Oracle® Identity Manager

Connector Guide for PeopleSoft Employee Reconciliation

Release 11.1.1
E25370-25
Sept 2021

Oracle Identity Manager Connector Guide for PeopleSoft Employee Reconciliation, Release 11.1.1

E25370-25

Copyright © 2014, 2020, Oracle and/or its affiliates.

Primary Author: Gowri G.R

Contributing Authors: Alankrita Prakash

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

What's New in the Oracle Identity Manager Connector for PeopleSoft Employee Reconciliation?

1 About the Connector

D 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 Human Resources Management Systems (HRMS).

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`

Documentation Updates

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

`http://download.oracle.com/docs/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 Employee Reconciliation?

This chapter provides an overview of the updates made to the software and documentation for release 11.1.1.5.0 of the PeopleSoft Employee Reconciliation connector.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

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

Software Updates

The following section discusses the software updates:

Software Updates in Release 11.1.1.5.0

The following are software updates in release 11.1.1.5.0:

- Dynamic Manager Linking for Incremental Updates
- Simplified PeopleSoft Listener Deployment
- New Configuration Lookup Definitions
- Resolved Issues

Dynamic Manager Linking for Incremental Updates

This release of the connector supports dynamic reconciliation of Manager ID values during incremental reconciliation operations.

When you perform a full reconciliation for the first time, you must run the PeopleSoft HRMS Manager Reconciliation scheduled task to reconcile the Manager ID values. During the subsequent incremental reconciliation operations, the Manager ID values are reconciled dynamically. Previously, you had to run the PeopleSoft HRMS Manager Reconciliation scheduled task after each incremental reconciliation operation.

See Reconciliation of the Manager ID Attribute for more information.

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.

New Configuration Lookup Definitions

This release of the connector has the following new configuration lookup definitions:

- Lookup.PSFT.HRMS.Configuration

  This lookup definition stores configuration information used by the connector. See Lookup.PSFT.HRMS.Configuration and Setting Up the Lookup.PSFT.HRMS.Configuration Lookup Definition for more information.

- Lookup.PSFT.HRMS.ManagerRecon.Configuration

  This lookup definition provides a list of values used by the PeopleSoft HRMS Manager Reconciliation scheduled task to read the values required to run the task. See Lookup.PSFT.HRMS.ManagerRecon.Configuration and Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task for more information.

Resolved Issues

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

Bug Number	Issue	Resolution
13091034	When the User ID attribute was reconciled into a UDF rather than into a User Login field in Oracle Identity Manager, the Manager ID value was not updated.	This issue has been resolved. The Manager ID value is now updated when the User ID attribute is reconciled into a UDF.

Documentation-Specific Updates

The following section discusses the documentation-specific updates:

Documentation-Specific Updates in Release 11.1.1.5.0

The following documentation-specific updates have been made in revision "25" of this guide:

The "Target System" row of Table 1-1 has been modified to include support for PeopleSoft HRMS 9.2 with PeopleTools 8.59.

The following documentation-specific updates have been made in revision "24" of this guide:

The "Target System" row of Table 1-1 has been modified to include support for PeopleSoft HRMS 9.2 with PeopleTools 8.58.

The following documentation-specific update has been made in revision "23" of this guide:

The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated.

The following documentation-specific updates have been made in revision "22" of this guide:

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 this guide:

- The "Target System" row of Table 1-1 has been modified to include support for PeopleSoft HRMS 9.2 with PeopleTools 8.57.
- The update on PeopleSoft HRMS 9.2 with PeopleTools 8.57 has been made in the following sections:
  - Creating a Permission List
  - Creating a Role for a Limited Rights UserAssigning the Required Privileges to the Target System Account
  - Assigning the Required Privileges to the Target System Account
  - Configuring the PeopleSoft Integration Broker
  - Configuring the PERSON_BASIC_FULLSYNC Service Operation
  - Configuring the WORKFORCE_FULLSYNC Service Operation
  - Configuring PeopleSoft Integration Broker
  - Configuring the PERSON_BASIC_SYNC Service Operation
  - Configuring the WORKFORCE_SYNC Service Operation

The following documentation-specific update has been made in revision "20" of this guide:

- The Code Key and Decode values in Step 5 of Setting Up the Lookup.PSFT.HRMS.ExclusionList Lookup Definition have been modified.
- The "Note" in Step 5c of Creating a Target System User Account for Connector Operations has been modified.

The following documentation-specific update has been made in revision "19" of this guide:

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 "18" of this guide:

- The "Target System" row of Table 1-1 has been modified to include support for PeopleSoft HRMS 9.2 with PeopleTools 8.56.
- The update on PeopleSoft HRMS 9.2 with PeopleTools 8.56 has been made in the following sections:
  - Creating a Permission List
  - Creating a Role for a Limited Rights UserAssigning the Required Privileges to the Target System Account
  - Assigning the Required Privileges to the Target System Account

  - Configuring the PeopleSoft Integration Broker
  - Configuring the PERSON_BASIC_FULLSYNC Service Operation
  - Configuring the WORKFORCE_FULLSYNC Service Operation
  - Configuring PeopleSoft Integration Broker
  - Configuring the PERSON_BASIC_SYNC Service Operation
  - Configuring the WORKFORCE_SYNC Service Operation

The following documentation-specific updates have been made in revision "17" of this guide:

- The description of the *ORACLE_COMMON* environment variable in Deploying the PeopleSoft Listener has been modified.
- The "Note" in "Displaying the EI Repository Folder" has been modified to include later versions of PeopleTools after 8.53.
- The "Note" in Step 3 of "Activating the WORKFORCE_FULLSYNC Service Operation" has been modified about the usage of WORKFORCE_SYNC.INTERNAL service operation.

The following documentation-specific updates have been made in revision "16" of this guide:

- The "Target System" row of Table 1-1 has been modified to include support for PeopleSoft HRMS 9.2 with PeopleTools 8.55.
- Information regarding the default status of an OIM User has been modified from "Active" to "Disabled" in Reconciliation of Effective-Dated Lifecycle Events.
- Information regarding PeopleSoft HRMS 9.2 with PeopleTools 8.55 has been added to the following sections:
  - Creating a Permission List
  - Creating a Role for a Limited Rights UserAssigning the Required Privileges to the Target System Account
  - Assigning the Required Privileges to the Target System Account
  - Configuring the PERSON_BASIC_FULLSYNC Service Operation
  - Configuring the WORKFORCE_FULLSYNC Service Operation
  - Configuring the PERSON_BASIC_SYNC Service Operation
  - Configuring the WORKFORCE_SYNC Service Operation
- Oracle Identity Manager interface names have been corrected throughout the document.

The following documentation-specific update has been made in revision "15" of this guide:

The "Target System" row of Table 1-1 has been modified to include support for PeopleSoft HRMS 9.1 with PeopleTools 8.53.

The following documentation-specific updates have been made in revision "14" of this guide:

- 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".
- All instances of *WLS_HOME* have been replaced with *WL_HOME* in Deploying the PeopleSoft Listener.

The following documentation-specific updates have been made in revision "13" of this guide:

- Information specific to HRMS 9.2 has been added to the "Note" present in the following sections:
  - Configuring the PERSON_BASIC_FULLSYNC Service Operation
  - Configuring the WORKFORCE_FULLSYNC Service Operation
  - Configuring the PERSON_BASIC_SYNC Service Operation
  - Configuring the WORKFORCE_SYNC Service Operation
- The first "Note" present in Configuring the WORKFORCE_FULLSYNC Service Operation has been modified.
- The "Target systems" row of Table 1-1 has been updated.
- The "Note" in Step 3 of the Activating the PERSON_BASIC_FULLSYNC Service Operation area of Configuring the PERSON_BASIC_SYNC Service Operation has been updated.
- The "Note" in Step 3.c of the Defining the Routing for the PERSON_BASIC_FULLSYNC Service Operation area of Configuring the PERSON_BASIC_SYNC Service Operation has been added.
- An issue related to workforce incremental reconciliation has been added to Troubleshooting.

The following documentation-specific updates have been made in revision "12" of this guide:

- 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 "11" of this guide:

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

The following are documentation-specific updates in revision "10" of this guide:

- 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 is a documentation-specific update in revision "9" of this guide:

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).

The following is a documentation-specific update in revision "8" of this guide:

The "Oracle Identity Manager" row in Table 1-1 has been modified.

The following are documentation-specific updates in revision "7" of this guide:

- 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 Testing Reconciliation.
- 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.

- HRMS 9.2 has been added to the first note in Configuring the WORKFORCE_FULLSYNC Service Operation.
- Information about password encryption has been added to Step 1.g in the procedure for Configuring PeopleSoft Integration Broker, in Configuring the PeopleSoft Integration Broker.
- The first point has been added to the note in the procedure for Displaying the EI Repository Folder in the following sections:
  - Configuring the PERSON_BASIC_FULLSYNC Service Operation
  - Configuring the WORKFORCE_FULLSYNC Service Operation
  - Configuring the PERSON_BASIC_SYNC Service Operation
  - Configuring the WORKFORCE_SYNC Service Operation
- A note has been added to the procedure for Activating the WORKFORCE_FULLSYNC Message in the following sections:
  - Configuring the PERSON_BASIC_FULLSYNC Service Operation
  - Configuring the WORKFORCE_FULLSYNC Service Operation
  - Configuring the PERSON_BASIC_SYNC Service Operation
  - Configuring the WORKFORCE_SYNC Service Operation
- The name of the "Known Issues" chapter has been changed to "Known Issues and Workarounds" In addition, Known Issues and Workarounds has been restructured.

The following are documentation-specific updates in revision "6" of this guide:

- The "Oracle Identity Manager" row in Table 1-1 has been modified.
- Displaying UDFs in Oracle Identity Manager 11.1.2.x or Later has been added.
- 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 Tasks

The following documentation-specific updates have been made in the earlier revisions of the release 11.1.1.5.0:

- Revision "5"

  Added Deploying the PeopleSoft Listener on WebSphere Application Server.

  Added a procedure to display UDFs in Oracle Identity Manager release 11.1.2 in Configuring the Scheduled Task for Person Data Reconciliation.

  Added bug 13497967 to Known Issues and Workarounds
- Revision "4"

  In Table 1-1 the PeopleSoft HRMS 9.1 with PeopleTools 8.52 has been added as a newly certified target system.
- Revision "3"

  In Table 1-1 the Oracle Identity Manager version has been updated to Release 11.1.1.5 BP02.

1 About the Connector

Oracle Identity Manager automates access rights management, and the security of resources to various target systems. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with target applications. This guide discusses the connector that enables you to use PeopleSoft HRMS as an authoritative (trusted) source of identity information for Oracle Identity Manager.

> **Note:**
>
> In this guide, PeopleSoft HRMS has been referred to as the **target system**.

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

This chapter contains the following sections:

- Certified Components
- Determining the Version of PeopleTools and the Target System
- Usage Recommendation
- Connector Architecture
- Features of the Connector
- Connector Objects Used During Reconciliation
- Roadmap for Deploying and Using the Connector

1.1 Certified Components

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

Table 1-1 Certified Components

Item	Requirement
Oracle Identity 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) and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and any later BP in this release track • Oracle Identity Manager release 11.1.1.5 BP06 and any later BP in this release track

Table 1-1 (Cont.) Certified Components

Item	Requirement
Target systems	The target system can be any one of the following: • PeopleSoft HRMS 8.9 with PeopleTools 8.49 • PeopleSoft HRMS 8.9 with PeopleTools 8.50 • PeopleSoft HRMS 9.0 with PeopleTools 8.49 • PeopleSoft HRMS 9.0 with PeopleTools 8.50 • PeopleSoft HRMS 9.0 with PeopleTools 8.52 • PeopleSoft HRMS 9.1 with PeopleTools 8.50 • PeopleSoft HRMS 9.1 with PeopleTools 8.51 • PeopleSoft HRMS 9.1 with PeopleTools 8.52 • PeopleSoft HRMS 9.1 with PeopleTools 8.53 • PeopleSoft HRMS 9.2 with PeopleTools 8.53 • PeopleSoft HRMS 9.2 with PeopleTools 8.54 • PeopleSoft HRMS 9.2 with PeopleTools 8.55 • PeopleSoft HRMS 9.2 with PeopleTools 8.56 • PeopleSoft HRMS 9.2 with PeopleTools 8.57 **Note:** If you are using Oracle Identity Governance 12c, then deploying and pinging PeopleSoft listener operations may not work as expected. Apply PeopleSoft Connector Patch 26419438 by using the following URL for these operations to work successfully: `https://support.oracle.com/` • PeopleSoft HRMS 9.2 with PeopleTools 8.58 • PeopleSoft HRMS 9.2 with PeopleTools 8.59
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 or later, or JRockit 1.6 or later
Other Software	You must 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: • PERSON_BASIC_FULLSYNC • WORKFORCE_FULLSYNC • PERSON_BASIC_SYNC • WORKFORCE_SYNC

1.2 Determining the Version of PeopleTools and the Target System

You might want to determine the versions of PeopleTools and the target system you are using to check whether this release of the connector supports that combination. To determine the versions of PeopleTools and the target system:

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

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

For example:

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

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

1.3 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 BP02 (11.1.1.5.2), then you must use the 9.1.0.2 version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 BP02 (11.1.1.5.2) 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.

1.4 Connector Architecture

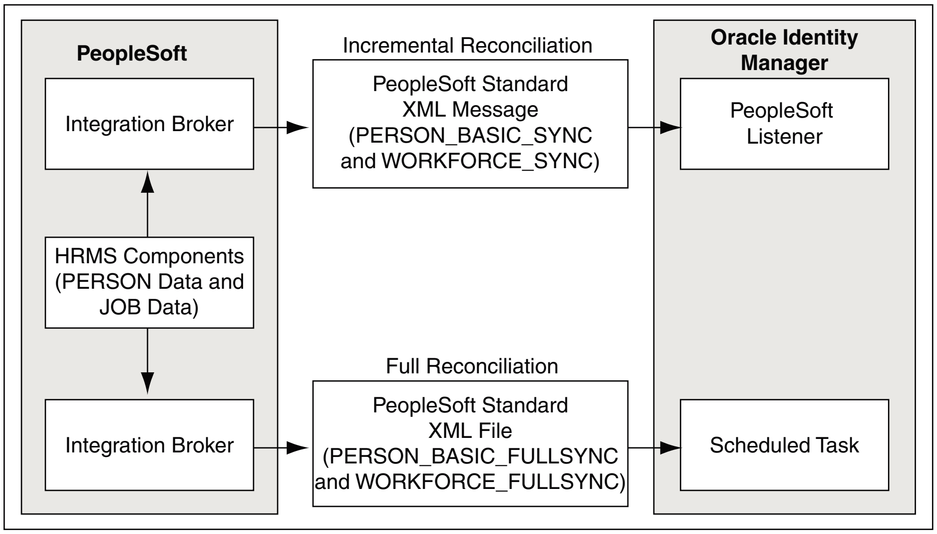
This section contains the following topics:

- About the Connector Architecture
- Full Reconciliation
- Incremental Reconciliation

1.4.1 About the Connector Architecture

Figure 1-1 shows the architecture of the connector.

Figure 1-1 Architecture of the Connector


PeopleSoft
Integration Broker
HRMS Components (PERSON Data and JOB Data)
Integration Broker
Incremental Reconciliation
PeopleSoft Standard XML Message (PERSON_BASIC_SYNC and WORKFORCE_SYNC)
Full Reconciliation
PeopleSoft Standard XML File (PERSON_BASIC_FULLSYNC and WORKFORCE_FULLSYNC)
Oracle Identity Manager
PeopleSoft Listener
Scheduled Task

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.

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

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

- Full Reconciliation
- Incremental Reconciliation

1.4.2 Full Reconciliation

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

PeopleSoft uses its standard message format PERSON_BASIC_FULLSYNC and WORKFORCE_FULLSYNC to send person data to external applications such as Oracle Identity Manager. Full reconciliation fetches all person records from the target system to reconcile records within Oracle Identity Manager. Full reconciliation within Oracle Identity Manager is implemented using the PERSON_BASIC_FULLSYNC and WORKFORCE_FULLSYNC XML files that PeopleSoft generates. See Support for Standard PeopleSoft Messages for more information about these messages.

Full reconciliation involves the following steps:

See Performing Full Reconciliation for the procedure to perform full reconciliation.

1. The PeopleSoft Integration Broker populates the XML files for the PERSON_BASIC_FULLSYNC and WORKFORCE_FULLSYNC messages with all the person data, such as biographical information and job information.
2. Copy these XML files to a directory on the Oracle Identity Manager host computer.
3. Configure the PeopleSoft HRMS Trusted Reconciliation scheduled task. The XML files are read by this scheduled task to generate reconciliation events.

1.4.3 Incremental Reconciliation

Incremental reconciliation involves real-time reconciliation of newly created or modified person data. You use incremental reconciliation to reconcile individual data changes after an initial, full reconciliation run has been performed. PERSON_BASIC_SYNC or WORKFORCE_SYNC are standard PeopleSoft messages to initiate incremental reconciliation. See Support for Standard PeopleSoft Messages for details. These messages are used to send specific person data for each transaction on the target system that involves addition or modification of person information. Incremental reconciliation is configured using PeopleSoft application messaging.

Incremental reconciliation involves the following steps:

Performing Incremental Reconciliation describes the procedure to configure incremental reconciliation.

1. When person data is added or updated in the target system, a PeopleCode event is generated.
2. The PeopleCode event generates an XML message, PERSON_BASIC_SYNC or WORKFORCE_SYNC, containing the modified person data and sends it in real time to the PeopleSoft listener over HTTP. The PeopleSoft listener is a Web application that is deployed on an 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.

1.5 Features of the Connector

The following are the features of the connector:

- Dedicated Support for Trusted Source Reconciliation
- Full and Incremental Reconciliation
- Support for Major Person Lifecycle Events
- Reconciliation of Effective-Dated Lifecycle Events
- Support for Standard PeopleSoft Messages
- Support for Resending Messages That Are Not Processed
- Validation and Transformation of Person Data
- Reconciliation of the Manager ID Attribute
- Target Authentication
- Support for Specifying Persons to Be Excluded from Reconciliation Operation

1.5.1 Dedicated Support for Trusted Source Reconciliation

The connector provides all the features required for setting up PeopleSoft HRMS as a trusted (authoritative) source of identity data for Oracle Identity Manager. Oracle Identity Manager uses this message for incremental reconciliation. In other words, the connector does not support provisioning operations and target resource reconciliation with PeopleSoft HRMS.

1.5.2 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 or modified are directly sent to the listener deployed on the Oracle Identity Manager host computer. The listener parses the records and sends reconciliation events to Oracle Identity Manager.

1.5.3 Support for Major Person Lifecycle Events

The connector helps you to manage all major person lifecycle events, from onboarding to termination and beyond a whole range of events that defines a long-term relationship a person establishes with an organization. This relationship can be defined as the person lifecycle.

The connector performs real-time reconciliation of changes in PeopleSoft including new person creation, changes to existing persons, and so on. Real-time reconciliation allows Oracle Identity Manager to immediately detect critical lifecycle events, such as job terminations, transfers, and so on. Oracle Identity Manager is thus able to take the appropriate action immediately.

Whenever the status of a person changes in PeopleSoft, the status of the OIM User changes as defined in the Lookup.PSFT.HRMS.WorkForceSync.EmpStatus lookup definition. See Lookup.PSFT.HRMS.WorkForceSync.EmpStatus for more information.

1.5.4 Reconciliation of Effective-Dated Lifecycle Events

On the target system, you can use the effective-dated feature to assign a future date to changes that you want to make to a person account.

The connector can distinguish between hire events and other events in the lifecycle of a person record on the target system. These events may be either current-dated or future-dated (in other words, effective-dated). A current-dated event is one in which the date of the event is prior to or same as the current date. A future-dated event is one in which the date the event will take effect is set in the future. For example, if the current date is 30-Jan-09 and if the date set for an event is 15-Feb-09, then the event is future-dated. During reconciliation, the manner in which an event is processed depends on the type of the event.

PeopleSoft uses two standard messages to reconcile a record. These are the PERSON_BASIC_SYNC and the WORKFORCE_SYNC messages. See Support for Standard PeopleSoft Messages for more information about these messages.

You run the PERSON_BASIC_SYNC message to create an OIM User. The default status of an OIM User is **Disabled**. See the **Employee Status** Code Key in the lookup definition described in Lookup.PSFT.Message.PersonBasicSync.Configuration.

The job-related information of a person is updated through the WORKFORCE_SYNC message. In addition, the status is modified depending on the information fetched from the **ACTION** node of the WORKFORCE_SYNC message XML. For example, the value for hire event is retrieved from the ACTION node of the WORKFORCE_SYNC message XML as `HIR`.

The Lookup.PSFT.HRMS.WorkForceSync.EmpStatus lookup definition provides a mapping for the value retrieved from the ACTION node of the XML message. In the lookup definition, the Code Key defines the action performed, and the Decode value is either `Active` or `Inactive`. Depending on the Decode value, the status of the person appears as `Active` or `Disabled` in Oracle Identity Manager.

For example, in this case the data fetched from the XML message is `HIR`. The Lookup.PSFT.HRMS.WorkForceSync.EmpStatus lookup definition stores the mapping for the HIR action, in the Decode column. If you want to display Active on the Oracle Identity Manager console as against the HIR action then define the following mapping in the lookup definition:Code Key: HIRDecode: Active

See Lookup.PSFT.HRMS.WorkForceSync.EmpStatus. for more information about this lookup definition.

Note:

In the context of the Effective Date feature, records for a particular person on the target system can be categorized into the following types:

- **Current:** The record with an effective date that is closest to or same as, but not greater than, the system date. There can be only one current record
- **History:** Records with dates that are earlier than that of the current-dated record
- **Future:** Records that have effective dates later than the system date

1.5.5 Support for Standard PeopleSoft Messages

PeopleSoft provides standard messages to send biographical data and job-related data to external applications, such as Oracle Identity Manager. The connector uses the following standard PeopleSoft messages that are delivered as part of PeopleSoft HRMS installation to achieve full reconciliation and incremental reconciliation:

- PERSON_BASIC_FULLSYNC

  This message contains all the basic biographical information of all persons. This information includes Employee ID, First Name, Last Name, and Employee Type. It is used for full reconciliation.
- PERSON_BASIC_SYNC

  This message contains the information about a particular person. This includes Employee ID and the information that is added or modified. During incremental reconciliation, PERSON_BASIC_SYNC messages are sent to Oracle Identity Manager.

  Note:

  It is only if a person is added in PeopleSoft that the triggering of PERSON_BASIC_SYNC creates an OIM User. But, if an OIM User has been created during full reconciliation, then the PERSON_BASIC_SYNC message contains modifications to personal data.
- WORKFORCE_FULLSYNC

  This message contains job-related details of all persons. This information includes Department, Supervisor ID, Manager ID, and Job Code. It is used for full reconciliation.
- WORKFORCE_SYNC

This message contains job-related details of a particular person. This information includes Employee ID and the information that is added or modified. It is used in incremental reconciliation.

> **Note:**
>
> When you reconcile records, it is mandatory to run the PERSON_BASIC_FULLSYNC message before WORKFORCE_FULLSYNC. If the WORKFORCE_FULLSYNC message is processed first, then Oracle Identity Manager stores the data for all those events in the **Event Received** state and processes them after person data is available through reconciliation performed using the PERSON_BASIC_FULLSYNC message.

1.5.6 Support for Resending Messages That Are Not Processed

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

If the connector is not able to process a message successfully, then 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`

1.5.7 Validation and Transformation of Person Data

You can configure validation of person data that is brought into Oracle Identity Manager during reconciliation. In addition, you can configure transformation of person data that is brought into Oracle Identity Manager during reconciliation.

- Configuring Validation of Data During Reconciliation provides information about setting up the validation feature.
- Configuring Transformation of Data During Reconciliation provides information about setting up the transformation feature.

1.5.8 Reconciliation of the Manager ID Attribute

The connector supports full and dynamic reconciliation of Manager ID values. The Manager ID attribute is one of the predefined OIM User form attributes. When you reconcile data while creating an OIM User, you can populate this field with manager details by running the PeopleSoft HRMS Manager Reconciliation scheduled task.

> **Note:**
>
> The target system also provides the Supervisor attribute, which is a lookup field on the target system UI. This value is populated in the Supervisor ID field, which is a UDF on the process form.

1.5.8.1 Full Reconciliation of the Manager ID Attribute

When you perform a full reconciliation for the first time, you must run the PeopleSoft HRMS Manager Reconciliation scheduled task to reconcile the Manager ID values.

See Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task for instructions on how to reconcile Manager ID values in this scenario.

1.5.8.2 Dynamic Reconciliation of the Manager ID Attribute

After you perform a full reconciliation for the first time, during the subsequent incremental reconciliation operations, the Manager ID values are reconciled dynamically.

The connector reconciles the manager information based on the Supervisor ID in Oracle Identity Manager and the job information fetched through the WORKFORCE_SYNC message.

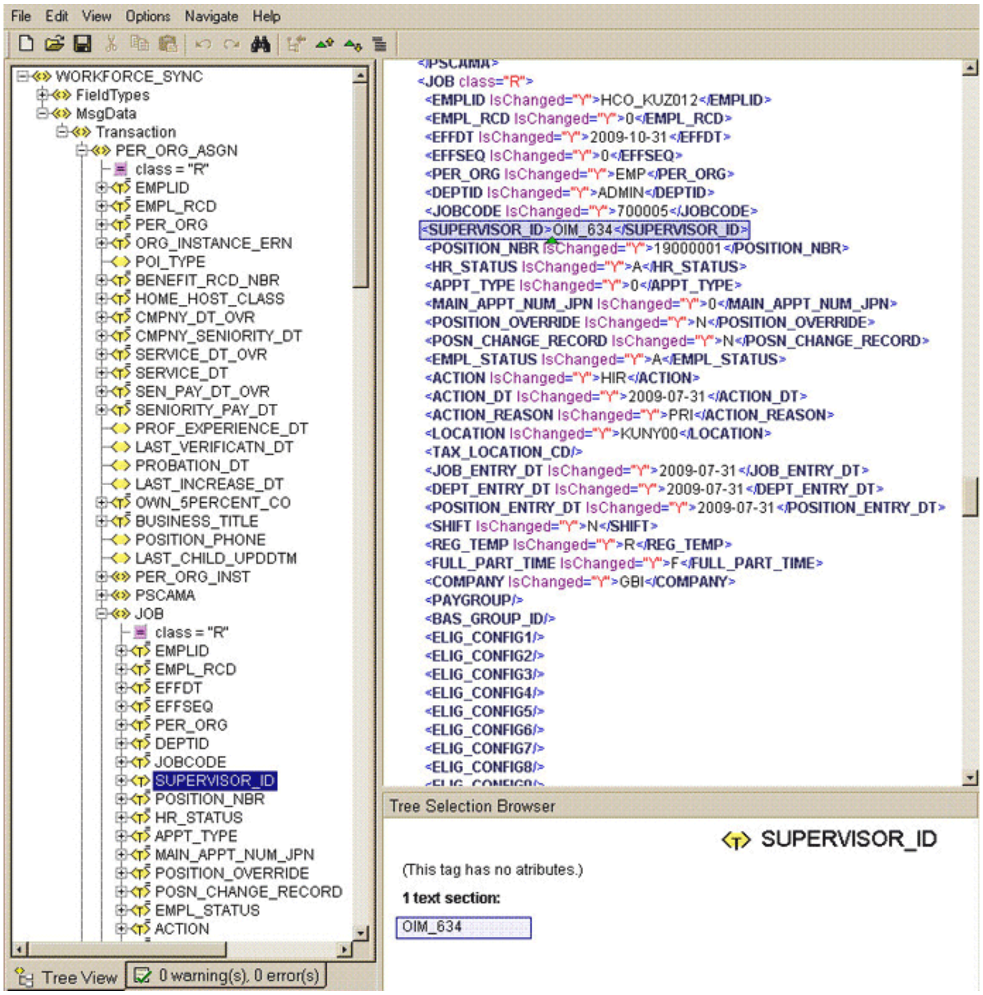
1.5.8.3 Steps in the Manager ID Reconciliation Process

This section describes the steps in the Manager ID reconciliation process, which applies to both full and dynamic reconciliation of the Manager ID values.

To update the job details of a person:

1. The Supervisor details for a person are retrieved from the target system when you run the WORKFORCE_FULLSYNC or the WORKFORCE_SYNC message.

