and DELETE_USER_PROFILE defined in this lookup definition. See Setting Up the Lookup.PSFT.Configuration Lookup Definition for instructions on configuring these message names in the lookup definition.

Lookup Definitions Used to Process USER_PROFILE Messages

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

- Lookup.PSFT.Message.UserProfile.Configuration
- Lookup.PSFT.UM.UserProfile.ReconAttrMap
- Mapping Entries in the Lookup.PSFT.UM.UserProfile.ReconAttrMap Lookup Definition
- Lookup.PSFT.UM.UserProfile.Recon
- Mapping the Entries in the Lookup.PSFT.UM.UserProfile.Recon Lookup Definition

- Lookup.PSFT.UM.UserProfile.UserStatus
- Lookup.PSFT.UM.UserProfile.ChildTables
- Lookup.PSFT.UM.UserProfile.Transformation

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 .ReconAttrMap	Name of the lookup definition that maps Oracle Identity Manager attributes with the attributes in the USER_PROFILE message during reconciliation operations. See Lookup.PSFT.UM.UserProfile.ReconAttrMap 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 during reconciliation operations.
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 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 User	Name of the IT resource

Code Key	Decode	Description
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.
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.
Primary Email Lookup	Lookup.PSFT.UM.PrimaryEmail	Name of the lookup definition used to specify whether an e-mail ID is primary or not
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 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 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.

Code Key	Decode	Description
Validation Lookup Definition	Lookup.PSFT.UM.ReconValidation	Name of the validation lookup definition for reconciliation See Configuring Validation of Data During Reconciliation for more information about adding entries in this lookup definition.

Lookup.PSFT.UM.UserProfile.ReconAttrMap

The Lookup.PSFT.UM.UserProfile.ReconAttrMap 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~None~None~CHILD=Email IDs
Email Type	EMAILTYPE~PSUSEREMAIL~None~None~CHILD=Email IDs
Employee ID	EMPLID~PSOPRALIAS~OPRALIASTYPE=EMP
Language Code	LANGUAGE_CD~PSOPRDEFN
Multi Language Code	MULTILANG~PSOPRDEFN
Navigator Home Permission List	DEFAULTNAVHP~PSOPRDEFN
Primary Email	EMAILID~PSUSEREMAIL~PRIMARY_EMAIL=Y
Primary Permission List	OPRCLASS~PSOPRDEFN
Process Profile Permission List	PRCSPRFLCLS~PSOPRDEFN
Return ID	OPRID~PSOPRDEFN~None~None~PRIMARY
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.

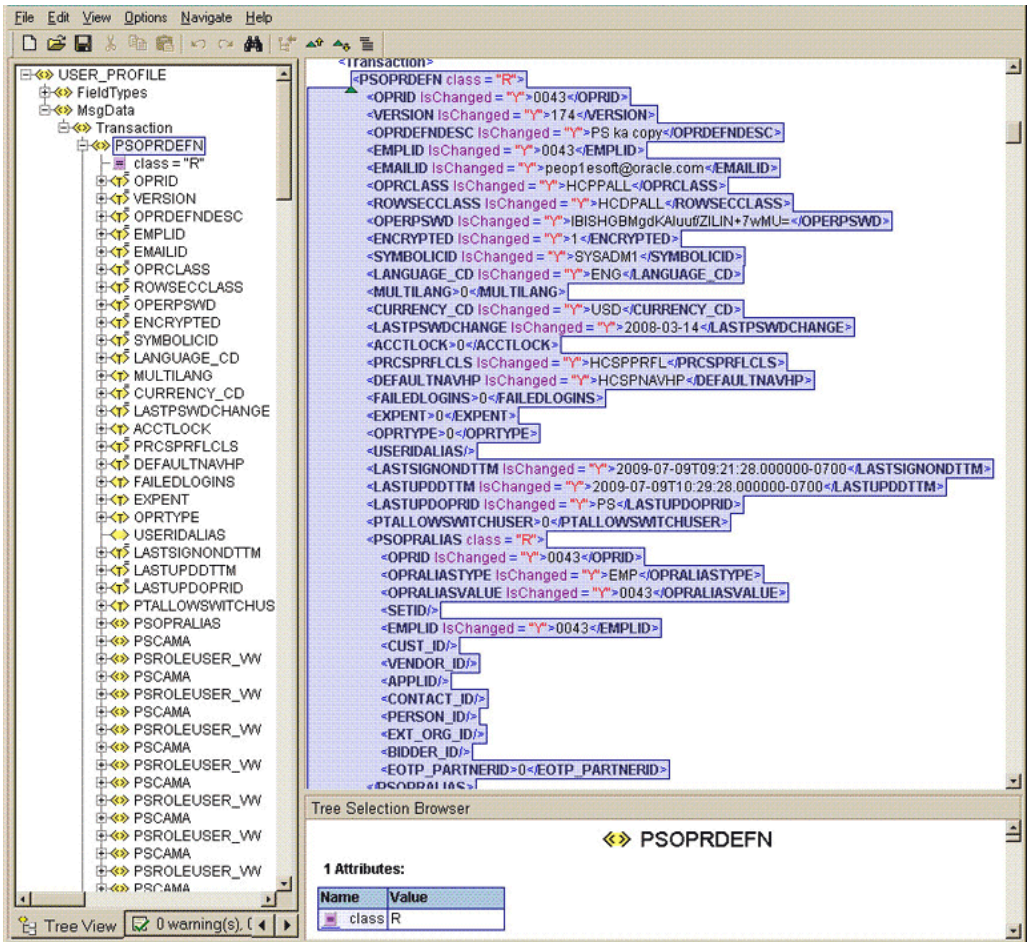
In case of multivalued attribute data, `CHILD` specifies that this is a Child data followed by the name of the table defined in the resource object to which the data corresponds.

Mapping Entries in the Lookup.PSFT.UM.UserProfile.ReconAttrMap Lookup Definition

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



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
```

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.ReconAttrMap 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.ReconAttrMap 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.

Mapping the Entries in the Lookup.PSFT.UM.UserProfile.Recon Lookup Definition

Consider the scenario discussed in Mapping Entries in the Lookup.PSFT.UM.UserProfile.ReconAttrMap Lookup Definition. 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.ReconAttrMap 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.ReconAttrMap 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.ReconAttrMap, 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.**

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

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

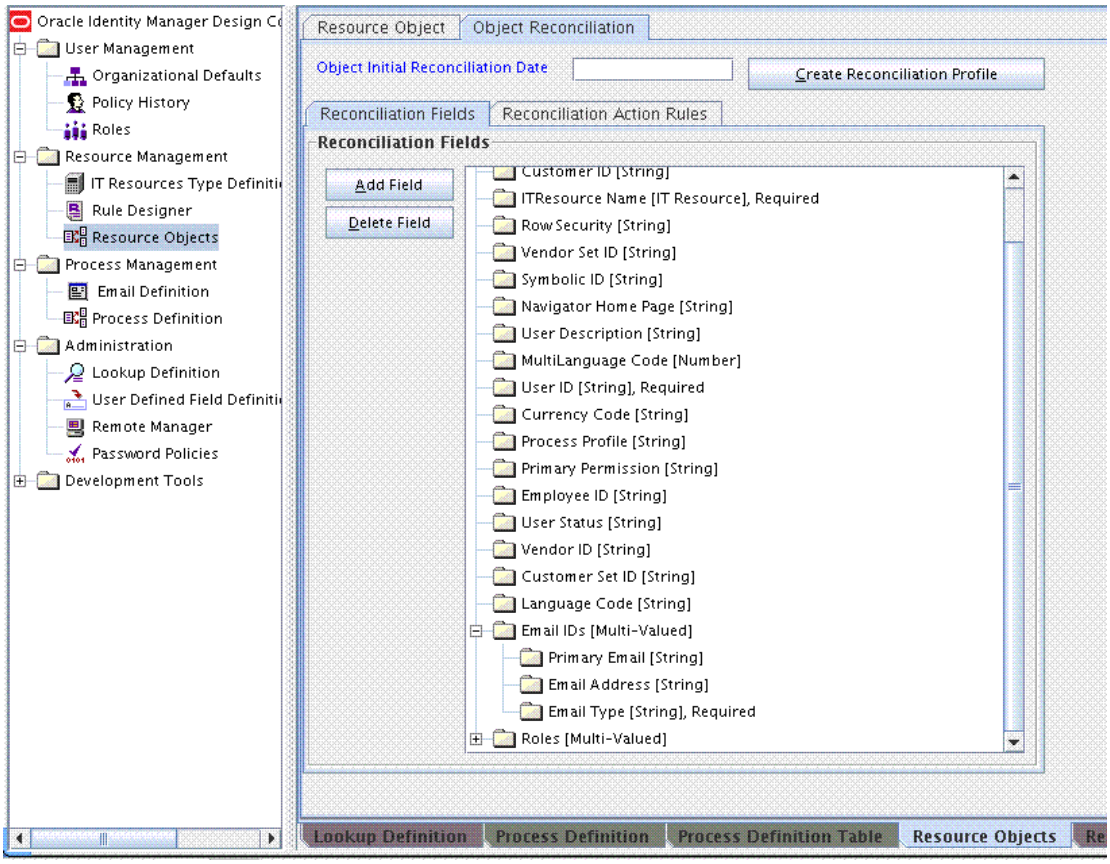
Lookup.PSFT.UM.UserProfile.ChildTables

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~Primary Email
Roles	Role Name

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 Configuring Transformation of Data During Reconciliation for more information about adding entries in this lookup definition.

Lookup Definitions Used to Process DELETE_USER_PROFILE Messages

The following lookup definitions are used to process DELETE_USER_PROFILE messages:

- Lookup.PSFT.Message.DeleteUserProfile.Configuration
- Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping
- Lookup.PSFT.UM.DeleteUserProfile.Recon

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 Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping for more information about this lookup definition.

Code Key	Decode	Description
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 User	Name of the IT resource
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 Lookup.PSFT.UM.DeleteUserProfile.Recon for more information about this lookup definition.
Resource Object	Peoplesoft User	Name of the resource object

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 **Note:** If you are using PeopleTools 8.52, replace the preceding default Decode value with the following value: EMPLID~PER_ORG_ASGN~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 Lookup.PSFT.UM.UserProfile.ReconAttrMap.

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

Other Lookup Definitions

The following are the predefined generic lookup definitions:

- Lookup.PSFT.UM.Prov.Configuration
- Lookup.PSFT.UM.ProvAttrMap
- Mappings in the Lookup.PSFT.UM.ProvAttrMap Lookup Definition
- Lookup.PSFT.UM.ProvValidation
- Lookup.PSFT.UM.ReconValidation
- Lookup Definitions for Exclusion Lists

Lookup.PSFT.UM.Prov.Configuration

The Lookup.PSFT.UM.Prov.Configuration lookup definition maps the provisioning configurations with the lookups.

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

Code Key	Decode
Provisioning Attribute Map	Lookup.PSFT.UM.ProvAttrMap

Code Key	Decode
Provisioning Exclusion List	Lookup.PSFT.UM.Prov.ExclusionList
Provisioning Validation Lookup	Lookup.PSFT.UM.ProvValidation

You can enable exclusions and validations during provisioning by adding the entries as shown in this lookup. To disable exclusions or validations, remove the corresponding entries in this lookup.

Lookup.PSFT.UM.ProvAttrMap

The Lookup.PSFT.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. These lookup definitions are used during provisioning.

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

Code Key	Decode
Currency Code[Lookup]	CurrencyCode
Customer ID	IDTypes~UM_IDTypes[IDType=CST]~Attributes~UM_Attributes[AttributeName=Customer ID]~AttributeValue
Customer Set ID	IDTypes~UM_IDTypes[IDType=CST]~Attributes~UM_Attributes[AttributeName=Set ID]~AttributeValue **Note:** For People Tools 8.48, the AttributeName is `SetID` (without space).
Employee ID	IDTypes~UM_IDTypes[IDType=EMP]~Attributes~UM_Attributes[AttributeName=Empl ID]~AttributeValue **Note:** For People Tools 8.48, the AttributeName is `EmplID` (without space).
Language Code[Lookup]	LanguageCode
Multi Language Code	MultiLanguageEnabled
Navigator Home Permission List[Lookup]	NavigatorHomePermissionList
Password	__PASSWORD__
Primary Permission List[Lookup]	PrimaryPermissionList
Process Profile Permission List[Lookup]	ProcessProfilePermissionList
Return ID	__UID__
Row Security Permission List[Lookup]	RowSecurityPermissionList
Symbolic ID	SymbolicID
UD_PS_EMAIL~Email Address	EmailAddresses~UM_EmailAddresses~EmailAddress
UD_PS_EMAIL~Email Type[Lookup]	EmailAddresses~UM_EmailAddresses~EmailType
UD_PS_EMAIL~Primary Email	EmailAddresses~UM_EmailAddresses~PrimaryEmail
UD_PSROLES~Role Name[Lookup]	Roles~UM_Roles~RoleName
User Description	UserDescription
User ID	__NAME__
User ID Alias	UserIDAlias

Code Key	Decode
Vendor ID	IDTypes~UM_IDTypes[IDType=VND]~Attributes~UM_Attributes[AttributeName=Vendor ID]~AttributeValue
Vendor Set ID	IDTypes~UM_IDTypes[IDType=VND]~Attributes~UM_Attributes[AttributeName=Set ID]~AttributeValue **Note:** For People Tools 8.48, the AttributeName is `SetID` (without space).

Mappings in the Lookup.PSFT.UM.ProvAttrMap Lookup Definition

The mappings in this lookup definition follow the Identity Connector Framework (ICF) conventions. The following is the format of the Code Key and Decode values in this lookup definition:

- *SUFFIX*[Lookup] means that the value of the attribute is retrieved from a lookup. For example, the value of the CurrencyCode attribute is retrieved from the Currency Code[Lookup] Code Key.
- For the Employee ID Code Key, Decode is the combination of the following elements separated by a tilde (~) character:

  IDTypes~UM_IDTypes[IDType=EMP]~Attributes~UM_Attributes[AttributeName=Empl ID]~AttributeValue

  In this format:

  - *IDTypes*: Refers to the ICF Parent Attribute Name
  - *UM_IDTypes*: Refers to the embedded ICF object class that contains *IDType* and *Attributes*. The default value of *IDType* is `EMP`.
  - *Attributes*: Refers to the ICF embedded object class that contains *AttributeName* and *AttributeValue*. The default value of *AttributeName* is `Empl ID`. The value of *AttributeValue* is retrieved from the form field.

  The following ICF hierarchy is created for the lookup:

  ```
  IDTypes [Objectclass UM_IDTypes]
          IDType : EMP
          Attributes [Objectclass UM_Attributes]
                  AttributeName : Empl ID
                  Attribute Value : <Form field mapping>
  ```

  This hierarchy is similar to the definition in PeoplesoftComponentInterfaces.xml, which is the default component interface map definition file.

  The same format holds true for the Customer ID, Customer Set ID, Vendor ID, and Vendor Set ID Code Keys.

- For the child form mappings, Code Key is the combination of the child form name and the child form attribute separated by a tilde (~) character.

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

  ICF Parent Attribute Name~ICF Embedded Object Class Name~Embedded Object Class Attribute

  The following ICF hierarchy is created for the email lookups:

```
EmailAddresses (Objectclass UM_EmailAddresses)
        EmailAddress
        EmailType
        PrimaryEmail
```

The same format holds true for the roles lookups.

- The following Code Keys are used for special configurations:
  - User ID: Refers to the key identifier for operations
  - Return ID: Refers to the UID returned after a create operation. This UID is used for further provisioning operations such as update and delete. This connector returns the User ID.
  - Password: Refers to the password field.

Lookup.PSFT.UM.ProvValidation

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

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

See Configuring Validation of Data During Provisioning for more information about adding entries in this lookup definition.

Lookup.PSFT.UM.ReconValidation

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

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

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

Lookup Definitions for Exclusion Lists

The Lookup.PSFT.UM.Prov.ExclusionList and Lookup.PSFT.UM.Recon.ExclusionList lookup definitions hold user IDs of target system accounts for which you do not want to perform provisioning and reconciliation operations, respectively.

The following is the format of the values stored in these lookups:

Code Key	Decode	Sample Values
User ID resource object field name	User ID of a user	Code Key: User ID Decode: User001

Code Key	Decode	Sample Values
User ID resource object field name with the [PATTERN] suffix	A regular expression supported by the representation in the `java.util.regex.Pattern` class	Code Key: User ID[PATTERN] To exclude users matching any of the user ID 's User001, User002, User088, then: Decode: User001|User002|User088 To exclude users whose user ID 's start with 00012, then: Decode: 00012* **See Also:** For information about the supported patterns, visit `http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html`

Setting Up the Lookup Definitions for Exclusion Lists describes the procedure to add entries in these lookup definitions.

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

This section discusses the following topics:

- User Attributes for Reconciliation
- Reconciliation Rules
- Reconciliation Action Rules

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.

Table 1-3 (Cont.) Attributes Used for Reconciliation

Resource Object Field	Target System Attribute	Description
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
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	PSUSEREMAIL.EMAILTYPE	E-mail type
Primary Email **Note:** To specify the e-mail address for an account, you must also specify the e-mail type of that e-mail address. You must have only one primary e-mail address if you provide e-mail addresses.	PSUSEREMAIL.PRIMARYEMAIL	Specifies if the e-mail address is primary
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)

Reconciliation Rules

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

- Overview of the Reconciliation Rule
- Viewing the Reconciliation Rules in the Design Console

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.

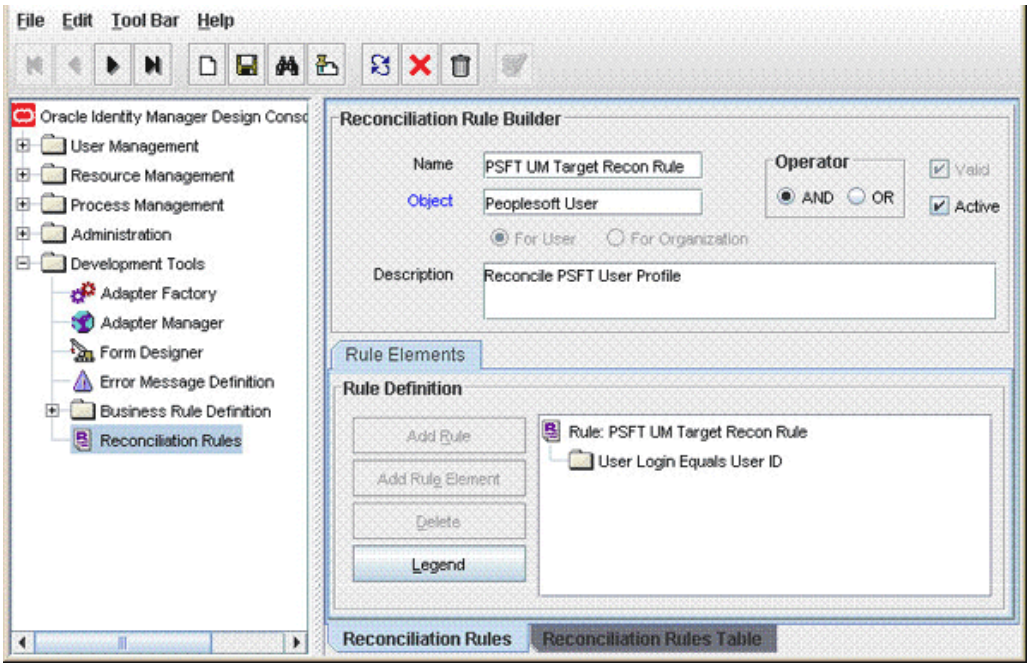
Viewing the Reconciliation Rules in the Design Console

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



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:

- Overview of the Reconciliation Action Rules
- Viewing the Reconciliation Action Rules in the Design Console

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

Viewing the Reconciliation Action Rules in the Design Console

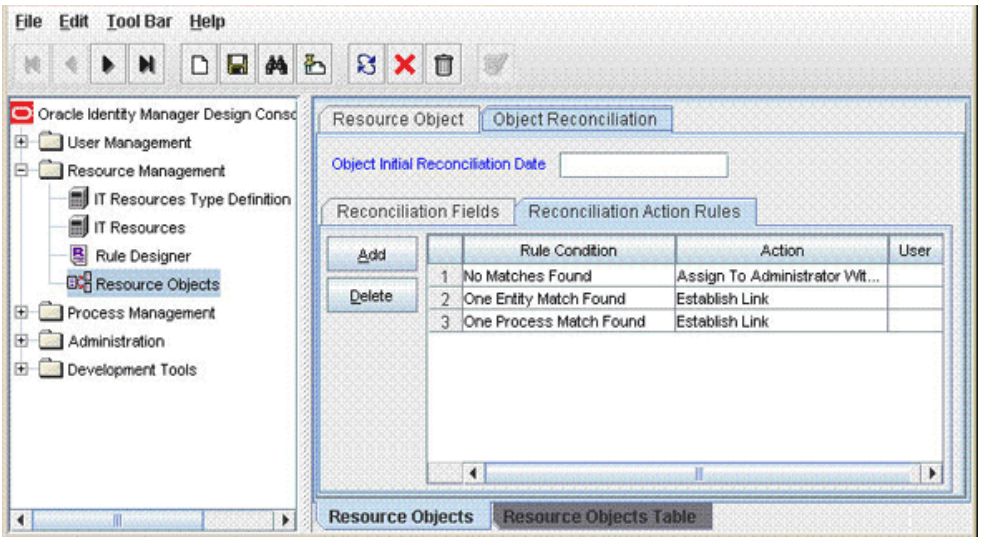
After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

> **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



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

This section discusses the following topics:

- User Provisioning Functions
- User Attributes for Provisioning

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:**
>
> Developing Provisioning Processes and Using the Adapter Factory in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* 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 Update User
Update the language code of a user	PSFT UM Update User
Update the currency code of a user	PSFT UM Update User
Update the Primary Permission list of a user	PSFT UM Update User
Update the Employee Id	PSFT UM Update ID Types
Update the Vendor Set Id	PSFT UM Update ID Types
Update the Vendor Id	PSFT UM Update ID Types
Update the Customer Set Id	PSFT UM Update ID Types
Update the Customer Id	PSFT UM Update ID Types
Update the Process Profile Permission list of a user	PSFT UM Update User
Update the Navigator Home Permission list of a user	PSFT UM Update User
Update the Row Security Permission list of a user	PSFT UM Update User
Update the User Id alias of a user	PSFT UM Update User
Add a role to a user	PSFT UM Modify Multiple Attr Data
Revoke a role from a user	PSFT UM Modify Multiple Attr Data
Update Role	PSFT UM Modify Multiple Attr Data
Add an e-mail address	PSFT UM Modify Multiple Attr Data
Revoke an e-mail address	PSFT UM Modify Multiple Attr Data
Update an e-mail address	PSFT UM Modify Multiple Attr Data
Lock or disable a user	PSFT UM Modify Lock Unlock User
Unlock or enable a user	PSFT UM Modify Lock Unlock User
Delete a user	PSFT UM Delete User

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
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 Permission List	PSOPRDEFN.DEFAULTNAVHP	Navigator home page address	PSFT UM Create User
Primary Permission List	PSOPRDEFN.OPRCLASS	Primary permission list	PSFT UM Create User
Customer ID	CUST_AL_SRCH.CUST_ID (CRM Table)	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	SETID_TBL.SETID (CRM Table)	Customer's SetID	PSFT UM Create User
Vendor ID	VENDOR.VENDOR_ID (FSCM Table)	Vendor ID	PSFT UM Create User
Vendor Set ID	SETID_TBL.SETID (FSCM Table)	Vendor's Set ID	PSFT UM Create User
Multivalued Fields			

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

OIM PeopleSoft UM Resources Process Form Field	Target System Attribute	Description	Adapter
Role Name	PSROLEUSER_VW.ROLENAME	The role name that is assigned to the user profile	PSFT UM Update Child Table Values
Email Address	PSUSEREMAIL.EMAILID	E-mail address (e-mail account)	PSFT UM Update Child Table Values
Email Type	PSUSEREMAIL.EMAILTYPE	Email type (e-mail account)	PSFT UM Update Child Table Values
Primary Email	PSUSEREMAIL.PRIMARY_EMAIL	Specifies if the e-mail address is primary	PSFT UM Update Child Table Values

Note:

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

Roadmap for Deploying and Using the Connector

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

- Deploying the Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Using the Connector describes guidelines on using the connector and the procedure to configure reconciliation runs.
- Extending the Functionality of the Connector describes procedures that you can perform to extend the functionality of the connector.
- Testing and Troubleshooting describes the procedure to use the connector testing utility for testing the connector.
- Known Issues and Workarounds lists known issues associated with this release of the connector.
- Determining the Root Audit Action Details provides information about root audit action.
- Setting Up SSL on Oracle WebLogic Server describes how to configure SSL on Oracle WebLogic Server for PeopleTools 8.50.
- Changing Default Message Versions describes how to activate and deactivate message versions.

2
Deploying the Connector

Deploying the connector involves the following steps:

- Preinstallation
- Installation
- Postinstallation
- Upgrading the Connector

Preinstallation

Preinstallation information is divided across the following sections:

- Preinstallation on Oracle Identity Manager
- Preinstallation on the Target System
- Installing and Configuring the Connector Server
- Running the Connector Server

Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Files and Directories on the Installation Media
- JDK Requirement for PeopleTools 8.53, PeopleTools 8.54, and PeopleTools 8.55
- JDK Requirement for PeopleTools 8.56 and PeopleTools 8.57

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
Files in the bundle directory	These JAR files contain bundles for the connector.
configuration/Peoplesoft_User-Management-CI.xml	This XML file contains configuration information that is used during connector installation.
Files in the dataset directory: ModifyProvisionedResource_PeoplesoftUser.xml ProvisionResource_PeoplesoftUser.xml	These XML files contain preconfigured datasets that can be used to configure the provisioning operations. **Note:** These files specific to Oracle Identity Manager release prior to 11.1.2.
JavaDoc	This directory contains information about the Java APIs used by the connector.

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

File in the Installation Media Directory	Description
lib/PSFT_UM-oim-integration.jar	This JAR file contains the class files that are specific to integration of the connector with PeopleSoft target systems. During connector deployment, this file is copied to the 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 Oracle Identity Manager database.
The following files and directories in the listener directory: base directory lib/deploytool.jar build.xml deploy.properties	The base directory contains the class files for the PeopleSoftOIMListener.ear file. 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, the PeopleSoft listener is deployed as an EAR file. The deploytool.jar file contains the class files required for deploying the listeners. The build.xml file contains configurations to build the listener EAR file. The deploy.properties file contains Oracle Identity Manager connection details.
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 If PeopleSoft Application Designer Project Is Not Imported and Creating the Application Engine Program If PeopleSoft Application Designer Project Is Imported. The project files contain the PeopleCode for the steps that you define for importing a Project from Application Designer. This is explained in 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
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 Oracle Identity Manager database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages
test/config/reconConfig.properties test/config/log.properties	These files are used by the InvokeListener.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 operations.

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

File in the Installation Media Directory	Description
test/lib/PSFTTest.jar	This JAR file is used by the testing utility for provisioning operations.
test/scripts/InvokeListener.bat test/scripts/InvokeListener.sh	This BAT file and the UNIX shell script call the testing utility for reconciliation.
test/scripts/PeoplesoftProvisioningTester.bat test/scripts/PeoplesoftProvisioningTester.sh	This BAT file and the UNIX shell script call the testing utility for provisioning.
xml/PeopleSoftComponentInterfaces.xml	This XML file contains PeopleSoft Component Interface map definitions for the connector components.
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
xml/PeoplesoftUserManagementRequestDatasets.xml	This XML file preconfigured request dataset for the PeopleSoft User Management connector that can be imported into the metadata store (MDS). **Note:** This dataset should *not* be imported if you are using Oracle Identity Manager release 11.1.2.*x* or later.

JDK Requirement for PeopleTools 8.53, PeopleTools 8.54, and PeopleTools 8.55

If you are using PeopleTools 8.53, PeopleTools 8.54, or PeopleTools 8.55, then the following is the JDK requirement:

- If you are already using a Connector Server, then it is mandatory to use JDK 1.7.0_02 as the minimum version in the Connector Server.
- If the you are not using Connector Server and Oracle Identity Manager is not using JDK 1.7.0_02, then follow one of the following steps:
  - Refer the Oracle Identity Manager certification matrix and upgrade the JDK version used by Oracle Identity Manager to JDK 1.7.0_02 if it is supported.
  - If JDK 1.7.0_02 is not supported for Oracle Identity Manager, then it is mandatory to use a Connector Server with minimum JDK 1.7.0_02. In addition, enter the name of this Connector Server as the value of the Connector Server name parameter of the IT resource.

JDK Requirement for PeopleTools 8.56 and PeopleTools 8.57

If you are using PeopleTools 8.56 or 8.57, then the following is the JDK requirement:

- If you are already using a Connector Server, then it is mandatory to use JDK 1.8.0_40 as the minimum version in the Connector Server.

- If the you are not using Connector Server and Oracle Identity Manager is not using JDK 1.8.0_40, then follow one of the following steps:
  - Refer the Oracle Identity Manager certification matrix and upgrade the JDK version used by Oracle Identity Manager to JDK 1.8.0_40 if it is supported.
  - If JDK 1.8.0_40 is not supported for Oracle Identity Manager, then it is mandatory to use a Connector Server with minimum JDK 1.8.0_40. In addition, enter the name of this Connector Server as the value of the Connector Server name parameter of the IT resource.

Preinstallation on the Target System

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:

- Importing a Project from Application Designer
- Creating a Target System User Account for Connector Operations

Importing a Project from Application Designer

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

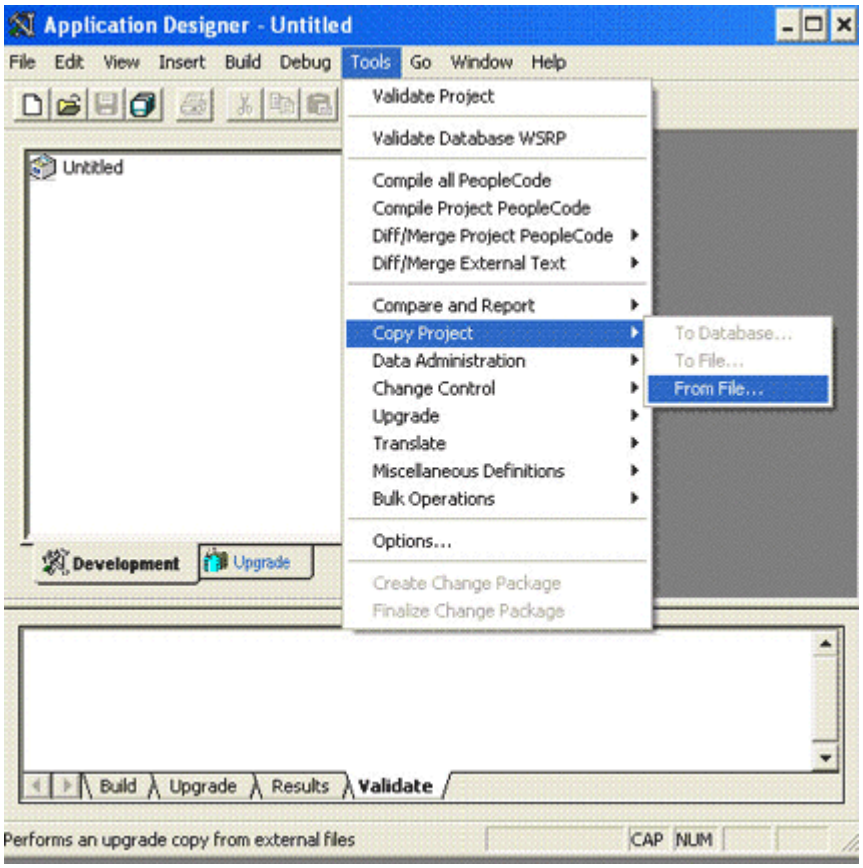
You can import the OIM_UM project created in Application Designer to automate the steps for creating a permission list. You can also create a permission list by manually performing the steps described in Creating a Permission List. If you import the OIM_UM project, then you need not perform the steps 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 If PeopleSoft Application Designer Project Is Not Imported and Creating the Application Engine Program If PeopleSoft Application Designer Project Is Imported 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 directories:
>
> *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.**



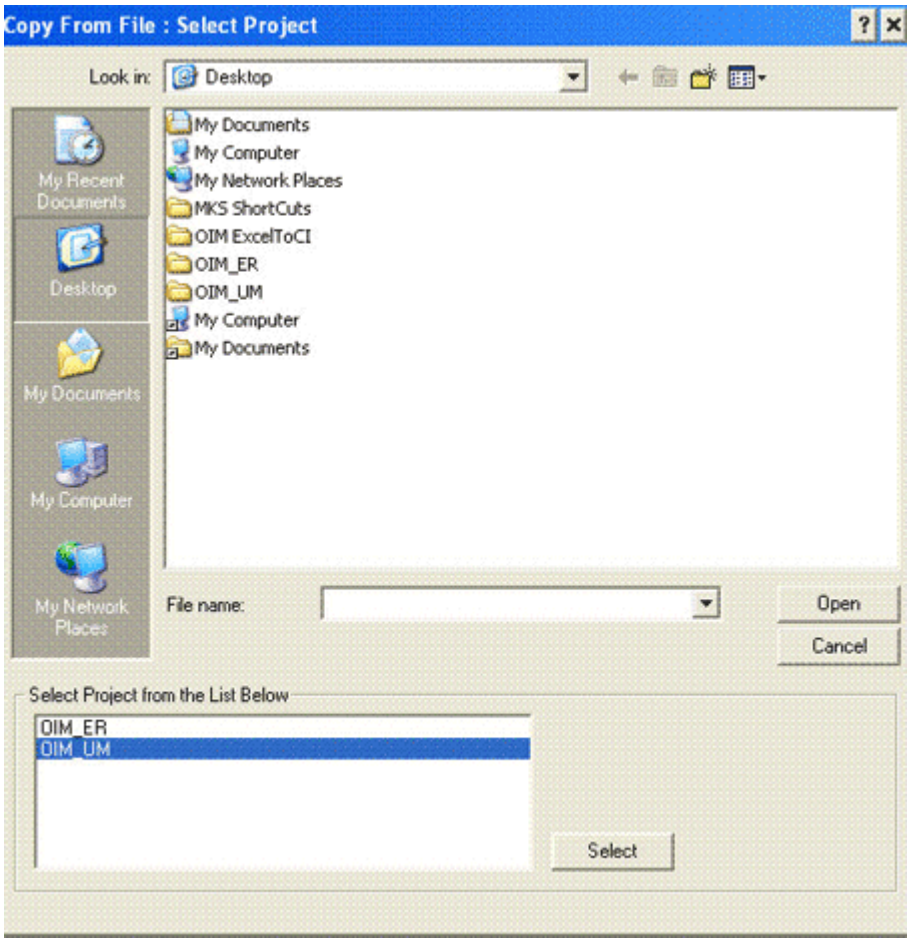
The Copy From File : Select Project dialog box appears.

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.

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.

- Creating a Permission List
- Creating a Role for a Limited Rights User
- Assigning the Required Privileges to the Target System Account

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 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:
   - For PeopleTools 8.54 and earlier releases, click **PeopleTools, Security, Permissions & Roles,** and then click **Permission Lists.**
   - For PeopleTools 8.55, 8.56, and 8.57, click **NavBar**, **Navigator**, **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.**

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:
   - For PeopleTools 8.54 and earlier releases, click **PeopleTools, Security, Permissions & Roles,** and then click **Roles.**
   - For PeopleTools 8.55, 8.56, and 8.57, click **NavBar**, **Navigator**, **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.**

> **Note:**
>
> Permission list EOEI9000 is not available in PeopleTools 8.53, PeopleTools 8.54, PeopleTools 8.55, 8.56, or PeopleTools 8.57, and is hence not applicable.

   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.**

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:
   - For PeopleTools 8.54 and earlier releases, click **PeopleTools**, **Security**, **User Profiles** , and then click **User Profiles**.

- For PeopleTools 8.55, 8.56, and 8.57, click **NavBar**, **Navigator**, **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.**

   > **Note:**
   >
   > Role EIR Administrator is not available in PeopleTools 8.53, PeopleTools 8.54, PeopleTools 8.55, 8.56, or PeopleTools 8.57 and is hence not applicable.

   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.

Installing and Configuring the Connector Server

This procedure is optional. If you want to run the connector code (bundle) remotely in a Connector Server, then install and configure the Connector Server as follows:

1. Create a new directory on the machine where you want to install the Connector Server. In this section, *CONNECTOR_SERVER_HOME* represents this directory.
2. Unzip the Connector Server package in your new directory from Step 1. The Connector Server package is available with the Identity Connector Framework (ICF).
3. In the ConnectorServer.properties file, set the following properties, as required by your deployment. The ConnectorServer.properties file is located in the conf directory.

Property	Description
connectorserver.port	Port on which the Connector Server listens for requests. The default is `8759`.
connectorserver.bundleDir	Directory where the connector bundles are deployed. The default is bundles.
connectorserver.libDir	Directory in which to place dependent libraries. The default is lib.

connectorserver.usessl	If set to true, the Connector Server uses SSL for secure communication. The default is `false`. If you specify `true`, use the following options on the command line when you start the Connector Server:
	`-Djavax.net.ssl.keyStore`
	`-Djavax.net.ssl.keyStoreType` (optional)
	`-Djavax.net.ssl.keyStorePassword`

connectorserver.ifaddress	Bind address. To set this property, uncomment it in the file (if necessary). The bind address can be useful if there are more NICs installed on the machine.
connectorserver.key	Connector Server key. The default password for this property is `changeit`.

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

     For more information, see Running the Connector Server on UNIX and Linux Systems or Running the Connector Server on Windows Systems.
   - For all other properties, edit the ConnectorServer.properties file manually.
5. The conf directory also contains the logging.properties file, which you can edit if required by your deployment.

> **Note:**
>
> For related information, see Running the Connector Server and Creating the IT Resource for the Connector Server.
>
> To configure the Connector Server to support multiple versions of the connector:
>
> - The connector JAR files copied to the *CONNECTOR_SERVER_HOME*/bundle directory must contain target system-specific copy of the psjoa.jar file. For PeopleTools 8.54, PeopleTools 8.55, PeopleTools 8.56, and PeopleTools 8.57, the directory must contain target system-specific copy of the psmanagement.jar file.
> - Ensure that there are no JAR files in the *CONNECTOR_SERVER_HOME*/lib directory.

Running the Connector Server

This procedure is optional. If you want to run the connector code (bundle) remotely in a Connector Server, then install and configure the Connector Server as described in Installing and Configuring the Connector Server. See Creating the IT Resource for the Connector Server for related information.

After installing and configuring the Connector Server, perform one of the following procedures to run the Connector Server depending on your platform:

- Running the Connector Server on UNIX and Linux Systems
- Running the Connector Server on Windows Systems

Running the Connector Server on UNIX and Linux Systems

To run the Connector Server on UNIX and Linux systems, use the connectorserver.sh script, as follows:

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Installing and Configuring the Connector Server.
2. Change to the *CONNECTOR_SERVER_HOME*/bin directory.
3. Use the `chmod` command to set the permissions to make the connectorserver.sh script executable.
4. Run the connectorserver.sh script. The script supports the following options.

Option	Description
/run [-J*java-option*]	Runs the Connector Server in the console. Optionally, you can specify one or more Java options. For example, to run the Connector Server with SSL: `./connectorserver.sh /run -J-Djavax.net.ssl.keyStore=mykeystore.jks -J-Djavax.net.ssl.keyStorePassword=password`
/start [-J*java-option*]	Runs the Connector Server in the background. Optionally, you can specify one or more Java options.
/stop	Stops the Connector Server, waiting up to 5 seconds for the process to end.
/stop *n*	Stops the Connector Server, waiting up to *n* seconds for the process to end.
/stop -force	Stops the Connector Server. Waits up to 5 seconds and then uses the kill -KILL command, if the process is still running.
/stop *n* -force	Stops the Connector Server. Waits up to *n* seconds and then uses the kill -KILL command, if the process is still running.
/setKey *key*	Sets the Connector Server key. The connectorserver.sh script stores the hashed value of *key* in the connectorserver.key property in the ConnectorServer.properties file.

Running the Connector Server on Windows Systems

To run the Connector Server on Windows systems, use the ConnectorServer.bat script as follows:

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

   The ConnectorServer.bat script supports the following options:

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

3. To stop the Connector Server, stop the respective Windows service.

Installation

You can run the connector code locally in Oracle Identity Manager or remotely in a Connector Server.

This section contains the following topics:

- Installation Options
- Installation on Oracle Identity Manager
- Installation on the Target System

Installation Options

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

- Run the connector code locally in Oracle Identity Manager.

In this scenario, you deploy the connector in Oracle Identity Manager.

- Run the connector code remotely in a Connector Server.

  In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server. See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing, configuring, and running the Connector Server.

Installation on Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

- Running the Connector Installer
- Copying the Connector Files and External Code Files
- Configuring the IT Resource
- Configuring the Connector to Support Multiple Versions of the Target System
- Deploying the PeopleSoft Listener
- Removing the PeopleSoft Listener

Running the Connector Installer

> **Note:**
>
> 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 Enabling Request-Based Provisioning if you want to use the request-based provisioning feature for this target system.

To run the Connector Installer:

1. Create a directory for the connector, for example, PSFT_UM-11.1.1.6.0, in the *OIM_HOME*/server/ConnectorDefaultDirectory/targetsystems-lib directory. This directory contains connector-specific files.
2. Copy the **psjoa.jar** file from the *PEOPLESOFT_HOME*/web/psjoa directory to the directory created in Step 1.

   > **Note:**
   >
   > If you are using PeopleTools 8.54, PeopleTools 8.55, PeopleTools 8.56, or PeopleTools 8.57, you must also copy the psmanagement.jar file from *PEOPLESOFT_HOME*/client-tools/class to the directory created in Step 1 of this procedure.

3. Copy the contents of the connector installation media directory into another directory to hold the installation files.

   For example: *OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_UM-11.1.1.6.0

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

4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.*x:*
     a. Log in to Oracle Identity Manager Administration and User Console by using the user account described in Creating the User Account for Installing Connectors of *Oracle Fusion Middleware Administering Oracle Identity Manager*.
     b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector.**
   - For Oracle Identity Manager release 11.1.2.*x:*
     a. Log in to Oracle Identity System Administration.
     b. In the left pane, under System Management, click **Manage Connector.**
5. In the Manage Connector page, click **Install**.
6. From the Connector List, select **PeopleSoft User Management 11.1.1.6.0.** 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, click **Refresh**.
   c. From the Connector List, select **PeopleSoft User Management 11.1.1.6.0.**
7. Click **Load**.
8. To start the installation process, click **Continue.**

   The following tasks are performed, in sequence:

   a. Configuration of connector libraries
   b. Import of the connector XML files (by using the Deployment Manager)
   c. Compilation of adapters

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

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.
9. 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 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. Configuring the IT resource for the connector.

   See Configuring the IT Resource for more information.

b. Configuring the scheduled tasks.

   See Configuring the Scheduled Jobs for Lookup Field Synchronization for more information.

c. Configuring the xmlMapping lookup in the configuration lookup definition.

   See Setting Up the Lookup.PSFT.Configuration Lookup Definition for more information.

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

Copying the Connector Files and External Code Files

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

File in the Installation Media Directory	Destination for Oracle Identity Manager
xml/PeoplesoftComponentInterfaces.xml	Copy to a path applicable to each node of the target system. Map the path to the xmlMapping lookup in the configuration lookup.
lib/PeopleSoftOIMListener.ear	*OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_UM-11.1.1.6.0/listener/

Table 2-2 (Cont.) Files to Be Copied to the Oracle Identity Manager Host Computer

File in the Installation Media Directory	Destination for Oracle Identity Manager
Files in the peoplecode directory	*OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_UM-11.1.1.6.0/peoplecode
Files in the test/scripts directory	*OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_UM-11.1.1.6.0/scripts
Files in the test/config directory	*OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_UM-11.1.1.6.0/config

> **Note:**
>
> You might want to configure the connector for different versions of the target system simultaneously. See Configuring the Connector to Support Multiple Versions of the Target System for more information about creating and placing the target system-specific JAR files.

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 User` IT resource is automatically created in Oracle Identity Manager. You must specify values for the parameters of this IT resource as follows:

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

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

     Log in to Oracle Identity System Administration.
2. If you are using Oracle Identity Manager release 11.1.1.x, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.*x,* in the left pane, under Configuration, click **IT Resource.**
4. In the IT Resource Name field on the Manage IT Resource page, enter `PSFT User` and then click **Search.**
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters.**

7. Click **Edit** and specify values for the parameters of the IT resource. Table 2-3 describes each parameter.
8. Click **Update** to save the values.

IT Resource Parameters

Table 2-3 describes the IT resource parameters.

Table 2-3 IT Resource Parameters

Parameter	Description
Configuration Lookup	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.
Connector Server Name	Name of the remote connector server IT resource, if any. See Creating the IT Resource for the Connector Server for related information.
IsActive	Specifies 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`
TopologyName	Name of the Segregation of Duties (SoD) topology, if any SoD integration exists. See Specifying a Value for the TopologyName IT Resource Parameter for more information.
URL	JOLT 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 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*.
User	User name of the target system account to be used for connector operations. You create this account by performing the procedure described in the Creating a Target System User Account for Connector Operations section. Sample value: `PS`
Password	Password of the target system account specified by the User parameter.

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.

Configuring the Connector to Support Multiple Versions of the Target System

You can configure the connector for multiple versions of the target system simultaneously.

This section contains the following topics:

- About Configuring a Connector to Support Multiple Versions of the Target System
- Configuring the Connector to Support Multiple Versions of the Target System

About Configuring a 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.

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.

Configuring the Connector to Support Multiple Versions of the Target System

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

1. From the connector package, copy the bundle JAR file in a temporary directory.

   Sample JAR file: `bundle/org.identityconnectors.peoplesoftintfc-1.0.5963.jar`

   Sample temporary directory: `c:\temp`

2. Run the following command to extract the manifest file, META-INF/MANIFEST.MF, from the JAR file:

   ```
   jar -xvf org.identityconnectors.peoplesoftintfc-1.0.5963.jar
   ```

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

3. Delete the bundle JAR file in the temporary directory.
4. Update the value of **ConnectorBundle-Version** in the manifest file to a new value.

   For example:

   ```
   ConnectorBundle-Version: 1.0.5964
   ```

5. Copy the **psjoa.jar** file (target specific) from the *PEOPLESOFT_HOME*/web/psjoa directory to the lib folder of the extracted bundle jar.

   > **Note:**
   >
   > If you are using PeopleTools 8.54, PeopleTools 8.55, PeopleTools 8.56, or PeopleTools 8.57, you must also copy the **psmanagement.jar** file (target specific) from the *PEOPLESOFT_HOME*/client-tools/class directory to the lib folder of the extracted bundle jar.De

6. Create a new bundle JAR file that contains the updated manifest file as follows:

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

      ```
      c:\temp
      ```

   b. Run the following command:

      ```
      jar -cvfm org.identityconnectors.peoplesoftintfc-1.0.5964.jar META-INF/
      MANIFEST.MF *
      ```

   The new connector bundle JAR name contains the new bundle version.

7. In the case of a remote connector server, copy the new bundle JAR file in the bundles directory of the remote connector server instead of posting the JAR file to the Oracle Identity Manager database. Skip to Step 8.
8. Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 6 to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

   - For Microsoft Windows:

     OIM_HOME/server/bin/UploadJars.bat

   - For UNIX:

     OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Select ICFBundle as the JAR type.

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

9. Create a copy of the configuration lookup, for example, Lookup.PSFTV2.Configuration.

   Ensure you update the new lookup with the bundle version.
10. Create a new PeopleSoft UM IT resource definition for the new bundle. Map the **Configuration Lookup** parameter of the new IT resource to Lookup.PSFTV2.Configuration.

    The new IT resource will use the new bundle and the corresponding third-party libraries without affecting the previous installations.
11. Repeat the preceding procedure for the other version of the target system, PeopleSoft 8.48.

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.

Note:

The PeopleSoft Employee Reconciliation and PeopleSoft User Management connectors have different IT resources. Therefore, you must configure separate HTTP nodes for messages of the Employee Reconciliation and User Management connectors.

Even if an existing node is configured to the PeopleSoft listener on Oracle Identity Manager, a separate node is required for messages of the PeopleSoft Employee Reconciliation connector.

A single listener is sufficient for both the connectors. You can configure the nodes to point to the same listener with different IT resource names.

If you are using IBM WebSphere Application Server, perform the procedure described in Deploying the PeopleSoft Listener on WebSphere Application Server.

See Also:

Upgrading the PeopleSoft Listener for information about upgrading the listener

This section contains the following topics:

- Prerequisites for Deploying the PeopleSoft Listener
- Deploying the PeopleSoft Listener on Oracle Identity Manager
- Prerequisites for Deploying the PeopleSoft Listener on WebSphere Application Server
- Deploying the PeopleSoft Listener on WebSphere Application Server
- Importing Oracle Identity Manager CA Root Certificate for WebLogic Server
- Importing Oracle Identity Manager CA Root Certificate for WebSphere Application Server

Prerequisites for Deploying the PeopleSoft Listener

Before deploying the PeopleSoft listener, perform the following steps:

- Ensure Apache Ant 1.7 or later and JDK 1.6 or later are installed.
- Set the following environment values in ant.properties:
  - *ORACLE_HOME* maps to the Oracle Identity Manager installation directory. For example, `/ps1/beahome/Oracle_IDM1`
  - *ORACLE_COMMON* maps to the oracle_common directory in *MW_HOME*, where *MW_HOME* is the directory in which Oracle Identity Management Suite is installed. For example, `/ps1/beahome/oracle_common`
  - *WLS_HOME* maps to the WebLogic Server directory. For example, `/middleware/wlserver_10.3`
  - *JAVA_HOME* maps to your JDK environment. For example, `C:\Program Files\Java\jdk1.6.0_24`

  - *PATH* must include the *JAVA_HOME*/bin directory. You can set the *PATH* variable using the `SET PATH=$JAVA_HOME/bin:$PATH` command.

- Build the **wlfullclient.jar** file in Oracle WebLogic server, for example, in the *WLS_HOME*/server/lib directory:

  1. Change directories to *WLS_HOME*/server/lib.
  2. Run the following command:

     ```
     java -jar ../../../modules/com.bea.core.jarbuilder_1.3.0.0.jar
     ```

     > **Note:**
     >
     > The exact jar file version can be different based on the WebLogic Server. Use the corresponding file with the name as `com.bea.core.jarbuilder` at the *WLS_HOME*/../modules/ directory.

- Start Oracle Identity Manager and the Admin Server.

Deploying the PeopleSoft Listener on Oracle Identity Manager

To deploy the PeopleSoft listener on Oracle Identity Manager:

1. Set the Oracle Identity Manager connection details in the listener/deploy.properties file.

   The listener directory is located in the connector package directory, for example, *OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_UM-11.1.1.6.0.

2. Run the following command:

   ```
   ant setup-listener
   ```

> **Note:**
>
> If you need to deploy the listener in an Oracle Identity Manager cluster, then:
>
> - Specify the name of the cluster for the `oim.server.name` property in the listener/deploy.properties file.
> - Update the following configurations appropriately with the URL of the listener, /PeopleSoftOIMListener:
>   - Front-end web server
>   - Load balancer
>   - PeopleSoft nodes
> - Copy the connector package into the *OIM_HOME*/server/ConnectorDefaultDirectory directory of every node.

Prerequisites for Deploying the PeopleSoft Listener on WebSphere Application Server

Before deploying the PeopleSoft listener, ensure Apache Ant 1.7 or later and JDK 1.6 or later are installed. Then, set the following environment values in the ant.properties file:

- *OIM_ORACLE_HOME* maps to the Oracle Identity Manager installation directory. For example, `/ps1/was/Oracle_IDM1`

  You can set this variable using the `setenv OIM_ORACLE_HOME <value>` command.

- *JAVA_HOME* maps to your JDK environment. For example, `/usr/local/packages/jdk16/`

  You can set this variable using the `setenv JAVA_HOME <value>` command.

- *PATH* must include the *JAVA_HOME*/bin directory. You can set this variable using the `setenv PATH $JAVA_HOME/bin:$PATH` command.

- Create the listener EAR file in listener directory. To do so:

  1. Change directories to $*OIM_ORACLE_HOME*/server/ConnectorDefaultDirectory/PSFT_UM-11.1.1.6.0/listener.
  2. Run the following commands:

```
rm -rf deployear
mkdir deployear
cp -rf base/PeopleSoftOIMListener.ear/META-INF deployear
cp -rf base/PeopleSoftOIMListener.ear/PeopleSoftOIMListener.war/WEB-INF
deployear
cp -rf $OIM_ORACLE_HOME/server/client/oimclient.jar deployear/WEB-INF/lib
cp -rf $OIM_ORACLE_HOME/server/platform/iam-platform-utils.jar deployear/WEB-
INF/lib
cp -rf $OIM_ORACLE_HOME/server/platform/iam-platform-auth-client.jar deployear/
WEB-INF/lib
cd deployear
sed -i 's/OIM_ADMIN_USER/xelsysadm/g' WEB-INF/web.xml
jar -cvf PeopleSoftOIMListener.war WEB-INF
rm -rf WEB-INF/
jar -cvf PeopleSoftOIMListener.ear META-INF PeopleSoftOIMListener.war
rm -rf META-INF
rm -rf PeopleSoftOIMListener.war
```

Deploying the PeopleSoft Listener on WebSphere Application Server

To deploy the PeopleSoft listener on IBM WebSphere Application Server:

1. Log in to the WebSphere Admin console.
2. Expand **Applications.**
3. Select **Enterprise Applications** from the list.
4. Click **Install** and browse for the listener EAR directory.
5. Select **Fast Path** and click **Next.**
6. Under **Map modules to servers,** select **oim_cluster** to map the listener EAR file.
7. Save the listener EAR application and start the service.
8. Go to the *$IBM_HTTP_SERVER*/Plugins/bin directory on the computer hosting the IBM HTTP Server as your Web server. Suppose this is Node A.

9. Copy configurewebserver1.sh to the *$WAS_HOME/*bin directory on the computer hosting the deployment manager.
10. Run the `./configurewebserver1.sh` command.

    This will generate the plugin-cfg.xml file.
11. Copy plugin-cfg.xml from Node A to another node, say Node C.

    For example, copy plugin-cfg.xml from Node A in *$WAS_HOME/*profiles/Dmgr01/config/cells/*CELL/*nodes/*NODE_C/*servers/webserver1/plugin-cfg.xml to *$IBM_HTTP_SERVER/*Plugins/config/webserver1 directory on Node C.
12. Perform syncNode for all nodes. To do so on Node A and another node, say Node B, run the following commands on both the nodes:

    > **Note:**
    >
    > Ensure that the deployment manager is running on Node A. If a node is not stopped, then kill the node from the command line.

    ```
    $WAS_HOME/profiles/<Custom01>/bin/stopNode.sh
    $WAS_HOME/profiles/<Custom01>/bin/syncNode.sh <dmgr host>  8879
    $WAS_HOME/profiles/<Custom01>/bin/startNode.sh
    $WAS_HOME/profiles/<Custom01>/bin/startServer.sh soa_server
    $WAS_HOME/profiles/<Custom01>/bin/startServer.sh oim_server
    ```

    In the above commands, 8879 is the SOAP connector port of the deployment manager. You can find SOAP connector port in the *$WAS_HOME/*profiles/*Dmgr01/*logs/AboutThisProfile.txt file.
13. Start IBM HTTP Server by running following command:

    ```
    $IBM_HTTP_SERVER/bin/apachectl start
    ```

    You can try to access Oracle Identity Manager from IBM HTTP Server by using the path such as `http://NODE_C/oim`.

Importing Oracle Identity Manager CA Root Certificate for WebLogic Server

If you have configured SSL in Oracle Identity Manager, for the PeopleSoft listener to work in SSL you must import Oracle Identity Manager CA root certificate into PeopleSoft WebServer.

To import the CA root certificate into PeopleSoft WebServer for WebLogic Server:

1. Identity the certificate of issuing authority, the root CA for Oracle Identity Manager.

   If you use the default demo certificate, then the root certificate is located in the following location:

   *MW_HOME/*wlserver_10.3/server/lib/CertGenCA.der

   If the certificate is issued by an external entity, then you must import the corresponding root certificate.
2. Use **pskeymanager** to import the root certificate into PeopleSoft WebServer keystore.

Importing Oracle Identity Manager CA Root Certificate for WebSphere Application Server

If you have configured SSL in Oracle Identity Manager, for the PeopleSoft listener to work in SSL you must import Oracle Identity Manager CA root certificate into PeopleSoft WebServer.

To import the CA root certificate into PeopleSoft WebServer for WebSphere Application Server:

1. Identity the certificate of issuing authority, the root CA for Oracle Identity Manager.

   In the WebSphere Admin console, navigate to Security, SSL certificate and key management, Key stores and certificates, CellDefaultTrustStore, and Signer certificates. Then, select **root** and click **Extract.**

   If the certificate is issued by a different entity, then you must import the corresponding root certificate.
2. Use **pskeymanager** to import the root certificate into PeopleSoft WebServer keystore.

Removing the PeopleSoft Listener

If you uninstall the connector, you must also remove the listener. Installing a new connector over a previously deployed listener creates discrepancies.

> **Note:**
>
> - This section is not a part of installation on Oracle Identity Manager. You might need this procedure to extend the connector.
> - See Upgrading the PeopleSoft Listener for more information about upgrading the listener.

This section contains the following topics:

- Removing the PeopleSoft Listener on WebSphere Application Server
- Removing the PeopleSoft Listener for WebLogic Server

Removing the PeopleSoft Listener on WebSphere Application Server

To remove the PeopleSoft listener on 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.ear** 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.**

Removing the PeopleSoft Listener for WebLogic Server

To remove the PeopleSoft listener from for WebLogic Server, run the following command from the listener directory:

```
ant undeploy
```

To remove the PeopleSoft listener of the connector of a previous release, perform the following procedure:

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.ear.** 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.ear.**
10. Click **Delete.**

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

Installation on the Target System

During this stage, you configure the target system to enable it for reconciliation and provisioning operations.

> **Note:**
>
> If the target system is PeopleSoft 9.1 with PeopleTools 8.51, the target system must be patched with the PeopleSoft USER_PROFILE project.

This information is provided in the following sections:

- Configuring the Target System for Lookup Reconciliation
- Configuring the Target System for Full Reconciliation
- Configuring the Target System for Incremental Reconciliation
- Configuring the Target System for Provisioning

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

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:

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 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 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.

Configuring the Target System for Full Reconciliation

Configuring the target system for full reconciliation involves configuring the USER_PROFILE message.

This section contains the following topics:

> **Note:**
>
> The screenshots are taken on PeopleTools 8.49 version. They may vary for other versions of PeopleTools.

- Creating the Remote Node
- 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

Displaying the EI Repository Folder

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

> **Note:**
>
> - If you are using PeopleTools 8.53 or later as the target system, do not perform the procedure described in this section.
> - Perform this procedure using the PeopleSoft administrator credentials.

To display the EI Repository folder:

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

Activating the USER_PROFILE Messages

> **Note:**
>
> If you are using PeopleTools 8.53 or later as the target system, do not perform the procedure described in this section.

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.**
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.

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 window:
   - For PeopleTools 8.54 and earlier releases, expand **Enterprise Components, Integration Definitions,** and then click **Full Data Publish Rules.**
   - For PeopleTools 8.55, 8.56, and 8.57, click **NavBar**, **Navigator**, **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.**
4. Click **Save.**

About Configuring the PeopleSoft Integration Broker

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.

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.

Configuring the PeopleSoft Integration Broker Gateway

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:
   - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Configuration,** and then click **Gateways.**
   - For PeopleTools 8.55, 8.56, and 8.57, click **NavBar**, **Navigator**, **PeopleTools, Integration Broker, Configuration,** and then click **Gateways.**
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.**

Creating the Remote Node

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 the PeopleSoft Internet Architecture window:
      - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Configuration,** and then click **Gateways.**
      - For PeopleTools 8.55 and 8.56, click **NavBar**, **Navigator**, **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 the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Nodes.**
   - For PeopleTools 8.55 and 8.56, click **NavBar**, **Navigator**, **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.

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:

> **Note:**
>
> If the message version is not the same as specified, then you can change the message version as described in Changing Default Message Versions.

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 or HRMS 9.2 and Oracle Identity Manager, you must send `version_84`. So, you must use the default version, `VERSION_84`, for HRMS 9.0 and HRMS 9.2.
>
> If you are using PeopleTools 8.53, then you must use PeopleSoft HRMS 9.2 as the minimum version.

4. In the Default Service Operation Version region, click **Active.**

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 the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Queues.**
   - For PeopleTools 8.55, 8.56, and 8.57, click **NavBar**, **Navigator**, **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:
   >
   > a. From the Queue Status list, select **Run.**
   >
   > b. Click **Save.**

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 the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
   - For PeopleTools 8.55, 8.56 and 8.57, click **NavBar**, **Navigator**, **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.
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 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.**

d. Click **Save.**

e. Click **Return to Search.**

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.

> **Note:**
>
> The PeopleSoft Employee Reconciliation and PeopleSoft User Management connectors have different IT resources. Therefore, you must configure separate HTTP nodes for messages of the Employee Reconciliation and User Management connectors.
>
> Even if an existing node is configured to the PeopleSoft listener on Oracle Identity Manager, a separate node is required for messages of the PeopleSoft Employee Reconciliation connector.
>
> A single listener is sufficient for both the connectors. You can configure the nodes to point to the same listener with different IT resource names.

This section contains the following topics:

- Setting Up the Security for the DELETE_USER_PROFILE Service Operation
- Defining the Routing for the DELETE_USER_PROFILE Service Operation
- Preventing Transmission of Unwanted Fields During Incremental Reconciliation
- Removing Unwanted Fields at Message Level

About 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.

Configuring PeopleSoft Integration Broker

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.

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 the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Nodes.**
   - For PeopleTools 8.55 and 8.56, click **NavBar**, **Navigator**, **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: Location

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

   Sample value: PSFT User

   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. Ping Node will fail if the IT resource is not specified correctly.

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:

a. Verify if `secureFileKeystorePath` in the integrationgateway.properties file is correct.

b. Verify if `secureFileKeystorePasswd` in the integrationgateway.properties file is correct.

c. 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.

Setting the CopyRowsetDelta Option

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

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

> **Note:**
>
> The screenshots are taken on PeopleTools 8.49 version. They may vary for other versions of PeopleTools.

To configure the USER_PROFILE service operation:

1. In the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
   - For PeopleTools 8.55 and 8.56, click **NavBar**, **Navigator**, **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.**
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:
   >
   > a. Click the Look up icon.
   >
   > b. 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.
   >
   > c. Select the node.
   >
   > d. Click **Save.**

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

Activating the DELETE_USER_PROFILE Service Operation

To activate the DELETE_USER_PROFILE service operation:

> **Note:**
>
> - If the message version is not the same as specified, then you can change the message version as described in Changing Default Message Versions.
> - The screenshots are taken on PeopleTools 8.49 version. They may vary for other versions of PeopleTools.

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.**
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 the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Queues.**
   - For PeopleTools 8.55 and 8.56, click **NavBar**, **Navigator**, **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:
   >
   > a. From the Queue Status list, select **Run.**
   >
   > b. Click **Save.**

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 the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**

- For PeopleTools 8.55 and 8.56, click **NavBar**, **Navigator**, **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.
4. Attach the permission list **OIMUM,** created as a part of the preinstalltion, in Step 3, (See 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.

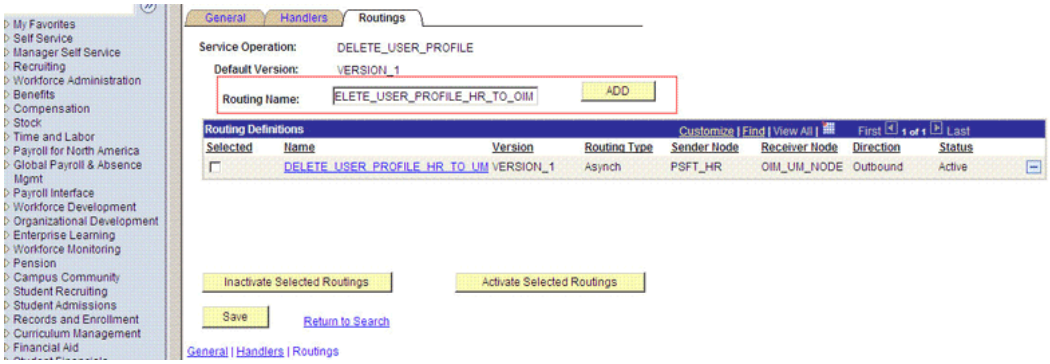
   a. Click the plus sign (+) to add a row for the Permission List field.
   b. In the Permission List field, enter **OIM** and then click the Look up Permission List icon.

      The **OIMUM** permission list appears.
   c. From the Access list, select **Full Access.**
   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:



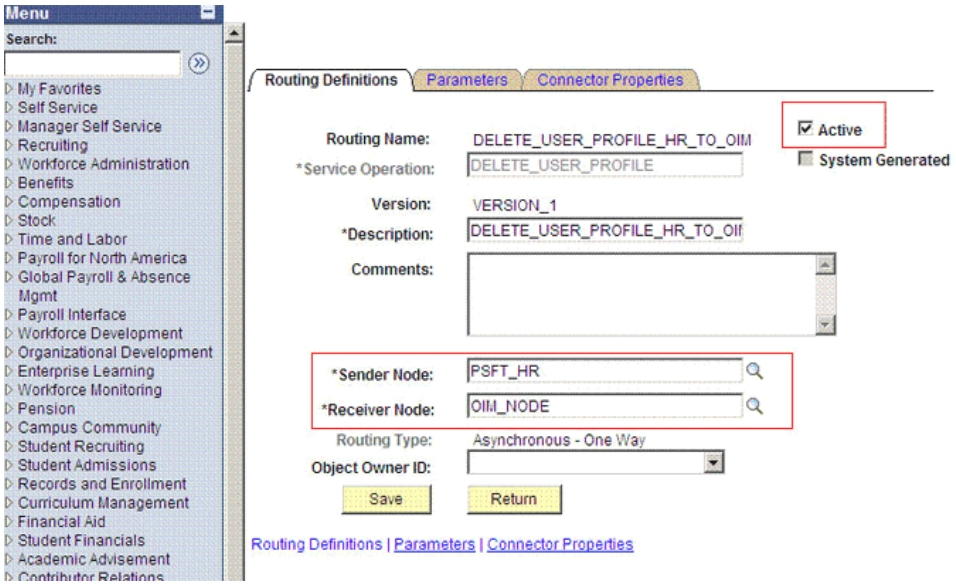
2. On the Routing Definition tab, enter the following:

   Sender Node: `PSFT_HR`

> **Note:**
>
> The sender node is the default active local node. To locate the sender node:
>
> a. Click the Look up icon.
>
> b. 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.
>
> c. Select the node.
>
> d. 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.

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 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 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`

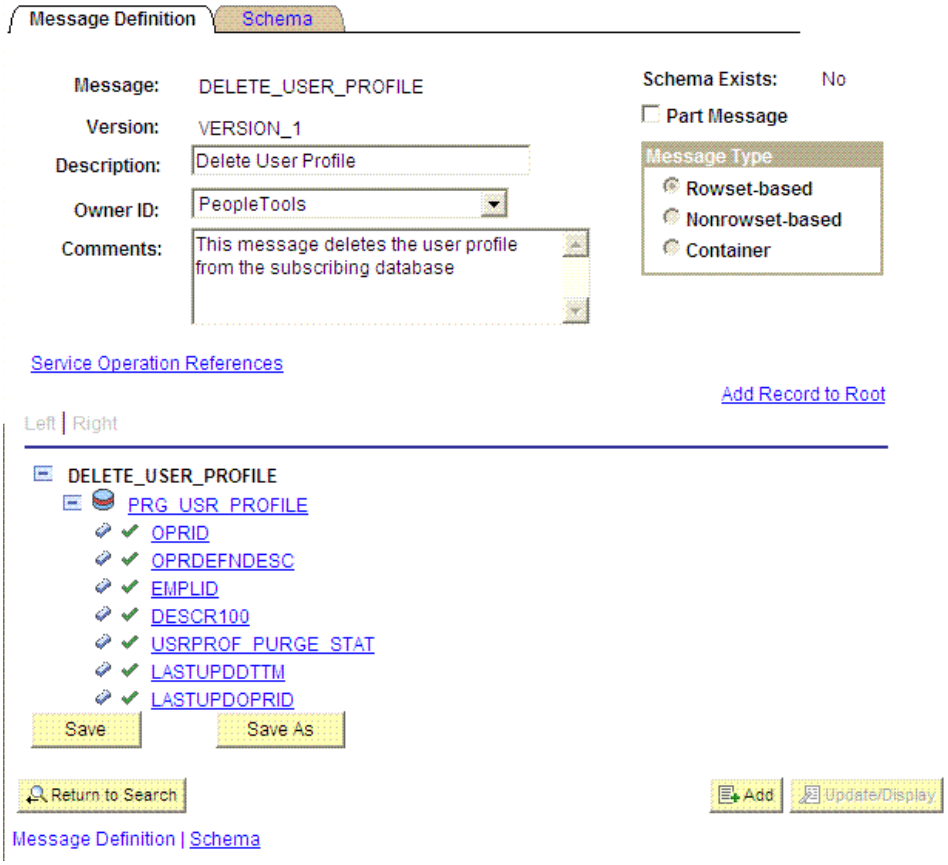
  In addition, refer to Chapter 43 of PeopleCode API Reference PeopleBook on Oracle Technology Network at the following location

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

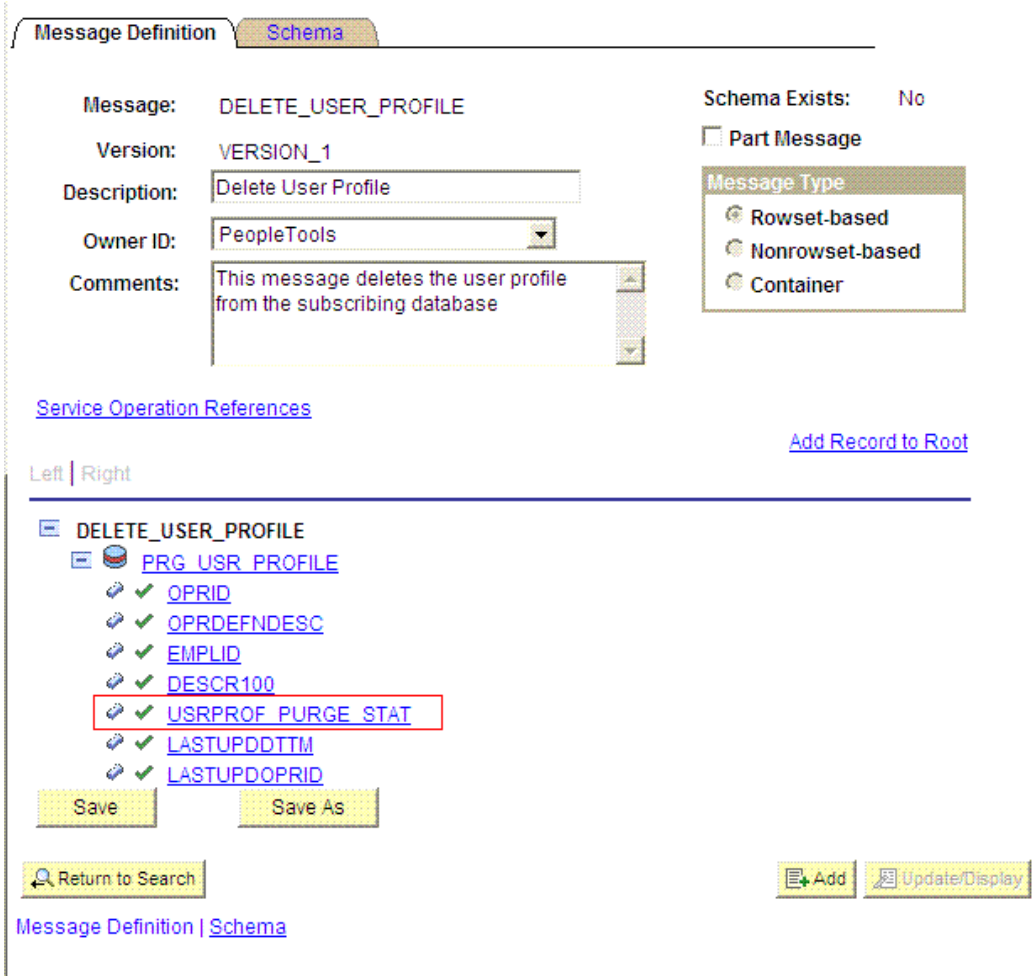
Removing Unwanted Fields at Message Level

To remove unwanted fields at the message level:

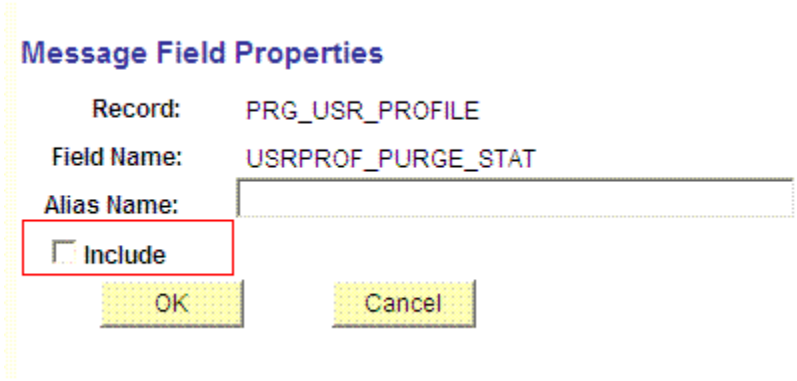
1. Expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Messages.**
2. Search for and open the desired message, for example, DELETE_USER_PROFILE.VERSION_1 used for incremental reconciliation.
3. Expand the message.



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.

Configuring the Target System for Provisioning

To configure the target system for provisioning, you are required to perform the following procedure for adding FIND Method Support to the USER_PROFILE Component Interface:

The default USER_PROFILE component interface does not support the FIND method. However, the PeopleSoft User Management connector requires the FIND method in order to support account iteration and list.

To add FIND method support to an existing USER_PROFILE component interface, follow these steps:

1. Load the USER_PROFILE component interface in the PeopleSoft Application Designer.
2. On the left window (which shows the USERMAINT Component), select the OPRID field under the PSOPRDEFN_SRCH object.

   Drag this field over to the right window (which shows the USER_PROFILE component interface).

   When you drop the field, a new key called FINDKEYS will be created in the USER_PROFILE component interface. Under that key, there will be a sub-key called OPRID.
3. Right-click on the OPRID name under FINDKEYS, and select **Edit Name.** Change the name to UserID.
4. Right click on USER_PROFILE component interface and select **Component Interface Properties.** Select the **Standard Methods** tab, then select the **Find** checkbox. Click **OK** to close the Component Interface Properties dialog.
5. Save your changes to the USER_PROFILE component interface.

The Find method is now visible under the METHODS field for the component interface. To verify the functionality of the new FIND method, right-click on the component interface and select **Test Component Interface.**

> **Note:**
>
> A PeopleSoft administrator should grant Full Access to the FIND method for the component interface (in addition to the Create, Get, Save, and SetPassword methods).
>
> See Connector Component Interfaces for the PeopleSoft User Management for information about component interface map definitions.

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
   ```

Postinstallation

Postinstallation information is divided across the following sections:

- Configuring Oracle Identity Manager
- Configuring SSL for Oracle Identity Manager
- Configuring SoD on Oracle Identity Manager
- Configuring the Target System
- Creating the IT Resource for the Connector Server

Configuring 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.

- Configuring Oracle Identity Manager 11.1.2 or Later
- Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging
- Setting Up the Lookup Definitions for Exclusion Lists
- Setting Up the Lookup.PSFT.UM.UserProfile.UserStatus Lookup Definition
- Setting Up the Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping Lookup Definition for PeopleTools 8.52
- Setting Up the Lookup.PSFT.Configuration Lookup Definition
- Setting up the Lookup.PSFT.Configuration Lookup Definition for Connection Pooling
- Enabling Request-Based Provisioning
- Localizing Field Labels in UI Forms

Configuring Oracle Identity Manager 11.1.2 or Later

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

- Creating and Activating a Sandbox
- Creating a New UI Form
- Creating an Application Instance
- Publishing a Sandbox

- Harvesting Entitlements and Sync Catalog
- Updating an Existing Application Instance with a New Form

Creating and Activating a Sandbox

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

1. On the upper navigation bar, click **Sandboxes.** The Manage Sandboxes page is displayed.
2. On the toolbar, click **Create Sandbox.** The Create Sandbox dialog box is displayed.
3. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.
4. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.
5. Click **Save and Close.** A message is displayed with the sandbox name and creation label.
6. Click **OK.** The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. Select the sandbox that you created.
8. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
9. On the toolbar, click **Activate Sandbox.**

   The sandbox is activated.

Creating a New UI Form

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

1. In the left pane, under Configuration, click **Form Designer.**
2. Under Search Results, click **Create.**
3. Select the resource type for which you want to create the form, for example, `Peoplesoft User`.
4. Enter a form name and click **Create.**

Creating an Application Instance

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

1. In the System Administration page, under Configuration in the left pane, click **Application Instances.**
2. Under Search Results, click **Create.**

3. Enter appropriate values for the fields displayed on the Attributes form and click **Save.**
4. In the Form drop-down list, select the newly created form and click **Apply.**
5. Publish the application instance for a particular organization.

Publishing a Sandbox

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

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

Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

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

Updating an Existing Application Instance with a New Form

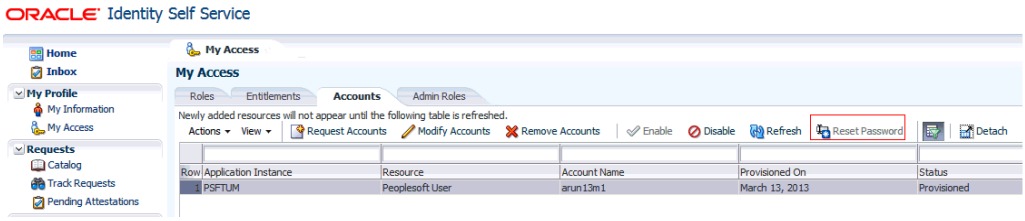
For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in Creating and Activating a Sandbox.
2. Create a new UI form for the resource as described in Creating a New UI Form.
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in Publishing a Sandbox.

Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later

In Oracle Identity Manager release 11.1.2.1.0 or later, you can reset password for an account after logging in as the user by navigating to My Access, Accounts tab.

The Reset Password option is enabled for only those accounts that follow the UD_*FORMNAME*_PASSWORD naming convention for the password field. Otherwise, this option would be disabled as shown in the following sample screenshot:

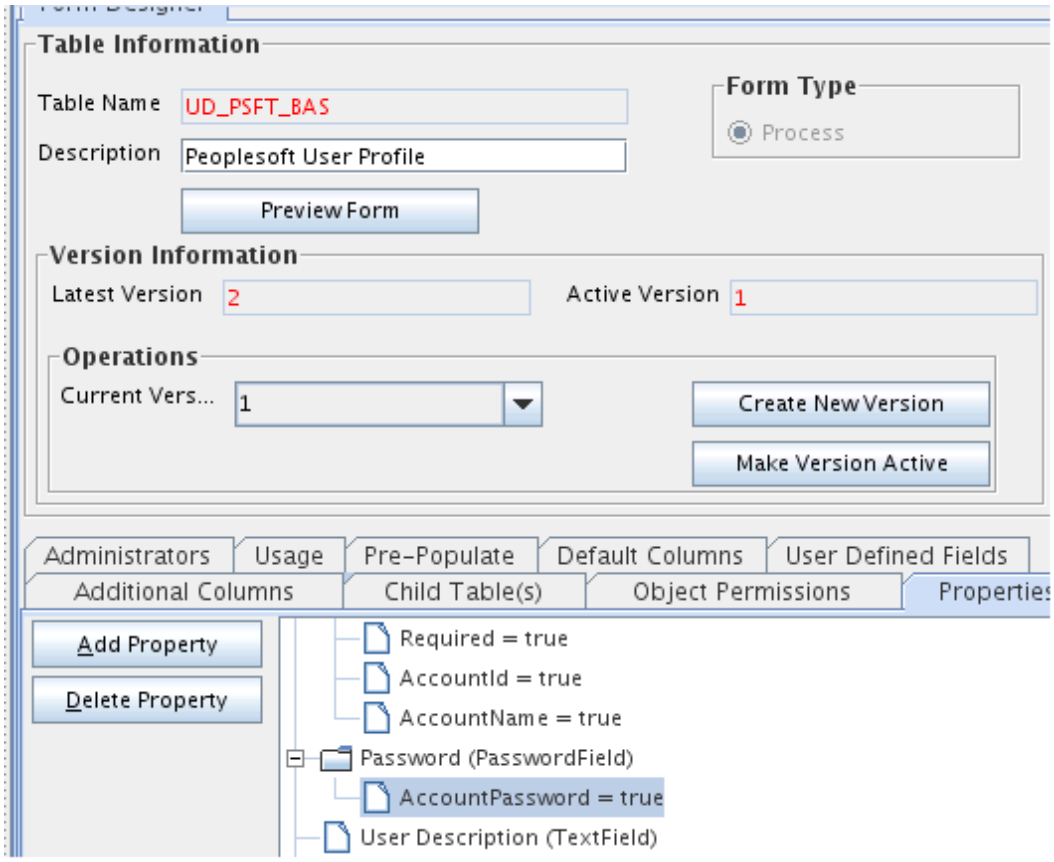


> **Note:**
>
> In Oracle Identity Manager 11.1.2 prior to release 11.1.2.1.0, if you want to change the password of a PeopleSoft User Management account under My Information, the account is not available for selection in the drop-down list of accounts. See bug 14697905 in Known Issues and Workarounds for more information about this known issue.

To enable the Reset Password option in Oracle Identity Manager release 11.1.2.1.0 or later:

1. Log in to Oracle Identity System Design console.
2. Under Development Tools, click **Form Designer.**
3. Enter `UD_PSFT_BAS` in the Table Name field and click the **Query for records** button.
4. Click **Create New Version.**
5. 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.
6. From the **Current Version** list, select the newly created version.
7. Click the **Properties** tab.
8. Select the password field, and click **Add Property.**
9. From the Property Name list, select **AccountPassword.**
10. In the Property Value field, enter `true`.
11. Click **Save.**

    The password field is tagged with the `AccountPassword = true` property as shown in the following screenshot:



12. Click **Make Version Active.**
13. Update the application instance with the new form as described in Updating an Existing Application Instance with a New Form .

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 Oracle Identity Manager database. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, switch to the *OIM_HOME*/server/bin directory.