   The Supervisor details are fetched from the SUPERVISOR_ID node of the message XML, as shown in the following screenshot:



```
</PSCAMA>
<JOB class="R">
 <EMPLID IsChanged="Y">HCO_KUZ012</EMPLID>
 <EMPL_RCD IsChanged="Y">0</EMPL_RCD>
 <EFFDT IsChanged="Y">2009-10-31</EFFDT>
 <EFFSEQ IsChanged="Y">0</EFFSEQ>
 <PER_ORG IsChanged="Y">EMP</PER_ORG>
 <DEPTID IsChanged="Y">ADMIN</DEPTID>
 <JOBCODE IsChanged="Y">700005</JOBCODE>
 <SUPERVISOR_ID>OIM_634</SUPERVISOR_ID>
 <POSITION_NBR IsChanged="Y">19000001</POSITION_NBR>
 <HR_STATUS IsChanged="Y">A</HR_STATUS>
 <APPT_TYPE IsChanged="Y">0</APPT_TYPE>
 <MAIN_APPT_NUM_JPN IsChanged="Y">0</MAIN_APPT_NUM_JPN>
 <POSITION_OVERRIDE IsChanged="Y">N</POSITION_OVERRIDE>
 <POSN_CHANGE_RECORD IsChanged="Y">N</POSN_CHANGE_RECORD>
 <EMPL_STATUS IsChanged="Y">A</EMPL_STATUS>
 <ACTION IsChanged="Y">HIR</ACTION>
 <ACTION_DT IsChanged="Y">2009-07-31</ACTION_DT>
 <ACTION_REASON IsChanged="Y">PRI</ACTION_REASON>
 <LOCATION IsChanged="Y">KUNY00</LOCATION>
 <TAX_LOCATION_CD/>
 <JOB_ENTRY_DT IsChanged="Y">2009-07-31</JOB_ENTRY_DT>
 <DEPT_ENTRY_DT IsChanged="Y">2009-07-31</DEPT_ENTRY_DT>
 <POSITION_ENTRY_DT IsChanged="Y">2009-07-31</POSITION_ENTRY_DT>
 <SHIFT IsChanged="Y">N</SHIFT>
 <REG_TEMP IsChanged="Y">R</REG_TEMP>
 <FULL_PART_TIME IsChanged="Y">F</FULL_PART_TIME>
 <COMPANY IsChanged="Y">GBI</COMPANY>
 <PAYGROUP/>
 <BAS_GROUP_ID/>
 <ELIG_CONFIG1/>
 <ELIG_CONFIG2/>
 <ELIG_CONFIG3/>
 <ELIG_CONFIG4/>
 <ELIG_CONFIG5/>
 <ELIG_CONFIG6/>
 <ELIG_CONFIG7/>
 <ELIG_CONFIG8/>
 <ELIG_CONFIG9/>
```

(This tag has no atributes.)

1 text section:

OIM_634

2. The connector populates the Supervisor ID field in the process form.
3. Run the PeopleSoft HRMS Manager Reconciliation scheduled task only if you perform full reconciliation for the first time. See Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task for instructions on how to reconcile Manager ID values in this scenario.
4. The scheduled task checks for the existence of an OIM User with the same User ID as that of Supervisor ID value. If a match is found, the Manager ID attribute is updated with the value of the Supervisor ID.

This sequence of steps can be illustrated by the following example:

Suppose Richard is a person on the target system with the user ID 02. John Doe, his manager, with user ID 01 exists on Oracle Identity Manager. During reconciliation of Richard's person record:

1. The Supervisor ID of Richard is fetched from the target system using the WORKFORCE_FULLSYNC or the WORKFORCE_SYNC message. The value fetched is 01.
2. The Supervisor ID field of Richard is populated with 01.
3. The scheduled task looks for an OIM User with the same Supervisor ID value. John's record matches the criterion.
4. The Manager ID field pertaining to Richard is populated with 01.

1.5.9 Target Authentication

Target authentication is done to validate whether Oracle Identity Manager should accept messages from the target system or not. It 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`.

1.5.10 Support for Specifying Persons to Be Excluded from Reconciliation Operation

You can specify a list of persons who must be excluded from all reconciliation operations. Persons whose User IDs you specify in the exclusion list are not affected by the reconciliation operation. See Lookup.PSFT.HRMS.ExclusionList for more information.

1.6 Connector Objects Used During Reconciliation

Trusted source reconciliation involves reconciling data of newly created or modified accounts on the target system into Oracle Identity Manager and adding or updating OIM Users.

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

This section discusses the following topics:

- User Attributes for Reconciliation
- Reconciliation Rules
- Reconciliation Action Rules
- Predefined Lookup Definitions

1.6.1 User Attributes for Reconciliation

Table 1-2 lists the identity attributes whose values are fetched from the target system during reconciliation.

Table 1-2 User Attributes for Reconciliation

OIM User Form Field	PeopleSoft HRMS/HCM Field	Description
User ID	PS_PERSON.EMPLID	The employee ID of the user This is a mandatory field for the creation of an OIM User.

Table 1-2 (Cont.) User Attributes for Reconciliation

OIM User Form Field	PeopleSoft HRMS/HCM Field	Description
Last Name	PS_NAMES.LAST_NAME	The last name of the user This is a mandatory field for the creation of an OIM User.
First Name	PS_NAMES.FIRST_NAME	The first name of the user This is a mandatory field for the creation of an OIM User.
Employee Type	PS_JOB.REG_TEMP PS_JOB.FULL_PART_TIME PS_JOB.PER_ORG	The employee type of the OIM User The combination of the values of the PS_JOB.REG_TEMP, PS_JOB.FULL_PART_TIME, and the PS_JOB.PER_ORG fields are used to specify the employee type of the OIM User. This is a mandatory field for the creation of an OIM User.
Status	PS_JOB.ACTION	The action to be taken for a person. It could be HIRE, TRANSFERED, and so on.
Start Date	PS_JOB.EFFDT	The effective date of a person's job record
Supervisor ID	PS_JOB.SUPERVISOR_ID	The supervisor ID of a person
Department	PS_JOB.DEPTID	The department ID of a person
Job ID	PS_JOB.JOBCODE	The job ID of a person

1.6.2 Reconciliation Rules

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

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

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

1.6.2.1 Overview of the Reconciliation Rule

The following is the process-matching rule:

Rule Name: Peoplesoft HRMS 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 Employee ID field of the employee on the target system.

For trusted source reconciliation, the User ID field of the OIM User form is matched against the Employee ID field on the target system. These are the key fields in Oracle Identity Manager and the target system, respectively.

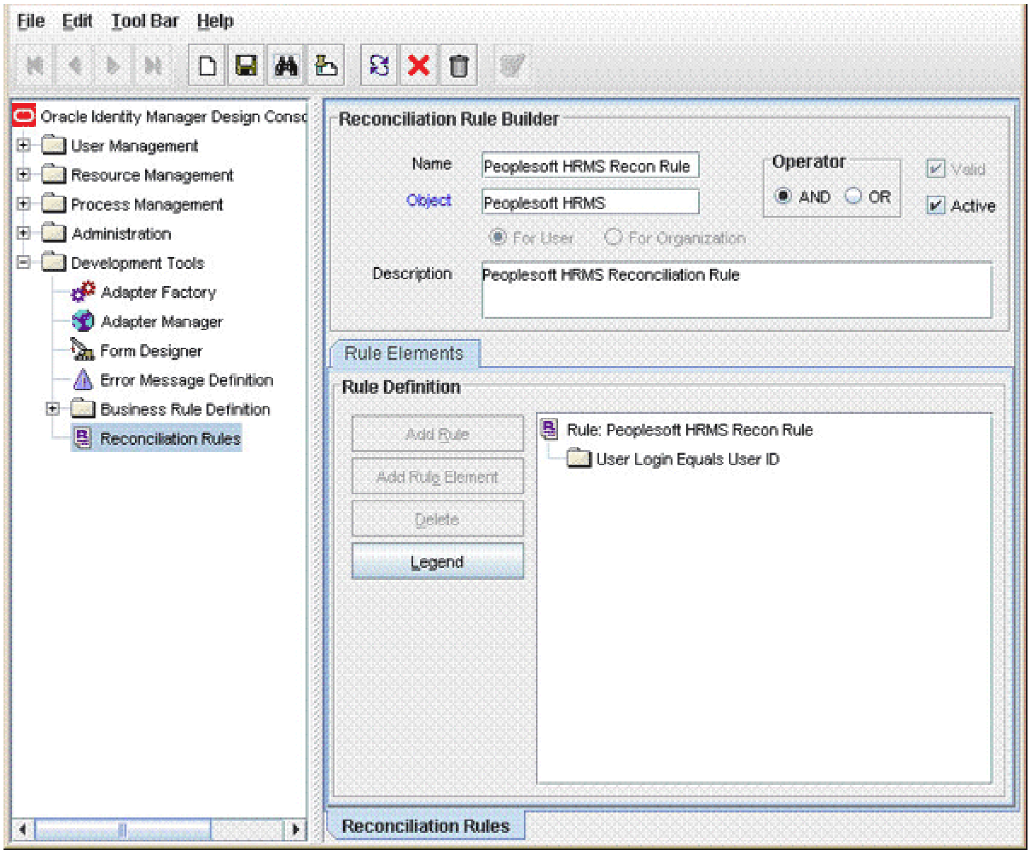
1.6.2.2 Viewing the Reconciliation Rule in the Design Console

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 ER.** Figure 1-2 shows this reconciliation rule.

Figure 1-2 Reconciliation Rule



Name: Peoplesoft HRMS Recon Rule

Object: Peoplesoft HRMS

● For User ○ For Organization

Description: Peoplesoft HRMS Reconciliation Rule

Operator: ● AND ○ OR

☑ Valid

☑ Active

Rule: Peoplesoft HRMS Recon Rule
User Login Equals User ID

1.6.3 Reconciliation Action Rules

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

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

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

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

1.6.3.1 Overview of the Reconciliation Action Rules

Table 1-3 lists the reconciliation action rules for this connector:

Table 1-3 Action Rules for Trusted Source Reconciliation

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

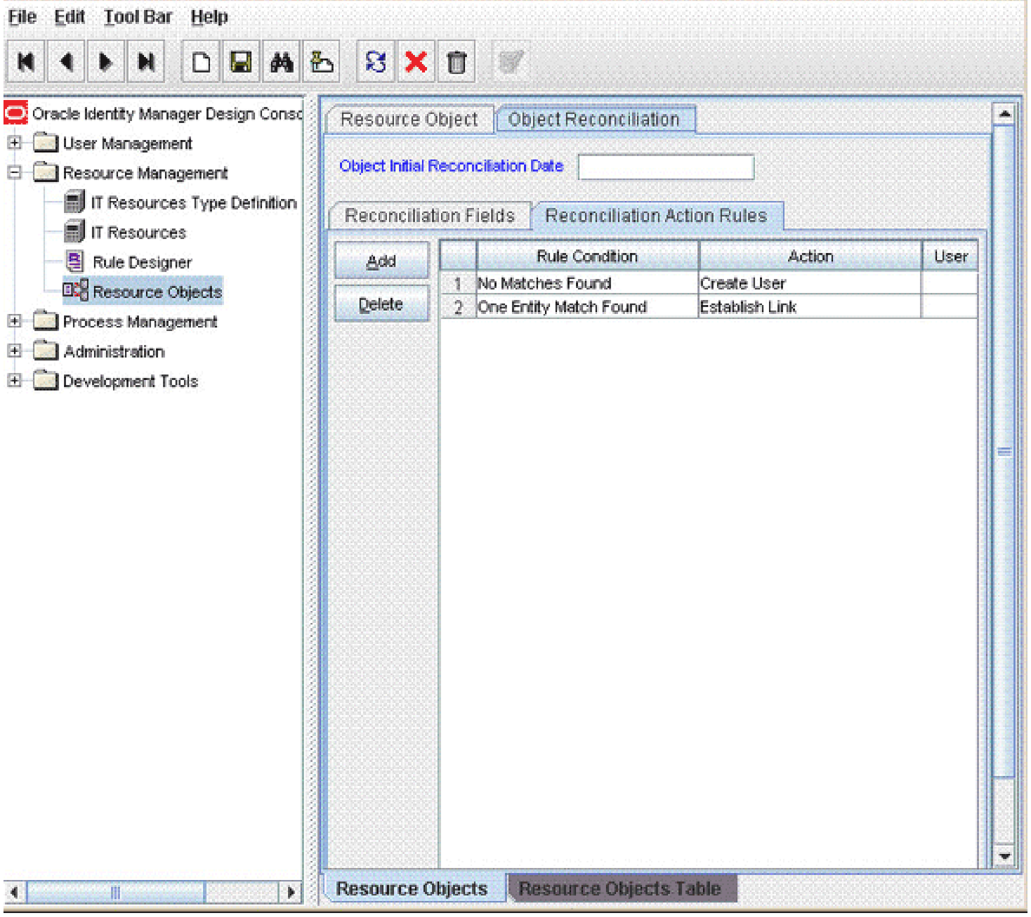
1.6.3.2 Viewing the Reconciliation Action Rules in the Design Console

After you deploy the connector, you can view the reconciliation action rules 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 HRMS** 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 1-3 shows these reconciliation action rules.

Figure 1-3 Reconciliation Action Rules



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

1.6.4 Predefined Lookup Definitions

The predefined lookup definitions can be categorized as follows:

- Lookup.PSFT.HRMS.Configuration
- Lookup.PSFT.HRMS.ManagerRecon.Configuration
- Lookup Definitions Used to Process PERSON_BASIC_SYNC Messages
- Lookup Definitions Used to Process WORKFORCE_SYNC Messages
- Other Lookup Definitions

1.6.4.1 Lookup.PSFT.HRMS.Configuration

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

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

Code Key	Decode	Description
Manager Recon Config Lookup	Lookup.PSFT.HRMS.ManagerRecon.Configuration	Name of the lookup used by the PeopleSoft HRMS Manager Reconciliation scheduled task to read the required values. See Lookup.PSFT.HRMS.ManagerRecon.Configuration for more information about this lookup definition.
HRMS Resource Exclusion List Lookup	Lookup.PSFT.HRMS.ExclusionList	Name of the Resource Exclusion lookup for PeopleSoft Employee Reconciliation See Lookup.PSFT.HRMS.Configuration for more information about this lookup definition.
Ignore Root Audit Action	No	Use this value if the Root PSCAMA audit action is required to be considered while parsing the XML message. Enter Yes if PSCAMA Audit Action is not taken into account. Here, the Root Audit Action is considered as a Change event. Enter 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.
PERSON_BASIC_FULLSYNC	Lookup.PSFT.Message.PersonBasicSync.Configuration	Name of the lookup definition for PERSON_BASIC_FULLSYNC message See Lookup.PSFT.Message.PersonBasicSync.Configuration for more information about this lookup definition. **Note:** The Decode value is the same as that of the PERSON_BASIC_SYNC message, because the data to be reconciled is the same for both messages.

Code Key	Decode	Description
PERSON_BASIC_SYNC	Lookup.PSFT.Message.PersonBasicSync.Configuration	Name of the lookup definition for the PERSON_BASIC_SYNC message See Lookup.PSFT.Message.PersonBasicSync.Configuration for more information about this lookup definition.
Target Date Format	yyyy-MM-dd	Data format of the Date type data in the XML file and messages You must not change this value.
WORKFORCE_FULLSYNC	Lookup.PSFT.Message.WorkForceSync.Configuration	Name of the lookup definition for the WORKFORCE_FULLSYNC message See Lookup.PSFT.Message.WorkForceSync.Configuration for more information about this lookup definition. **Note:** The Decode value is the same as that of the WORKFORCE_ SYNC because the data to be reconciled is the same for both messages.
WORKFORCE_SYNC	Lookup.PSFT.Message.WorkForceSync.Configuration	Name of the lookup definition for the WORKFORCE_SYNC message See Lookup.PSFT.HRMS.ManagerRecon.Configuration for more information about this lookup definition.

You can configure the message names, such as the PERSON_BASIC_SYNC, WORKFORCE_SYNC, PERSON_BASIC_FULLSYNC, and WORKFORCE_FULLSYNC defined in this lookup definition. Setting Up the Lookup.PSFT.HRMS.Configuration Lookup Definition describes the procedure to configure these message names.

1.6.4.2 Lookup.PSFT.HRMS.ManagerRecon.Configuration

The Lookup.PSFT.HRMS.ManagerRecon.Configuration lookup definition provides a list of values used by the PeopleSoft HRMS Manager Reconciliation scheduled task to read the values required to run the task.

If you want to modify the PeopleSoft HRMS Manager Reconciliation scheduled task, for example, when the Employee ID field is mapped to a UDF, then you must modify the values in this lookup as per the changes made to the task.

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

Code Key	Decode
Employee ID RO	Name of the Resource Object field for Employee ID of a person. Sample value: `User ID`
Employee ID UDF	Metadata of the field of the person form with which EMPL ID from the target system is mapped. Sample value: `Users.User ID`
Manager UDF	Metadata of the Supervisor ID field of the person form. Sample value: `USR_UDF_SUPERVISOR_ID`

See Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task for instructions on how to configure and run the PeopleSoft HRMS Manager Reconciliation scheduled task.

1.6.4.3 Lookup Definitions Used to Process PERSON_BASIC_SYNC Messages

The following lookup definitions are used to process PERSON_BASIC_SYNC messages:

1.6.4.3.1 Lookup.PSFT.Message.PersonBasicSync.Configuration

The Lookup.PSFT.Message.PersonBasicSync.Configuration lookup definition provides the configuration-related information for the PERSON_BASIC_SYNC and PERSON_BASIC_FULLSYNC messages.

The lookup definition has the following entries:

Code Key	Decode	Description
Attribute Mapping Lookup	Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping	Name of the lookup definition that maps Oracle Identity Manager attributes with the attributes in the PERSON_BASIC_SYNC and PERSON_BASIC_FULLSYNC message XML See Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping for more information about this lookup definition.
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 the Limited Reconciliation.
Custom Query Lookup Definition	Lookup.PSFT.HRMS.CustomQuery	This entry holds the name of the lookup definition that maps resource object fields with OIM User form fields. This lookup definition is used during application of the custom query. See Limited Reconciliation for more information.

Code Key	Decode	Description
Data Node Name	Transaction	Name of the node in the XML files to execute a transaction Default value: `Transaction` You must not change the default value.
Employee Status	Active	Default status of an employee during the creation of an OIM User **Note:** You can change the status to Disabled, if you want the status to be Inactive when the OIM User is created.
Employee Type Lookup	Lookup.PSFT.HRMS.PersonBasicSync.EmpType	Name of the lookup definition that maps Oracle Identity Manager attributes with employee type attributes obtained from XML message See Lookup.PSFT.HRMS.PersonBasicSync.EmpType for more information about this lookup definition.
Message Handler Class	oracle.iam.connectors.psft.common.handler.impl.PSFTPersonSyncReconMessageHandlerImpl	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. **See Also:** Configuring the Connector Messages
Message Parser	oracle.iam.connectors.psft.common.parser.impl.PersonMessageParser	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. See Also: Configuring the Connector Messages
Organization	Xellerate Users	Default organization in Oracle Identity Manager

Code Key	Decode	Description
Recon Lookup Definition	Lookup.PSFT.HRMS.PersonBasicSync.Recon	Name of the lookup definition that maps Oracle Identity Manager attributes with the Resource Object attributes See Lookup.PSFT.HRMS.PersonBasicSync.Recon for more information about this lookup definition.
Resource Object	Peoplesoft HRMS	Name of the resource object
Transformation Lookup Definition	Lookup.PSFT.HRMS.PersonBasicSync.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 Type	End-User	It specifies the value with which a person is created in Oracle Identity Manager using the PERSON_BASIC_SYNC message.
Use Transformation	No	Enter `yes` to implement transformation while reconciling records. Otherwise, enter `no`.
Use Validation	No	Enter `yes` to implement validation while reconciling records. Otherwise, enter `no`.
Validation Lookup Definition	Lookup.PSFT.HRMS.PersonBasicSync.Validation	Name of the validation lookup definition See Configuring Validation of Data During Reconciliation for more information about adding entries in this lookup definition.

1.6.4.3.2 Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping

The Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping lookup definition maps OIM User attributes with the attributes defined in the PERSON_BASIC_SYNC message. The following table provides the format of the values stored in this lookup definition:

Code Key	Decode
Emp Type	PER_ORG~PERSON
First Name	FIRST_NAME~NAMES~NAME_TYPE=PRI~EFFDT
Last Name	LAST_NAME~NAMES~NAME_TYPE=PRI~EFFDT
User ID	EMPLID~PERSON~None~None~PRIMARY

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`

In this format:

`NODE:` Name of the node in the PERSON_BASIC_SYNC message XML file 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.

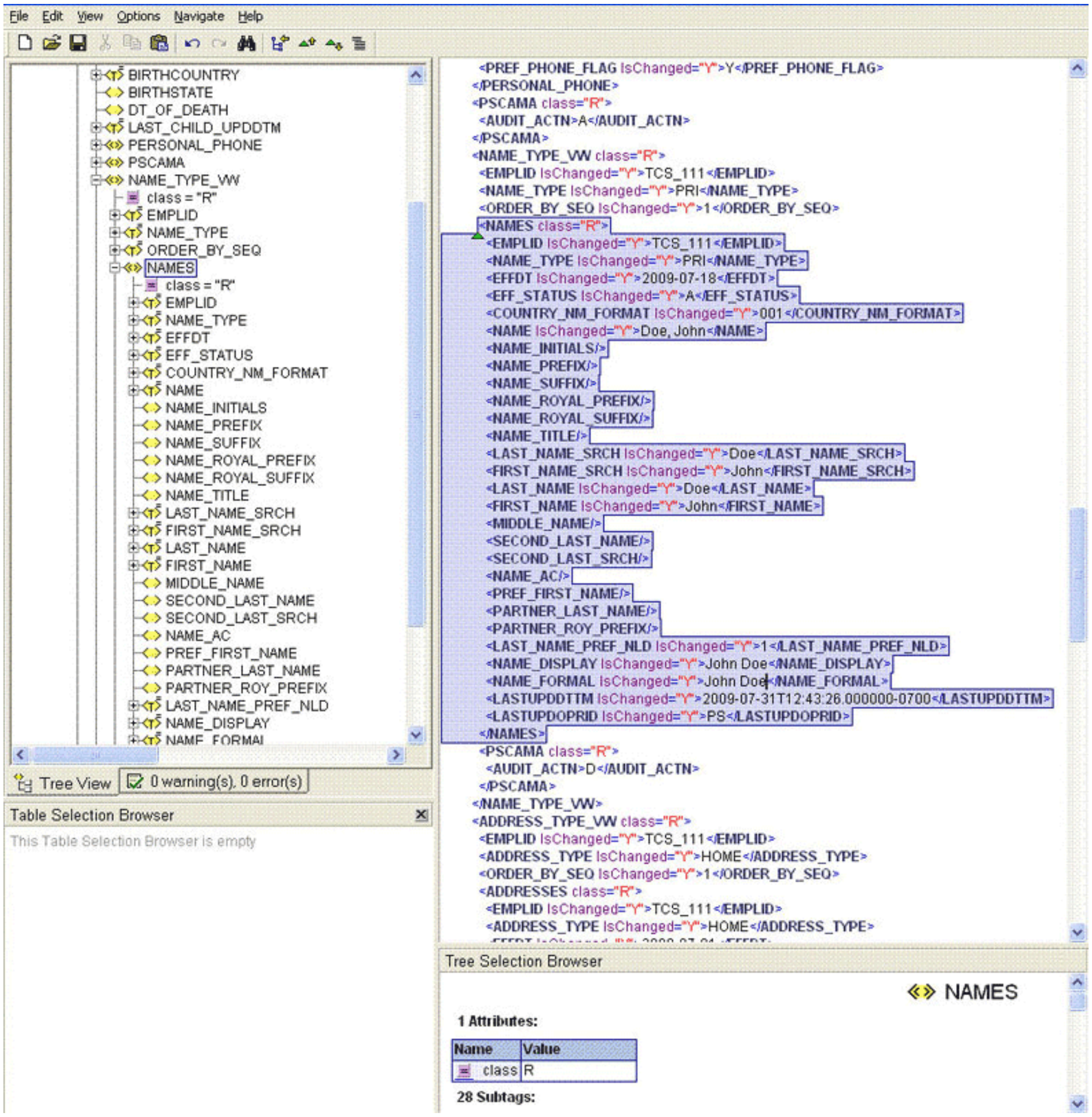
For example, in the PERSON_BASIC_SYNC message, the rowset NAME_TYPE_VW lists the names assigned to a person. The names assigned could be primary, secondary, or nickname, depending on how it is configured in PeopleSoft.

If you want to use the primary name to create an OIM User, then you must locate the NAME_TYPE node with the value PRI to fetch First Name and Last Name from the XML message. Therefore, you must provide the following mapping in Decode column for First Name:

```
FIRST_NAME~NAMES~NAME_TYPE=PRI~EFFDT
```

In this format, NAME_TYPE specifies the TYPE NODE to consider, and PRI specifies that name of type PRI (primary) must be considered while fetching data from the XML messages. All other names types are then ignored.

The NAME_TYPE node with PRI value is shown in the following screenshot:



```
  <PREF_PHONE_FLAG IsChanged="Y">Y</PREF_PHONE_FLAG>
 </PERSONAL_PHONE>
 <PSCAMA class="R">
  <AUDIT_ACTN>A</AUDIT_ACTN>
 </PSCAMA>
 <NAME_TYPE_VW class="R">
  <EMPLID IsChanged="Y">TCS_111</EMPLID>
  <NAME_TYPE IsChanged="Y">PRI</NAME_TYPE>
  <ORDER_BY_SEQ IsChanged="Y">1</ORDER_BY_SEQ>
  <NAMES class="R">
   <EMPLID IsChanged="Y">TCS_111</EMPLID>
   <NAME_TYPE IsChanged="Y">PRI</NAME_TYPE>
   <EFFDT IsChanged="Y">2009-07-18</EFFDT>
   <EFF_STATUS IsChanged="Y">A</EFF_STATUS>
   <COUNTRY_NM_FORMAT IsChanged="Y">001</COUNTRY_NM_FORMAT>
   <NAME IsChanged="Y">Doe, John</NAME>
   <NAME_INITIALS/>
   <NAME_PREFIX/>
   <NAME_SUFFIX/>
   <NAME_ROYAL_PREFIX/>
   <NAME_ROYAL_SUFFIX/>
   <NAME_TITLE/>
   <LAST_NAME_SRCH IsChanged="Y">Doe</LAST_NAME_SRCH>
   <FIRST_NAME_SRCH IsChanged="Y">John</FIRST_NAME_SRCH>
   <LAST_NAME IsChanged="Y">Doe</LAST_NAME>
   <FIRST_NAME IsChanged="Y">John</FIRST_NAME>
   <MIDDLE_NAME/>
   <SECOND_LAST_NAME/>
   <SECOND_LAST_SRCH/>
   <NAME_AC/>
   <PREF_FIRST_NAME/>
   <PARTNER_LAST_NAME/>
   <PARTNER_ROY_PREFIX/>
   <LAST_NAME_PREF_NLD IsChanged="Y">1</LAST_NAME_PREF_NLD>
   <NAME_DISPLAY IsChanged="Y">John Doe</NAME_DISPLAY>
   <NAME_FORMAL IsChanged="Y">John Doe</NAME_FORMAL>
   <LASTUPDDTTM IsChanged="Y">2009-07-31T12:43:26.000000-0700</LASTUPDDTTM>
   <LASTUPDOPRID IsChanged="Y">PS</LASTUPDOPRID>
  </NAMES>
  <PSCAMA class="R">
   <AUDIT_ACTN>D</AUDIT_ACTN>
  </PSCAMA>
 </NAME_TYPE_VW>
 <ADDRESS_TYPE_VW class="R">
  <EMPLID IsChanged="Y">TCS_111</EMPLID>
  <ADDRESS_TYPE IsChanged="Y">HOME</ADDRESS_TYPE>
  <ORDER_BY_SEQ IsChanged="Y">1</ORDER_BY_SEQ>
  <ADDRESSES class="R">
   <EMPLID IsChanged="Y">TCS_111</EMPLID>
   <ADDRESS_TYPE IsChanged="Y">HOME</ADDRESS_TYPE>
```

1 Attributes:

Name	Value
class	R

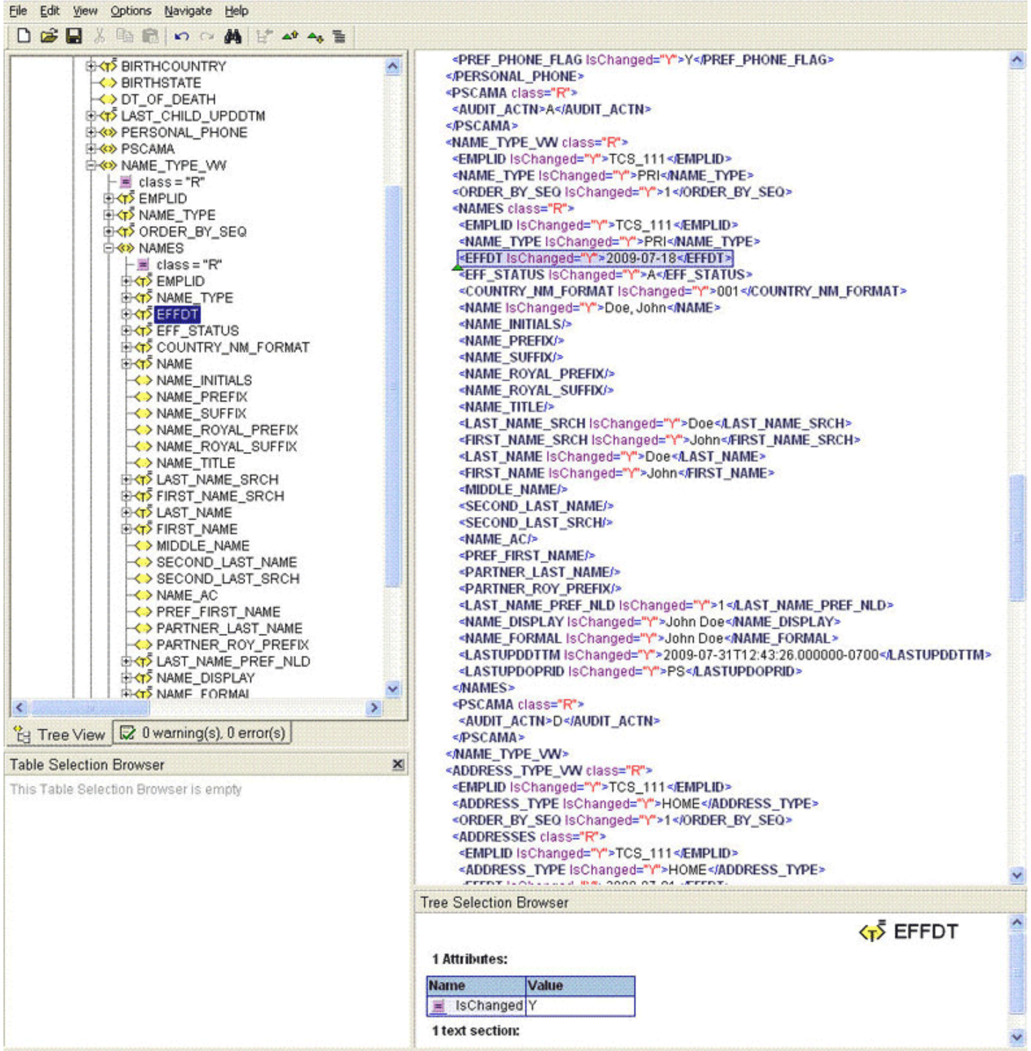
28 Subtags:

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

For example, names can be effective-dated in PeopleSoft. The EFFDT node in XML provides the date on which the name becomes effective for the OIM User.

The EFFDT node is shown in the following screenshot:



```
   <PREF_PHONE_FLAG IsChanged="Y">Y</PREF_PHONE_FLAG>
  </PERSONAL_PHONE>
  <PSCAMA class="R">
   <AUDIT_ACTN>A</AUDIT_ACTN>
  </PSCAMA>
  <NAME_TYPE_VW class="R">
   <EMPLID IsChanged="Y">TCS_111</EMPLID>
   <NAME_TYPE IsChanged="Y">PRI</NAME_TYPE>
   <ORDER_BY_SEQ IsChanged="Y">1</ORDER_BY_SEQ>
   <NAMES class="R">
    <EMPLID IsChanged="Y">TCS_111</EMPLID>
    <NAME_TYPE IsChanged="Y">PRI</NAME_TYPE>
    <EFFDT IsChanged="Y">2009-07-18</EFFDT>
    <EFF_STATUS IsChanged="Y">A</EFF_STATUS>
    <COUNTRY_NM_FORMAT IsChanged="Y">001</COUNTRY_NM_FORMAT>
    <NAME IsChanged="Y">Doe, John</NAME>
    <NAME_INITIALS/>
    <NAME_PREFIX/>
    <NAME_SUFFIX/>
    <NAME_ROYAL_PREFIX/>
    <NAME_ROYAL_SUFFIX/>
    <NAME_TITLE/>
    <LAST_NAME_SRCH IsChanged="Y">Doe</LAST_NAME_SRCH>
    <FIRST_NAME_SRCH IsChanged="Y">John</FIRST_NAME_SRCH>
    <LAST_NAME IsChanged="Y">Doe</LAST_NAME>
    <FIRST_NAME IsChanged="Y">John</FIRST_NAME>
    <MIDDLE_NAME/>
    <SECOND_LAST_NAME/>
    <SECOND_LAST_SRCH/>
    <NAME_AC/>
    <PREF_FIRST_NAME/>
    <PARTNER_LAST_NAME/>
    <PARTNER_ROY_PREFIX/>
    <LAST_NAME_PREF_NLD IsChanged="Y">1</LAST_NAME_PREF_NLD>
    <NAME_DISPLAY IsChanged="Y">John Doe</NAME_DISPLAY>
    <NAME_FORMAL IsChanged="Y">John Doe</NAME_FORMAL>
    <LASTUPDDTTM IsChanged="Y">2009-07-31T12:43:26.000000-0700</LASTUPDDTTM>
    <LASTUPDOPRID IsChanged="Y">PS</LASTUPDOPRID>
   </NAMES>
   <PSCAMA class="R">
    <AUDIT_ACTN>D</AUDIT_ACTN>
   </PSCAMA>
  </NAME_TYPE_VW>
  <ADDRESS_TYPE_VW class="R">
   <EMPLID IsChanged="Y">TCS_111</EMPLID>
   <ADDRESS_TYPE IsChanged="Y">HOME</ADDRESS_TYPE>
   <ORDER_BY_SEQ IsChanged="Y">1</ORDER_BY_SEQ>
   <ADDRESSES class="R">
    <EMPLID IsChanged="Y">TCS_111</EMPLID>
    <ADDRESS_TYPE IsChanged="Y">HOME</ADDRESS_TYPE>
```

1 Attributes:

Name	Value
IsChanged	Y

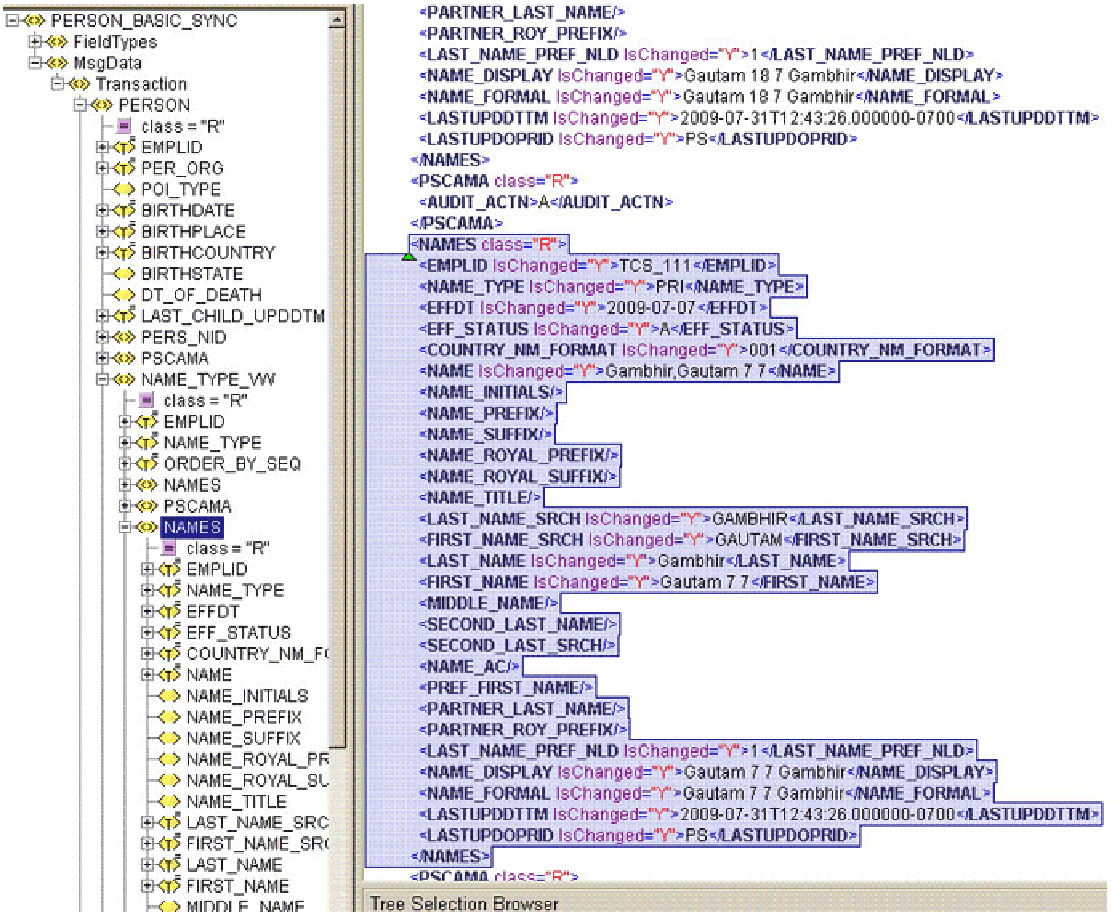
1 text section:

`Primary:` Specifies if the node is a mandatory field on Oracle Identity Manager.

The following scenario illustrates how to map the entries in the lookup definition. On the target system, there is no direct equivalent for the First Name attribute of the OIM User. As a workaround, a combination of elements is used to decipher the value for each Code Key entry in the preceding table.

If you want to retrieve the value for the Code Key, `First Name`, then the name of the NODE will be FIRST_NAME as depicted in the XML file. See the sample XML file in Figure 1-4 for more information about each node in the PERSON_BASIC_SYNC message.

Figure 1-4   Sample XML File for PERSON_BASIC_SYNC Message



```
  <PARTNER_LAST_NAME/>
  <PARTNER_ROY_PREFIX/>
  <LAST_NAME_PREF_NLD IsChanged="Y">1</LAST_NAME_PREF_NLD>
  <NAME_DISPLAY IsChanged="Y">Gautam 18 7 Gambhir</NAME_DISPLAY>
  <NAME_FORMAL IsChanged="Y">Gautam 18 7 Gambhir</NAME_FORMAL>
  <LASTUPDDTTM IsChanged="Y">2009-07-31T12:43:26.000000-0700</LASTUPDDTTM>
  <LASTUPDOPRID IsChanged="Y">PS</LASTUPDOPRID>
</NAMES>
<PSCAMA class="R">
  <AUDIT_ACTN>A</AUDIT_ACTN>
</PSCAMA>
<NAMES class="R">
  <EMPLID IsChanged="Y">TCS_111</EMPLID>
  <NAME_TYPE IsChanged="Y">PRI</NAME_TYPE>
  <EFFDT IsChanged="Y">2009-07-07</EFFDT>
  <EFF_STATUS IsChanged="Y">A</EFF_STATUS>
  <COUNTRY_NM_FORMAT IsChanged="Y">001</COUNTRY_NM_FORMAT>
  <NAME IsChanged="Y">Gambhir,Gautam 7 7</NAME>
  <NAME_INITIALS/>
  <NAME_PREFIX/>
  <NAME_SUFFIX/>
  <NAME_ROYAL_PREFIX/>
  <NAME_ROYAL_SUFFIX/>
  <NAME_TITLE/>
  <LAST_NAME_SRCH IsChanged="Y">GAMBHIR</LAST_NAME_SRCH>
  <FIRST_NAME_SRCH IsChanged="Y">GAUTAM</FIRST_NAME_SRCH>
  <LAST_NAME IsChanged="Y">Gambhir</LAST_NAME>
  <FIRST_NAME IsChanged="Y">Gautam 7 7</FIRST_NAME>
  <MIDDLE_NAME/>
  <SECOND_LAST_NAME/>
  <SECOND_LAST_SRCH/>
  <NAME_AC/>
  <PREF_FIRST_NAME/>
  <PARTNER_LAST_NAME/>
  <PARTNER_ROY_PREFIX/>
  <LAST_NAME_PREF_NLD IsChanged="Y">1</LAST_NAME_PREF_NLD>
  <NAME_DISPLAY IsChanged="Y">Gautam 7 7 Gambhir</NAME_DISPLAY>
  <NAME_FORMAL IsChanged="Y">Gautam 7 7 Gambhir</NAME_FORMAL>
  <LASTUPDDTTM IsChanged="Y">2009-07-31T12:43:26.000000-0700</LASTUPDDTTM>
  <LASTUPDOPRID IsChanged="Y">PS</LASTUPDOPRID>
</NAMES>
<PSCAMA class="R">
```

The PARENT NODE for the NODE FIRST_NAME will be NAMES. Now suppose, you have a scenario where you have multiple FIRST_NAME nodes in the XML file to support the effective-dated feature for this attribute. In this case, you must identify the TYPE NODE for the PARENT NODE that has the value PRI. In this example, the TYPE NODE is NAME_TYPE with the value PRI.

Next, you must locate the EFFECTIVE DATED NODE for `FIRST_NAME` in the XML file. This node provides the value when the event becomes effective-dated.

In Oracle Identity Manager, you must specify a mandatory field, such as `User ID` for reconciliation. This implies that to retrieve the value from XML, you must mention `User ID` as the primary node.

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 using a tilde (~) to create the Decode entry for First Name as follows:

NODE: `FIRST_NAME`

PARENT NODE: `NAMES`

TYPE NODE=Value: `NAME_TYPE=PRI`

EFFECTIVE DATED NODE: `EFFDT`

So, the Decode column for First Name is as follows:

```
FIRST_NAME~NAMES~NAME_TYPE=PRI~EFFDT
```

1.6.4.3.3 Lookup.PSFT.HRMS.PersonBasicSync.Recon

The Lookup.PSFT.HRMS.PersonBasicSync.Recon lookup definition maps the resource object field name with the value fetched from the Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping lookup definition. The following is the format of the values stored in this lookup definition:

Code Key	Decode
Employee Type	Emp Type~Employee Type Lookup
First Name	First Name
Last Name	Last Name
User ID	User 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`

In this format:

`ATTRIBUTE`: Refers to the Code Key of the Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping lookup definition

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

Consider the scenario discussed in Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping. In this example, you fetched First Name from the FIRST_NAME node of the XML file.

Now, you must map this First Name defined in the Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping lookup definition with the resource object attribute First Name defined in the Lookup.PSFT.HRMS.PersonBasicSync.Recon lookup definition Code Key.

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

Code Key: First Name

Decode: First

In other words, the value for First Name in the Lookup.PSFT.HRMS.PersonBasicSync.Recon lookup definition is fetched from First, defined in the attribute mapping lookup definition.

The same process holds true for Last Name and User ID.

However, to fetch the value of the Employee Type resource object, you must consider the Employee Type lookup definition. `Emp Type` is defined in the message-specific attribute lookup, Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping, which has a value `EMP`, which is fetched from the `PER_ORG` node in the XML.

Now, Employee Type Lookup is defined in the message-specific configuration, Lookup.PSFT.Message.PersonBasicSync.Configuration lookup definition. The mapping is as follows:

Code Key: Employee Type Lookup

Decode: Lookup.PSFT.HRMS.PersonBasicSync.EmpType

In other words, you must search the value `EMP` in the Lookup.PSFT.HRMS.PersonBasicSync.EmpType lookup definition. The mapping in the Lookup.PSFT.HRMS.PersonBasicSync.EmpType lookup definition is defined as follows:

Code Key: EMP

Decode: Full-Time

When you create an OIM User, the Employee Type field has Full-Time Employee as the value.

1.6.4.3.4 Lookup.PSFT.HRMS.PersonBasicSync.EmpType

The Lookup.PSFT.HRMS.PersonBasicSync.EmpType lookup definition is used when person data is received for an account.

The lookup definition has the following entries:

Code Key	Decode
EMP	Full-Time
CWR	Part-Time
POI	Temp

In the preceding table:

- CWR represents Contingent Worker.
- EMP represents Employee.
- POI represents Person of Interest.

1.6.4.3.5 Lookup.PSFT.HRMS.PersonBasicSync.Validation

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

The Lookup.PSFT.HRMS.PersonBasicSync.Validation lookup definition is empty by default.

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

1.6.4.3.6 Lookup.PSFT.HRMS.PersonBasicSync.Transformation

The Lookup.PSFT.HRMS.PersonBasicSync.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.HRMS.PersonBasicSync.Transformation lookup definition is empty by default.

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

1.6.4.4 Lookup Definitions Used to Process WORKFORCE_SYNC Messages

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

1.6.4.4.1 Lookup.PSFT.Message.WorkForceSync.Configuration

The Lookup.PSFT.Message.WorkForceSync.Configuration lookup definition provides the configuration-related information for the WORKFORCE_SYNC and WORKFORCE_FULLSYNC messages for reconciliation.

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

Code Key	Decode	Description
Attribute Mapping Lookup	Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping	Name of the lookup definition that maps Oracle Identity Manager attributes with attributes in the WORKFORCE_SYNC and WORKFORCE_FULLSYNC message XML See Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping for more information about this lookup definition.
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.
Custom Query Lookup Definition	Lookup.PSFT.HRMS.CustomQuery	This entry holds the name of the lookup definition that maps resource object fields with OIM User form fields. This lookup definition is used during application of the custom query. See Limited Reconciliation for more information.
Data Node Name	Transaction	Name of the node in the XML files to run a transaction

Code Key	Decode	Description
Employee Status Lookup	Lookup.PSFT.HRMS.WorkForceSync.EmpStatus	Name of the lookup definition that maps the value of the ACTION node retrieved from the WORKFORCE_SYNC message XML with the status to be shown on Oracle Identity Manager for an employee See Lookup.PSFT.HRMS.WorkForceSync.EmpStatus for more information about this lookup definition.
Employee Type Lookup	Lookup.PSFT.HRMS.WorkForceSync.EmpType	Name of the lookup definition that stores all valid person types and components of the Employee person type in the target system See Lookup.PSFT.HRMS.WorkForceSync.EmpType for more information about this lookup definition.
Message Handler Class	oracle.iam.connectors.psft.common.handler.impl.PSFTWorkForceSyncReconMessageHandlerImpl	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. **See Also:** Configuring the Connector Messages.
Message Parser	oracle.iam.connectors.psft.common.parser.impl.JobMessageParser	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. **See Also:** Configuring the Connector Messages.

Code Key	Decode	Description
Recon Lookup Definition	Lookup.PSFT.HRMS.WorkForceSync.Recon	Name of the lookup definition that maps Oracle Identity Manager attribute with Resource Object attribute See Lookup.PSFT.HRMS.WorkForceSync.Recon for more information about this lookup definition.
Resource Object	Peoplesoft HRMS	Name of the resource object
Transformation Lookup Definition	Lookup.PSFT.HRMS.WorkForceSync.Transformation	Name of the transformation lookup definition It is empty by default. See Lookup.PSFT.HRMS.WorkForceSync.Transformation for more information about this lookup definition.
Use Transformation	No	Enter yes to implement transformation while reconciling records. Otherwise, enter no.
Use Validation	No	Enter yes to implement validation while reconciling records. Otherwise, enter no.
Validation Lookup Definition	Lookup.PSFT.HRMS.WorkForceSync.Validation	Name of the validation lookup definition It is empty by default. See Lookup.PSFT.HRMS.WorkForceSync.Validation for more information about this lookup definition.

1.6.4.4.2 Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping

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

Code Key	Decode
Department	DEPTID~JOB~None~EFFDT
Full Part Time	FULL_PART_TIME~JOB~None~EFFDT
Job ID	JOBCODE~JOB~None~EFFDT
Per Org	PER_ORG~JOB~None~EFFDT
Reg Temp	REG_TEMP~JOB~None~EFFDT
Start Date	EFFDT~JOB~None~EFFDT
Status	ACTION~JOB~None~EFFDT
Supervisor ID	SUPERVISOR_ID~JOB~NONE~EFFDT

Code Key	Decode
User ID	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`

In this format:

`NODE`: Name of the node in the WORKFORCE_SYNC message XML file 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, if any.

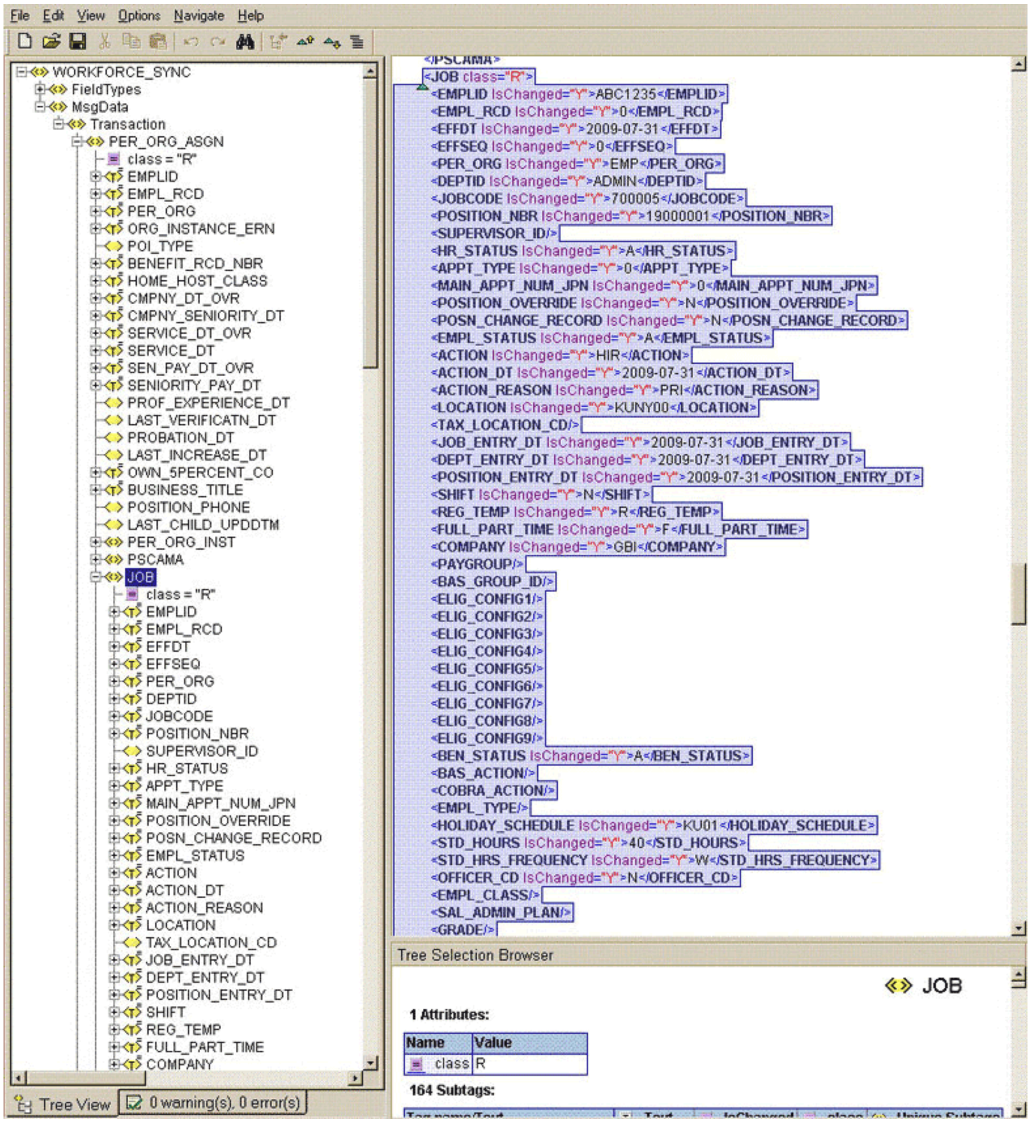
PeopleSoft supports effective-dated events. The value refers to the name of the node that provides information about the date on which the event becomes effective.

For example, Department can be effective-dated in PeopleSoft. The EFFDT node in XML provides the date on which the name becomes effective for the OIM User.

`PRIMARY`: Specifies if the node is a mandatory field.

The following scenario illustrates how to map the entries in the lookup definition. On the target system, there is no direct equivalent for the `Department` attribute of the OIM User. As a workaround, a combination of elements is used to decipher the value. See the sample XML file in Figure 1-5 for more information about each node in the WORKFORCE_SYNC message XML.

Figure 1-5   Sample XML File for WORKFORCE_SYNC Message



```
WORKFORCE_SYNC
  FieldTypes
  MsgData
    Transaction
      PER_ORG_ASGN
        class = "R"
        EMPLID
        EMPL_RCD
        PER_ORG
        ORG_INSTANCE_ERN
        POI_TYPE
        BENEFIT_RCD_NBR
        HOME_HOST_CLASS
        CMPNY_DT_OVR
        CMPNY_SENIORITY_DT
        SERVICE_DT_OVR
        SERVICE_DT
        SEN_PAY_DT_OVR
        SENIORITY_PAY_DT
        PROF_EXPERIENCE_DT
        LAST_VERIFICATN_DT
        PROBATION_DT
        LAST_INCREASE_DT
        OWN_5PERCENT_CO
        BUSINESS_TITLE
        POSITION_PHONE
        LAST_CHILD_UPDDTM
        PER_ORG_INST
        PSCAMA
        JOB
          class = "R"
          EMPLID
          EMPL_RCD
          EFFDT
          EFFSEQ
          PER_ORG
          DEPTID
          JOBCODE
          POSITION_NBR
          SUPERVISOR_ID
          HR_STATUS
          APPT_TYPE
          MAIN_APPT_NUM_JPN
          POSITION_OVERRIDE
          POSN_CHANGE_RECORD
          EMPL_STATUS
          ACTION
          ACTION_DT
          ACTION_REASON
          LOCATION
          TAX_LOCATION_CD
          JOB_ENTRY_DT
          DEPT_ENTRY_DT
          POSITION_ENTRY_DT
          SHIFT
          REG_TEMP
          FULL_PART_TIME
          COMPANY
```

```
</PSCAMA>
<JOB class="R">
  <EMPLID IsChanged="Y">ABC1235</EMPLID>
  <EMPL_RCD IsChanged="Y">0</EMPL_RCD>
  <EFFDT IsChanged="Y">2009-07-31</EFFDT>
  <EFFSEQ IsChanged="Y">0</EFFSEQ>
  <PER_ORG IsChanged="Y">EMP</PER_ORG>
  <DEPTID IsChanged="Y">ADMIN</DEPTID>
  <JOBCODE IsChanged="Y">700005</JOBCODE>
  <POSITION_NBR IsChanged="Y">19000001</POSITION_NBR>
  <SUPERVISOR_ID/>
  <HR_STATUS IsChanged="Y">A</HR_STATUS>
  <APPT_TYPE IsChanged="Y">0</APPT_TYPE>
  <MAIN_APPT_NUM_JPN IsChanged="Y">0</MAIN_APPT_NUM_JPN>
  <POSITION_OVERRIDE IsChanged="Y">N</POSITION_OVERRIDE>
  <POSN_CHANGE_RECORD IsChanged="Y">N</POSN_CHANGE_RECORD>
  <EMPL_STATUS IsChanged="Y">A</EMPL_STATUS>
  <ACTION IsChanged="Y">HIR</ACTION>
  <ACTION_DT IsChanged="Y">2009-07-31</ACTION_DT>
  <ACTION_REASON IsChanged="Y">PRI</ACTION_REASON>
  <LOCATION IsChanged="Y">KUNY00</LOCATION>
  <TAX_LOCATION_CD/>
  <JOB_ENTRY_DT IsChanged="Y">2009-07-31</JOB_ENTRY_DT>
  <DEPT_ENTRY_DT IsChanged="Y">2009-07-31</DEPT_ENTRY_DT>
  <POSITION_ENTRY_DT IsChanged="Y">2009-07-31</POSITION_ENTRY_DT>
  <SHIFT IsChanged="Y">N</SHIFT>
  <REG_TEMP IsChanged="Y">R</REG_TEMP>
  <FULL_PART_TIME IsChanged="Y">F</FULL_PART_TIME>
  <COMPANY IsChanged="Y">GBI</COMPANY>
  <PAYGROUP/>
  <BAS_GROUP_ID/>
  <ELIG_CONFIG1/>
  <ELIG_CONFIG2/>
  <ELIG_CONFIG3/>
  <ELIG_CONFIG4/>
  <ELIG_CONFIG5/>
  <ELIG_CONFIG6/>
  <ELIG_CONFIG7/>
  <ELIG_CONFIG8/>
  <ELIG_CONFIG9/>
  <BEN_STATUS IsChanged="Y">A</BEN_STATUS>
  <BAS_ACTION/>
  <COBRA_ACTION/>
  <EMPL_TYPE/>
  <HOLIDAY_SCHEDULE IsChanged="Y">KU01</HOLIDAY_SCHEDULE>
  <STD_HOURS IsChanged="Y">40</STD_HOURS>
  <STD_HRS_FREQUENCY IsChanged="Y">W</STD_HRS_FREQUENCY>
  <OFFICER_CD IsChanged="Y">N</OFFICER_CD>
  <EMPL_CLASS/>
  <SAL_ADMIN_PLAN/>
  <GRADE/>
```

JOB

1 Attributes:

Name	Value
class	R

164 Subtags:

If you want to fetch the value for the Department Code Key from the XML then the NODE is DEPTID. The PARENT NODE for DEPTID is JOB. There is no Type Node defined for this attribute. Therefore, the value None is specified in the Decode combination. But, you must locate the EFFDT node in the XML for that parent node. In Oracle Identity Manager, you must specify a mandatory field, such as User ID for reconciliation. In other words, it implies that you have to specify User ID as the primary node to retrieve the value from XML.