> **Note:**
>
> You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:
>
> *OIM_HOME*/server/bin/*SCRIPT_FILE_NAME*

2. Enter 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
> ```

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`

Enabling Logging

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

This section contains the following topics:

- Log Levels and ODL Message Types
- Logger Names
- Enabling Logging in Oracle WebLogic Server

Log Levels and ODL Message Types

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:

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

- 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 2-4.

Table 2-4 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.

Logger Names

You can specify the following logger names for logging of information:

- Logger name for Identity Connector Framework (ICF) integration: `ORACLE.IAM.CONNECTORS.ICFCOMMON`
- Logger name for ICF connectors: `ORG.IDENTITYCONNECTORS`
- Logger name for PeopleSoft operations: `ORACLE.IAM.CONNECTORS.PSFT`

There are separate loggers for the PeopleSoft operations and the connector operations. The logger for the PeopleSoft operations uses Java-based logging and the logger name is `ORACLE.IAM.CONNECTORS.PSFT`. The logger for the connector operations uses org.identityconnectors.common.logging.Log and the logger name is `ORG.IDENTITYCONNECTORS.PEOPLESOFT`.

The logger name for the connector operations must include the package name of the connector for which you want to enable logging. For example, `ORG.IDENTITYCONNECTORS`, `ORG.IDENTITYCONNECTORS.PEOPLESOFT`, and `ORG.IDENTITYCONNECTORS.PEOPLESOFT.COMPINTFC` are valid logger names.

Enabling Logging in Oracle WebLogic Server

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="ORG.IDENTITYCONNECTORS.PEOPLESOFT.COMPINTFC"
level="[LOG_LEVEL]" useParentHandlers="false">
     <handler name="psft-um-handler"/>
     <handler name="console-handler"/>
   </logger>

<logger name="ORACLE.IAM.CONNECTORS.PSFT" 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 2-4 lists the supported message type and level combinations.

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

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

```
<log_handler name='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\oim_s
erver1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="ORG.IDENTITYCONNECTORS.PEOPLESOFT.COMPINTFC"
level="NOTIFICATION:1" useParentHandlers="false">
     <handler name="psft-um-handler"/>
     <handler name="console-handler"/>
   </logger>

<logger name="ORACLE.IAM.CONNECTORS.PSFT" 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.

> **Note:**
>
> The logging level for console-handler must be as fine as the level set in the loggers.For example, if the `NOTIFICATION:1` level is specified in the `ORACLE.IAM.CONNECTORS.PSFT` logger, and the console-handler has `ERROR:1` level, then only logs at `ERROR:1` or coarser levels would be available.

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.

Setting Up the Lookup Definitions for Exclusion Lists

In the Lookup.PSFT.UM.Prov.ExclusionList and Lookup.PSFT.UM.Recon.ExclusionList lookup definitions, enter the user IDs of target system accounts for which you do not want to perform provisioning and reconciliation operations, respectively. See Lookup Definitions for Exclusion Lists for information about the format of the entries in these lookups.

To add entries in the lookup for exclusions during provisioning operations:

> **Note:**
>
> To specify user IDs to be excluded during reconciliation operations, add entries in the Lookup.PSFT.UM.Recon.ExclusionList lookup.

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the **Lookup.PSFT.UM.Prov.ExclusionList** lookup definition.
3. Click **Add.**
4. In the Code Key and Decode columns, enter the first user ID to exclude.

   > **Note:**
   >
   > The Code Key represents the resource object field name on which the exclusion list is applied during provisioning operations.

5. Repeat Steps 3 and 4 for the remaining user IDs to exclude.

   For example, if you do not want to provision users with user IDs User001, User002, and User088 then you must populate the lookup definition with the following values:

Code Key	Decode
User ID	User001
User ID	User002
User ID	User088

You can also perform pattern matching to exclude user accounts. You can specify regular expressions supported by the representation in the `java.util.regex.Pattern` class.

> **See Also:**
>
> For information about the supported patterns, visit `http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html`

For example, if you do not want to provision users matching any of the user IDs User001, User002, and User088, then you must populate the lookup definition with the following values:

Code Key	Decode
User ID[PATTERN]	User001|User002|User088

If you do not want to provision users whose user IDs start with 00012, then you must populate the lookup definition with the following values:

Code Key	Decode
User ID[PATTERN]	00012*

6. Click the save icon.

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 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.

Setting Up the Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping Lookup Definition for PeopleTools 8.52

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

Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping for more information about this lookup definition.

By default, the this lookup definition has the following entries:

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

If you are using PeopleTools 8.52, modify the Decode value in this 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.DeleteUserProfile.AttributeMapping lookup definition.
3. In the Decode column for the **User ID** Code Key, enter the following value.

   EMPLID~PER_ORG_ASGN~None~None~PRIMARY
4. Click the **Save** icon.

Setting Up the Lookup.PSFT.Configuration Lookup Definition

You can configure the message names, such as USER_PROFILE and DELETE_USER_PROFILE, defined in the Lookup.PSFT.Configuration lookup definition.

This section contains the following topics:

- About Setting Up the Lookup.PSFT.Configuration Lookup Definition
- Setting the Code Key Value

About 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 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.VERSION_84

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.

You must map the **xmlMapping** lookup with the path to the PeopleSoft Component Interface map definition file, PeopleSoftComponentInterfaces.xml. By default, the PeopleSoftComponentInterfaces.xml file is located in the xml directory of the connector package.

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.

Setting the Code Key Value

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.

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

By default, this connector uses the Identity Connector Framework (ICF) connection pooling.

This section contains the following topics:

- Connection Pooling Properties
- Modifying the Connection Pooling Properties

Connection Pooling Properties

Table 2-5 lists the connection pooling properties, their description, and default values set in ICF.

Table 2-5 Connection Pooling Properties

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

Modifying the Connection Pooling Properties

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

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

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

Enabling Request-Based Provisioning

> **Note:**
>
> This procedure is only applicable to Oracle Identity Manager releases prior to release 11.1.2. Do *not* enable request-based provisioning if you want to use the direct provisioning feature of the connector.

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

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.
- Direct provisioning cannot be used if you enable request-based provisioning.

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

- Copying Predefined Request Datasets
- Importing Request Datasets into MDS
- Enabling the Auto Save Form Feature
- Running the PurgeCache Utility

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 dataset directory on the installation media:

- ModifyProvisionedResource_PeoplesoftUser.xml
- ProvisionResource_PeoplesoftUser.xml

Copy the files from the dataset 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 Validating Request Data in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about modifying request datasets.

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 Migrating User Modifiable Metadata Files in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.
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.

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.

Running the PurgeCache Utility

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

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

Localizing Field Labels in UI Forms

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

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

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.

5. Extract the contents of the archive, and open one of the following files in a text editor:
   - For Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and later:

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

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

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

   b. Replace with the following text:

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

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

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

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

      ```
      <trans-unit id="$
      {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_PSF
      T_BAS_LANGUAGE_CD__c_description']}">
      <source>Language Code</source>
      </target>
      </trans-unit>
      <trans-unit
      id="sessiondef.oracle.iam.ui.runtime.form.model.PSFTUM.entity.PSFTUMEO.UD_PSFT_
      BAS_LANGUAGE_CD__c_LABEL">
      <source>Language Code</source>
      </target>
      </trans-unit>
      ```

   d. Open the resource file from the connector package, for example PSFT-UM_fr.properties, and get the value of the attribute from the file, for example, global.udf.UD_PSFT_BAS_LANGUAGE_CD= Code de langue.
   e. Replace the original code shown in Step 6.c with the following:

      ```
      <trans-unit id="$
      {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_PSF
      T_BAS_LANGUAGE_CD__c_description']}">
      <source> Language Code</source>
      <target> Code de langue</target>
      </trans-unit>
      <trans-unit
      id="sessiondef.oracle.iam.ui.runtime.form.model.PSFTUM.entity.PSFTUMEO.UD_PSFT_
      BAS_LANGUAGE_CD__c_LABEL">
      ```

```
<source> Language Code</source>
<target> Code de langue</target>
</trans-unit>
```

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

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

   Sample file name: BizEditorBundle_fr.xlf.

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

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

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

Configuring SSL for Oracle Identity Manager

The following sections describe the procedure to configure SSL connectivity between Oracle Identity Manager and the target system:

- Configuring SSL on IBM WebSphere Application Server
- Configuring SSL on Oracle WebLogic Server

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
- Receiving a Signed Certificate Issued By a CA

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.

Receiving a Signed Certificate Issued By a CA

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.

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:**
>
> Setting Up SSL on Oracle WebLogic Server

- Configuring SSL on Oracle WebLogic Server with a Signed Certificate
- Configuring SSL on Oracle WebLogic Server with a CA Certificate

Configuring SSL on Oracle WebLogic Server with a Signed Certificate

To configure SSL connectivity between Oracle Identity Manager on Oracle WebLogic Server and the target system with a self-signed certificate:

To generate the keystore:

1. Generate the keystore. To do so:
   a. 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.

   b. 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.

c. 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
```

d. When prompted for the private key password, enter the same password used for the keystore, for example, `example1234`.

e. 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.

2. After generating and importing the keystore, start Oracle WebLogic Server. To configure Oracle WebLogic Server, 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.

3. Click the **Keystore & SSL** tab, and then click **Change.**

4. From the Keystores list, select **Custom identity And Java Standard Trust,** and then click **Continue.**

5. 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 this procedure, 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.**

6. Specify the private key alias, pass phrase and the confirm pass phrase as the keystore password. Click **Continue.**

7. Click **Finish.**

8. 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:

> **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.

1. The connector requires Certificate Services to be running on the host computer. To generate the keystore:

a. 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.

b. 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.

c. 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.

d. Get the certificate from a CA by using the certificate request generated in the previous step, and store the certificate in a file.

e. 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
```

f. 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.

2. After creating and importing the keystore to the system, start Oracle WebLogic Server. To configure Oracle WebLogic Server, 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.
3. Click the **Keystore & SSL** tab, and click the **Change** link.
4. From the Keystores list, select **Custom Identity And Custom Trust,** and then click **Continue.**
5. 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 this procedure, 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 this procedure, 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.**
6. Specify the alias name and private key password. Click **Continue.**
7. Click **Finish.**

8. 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 SoD on Oracle Identity Manager

This section discusses the following procedures for configuring SoD on Oracle Identity Manager release 11.1.1.3 BP02:

- Updating OAACG IT Resource Instance
- The TopologyName IT Resource Parameter
- Specifying a Value for the TopologyName IT Resource Parameter
- Disabling SoD
- Enabling SoD

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 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.

Table 2-6 (Cont.) OAACG Environment Values

Field Name	Sample Value	Description
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.**

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. If you are using default SIL registration, then specify `oaacgpsft` as the value of the topologyName parameter.

See Configuring the IT Resource section for information about specifying values for parameters of the IT resource.

Specifying a Value for the TopologyName IT Resource Parameter

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 User" IT resource or open any IT resource, which you have configured for PeopleSoft User Management Connector.
5. In the Topology Name attribute, enter **oaacgpsft**.
6. Click **Save**.

Disabling SoD

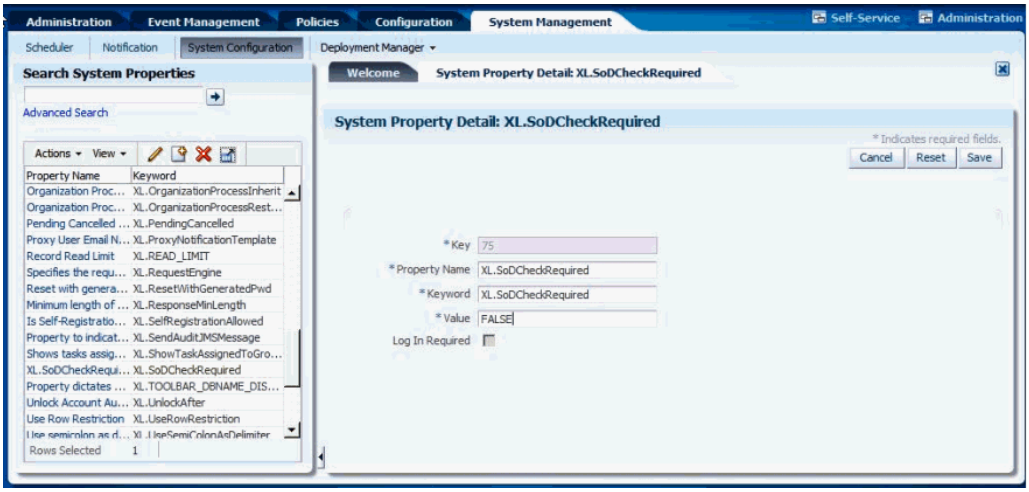
To disable SoD:

> **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 2-1 shows the details of disabling SoD.

Figure 2-1 Disable SoD



Enabling SoD

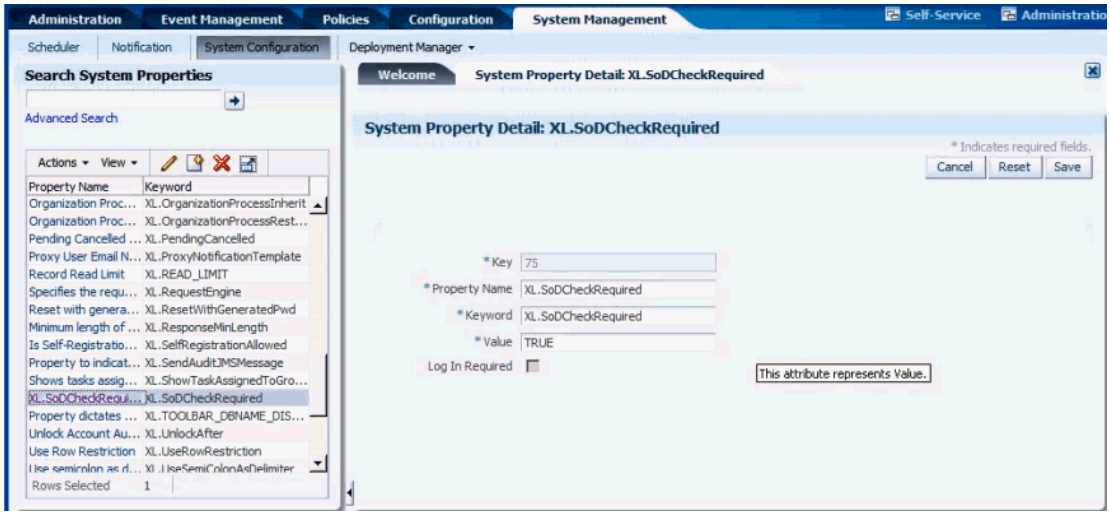
To enable SoD:

> **Note:**
>
> If you are enabling SoD for the first time, then see Enabling and Disabling SoD in *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 2-2 shows the details of enabling SoD.

Figure 2-2 Enable SoD



Configuring the Target System

Postinstallation on the target system involves 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 Configuring SSL for Oracle Identity Manager.

   > **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.

Creating the IT Resource for the Connector Server

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

This section contains the following topics:

- Creating the IT Resource
- IT Resource Parameters

> **Note:**
>
> Before you deploy the connector bundle remotely in a Connector Server, you must deploy the connector in Oracle Identity Manager by performing the procedures described in Installation.

Creating the IT Resource

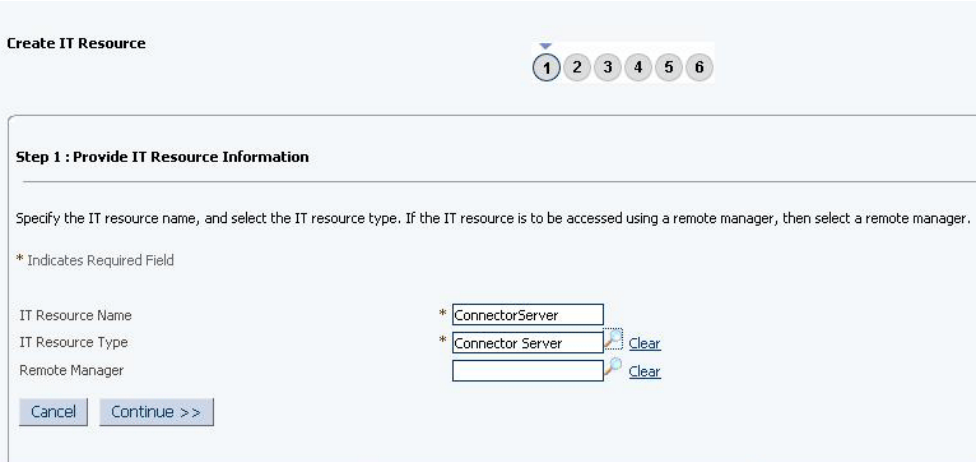
To create the IT resource for the Connector Server:

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

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

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

Figure 2-3 Step 1: Provide IT Resource Information



6. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. Figure 2-4 shows the Step 2: Specify IT Resource Parameter Values page.

Figure 2-4 Step 2: Specify IT Resource Parameter Values

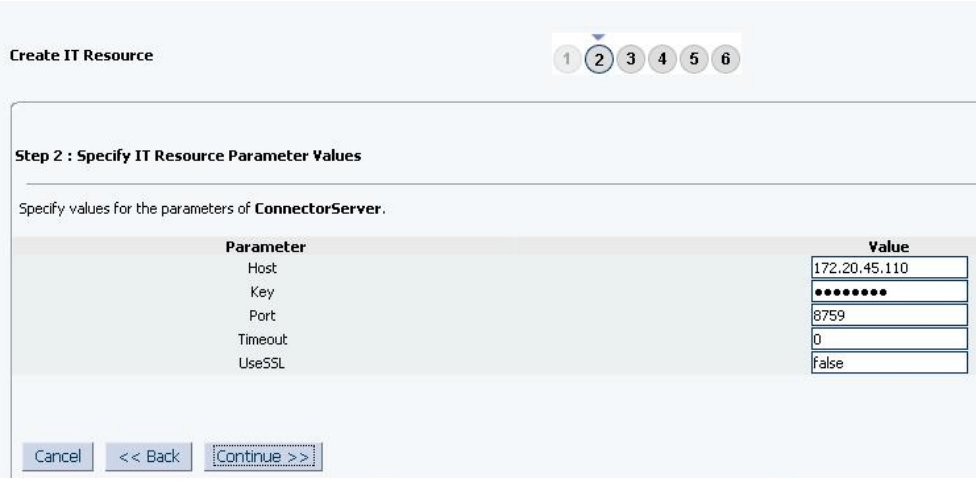


Table 2-7 provides information about the parameters of the IT resource.

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

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

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

a. Click **Assign Group**.

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

c. Click **Assign**.

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

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

a. Click **Update Permissions**.

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

c. Click **Update**.

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

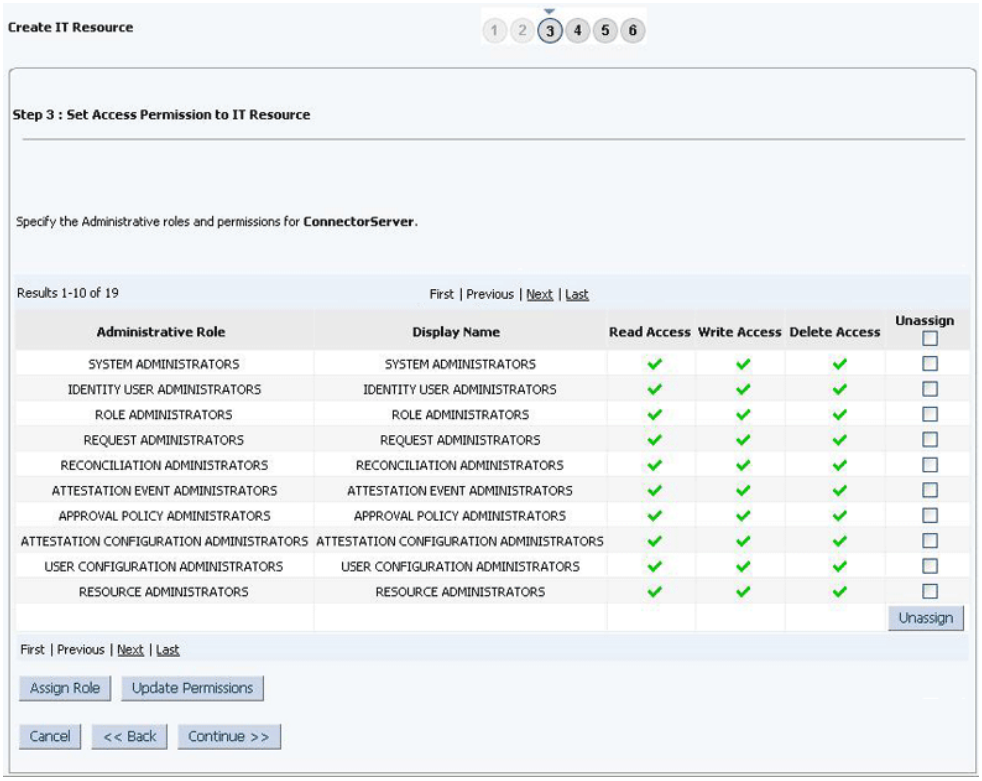
> **Note:**
>
> - This step is optional.
> - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

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

b. Click **Unassign.**

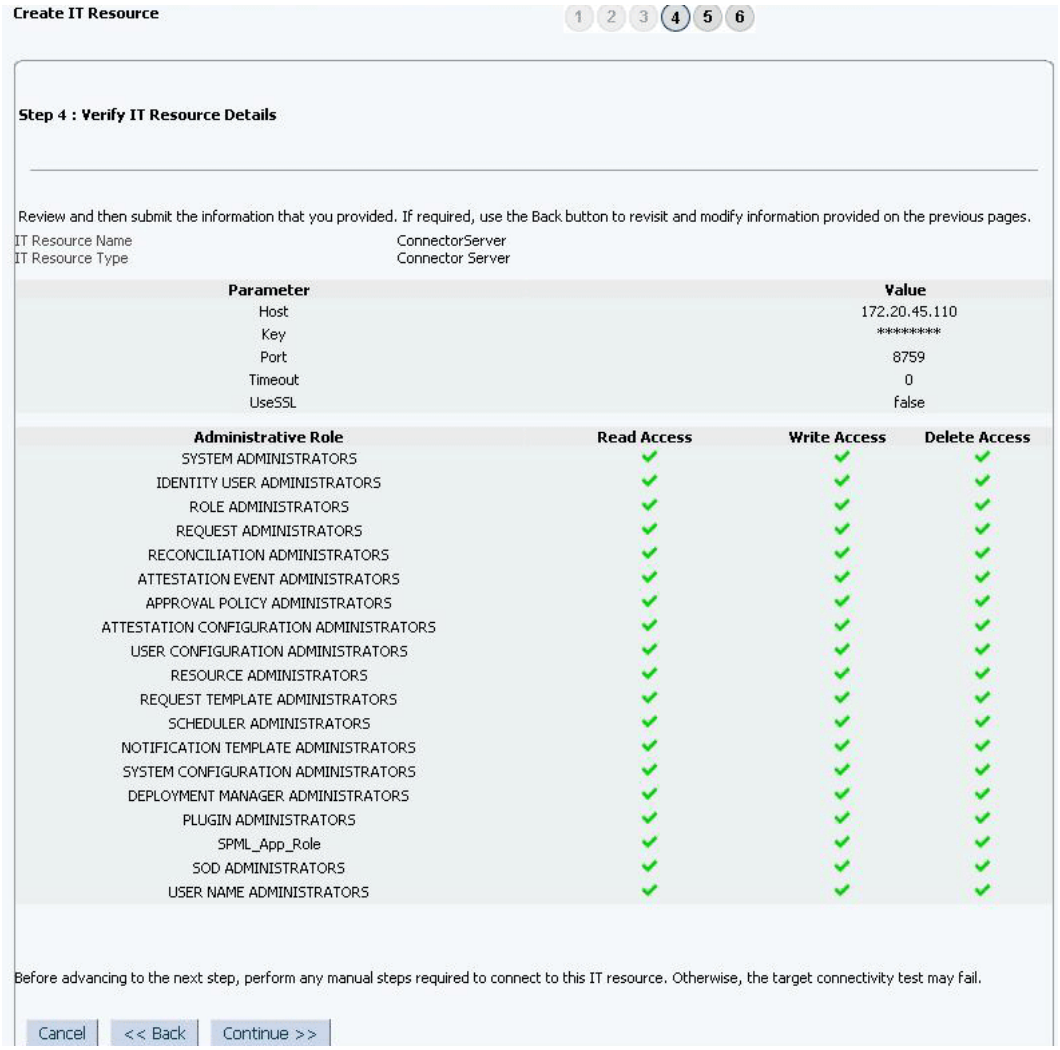
10. Click **Continue**. Figure 2-5 shows the Step 3: Set Access Permission to IT Resource page.

Figure 2-5 Step 3: Set Access Permission to IT Resource



11. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.
12. To proceed with the creation of the IT resource, click **Continue**. Figure 2-6 shows Step 4: Verify IT Resource Details page.

Figure 2-6 Step 4: Verify IT Resource Details

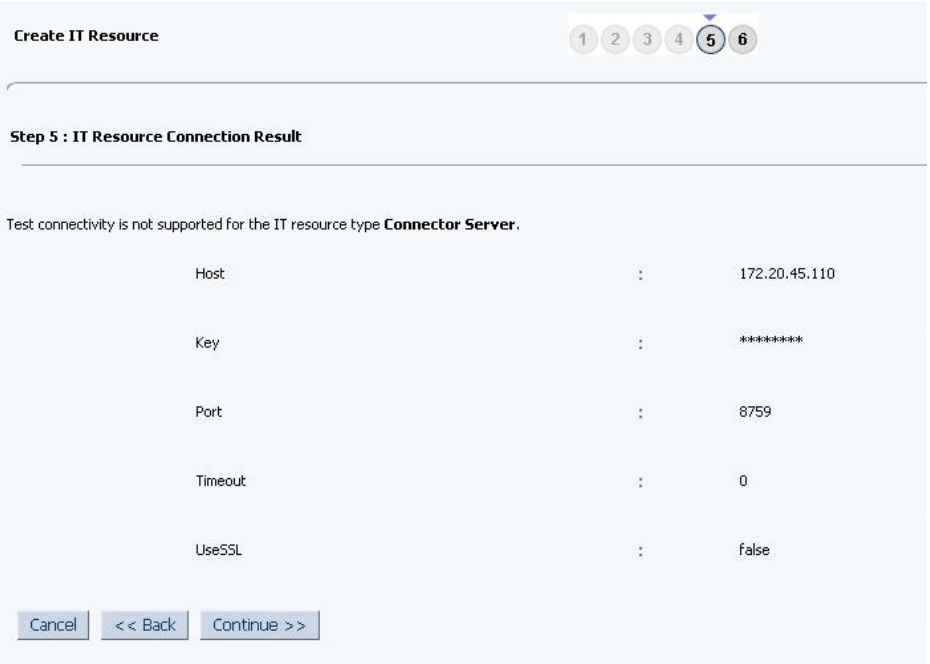


13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:

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

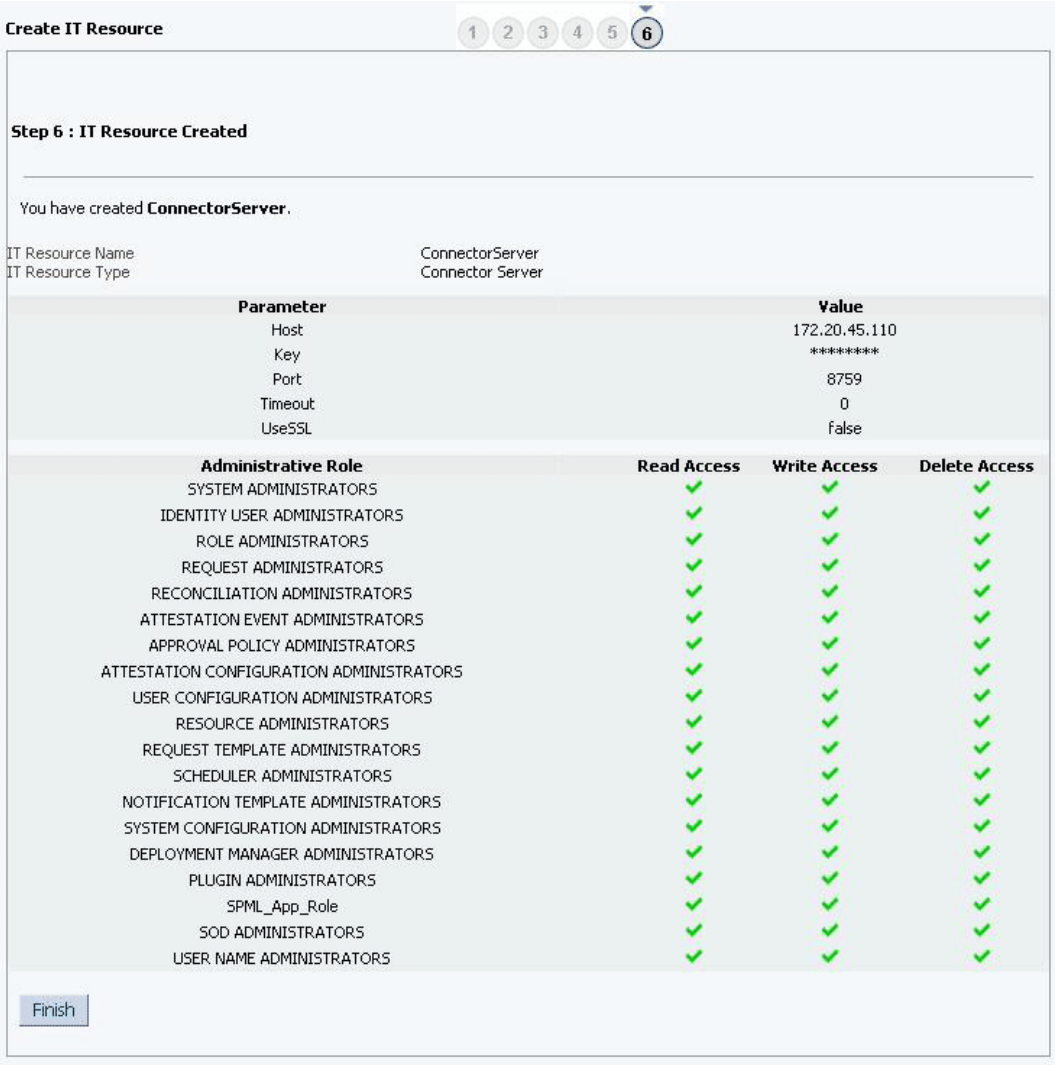
    Figure 2-7 shows the Step 5: IT Resource Connection Result page.

Figure 2-7 Step 5: IT Resource Connection Result



14. Click **Finish**. Figure 2-8 shows the IT Resource Created Page.

Figure 2-8 Step 6: IT Resource Created



IT Resource Parameters

Table 2-7 provides information about the parameters of the IT resource.

Table 2-7 Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: `RManager`
Key	Enter the key for the Java connector server.
Port	Enter the number of the port at which the connector server is listening. Default value: `8759`

Table 2-7 (Cont.) Parameters of the IT Resource for the Connector Server

Parameter	Description
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: `300` **Note:** A value of 0 (zero) indicates unlimited timeout.
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter `false`. Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, run the connector server by using the /setKey [*key*] option. The value of this key must be specified as the value of the Key IT resource parameter of the connector server.

Upgrading the Connector

You can upgrade the PeopleSoft User Management connector while in production, and with no downtime. Your customizations will remain intact and the upgrade should be transparent to your users. Form field names are preserved from the legacy connector.

To upgrade the PeopleSoft User Management connector, perform the steps listed in Prerequisites for Upgrading the Connector.

Then, perform one of the following procedures depending on the version of the existing connector:

- Upgrade the Connector from Release 11.1.1.5.0
- Upgrade the Connector from Release 9.1.1.6

> **See Also:**
>
> Upgrading Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information of these steps

Prerequisites for Upgrading the Connector

Before you perform the upgrade procedures:

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

You might encounter the following issue during or after performing the upgrade procedures:

- After the upgrade process, an additional IT resource is created with the name PSFT User, in addition to converting existing IT resources. The additional IT resource is created because the default IT resource name has been changed.

  As a workaround, if the additional IT resource is unused, you can delete it.

Upgrade the Connector from Release 11.1.1.5.0

To upgrade the PeopleSoft User Management connector from release 11.1.1.5.0 to this release of the connector, perform the following steps:

1. Set entitlement tagging for PeopleSoft child form (UD_PSROLES) as follows:
   a. Log in to the Oracle Identity Manager Design Console.
   b. Expand **Development Tools** and then double-click **Form Designer.**
   c. Enter the name of the PeopleSoft Roles child form, `UD_PSROLES`, 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. Click the **Properties** tab.
   h. Select the Role Name field, and click **Add Property.**
   i. From the Property Name list, select **Entitlement.**
   j. In the Property Value field, enter `true`.
   k. Click **Make Version Active.**
2. Set IT resource, Account ID, and Account Name tagging in the process form (UD_PSFT_BAS) as follows:
   a. In the Oracle Identity Manager Design Console, expand **Development Tools** and then double-click **Form Designer.**
   b. Enter the name of the PeopleSoft parent form, `UD_PSFT_BAS`, in the Table Name field and click the **Query for records** button.
   c. Click **Create New Version.**
   d. 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.
   e. From the **Current Version** list, select the newly created version.
   f. Click the **Properties** tab.
   g. Select the Server (IT resource) field, and click **Add Property.**
   h. From the Property Name list, select **ITResource.**
   i. In the Property Value field, enter `true`.
   j. Select the User Id field, and click **Add Property.**
   k. From the Property Name list, select **AccountName.**
   l. In the Property Value field, enter `true`.
   m. Select the User Id field, and click **Add Property.**

n. From the Property Name list, select **AccountID.**

o. In the Property Value field, enter `true`.

p. Update the parent form to add the child form created in Step 1.

q. Click **Make Version Active.**

r. Recreate the form in the user interface (UI) and update the application instance with the new form as described in Updating an Existing Application Instance with a New Form .

3. Set the status of Task to Object Status Mapping of the Role Updated process task to None as follows:

a. In the Oracle Identity Manager Design Console, expand **Process Management** and then double-click **Process definition.**

b. In the Name field, enter `Peoplesoft User Management` and then click the **Query for records** button.

c. Under Tasks, open the **Role Updated** task.

d. In the Task to Object Status Mapping tab, change the object status of status C from Provisioned to `None`.

e. Repeat Steps 3.c and 3.d for the Email Updated task.

4. Update the bundle in the Oracle Identity Manager database with the latest bundle JAR from this release as described in Upgrading the Connector Files and External Code Files.

Upgrade the Connector from Release 9.1.1.6

To upgrade the PeopleSoft User Management connector from release 9.1.1.6 to this release of the connector, perform the following procedures:

- Running the Upgrade Wizard
- Upgrading the Connector Files and External Code Files
- Upgrading the Configurations
- Upgrading the Customizations
- Upgrading the PeopleSoft Listener
- Migrating the Form Data
- Updating the PeopleSoft Target System
- Compiling the Adapters

Running the Upgrade Wizard

To upgrade the connector in wizard mode:

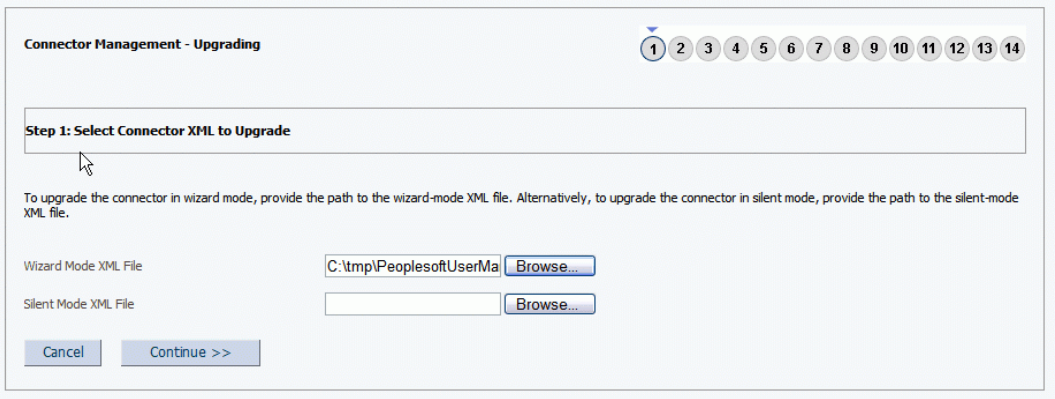
1. Create a copy of the following XML file in a temporary directory, for example, `c:\tmp`:

   OIM_HOME/server/ConnectorDefaultDirectory/PSFT_UM-11.1.1.6.0/xml/PeoplesoftUserManagement-ConnectorConfig.xml

The PeoplesoftUserManagement-ConnectorConfig.xml file contains definitions for the connector components. See Files and Directories on the Installation Media for more information.

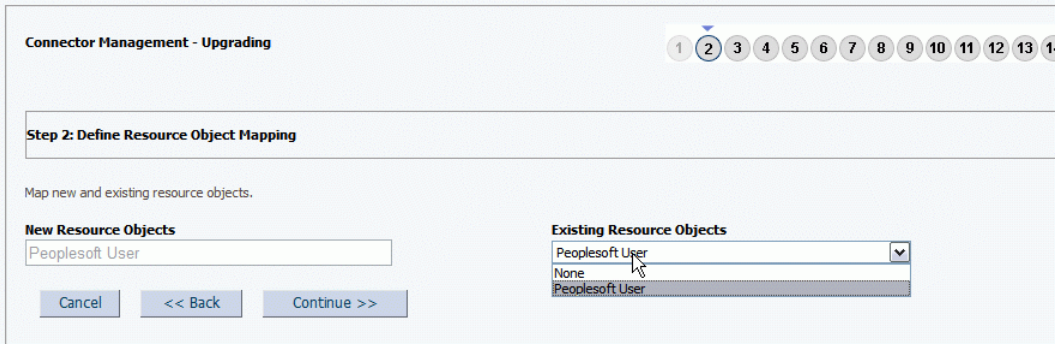
2. Log in to the Administrative and User Console.
3. On the Welcome to Identity Manager Advanced Administration page, under the System Management section, click **Manage Connector.**
4. Search for the Peoplesoft User Management connector and click the upgrade icon.
5. In the Step 1: Select Connector XML to Upgrade dialog, click **Browse** and provide the path to the Wizard mode XML file, which is the PeoplesoftUserManagement-ConnectorConfig.xml file created in Step 1.

   For example, `c:\tmp\PeoplesoftUserManagement-ConnectorConfig.xml`

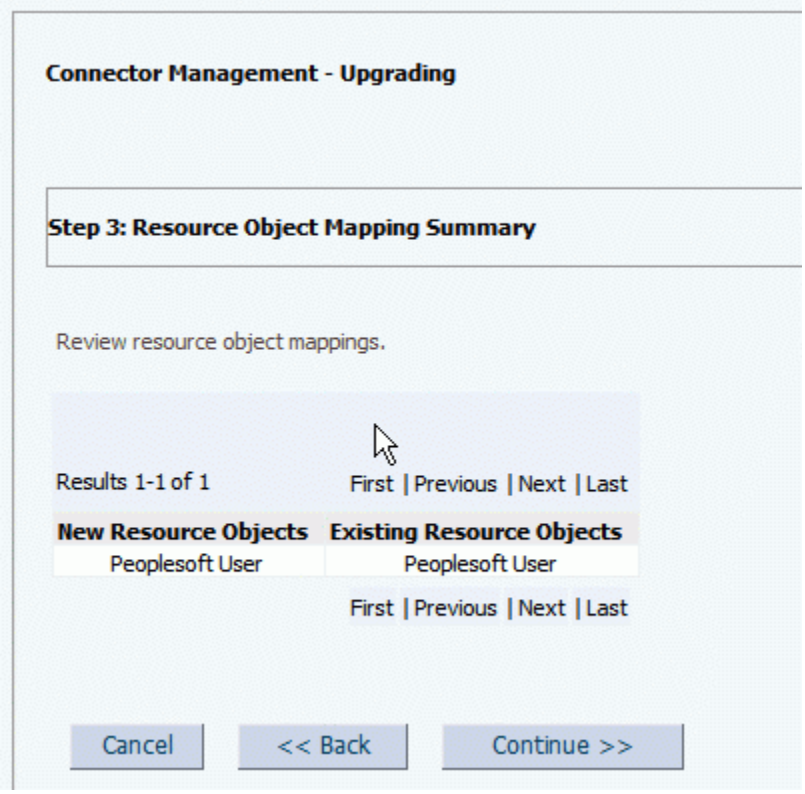


Then, click **Continue.**

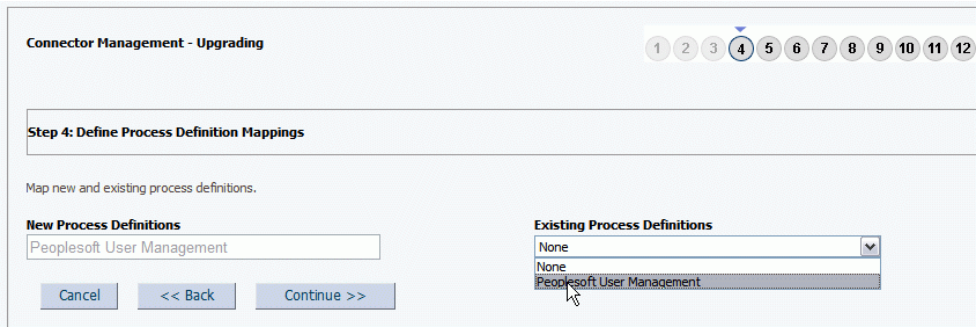
6. In the Step 2: Define Resource Object Mapping dialog, map the new and existing resource objects, as shown in the following sample screenshot. Then, click **Continue.**



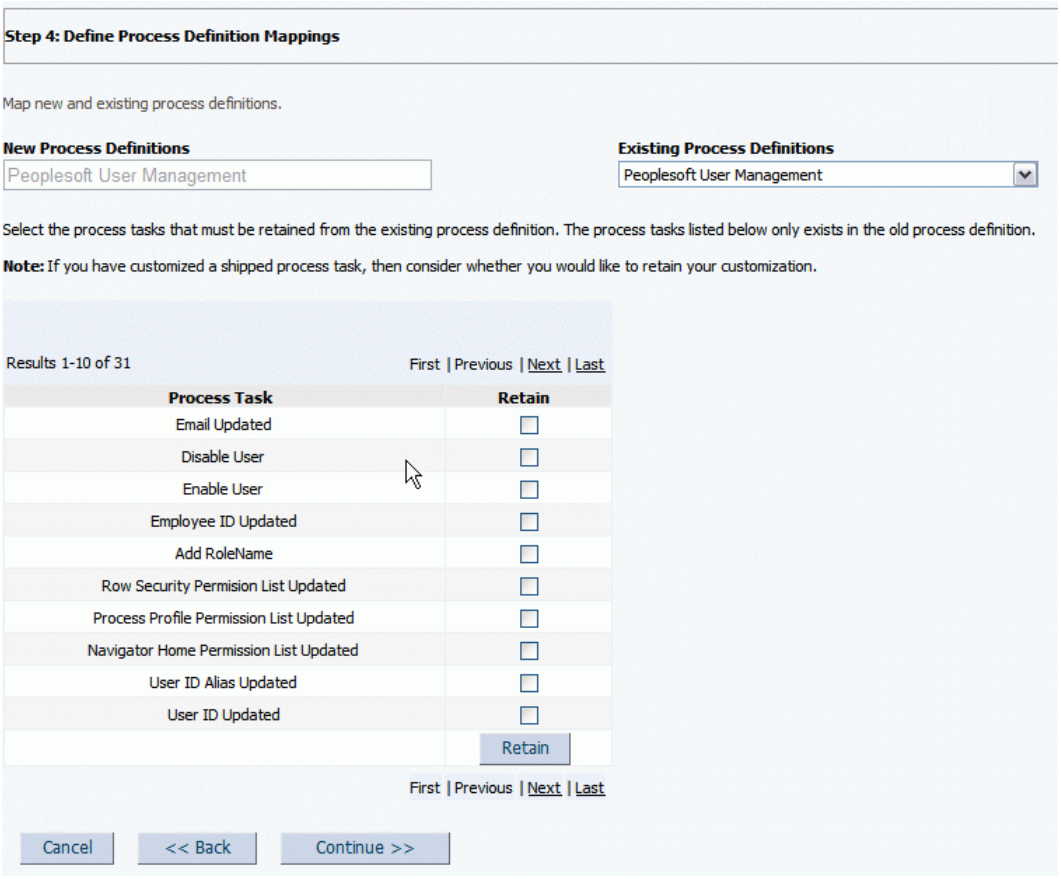
7. In the Step 3: Resource Object Mapping Summary dialog, verify the mapping summary of the new and existing resource objects, and click **Continue.**



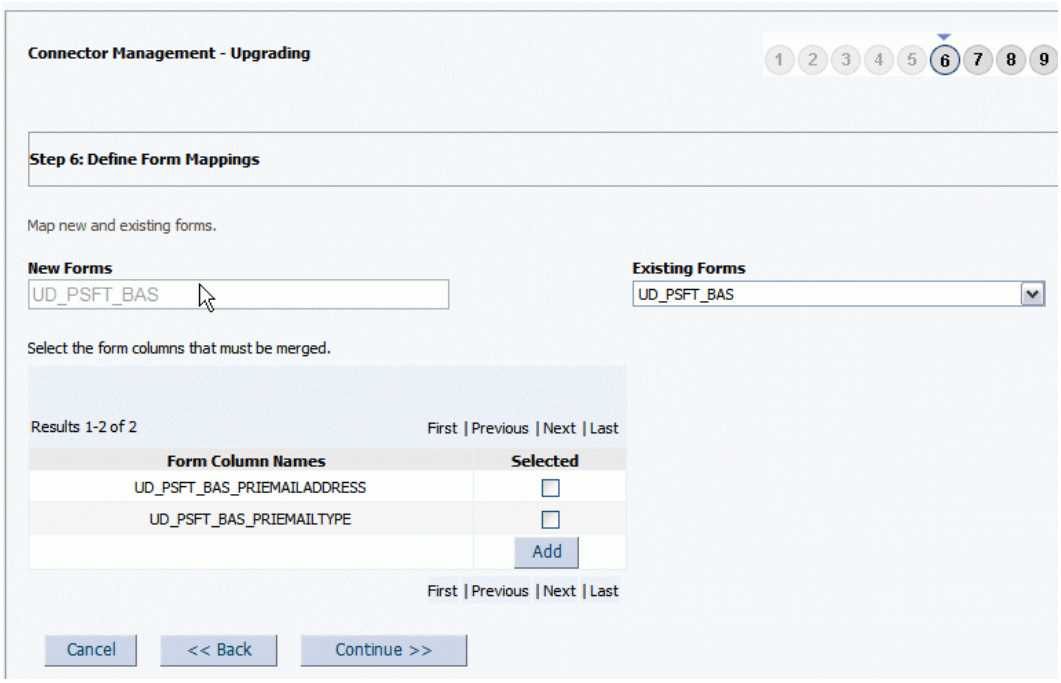
8. In the Step 4: Define Process Definition Mappings dialog, map the new and existing process definitions, as shown in the following sample screenshots.

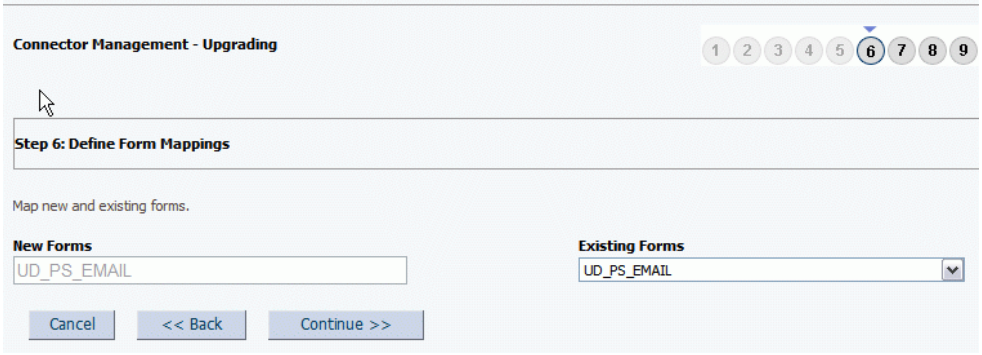


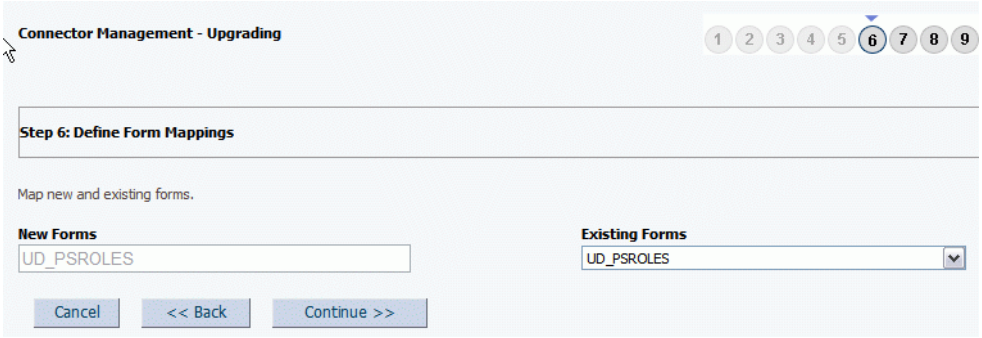
Select the process tasks that you want to retain from the existing process definitions. Then, click **Continue.**



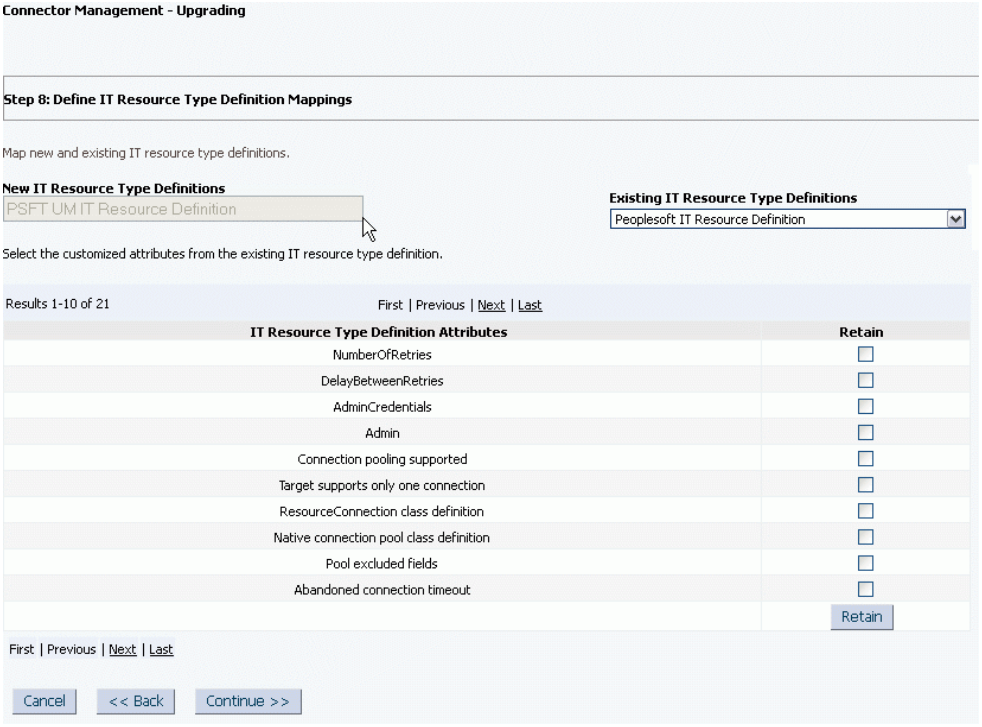
9. In the Step 5: Process Definition Mapping Summary dialog, verify the mapping summary of the new and existing process definitions, and click **Continue.**
10. In the Step 6: Define Form Mappings dialog, map the new and existing forms, as shown in the following sample screenshots. Then, click **Continue.**

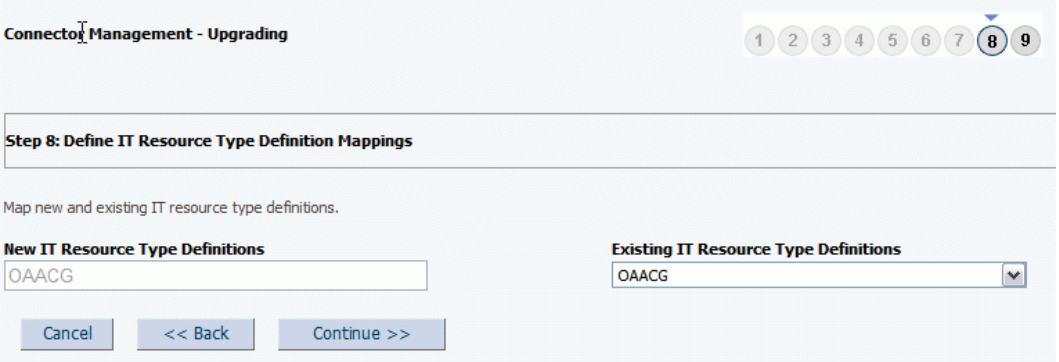




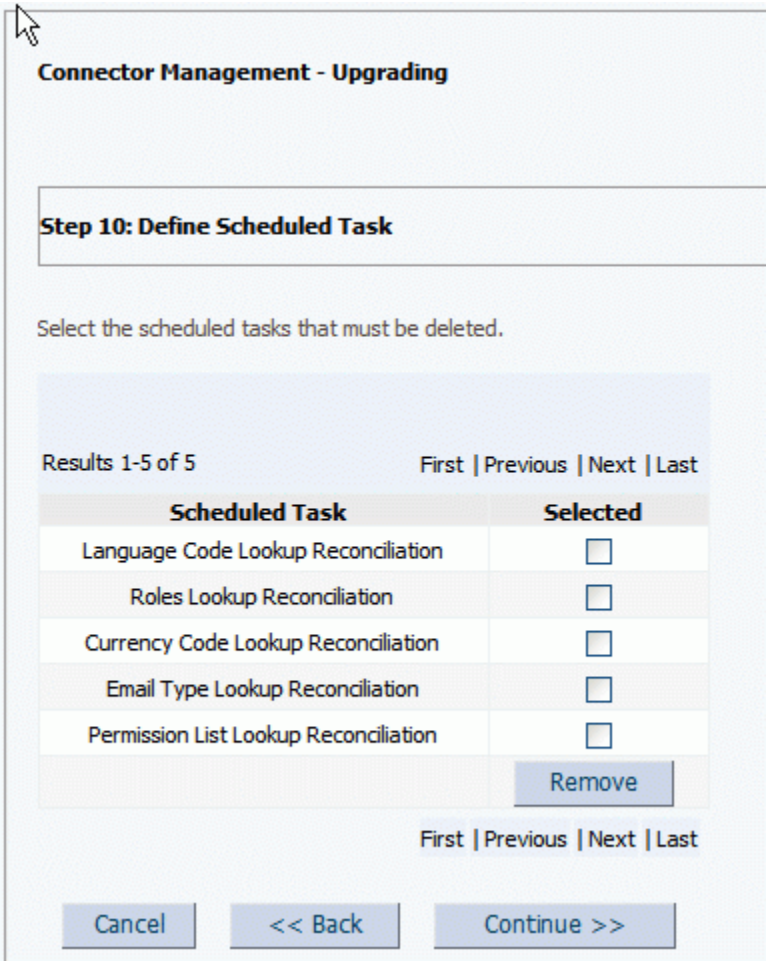


11. In the Step 7: Form Mapping Summary dialog, verify the mapping summary of the new and existing forms, and click **Continue.**
12. In the Step 8: Define IT Resource Type Definition Mappings dialog, map the new and existing IT resource type definitions, as shown in the following sample screenshots. Then, click **Continue.**

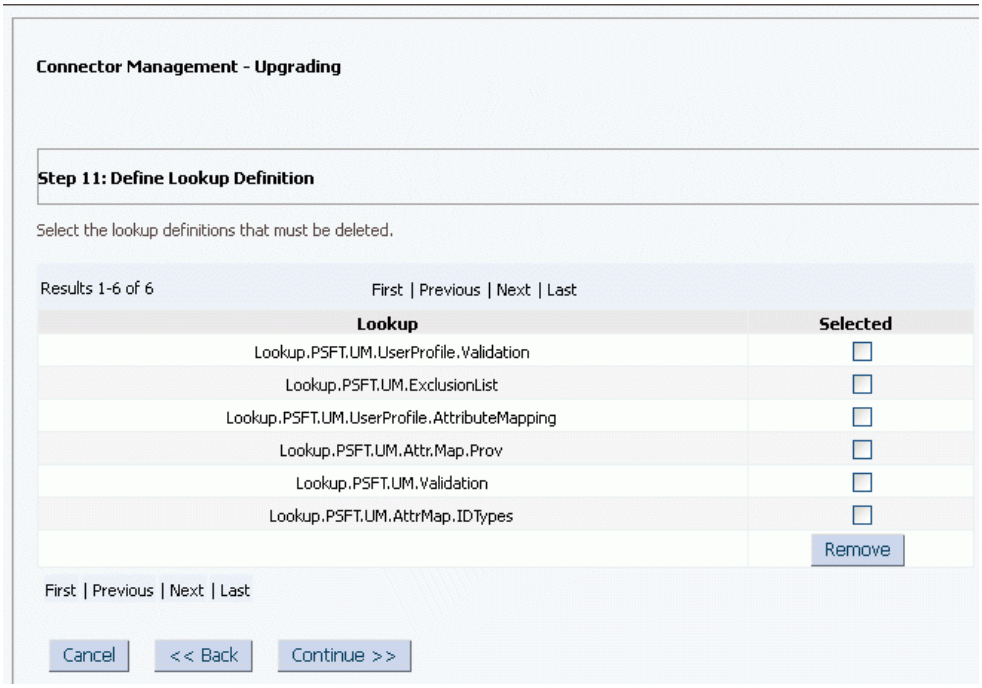




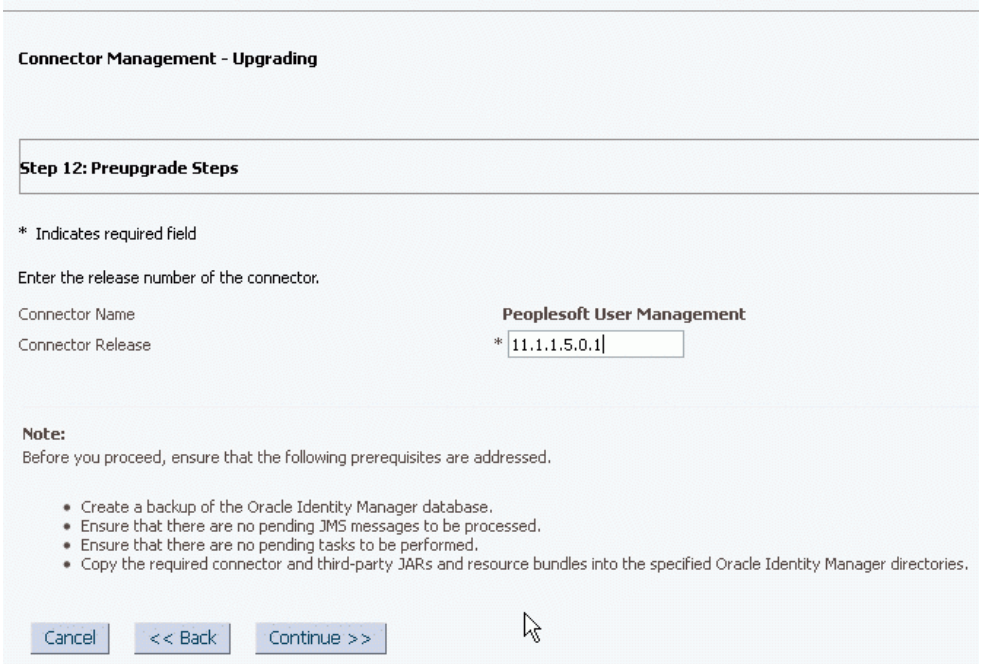
13. In the Step 9: IT Resource Type Definition Mapping Summary dialog, verify the mapping summary of the new and existing IT resource type definitions, and click **Continue.**
14. In the Step 10: Define Scheduled Task dialog, select the scheduled tasks that must be deleted. Then, click **Continue.**



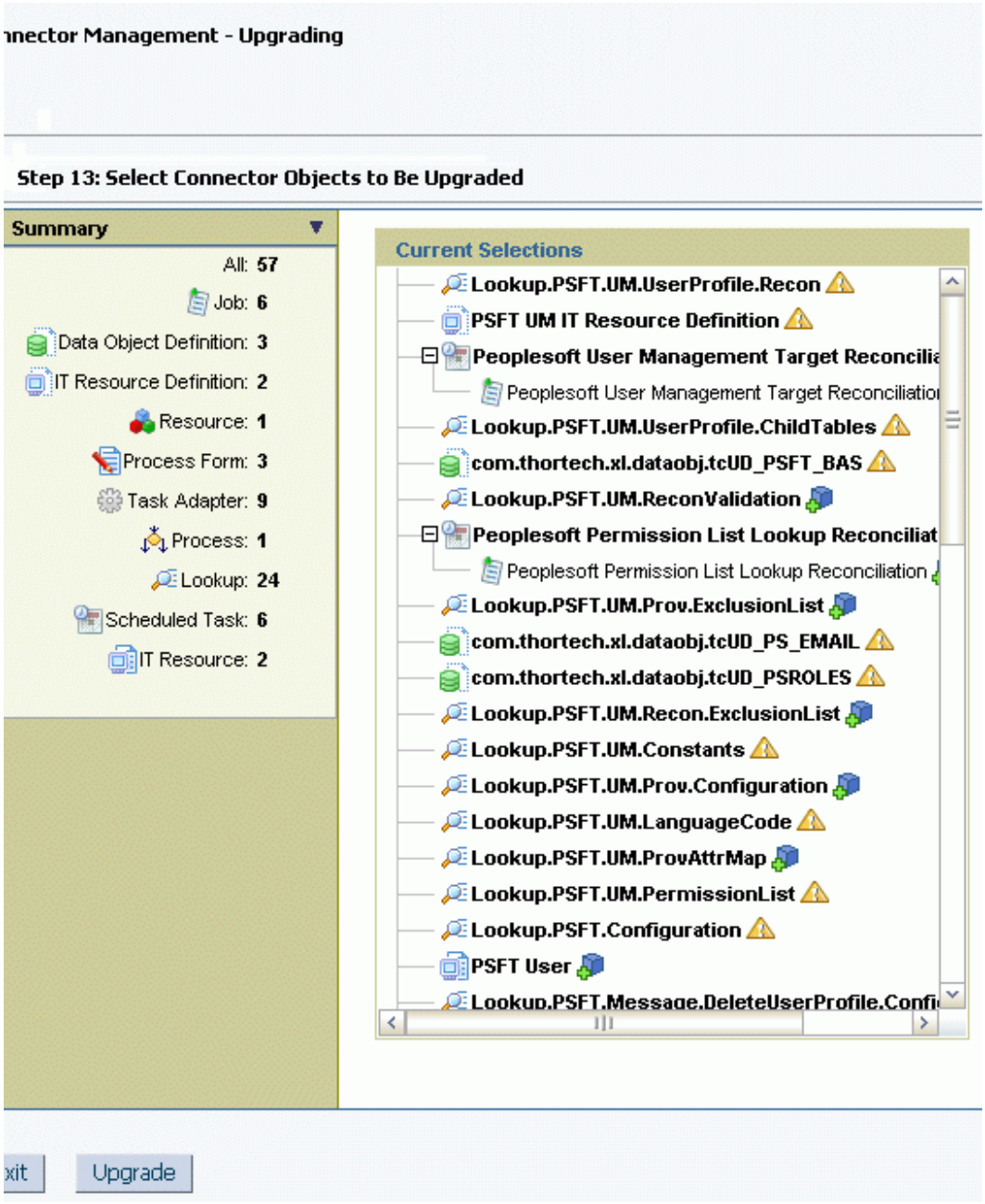
15. In the Step 11: Define Lookup Definition dialog, select the lookup definitions that must be deleted. Then, click **Continue.**



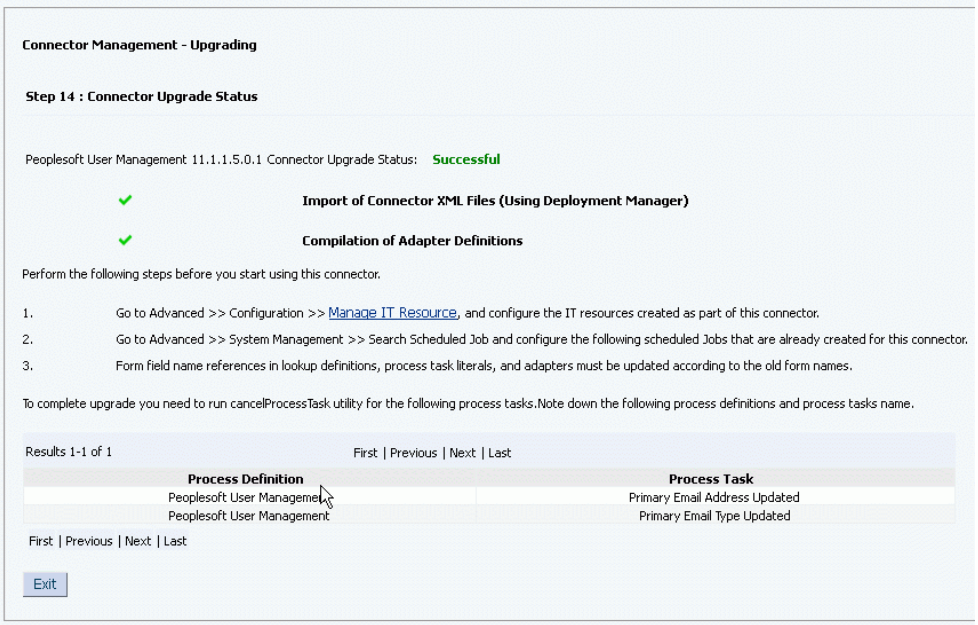
16. In the Step 12: Preupgrade Steps dialog, enter the release number of the connector. Verify and ensure the prerequisites are addressed as per the Note section. Then, click **Continue.**



17. In the Step 13: Select Connector Objects to be Upgraded dialog, ensure there are no red cross-shaped icons in the Current Selections section. Then, click **Upgrade.**



18. In the Step 14: Connector Upgrade Status dialog, verify the upgrade status. Perform the specified steps before using the connector and to complete the upgrade process, as shown in the following sample screenshot. Then, click **Exit.**



Upgrading the Connector Files and External Code Files

To upgrade the connector files and external code files:

1. Run the Oracle Identity Manager Delete JARs utility to delete the JAR files from the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

> **Note:**
>
> Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

- For Microsoft Windows:

  OIM_HOME/server/bin/DeleteJars.bat

- For UNIX:

  OIM_HOME/server/bin/DeleteJars.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 files being deleted, and the location from which the JAR files are to be deleted.

Select the JAR files and indicate the JAR types as specified in the following table:

JAR File Name	JAR Type
PSFTUM.jar	1 - JavaTasks
PSFTCommon.jar	1 - JavaTasks
CustomClassLoader.jar	1 - JavaTasks

JAR File Name	JAR Type
Common.jar Select this JAR file only if no other connector is using it.	1 - JavaTasks
psjoa.jar	3 - ThirdParty
peoplesoft.jar	3 - ThirdParty

> **See Also:**
>
> Delete JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Delete JARs utility

2. Patch the psjoa.jar file in the connector bundle as follows:

   a. Open the command prompt and navigate to the bundle JAR file.

      For example:

      ```
      cd PSFT_UM-11.1.1.6.0/bundle bundle/
      org.identityconnectors.peoplesoftintfc-1.0.5963.jar
      ```

   b. Run the following command to create a lib directory.

      ```
      mkdir lib
      ```

   c. Copy the **psjoa.jar** file (target specific) from the *PEOPLESOFT_HOME*/web/psjoa directory to the new lib directory.

      For example:

      ```
      cp psjoa/psjoa.jar lib
      ```

   d. Run the following command:

      ```
      jar -uvf org.identityconnectors.peoplesoftintfc-1.0.5963.jar lib/psjoa.jar
      ```

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

   - 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 files being uploaded, and the location from which the JAR files are to be uploaded.

   Select the JAR files and indicate the JAR types as specified in the following table:

JAR File Name	JAR Type
bundle/org.identityconnectors.peoplesoftintfc-1.0.5963.jar	4 - ICFBundle
lib/PSFTCommon.jar	1 - JavaTasks

JAR File Name	JAR Type
lib/PSFT_UM-oim-integration.jar	1 - JavaTasks

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

Upgrading the Configurations

To upgrade the connector configurations:

1. Update the IT resource with connection parameters.

   The existing IT resources will be mapped to the new definitions. See Configuring the IT Resource for information about this step.

2. Configure PeopleSoft target system for multiple versions as per the Identity Connector Framework (ICF) conventions.

   See Configuring the Connector to Support Multiple Versions of the Target System for information about this step.

3. Update the xmlMapping entry in the Lookup.PSFT.Configuration lookup definition.

   See Setting Up the Lookup.PSFT.Configuration Lookup Definition for information about this step.

Upgrading the Customizations

To upgrade the connector customizations:

1. Update the validation customizations as follows:
   - Re-compile, package, and update the validation code in the Oracle Identity Manager database and in the PeopleSoft listener.

     Sample validation classes are available in Configuring Validation of Data During Reconciliation and Configuring Validation of Data During Provisioning.
   - Update the entries in the provisioning validation lookup, Lookup.PSFT.UM.ProvValidation.

     See Lookup.PSFT.UM.ProvValidation for information about this step.
   - Update the entries in the reconciliation validation lookup, Lookup.PSFT.UM.ReconValidation.

     See Lookup.PSFT.UM.ReconValidation for information about this step.
2. Update the transformation customizations as follows:
   - Re-compile, package, and update the transformation code in the Oracle Identity Manager database and in the PeopleSoft listener.

     Sample transformation class is available in Configuring Transformation of Data During Reconciliation.

- Update the entries in the reconciliation transformation lookup, Lookup.PSFT.UM.UserProfile.Transformation.

  See Lookup.PSFT.UM.UserProfile.Transformation for information about this step.

3. Update the resource exclusion customizations as follows:
   - Re-write the resource exclusion rules as per the Identity Connector Framework (ICF) conventions.

     For more information, see Configuring Resource Exclusion Lists in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
   - Update the entries in the provisioning exclusion list lookup, Lookup.PSFT.UM.Prov.ExclusionList.
   - Update the entries in the reconciliation exclusion list lookup, Lookup.PSFT.UM.Recon.ExclusionList.

   See Lookup Definitions for Exclusion Lists for information about the preceding steps.
4. Add custom provisioning and reconciliation attributes.

   If any custom provisioning and reconciliation attributes were added in the previous connector, add the same attributes in the new version of the connector.

   See Adding New Attributes for Provisioning and Adding New Attributes for Reconciliation for information about this step.
5. Add custom ID types.

   If any new ID types were added in addition to the default ID types, add the same ID types in the new version of the connector.

   See Adding New ID Types for Provisioning and Adding New ID Types for Reconciliation for information about this step.
6. If you are using Oracle Identity Manager release 11.1.2.*x* or later, you must create a new UI form and attach it to an existing application instance to view the user-defined fields (UDFs or custom attributes).

   For more information about UDFs, see Configuring Custom Attributes in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

Upgrading the PeopleSoft Listener

> **Note:**
>
> If you upgrade the connector, you must also upgrade the listener. Installing a new connector over a previously deployed listener creates discrepancies.

To upgrade the PeopleSoft listener:

1. Remove the existing PeopleSoft listener by performing the procedure described in Removing the PeopleSoft Listener.
2. Deploy the new PeopleSoft listener by performing the procedure described in Deploying the PeopleSoft Listener.

If there are any validation or transformation JARs, you must add the JARs to the deployable connector bundle JAR and re-deploy the listener. See Configuring Validation of Data During

Reconciliation, Configuring Transformation of Data During Reconciliation, and Configuring Validation of Data During Provisioning for more information.

Migrating the Form Data

The Form Version Control (FVC) utility is used to migrate data changes on a form after an upgrade operation.

> **Note:**
>
> After performing this procedure, you cannot revert the data changes.

To run the FVC utility:

1. In a text editor, open the fvc.properties file located in the *OIM_DC_HOME* directory and include the following entries:

```
ResourceObject;Peoplesoft User
FormName;UD_PSFT_BAS
FromVersion;9
ToVersion;v_11.1.1.6.0
ParentParent;UD_PSFT_BAS_OPRID;UD_PSFT_BAS_RETURN
ChildConstant;UD_PS_EMAIL;UD_PS_EMAIL_PRIMARYEMAIL;N
MultipleParentChild;UD_PSFT_BAS_PRIEMAILTYPE:UD_PS_EMAIL_EMAILTYPE;UD_PSFT_BA
S_PRIEMAILADDRESS:UD_PS_EMAIL_EMAILADDRESS;'Y':UD_PS_EMAIL_PRIMARYEMAIL
```

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

   - **For Microsoft Windows:**

     OIM_DC_HOME/fvcutil.bat

   - **For UNIX:**

     OIM_DC_HOME/fvcutil.sh

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

   > **Note:**
   >
   > If you encounter the following error in the debug logs, you can ignore it:
   >
   > ```
   > ERROR  [Exception Thor.API.Exceptions.tcAPIException: The following
   >  required fields have not been given values:Email Address : The
   >  following required fields have not been given values:Email Address
   >  : The following required fields have not been given values:Email
   >  Address : The following required fields have not been given
   >  values:Email Address - Updation of form data failed for
   >  user=RDRAVIDS, object instance key=12, proc instance key=18,
   >  form instance version=0
   > ```

Updating the PeopleSoft Target System

To update the PeopleSoft target system for the upgrade process:

1. Enable the Find and Get methods on the USER_PROFILE component interface. To do so:
   a. To open the PeopleSoft Application Designer, click **Start** and then select **Programs, Peoplesoft8.*x***, and **Application Designer.**
   b. On the Application Designer page, click **Open** from the **File** menu.
   c. In the Open Definition dialog box, select **Component Interface** from the **Definition** list.
   d. Enter `USER_PROFILE` in the **Name** field, and then click **Open.**

      All the component interfaces with names that start with `USER_PROFILE` are displayed in the Open Definition dialog box.
   e. Double-click the **USER_PROFILE** entry.
   f. Drag the **User ID** field from the USERMAINT definition and drop to the component interface definition on the right hand side, as shown in the following screenshot. This will set the Find and Get keys.
   g. Right-click on the USER_PROFILE component interface and click Component Interface Properties.
   h. In the Properties dialog, click the Standard Methods tab, and then select the **Get** check-box.
   i. Click **OK** and save the component interface.
2. Update the OIM_NODE node based on HTTP Connector. To do so:
   a. Open the OIM_NODE node that is configured for the PeopleSoft listener.
   b. Update the IT resource header type from Host to Location.

Compiling the Adapters

At the end of the upgrade process, you must compile every adapter that resides within the Oracle Identity Manager database.

To compile the adapters:

1. Log in to Oracle Identity Manager Design Console.
2. Expand Development Tools and double-click **Adapter Manager.**

   The Adapter Manager form is used to compile multiple adapters simultaneously.
3. Select the **Compile All** check box.
4. Click the **Start** button.

3
Using the Connector

This chapter contains the following sections:

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.

1. Configure and run the scheduled job to synchronize the lookup fields. See Configuring the Scheduled Jobs for Lookup Field Synchronization for more information.
2. Generate XML files for the USER_PROFILE message for all users. See Performing Full Reconciliation for more information.
3. Copy these XML files to a on the Oracle Identity Manager host computer.
4. Configure and run the PeopleSoft User Management Target Reconciliation scheduled job for the USER_PROFILE message. The XML files are read by this scheduled job to generate reconciliation events. See Configuring the Scheduled Job for User Data Reconciliation for more information.

Change from full reconciliation to incremental reconciliation. See Performing Incremental Reconciliation for instructions.

Configuring the Scheduled Jobs for Lookup Field Synchronization

When you run the Connector Installer, scheduled jobs for lookup field synchronization are automatically created in Oracle Identity Manager. These scheduled jobs are used to

synchronize the values of the lookup fields between the target system and Oracle Identity Manager.

This section contains the following topics:

- Scheduled Jobs for Lookup Field Reconciliation
- Scheduled Job Attributes

Scheduled Jobs for Lookup Field Reconciliation

When you run the Connector Installer, the following scheduled jobs for lookup field synchronization are automatically created in Oracle Identity Manager:

- Peoplesoft Currency Code Lookup Reconciliation
- Peoplesoft Email Type Lookup Reconciliation
- Peoplesoft Language Code Lookup Reconciliation
- Peoplesoft Permission List Lookup Reconciliation
- Peoplesoft Roles Lookup Reconciliation
- Peoplesoft User Management Target Reconciliation

These scheduled jobs 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 job. See Configuring Scheduled Jobs for instructions on running the scheduled job.

> **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.

Scheduled Job Attributes

Table 3-1 describes the attributes of the scheduled jobs or lookup field synchronization.

Table 3-1 Scheduled Job Attributes for Lookup Field Synchronization

Attribute	Description
IT Resource Name	Enter the name of the IT resource. Default Value: `PSFT User`
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 job. Default value: Enter a Value Sample value: `C:\PSFTUM\LookupRecon\Roles.properties`

Table 3-1 (Cont.) Scheduled Job Attributes for Lookup Field Synchronization

Attribute	Description
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: `Peoplesoft Language Code Lookup Reconciliation`
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 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`

Configuring Reconciliation

This section discusses the following topics related to configuring reconciliation:

- Performing Lookup Reconciliation
- Performing Full Reconciliation
- Performing Incremental Reconciliation
- Limited Reconciliation

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 job.

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.

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.

> **Note:**
>
> If the target version is PeopleSoft HRMS 9.1 with PeopleTools 8.51, you must use PeopleTools 8.51.13 release for full reconciliation.

The following sections discuss the procedures involved in full reconciliation:

- Generating XML Files
- Importing XML Files into Oracle Identity Manager

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 Configuring the Target System for Full Reconciliation for more information.
> - 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.
> - You must run the Application Engine program if you are performing the full reconciliation for the first time. See Performing Lookup Reconciliation 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.**
7. From the **Server Name** list, select the appropriate server.
8. Select **Full Table Data Publish** process list, and click **OK.**

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 About Configuring the PeopleSoft Integration Broker through Creating the Remote Node for more information.

   Copy these XML files to a on the Oracle Identity Manager host computer. Ensure that the permissions for these XML files are sufficiently restrictive. By default, the permissions are set to 644. You can set them to 640.

> **Note:**
>
> After you have performed this procedure:
>
> - Remove the permission list created in Setting Up the Security for the USER_PROFILE Service Operation section. This is for security purposes.
> - Ensure to disable the USER_PROFILE_HR_TO_UMFILE routing created earlier.

Importing XML Files into Oracle Identity Manager

This section describes the procedure to import XML files into Oracle Identity Manager.

It contains the following topics:

- Configuring the Scheduled Job for User Data Reconciliation
- Attributes of the Scheduled Job for Reconciliation of User Data

Configuring the Scheduled Job for User Data Reconciliation

When you run the Connector Installer, the PeopleSoft User Management Target Reconciliation scheduled job is automatically created in Oracle Identity Manager.

The PeopleSoft User Management Target Reconciliation scheduled job is used for target resource reconciliation. In addition, this same scheduled job is used to reconcile data of deleted users from a target resource into Oracle Identity Manager.

The scheduled job 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 job. See Configuring Scheduled Jobs for instructions on configuring the scheduled job.

Attributes of the Scheduled Job for Reconciliation of User Data

Table 3-2 describes the attributes of the scheduled job for reconciliation of user data.

Table 3-2 Attributes of the Scheduled Job 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 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 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 Configuring the IT Resource section. Default value: `PSFT User`

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.VERSION_84` **Note:** This value must match the entry in the Lookup.PSFT.Configuration lookup definition, as it is used to determine the class name of the message handler. See Lookup.PSFT.Configuration for information about the lookup.
Task Name	This attribute holds the name of the scheduled task. Default value: `PeopleSoft User Management Target Reconciliation`

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 Deploying the PeopleSoft Listener.

Limited Reconciliation

You can configure limited reconciliation to specify the subset of target system records that must be fetched into Oracle Identity Manager.

This section contains the following topics:

About 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 job.

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
```

Configuring Limited Reconciliation

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.

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.

This section contains the following topics:

About Resending 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.

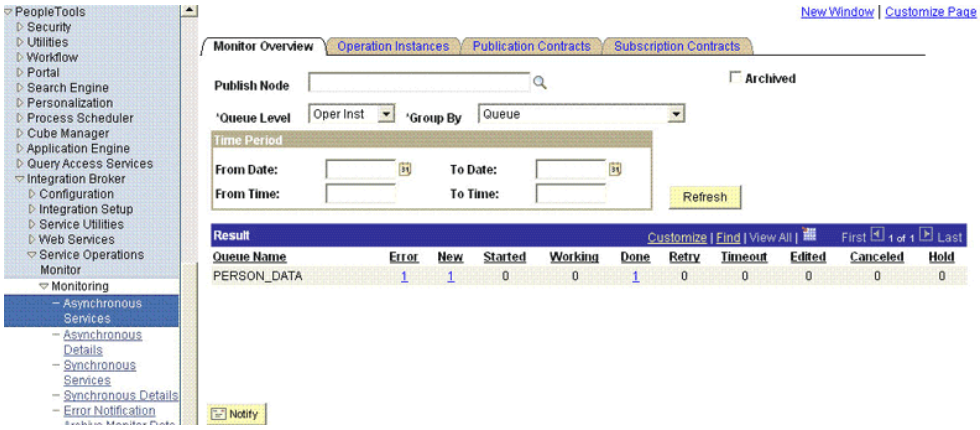
If the status of the message is `New` or `Started` and it does not change to `Timeout` or `Done`, then you must restart the PeopleSoft application server after you restart Oracle Identity Manager.

> **Note:**
>
> PeopleSoft supports this functionality for a limited rights user described in Creating a Role for a Limited Rights User. But, you can specify users who have rights to perform this job based on the security policy of your organization.