1.6.4.4.3 Lookup.PSFT.HRMS.WorkForceSync.Recon

This Lookup.PSFT.HRMS.WorkForceSync.Recon lookup definition maps the resource object field name with the value fetched from the Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping lookup definition. The following is the format of the values stored in this lookup definition:

Code Key	Decode
Department	Department
Effective Start Date	Start Date
Employee Type	*PER ORG##REG TEMP##FULL PART TIME~EMPLOYEE TYPE LOOKUP*
Job Code	Job ID
Status	*STATUS~EMPLOYEE STATUS LOOKUP*
Supervisor ID	Supervisor ID
User ID	User 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
```

In this format:

ATTRIBUTE: Refers to the Code Key of the Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping lookup definition

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

Consider the scenario discussed in Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping. In this example, you fetched the `Department` defined in the Code Key column from the `DEPTID` node of the XML file.

Now, you must map this `Department` defined in the Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping lookup definition with the resource object attribute, `Department` defined in the Lookup.PSFT.HRMS.WorkForceSync.Recon lookup definition.

For example, if the name of the Code Key column in the Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping lookup definition is `Dept`, then you must define the mapping as follows:

Code Key: Department

Decode: Dept

In other words, this implies that the value for `Department` in the Lookup.PSFT.HRMS.WorkForceSync.Recon lookup definition is fetched from `Dept` defined in the attribute mapping lookup.

Similarly, values for all other attributes are fetched from the XML.

However, to fetch the value of the `Employee Type` resource object, you must concatenate the values obtained from `Per Org`, `Reg Temp`, and `Full Part Time` resource objects defined in the attribute lookup. This value is then searched in the Employee Type Lookup. The values obtained from each node are combined using a double hash (##).

The `Per Org` defined in the Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping lookup definition has a value `EMP` that is fetched from the `PER_ORG` node in the XML. Similarly, the values obtained for `Reg Temp` and `Full Part Time` from XML are `T` and `P`, respectively. If you combine these values, it becomes a concatenated string of the following format:

```
EMP##T##P
```

Now, you must locate this value in the Employee Type Lookup, which is defined in the message-specific configuration, Lookup.PSFT.Message.WorkForceSync.EmpType lookup definition. The mapping is as follows:

Code Key: EMP##T##P

Decode: Temp

Therefore, during reconciliation, the value for the EMP##T##P employee type is reconciled into the corresponding Employee Type field of Oracle Identity Manager.

1.6.4.4.4 Lookup.PSFT.HRMS.WorkForceSync.EmpStatus

The Lookup.PSFT.HRMS.WorkForceSync.EmpStatus lookup definition maps the value retrieved from the ACTION node of the WORKFORCE_SYNC message XML with the status to be shown on Oracle Identity Manager for the employee.

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

Code Key: ACTION value retrieved from the WORKFORCE_SYNC message XML

Decode: Active or Disabled in Oracle Identity Manager

> **Note:**
>
> You must define the mapping for all Actions to be performed on the target system in this lookup definition.

Code Key	Decode
ADD	Active
ADL	Active
ASG	Disabled
BON	Active
COM	Disabled
DEM	Disabled
DTA	Disabled
FSC	Disabled
HIR	Active
JED	Disabled
JRC	Active
LOA	Disabled
LOF	Disabled
LTO	Disabled
PAY	Active

Code Key	Decode
PLA	Disabled
POI	Active
POS	Disabled
PRB	Disabled
PRO	Active
REC	Active
STD	Disabled
SUB	Disabled
TDL	Disabled
TER	Disabled
TWB	Disabled
TWP	Disabled
XFR	Active

For example, for the action HIRE for an employee, the data fetched from the ACTION node of the XML message is `HIR`. The Decode column of the lookup definition stores the corresponding mapping for this action. To display `Active` on Oracle Identity Manager for the action HIRE, you must define the following mapping:

Code Key: HIR

Decode: Active

See Setting Up the Lookup.PSFT.HRMS.WorkForceSync.EmpStatus Lookup Definition for adding an entry in this lookup definition.

1.6.4.4.5 Lookup.PSFT.HRMS.WorkForceSync.EmpType

The connector can reconcile all valid person types that are stored in the target system, and all components of the Employee person type. The following example describes how this is done.

The record of a temporary, part-time, Contingent Worker is reconciled from the target system. During reconciliation, you use the Lookup.PSFT.HRMS.WorkForceSync.EmpType lookup definition to determine the Employee Type field to which the person type is mapped. In this lookup definition, the person type value from the target system is used as the Code Key, and its corresponding Decode value is used to fill the specific Employee Type field. Therefore, during reconciliation, the value of the temporary, part-time, Contingent Worker person type is reconciled into the corresponding Employee Type field of Oracle Identity Manager.

The Lookup.PSFT.HRMS.WorkForceSync.EmpType lookup definition has the following entries:

> **Note:**
>
> The Decode values are case-sensitive.

Code Key	Decode
CWR##R##D	Consultant
CWR##R##F	Consultant
CWR##R##P	Full-Time
CWR##T##D	Consultant
CWR##T##F	Temp
CWR#T##P	Intern
EMP##R##D	Consultant
EMP##R##F	Full-Time
EMP##R##P	Temp
EMP##T##D	Consultant
EMP##T##F	Part-Time
EMP##T##P	Temp
POI##R##D	Consultant
POI##R##F	Full-Time
POI##R##P	Temp
POI##T##D	Consultant
POI##T##F	Part-Time
POI##T##P	Temp

In the preceding table:

- CWR represents Contingent Worker.
- EMP represents Employee.
- POI represents Person of Interest.
- R represents Regular.
- T represents Temporary.
- D represents On-Demand.
- F represents Full Time.
- P represents Part Time.

1.6.4.4.6 Lookup.PSFT.HRMS.WorkForceSync.Validation

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

The Lookup.PSFT.HRMS.WorkForceSync.Validation lookup is empty by default.

1.6.4.4.7 Lookup.PSFT.HRMS.WorkForceSync.Transformation

The Lookup.PSFT.HRMS.WorkForceSync.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.HRMS.WorkForceSync.Transformation lookup is empty by default.

1.6.4.5 Other Lookup Definitions

The following are the predefined generic lookup definitions:

1.6.4.5.1 Lookup.PSFT.HRMS.ExclusionList

The Lookup.PSFT.HRMS.ExclusionList lookup definition provides a list of user IDs or person IDs that cannot be created on Oracle Identity Manager.

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

Code Key: User ID resource object field name

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

See Setting Up the Lookup.PSFT.HRMS.ExclusionList Lookup Definition for more information.

1.6.4.5.2 Lookup.PSFT.HRMS.CustomQuery

You can configure limited reconciliation to specify the subset of target system records that must be fetched into Oracle Identity Manager. This subset is defined on the basis of attribute values that you specify in a query condition, which is then applied during reconciliation.

The Lookup.PSFT.HRMS.CustomQuery lookup definition maps resource object fields with OIM User form fields. It is used during application of the query condition that you create. See Limited Reconciliation for more information. Setting Up the Lookup.PSFT.HRMS.CustomQuery Lookup Definition provides instructions on how to add an entry in this lookup definition.

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

Code Key: Resource object field name

Decode: Column name of the USR table

Code Key	Decode
Department	USR_UDF_DEPARTMENT_ID
Effective Start Date	Users.Start Date
Employee Type	Users.Role
First Name	Users.First Name
Last Name	Users.Last Name
Manager ID	Users.Manager Login
Manager Name	USR_UDF_MANAGER_NAME
Organization Name	Organizations.Organization Name
Status	Users.Status

Code Key	Decode
Supervisor ID	USR_UDF_SUPERVISOR_ID
User ID	Users.User ID
User Type	Users.Xellerate Type

1.7 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 provides information about the tasks that must be performed each time you want to run reconciliation.
- Extending the Functionality of the Connector describes procedures that you can perform to extend the functionality of the connector.
- Testing and Troubleshooting provides information about testing the connector.
- Known Issues and Workarounds lists the known issues associated with this release of the connector.
- Determining the Root Audit Action Details provides information about root audit action.
- Configuring the Connector Messages describes the procedure to configure the connector messages of release 9.1.0.*x.y* with that of the current release.
- 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:

> **Note:**
>
> In this guide, PeopleSoft HRMS is referred to as the **target system**.

- Preinstallation
- Installation
- Postinstallation
- Upgrading the Connector

2.1 Preinstallation

Preinstallation information is divided across the following sections:

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

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topic:

2.1.1.1 Files and Directories on the Installation Media

Table 2-1 lists the files and directories on the installation media.

Table 2-1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
configuration/ PSFT_Employee_Reconciliation-CI.xml	This XML file contains configuration information that is used during connector installation.
JavaDoc	This directory contains information about the Java APIs used by the connector.
lib/PSFT_ER-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.

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

File in the Installation Media Directory	Description
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 README.txt	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 is the deployment script, which contains configurations to deploy the listener. The deploy.properties file contains Oracle Identity Manager connection details. The README.txt file contains instructions to deploy, remove, and redeploy the listener.
The following project files in the peoplecode directory: OIM_ER OIM_ER_DELETE	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_ER.ini • OIM_ER.xml • OIM_ER_DELETE.ini • OIM_ER_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/lib/PSFTTest.jar	This JAR file is used by the testing utility for reconciliation.
test/scripts/InvokeListener.bat test/scripts/InvokeListener.sh	This BAT file and the UNIX shell script call the testing utility for reconciliation.
xml/PeoplesoftHRMS-ConnectorConfig.xml	This XML file contains definitions for the connector components. • Resource object • Process definition • IT resource type • Reconciliation rules • Scheduled tasks • Lookup definitions

2.1.2 Preinstallation on the Target System

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

You must create limited rights users who have restricted rights to access resources in the production environment to perform PeopleSoft-specific installation or maintenance operations.

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

2.1.2.1 Importing a Project from Application Designer

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

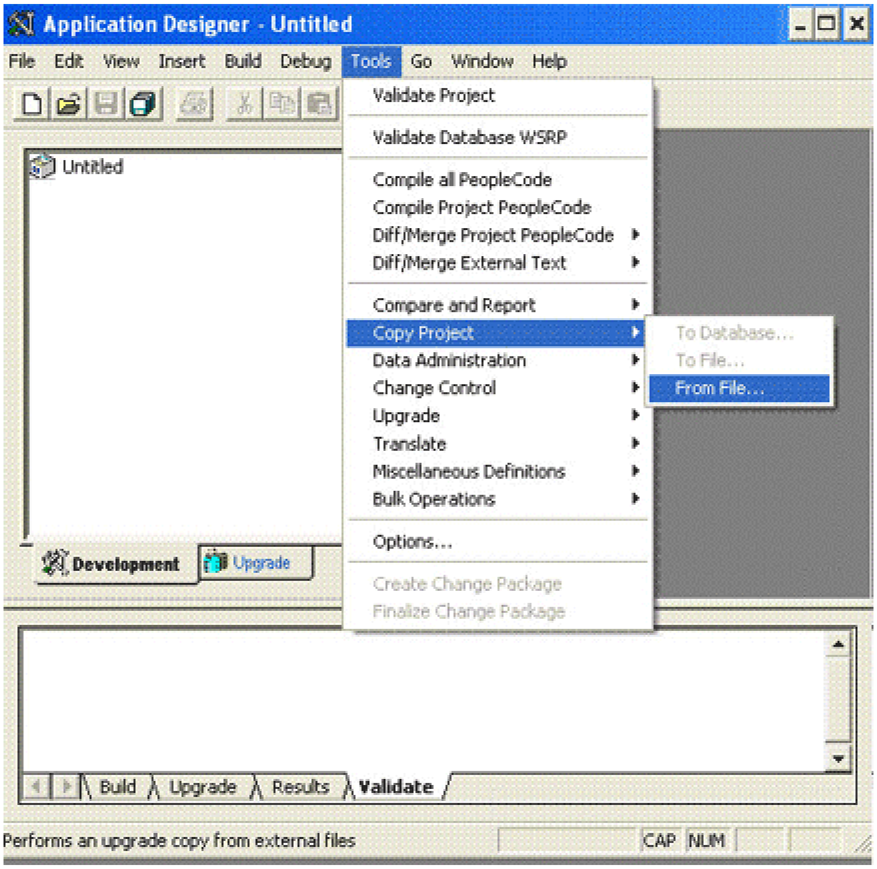
You can import the OIM_ER project created in Application Designer to automate the steps for creating a permission list. You can also create a permission list by manually performing the steps described in Creating a Permission List If you import the project, OIM_ER then you need not perform the steps mentioned in this section.

> **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/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/peoplecode/OIM_ER
>
> *OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/peoplecode/OIM_ER_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.**



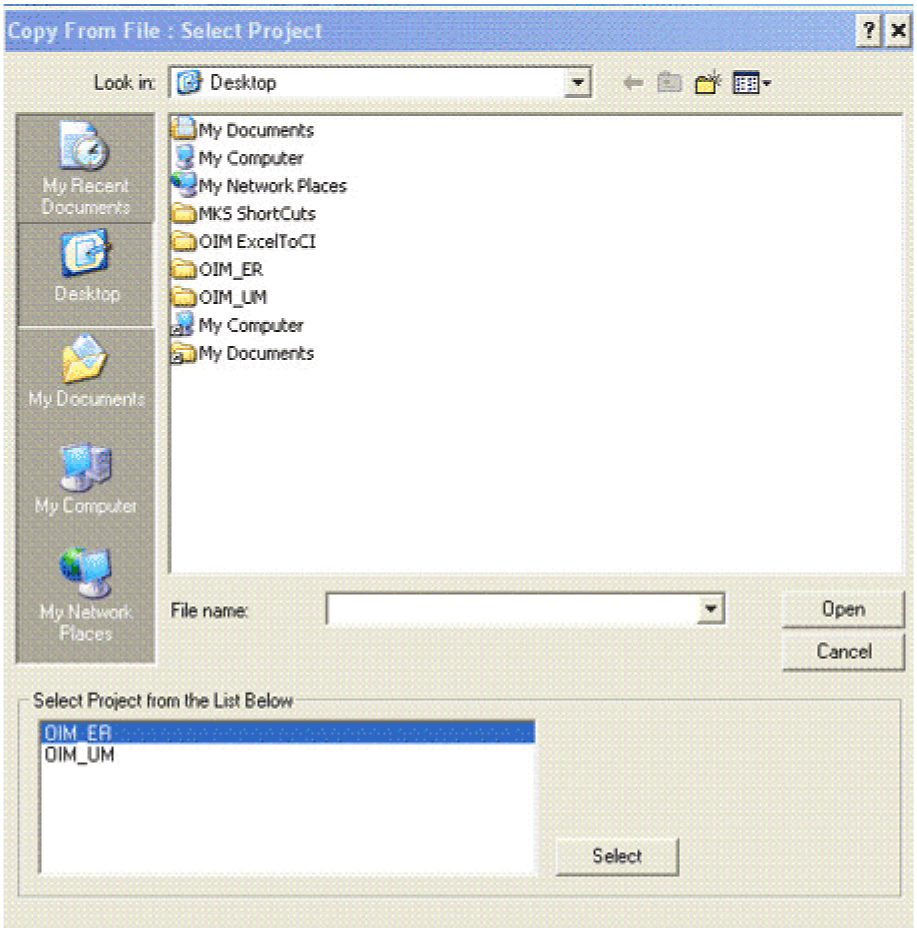
The Copy From File : Select Project dialog box appears.

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_ER.ini and OIM_ER.xml files in OIM_ER folder.

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



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

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

2.1.2.2 Creating a Target System User Account for Connector Operations

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

The following sections describe the procedures to create this target system account:

> **Note:**
>
> For creating the target system account, you must log into 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

2.1.2.2.1 Creating a Permission List

To create a permission list:

> **Note:**
>
> You can skip this section if you have imported a project from Application Designer. See 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, expand **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, `OIMER`, and then click **Add.**
4. On the General tab, enter a description for the permission list in the **Description** field.
5. On the Pages tab, click the search icon for Menu Name and perform the following:
   a. 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**.

   b. 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

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

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

e. 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.**

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

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

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

i. 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.**

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

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

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

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

n. On the Component Permissions page, click **Edit Pages** for the EO_EFFDTPUB component name.

o. Click **Select All,** and then click **OK.** Click **OK** on the Components Permissions page. The application returns to the Pages tab.

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

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

   - App Engine Program
   - Message
   - Component
   - Project

- Application Package

8. Click **OK.**
9. 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.
10. Click **OK.** The application returns to the People Tools tab.
11. On the Process tab, click the **Process Group Permissions** link. The Process Group Permission page is displayed.
12. In the Process Group lookup, click the search icon. From the list, select **TLSALL.**
13. On the Process Group Permission page, click the plus sign (+) to add another row for **Process Group.**
14. In the Process Group lookup, click the search icon. From the list, select **STALL.** The application returns to the Process Group Permission page.
15. Click **OK.**
16. 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.

2.1.2.2.2 Creating a Role for a Limited Rights User

To create a role for a limited rights user:

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

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

   For example:

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

2. In the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier releases, expand **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, `OIMER`, 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 `OIMER` and then click **Lookup.** From the list, select **OIMER.**
   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 and above, 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.**

6. Click **Save.**

2.1.2.2.3 Assigning the Required Privileges to the Target System Account

To assign the required privileges to the target system account:

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, expand **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, `OIMER,` 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 `OIMER` and then click **Lookup.** From the list, select **OIMER.** 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:
   a. In the Roles lookup, enter `OIMER` and then click **Lookup.** From the list, select **OIMER.**
   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, and is hence not applicable.

f. Click **Save** to save this user profile. This profile is also used for a person with limited rights in PeopleSoft for performing all reconciliation-related configurations.

2.2 Installation

Installation information is divided across the following sections:

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

2.2.1 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
- IT Resource Parameters
- Deploying the PeopleSoft Listener
- Removing the PeopleSoft Listener

2.2.1.1 Running the Connector Installer

To run the Connector Installer:

1. Create a directory for the connector, for example, PSFT_ER-11.1.1.5.0, in the *OIM_HOME*/server/ConnectorDefaultDirectory directory.
2. Copy the contents of the connector installation media directory into directory created in Step 1.
3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.*x:*
     a. Log in to the Administrative and User Console.

    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 Identity System Administration.

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

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

5. From the Connector List list, select **PeopleSoft Employee Reconciliation 11.1.1.5.0.** 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 list, click **Refresh**.

   c. From the Connector List list, select **PeopleSoft Employee Reconciliation 11.1.1.5.0.**

6. Click **Load**.

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

   The following tasks are performed, in sequence:

   a. Configuration of connector libraries

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

   c. Compilation of adapter definitions

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

   - Retry the installation by clicking **Retry.**

   - Cancel the installation and begin again from Step 1.

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

   a. Configuring the IT resource for the connector

      See Configuring the IT Resource for more information.

   b. Configuring the scheduled tasks

      See Configuring Scheduled Tasks 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.

2.2.1.2 Copying the Connector Files and External Code Files

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

If the connector files are extracted to the *OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/ directory on the Oracle Identity Manager host computer, then there is no need to copy these files manually.

Note:

- The directory paths given in the first column of this table correspond to the location of the connector files in the PeopleSoft Employee Reconciliation directory 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.
- While installing Oracle Identity Manager in a cluster, you copy the contents of the installation directory to each node of the cluster. Then, restart each node. Similarly, after you install the connector, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster.

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
lib/PeopleSoftOIMListener.ear	*OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/listener
Files in the test/scripts directory	*OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/scripts
Files in the test/config directory	*OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/config

2.2.1.3 Configuring the IT Resource

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

When you run the Connector Installer, the `PSFT HRMS` 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 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, then under Configuration, click **IT Resource.**
4. In the IT Resource Name field on the Manage IT Resource page, enter `PSFT HRMS` and then click **Search.**
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters.**
7. Specify values for the parameters discussed in Table 2-3. The remaining parameters of IT resource are not applicable for this connector.
8. To save the values, click **Update.**

2.2.1.4 IT Resource Parameters

Table 2-3 lists the IT resource parameters applicable to the connector.

Table 2-3   IT Resource Parameters

Parameter	Description
Configuration Lookup	This parameter holds the name of the lookup definition that contains configuration information. Default value: `Lookup.PSFT.HRMS.Configuration` **Note:** You must not change the value of this parameter. However, if you create a copy of all the connector objects, then you can specify the unique name of the copy of this lookup definition as the value of the Configuration Lookup Name parameter in the copy of the IT resource.
IsActive	This parameter is used to specify whether the specified IT Resource is in use or not. Enter one of the following as the value of the IsActive parameter: Enter `yes` as the value to specify that the target system installation represented by this IT resource is active. If you specify yes as the value, then the connector processes messages sent from this target system installation. Enter `no` as the value if you do not want the connector to process messages sent from this target system installation. Default value: `Yes`

2.2.1.5 Deploying the PeopleSoft 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 IBM WebSphere Application Server
- Deploying the PeopleSoft Listener on WebSphere Application Server
- Importing Oracle Identity Manager CA Root Certificate into PeopleSoft WebServer

2.2.1.5.1 Prerequisites for 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:**
>
> - If you have already deployed a listener for the PeopleSoft User Management connector, then you can skip this procedure.
>
>   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.
> - 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.
> - If you are using IBM WebSphere Application Server, then perform the procedure described in Deploying the PeopleSoft Listener on WebSphere Application Server.
> - If you are using Oracle Identity Governance 12c, then deploying and pinging PeopleSoft listener operations may not work as expected. Apply PeopleSoft Connector Patch 26419438 by using the following URL for these operations to work successfully: `https://support.oracle.com/`

> **See Also:**
>
> Upgrading the PeopleSoft Listener for information about upgrading the 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`
  - *WL_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 *WL_HOME*/server/lib directory:
  1. Change directories to *WL_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 *WL_HOME*/../modules/ directory.
- Start Oracle Identity Manager and the Admin Server.

2.2.1.5.2 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_ER-11.1.1.5.0.
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.

2.2.1.5.3 Prerequisites for Deploying the PeopleSoft Listener on IBM 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_ER-11.1.1.5.0/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
     ```

2.2.1.5.4 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`.

2.2.1.5.5 Importing Oracle Identity Manager CA Root Certificate into PeopleSoft WebServer

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 do so, perform one of the following procedures depending on the PeopleSoft WebServer you are using:

- For Oracle 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.

- For IBM 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.

2.2.1.6 Removing the PeopleSoft Listener

> **Note:**
>
> - This section is not a part of installation on Oracle Identity Manager. You might need this procedure to extend the connector.
> - If you uninstall the connector, you must also remove the listener. Installing a new connector over a previously deployed listener creates discrepancies.
> - Do not remove the listener if the PeopleSoft User Management connector is installed and if it is using the listener.

> **See Also:**
>
> Upgrading the PeopleSoft Listener for information about upgrading the listener

To remove the PeopleSoft listener:

- Removing the PeopleSoft Listener for BM WebSphere Application Server
- Removing the PeopleSoft Listener for Oracle WebLogic Server

2.2.1.6.1 Removing the PeopleSoft Listener for BM WebSphere Application Server

To remove the PeopleSoft listener for IBM WebSphere Application Server:

1. Log in to the WebSphere Admin console.
2. Expand **Applications.**

3. Select **Enterprise Applications** from the list.

   A list of deployed applications is shown in 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.**

2.2.1.6.2 Removing the PeopleSoft Listener for Oracle WebLogic Server

From the listener directory, run the following command:

```
ant undeploy
```

To remove the PeopleSoft listener of the connector of a previous release:

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.

2.2.2 Installation on the Target System

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

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

2.2.2.1 Configuring the Target System for Full Reconciliation

As described in About the Connector, full reconciliation is used to reconcile all existing person data into Oracle Identity Manager. The PeopleCode that is activated in response to these events extracts the required person data through the following components:

For PeopleSoft 9.0:

PERSONAL_DATA, JOB_DATA, JOB_DATA_EMP, JOB_DATA_CONCUR, and JOB_DATA_CWR

Configuring the target system for full reconciliation involves creation of XML files for full reconciliation by performing the following procedures:

- Configuring the PeopleSoft Integration Broker
- Configuring the PERSON_BASIC_FULLSYNC Service Operation
- Configuring the WORKFORCE_FULLSYNC Service Operation

2.2.2.1.1 Configuring the PeopleSoft Integration Broker

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

- Configuring PeopleSoft Integration Broker Gateway
- Configuring PeopleSoft Integration Broker

2.2.2.1.1.1 Configuring PeopleSoft Integration Broker Gateway

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

To configure the PeopleSoft Integration Broker gateway:

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

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

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

   For example:

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

2. To display the Gateway component details:

   - 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
   IPADDRESS: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`.

2.2.2.1.1.2 Configuring PeopleSoft Integration Broker

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

To configure PeopleSoft Integration Broker, create a remote node as follows:

1. In the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier click, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Nodes.**
   - For PeopleTools 8.55, 8.56, and 8.57, click **NavBar**, **Navigator**, **PeopleTools**, **Integration Broker, Integration Setup**, and then click **Nodes.**
2. On the Add a New Value tab, enter the node name, for example, `OIM_FILE_NODE`, and then click **Add.**
3. 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`.
4. Make this node a remote node by deselecting the **Local Node** check box and selecting the **Active Node** check box.
5. Ensure that the Node Type is **PIA.**
6. For PeopleTools 8.56 or earlier, perform the following steps. If you are using PeopleTools 8.57, skip this step and perform step 7.
   a. On the Connectors tab, search for the following information by clicking the Lookup icon:

Gateway ID: LOCAL

Connector ID: FILEOUTPUT

b. 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: Any location writable by the Integration Broker. This location is used to generate the full data publish files.

Property ID: PROPERTY

Property Name: Password

Required value: Same value as of **ig.fileconnector.password** in the integrationGateway.properties file. If the password is not already encrypted, that you can encrypt it as follows:

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

ii) Click **Encrypt.**

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

> **Note:**
>
> To locate the intergrationGateway.properties file, perform the following steps using the PeopleSoft administrator credentials:
>
> i. In PeopleSoft Internet Architecture:
>
>   - 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**
>
> ii. In the Integration Gateway ID field, enter `LOCAL`, and then click **Search.**
>
> iii. Click the **Gateway Setup Properties** link.
>
>   You are prompted to enter the user ID and password.
>
> iv. Specify the following values:
>
>   In the UserID field, enter the appropriate user ID.
>
>   In the Password field, enter the appropriate password.

7. For PeopleTools 8.57, perform the following steps:

   a. On the Connectors tab of the PeopleSoft Internet Architecture window, search for the following information by clicking the Lookup icon:

      Gateway ID: LOCAL

      Connector ID: FTPTARGET

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

      Property ID: HEADER

      Property Name: sendUncompressed

      Required value: Y

      Property ID: FTPTARGET

      Property Name: HOSTNAME

      Required value: Enter the hostname of the computer on which you want to generate the files. You can also give OIM hostname if ftp port is open.

      Property ID: FTPTARGET

      Property Name: USERNAME

      Required value: Enter the hostname of the computer on which you want to generate the files.

      Property ID: FTPTARGET

      Property Name: PASSWORD

      Required value: Enter the password of the computer on which you want to generate the files. Password should be in encrypted form. If the password is not already encrypted, then you can encrypt it as follows:

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

ii) Click **Encrypt**.

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

Property ID: FTPTARGET

Property Name: TYPE

Required value: ASCII

Property ID: FTPTARGE

Property Name: METHOD

Required value: PUT

Property ID: FTPTARGET

Property Name: FTPS

Required value: N

Property ID: FTPTARGET

Property Name: FTPMODE

Required value: ACTIVE

Property ID: FTPTARGET

Property Name: DIRECTORY

Required value: Enter the location where you want to generate xmls.

Property ID: FTPTARGET

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

2.2.2.1.2 Configuring the PERSON_BASIC_FULLSYNC Service Operation

The PERSON_BASIC_FULLSYNC message contains the basic personal information about all the persons. This information includes the Employee ID, First Name, Last Name, and Employee Type.

To configure the PERSON_BASIC_FULLSYNC service operation perform the following procedures:

> **Note:**
>
> The procedure remains the same for PeopleTools 8.49 with HRMS 9.0, PeopleTools 8.50 with HRMS 9.1, PeopleTools 8.53 through 8.57 with HRMS 9.2. The screenshots are taken on PeopleTools 8.49 version. Publishing Messages With VERSION_5 contains a summary of the procedure for PeopleTools 8.51 with HRMS 9.1.

- Activating the PERSON_BASIC_FULLSYNC Service Operation
- Verifying the Queue Status for the PERSON_BASIC_FULLSYNC Service Operation
- Setting Up the Security for the PERSON_BASIC_FULLSYNC Service Operation
- Defining the Routing for the PERSON_BASIC_FULLSYNC Service Operation
- Displaying the EI Repository Folder
- Activating the PERSON_BASIC_FULLSYNC Message
- Activating the Full Data Publish Rule
- Publishing Messages With VERSION_5

2.2.2.1.2.1 Activating the PERSON_BASIC_FULLSYNC Service Operation

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

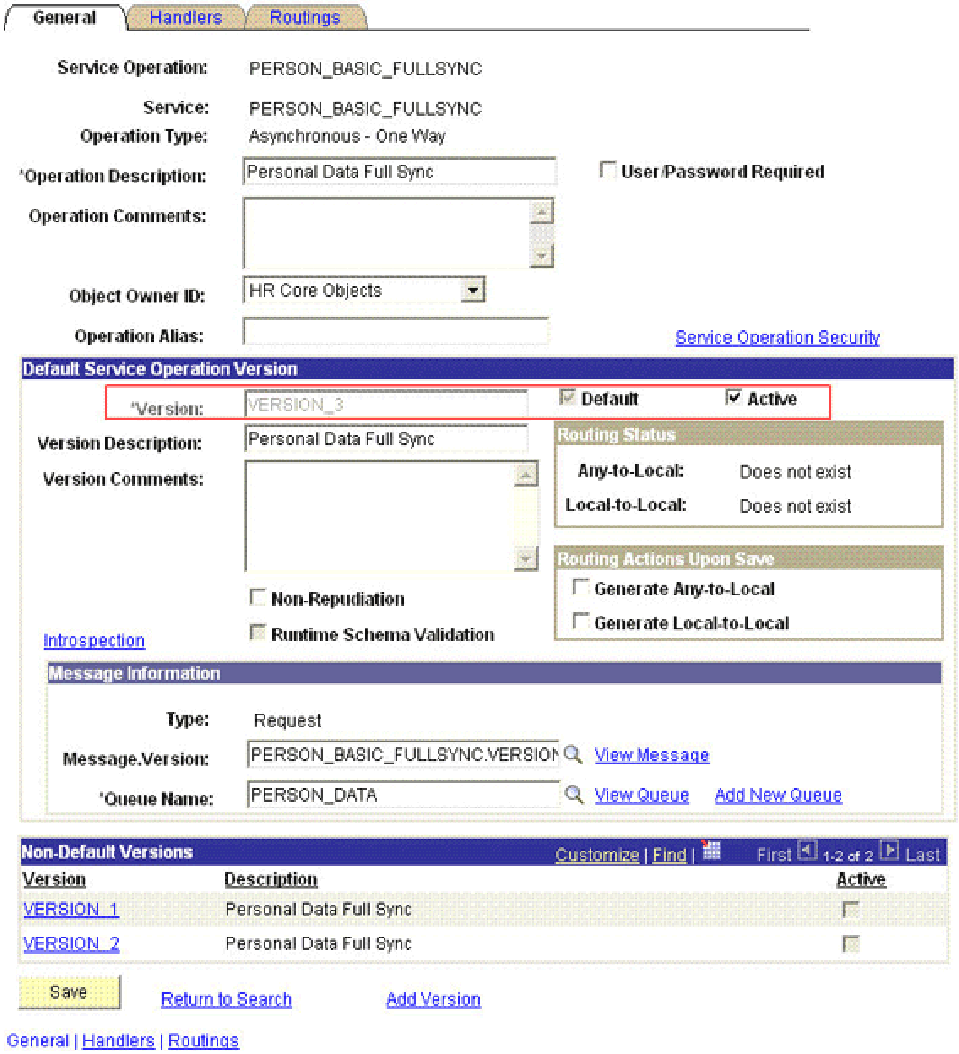
To activate the PERSON_BASIC_FULLSYNC service operation:

> **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 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. On the Find Service Operation tab, enter `PERSON_BASIC_FULLSYNC` in the **Service** field, and then click **Search.**
3. Click the **PERSON_BASIC_FULLSYNC** link.

   > **Note:**
   >
   > In PeopleSoft HRMS, there are three versions of the message associated with this service operation. But, when you integrate PeopleSoft HRMS 9.0 or later and Oracle Identity Manager, you must use the default version `VERSION_3`.

   The following screenshot displays the default version associated with this service operation:



Service Operation: PERSON_BASIC_FULLSYNC

Service: PERSON_BASIC_FULLSYNC

Operation Type: Asynchronous - One Way

*Operation Description: Personal Data Full Sync   □ User/Password Required

Operation Comments:

Object Owner ID: HR Core Objects

Operation Alias:

Default Service Operation Version

*Version: VERSION_3   ☑ Default   ☑ Active

Version Description: Personal Data Full Sync

Version Comments:

□ Non-Repudiation

□ Runtime Schema Validation

Routing Status

Any-to-Local: Does not exist

Local-to-Local: Does not exist

Routing Actions Upon Save

□ Generate Any-to-Local

□ Generate Local-to-Local

Message Information

Type: Request

Message.Version: PERSON_BASIC_FULLSYNC.VERSION

*Queue Name: PERSON_DATA

Non-Default Versions

Version	Description	Active
VERSION_1	Personal Data Full Sync	□
VERSION_2	Personal Data Full Sync	□

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

2.2.2.1.2.2 Verifying the Queue Status for the PERSON_BASIC_FULLSYNC Service Operation

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

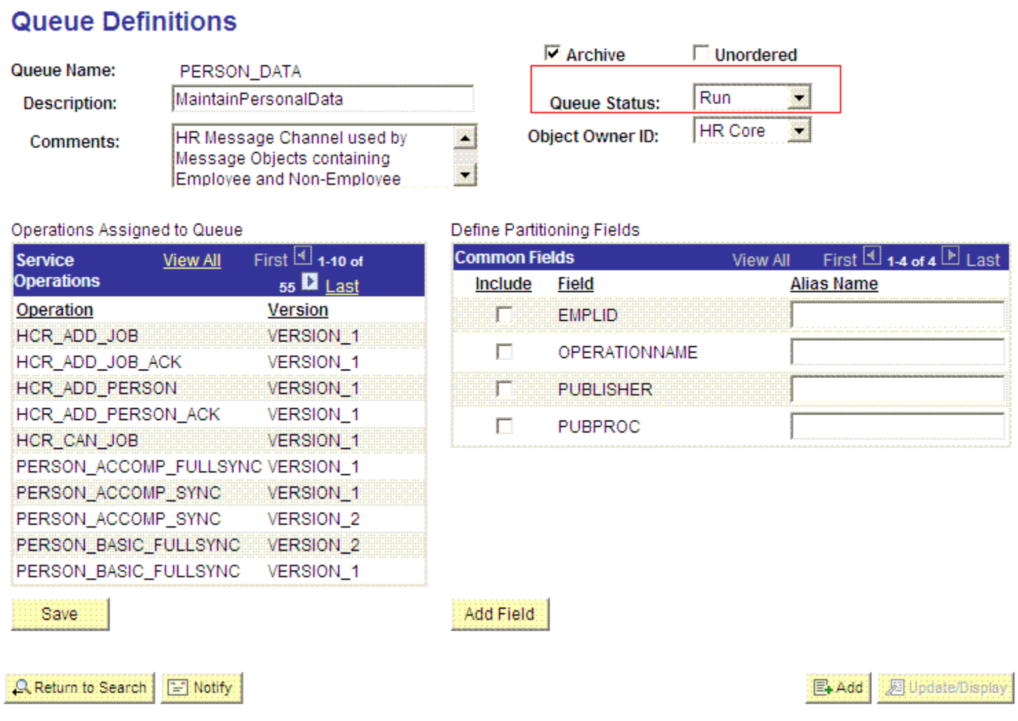
To ensure that the status of the queue for the PERSON_BASIC_FULLSYNC service operation is Run:

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 **PERSON_DATA** 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.**

The queue status is highlighted in the following screenshot:



Queue Definitions

Queue Name: PERSON_DATA

Description: MaintainPersonalData

Comments: HR Message Channel used by Message Objects containing Employee and Non-Employee

☑ Archive ☐ Unordered

Queue Status: Run

Object Owner ID: HR Core

Operations Assigned to Queue

Service Operations — View All — First 1-10 of 55 Last

Operation	Version
HCR_ADD_JOB	VERSION_1
HCR_ADD_JOB_ACK	VERSION_1
HCR_ADD_PERSON	VERSION_1
HCR_ADD_PERSON_ACK	VERSION_1
HCR_CAN_JOB	VERSION_1
PERSON_ACCOMP_FULLSYNC	VERSION_1
PERSON_ACCOMP_SYNC	VERSION_1
PERSON_ACCOMP_SYNC	VERSION_2
PERSON_BASIC_FULLSYNC	VERSION_2
PERSON_BASIC_FULLSYNC	VERSION_1

Define Partitioning Fields

Common Fields — View All — First 1-4 of 4 Last

Include	Field	Alias Name
☐	EMPLID	
☐	OPERATIONNAME	
☐	PUBLISHER	
☐	PUBPROC	

4. Click **Return to Search.**

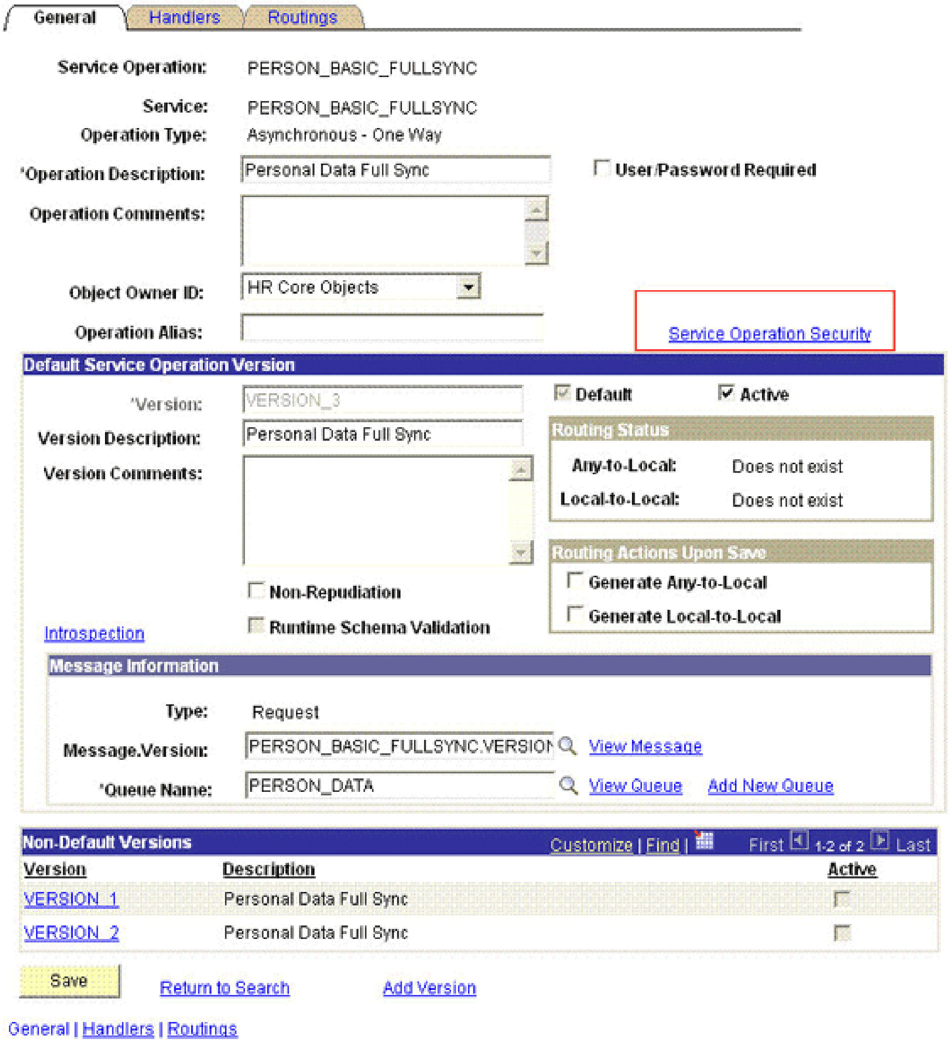
2.2.2.1.2.3 Setting Up the Security for the PERSON_BASIC_FULLSYNC Service Operation

A person on the target system who has permission to modify or add personal or job information of a person 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 PERSON_BASIC_FULLSYNC service operation:

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

   The link is highlighted in the following screenshot:



Service Operation: PERSON_BASIC_FULLSYNC

Service: PERSON_BASIC_FULLSYNC

Operation Type: Asynchronous - One Way

*Operation Description: Personal Data Full Sync

□ User/Password Required

Operation Comments:

Object Owner ID: HR Core Objects

Operation Alias:

Service Operation Security

Default Service Operation Version

*Version: VERSION_3

☑ Default ☑ Active

Version Description: Personal Data Full Sync

Version Comments:

Routing Status

Any-to-Local:	Does not exist
Local-to-Local:	Does not exist

Routing Actions Upon Save

□ Generate Any-to-Local

□ Generate Local-to-Local

□ Non-Repudiation

□ Runtime Schema Validation

Introspection

Message Information

Type: Request

Message.Version: PERSON_BASIC_FULLSYNC.VERSION View Message

*Queue Name: PERSON_DATA View Queue Add New Queue

Non-Default Versions Customize | Find | First 1-2 of 2 Last

Version	Description	Active
VERSION_1	Personal Data Full Sync	□
VERSION_2	Personal Data Full Sync	□

Save Return to Search Add Version

General | Handlers | Routings

4. Attach the **OIMER** permission list to the PERSON_BASIC_FULLSYNC service operation. This list is created in Step 3 of the preinstallation procedure discussed in Creating a Permission List.

   To attach the permission list:

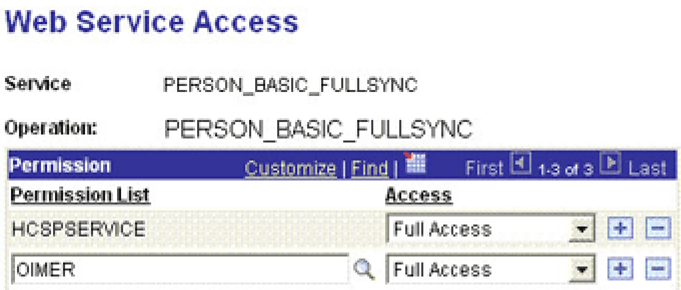
   a. Click the plus sign (+) to add a row to the Permission List field.

   b. In the Permission List field, enter `OIMER` and then click the Look up Permission List icon.

      The **OIMER** permission list appears.

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

      The following screenshot displays the preceding steps:



Web Service Access

Service PERSON_BASIC_FULLSYNC

Operation: PERSON_BASIC_FULLSYNC

Permission List	Access
HCSPSERVICE	Full Access
OIMER	Full Access

d. Click **Save.**

e. Click **Return to Search.**

2.2.2.1.2.4 Defining the Routing for the PERSON_BASIC_FULLSYNC Service Operation

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

To define the routing for PERSON_BASIC_FULLSYNC service operation:

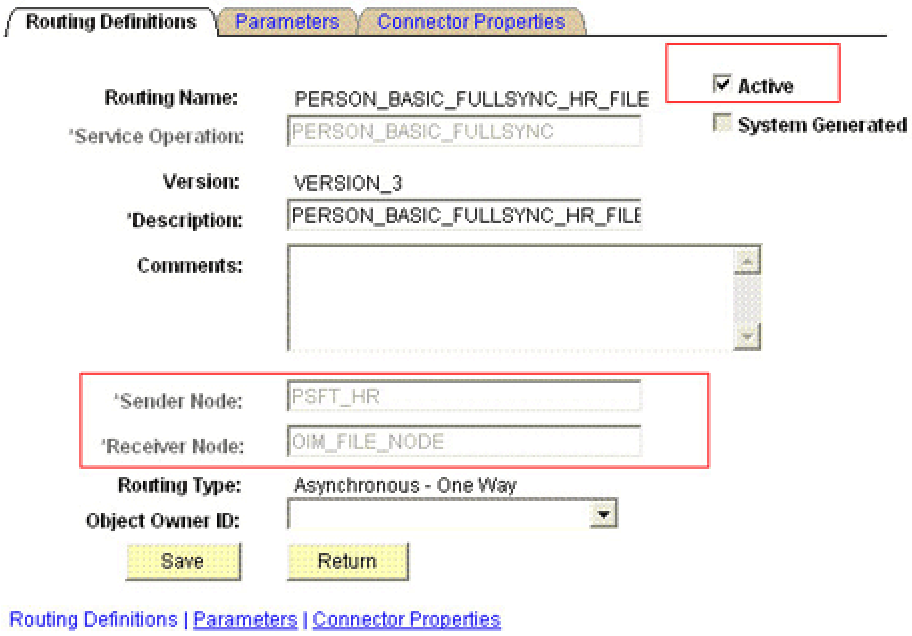
1. On the Routing tab, enter `PERSON_BASIC_FULLSYNC_HR_FILE` as the routing name and then click **Add.**
2. On the Routing Definitions tab, enter the following:

   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_FILE_NODE`

   The following screenshot displays the Sender and Receiver nodes:



Routing Name: PERSON_BASIC_FULLSYNC_HR_FILE

☑ Active

□ System Generated

*Service Operation: PERSON_BASIC_FULLSYNC

Version: VERSION_3

*Description: PERSON_BASIC_FULLSYNC_HR_FILE

Comments:

*Sender Node: PSFT_HR

*Receiver Node: OIM_FILE_NODE

Routing Type: Asynchronous - One Way

Object Owner ID:

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

2.2.2.1.2.5 Displaying the EI Repository Folder

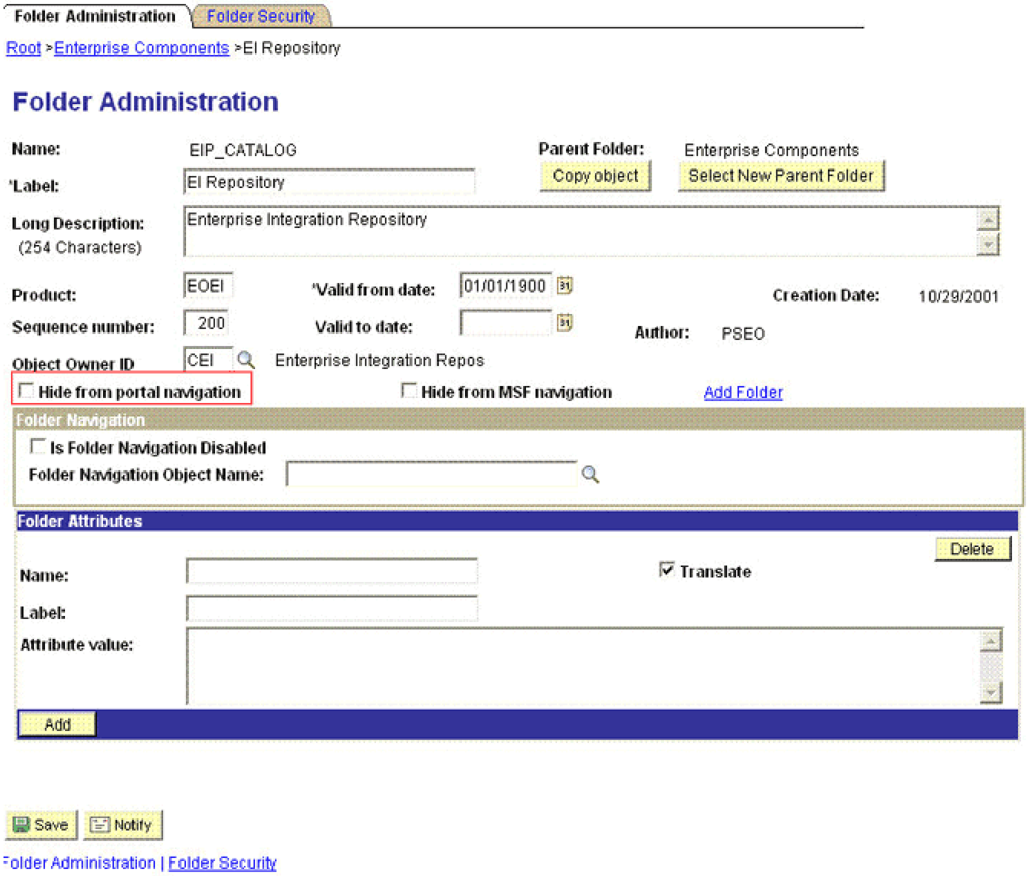
EI Repository is a hidden folder in PeopleSoft. Therefore, you must display this folder.

To display the EI Repository folder:

> **Note:**
>
> - If you are using PeopleTools 8.53, PeopleTools 8.54, PeopleTools 8.55, PeopleTools 8.56, or PeopleTools 8.57 as the target system, then do not perform the procedure described in this section.
> - Perform this procedure using the PeopleSoft administrator credentials.

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

   The following screenshot displays the Hide from portal navigation check box:



Root > Enterprise Components > EI Repository

Folder Administration

Name: EIP_CATALOG

Parent Folder: Enterprise Components

*Label: EI Repository

Long Description: (254 Characters) Enterprise Integration Repository

Product: EOEI

*Valid from date: 01/01/1900

Creation Date: 10/29/2001

Sequence number: 200

Valid to date:

Author: PSEO

Object Owner ID: CEI Enterprise Integration Repos

□ Hide from portal navigation

□ Hide from MSF navigation

Folder Navigation

□ Is Folder Navigation Disabled

Folder Navigation Object Name:

Folder Attributes

Name:

☑ Translate

Label:

Attribute value:

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

2.2.2.1.2.6 Activating the PERSON_BASIC_FULLSYNC Message

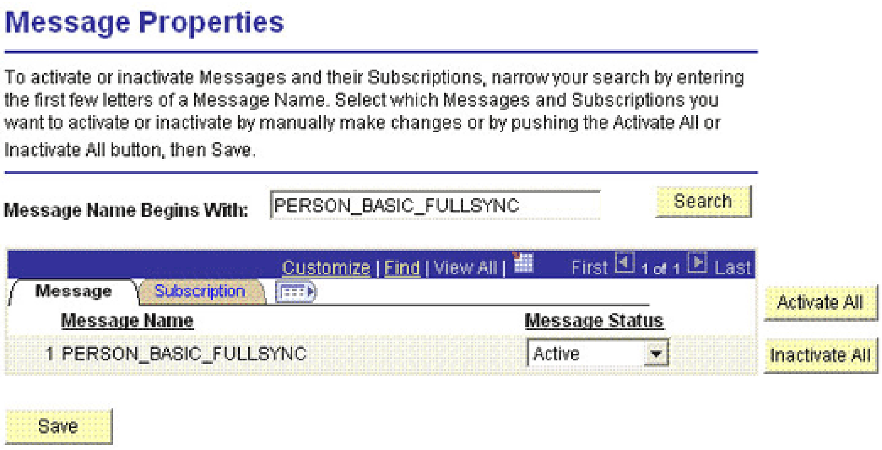
You must activate the PERSON_BASIC_FULLSYNC message so that it can be processed.

To activate the PERSON_BASIC_FULLSYNC message:

> **Note:**
>
> If you are using PeopleTools 8.53, PeopleTools 8.54, PeopleTools 8.55, PeopleTools 8.56, or PeopleTools 8.57 as the target system, then do not perform the procedure described in this section.

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

   The following screenshot displays the message to be activated:



Message Properties

To activate or inactivate Messages and their Subscriptions, narrow your search by entering the first few letters of a Message Name. Select which Messages and Subscriptions you want to activate or inactivate by manually make changes or by pushing the Activate All or Inactivate All button, then Save.

Message Name Begins With: PERSON_BASIC_FULLSYNC

	Message Name	Message Status
1	PERSON_BASIC_FULLSYNC	Active

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

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

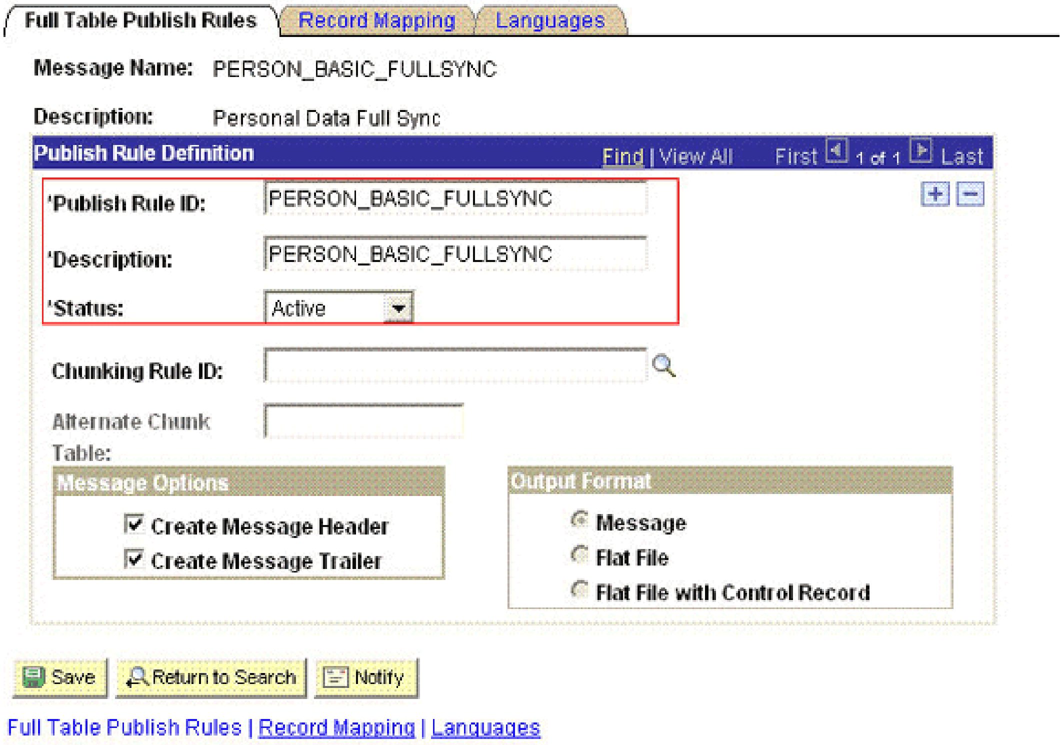
2.2.2.1.2.7 Activating the Full Data Publish Rule

You must define and activate the Full Data Publish 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 PERSON_BASIC_FULLSYNC message.
3. In the Publish Rule Definition region:
   a. In the Publish Rule ID field, enter `PERSON_BASIC_FULLSYNC`.
   b. In the Description field, enter `PERSON_BASIC_FULLSYNC`.
   c. From the Status list, select **Active.**

   The following screenshot displays the preceding steps:



Message Name: PERSON_BASIC_FULLSYNC

Description: Personal Data Full Sync

*Publish Rule ID:	PERSON_BASIC_FULLSYNC