Resending Messages Manually

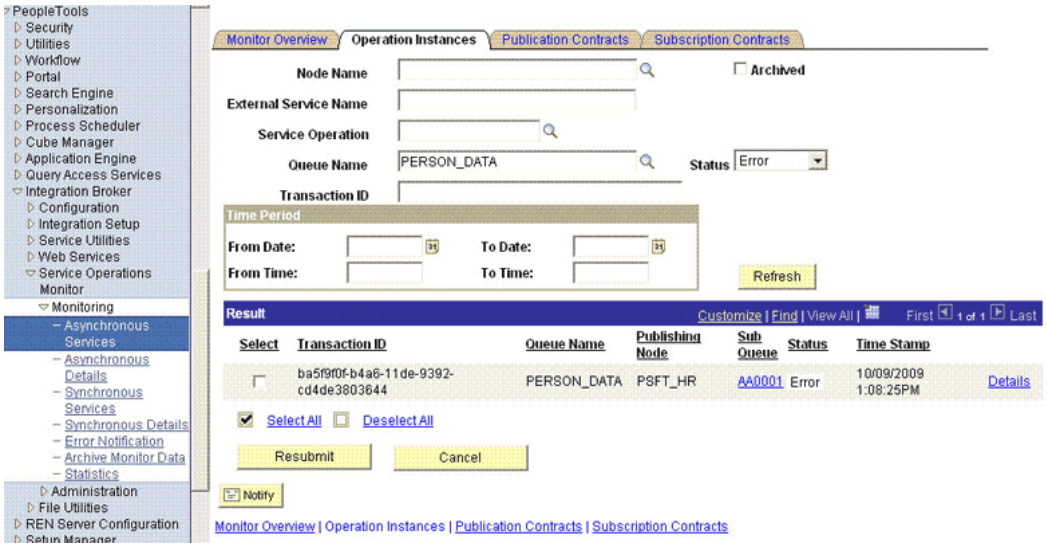
To ensure that all the messages generated on the target system reach Oracle Identity Manager, manually resend messages in Error or TimeOut status. To do so:

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.

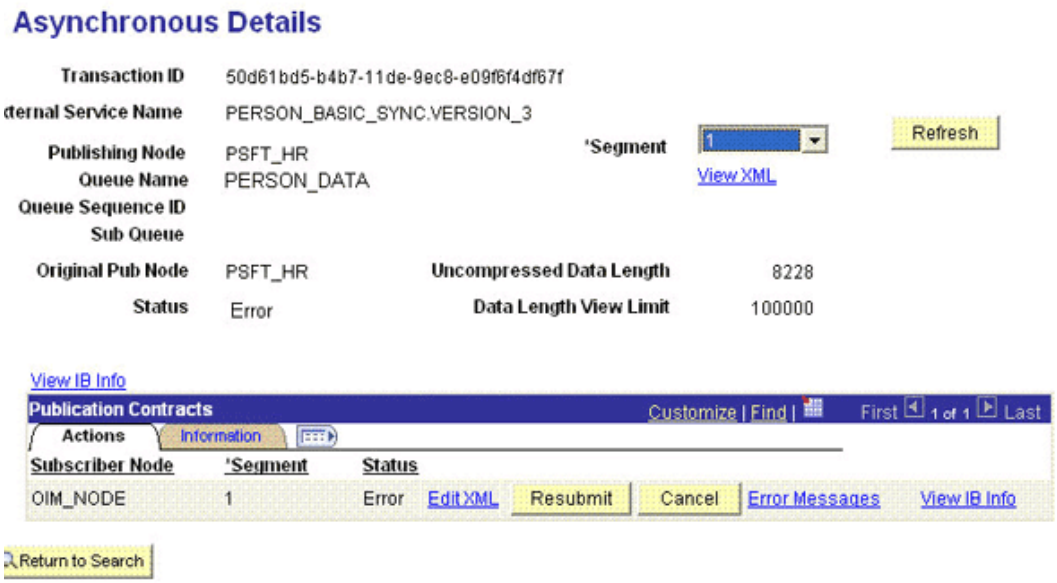


   The number is in the form of a link, which when clicked displays the details of the message.
3. Click the link pertaining to the message to be resent, for example, the link under the Error or the TimeOut column.

   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.

Performing Provisioning Operations in Oracle Identity Manager 11.1.1.x

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:

- Direct Provisioning on Oracle Identity Manager
- Request-Based Provisioning in Oracle Identity Manager
- Switching Between Request-Based Provisioning and Direct Provisioning

Direct Provisioning on Oracle Identity Manager

This section describes the prerequisites and the procedure to perform direct provisioning. It contains the following sections:

- Prerequisites
- Performing Direct Provisioning

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.

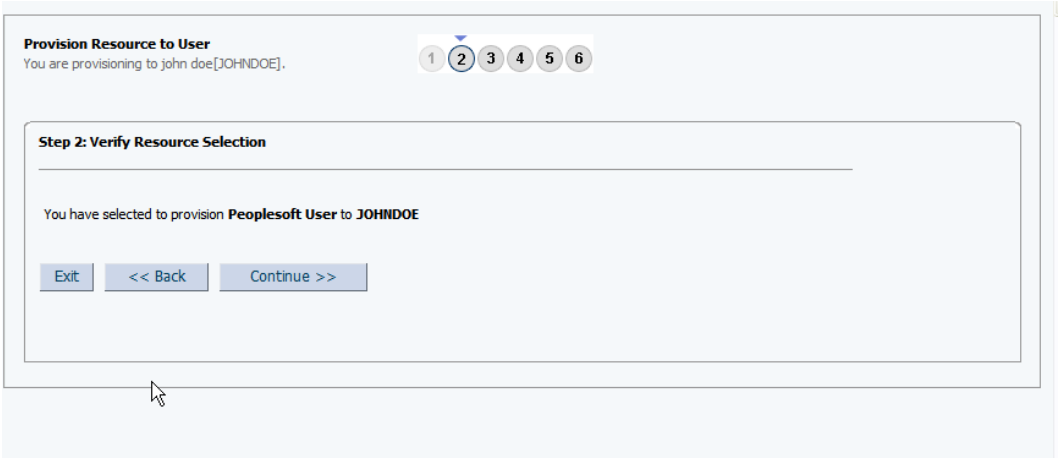
If you configure the connector for request-based provisioning, then the process form is suppressed and object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then see Switching Between Request-Based Provisioning and Direct Provisioning.

Performing Direct Provisioning

To provision a resource by using the direct provisioning approach:

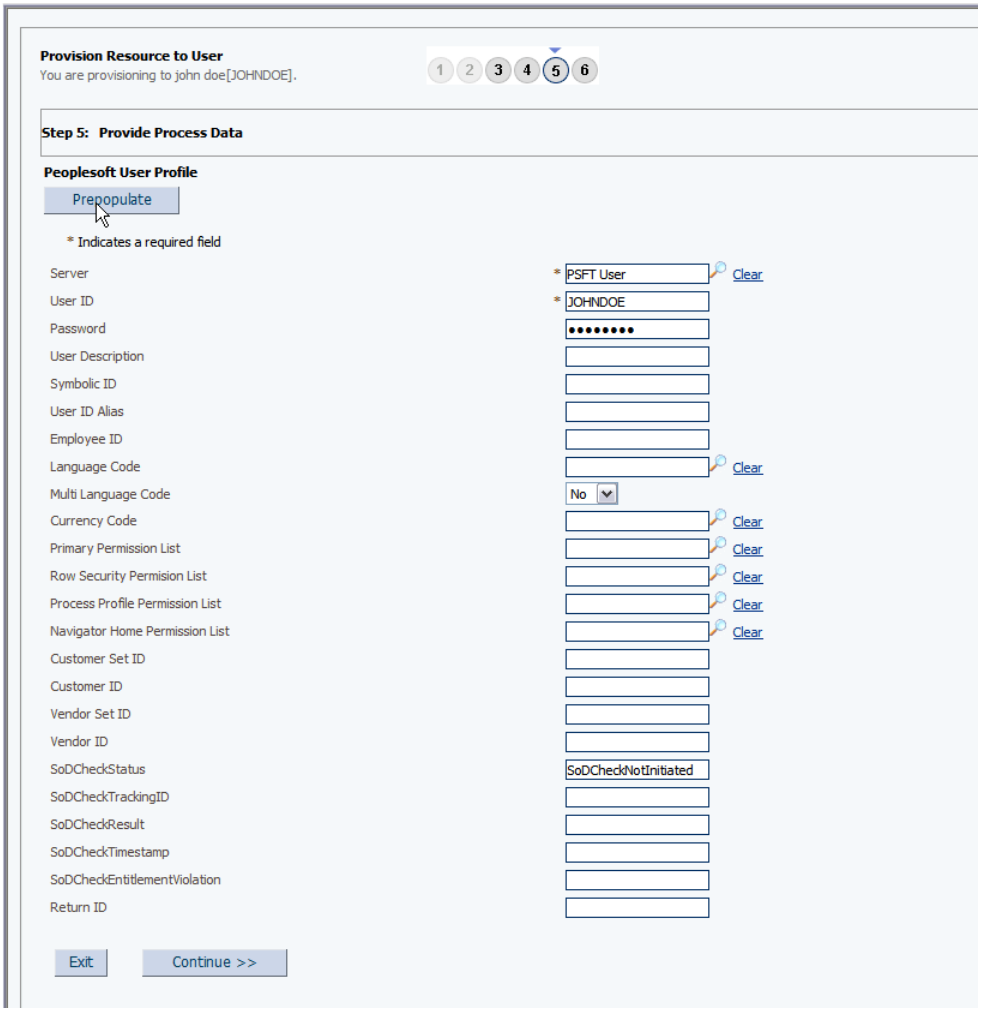
1. Log in to the Administrative and User Console.
2. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced.**

3. Click the **Administration** tab.
4. If you want to first create the OIM User and then provision a resource, then:
   - On the Welcome to Identity Administration page, in the Users region, click **Create User.**
   - On the Create User page, enter values for the OIM User fields, and then click **Save.**
5. If you want to provision a target system account to an existing OIM User, then:
   - On the Welcome to Identity Administration page, in the Users region, click **Advanced Search - Users.**
   - 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.
6. Click the **Resources** tab.
7. Click **Add.** The Provision Resource to User page is displayed in a new window.
8. On the Select a Resource page, select **Peoplesoft User** from the list, and then click **Continue.**
9. On the Verify Resource Selection page, click **Continue.**

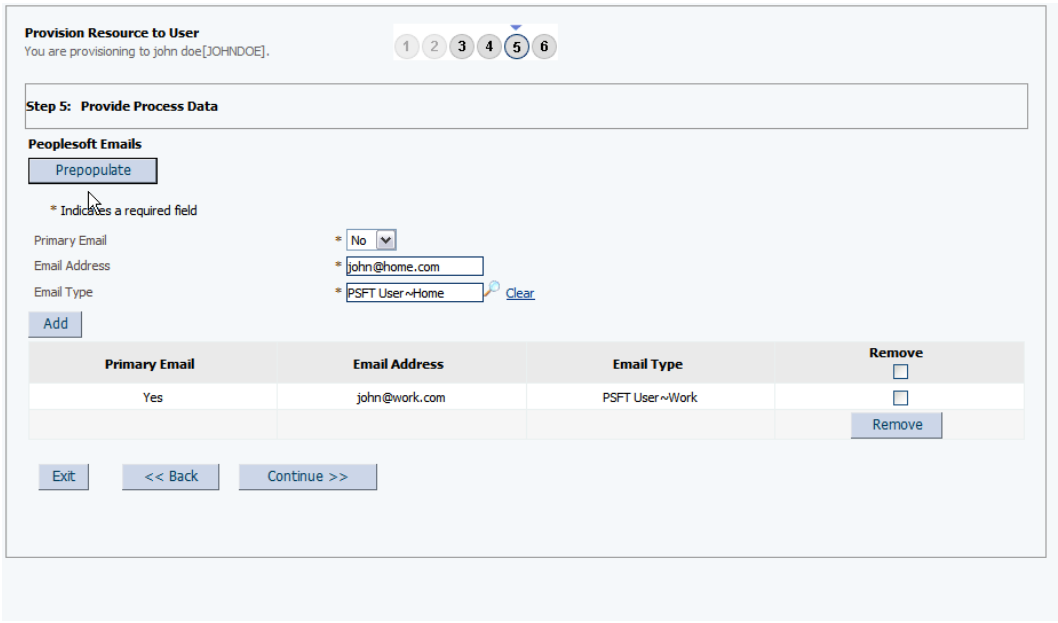


10. On Provide Process Data page, enter the details of the account that you want to create on the target system, and then click **Continue.**

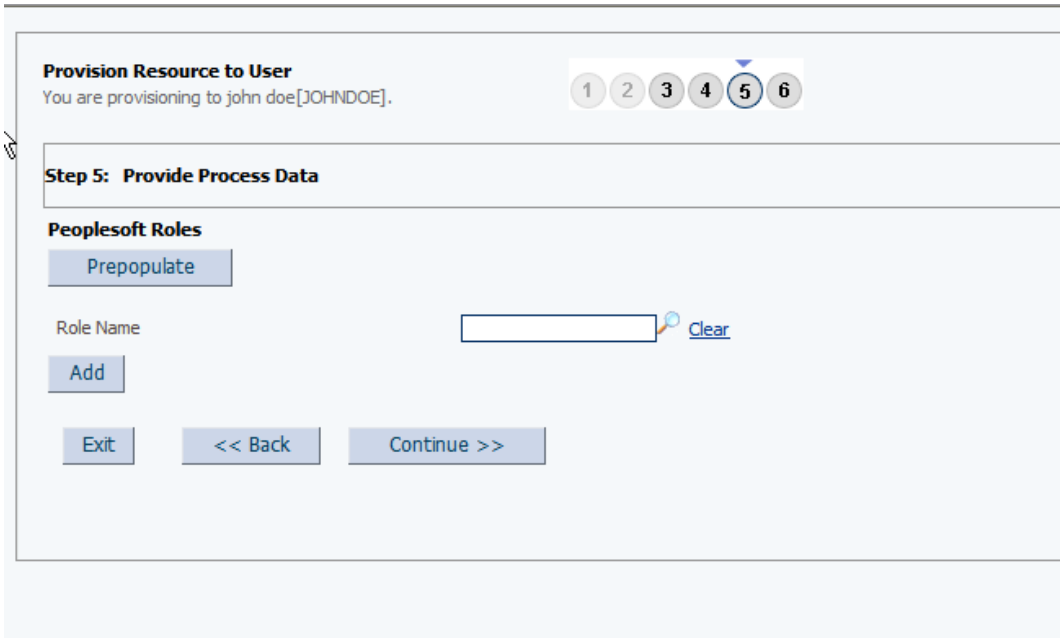
> **Note:**
>
> You can assign multiple ID types to a user profile on the PeopleSoft target system. However, a single instance of an ID type can be assigned to the same user.
>
> For example, you can link a user profile to Employee ID and Vendor ID during provisioning. However, the same user cannot be linked to two Employee ID instances.



11. 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.**

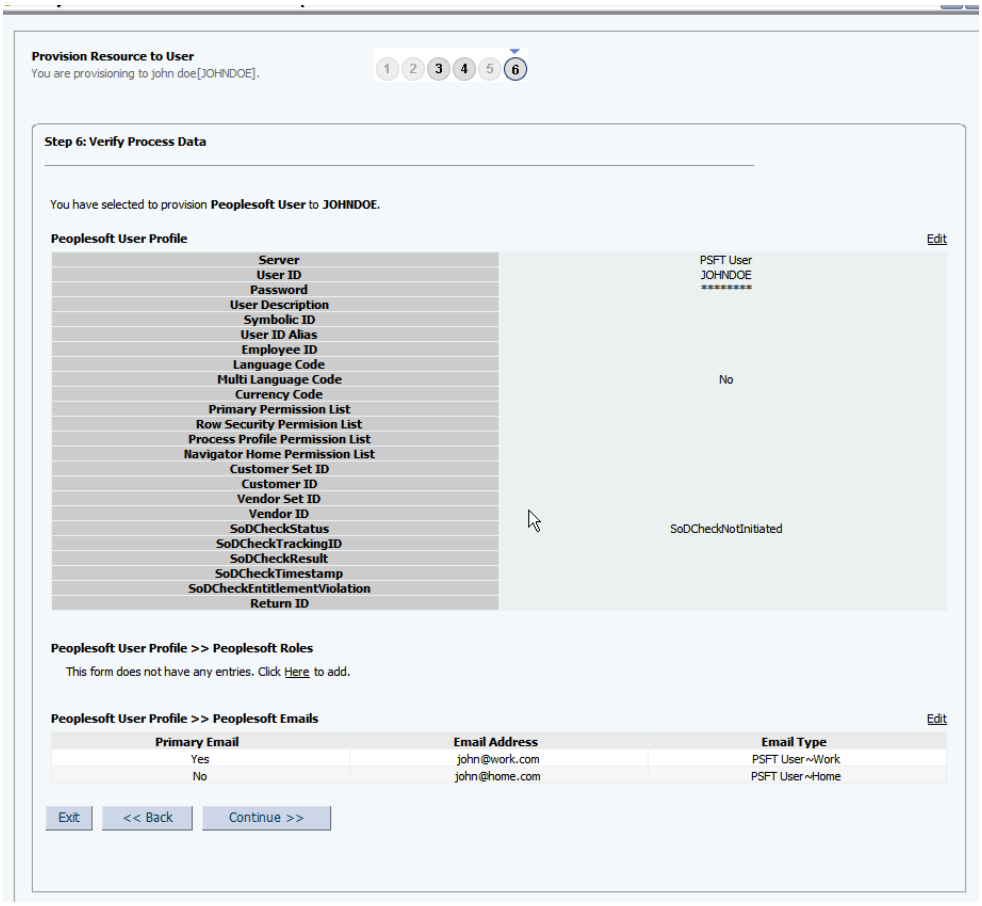


12. On the Provide Process Data page for role data, specify the role name, and then click **Add.** If you want to add more than one role, repeat the process. Then, click **Continue.**



13. 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.



14. The "Provisioning has been initiated" message is displayed. Close this window, and click **Refresh** to view details of the newly provisioned resource.

> **See Also:**
>
> Connector Objects Used During Provisioning for more information about the provisioning functions supported by this connector and the process form fields used for provisioning

Request-Based Provisioning in Oracle Identity Manager

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:

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

End User's Role in Request-Based Provisioning

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

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.

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.

Switching Between Request-Based Provisioning and Direct Provisioning

The following topics describe switching between request-based provisioning and direct provisioning:

- Switching From Request-Based Provisioning to Direct Provisioning
- Switching From Direct Provisioning to Request-Based Provisioning

> **Note:**
>
> It is assumed that you have performed the procedure described in Enabling Request-Based Provisioning.

Switching From Request-Based Provisioning to Direct Provisioning

To switch from request-based provisioning to direct provisioning:

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.

Switching From Direct Provisioning to Request-Based Provisioning

To switch from direct provisioning to request-based provisioning:

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.

Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2.*x*

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

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

1. Log in to Identity Self Service.
2. Create a user. See Managing Users in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.

   If you want to provision a Microsoft Exchange mailbox to an existing OIM User, then, on the Users page, search for the required user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance, and then click **Checkout.**
5. Specify values for fields in the application form and then click **Ready to Submit.**
6. Click **Submit.**
7. If you want to provision entitlements, then:
   a. On the Entitlements tab, click **Request Entitlements.**
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
   c. Click **Submit.**

Configuring Scheduled Jobs

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

See Configuring the Scheduled Jobs for Lookup Field Synchronization for a list of scheduled jobs that you must configure.

To configure a scheduled job:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.*x*:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   - For Oracle Identity Manager release 11.1.2.*x:*
     a. Log in to Identity System Administration.
     b. In the left pane, under System Management, click **Scheduler.**
2. Search for and open the scheduled job as follows:
   a. If you are using Oracle Identity Manager release 11.1.1.x, then on the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
   b. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   c. In the search results table on the left pane, click the scheduled job in the Job Name column.
3. On the Job Details tab, you can modify the following parameters:
   - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

   > **Note:**
   >
   > See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

4. Specify values for the attributes of the scheduled job. To do so:

   On the Job Details tab, under the Parameters section, specify values for the attributes of the scheduled job. See Table 3-2 for more information about the attributes of the scheduled job.

> **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.

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

> **Note:**
>
> The Stop Execution option is not available in the Administrative and User Console. If you want to stop a job, then click **Stop Execution** on the Task Scheduler form of the Design Console.

Provisioning Operations Performed in an SoD-Enabled Environment

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:

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 Web service of Oracle Application Access Controls Governor receives the entitlement data.
5. 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.
6. The status of the process task that received the response depends on the response. 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.

Direct Provisioning in an SoD-Enabled Environment

The procedure for direct provisioning in an SoD-enabled environment is similar to the procedure for direct provisioning in a typical 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.**
7. On the Step 2: Verify Resource Selection page, click **Continue.**
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.**

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.**
10. On the Step 4: Verify Process Data page, verify the data that you have provided and then click **Continue.**
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.

> **Note:**
>
> If Oracle Identity Manager is not SoD enabled, then SOD Check Status field shows SODCheckNotInitiated.

13. To view the Resource Provisioning Details page, on the Resources tab of the user details page, select **Resource History.**

> **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 SoD validation process is initiated, the results of the 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.

    On this page, 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.

    On this page, 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.

17. After the SoD validation process is initiated, the results of the 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.

    On this form, 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.

    On the Resource Provisioning Details page, the state of the Add Role to User task is completed.

Request-Based Provisioning in an SoD-Enabled Environment

> **Note:**
>
> This procedure is not applicable to Oracle Identity Manager release 11.1.2.*x* or later.
>
> See Configuring SoD on Oracle Identity Manager for related information.

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.

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 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.

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.

4

Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

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

Adding New Attributes for 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, perform the procedures described in the following sections. In these sections, the Worklist User attribute in the USER_PROFILE PeopleSoft Component Interface is added. You can follow the same procedures to add other attributes.

Verifying the Attribute Definition in PeopleSoft Component Interface

You must verify that the new attribute, Worklist User, is listed as one of the properties of the USER_PROFILE Component Interface. Only the attributes listed under properties are supported for provisioning. If the attribute exists, verify and note the definition of the attribute.

To verify the definition of the attribute in the USER_PROFILE Component Interface:

1. To open the PeopleSoft 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 click **Open.**
5. Double-click the **USER_PROFILE** entry.
6. Expand **PROPERTIES** and select the **Worklist User** attribute. In addition, note that the Comment field of the Worklist User attribute has the following entry:

   ```
   Y for Yes, N for No
   ```

   The Comment entry means that the Worklist User attribute supports two values, `Y` and `N`.
7. Right-click **Worklist User** and click **View Definition.**

   Note that the Worklist User attribute is of `Char` type and of length `1` character in upper case format. You must match this definition in the lookup definition entry for the new attribute.

Adding the Attribute to the PeopleSoft Component Interface Map Definition

The PeopleSoft User Management connector performs user provisioning by invoking methods and setting properties on PeopleSoft Component Interfaces. Component Interface definitions are assigned in the PeopleSoft Component Interface configuration objects. You can add and modify the definitions by editing a copy of the `PeopleSoftComponentInterfaces.xml` file located in the xml of the connector package.

> **See Also:**
>
> Connector Component Interfaces for the PeopleSoft User Management for more information about the PeopleSoft Component Interface map definition

To add the new attribute to the PeopleSoft Component Interface map definition XML file:

1. In a text editor, open the PeopleSoft Component Interface map definition file, PeopleSoftComponentInterfaces.xml.
2. Add the new attribute to the corresponding Object, USER_PROFILE_8_4X, into the `<List>` element under the `<Attribute name="properties">` element.

   The following extract of the PeopleSoftComponentInterfaces.xml file shows the Worklist User attribute added to the USER_PROFILE Component Interface definition:

```
<Object name="USER_PROFILE_8_4X">
    <Attribute name="componentInterface" value="USER_PROFILE" />
        <Attribute name="getKey" value="UserID" />
        <Attribute name="findKey" value="UserID" />
        <Attribute name="createKey" value="UserID" />
        <Attribute name="properties">
        <List>
            <Object name="RowSecurityPermissionList" />
            <Object name="SupervisingUserID" />
            <Object name="SymbolicID" />
            <Object name="UserDescription" />
            <!--Additional fields so that modification is not required-->
            <Object name="EffectiveDateFrom" />
            <Object name="EffectiveDateTo" />
            <Object name="ExpertEntry" />
            <Object name="WorklistUser" />
            <Object name="EmailUser" />
        </List>
    </Attribute>
</Object>
```

Configuring the Attribute in Oracle Identity Manager

Configuring the attribute in Oracle Identity Manager involves the following steps:

- Adding a New Column in the Process Form
- Creating a New Lookup Definition
- Associating the New Lookup With the Worklist User Process Form
- Adding a Mapping for the New AttributeUpdating the Request Dataset
- Updating the Request Dataset

> **Note:**
>
> If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Creating a New UI Form and Updating an Existing Application Instance with a New Form for the procedures.

Adding a New Column in the Process Form

Add a new column in the process form by performing the following:

1. Log in to Oracle Identity Manager Design Console.

2. Expand **Development Tools** and then double-click **Form Designer.**
3. Enter `UD_PSFT_BAS` in the Table Name field and click the **Query for records** button.
4. Click **Create New Version.**
5. 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.
6. From the **Current Version** list, select the newly created version.
7. On the Additional Columns tab, click **Add.**
8. Enter `UD_PSFT_BAS_WORKLIST` in the Name field and `Worklist User` in the Field Label field. Specify other values as shown in the following figure.
9. Click **Make Version Active.**

Creating a New Lookup Definition

Create a new lookup definition of Lookup Type for the attribute, for example, Lookup.PSFT.UM.WorklistUser. Add the following Code Key and Decode entries:

Code Key	Decode
Y	Yes
N	No

The following figure shows the mapping for the new lookup:

Associating the New Lookup With the Worklist User Process Form

Associate the new lookup, Lookup.PSFT.UM.WorklistUser, with the Worklist User process form. To do so:

1. In the process form, click the **Properties** tab.
2. Select **Worklist User (ComboBox)** and click **Add Property.**
3. In the Add Property dialog, specify the following entries:

   Property Name: Lookup Code

   Property Value: Lookup.PSFT.UM.WorklistUser
4. Click the save button and click **Make Version Active.**

Adding a Mapping for the New Attribute

Add a mapping for the new attribute to the Lookup.PSFT.UM.ProvAttrMap lookup definition. To do so:

1. Expand **Administration** and then double-click **Lookup Definition.**
2. Enter the Lookup.PSFT.UM.ProvAttrMap as the name of the lookup definition in the **Code** field and click the **Query for records** button.
3. Click **Add** and the following Code Key and Decode values:

Code Key	Decode
Worklist User	WorklistUser

The Code Key value maps to the process form label and the Decode value maps to the entry in the PeopleSoftComponentInterfaces.xml file for the new attribute.

> **Note:**
>
> To enable the update on the new attribute, perform the procedure described in Enabling Update on a New Attribute for Provisioning.

Updating the Request Dataset

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:

1. In a text editor, open the XML file located in the *OIM_HOME*/server/ConnectorDefault/PSFT_UM-11.1.1.6.0/dataset for editing.
2. Add the AttributeReference element and specify values for the mandatory attributes of this element.

   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 table name 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.

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

   See Running the PurgeCache Utility in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.
5. Import into MDS, the request dataset definitions in XML format.

   See Importing Request Datasets into MDS for detailed information about the procedure.

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 Adding New Attributes for Provisioning.

1. Log in to 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 **ADPPSFTUPDATEATTRIBUTEVALUE** 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 **AttrFieldName.** A window is displayed for editing the data mapping of the variable.

e. From the Map To list, select **Literal.**

f. 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.ProvAttrMap lookup definition.

g. In the Adapter Variables region, double-click **ITResourceFieldName.** A window is displayed for editing the data mapping of the variable.

h. From the Map To list, select **Literal.**

i. In the Literal Value field, enter `UD_PSFT_BAS_SERVER` as the column name of the ITResource field.

j. In the Adapter Variables region, double-click **objectType.** A window is displayed for editing the data mapping of the variable.

k. From the Map To list, select **Literal.**

l. In the Literal Value field, enter `User` and then save.

m. In the Adapter Variables region, double-click **procInstanceKey.** A window is displayed for editing the data mapping of the variable.

n. From the Map To list, select **Process Data** and from the Qualifier list, select **Process Instance** and then save.

7. Perform the mappings and save the form.

8. Click the **Responses** tab of the Worklist Updated task. The `SUCCESS` 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.

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.ReconAttrMap 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 Oracle Identity Manager Design Console, make the required changes as follows:

> **See Also:**
>
> Adding Target System Attributes for Target Reconciliation in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed instructions on performing the following steps

a. Add a new attribute on the process form. See Adding New Attributes for Provisioning for more information.

b. Expand **Resource Management** and then double-click **Resource Objects.**

c. In the Name field, enter the name of the object definition and then click the **Query for records** button.

d. On the Object Reconciliation tab, click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

e. Add a reconciliation field corresponding to the new attribute in the Peoplesoft User resource object. For example, you can add the WorkList reconciliation field.

f. Modify the Peoplesoft User Management process definition to include the mapping between the newly added field and the corresponding reconciliation field.

2. Add the new attribute in the message-specific attribute mapping lookup definition, for example, the Lookup.PSFT.UM.UserProfile.ReconAttrMap 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.

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

4. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Creating a New UI Form and Updating an Existing Application Instance with a New Form for the procedures.

Adding New ID Types for Provisioning

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.

This section contains the following topics:

- About Adding New ID Types for Provisioning
- Adding a New ID Type for Provisioning

About 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:

- You can assign multiple ID types to a user profile on the PeopleSoft target system. However, a single instance of an ID type can be assigned to the same user.

  For example, you can link a user profile to Employee ID and Vendor ID during provisioning. However, the same user cannot be linked to two Employee ID instances.
- 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.

Adding a New ID Type for Provisioning

Suppose you want to add a new ID type Equation SQL Auth Class with attribute EQS ID for provisioning. 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 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 EQS ID, for example `Operator Alias Value`. In addition, enter other values, such as the field label as `EQS ID`.
   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.ProvAttrMap` as the name of the lookup definition in the Code field and click the **Query for records** button.

d. Modify the Lookup.PSFT.UM.ProvAttrMap lookup definition by adding a new row with the following values:

   Code Key: Column name of the form

   Decode: Enter a combination of elements similar to the following Decode for the EQS ID type:

   IDTypes~UM_IDTypes[IDType=EQS]~Attributes~UM_Attributes[AttributeName=Operator Alias Value]~AttributeValue

   In this format:

   - *IDTypes*: Refers to the Identity Connector Framework (ICF) Parent Attribute Name
   - *UM_IDTypes*: Refers to the embedded ICF object class that contains *IDType* and *Attributes*. The default value of *IDType* is `EQS`.
   - *Attributes*: Refers to the ICF embedded object class that contains *AttributeName* and *AttributeValue*. The default value of *AttributeName* is `Operator Alias Value`. The value of *AttributeValue* is retrieved from the form field.

   See Lookup.PSFT.UM.ProvAttrMap for more information about the format of the elements in Decode.

   To add Equation SQL Auth Class ID type with ID type value EQS, and attribute name Operator Alias Value, you must define a mapping similar to the Employee ID mapping in the Lookup.PSFT.UM.ProvAttrMap lookup definition.

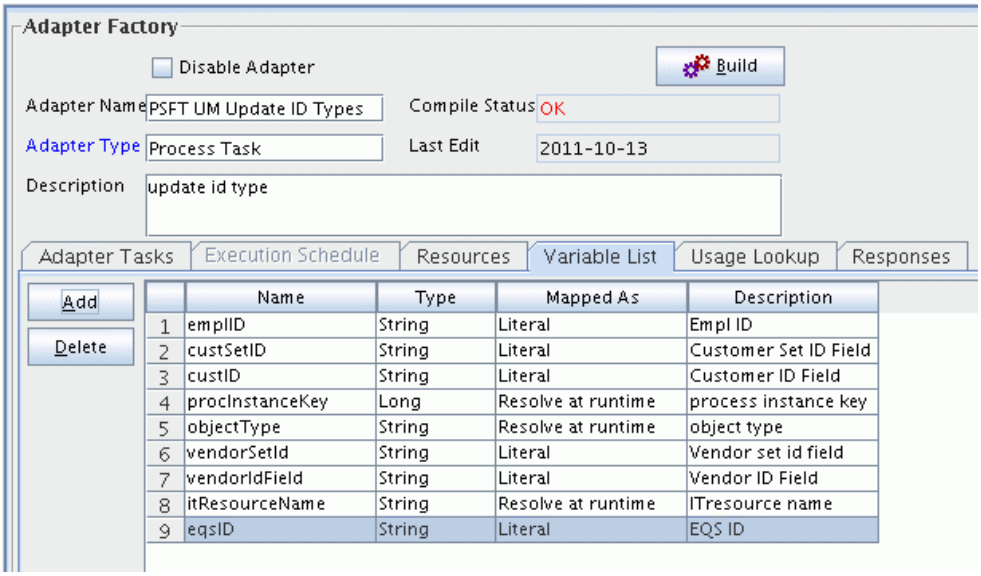
3. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this ID type visible. See Creating a New UI Form and Updating an Existing Application Instance with a New Form for the procedures.

Enabling Update on a New ID Type for Provisioning

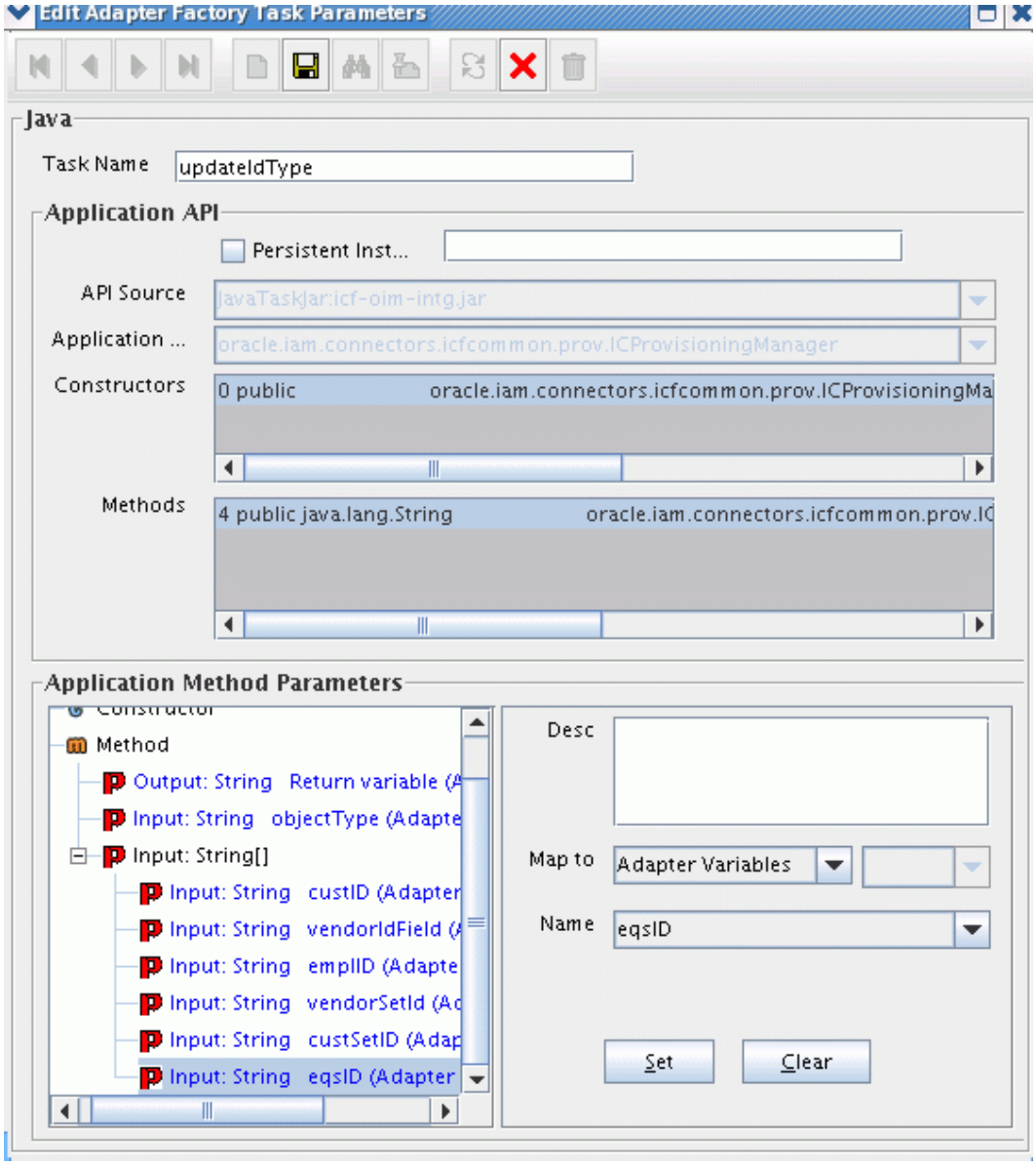
Suppose, you want to update the EQS ID field as described in Adding New ID Types for Provisioning. Then, perform the following procedure:

To update the newly added ID type attributes:

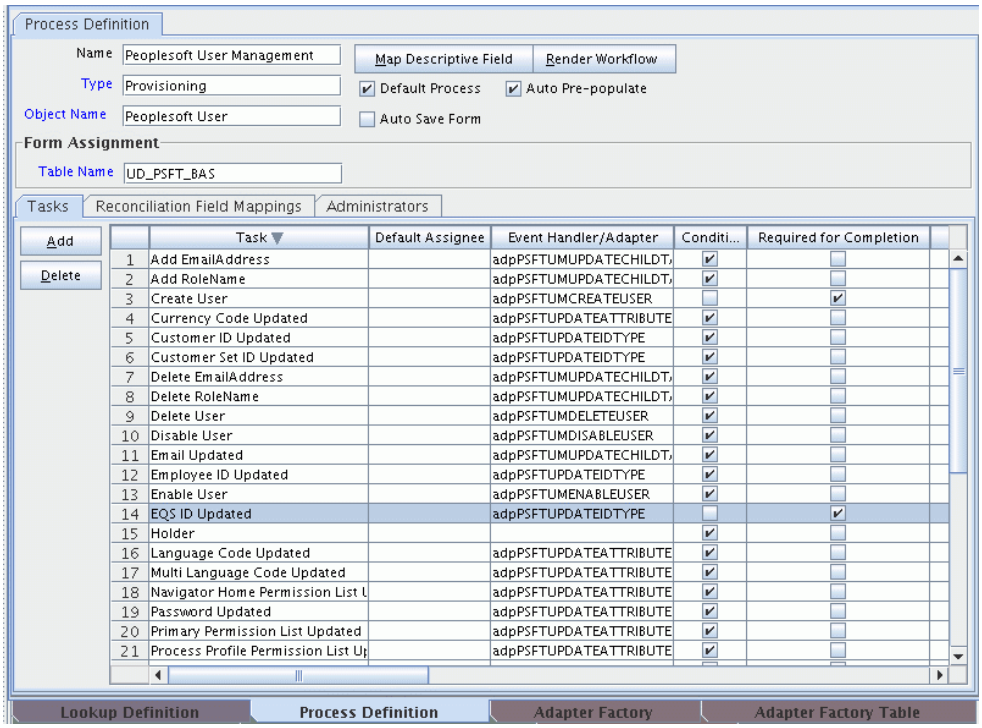
1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools** and then double-click **Adapter Factory.**
3. Enter `PSFT UM Update ID Types` in the Adapter Name field, and then click the **Query for records** button.
4. In the Adapter Tasks tab, expand PSFT UM Update ID Types, and then select **updateIdType**.
5. Click the **Variable List** tab and add the attribute names along with their types and mappings based on your entries in Adding New ID Types for Provisioning. Click the save button.



6. In the Adapter Tasks tab, expand PSFT UM Update ID Types, and then double-click **updateIdType**.
7. In the **Edit Adapter Factory Task Parameters** dialog, in the Application Method Parameters section, expand **Method,** and then right-click on the **Input: String[]** type of parameter. Click on **Add String** and add the attributes that you added in Step 5 one at a time. For each attribute, select values for the **MapTo** and **Name** fields. Click the save button.



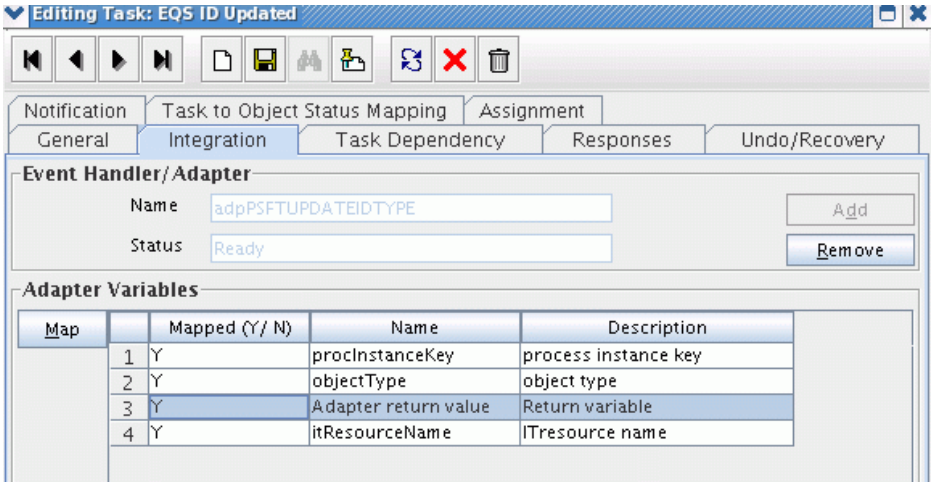
8. Expand **Process Management** and then double-click **Process definition.**
9. Enter `Peoplesoft User Management` in the Name field, and then click the **Query for records** button.
10. Add a new task, for example `EQS ID Updated`, and save the task.



11. Double-click the EQS ID Updated task, click the **Integration** tab, and then click **Add.**

12. Select **Adapter** as the handler type and then perform the following:

    a. Select **ADPPSFTUPDATEIDTYPE** as shown in the following mapping, and then click the save button.



    b. In the Adapter Variables region, double-click **Adapter return value** and select **Response Code** from the Map To list. Click the save button.

    c. In the Adapter Variables region, double-click **objectType** and select **Literal** from the Map To list.

    d. Enter `User` in the Literal Value field and click the save button.

    e. In the Adapter Variables region, double-click **ITResourceName** and select **Literal** from the Map To list.

f. In the Literal Value field, enter `UD_PSFT_BAS_SERVER` as the column name for the new attribute that was added in the Lookup.PSFT.UM.ProvAttrMap lookup definition.

g. In Adapter Variables region, double-click **ProcessInstanceKey.**

h. From the Map To list, select **Process Data,** and from the Qualifier list, select **Process Instance** and then click the save button.

13. Perform the mappings and save the format.

14. Click the **Responses** tab of the EQS ID Updated task. The SUCCESS response should be mapped with status **C** and all other responses with status **R**.

Adding New ID Types for Reconciliation

Suppose, you want to reconcile the EQS ID field as described in Adding New ID Types for Provisioning, then perform the following procedure:

To add a new ID type for reconciliation:

1. Add new ID Type attribute on the process form. For the procedure to add a new ID Type attribute, see Adding New ID Types for Provisioning.

2. Create a reconciliation profile for the new ID type attribute. To do so:

   a. Expand **Resource Management** and then double-click **Resource Objects.**

   b. In the Name field, enter the name of the object definition and then click the **Query for records** button.

   c. Click the **Object Reconciliation** tab and add a reconciliation field corresponding to the new attribute in the Peoplesoft User resource object. Click the save button.

   d. Click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

3. Modify the Peoplesoft User Management process definition to include the mapping between the newly added field and the corresponding reconciliation field.

4. Add the new attribute in the message-specific attribute mapping lookup definition, for example, the Lookup.PSFT.UM.UserProfile.ReconAttrMap lookup definition for the USER_PROFILE message.

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

Code Key	Decode
AttributeName	*OPRALIASVALUE~PSOPRALIAS~OPRALIASTYPE=EQS*

   For example:

   Code Key: EQS

   Decode: EQS_ID~PSOPRALIAS

   In this example, `EQS` is the reconciliation field and its equivalent target system field is EQS_ID.

5. 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.

   In this example, the following values must be added to this lookup:

Code Key	Decode
EQS ID	EQS ID

6. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this ID type visible. See Creating a New UI Form and Updating an Existing Application Instance with a New Form for the procedures.

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 User ID 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.

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

You must create a class with the following signature:

```
public boolean validate(HashMap arg0, HashMap arg1, String arg2)
```

In this signature code:

- `arg0` contains primary table field values
- `arg1` contains child table field values
- `arg2` is the field on which validation needs to be done

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

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

public boolean validate(HashMap hmUserDetails,
         HashMap hmEntitlementDetails, String field) {
            /*
         * You must write code to validate attributes. Parent
         * data values can be fetched by using hmUserDetails.get(field)
         * For child data values, loop through the
         * ArrayList/Vector fetched by hmEntitlementDetails.get("Child
Table")
         * Depending on the outcome of the validation operation,
```

```
        * the code must return true or false.
        */
        /*
        * In this sample code, the value "false" is returned if the field
        * contains the number sign (#). Otherwise, the value "true" is
        * returned.
        */
           boolean valid=true;
           String sUserID=(String) hmUserDetails.get(field);
           for(int i=0;i<sUserID.length();i++){
             if (sUserID.charAt(i) == '#'){
                   valid=false;
                   break;
             }
           }
           return valid;
      }
    } /* End */
```

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

> **Note:**
>
> Before you use this utility, verify that the `WL_HOME` environment variable is set to the in which Oracle WebLogic Server is installed.

   - For Microsoft Windows:

     OIM_HOME/server/bin/UploadJars.bat

   - For UNIX:

     OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Search for and open the message-specific configuration lookup definition, in this example, the **Lookup.PSFT.Message.UserProfile.Configuration** lookup definition for the USER_PROFILE message. See 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.ReconValidation.
   c. Search for and open the **Lookup.PSFT.UM.ReconValidation** lookup definition.
   d. In the Code Key column, enter `User ID`. In the Decode column, enter `com.validate.MyValidation`.

Here, the Code Key value specifies the column name of the field you want to validate. The Decode value is the complete package name of the Java class that has the validation logic.

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.ear file from the application server.

6. Copy the validation JAR file created in Step 2 to the following :

   PeoplSoftOIMListener.ear/PeoplSoftOIMListener.war/WEB-INF/lib

7. Redeploy the PeopleSoftOIMListener.ear file on the application server. See Deploying the PeopleSoft Listener for the procedure.

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.

> **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 com.transform;
import java.util.*;
public class MyTransform {

      /*
      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;
        }
} /* End */
```

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

   > **Note:**
   >
   > Before you use this utility, verify that the `WL_HOME` environment variable is set to the in which Oracle WebLogic Server is installed.

   - For Microsoft Windows:

     OIM_HOME/server/bin/UploadJars.bat

   - For UNIX:

     OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.
4. If you created the Java class for 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 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 `Currency Code`. In the Decode column, enter `com.transform.MyTransform`.

      Here, the Code Key value specifies the column name of the field you want to validate. The Decode value is the complete package name of the Java class that has the transformation logic.

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.ear file from the application server.
6. Copy the transformation JAR file created is Step 2 to the following :

   PeoplSoftOIMListener.ear/PeoplSoftOIMListener.war/WEB-INF/lib
7. Redeploy the PeopleSoftOIMListener.ear file on the application server. See Deploying the PeopleSoft Listener for the procedure.

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.

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

You must create a class with the following signature:

```
public boolean validate(HashMap arg0, HashMap arg1, String arg2)
```

In this signature code:

- `arg0` contains primary table field values
- `arg1` contains child table field values
- `arg2` is the field on which validation needs to be done

The following sample validation class checks whether the value in the user ID attribute contains the number sign (#):

```
package com.validation;
import java.util.HashMap;

public class Validator {
```

```
    public boolean validate(HashMap hmUserDetails, HashMap hmEntitlementDetails,
String sField) {

        /* 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 sGivenName = (String) hmUserDetails.get(sField);
        for (int i = 0; i < sGivenName.length(); i++) {
            if (sGivenName.charAt(i) == '#') {
                valid = false;
                break;
            }
        }
        return valid;
    }
} /* End */
```

2. Create a JAR file to hold the Java class.
3. Update the Lookup.PSFT.UM.Prov.Configuration lookup definition by performing the following steps:

> **See Also:**
>
> Lookup.PSFT.UM.Prov.Configuration for more information about the lookup

   a. Log in to the Design Console.
   b. Search for and open the **Lookup.PSFT.UM.Prov.Configuration** lookup definition.
   c. In the Code Key column, enter `Provisioning Validation Lookup`. In the Decode column, enter `Lookup.PSFT.UM.ProvValidation`.
   d. Save the changes to the lookup definition.
4. Create a new lookup definition Lookup.PSFT.UM.ProvValidation and update the lookup by performing the following steps:

> **See Also:**
>
> Creating Lookups in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about creating a new lookup definition

a. In the Code Key column, enter `User ID`. In the Decode column, enter `com.validation.Validator`.

   Here, the Code Key value specifies the column name of the field you want to validate. The Decode value is the complete package name of the Java class that has the validation logic.

b. Save the changes to the lookup definition.

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

> **Note:**
>
> Before you use this utility, verify that the `WL_HOME` environment variable is set to the 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.

6. Run the PurgeCache utility to purge the Oracle Identity Manager cache.

   See Clearing Content Related to Connector Resource Bundles from the Server Cache for more information about the PurgeCache utility.

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.

Configuring the Connector for Multiple Installations of the Target System

You can configure the connector for multiple installations of the target system by creating copies of the connector objects, such as the IT resource, process form, process definition, and resource object.

This section contains the following topics:

About 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.

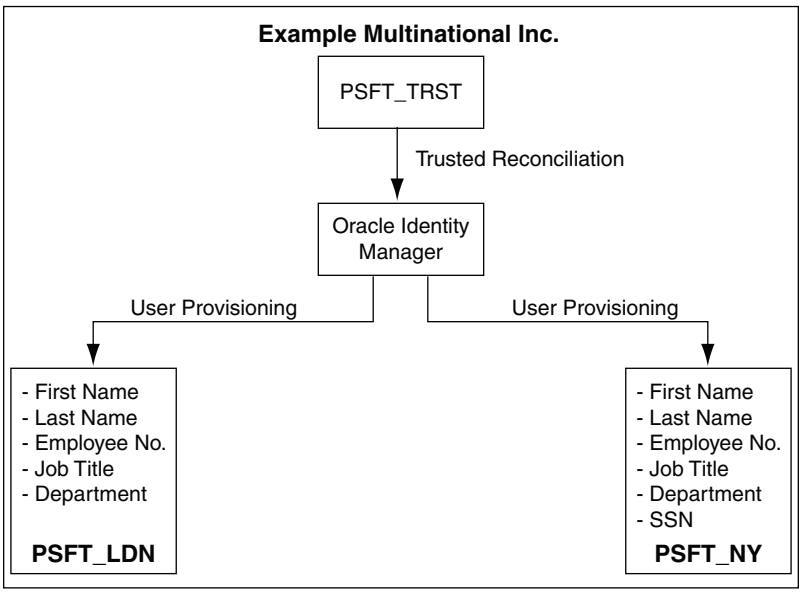
The company has a trusted (authoritative) source of identity data for Oracle Identity Manager, for example PSFT_TRST. The company uses the PeopleSoft Employee Reconciliation connector to reconcile person records, which in turn creates OIM Users.

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.

Connector Objects and Their Associations

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 User	• 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.
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.

Table 4-1 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Description
Message-specific Configuration Lookup Definition	• Lookup.PSFT.Message.UserProfile.Configuration • Lookup.PSFT.Message.DeleteUserProfile.Configuration	Attribute mapping lookup definitions: • Lookup.PSFT.UM.UserProfile.ReconAttrMap • 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.ProvAttrMap • 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	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.

Creating Copies of the Connector Objects

To create copies of the connector objects:

1. Create a copy of the IT resource. See 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. 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 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.ReconAttrMap 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 Job for User Data Reconciliation for information about this scheduled task.

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.

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.

You can enable this feature after you deploy the Oracle Identity Manager. To enable the Dependent Lookup Fields feature, perform the following procedures:

> **Note:**
>
> To provision a resource, you enter the required values in the process form with at least 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*

- Updating the UD_PSFT_BAS Form
- Updating the UD_PS_EMAIL Form
- Updating the UD_PSROLES Form

Updating the UD_PSFT_BAS Form

This section describes how to update the UD_PSFT_BAS form. It contains the following topics:

- Creating a New Version of the UD_PSFT_BAS Form
- Adding Properties for the Primary Permission List Lookup Field
- Adding Properties for the Lookup Query

Creating a New Version of the UD_PSFT_BAS Form

To create a new version of the UD_PSFT_BAS form:

1. On Oracle Identity Manager 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.

Adding Properties for the Primary Permission List Lookup Field

To add properties for the Primary Permission List lookup field:

1. From the **Current Version** list, select the version that you created.
2. Open the **Properties** tab.
3. Add properties for the **Primary Permission List** 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.PermissionList
   b. Select **Primary Permission List,** 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 Permission List,** 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 Permission List,** 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 Permission List,** 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 Permission List,** 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.PermissionList'
      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.PermissionList' AND
lkv_encoded like '$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
```

I. Click the Save icon, and then close the dialog box.

Adding Properties for the Lookup Query

To add properties for the lookup query:

1. Perform Steps 6a through 6j in Adding Properties for the Primary Permission List Lookup Field. Add the properties that you added for the Primary Permission List field on the UD_PSFT_BAS form.
2. 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, 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)		
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 AND lku_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 AND lku_type_string_key = 'Lookup.PSFT.UM.CurrencyCode' AND lkv_encoded like'$Formdata.UD_PSFT_BAS_SERVER$' + '~%'
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 AND lku_type_string_key = 'Lookup.PSFT.UM.PermissionList' 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
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 AND lku_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 AND lku_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 AND lku_type_string_key = 'Lookup.PSFT.UM.PermissionList' AND lkv_encoded like'$Formdata.UD_PSFT_BAS_SERVER$' + '~%'

3. Click the Save icon to save the changes to the form.
4. Click **Make Version Active.**

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 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 6b of the procedure described in Updating the UD_PSFT_BAS Form, select **Email Type** instead of Primary Permission List.
   b. Perform Steps 6c through 6j. Add the properties that you added for the Email Type field on the UD_PS_EMAIL form.

c. When you perform Step 6k, 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 AND lku_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.**

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 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 6b of the procedure described in Updating the UD_PSFT_BAS Form, select **Role Name** instead of Primary Permission List.
   b. Perform Steps 6c through 6j. Add the properties that you added for the Role Name field on the UD_PSROLES form.
   c. When you perform Step 6k, 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.**

Connector Component Interfaces for the PeopleSoft User Management

The PeopleSoft User Management connector performs user provisioning by invoking methods and setting properties on PeopleSoft Component -Interfaces. Component interface definitions are assigned in the PeopleSoft Component Interface configuration objects. You can modify the definitions by editing a copy of the `PeopleSoftComponentInterfaces.xml` file located in the xml of the connector package. This XML file is mapped to the xmlMapping entry in the Lookup.PSFT.Configuration lookup definition.

This section includes the following information about configuring and implementing component interfaces with the PeopleSoft User Management connector:

- Creating Component Interface Map Definitions
- Customizing PeopleSoft Component Interface Resource Objects

> **Note:**
>
> See Configuring the Target System for Provisioning.

Creating Component Interface Map Definitions

The component interface map contains the list of component interfaces available to the connector. The `interfaces` object contains a list of component interfaces. If you have a custom component interface, you must define your own component interface definition in the map. Edit the PeopleSoft Component Interfaces Configuration object and add your definition as an additional Object into the `<List>` element under the `<Attribute name='interfaces'>` element.

This section contains the following topics:

- Component Interface Definition
- Default Component Interfaces Supported

Component Interface Definition

Each available component interface has its own definition. Key elements of a component interface definition include:

- `name`. The label of a component interface. It often matches the value of the `componentInterface` attribute, but this is not a requirement. The value will be displayed in the drop-down menu on the connector's Resource Parameters page.
- `componentInterface` attribute. The name of the component interface, as defined in PeopleSoft.
- `getKey` attribute. The name of the component interface property that is set when performing a PeopleSoft GET operation. If `getKey` is not defined, then the `key` attribute is used instead.

- `findKey` attribute. The name of the component interface property that is set when performing a PeopleSoft FIND operation. If `findKey` is not defined, then the `key` attribute is used instead.
- `createKey` attribute. The name of the component interface property that is set when performing a PeopleSoft CREATE operation. If `createKey` is not defined, then `key` attribute is used instead.
- `key` attribute. Deprecated. Use `getKey`, `findKey`, or `createKey` instead.
- `properties` attribute. A list of properties that can be read or set from the PeopleSoft component interface.

Each Object in the **properties** list must have the following attribute:

- `name`. The name of the property. This must match exactly with the name of a property exposed by the PeopleSoft component interface identified by the `componentInterface` property. The names of the properties are candidates to be listed as resource user attributes on the Account Attributes page.

  If this a collection property, then you must define additional attributes. A collection property defines its key property and its own nested set of simple and/or complex properties:

  `isCollection` attribute. If the property is a collection, then set this to true.

  `key` attribute. If the property is a collection, set this to the name of the property that uniquely identifies each item of the collection.

  `properties` attribute. The list of properties that can be read/set for each item of the collection. To support arbitrary complexity, each member of this list is an Object with the same allowed attributes as the parent. That is, it can contain its own `name`, `isCollection`, `key`, and `properties` attributes.

- `disableRule` attribute. An Object that defines the logic to compute and set the user disable state.

  This attribute contains the following attributes:

  `property` attribute. The property to check. The value must be listed in the `properties` attribute for the `componentInterface` object.

  `trueValue` attribute. A value that indicates the user is disabled.

  `falseValue` attribute. A value that indicates the user is enabled.

- `supportedObjectTypes` attribute. A list of supported resource object types. Each object defines a set of features.

  `features` attribute. A list supported features. Possible feature types include view, get, list, find, create, saveas, update, rename, and delete.

Default Component Interfaces Supported

The default Component Interface configuration object defines the following interfaces:

- USER_PROFILE. Performs create, read, and update actions. See USER_PROFILE Component Interface.
- DELETE_USER_PROFILE. Deletes user accounts. See DELETE_USER_PROFILE Component Interface.

USER_PROFILE Component Interface

The default USER_PROFLE component interface definition is used to perform create, read, and update actions. The `key` and `findKey` attributes are set to UserID, because the USER_PROFILE component interface assigns the UserID field for the GETKEYS and FINDKEYS keys.

The default definition for the USER_PROFILE component interface does not define all of the possible properties. It has been simplified to include those used in the sample user form. If you need to add more resource user attributes to the Account Attributes page, then the component interface definition must be updated first. A resource user attribute cannot be added to that page unless it is listed in the component interface definition.

Most properties are defined in USER_PROFILE are simple objects. However, the IDTypes and Roles objects are collections and can have multiple values. IDTypes contains a collection of its own, Attributes. These objects must include the `isCollection` attribute, the key name for the collection, and at least one property.

> **See Also:**
>
> Configuring the Target System for Provisioning

DELETE_USER_PROFILE Component Interface

The DELETE_USER_PROFILE component interface definition is used to delete user profile definitions. The OPRID key determines which user profile is to be deleted. Since the component interface does not have properties, none are listed in the definition.

Customizing PeopleSoft Component Interface Resource Objects

The PeopleSoft Component Interface map definition file can be edited so that resource objects can be managed. Use a text editor to add an `ObjectType` element to the definition file. For example, to add support for the Role resource object, add an `ObjectType` element similar to the following example:

```
<ObjectTypes>
<ObjectType name='Role' icon='role'>
   <ObjectFeatures>
      <ObjectFeature name='find'/>
   </ObjectFeatures>
   <ObjectAttributes idAttr='ROLENAME' displayNameAttr='ROLENAME'
descriptionAttr='DESCR'>
      <ObjectAttribute name='ROLENAME' type='string'/>
      <ObjectAttribute name='DESCR' type='string'/>
      <ObjectAttribute name='ROLESTATUS' type='string'/>
   </ObjectAttributes>
</ObjectType>
</ObjectTypes>
```

The `ObjectType` name (for example, Role) must match the name of one of the objects in the `supportedObjectTypes` list of exactly one component interface definition. Each

`ObjectFeature` (for example, find) must have a corresponding feature in the `features` list in that same `supportedObjectTypes`. The matched component interface is used to perform the resource feature. If there are multiple matches, the first one found will be used.

The following example is part of the component interface definition for the ROLE_MAINT component interface in the component interface map. Note that the Object name Role is found and that an item in the features list is named find.

```
<Attribute name='supportedObjectTypes' >
   <List>
      <Object name='Role'>
         <Attribute name='features' >
            <List>
               <Object name='find' />
               <Object name='get' />
            </List>
         </Attribute>
      </Object>
   </List>
</Attribute>
```

5
Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. The installation media includes a testing utility to test connector operations.

> **Note:**
>
> Using the testing utility, you can test connectivity and perform sanity tests on basic connector operations.The testing utility does not support functions such as validation, transformation, resource exclusion, multiple-version support, and remote connector server.

This chapter discusses the following topics related to connector testing:

- Testing Reconciliation
- Testing Provisioning
- Troubleshooting

Testing Reconciliation

The 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 on the installation media. See Files and Directories on the Installation Media for more information.

To run the testing utility for reconciliation:

1. Open and edit the test/config/reconConfig.properties file as follows:
   a. 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
      ```

   b. 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 path and file name that you specify.

c. Enter a value for the MessageType. For a ping message, specify `Ping, None,` or `otherwise` as shown in the following example:

```
MessageType=None
```

d. Enter a value for **ITResourceName.** This value must match the active IT resource in Oracle Identity Manager.

For example:

```
ITResourceName=PSFT User
```

e. Enter the name of the message for which you are run the testing utility.

For example:

```
MessageName=USER_PROFILE
```

2. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then include the jrf.jar, jrf-api.jar, and jrf-client.jar files to the classpath.

These JAR files are located in the $*ORACLE_COMMON*/modules/oracle.jrf_11.1.1 .

3. Open a command window, and navigate to the scripts .

You must run the testing utility from the *OIM_HOME*/server/ConnectorDefault/*CONN_HOME*/test/scripts , where *CONN_HOME* is the connector .

For example:

OIM_HOME/server/ConnectorDefault/PSFT_UM_11.1.1.6.0/test/scripts

4. 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.

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.

This section contains the following topics:

- About Testing Provisioning
- Running the Testing Utility for Provisioning

About Testing Provisioning

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.

You must ensure that Oracle Identity Manager is running. You must copy the psjoa.jar file from the *PEOPLESOFT_HOME*/web/psjoa to the *OIM_HOME*/server/ConnectorDefault/PSFT_UM_11.1.1.6.0/test/thirdparty .

Running the Testing Utility for Provisioning

To run the testing utility for provisioning:

1. Create the wlfullclient.jar file by using the WebLogic JarBuilder Tool. See Oracle WebLogic Server documentation for more information.
2. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then include the jrf.jar, jrf-api.jar, and jrf-client.jar files to the classpath.

   These JAR files are located in the $*ORACLE_COMMON*/modules/oracle.jrf_11.1.1 .
3. Modify the attributes of the config.properties file using the values specified in the following table. This file is located in the config on the installation media. Table 5-1 describes each property:
4. After you specify values in the config.properties file, run the PeoplesoftProvisioningTester.sh or PeoplesoftProvisioningTester.bat file. This file is located in the test/scripts on the installation media.

Properties of the config.properties File

Table 5-1 describes each property of the config.properties file.

Table 5-1 Properties of config.properties File

Property	Description	Default Value
ACTION	Action that you want the testing utility to perform. You can enter one of the following values: `CONNECT, CREATE, DELETE, ENABLE, DISABLE, UPDATEUSER, UPDATEPASSWORD`	`CONNECT`
LOG LEVEL	Logging level of the testing utility. You can enter one of the following values: `OFF, INFO, FINE`	`OFF`
IT_RESOURCE_NAME	Name of the IT resource that the testing utility must use	`PSFT User`
Oracle Identity Manager login properties:		
SECURITY AUTH LOGIN CONFIG FILE	Configuration file for security authorization	`../../../../config/authwl.conf`

Table 5-1 (Cont.) Properties of config.properties File

Property	Description	Default Value
OIM CONNECTION URL	URL to connect to Oracle Identity Manager	`t3://localhost:8003`
CONTEXT FACTORY	Path to the WebLogic context factory	`weblogic.jndi.WLInitialContextFactory`
OIM ADMIN USER	Admin user ID to log into Oracle Identity Manager Sample value: `xelsysadm`	NA
Attributes:	Enter Create User and Update User data that must be set during the test provisioning operation:	
USERID	User ID	NA
USERIDALIAS	User ID alias	NA
ALTERNATEUSERID	Alternate User ID	NA
SYMBOLICID	Symbolic ID	NA
LANGUAGECODEENG	Language Code	NA
CURRENCYCODE	Currency Code	NA
NAVIGATORHOMEPERMISSIONLIST	Navigator Home Permission List	NA
MULTILANGUAGEENABLED	Multi-language enabled or disabled	`0`
PRIMARYPERMISSIONLIST	Primary Permission List	NA
PROCESSPROFILEPERMISSIONLIST	Process Profile Permission List	NA
REASSIGNWORK	Reassign Work	NA
REASSIGNUSERID	Reassign User ID	NA
ROWSECURITYPERMISSIONLIST	Row Security Permission List	NA
SUPERVISINGUSERID	Supervising User ID	NA
USERDESCRIPTION	User Description	NA
EFFECTIVEDATEFROM	Effective Date From	NA
EFFECTIVEDATETO	Effective Date To	NA
EXPERTENTRY	Expert Entry	NA
WORKLISTUSER	Worklist User	NA
EMPLID	Employee ID	NA
VENDOR ID	Vendor ID	NA
VENDOR SET ID	Vendor Set ID	NA
CUSTOMER ID	Customer ID	NA
CUSTOMER SET ID	Customer Set ID	NA
PRIMARY EMAIL TYPE	Primary Email Type	`WORK`

Table 5-1 (Cont.) Properties of config.properties File

Property	Description	Default Value
WORK EMAIL	Work Email Sample value: `abcd@work.com`	NA
BUS EMAIL	Business Email Sample value: `abcd@bus.com`	NA
HOME EMAIL	Home Email	NA
BB Email	BB Email Type, in 1~EMAILTYPE format	NA
OTH Email	Other Email	NA
ROLES	Roles	NA

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 2-3 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	• Ensure that the target system-specific psjoa.jar file is present in the connector bundle, in the *OIM_HOME*/server/ConnectorDefault/PSFT_UM_11.1.1.6.0/test/lib .
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 2-3 for more information. It should contain the correct host name and port.

Problem Description	Solution

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

You might receive one of the following error messages:
`Exception:`
`org.identityconnectors.framework.common.exceptions.ConnectorException:`
`Cannot connect to peoplesoft :`
`PeopleTools release (8.51.02) for web server '' is not the same as Application Server PeopleTools release (8.50.10).`
`Access denied. at org.identityconnectors.peoplesoft.common.SessionWrapper.connect(SessionWrapper.java:65)`
 	
`org.identityconnectors.framework.server.impl.ConnectionListener processOperationRequest`
`SEVERE: Cannot connect to peoplesoft :`
`Failed to deserialize GetCertificate request data`
`org.identityconnectors.framework.common.exceptions.ConnectorException: Cannot connect to peoplesoft : Failed to`
`deserialize GetCertificate request data`
	You must ensure the psjoa.jar version is correct. It should be specific to the PeopleTools version.

Problem Description	Solution

You might receive the following error message:
 	
`Exception:`
` Running CREATEUSERTarget Class =`
`oracle.iam.connectors.icfcommon.prov.ICPr`
`ovisioningManager`
`<Aug 23, 2011 3:58:43 AM PDT>`
`<Error><ORACLE.IAM.CONNECTORS.ICFCOMMON.PROV`
`.IC`
`PROVISIONINGMANAGER> <BEA-000000>`
`<oracle.iam.connectors.icfcommon.prov.IC`
`ProvisioningManager : createObject :`
` Error while creating user`
`oracle.iam.connectors.icfcommon.exception`
`s.IntegrationException: Can't read from`
`URL[file:///path/to/PeopleSoftComponentIn`
`terfaces.xml] at`
`oracle.iam.connectors.icfcommon.service.o`
`im9.OIM9Configuration$ConfigurationHandle`
`r$LoadFromURLTagHandler.handle`
` (OIM9Configuration.java:412)`
	You must ensure you provide the correct path to the PeopleSoftComponentInterfaces.xml file in the Lookup.PSFT.Configuration lookup.

Problem Description	Solution

You might receive the following error message while provisioning Employee ID, Vendor Set ID, or Customer Set ID:
 	
`Exception:`
` <Aug 24, 2011 2:07:15 AM PDT> <Error>`
`<ORACLE.IAM.CONNECTORS.ICFCOMMON.PROV.ICP`
`ROVISIONINGMANAGER>`
`<BEA-000000><oracle.iam.connectors.icfcommon`
`.prov.ICP`
`rovisioningManager : createObject : Error`
` while creating user`
`org.identityconnectors.framework.common.e`
`xceptions.ConnectorException:Cannot create`
`user at`
`org.identityconnectors.peoplesoft.compint`
`fc.PeopleSoftCompIntfcCreateOp.create`
`(PeoplesoftCompIntfcCreateOp.java:120) at`
`org.identityconnectors.peoplesoft.compint`
`fc.PeopleSoftCompIntfcConnector.create`
` (PeopleSoftCompIntfcConnector.java:126)`
`....`
`..`
`at weblogic.servlet.internal.WebAppServletCo`
`ntext.execute(WebAppServletContext.java:2`
`183)at`
`weblogic.servlet.internal.ServletRequestI`
`mpl.run(ServletRequestImpl.java:1454)at`
`weblogic.work.ExecuteThread.execute(Execu`
`teThread.java:209)at`
`weblogic.work.ExecuteThread.run(ExecuteTh`
`read.java:178)Caused By:`
`psft.pt8.joa.JOAException:`
` Error invoking method [Save]Message`
`item[0] : (2,104) : Field does`
` not exist -- PSOPRALIAS.. (2,104)`
` PSOPRALIAS_WRK.ATTRVALUE.FieldChange`
`PCPC:2067  Statement:22Message item[1] :`
`(91,34) : Error`
` changing value.`
`{USER_PROFILE.IDTypes(1).Attributes(2).At`
`tributeValue} (91,34)Message item[2] :`
`(0,0) : Failed to`
` execute PSBusComp requestat`
`org.identityconnectors.peoplesoft.common.`
`InterfaceWrapper.handleMethodResult`
`(InterfaceWrapper.java:134)....`
	To resolve this issue:
	
	1. Verify the PeopleSoft target system for the EmplID attribute name in the USER_PROFILE component interface.
	
	Depending on the version of PeopleSoft, the attribute name will be **EmplID** or **Empl ID.**
	
	Similarly, for Vendor Set ID and Customer Set ID, the attribute name will be **Set ID** or **SetID.**
	
	2. Update the entry in the Lookup.PSFT.UM.ProvAttrMap lookup with the attribute name that you verified in the preceding step.
	
	For example, if the attribute name is EmplID in PeopleSoft, update the decode value for Employee ID to:
	
	`IDTypes~UM_IDTypes[IDType=EMP]~Att`
	`ributes~UM_Attributes[AttributeNam`
	`e=EmplID]~AttributeValue`
	
	3. If required, perform the preceding step for the Set ID decode value for Vendor Set ID or Customer Set ID.

Problem Description	Solution
The following issue is observed if the JDK version used by Oracle Identity Manager has been changed from 1.7 to an earlier version: Provisioning operation fails and an error is displayed.	To fix the issue, recompile all the adapters by performing the following procedure: 1. Login to the Oracle Identity System Design Console. 2. Expand **Development Tools** and click on **Adapter Manager.** 3. Select Compile All, and click the **Start** button. 4. Ensure that the status for all the adapters is OK.
You might receive the following error message: `org.identityconnectors.framework.common.exceptions.ConnectorException: Cannot connect to peoplesoft : DOWNbea.jolt.ServiceException: Invalid Session`	You must apply Patch 18391274 and retest the provisioning operation. To obtain the patch, go to following URL, click **Patches and Updates**, and search for the patch number: `https://support.oracle.com/`
User target delete reconciliation fails on Oracle Identity Manager Release 2 and any later BP in this release track.	You must set the following values for the various fields in the Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping and Lookup.PSFT.UM.DeleteUserProfile.Recon lookup definitions: • In the Lookup.PSFT.UM.DeleteUserProfile.AttributeMapping lookup definition, set `Return ID` as the value for the Code Key variable and `OPRID~PRG_USR_PROFILE~None~None~PRIMARY` for Decode. • In the Lookup.PSFT.UM.DeleteUserProfile.Recon lookup definition, set `Return ID` as the value for the Code Key and Decode variables. Additionally, perform the following procedure: 1. Login to the Design Console. 2. Expand **Process Management** and double-click **Process Definition.** 3. Search for and open the **Peoplesoft User Management** process definition. 4. Navigate and open the **User ID** window. 5. Select the **Case In-sensitive** option. 6. Click **Save.** Finally, to complete the workaround, re-create a Reconciliation Profile.

Problem Description	Solution
You might receive the following error message: `psjoa compiled version not supported`	You must install Oracle Identity Manager against the latest version of Java 1.7 or above. Alternatively you can install the Connector Server with the latest version of Java 1.7 or above.

6

Known Issues and Workarounds

The following is an issue and workaround associated with this release of the connector:

Oracle Identity Manager Issues

The following is an issue and workaround associated with Oracle Identity Manager:

Unable To Update All ID Type Attributes In a Single Process Form Update

Vendor ID and Vendor Set ID attributes need to be updated together as they are related attributes, and the target system does not allow modifying one attribute, either Vendor ID or Vendor Set ID. When these attributes are updated from Oracle Identity Manager, it triggers one update each for individual attribute, resulting in failure of attributes update.

As a workaround, use Bulk Attribute Propagation to propagate changes for more than one process form attribute to the target in a single task.

A

Determining the Root Audit Action Details

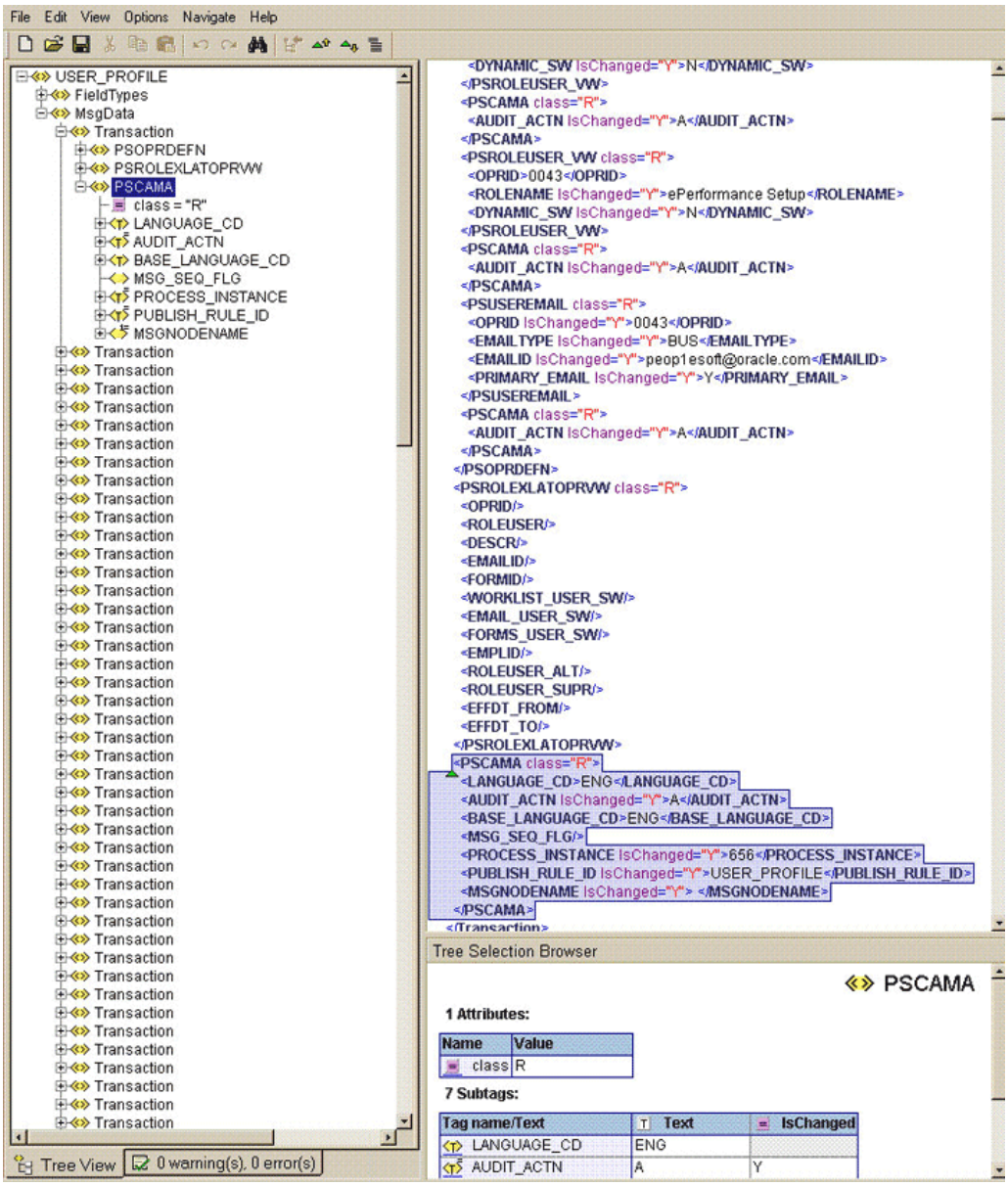
An XML message that is published by PeopleSoft contains a Transaction node. In case of full reconciliation, the XML file for USER_PROFILE message has multiple transaction nodes. However, in case of incremental reconciliation, the XML message has only one transaction node.

This section contains the following topics:

The PSCAMA Subnode

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:

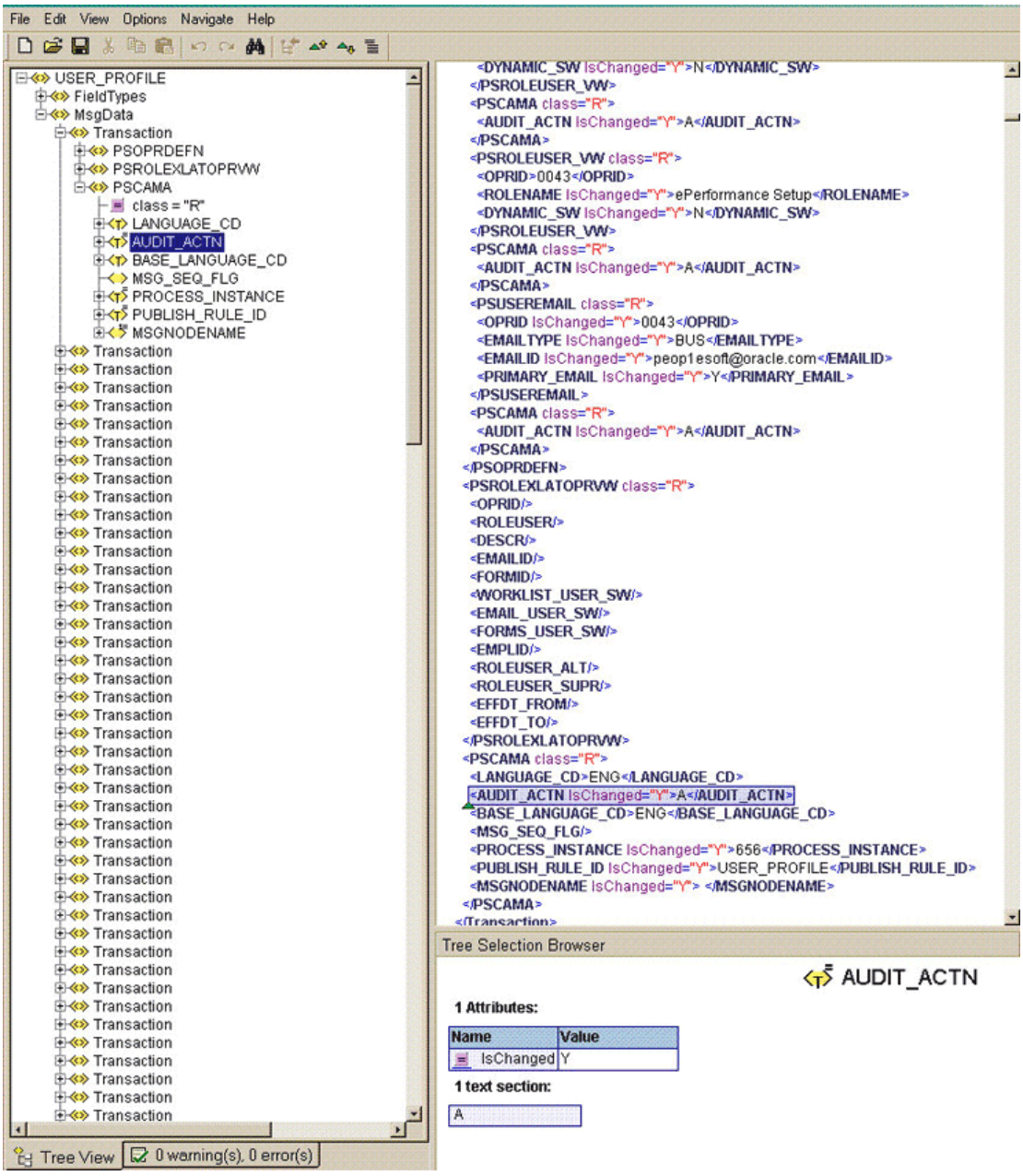
- Language in which the data is written
- Type of transaction the row represents, such as add, update, or delete

When receiving a message, PeopleCode inspects the PSCAMA node for this information and responds accordingly.

The AUDIT_ACTN Subnode

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.

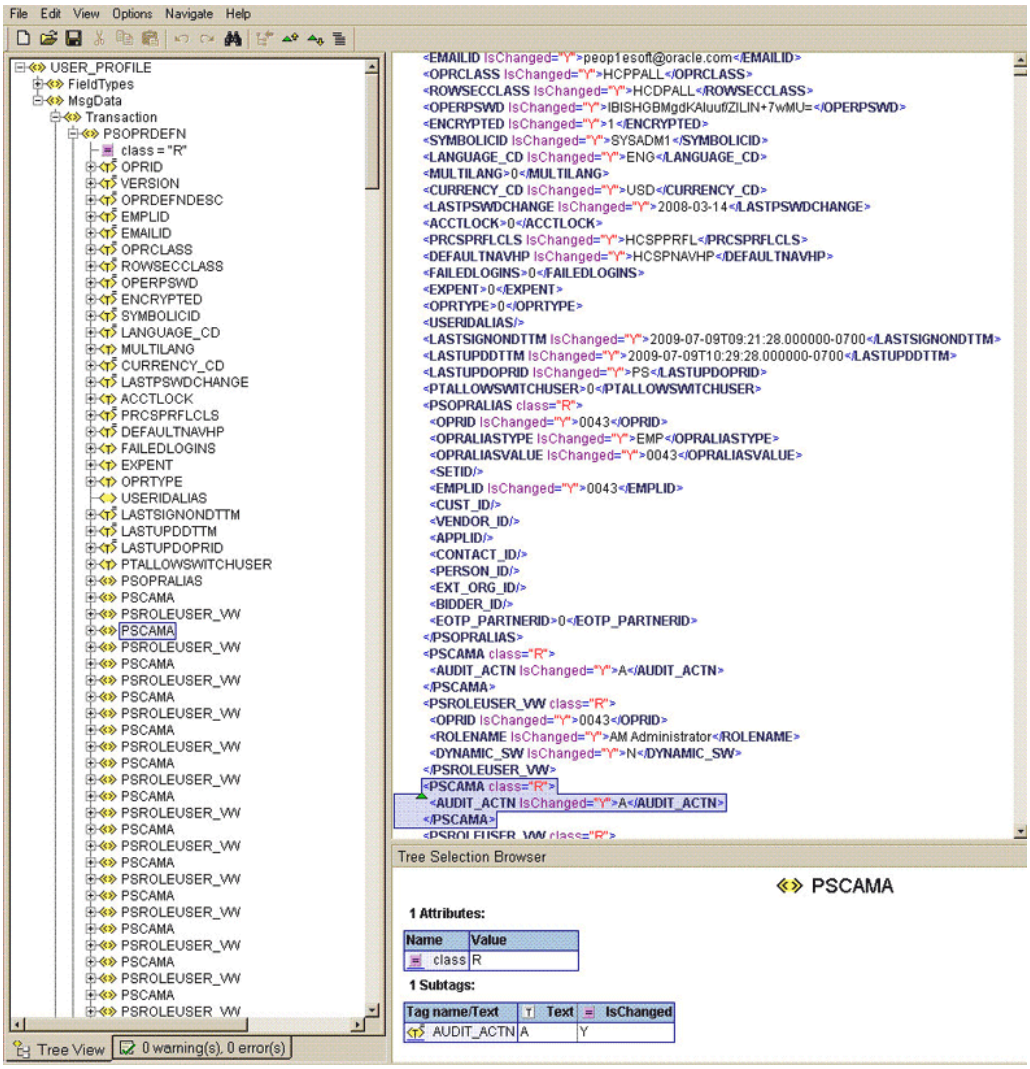
The AUDIT_ACTN node is shown in the following screenshot:



The Root Audit Action

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">IBISHGBMgdKAluuf/ZILIN+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, perform the following steps:

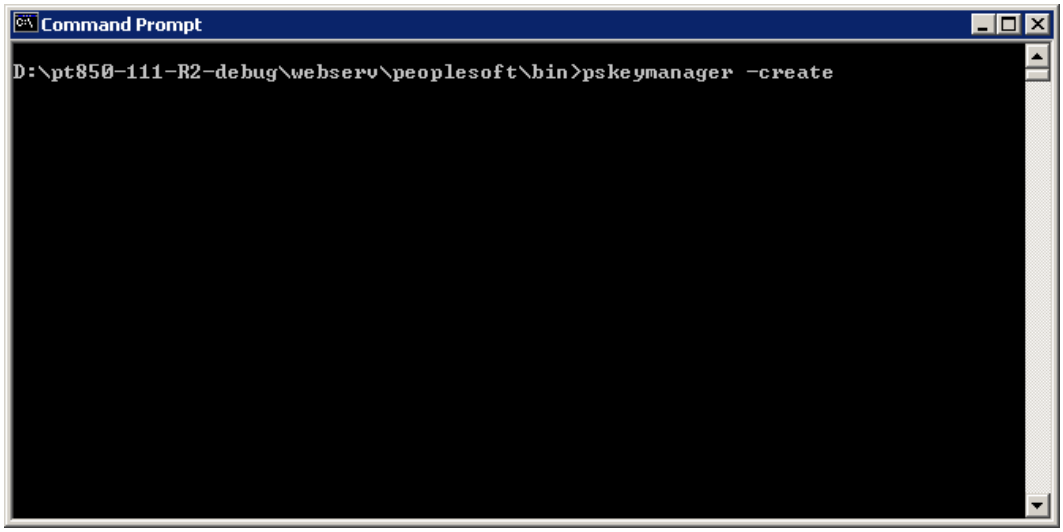
- Generating Signed Public Encryption Key and Certificate Signing Request
- Submitting CSRs to CAs for Signing
- Downloading the Root Certificate
- Importing a Server-Side Public Key into a Keystore
- Generating and Importing Public Keys
- Configuring the Oracle WebLogic Server to Use the Keystore
- Adding Root Certificate
- Configuring the Peoplesoft Certificates

Generating Signed Public Encryption Key and Certificate Signing Request

Generate signed public encryption key and certificate signing request (CSR).

1. Start PSKeyManager by navigating to the appropriate on the MS-DOS command prompt.
2. Enter the following at the command line:

```
pskeymanager -create
```



The PSKeyManager opens.

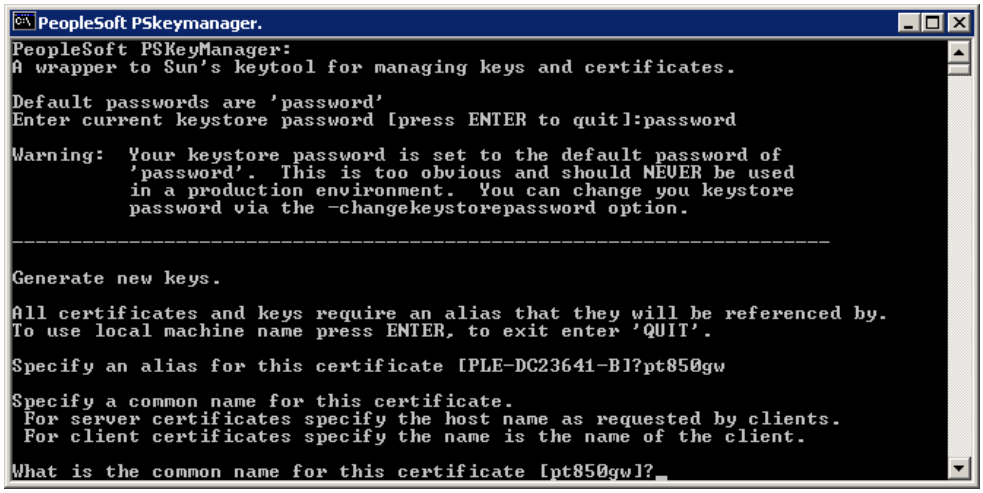
3. Enter the following at the command line:

   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

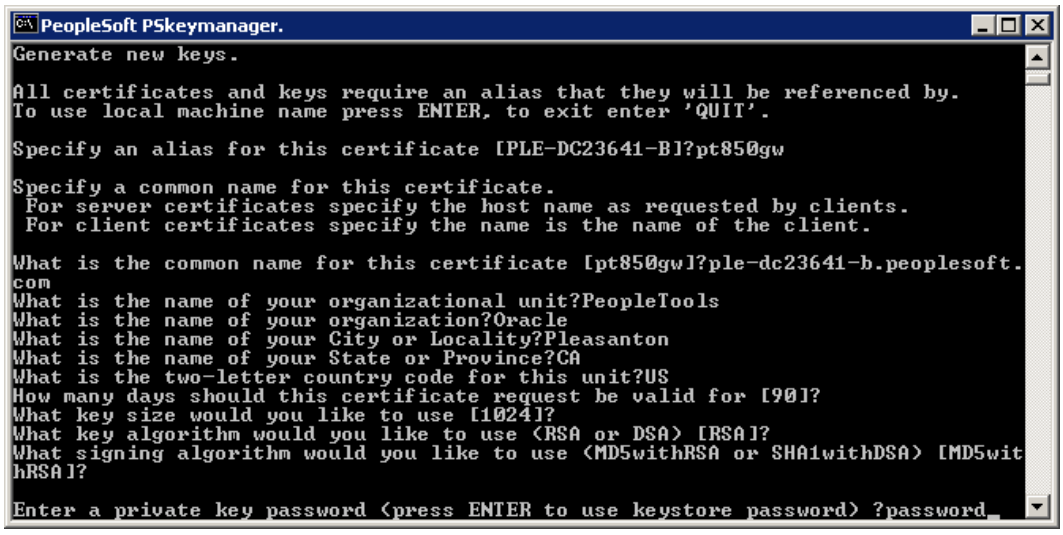
   Number of days the certificate should be valid (Default is 90.)

   Key size to use (Default is 1024.)

   Key algorithm (Default is RSA.)

   Signing algorithm (Default is MD5withRSA or SHA1withDSA.)

4. At the `Enter a private key password <press ENTER to use keystore password>` prompt, specify the password or press **Enter.**

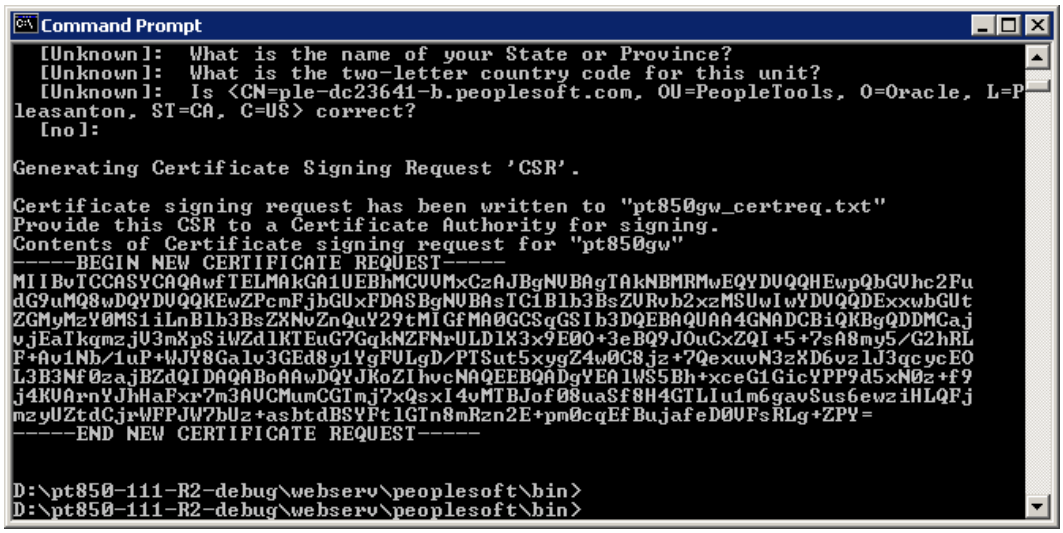


5. Verify that the values you entered are correct, and press **Enter.**

   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-----
MIIBtDCCAR0CAQAwdDELMAkGA1UEBhMCVVMxEDAOBgNVBAgTB0FyaXpvbmExEDAOBgNVBAcTB1Bob2VuaXg
xFDASBgNVBAoTC1Blb3BsZVRvb2xzMRMwEQYDVQQLEwpZW9wbGVzb2Z0MRYwFAYDVQQDEw1NREFXU09OMDU
xNTAzMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC43lCZWxrsyxven5QethAdsLIEEPhhhl7TjA0r8p
xpO+ukD8LI7TlTntPOMU535qMGfk/
jYtG0QbvpwHDYePyNMtVou6wAs2yr1B+wJSp6Zm42m8PPihfMUXYLG9RiIqcmp2FzdIUi4M07J8ob8rf0W+
Ni1bGW2dmXZ0jGvBmNHQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAKx/
ugTt0soNVmiH0YcI8FyW8b81FWGIR0f1Cr2MeDiOQ2pty24dKKLUqIhogTZdFAN0ed6Ktc82/5xBoH1gv7Y
eqyPBJvAxW6ekMsgOEzLq9OU3ESezZorYFdrQTzqsEXUp1A+cZdfo0eKwZTFmjNAsh1kis+HOLoQQwyjgax
YI=
-----END NEW CERTIFICATE REQUEST-----
```



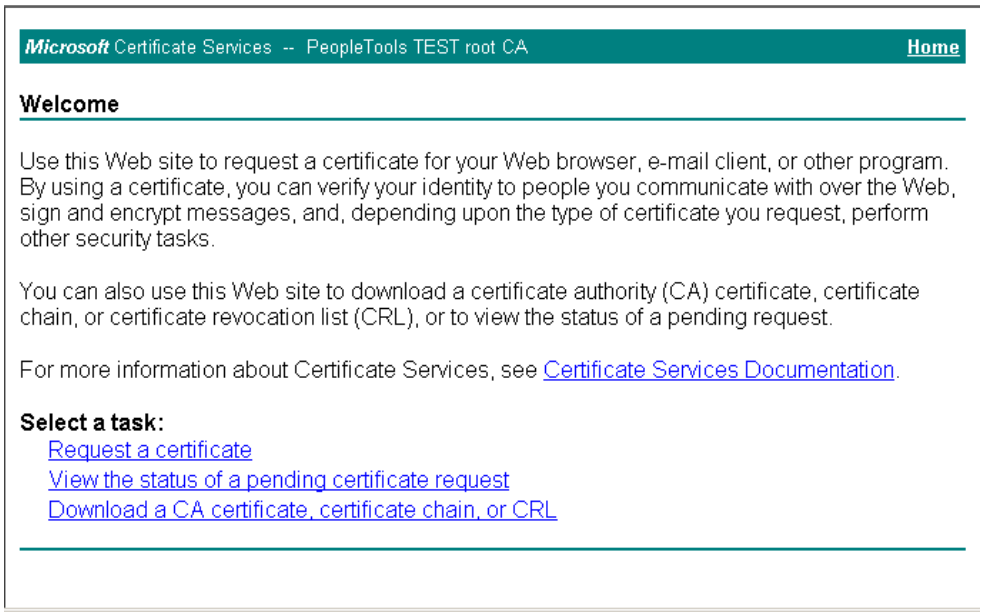
The CSR is a text file, and is written to the <*PSFT_HOME*>\webserv\peoplesoft . The file name is <host_name>_certreq.txt.

Submitting CSRs to CAs for Signing

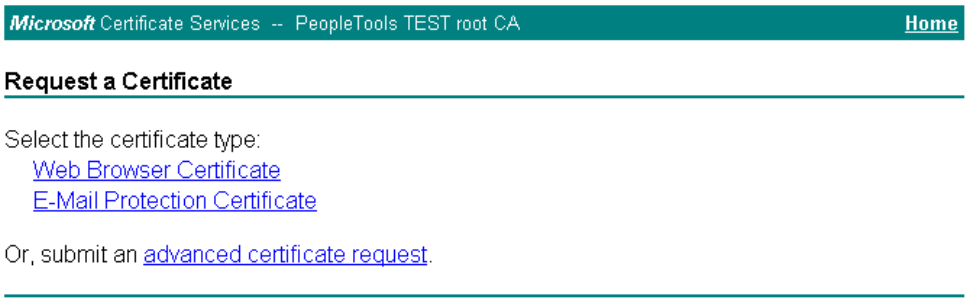
Submit CSRs to CAs for signing:

> **Note:**
>
> The set of pages are different depending on what CA you plan on using.

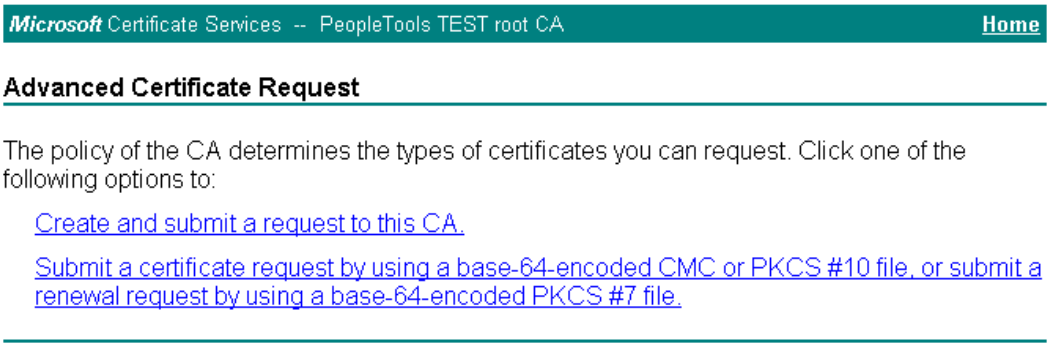
1. Click **Download a CA certificate, certificate chain, or CRL**.



2. Click **advanced certificate request.**

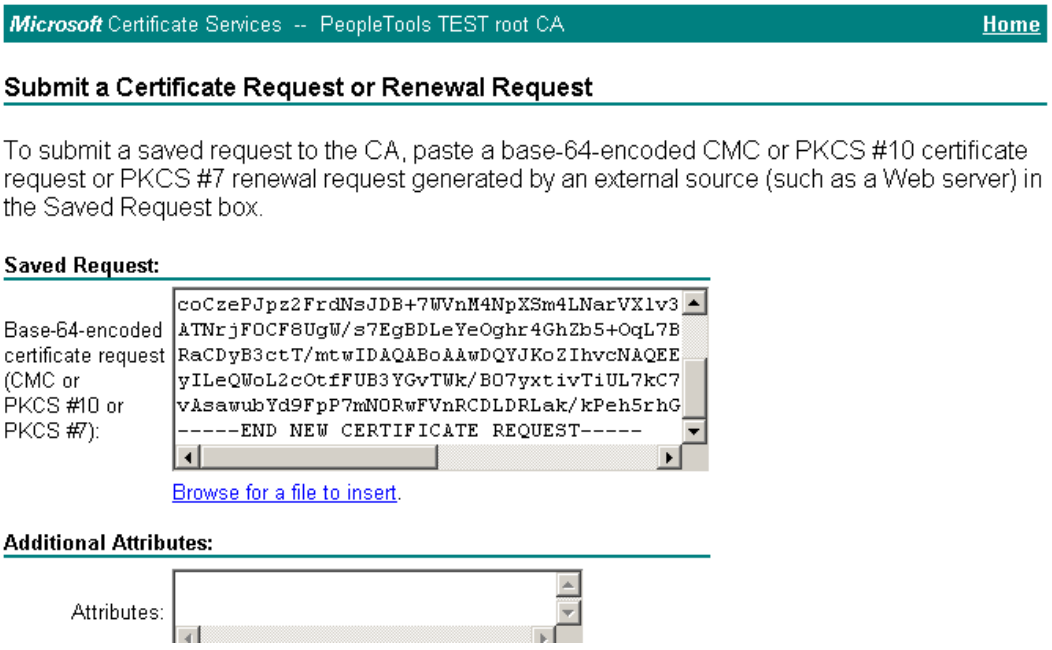


3. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.**



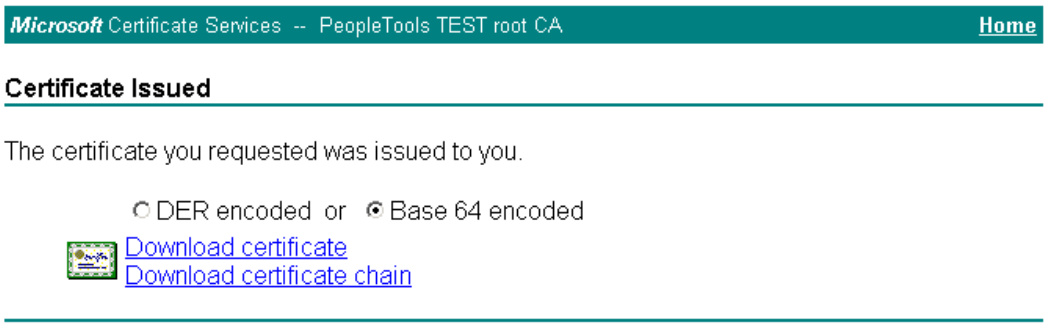
The Submit a Certificate Request or Renewal page appears.

4. 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.

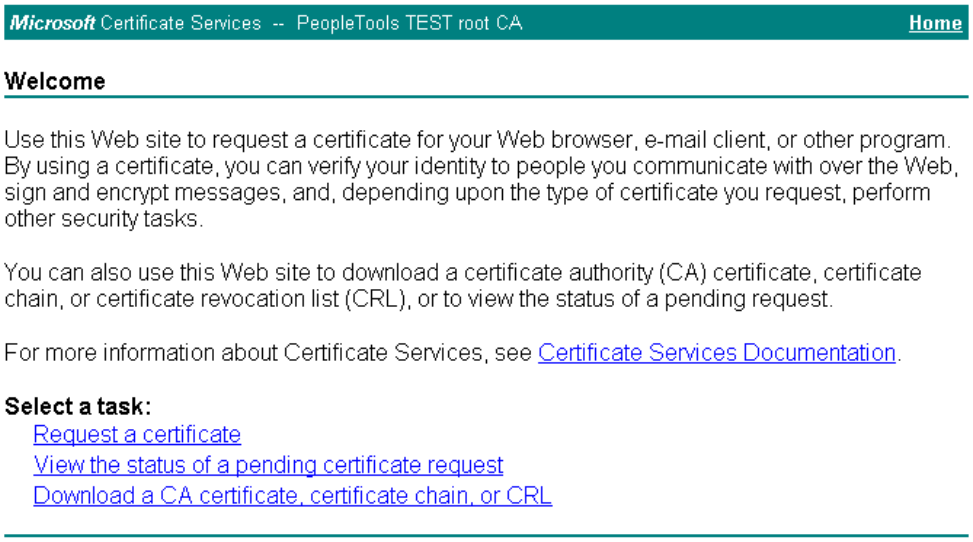
5. Download and save the signed public key on your local drive.



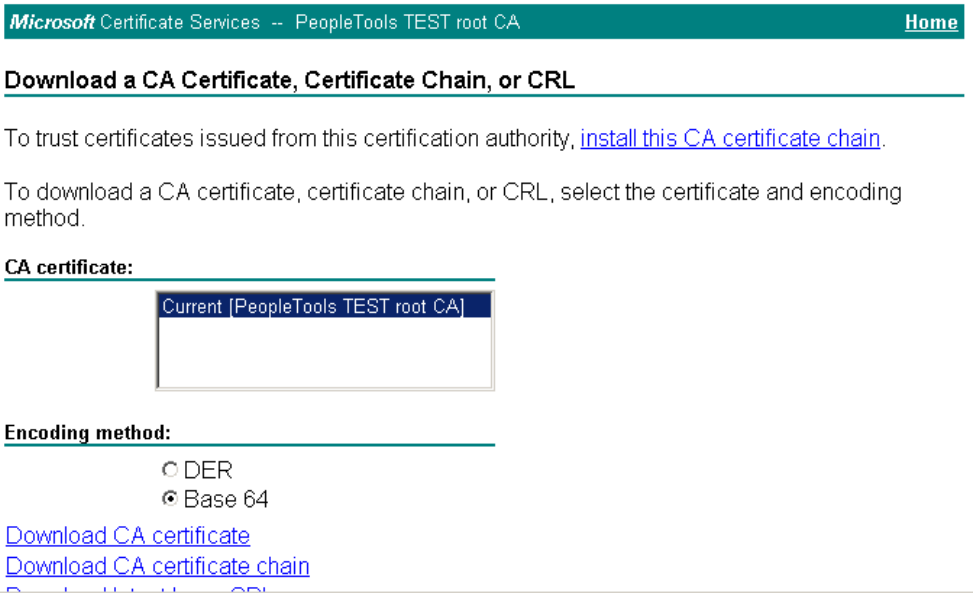
Downloading the Root Certificate

Download the root certificate.

1. Click **Download a CA certificate, certificate chain, or CRL.**



2. From the **CA certificate** list, select the certificate.



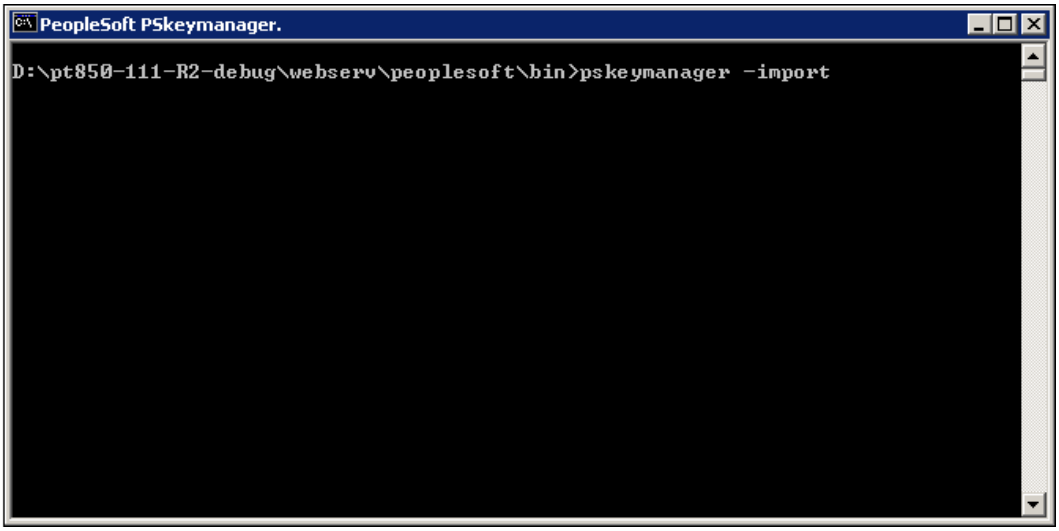
3. Download and save the root certificate on your local drive.

Importing a Server-Side Public Key into a Keystore

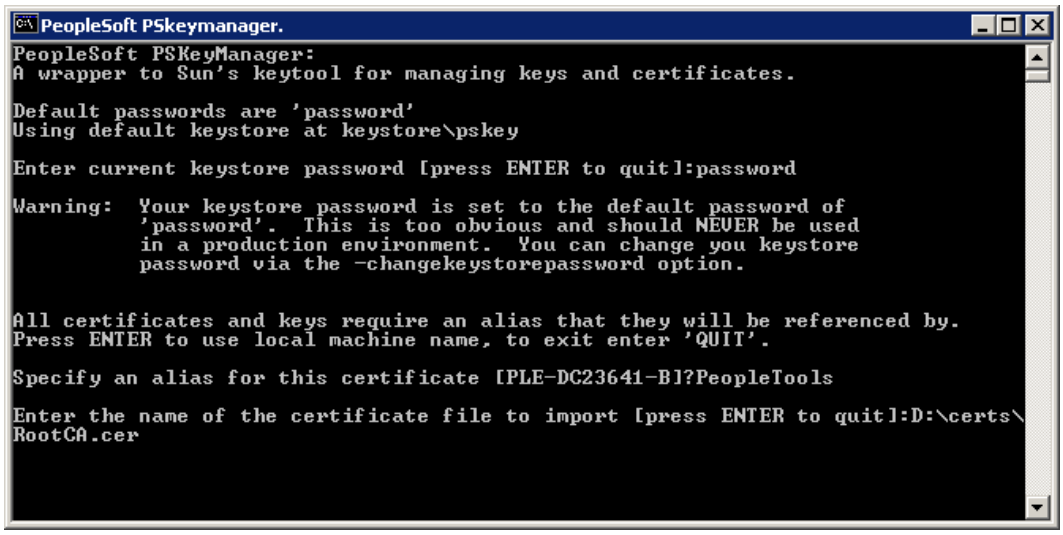
Import a server-side public key into a keystore.

1. Open PSKeyManager.
2. Navigate to the required on the MS-DOS command prompt.
3. Enter the following at the command line:

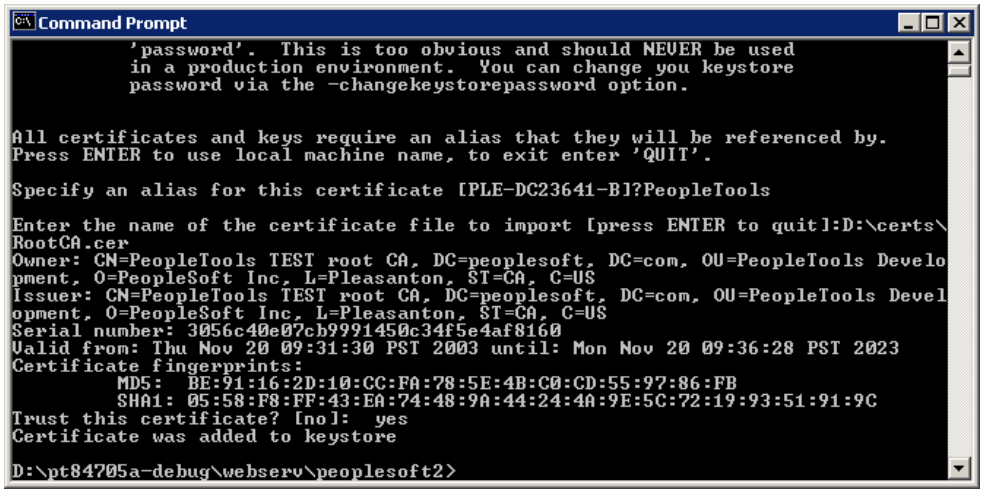
```
pskeymanager -import
```



4. At the `Enter current keystore password` command prompt, enter the password and press **Enter.**
5. At the `Specify an alias for this certificate <host_name>?` command prompt, enter the certificate alias and press **Enter.**
6. At the `Enter the name of the certification file to import` command prompt, enter the path and name of the certificate to import.



7. At the `Trust this certificate` command prompt, enter **Yes** and press **Enter.**



Generating and Importing Public Keys

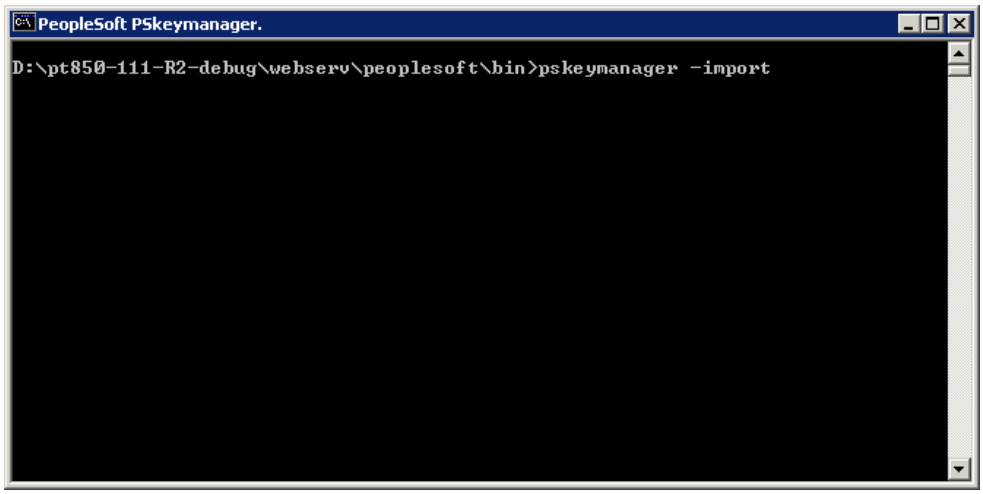
Generate and import public keys.

1. Place the public key from your CA in the keystore. The location of the keystore is as follows:

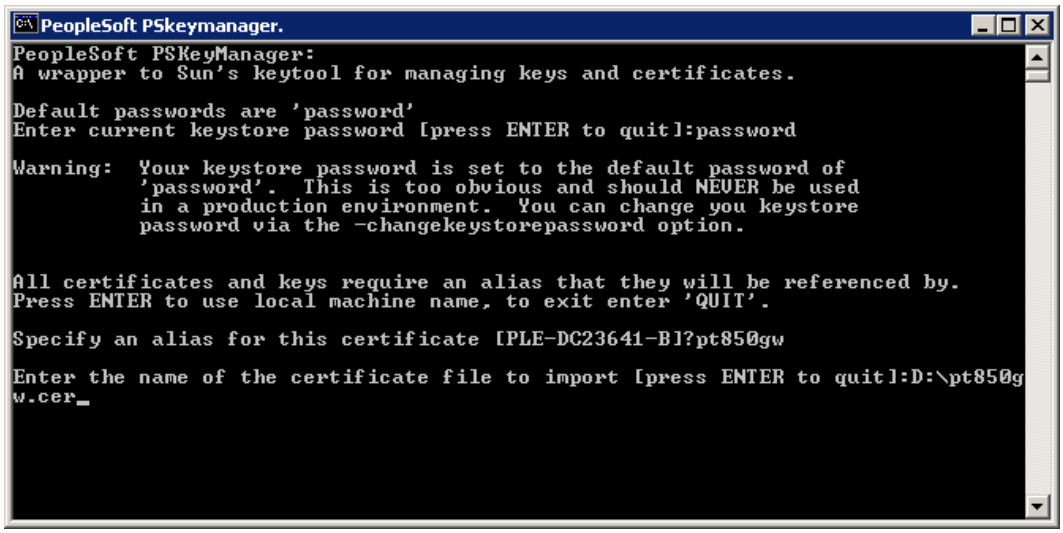
   <PSFT_HOME>\webserv\peoplesoft\keystore

2. Install the certificate for server authentication SSL on Oracle WebLogic Server using the following command:

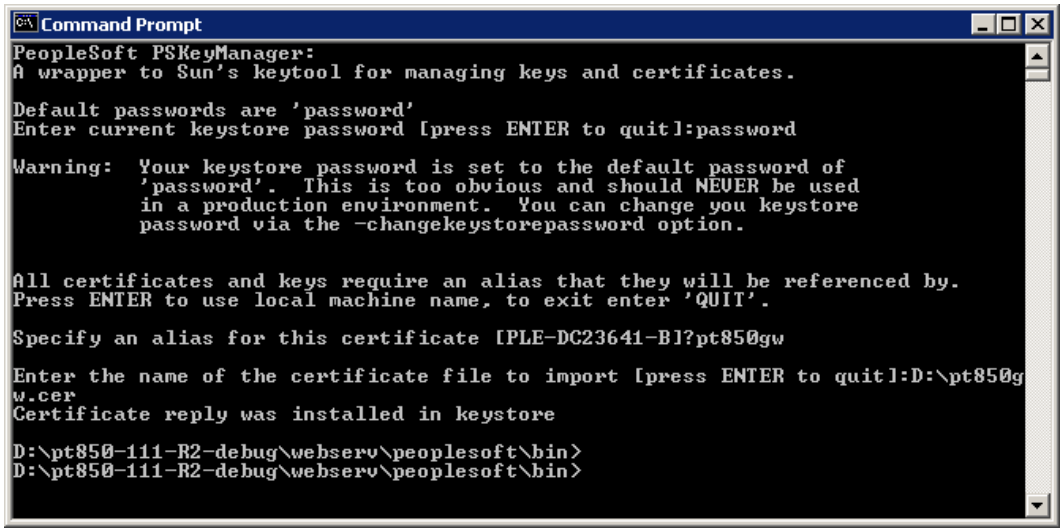
   ```
   pskeymanager -import
   ```



3. At the `Enter current keystore password` command prompt, enter the password and press **Enter.**
4. At the `Specify an alias for this certificate <host_name>?` command prompt, enter the certificate alias and press **Enter.**
5. At the `Enter the name of the certification file to import` command prompt, enter the path and name of the certificate to import.



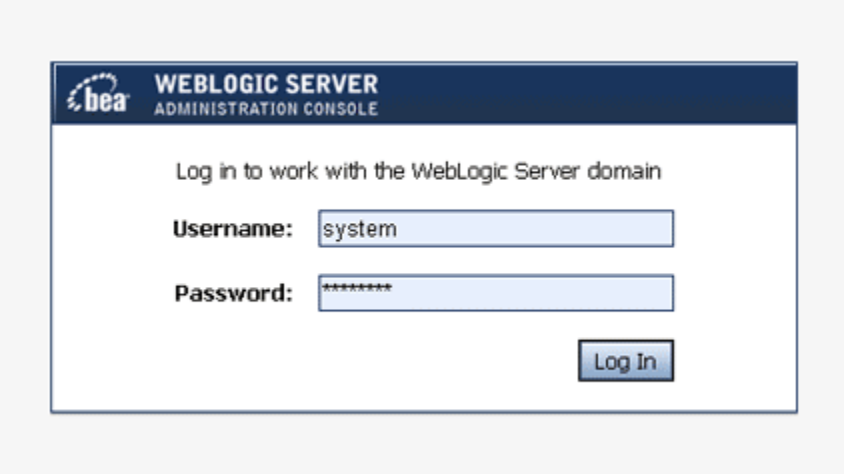
Certificate is successfully installed in the keystore.



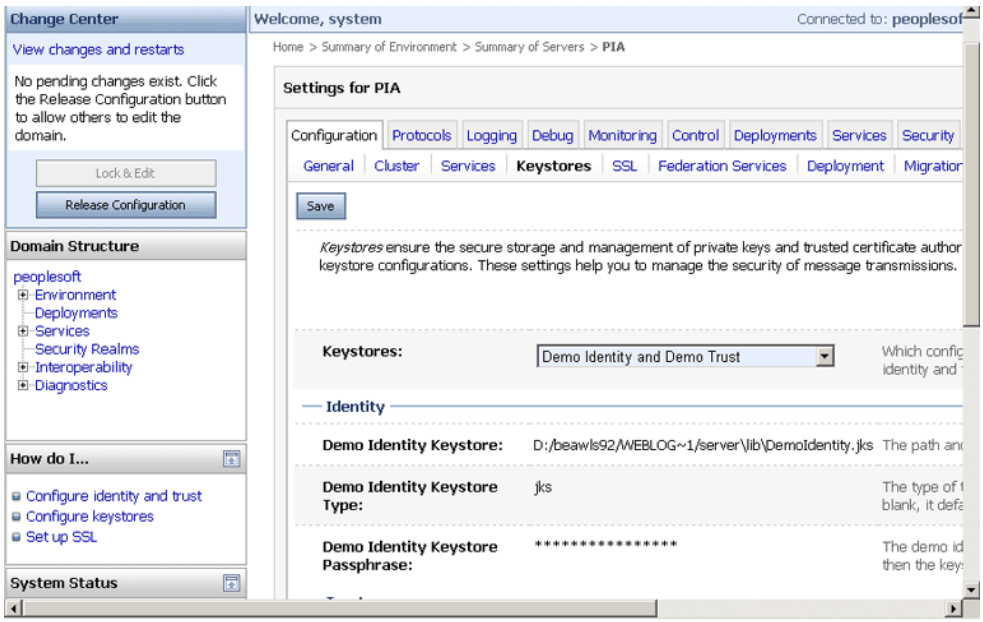
Configuring the Oracle WebLogic Server to Use the Keystore

Configuring the Oracle WebLogic Server to use the keystore.

1. Log in to Oracle WebLogic Administration Console.



2. Expand **PeopleSoft, Environment, Servers, PIA** to setup the SSL configuration for the PIA server.



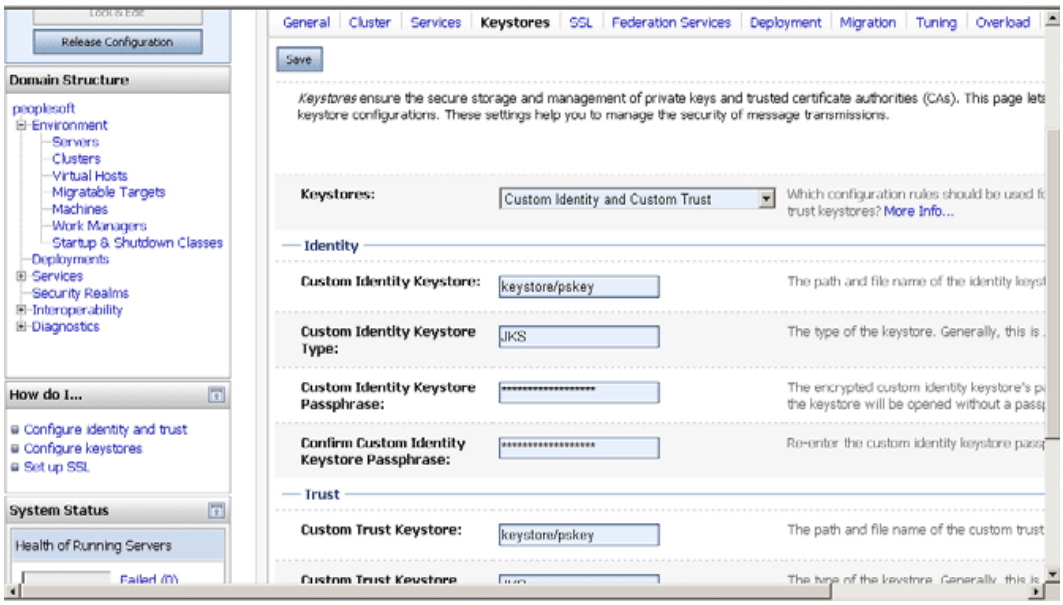
3. Click the **Keystores** tab.
4. From the **Keystores** list, select **Custom Identity and Custom Trust.**
5. In the **Identity** region, complete the following fields:

   - In the Custom Identity Keystore field, enter `keystore/pskey`.

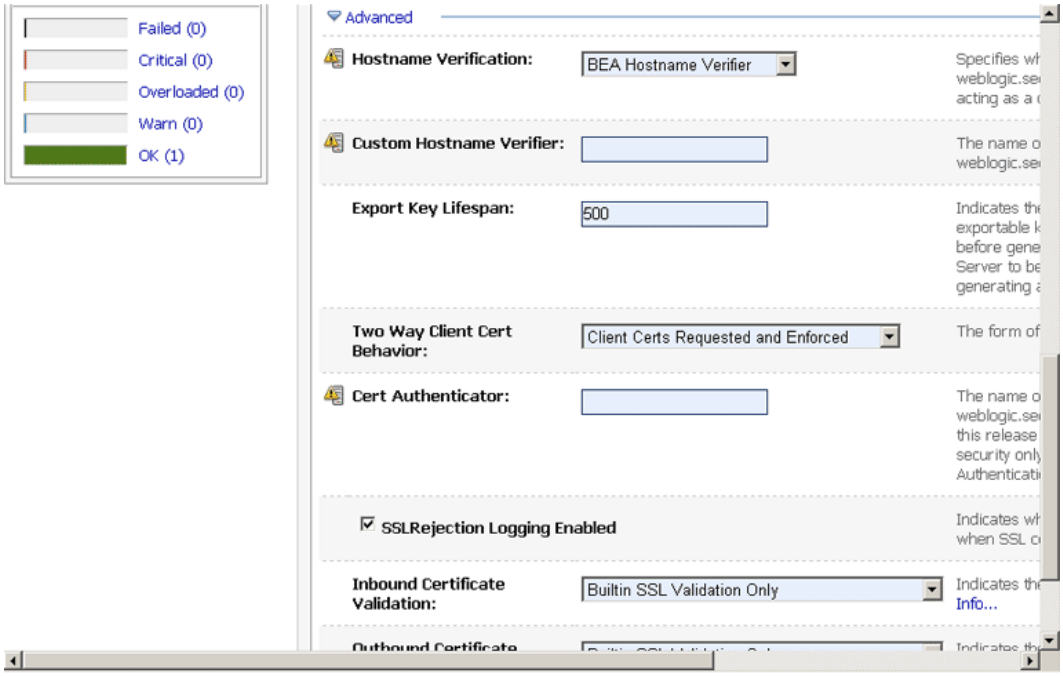
   - In the Custom Identity Keystore Type field, enter `JKS`.