*Description:	PERSON_BASIC_FULLSYNC
*Status:	Active
Chunking Rule ID:	
Alternate Chunk Table:	

Message Options

☑ Create Message Header
☑ Create Message Trailer

Output Format

● Message
○ Flat File
○ Flat File with Control Record

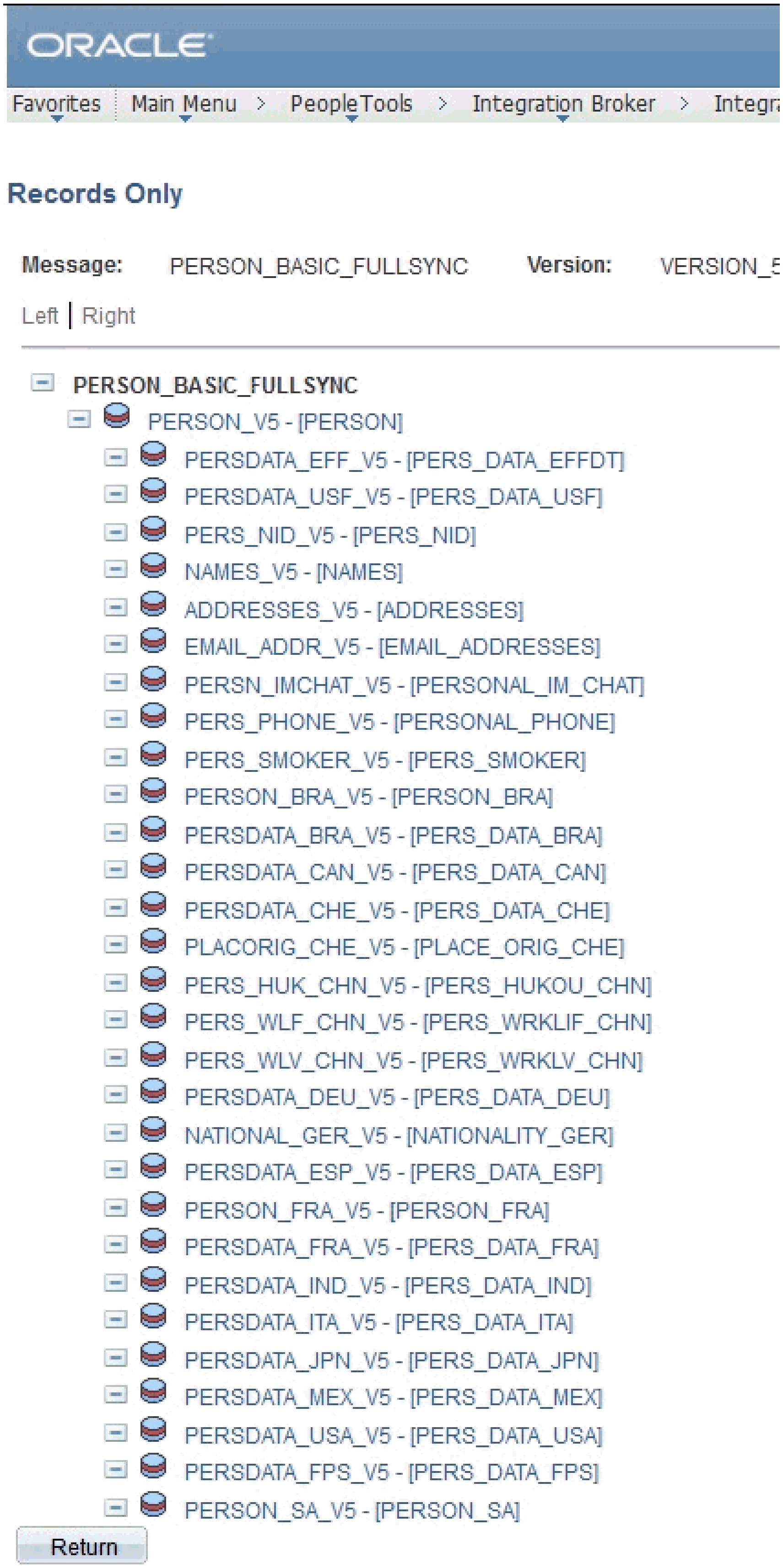
4. Click **Save.**

2.2.2.1.2.8 Publishing Messages With VERSION_5

The following is a summary of steps to publish messages with VERSION_5 for PeopleTools 8.51 with PeopleSoft HRMS 9.1:

1. In the VERSION_5 message, map all alias attributes to their original attributes. For example, map PERSON_V5 to PERSON.

   You can verify the original attributes in INTERNAL or VERSION_3 message. Most of the attribute names within brackets in VERSION_5 message will be original attribute names. However, you can confirm the alias attribute names with the original message.

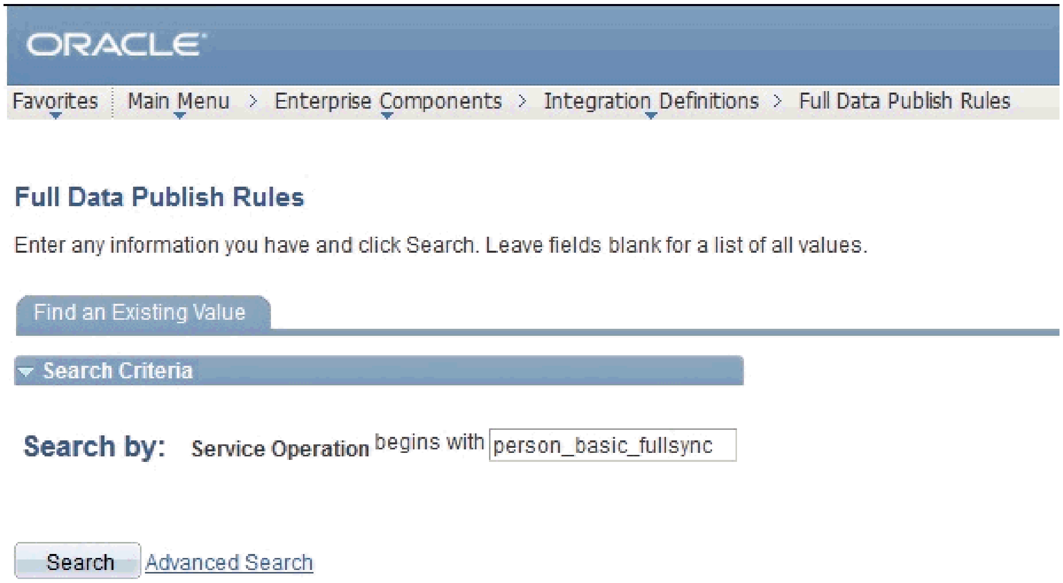


Records Only

Message: PERSON_BASIC_FULLSYNC Version: VERSION_5

PERSON_BASIC_FULLSYNC
- PERSON_V5 - [PERSON]
  - PERSDATA_EFF_V5 - [PERS_DATA_EFFDT]
  - PERSDATA_USF_V5 - [PERS_DATA_USF]
  - PERS_NID_V5 - [PERS_NID]
  - NAMES_V5 - [NAMES]
  - ADDRESSES_V5 - [ADDRESSES]
  - EMAIL_ADDR_V5 - [EMAIL_ADDRESSES]
  - PERSN_IMCHAT_V5 - [PERSONAL_IM_CHAT]
  - PERS_PHONE_V5 - [PERSONAL_PHONE]
  - PERS_SMOKER_V5 - [PERS_SMOKER]
  - PERSON_BRA_V5 - [PERSON_BRA]
  - PERSDATA_BRA_V5 - [PERS_DATA_BRA]
  - PERSDATA_CAN_V5 - [PERS_DATA_CAN]
  - PERSDATA_CHE_V5 - [PERS_DATA_CHE]
  - PLACORIG_CHE_V5 - [PLACE_ORIG_CHE]
  - PERS_HUK_CHN_V5 - [PERS_HUKOU_CHN]
  - PERS_WLF_CHN_V5 - [PERS_WRKLIF_CHN]
  - PERS_WLV_CHN_V5 - [PERS_WRKLV_CHN]
  - PERSDATA_DEU_V5 - [PERS_DATA_DEU]
  - NATIONAL_GER_V5 - [NATIONALITY_GER]
  - PERSDATA_ESP_V5 - [PERS_DATA_ESP]
  - PERSON_FRA_V5 - [PERSON_FRA]
  - PERSDATA_FRA_V5 - [PERS_DATA_FRA]
  - PERSDATA_IND_V5 - [PERS_DATA_IND]
  - PERSDATA_ITA_V5 - [PERS_DATA_ITA]
  - PERSDATA_JPN_V5 - [PERS_DATA_JPN]
  - PERSDATA_MEX_V5 - [PERS_DATA_MEX]
  - PERSDATA_USA_V5 - [PERS_DATA_USA]
  - PERSDATA_FPS_V5 - [PERS_DATA_FPS]
  - PERSON_SA_V5 - [PERSON_SA]

2. In the PeopleSoft Internet Architecture window:
   - For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Full Data Publish Rules.**
   - For PeopleTools 8.55, 8.56, and 8.57, click **NavBar**, **Navigator**, **PeopleTools, Integration Broker**, **Integration Setup,** and then click **Full Data Publish Rules.**
3. Under the Search Criteria region, enter `PERSON_BASIC_FULLSYNC` in the **Service Operation** field, and then click **Search.**

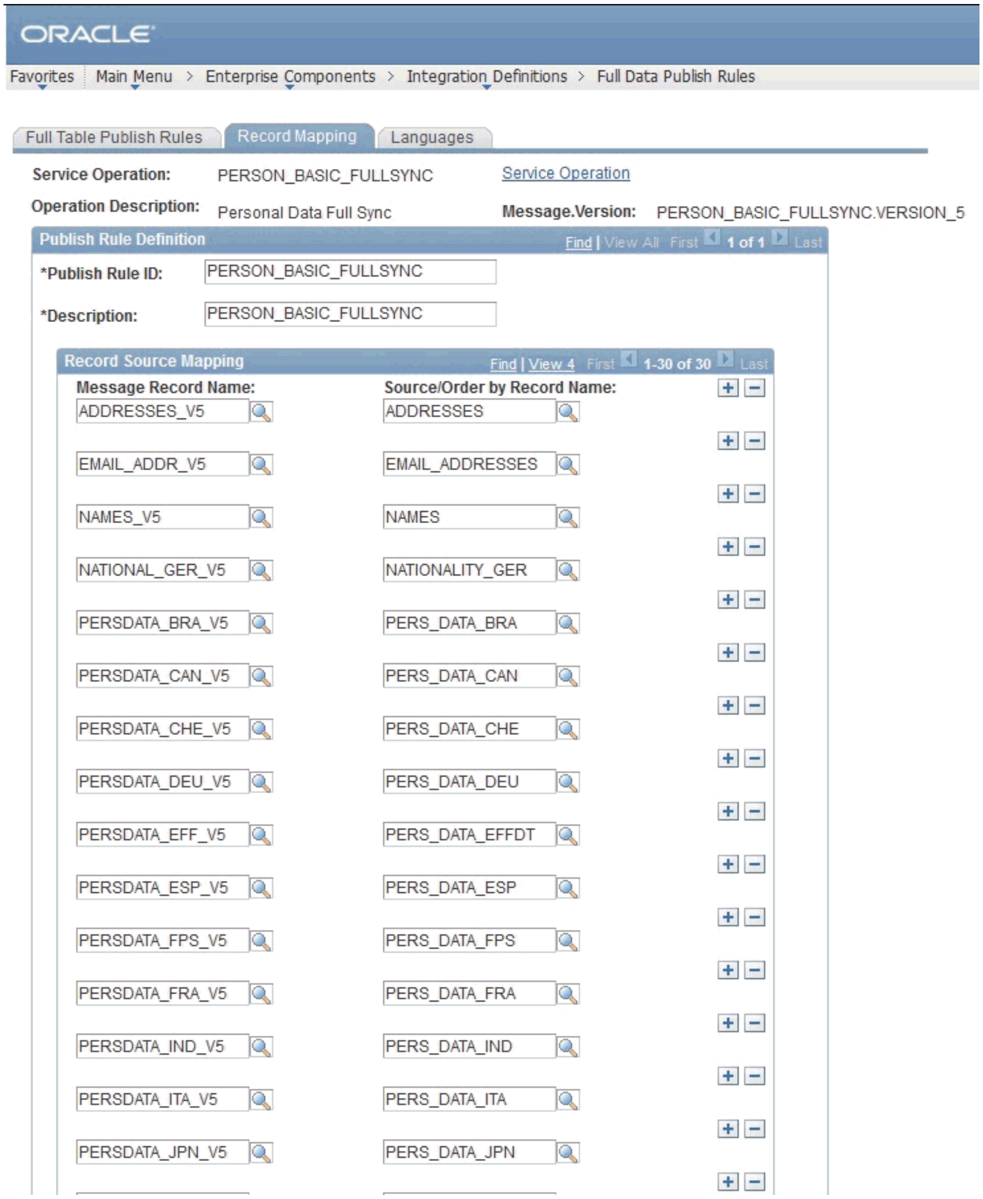

ORACLE
Favorites
Main Menu > Enterprise Components > Integration Definitions > Full Data Publish Rules
Find an Existing Value
Search Criteria
Search
Advanced Search

Full Data Publish Rules

Enter any information you have and click Search. Leave fields blank for a list of all values.

Search by: Service Operation begins with person_basic_fullsync

4. In the PERSON_BASIC_FULLSYNC publish rule, click the **Record Mapping** tab.
5. Map all the aliases in VERSION_5 message to the original attributes as displayed in the following screenshot.


ORACLE
Favorites | Main Menu > Enterprise Components > Integration Definitions > Full Data Publish Rules
Full Table Publish Rules
Record Mapping
Languages
Service Operation
Find | View All First 1 of 1 Last
Find | View 4 First 1-30 of 30 Last

Service Operation: PERSON_BASIC_FULLSYNC

Operation Description: Personal Data Full Sync

Message.Version: PERSON_BASIC_FULLSYNC.VERSION_5

Publish Rule Definition

*Publish Rule ID: PERSON_BASIC_FULLSYNC

*Description: PERSON_BASIC_FULLSYNC

Record Source Mapping

Message Record Name:	Source/Order by Record Name:
ADDRESSES_V5	ADDRESSES
EMAIL_ADDR_V5	EMAIL_ADDRESSES
NAMES_V5	NAMES
NATIONAL_GER_V5	NATIONALITY_GER
PERSDATA_BRA_V5	PERS_DATA_BRA
PERSDATA_CAN_V5	PERS_DATA_CAN
PERSDATA_CHE_V5	PERS_DATA_CHE
PERSDATA_DEU_V5	PERS_DATA_DEU
PERSDATA_EFF_V5	PERS_DATA_EFFDT
PERSDATA_ESP_V5	PERS_DATA_ESP
PERSDATA_FPS_V5	PERS_DATA_FPS
PERSDATA_FRA_V5	PERS_DATA_FRA
PERSDATA_IND_V5	PERS_DATA_IND
PERSDATA_ITA_V5	PERS_DATA_ITA
PERSDATA_JPN_V5	PERS_DATA_JPN

6. Click **Save.**

7. Publish the message.

   You can verify that the name of message matches with the lookup definition message name.

2.2.2.1.3 Configuring the WORKFORCE_FULLSYNC Service Operation

The WORKFORCE_FULLSYNC message contains the job-related details of all persons. This information includes the Department, Supervisor ID, Manager ID, and Job Code.

To configure the WORKFORCE_FULLSYNC service operation perform the following procedures:

> **Note:**
>
> In PeopleSoft HRMS, there are many versions of the message associated with this service operation. But, when you integrate PeopleSoft HRMS and Oracle Identity Manager, you must send the following versions depending on the version of HRMS:
>
> - Use `WORKFORCE_FULLSYNC.INTERNAL` for HRMS 8.9 Bundle 23 or later, HRMS 9.0 Bundle 14 or later, HRMS 9.1 Bundle 3 or later, and HRMS 9.2 Image 4 or later.
> - Use `WORKFORCE_FULLSYNC.VERSION_3` for other versions of HRMS.

- Activating the WORKFORCE_FULLSYNC Service Operation
- Verifying the Queue Status for the WORKFORCE_FULLSYNC Service Operation
- Setting Up the Security for the WORKFORCE_FULLSYNC Service Operation
- Defining the Routing for the WORKFORCE_FULLSYNC Service Operation
- Displaying the EI Repository Folder
- Activating the WORKFORCE_FULLSYNC Message
- Activating the Full Data Publish Rule

> **Note:**
>
> The procedure remains the same for PeopleTools 8.49 with HRMS 9.0, PeopleTools 8.50 with HRMS 9.1, PeopleTools 8.53 through 8.57 with HRMS 9.2. The screenshots are taken on version PeopleTools 8.49.

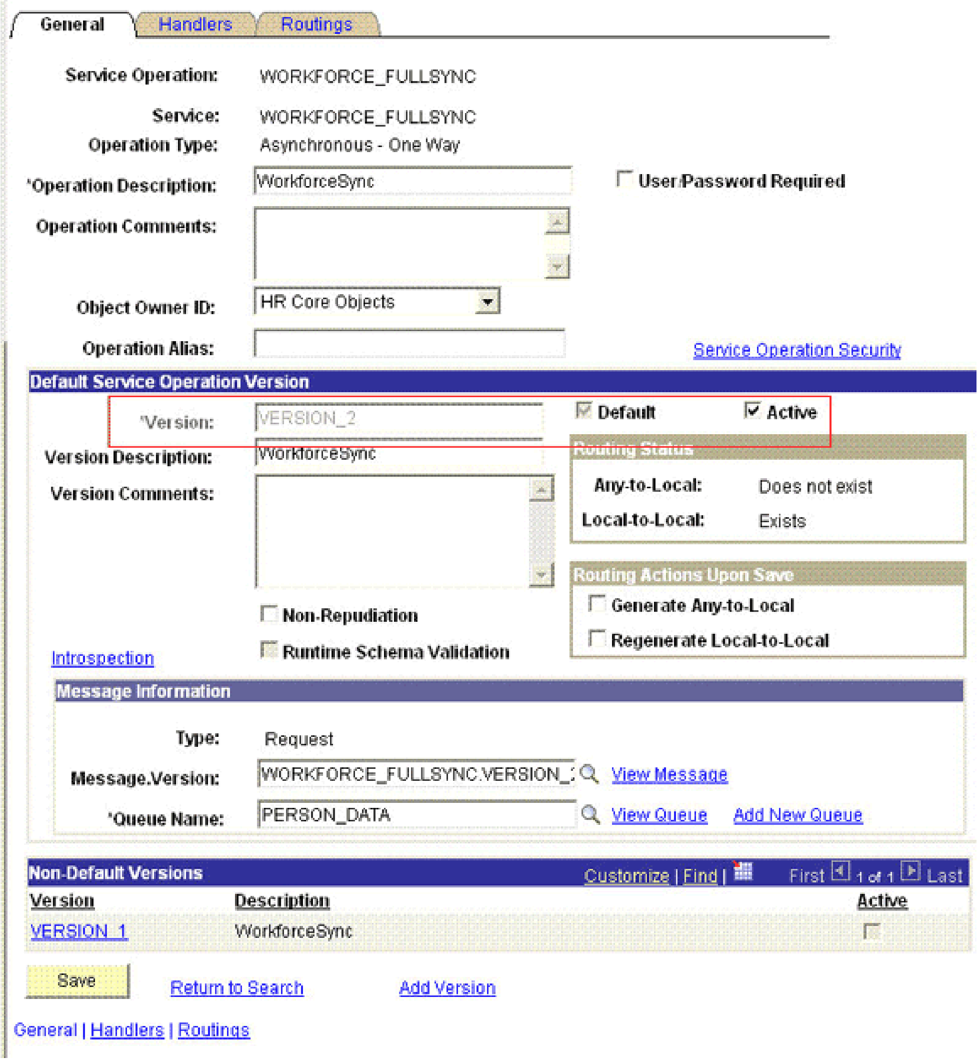
2.2.2.1.3.1 Activating the WORKFORCE_FULLSYNC Service Operation

To activate the WORKFORCE_FULLSYNC 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 the PeopleSoft Internet Architecture window:
   - For PeopleSoft 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. On the Find Service Operation tab, enter `WORKFORCE_FULLSYNC` in the **Service** field, and then click **Search.**
3. Click the **WORKFORCE_FULLSYNC** link.

The following screenshot displays the default version of the WORKFORCE_FULLSYNC service operation:



Service Operation: WORKFORCE_FULLSYNC

Service: WORKFORCE_FULLSYNC

Operation Type: Asynchronous - One Way

*Operation Description: WorkforceSync

□ User/Password Required

Operation Comments:

Object Owner ID: HR Core Objects

Operation Alias:

Service Operation Security

Default Service Operation Version

*Version: VERSION_2 ☑ Default ☑ Active

Version Description: WorkforceSync

Version Comments:

Routing Status

Any-to-Local: Does not exist

Local-to-Local: Exists

Routing Actions Upon Save

□ Generate Any-to-Local

□ Regenerate Local-to-Local

□ Non-Repudiation

□ Runtime Schema Validation

Introspection

Message Information

Type: Request

Message.Version: WORKFORCE_FULLSYNC.VERSION_: View Message

*Queue Name: PERSON_DATA View Queue Add New Queue

Non-Default Versions Customize | Find | First 1 of 1 Last

Version	Description	Active
VERSION_1	WorkforceSync	□

Save Return to Search Add Version

General | Handlers | Routings

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

2.2.2.1.3.2 Verifying the Queue Status for the WORKFORCE_FULLSYNC Service Operation

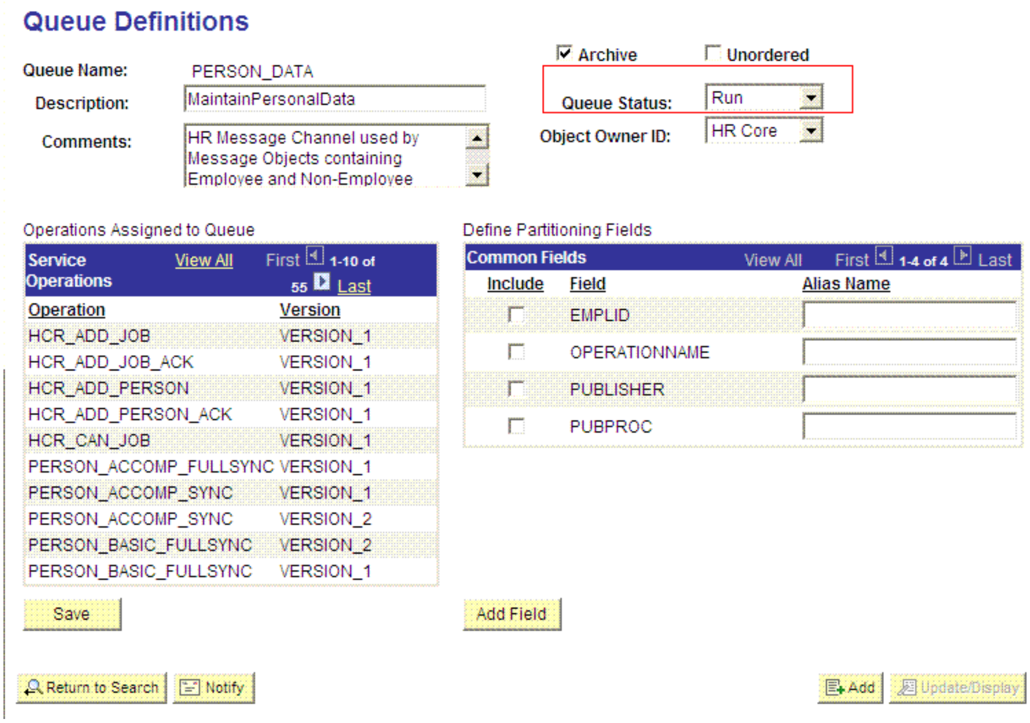
To ensure that the status of the queue for the WORKFORCE_FULLSYNC service operation is Run:

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 **PERSON_DATA** 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.**

The queue status is shown in the following screenshot:



Queue Definitions

Queue Name: PERSON_DATA

Description: MaintainPersonalData

Comments: HR Message Channel used by Message Objects containing Employee and Non-Employee

☑ Archive ☐ Unordered

Queue Status: Run

Object Owner ID: HR Core

Operations Assigned to Queue

Operation	Version
HCR_ADD_JOB	VERSION_1
HCR_ADD_JOB_ACK	VERSION_1
HCR_ADD_PERSON	VERSION_1
HCR_ADD_PERSON_ACK	VERSION_1
HCR_CAN_JOB	VERSION_1
PERSON_ACCOMP_FULLSYNC	VERSION_1
PERSON_ACCOMP_SYNC	VERSION_1
PERSON_ACCOMP_SYNC	VERSION_2
PERSON_BASIC_FULLSYNC	VERSION_2
PERSON_BASIC_FULLSYNC	VERSION_1

Define Partitioning Fields

Include	Field	Alias Name
☐	EMPLID	
☐	OPERATIONNAME	
☐	PUBLISHER	
☐	PUBPROC	

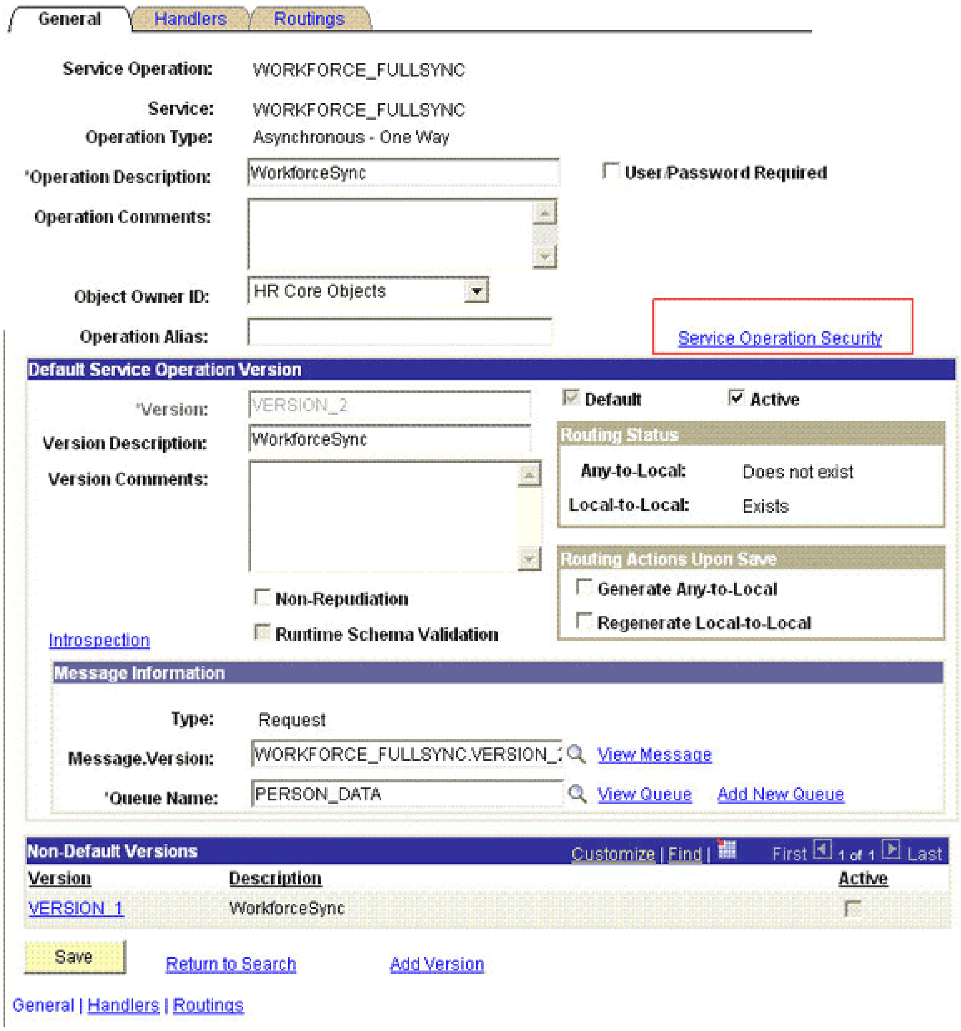
4. Click **Return to Search.**

2.2.2.1.3.3 Setting Up the Security for the WORKFORCE_FULLSYNC Service Operation

To set up the security for the WORKFORCE_FULLSYNC 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 an open the **WORKFORCE_FULLSYNC** service operation.
3. On the General tab, click the **Service Operation Security** link.

   The link is shown in the following screenshot:



Service Operation: WORKFORCE_FULLSYNC

Service: WORKFORCE_FULLSYNC

Operation Type: Asynchronous - One Way

*Operation Description: WorkforceSync

□ User/Password Required

Operation Comments:

Object Owner ID: HR Core Objects

Operation Alias:

Default Service Operation Version

*Version: VERSION_2

☑ Default ☑ Active

Version Description: WorkforceSync

Version Comments:

Routing Status

Any-to-Local: Does not exist

Local-to-Local: Exists

Routing Actions Upon Save

□ Generate Any-to-Local

□ Regenerate Local-to-Local

□ Non-Repudiation

□ Runtime Schema Validation

Message Information

Type: Request

Message.Version: WORKFORCE_FULLSYNC.VERSION_:

*Queue Name: PERSON_DATA

Non-Default Versions

Version	Description	Active
VERSION_1	WorkforceSync	□

4. Attach the **OIMER** permission list to the **WORKFORCE_FULLSYNC** service operation. This list is created in Step 3 of the preinstallation procedure discussed in Creating a Permission List.

   To attach the permission list:

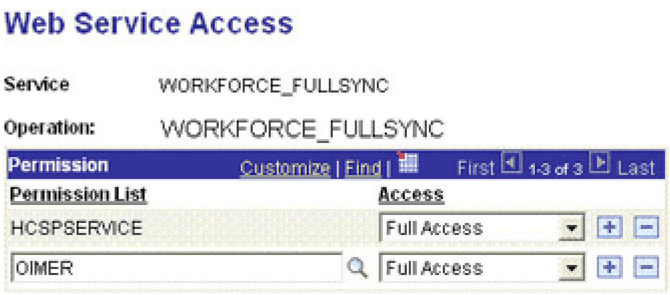
   a. Click the plus sign (+) to add a row to the Permission List field.

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

      The **OIMER** permission list appears.

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

      The following screenshot displays the Access list with Full Access:



Web Service Access

Service: WORKFORCE_FULLSYNC

Operation: WORKFORCE_FULLSYNC

Permission List	Access
HCSPSERVICE	Full Access
OIMER	Full Access

d. Click **Save.**

e. Click **Return to Search.**

2.2.2.1.3.4 Defining the Routing for the WORKFORCE_FULLSYNC Service Operation

To define the routing for the WORKFORCE_FULLSYNC service operation:

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

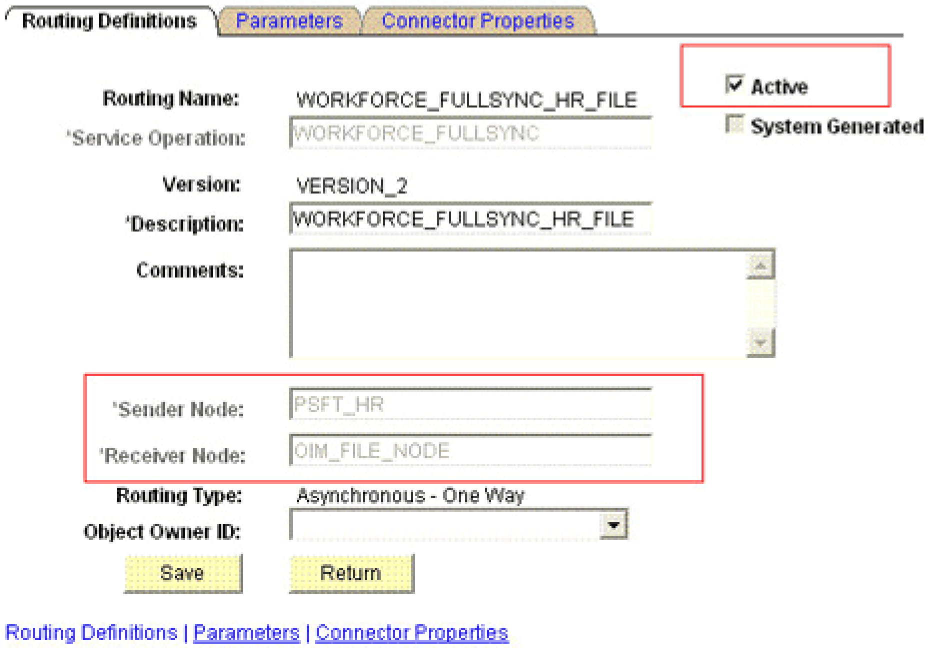
2. On the Routing Definitions tab, enter the following:

   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_FILE_NODE`

   The following graphic displays both the Sender and the Receiver nodes:



☑ Active
□ System Generated

Routing Name:	WORKFORCE_FULLSYNC_HR_FILE
*Service Operation:	WORKFORCE_FULLSYNC
Version:	VERSION_2
*Description:	WORKFORCE_FULLSYNC_HR_FILE
Comments:	
*Sender Node:	PSFT_HR
*Receiver Node:	OIM_FILE_NODE
Routing Type:	Asynchronous - One Way
Object Owner ID:	

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

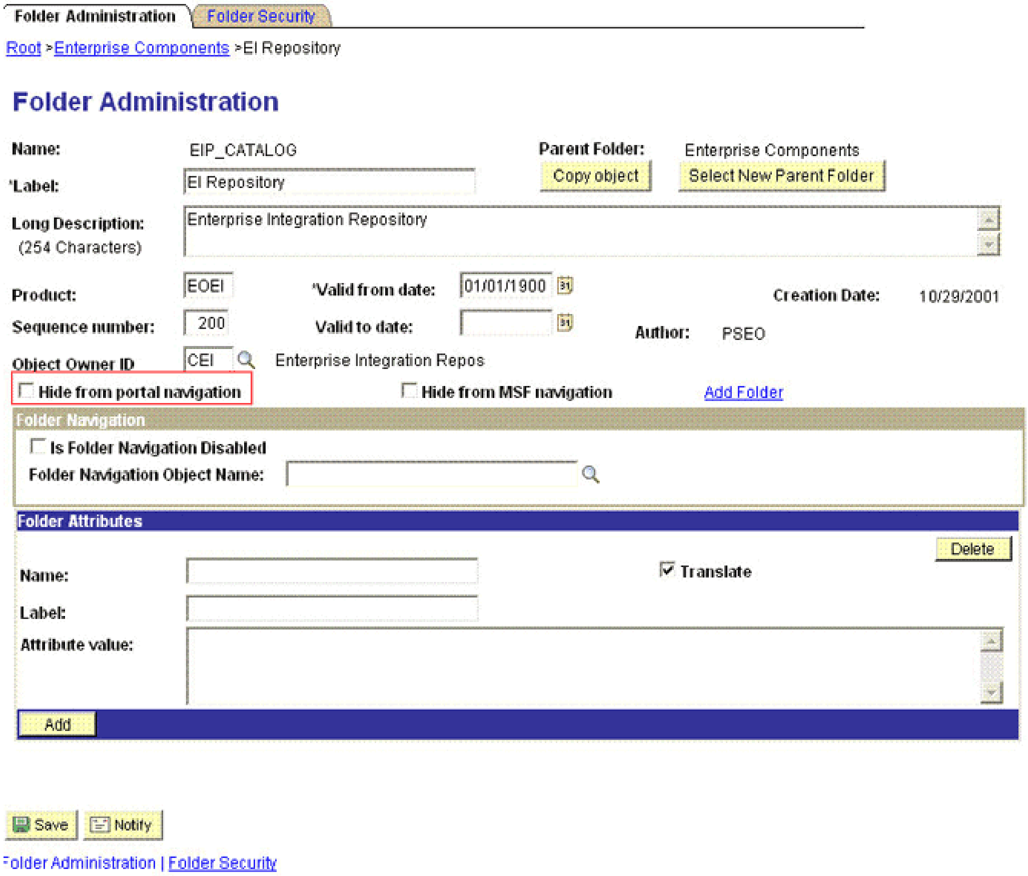
2.2.2.1.3.5 Displaying the EI Repository Folder

To display the EI Repository folder:

> **Note:**
>
> - If you are using PeopleTools 8.53 or later, then do not perform the procedure mentioned in this section.
> - If you have performed this procedure as described in "Displaying the EI Repository Folder", then you can skip this section.
> - Perform this procedure using the PeopleSoft administrator credentials.

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

   The following screenshot displays the Hide from portal navigation check box:



Root >Enterprise Components >EI Repository

Folder Administration

Name: EIP_CATALOG

Parent Folder: Enterprise Components

*Label: EI Repository

Long Description: (254 Characters) Enterprise Integration Repository

Product: EOEI

*Valid from date: 01/01/1900

Creation Date: 10/29/2001

Sequence number: 200

Valid to date:

Author: PSEO

Object Owner ID CEI Enterprise Integration Repos

□ Hide from portal navigation

□ Hide from MSF navigation

Folder Navigation

□ Is Folder Navigation Disabled

Folder Navigation Object Name:

Folder Attributes

Name:

☑ Translate

Label:

Attribute value:

Folder Administration | Folder Security

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

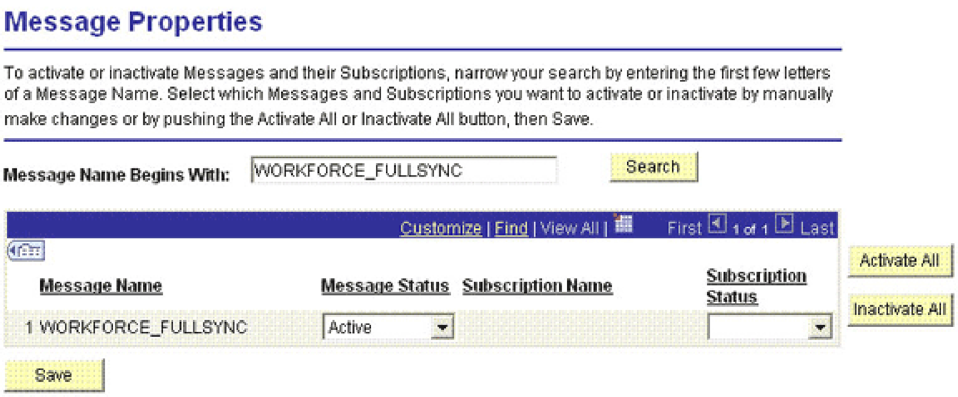
2.2.2.1.3.6 Activating the WORKFORCE_FULLSYNC Message

To activate the WORKFORCE_FULLSYNC message:

> **Note:**
>
> If you are using PeopleTools 8.53, PeopleTools 8.54, PeopleTools 8.55, PeopleTools 8.56, PeopleTools 8.57, then do not perform the procedure mentioned in this section.

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

   The following screenshot displays the message to be activated:



Message Properties

To activate or inactivate Messages and their Subscriptions, narrow your search by entering the first few letters of a Message Name. Select which Messages and Subscriptions you want to activate or inactivate by manually make changes or by pushing the Activate All or Inactivate All button, then Save.

Message Name Begins With: WORKFORCE_FULLSYNC

Message Name	Message Status	Subscription Name	Subscription Status
1 WORKFORCE_FULLSYNC	Active		

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

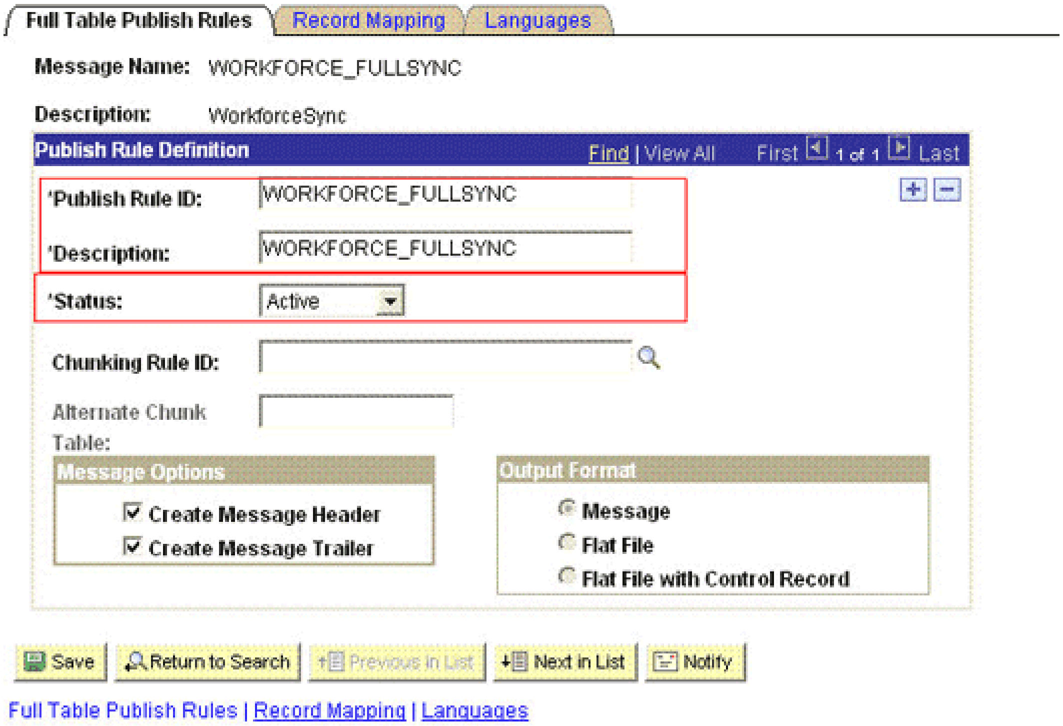
> **Note:**
>
> To perform this step, your User Profile must have the EIR Administrator role consisting of **EOEI9000** and **EOCO9000** permission lists.

2.2.2.1.3.7 Activating the Full Data Publish Rule

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 **WORKFORCE_FULLSYNC** message.
3. In the Publish Rule Definition region:
   a. In the Publish Rule ID field, enter `WORKFORCE_FULLSYNC`.
   b. In the Description field, enter `WORKFORCE_FULLSYNC`.
   c. From the Status list, select **Active.**

   The following screenshot displays the preceding steps:



Message Name: WORKFORCE_FULLSYNC

Description: WorkforceSync

*Publish Rule ID: WORKFORCE_FULLSYNC

*Description: WORKFORCE_FULLSYNC

*Status: Active

Chunking Rule ID:

Alternate Chunk Table:

☑ Create Message Header
☑ Create Message Trailer

● Message
○ Flat File
○ Flat File with Control Record

4. Click **Save.**

2.2.2.2 Configuring the Target System for Incremental Reconciliation

Configuring the target system for incremental reconciliation involves configuring PeopleSoft Integration Broker and configuring the PERSON_BASIC_SYNC and WORKFORCE_SYNC messages.

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 PeopleSoft 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 to external applications 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
- Configuring the PERSON_BASIC_SYNC Service Operation
- Configuring the WORKFORCE_SYNC Service Operation
- Preventing Transmission of Unwanted Fields During Incremental Reconciliation

2.2.2.2.1 Configuring PeopleSoft Integration Broker

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

2.2.2.2.1.1 Configuring PeopleSoft Integration Broker Gateway

Section "Configuring PeopleSoft Integration Broker Gateway" describes the procedure to configure the PeopleSoft Integration Broker gateway.

2.2.2.2.1.2 Configuring PeopleSoft Integration Broker

To configure 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 User Management 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.

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, 8.56, and 8.57, 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, specify the SuperUserID in the **Default User ID** field. For example, `PS`.

d. Make this node a remote node by deselecting the **Local Node** check box and selecting the **Active Node** check box.

e. Ensure Node Type is **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 PeopleSoft HRMS

   Sample value: PSFT HRMS

   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://ORACLE_IDENTITY_MANAGER_SERVER_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 Oracle WebLogic Server:

   ```
   http://10.121.16.42:7001/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 Oracle WebLogic Server:

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

> **Note:**
>
> The ports may vary depending on the installation that you are using.

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

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

> **Note:**
>
> Ping also validates the target authentication, in this case, the IT resource name.

Before the XML messages are sent from the target system to Oracle Identity Manager, you must verify whether the PeopleSoft node is running. You can do so by clicking the **Ping Node** button in the **Connectors** tab. To access the Connectors tab, click **PeopleTools, Integration Broker, Integration Setup,** and then **Nodes.**

Note:

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

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

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

```
secureFileKeystorePath=<path to pskey>
```

```
secureFileKeystorePasswd=password
```

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

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

   <*PIA_HOME*>\webserv\peoplesoft\bin

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

2.2.2.2.2 Configuring the PERSON_BASIC_SYNC Service Operation

The PERSON_BASIC_SYNC message contains the updated information about a particular person. This information includes the Employee ID and the information that is added or modified.

To configure the PERSON_BASIC_SYNC service operation perform the following procedures:

Note:

The procedure remains the same for PeopleTools 8.49 with HRMS 9.0, PeopleTools 8.50 with HRMS 9.1, PeopleTools 8.53 through 8.57 with HRMS 9.2. The screenshots are taken on PeopleTools 8.49 version.

- Activating the PERSON_BASIC_SYNC Service Operation
- Verifying the Queue Status for the PERSON_BASIC_SYNC Service Operation
- Setting Up the Security for the PERSON_BASIC_SYNC Service Operation

- Defining the Routing for the PERSON_BASIC_SYNC Service Operation
- Displaying the EI Repository Folder
- Activating the PERSON_BASIC_SYNC Message

2.2.2.2.2.1 Activating the PERSON_BASIC_SYNC Service Operation

To activate the PERSON_BASIC_SYNC service operation:

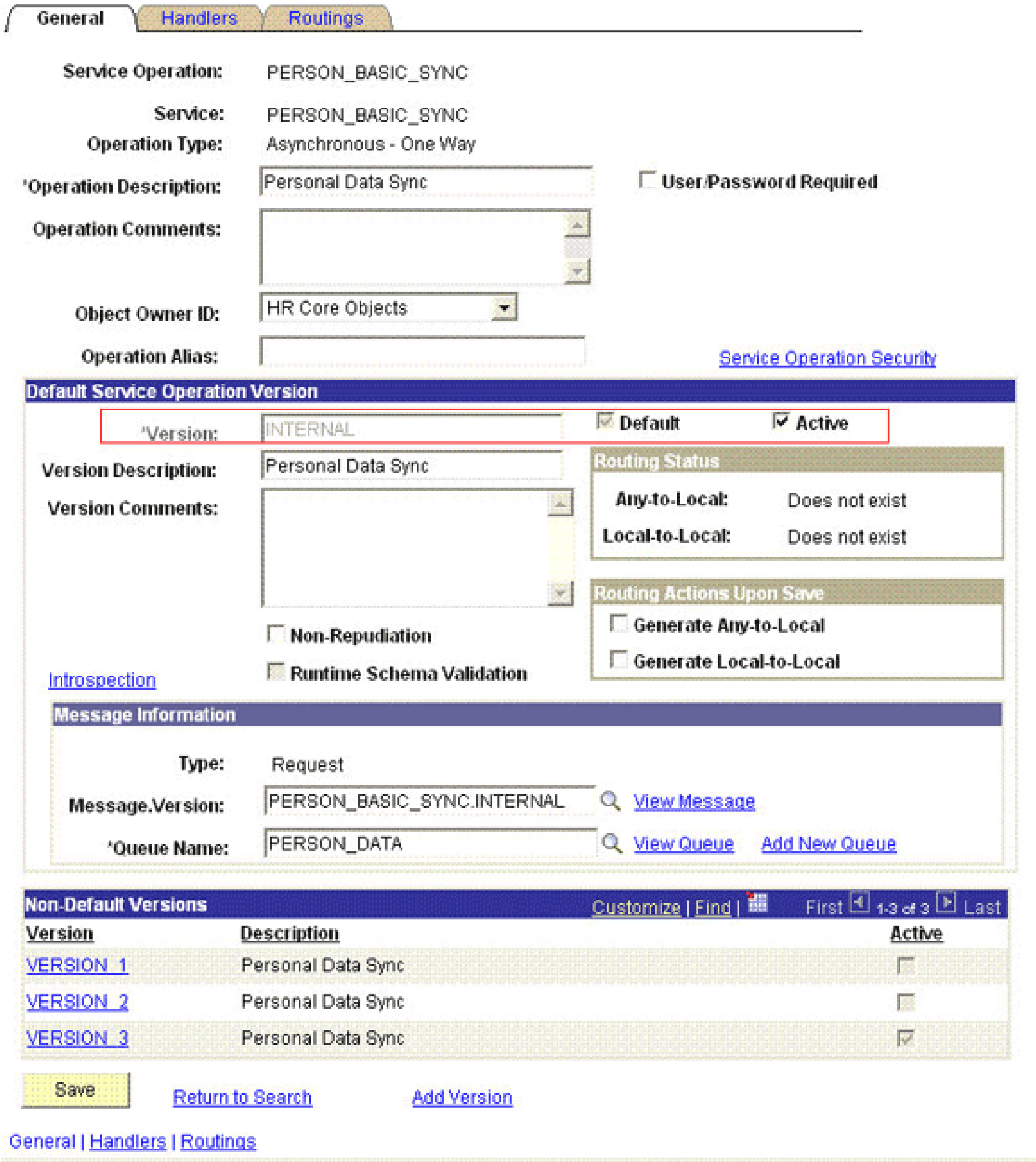
> **Note:**
>
> If the message version is not the same as specified, then you can change the message version as described in Changing Default Message Versions.

1. In 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. On the Find Service Operation tab, enter `PERSON_BASIC_SYNC` in the **Service** field, and then click **Search.**
3. Click the **PERSON_BASIC_SYNC** link.

   > **Note:**
   >
   > - In PeopleSoft HRMS, there are four versions of the message associated with this service operation. But, when you integrate PeopleSoft HRMS 9.0 and Oracle Identity Manager, you must send `VERSION_3.` The default version for PeopleSoft HRMS is `INTERNAL`. Therefore, you must convert the default version to `VERSION_3.` This conversion is carried out using the transformation program `HMTF_TR_OA.`
   >
   >   If you are using PeopleSoft HRMS 9.2 Image 4 or later, then use the `HCM_MSG_XFRM` transform program instead of `HMTF_TR_OA.`
   > - For PeopleTools 8.57, use the default version type `INTERNAL`. Skip the steps specific to version_3.

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

   The following screenshot displays the default version of the PERSON_BASIC_SYNC service operation:



Service Operation: PERSON_BASIC_SYNC

Service: PERSON_BASIC_SYNC

Operation Type: Asynchronous - One Way

*Operation Description: Personal Data Sync

□ User/Password Required

Operation Comments:

Object Owner ID: HR Core Objects

Operation Alias:

Service Operation Security

Default Service Operation Version

*Version: INTERNAL ☑ Default ☑ Active

Version Description: Personal Data Sync

Version Comments:

Routing Status

Any-to-Local:	Does not exist
Local-to-Local:	Does not exist

Routing Actions Upon Save

□ Generate Any-to-Local

□ Generate Local-to-Local

□ Non-Repudiation

□ Runtime Schema Validation

Introspection

Message Information

Type: Request

Message.Version: PERSON_BASIC_SYNC.INTERNAL View Message

*Queue Name: PERSON_DATA View Queue Add New Queue

Non-Default Versions Customize | Find | First 1-3 of 3 Last

Version	Description	Active
VERSION_1	Personal Data Sync	□
VERSION_2	Personal Data Sync	□
VERSION_3	Personal Data Sync	☑

5. Click **Save.**

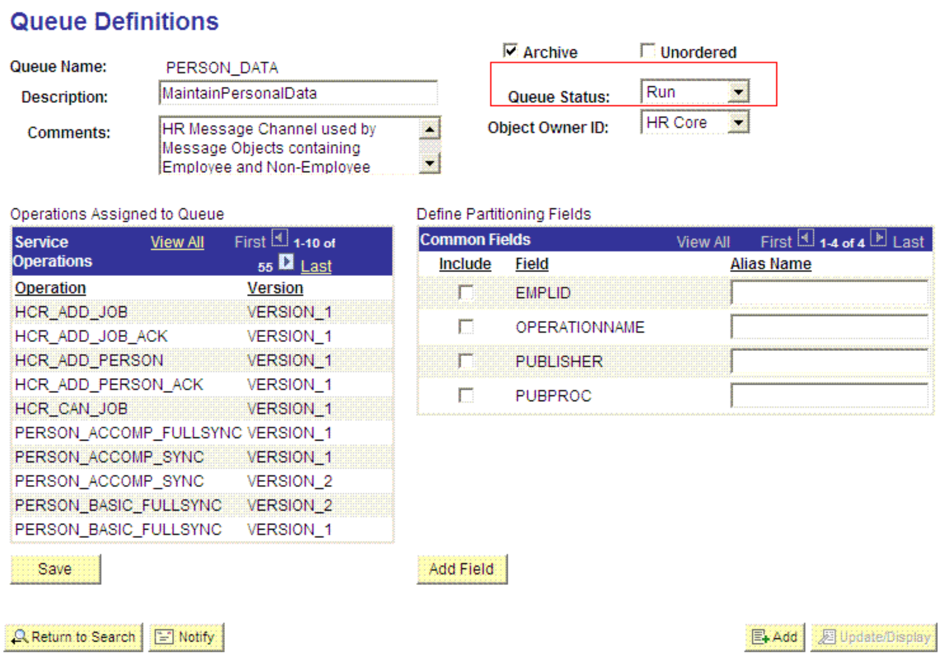
2.2.2.2.2.2 Verifying the Queue Status for the PERSON_BASIC_SYNC Service Operation

To ensure that the status of the queue for the PERSON_BASIC_SYNC 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 **PERSON_DATA** 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.**

The queue status is shown in the following screenshot:



Queue Definitions

Queue Name: PERSON_DATA

Description: MaintainPersonalData

Comments: HR Message Channel used by Message Objects containing Employee and Non-Employee

☑ Archive ☐ Unordered

Queue Status: Run

Object Owner ID: HR Core

Operations Assigned to Queue

Service Operations — View All — First 1-10 of 55 Last

Operation	Version
HCR_ADD_JOB	VERSION_1
HCR_ADD_JOB_ACK	VERSION_1
HCR_ADD_PERSON	VERSION_1
HCR_ADD_PERSON_ACK	VERSION_1
HCR_CAN_JOB	VERSION_1
PERSON_ACCOMP_FULLSYNC	VERSION_1
PERSON_ACCOMP_SYNC	VERSION_1
PERSON_ACCOMP_SYNC	VERSION_2
PERSON_BASIC_FULLSYNC	VERSION_2
PERSON_BASIC_FULLSYNC	VERSION_1

Define Partitioning Fields

Common Fields — View All — First 1-4 of 4 Last

Include	Field	Alias Name
☐	EMPLID	
☐	OPERATIONNAME	
☐	PUBLISHER	
☐	PUBPROC	

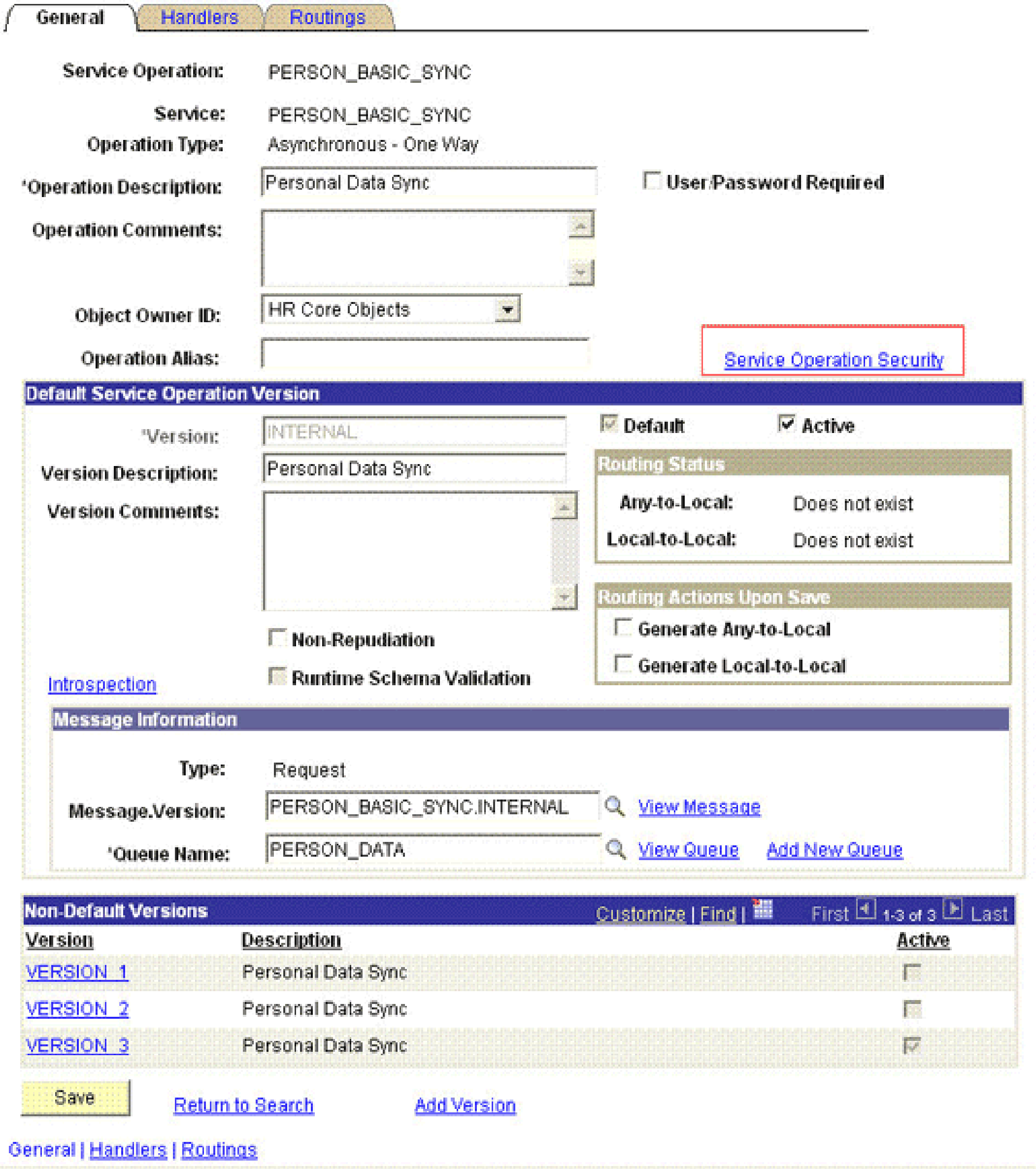
4. Click **Return to Search.**

2.2.2.2.2.3 Setting Up the Security for the PERSON_BASIC_SYNC Service Operation

To set up the security for the PERSON_BASIC_SYNC service operation:

1. In PeopleSoft Internet Architecture:
   - 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 an open the **PERSON_BASIC_SYNC** service operation.
3. On the General tab, click the **Service Operation Security** link.

   The link is shown in the following screenshot:



Service Operation: PERSON_BASIC_SYNC

Service: PERSON_BASIC_SYNC

Operation Type: Asynchronous - One Way

*Operation Description: Personal Data Sync

□ User/Password Required

Operation Comments:

Object Owner ID: HR Core Objects

Operation Alias:

Service Operation Security

Default Service Operation Version

*Version: INTERNAL

☑ Default ☑ Active

Version Description: Personal Data Sync

Version Comments:

Routing Status

Any-to-Local: Does not exist

Local-to-Local: Does not exist

Routing Actions Upon Save

□ Generate Any-to-Local

□ Generate Local-to-Local

□ Non-Repudiation

□ Runtime Schema Validation

Introspection

Message Information

Type: Request

Message.Version: PERSON_BASIC_SYNC.INTERNAL View Message

*Queue Name: PERSON_DATA View Queue Add New Queue

Non-Default Versions Customize | Find | First 1-3 of 3 Last

Version	Description	Active
VERSION_1	Personal Data Sync	□
VERSION_2	Personal Data Sync	□
VERSION_3	Personal Data Sync	☑

4. Attach the **OIMER** permission list to the **PERSON_BASIC_SYNC** 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 OIMER permission list. The OIMER permission list is used as an example. But, to implement this procedure you must use the permission list (attached through a role) to the user profile that has the privilege to modify personal data in the target system.

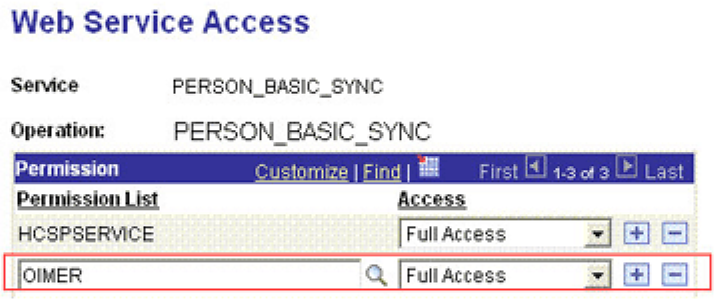
   a. Click the plus sign (+) to add a row for the Permission List field.

b. In the Permission List field, enter `OIMER` and then click the Look up Permission List icon.

   The **OIMER** permission list appears.

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

   The following screenshot displays the permission list with Full Access:



Web Service Access

Service PERSON_BASIC_SYNC

Operation: PERSON_BASIC_SYNC

Permission

Permission List	Access
HCSPSERVICE	Full Access
OIMER	Full Access

d. Click **Save.**

e. Click **Return to Search.**

5. In the Non-Default Version region, click the **VERSION_3** link to view the details.

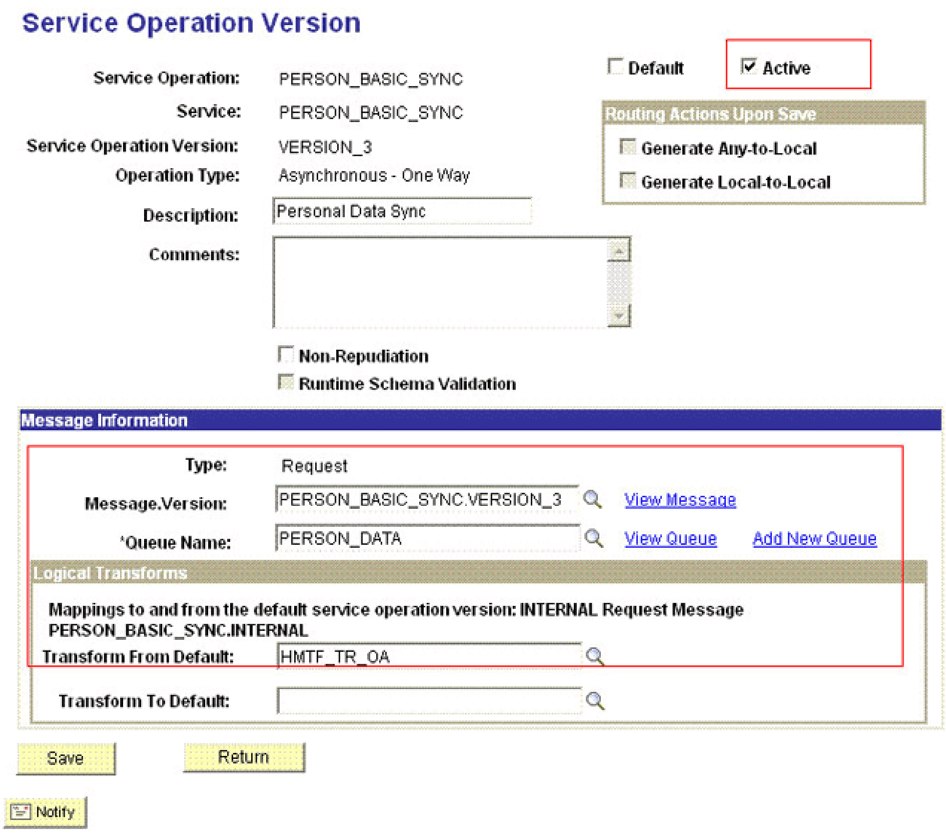
> **Note:**
>
> Skip this step for version type INTERNAL.

a. Click **Active.**

b. Enter `HMTF_TR_OA` in the Transform From Default field.

> **Note:**
>
> If the Transform From Default field is not available in the region, you can ignore this step.