   - In the Custom Identity Keystore Passphrase field, enter `password`.

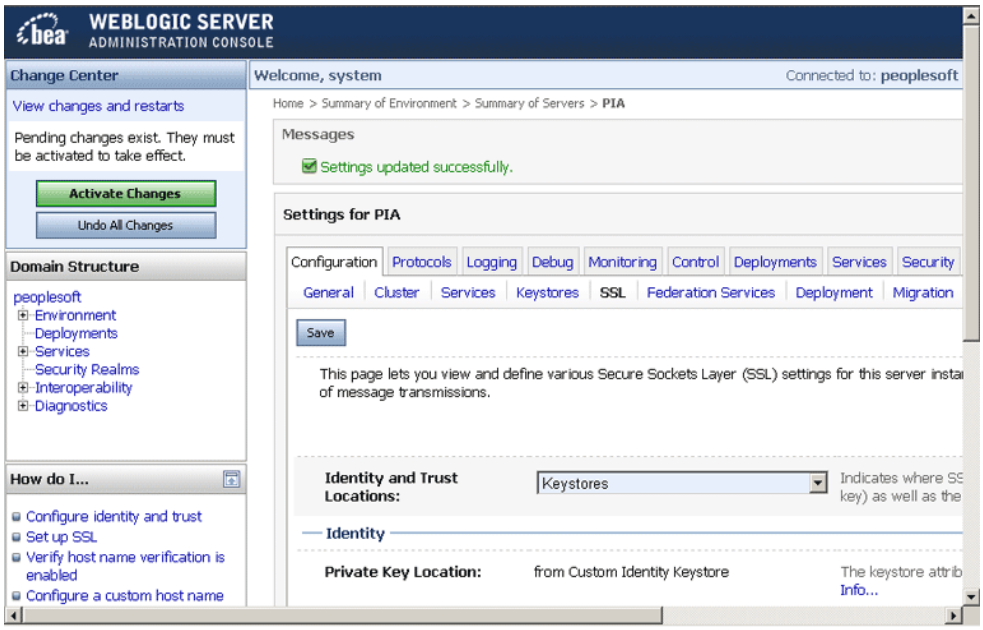
   - In the Confirm Custom Identity Keystore Passphrase field, enter `password` again.



6. On the SSL tab, ensure that the parameter **Two Way Client Cert Behavior** is set to **Client Certs Requested and Enforced.**



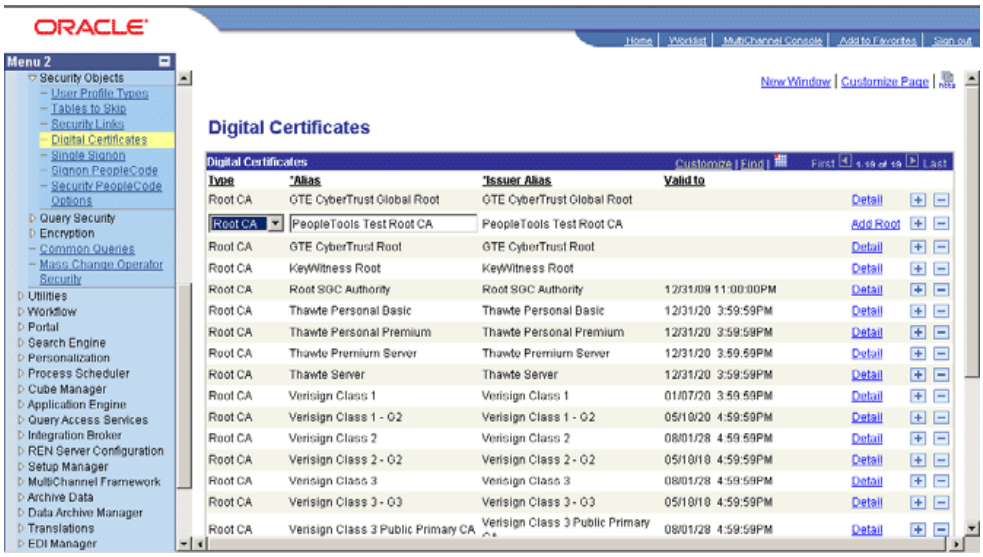
7. Click the **Activate Changes** button.



Adding Root Certificate

Add root certificate.

1. Expand **Security, Security Objects,** and then click **Digital Certificates.**



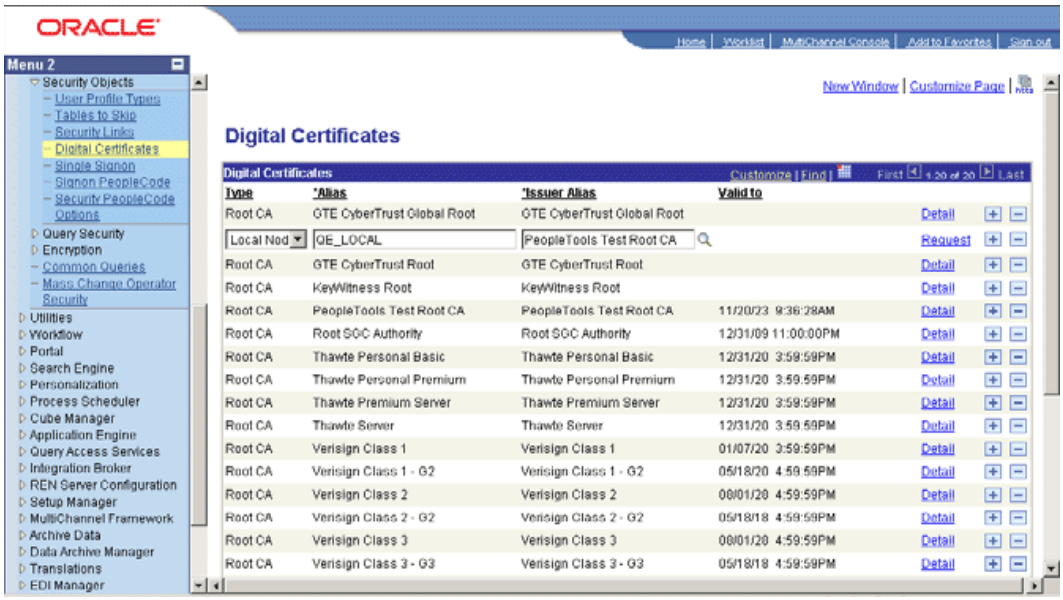
2. Click **Add Root.**

Configuring the Peoplesoft Certificates

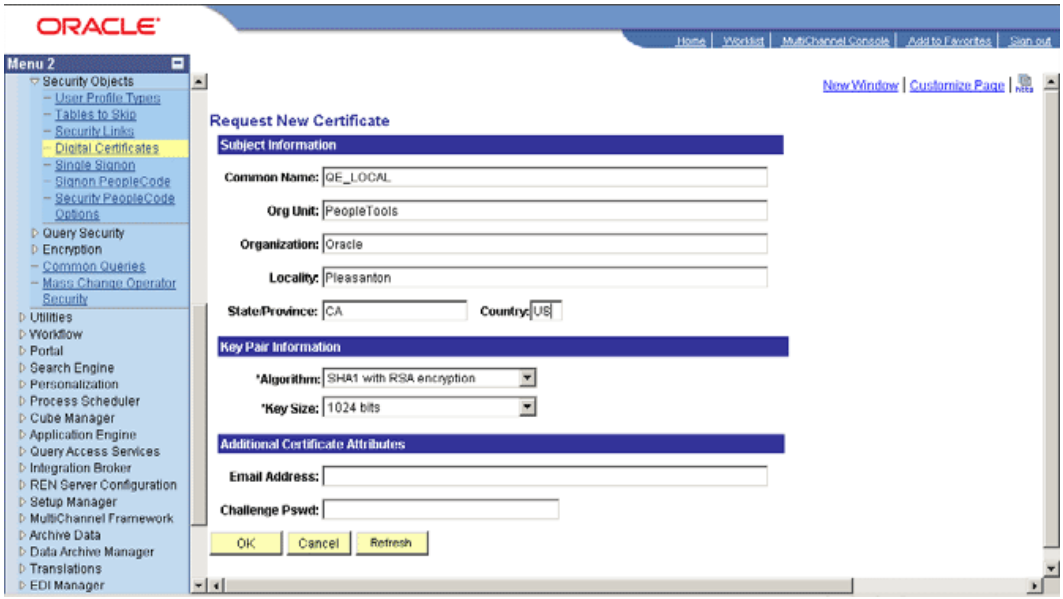
Configure the Peoplesoft certificates.

> **Note:**
>
> You can use the same root certificate generated in Step 2.

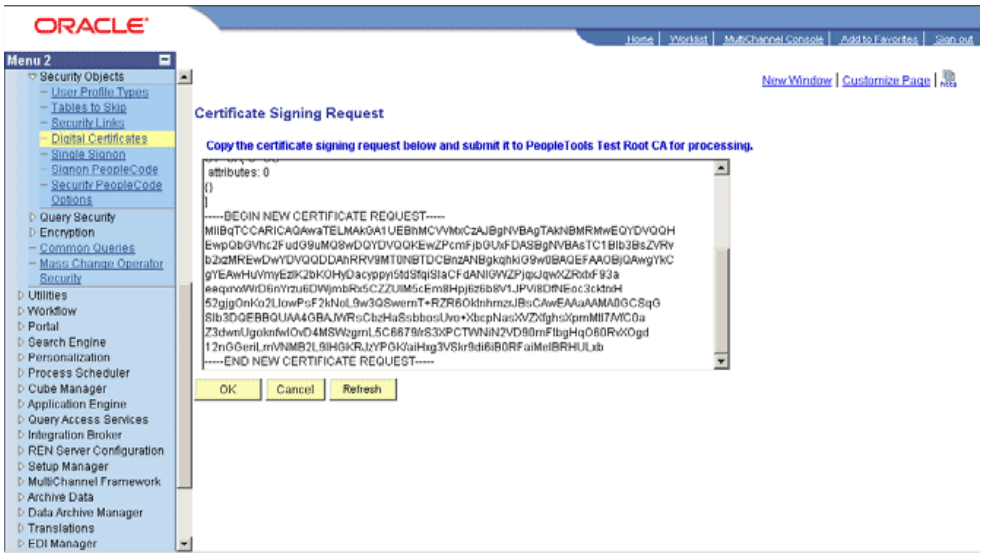
1. Expand **Security, Security Objects,** and then click **Digital Certificates.**
2. Add a local node type certificate.
3. Set **Alias** to the default local node.



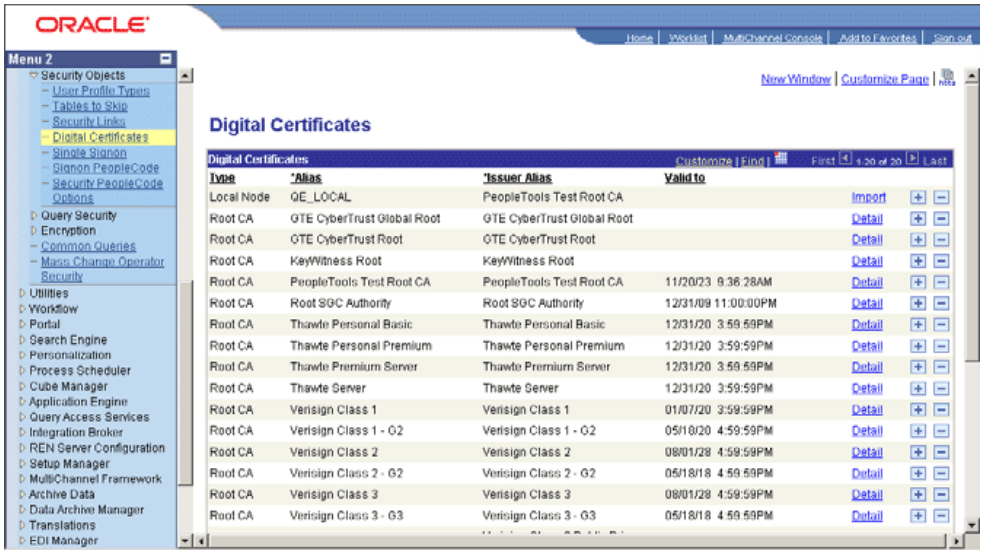
4. Click **Request.**
5. Send this certificate request to the CA to get a new certificate.



6. Click **OK.**

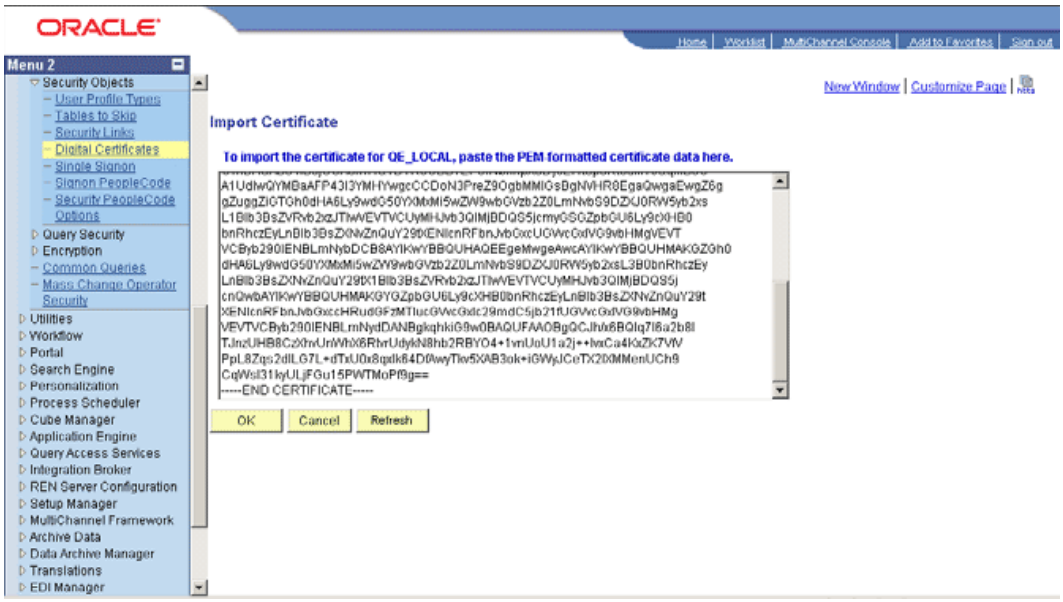


7. Ensure that the local node appears on the Digital Certificates list.

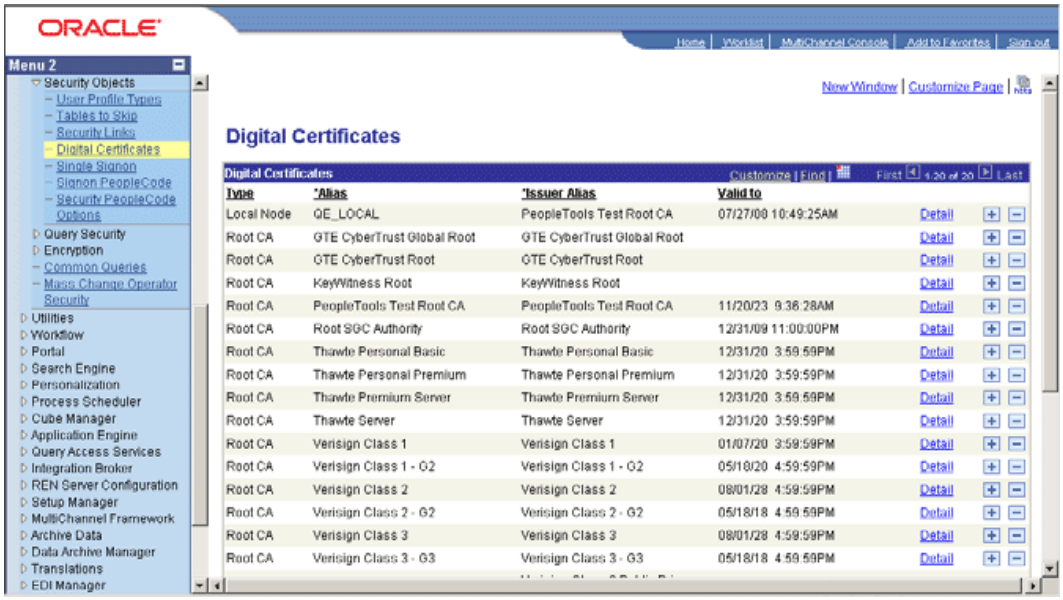


8. Click **Import.**

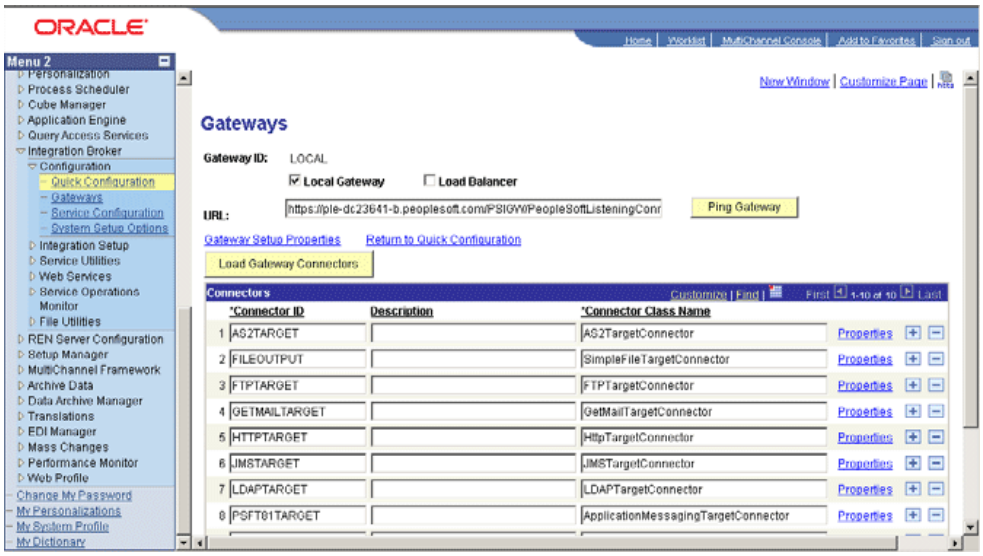
   The Import Certificate page appears.



9. Click **OK.**



10. Click **Load Gateway Connectors.**

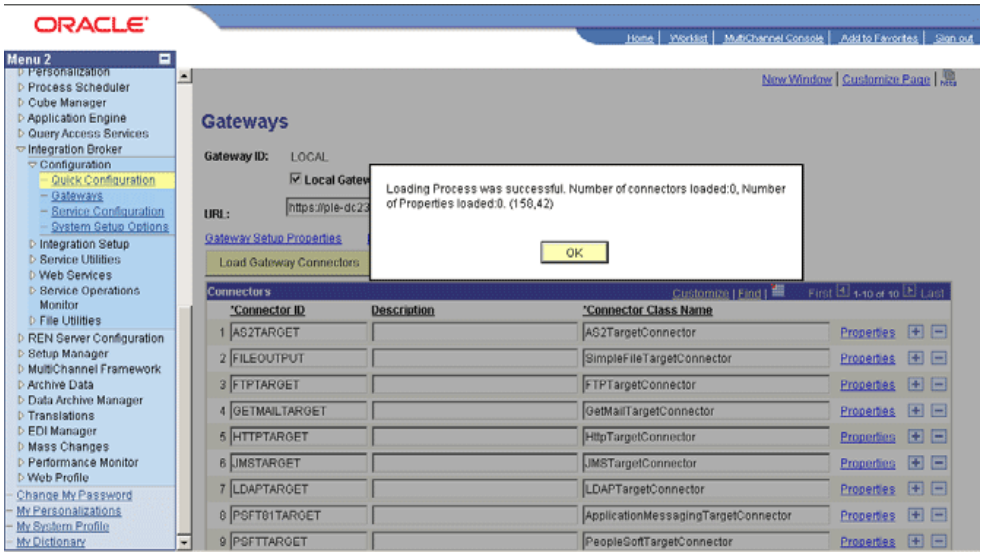


The following message appear:

```
Loading Process was successful. Number of connectors loaded:0. Number of
Properties loaded:0. (158,42)
```

Click **OK.**

11. Click **Ping Node** to ping your local node.



C

Changing Default Message Versions

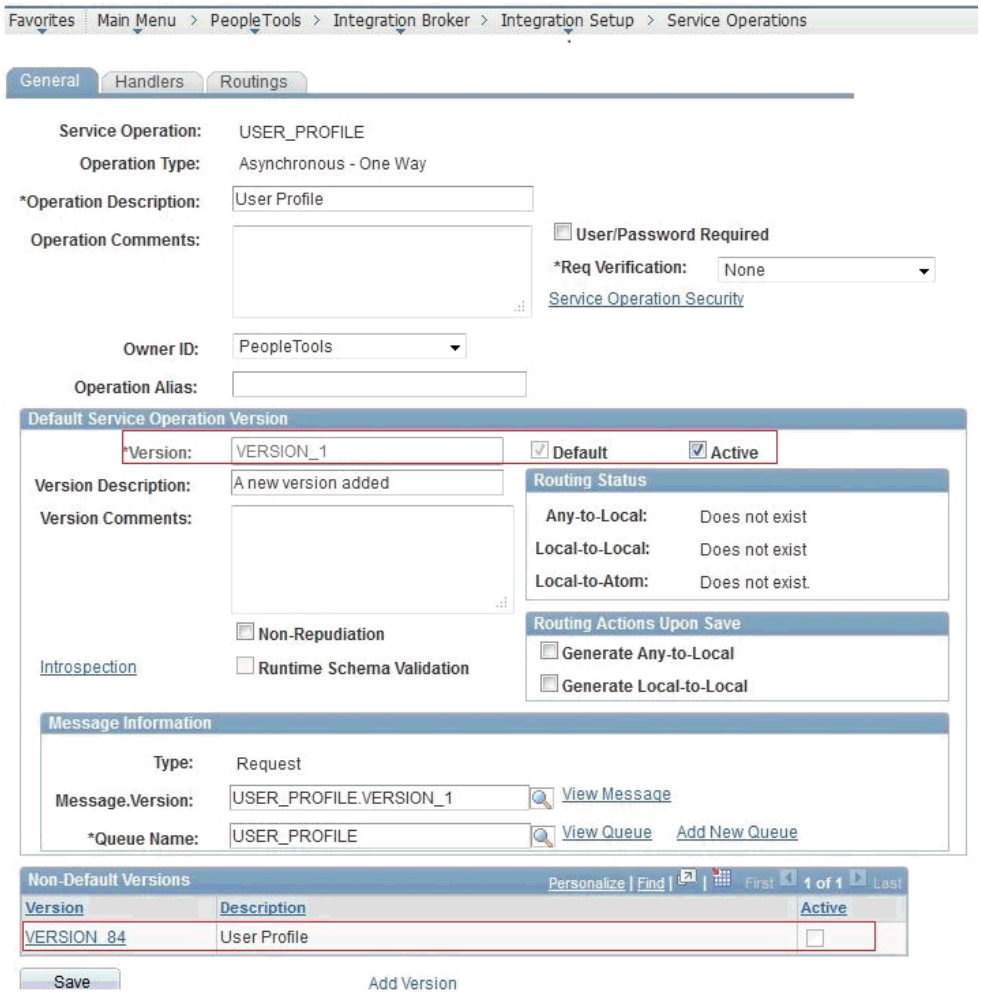
This appendix describes the following procedures:

- Activating a Message Version
- Deactivating a Message Version

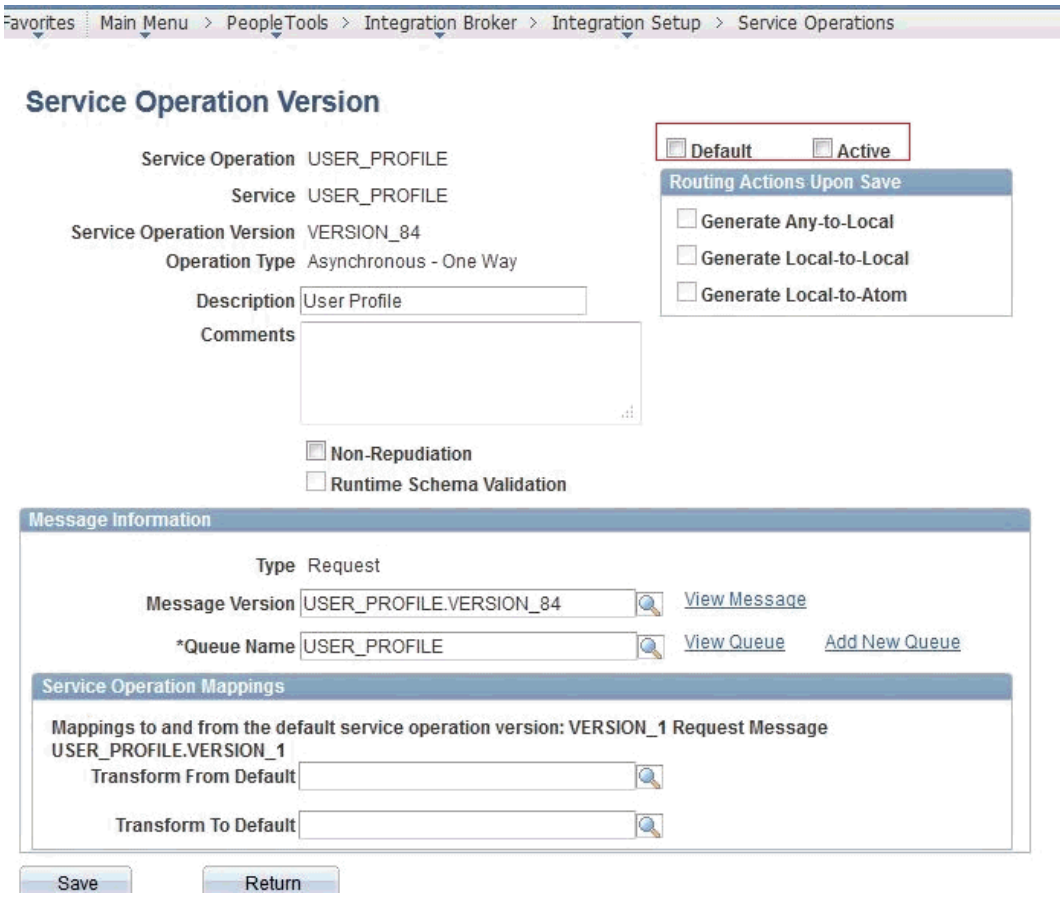
Activating a Message Version

To activate a message version:

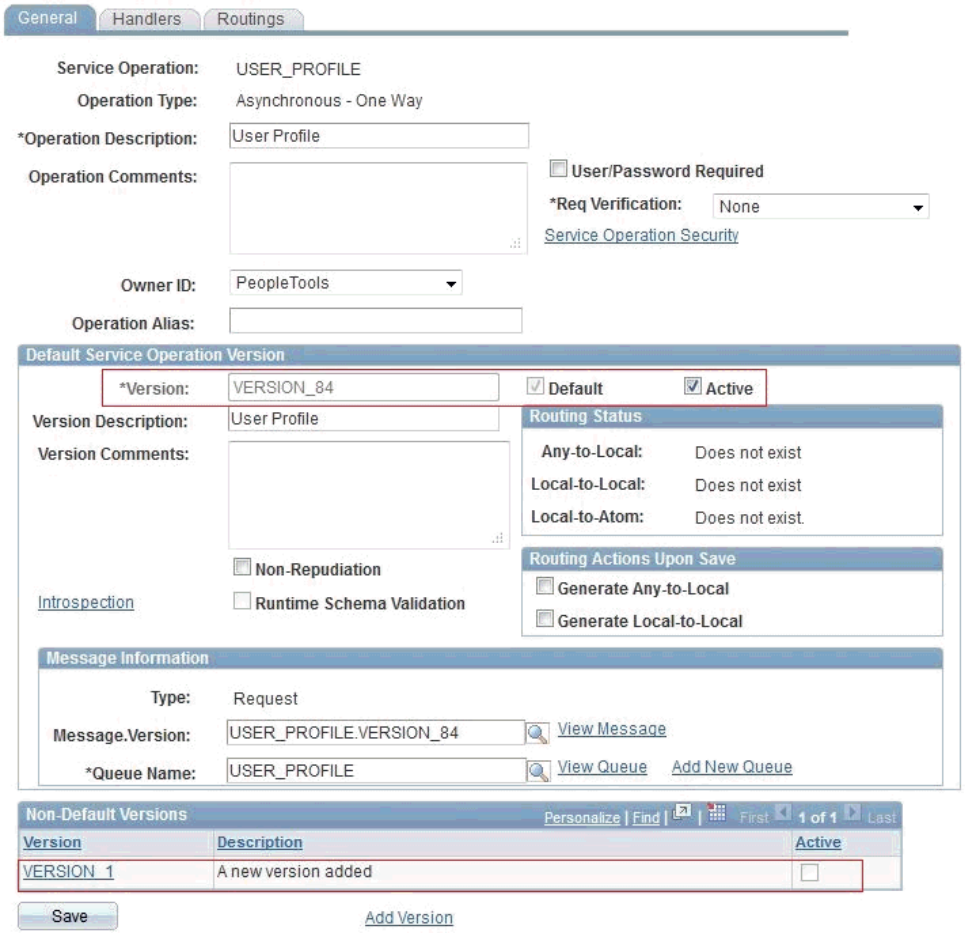
1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
2. Click the **Find Services Operation** tab and enter the Service Operation name, such as USER_PROFILE, in the **Service Operation** field. Then, click **Search.**
3. The following screenshot displays USER_PROFILE with VERSION_1 message set as active and default. To set VERSION_84 as Default and Active, click the VERSION_84 link in the Non-Default Versions region.



4. Select the **Default** and **Active** checkboxes highlighted in the following screenshot and click **Save.**



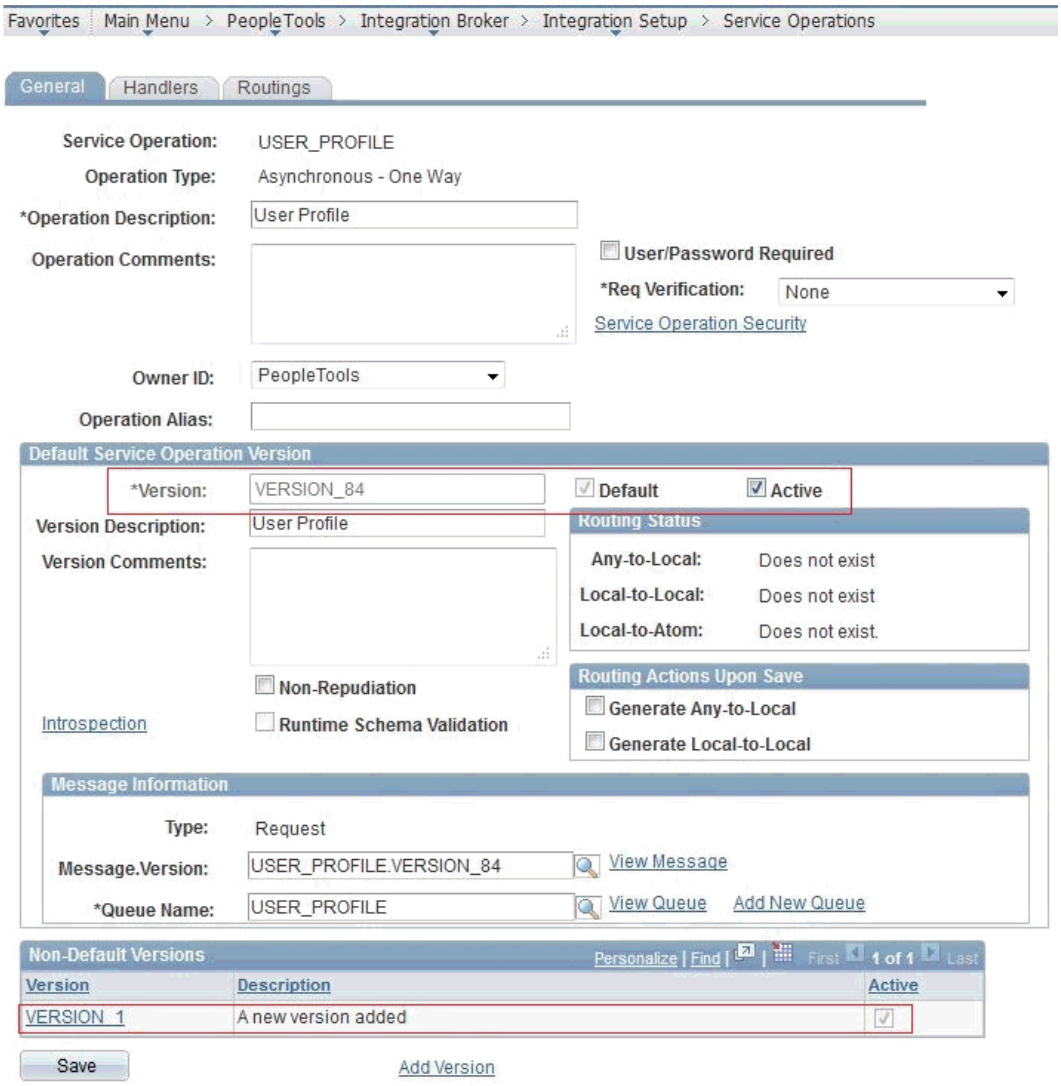
Then, the VESRION_84 message is activated and set as default.



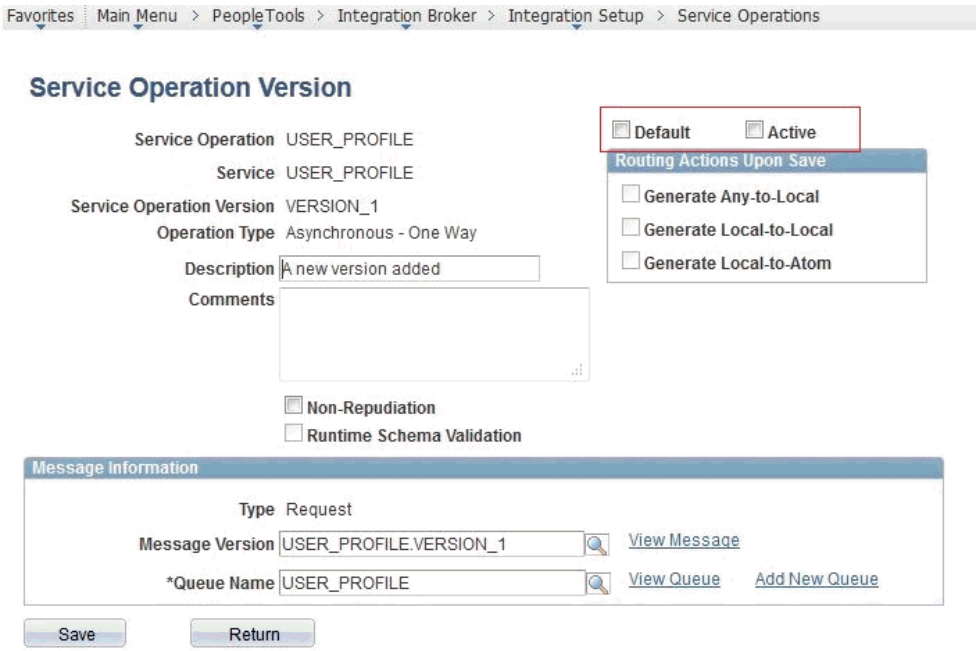
Deactivating a Message Version

To deactivate a message version:

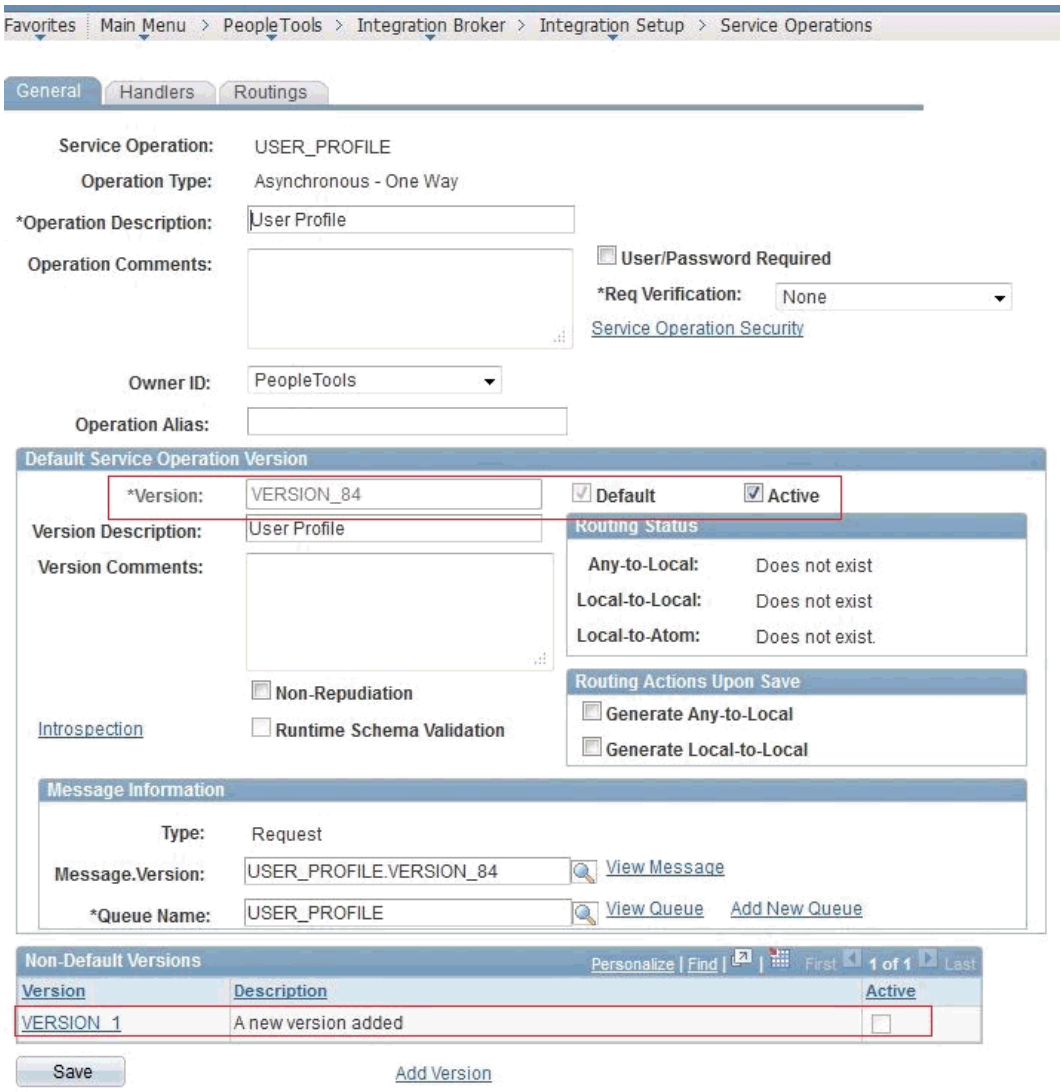
1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
2. Click the **Find Services Operation** tab and enter the Service Operation name, such as USER_PROFILE, in the **Service Operation** field. Then, click **Search.**
3. The following screenshot displays USER_PROFILE with VERSION_84 message set as active and default. To deactivate the non-default VERSION_1 message, click the VERSION_1 link in the Non-Default Versions region.



4. Deselect the **Default** and **Active** checkboxes highlighted in the following screenshot and click **Save.**



Then, the VESRION_1 message is deactivated.


Favorites
Main Menu > PeopleTools > Integration Broker > Integration Setup > Service Operations
General
Handlers
Routings
Service Operation: USER_PROFILE
Operation Type: Asynchronous - One Way
*Operation Description: User Profile
Operation Comments:
User/Password Required
*Req Verification: None
Service Operation Security
Owner ID: PeopleTools
Operation Alias:
Default Service Operation Version
*Version: VERSION_84
Default
Active
Version Description: User Profile
Version Comments:
Routing Status
Any-to-Local: Does not exist
Local-to-Local: Does not exist
Local-to-Atom: Does not exist.
Non-Repudiation
Introspection
Runtime Schema Validation
Routing Actions Upon Save
Generate Any-to-Local
Generate Local-to-Local
Message Information
Type: Request
Message.Version: USER_PROFILE.VERSION_84
View Message
*Queue Name: USER_PROFILE
View Queue
Add New Queue
Non-Default Versions
Personalize | Find | First 1 of 1 Last
Version
Description
Active
VERSION_1
A new version added
Save
Add Version

Index