The following screenshot displays the preceding steps:



Service Operation Version

□ Default ☑ Active

Service Operation: PERSON_BASIC_SYNC
Service: PERSON_BASIC_SYNC
Service Operation Version: VERSION_3
Operation Type: Asynchronous - One Way
Description: Personal Data Sync
Comments:

Routing Actions Upon Save
□ Generate Any-to-Local
□ Generate Local-to-Local

□ Non-Repudiation
□ Runtime Schema Validation

Message Information

Type: Request
Message.Version: PERSON_BASIC_SYNC.VERSION_3
*Queue Name: PERSON_DATA

Logical Transforms

Mappings to and from the default service operation version: INTERNAL Request Message PERSON_BASIC_SYNC.INTERNAL
Transform From Default: HMTF_TR_OA
Transform To Default:

c. Click **Save,** and then click **Return.**

6. On the Handlers Tab, ensure that the Status is **Active** for the Type column that contains **OnNotify** PeopleCode.

7. Click **Save.**

2.2.2.2.2.4 Defining the Routing for the PERSON_BASIC_SYNC Service Operation

To define the routing for the PERSON_BASIC_SYNC service operation:

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

2. On the Routing Definitions 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**

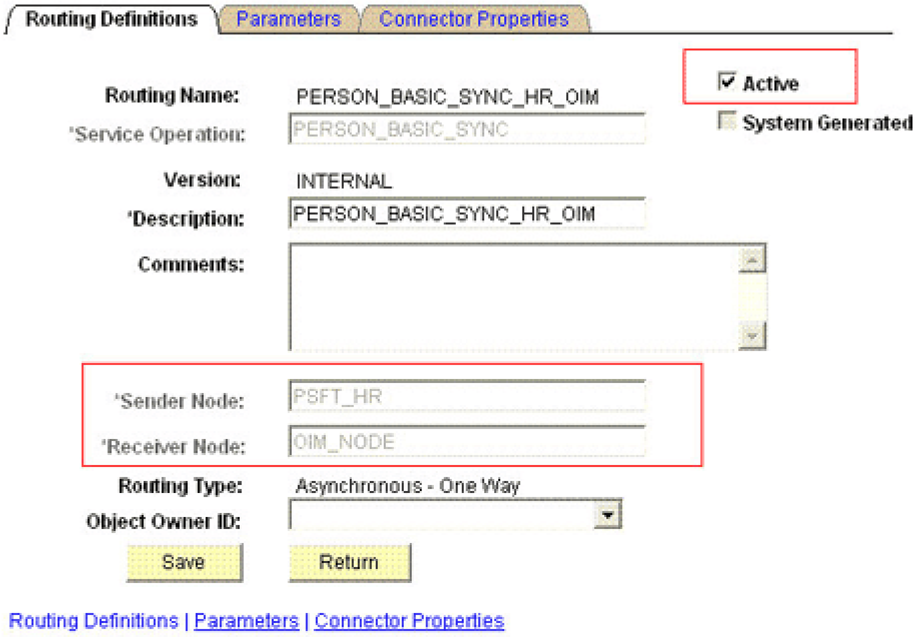
   Only one node can meet all the above conditions at a time.

c. Select the node.

d. Click **Save.**

Receiver Node: `OIM_NODE`

The following screenshot displays the Sender and Receiver nodes:



Routing Name:	PERSON_BASIC_SYNC_HR_OIM
*Service Operation:	PERSON_BASIC_SYNC
Version:	INTERNAL
*Description:	PERSON_BASIC_SYNC_HR_OIM
Comments:	
*Sender Node:	PSFT_HR
*Receiver Node:	OIM_NODE
Routing Type:	Asynchronous - One Way
Object Owner ID:	

☑ Active
□ System Generated

3. On the Parameters tab, enter the following information:

Note:

Skip this step for version type `INTERNAL`.

a. In the External Alias field, enter `PERSON_BASIC_SYNC.VERSION_3`.

b. In the Message.Ver into Transform 1 field, enter `PERSON_BASIC_SYNC.INTERNAL`.

   Here, you specify the name of the default message that you must convert.

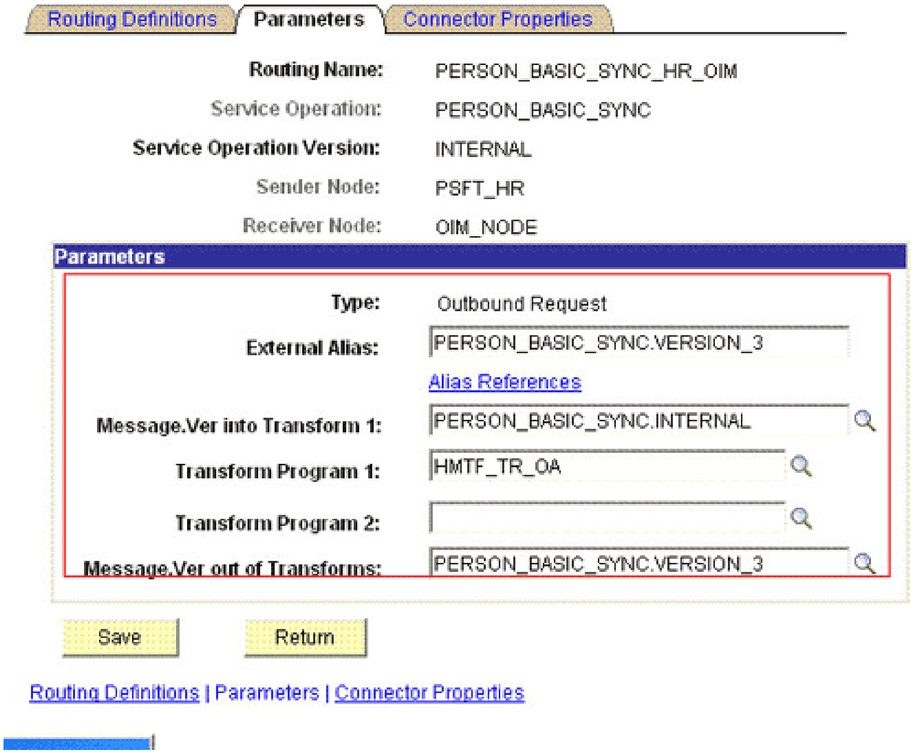
c. In the Transform Program 1 field, enter the name of the transformation program, `HMTF_TR_OA`.

> **Note:**
>
> For PeopleSoft HRMS 9.2 Image 4 or later, the value for the Transform program 1 field must be `HCM_MSG_XFRM` instead of `HMTF_TR_OA`.

d. In the Message.Ver out of Program field, enter `PERSON_BASIC_SYNC.VERSION_3`.

   Here, you specify the name into which you want to transform the message mentioned in Step b.

   The following screenshot displays the preceding steps:



Routing Name:	PERSON_BASIC_SYNC_HR_OIM
Service Operation:	PERSON_BASIC_SYNC
Service Operation Version:	INTERNAL
Sender Node:	PSFT_HR
Receiver Node:	OIM_NODE

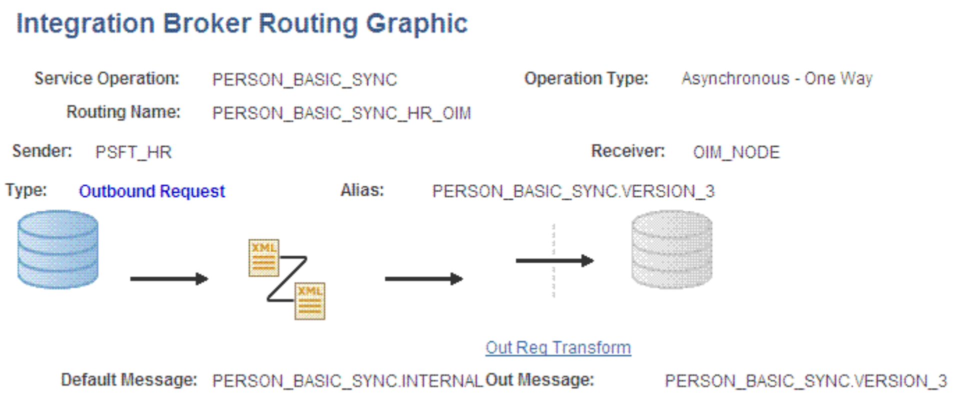
Parameters

Type:	Outbound Request
External Alias:	PERSON_BASIC_SYNC.VERSION_3
	Alias References
Message.Ver into Transform 1:	PERSON_BASIC_SYNC.INTERNAL
Transform Program 1:	HMTF_TR_OA
Transform Program 2:	
Message.Ver out of Transforms:	PERSON_BASIC_SYNC.VERSION_3

e. Click **Save.**

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

The following graphic displays the routing PERSON_BASIC_SYNC_HR_OIM and its transformation:



Integration Broker Routing Graphic

Service Operation: PERSON_BASIC_SYNC

Operation Type: Asynchronous - One Way

Routing Name: PERSON_BASIC_SYNC_HR_OIM

Sender: PSFT_HR

Receiver: OIM_NODE

Type: Outbound Request

Alias: PERSON_BASIC_SYNC.VERSION_3

Default Message: PERSON_BASIC_SYNC.INTERNAL

Out Message: PERSON_BASIC_SYNC.VERSION_3

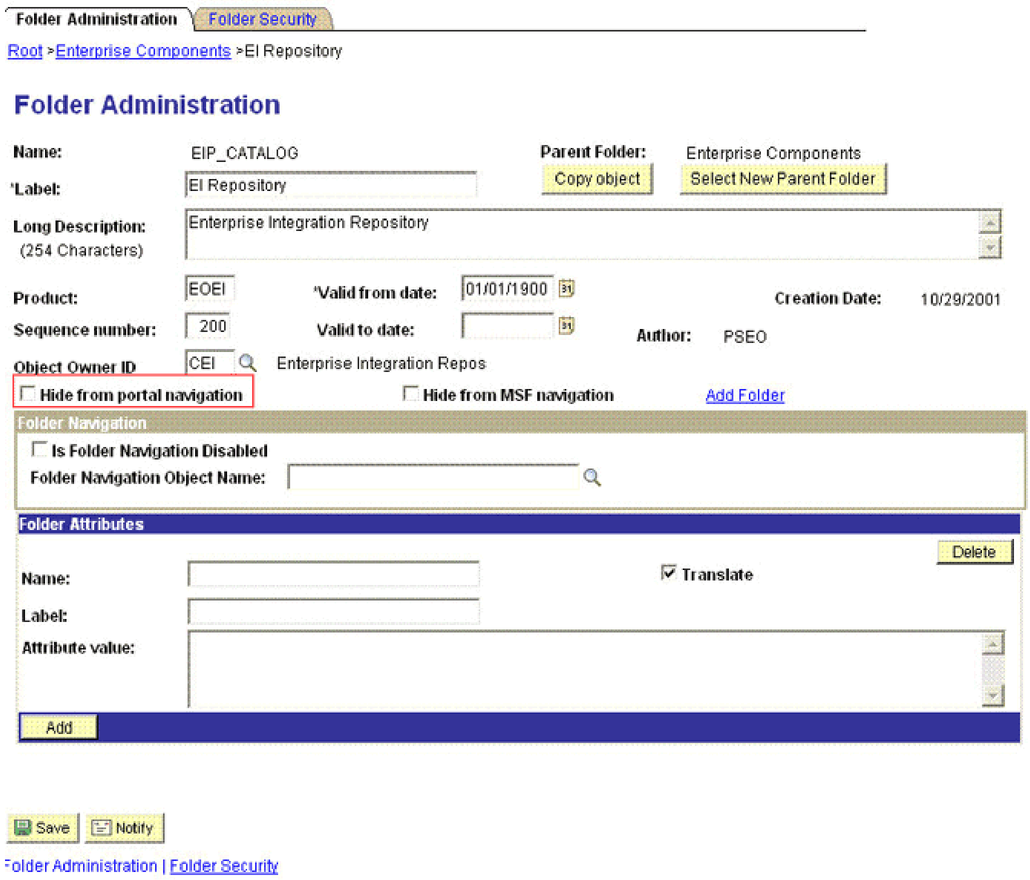
2.2.2.2.2.5 Displaying the EI Repository Folder

To display the EI Repository folder:

> **Note:**
>
> - If you are using PeopleTools 8.53, then do not perform the procedure described in this section.
> - If you have performed this procedure as described in "Displaying the EI Repository Folder", then you can skip this section.
> - Perform this procedure using the PeopleSoft administrator credentials.

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

   The following screenshot displays the Hide from portal navigation check box:



Folder Administration | Folder Security

Root > Enterprise Components > EI Repository

Folder Administration

Name:	EIP_CATALOG	Parent Folder:	Enterprise Components
*Label:	EI Repository	Copy object	Select New Parent Folder
Long Description: (254 Characters)	Enterprise Integration Repository		
Product:	EOEI	*Valid from date: 01/01/1900	Creation Date: 10/29/2001
Sequence number:	200	Valid to date:	Author: PSEO
Object Owner ID	CEI	Enterprise Integration Repos	

☐ Hide from portal navigation ☐ Hide from MSF navigation Add Folder

Folder Navigation

☐ Is Folder Navigation Disabled

Folder Navigation Object Name:

Folder Attributes

Delete

Name: ☑ Translate

Label:

Attribute value:

Add

Save Notify

Folder Administration | Folder Security

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

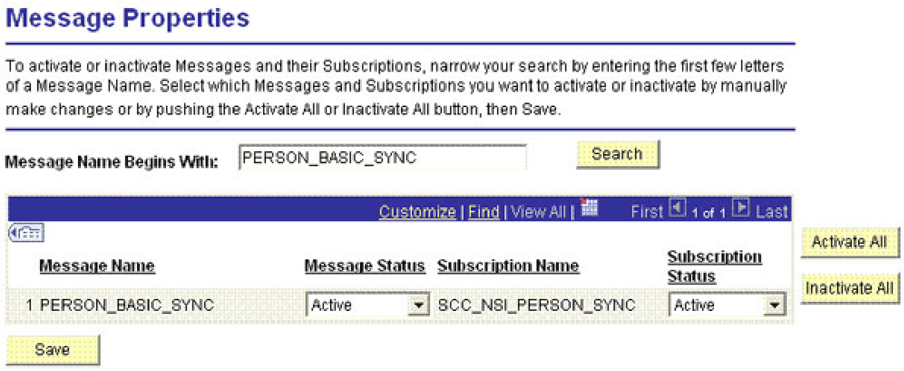
2.2.2.2.2.6 Activating the PERSON_BASIC_SYNC Message

To activate PERSON_BASIC_SYNC messages:

> **Note:**
>
> If you are using PeopleTools 8.53, then do not perform the procedure described in this section.

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

   The following screenshot displays the message to be activated:



Message Properties

To activate or inactivate Messages and their Subscriptions, narrow your search by entering the first few letters of a Message Name. Select which Messages and Subscriptions you want to activate or inactivate by manually make changes or by pushing the Activate All or Inactivate All button, then Save.

Message Name Begins With: PERSON_BASIC_SYNC

	Message Name	Message Status	Subscription Name	Subscription Status
1	PERSON_BASIC_SYNC	Active	SCC_NSI_PERSON_SYNC	Active

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

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

2.2.2.2.3 Configuring the WORKFORCE_SYNC Service Operation

This message contains the job-related details of a particular person. This information includes Employee ID and the information that is added or modified.

To configure the WORKFORCE_SYNC service operation, perform the following procedures:

> **Note:**
>
> The procedure remains the same for PeopleTools 8.49 with HRMS 9.0, PeopleTools 8.50 with HRMS 9.1, PeopleTools 8.53 through 8.57 with HRMS 9.2. The screenshots are taken on version PeopleTools 8.49.
>
> For PeopleTools 8.57, configure WORKFORCE_SYNC with default version type INTERNAL. Skip the steps for other version types.

- Activating the WORKFORCE_SYNC Service Operation
- Verifying the Queue Status for the WORKFORCE_SYNC Service Operation
- Setting Up the Security for the WORKFORCE_SYNC Service Operation
- Defining the Routing for the WORKFORCE_SYNC Service Operation
- Displaying the EI Repository Folder
- Activating the WORKFORCE_SYNC Message

2.2.2.2.3.1 Activating the WORKFORCE_SYNC Service Operation

To activate the WORKFORCE_SYNC service operation:

Note:

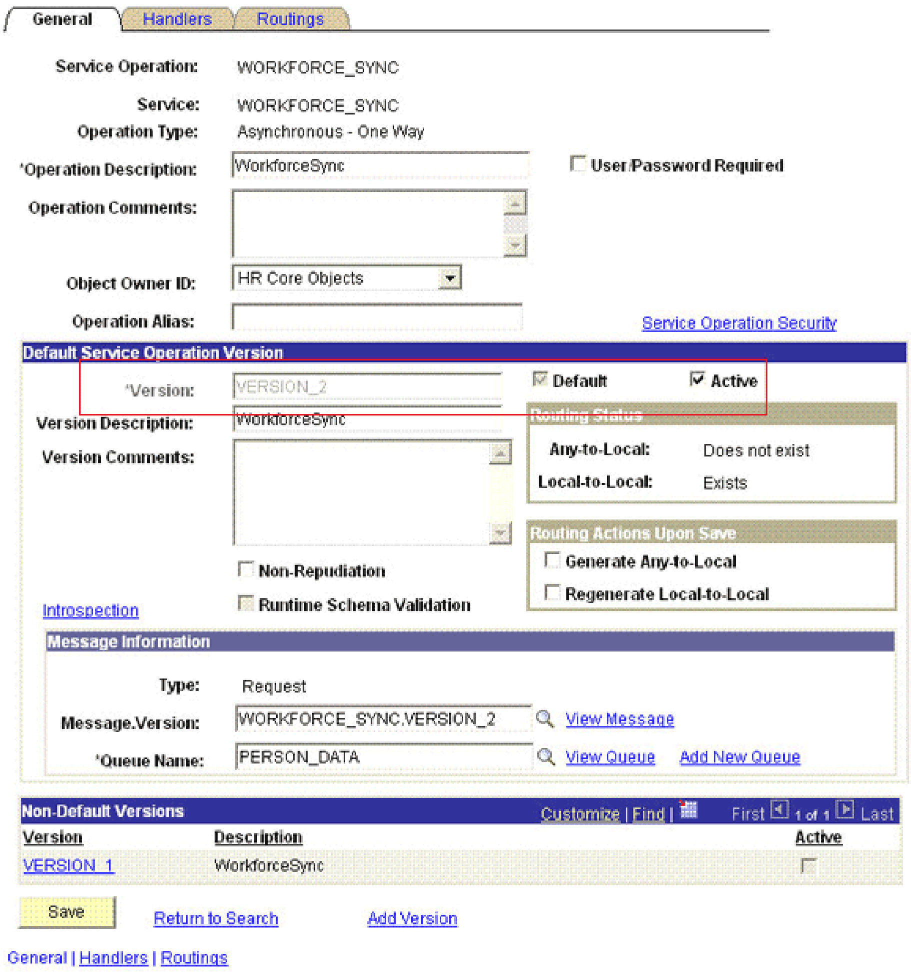
If the message version is not the same as specified, then you can change the message version as described in Changing Default Message Versions.

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

   Note:

   In PeopleSoft HRMS, there are many versions of the message associated with this service operation. But, when you integrate PeopleSoft HRMS and Oracle Identity Manager, you must use the WORKFORCE_SYNC.INTERNAL version of the service operation.

   The following screenshot displays the default version of the WORKFORCE_SYNC service operation:



Service Operation: WORKFORCE_SYNC

Service: WORKFORCE_SYNC

Operation Type: Asynchronous - One Way

*Operation Description: WorkforceSync

□ User/Password Required

Operation Comments:

Object Owner ID: HR Core Objects

Operation Alias:

Default Service Operation Version

*Version: VERSION_2

☑ Default ☑ Active

Version Description: WorkforceSync

Version Comments:

Routing Status

Any-to-Local:	Does not exist
Local-to-Local:	Exists

□ Non-Repudiation

□ Runtime Schema Validation

Routing Actions Upon Save

□ Generate Any-to-Local

□ Regenerate Local-to-Local

Message Information

Type: Request

Message.Version: WORKFORCE_SYNC.VERSION_2

*Queue Name: PERSON_DATA

Non-Default Versions

Version	Description	Active
VERSION_1	WorkforceSync	□

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

2.2.2.2.3.2 Verifying the Queue Status for the WORKFORCE_SYNC Service Operation

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

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

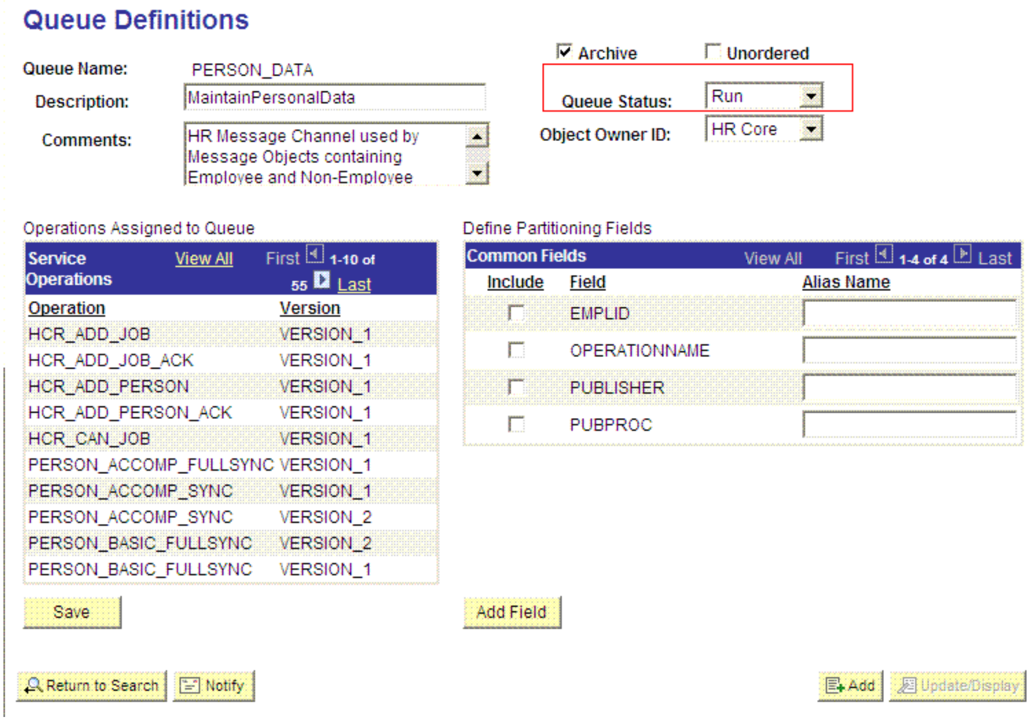
Note:

If the queue status is not Run:

a. From the Queue Status list, select **Run.**

b. Click **Save.**

The queue status is shown in the following screenshot:



Queue Definitions

☑ Archive □ Unordered

Queue Name: PERSON_DATA

Description: MaintainPersonalData

Queue Status: Run

Comments: HR Message Channel used by Message Objects containing Employee and Non-Employee

Object Owner ID: HR Core

Operations Assigned to Queue

Service Operations — View All — First 1-10 of 55 Last

Operation	Version
HCR_ADD_JOB	VERSION_1
HCR_ADD_JOB_ACK	VERSION_1
HCR_ADD_PERSON	VERSION_1
HCR_ADD_PERSON_ACK	VERSION_1
HCR_CAN_JOB	VERSION_1
PERSON_ACCOMP_FULLSYNC	VERSION_1
PERSON_ACCOMP_SYNC	VERSION_1
PERSON_ACCOMP_SYNC	VERSION_2
PERSON_BASIC_FULLSYNC	VERSION_2
PERSON_BASIC_FULLSYNC	VERSION_1

Define Partitioning Fields

Common Fields — View All — First 1-4 of 4 Last

Include	Field	Alias Name
□	EMPLID	
□	OPERATIONNAME	
□	PUBLISHER	
□	PUBPROC	

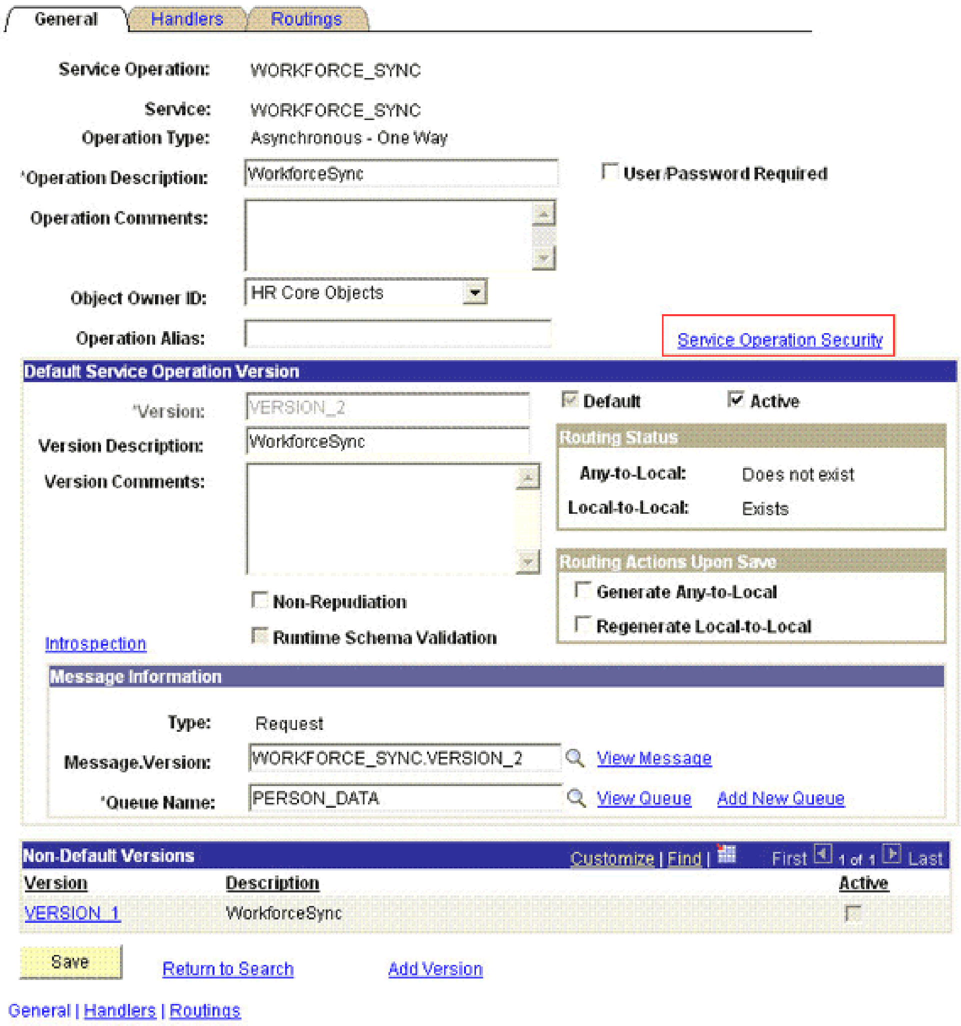
4. Click **Return to Search.**

2.2.2.2.3.3 Setting Up the Security for the WORKFORCE_SYNC Service Operation

To set up the security for the WORKFORCE_SYNC service operation:

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

   The following screenshot displays the link:



Service Operation: WORKFORCE_SYNC

Service: WORKFORCE_SYNC

Operation Type: Asynchronous - One Way

*Operation Description: WorkforceSync

□ User/Password Required

Operation Comments:

Object Owner ID: HR Core Objects

Operation Alias:

Default Service Operation Version

*Version: VERSION_2

☑ Default ☑ Active

Version Description: WorkforceSync

Version Comments:

Routing Status

Any-to-Local:	Does not exist
Local-to-Local:	Exists

Routing Actions Upon Save

□ Generate Any-to-Local

□ Regenerate Local-to-Local

□ Non-Repudiation

□ Runtime Schema Validation

Message Information

Type: Request

Message.Version: WORKFORCE_SYNC.VERSION_2

*Queue Name: PERSON_DATA

Non-Default Versions

Version	Description	Active
VERSION_1	WorkforceSync	□

4. Attach the **OIMER** permission list to the **WORKFORCE_SYNC** 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 OIMER permission list. The OIMER permission list is used as an example. But, to implement this procedure you must use the permission list (attached through a role) to the user profile that has the privilege to modify job data in the target system.

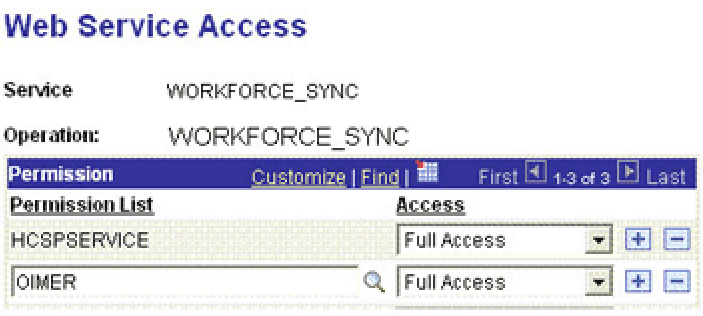
   a. Click the plus sign (+) to add a row to the Permission List field.

   b. In the Permission List field, enter `OIMER` and then click the Look up Permission List icon.

      The **OIMER** permission list appears.

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

The following screenshot displays the permission list with Full Access:



Web Service Access

Service: WORKFORCE_SYNC

Operation: WORKFORCE_SYNC

Permission — Customize | Find | First 1-3 of 3 Last

Permission List	Access
HCSPSERVICE	Full Access
OIMER	Full Access

d. Click **Save.**

e. Click **Return to Search.**

2.2.2.2.3.4 Defining the Routing for the WORKFORCE_SYNC Service Operation

To define the routing for the WORKFORCE_SYNC service operation:

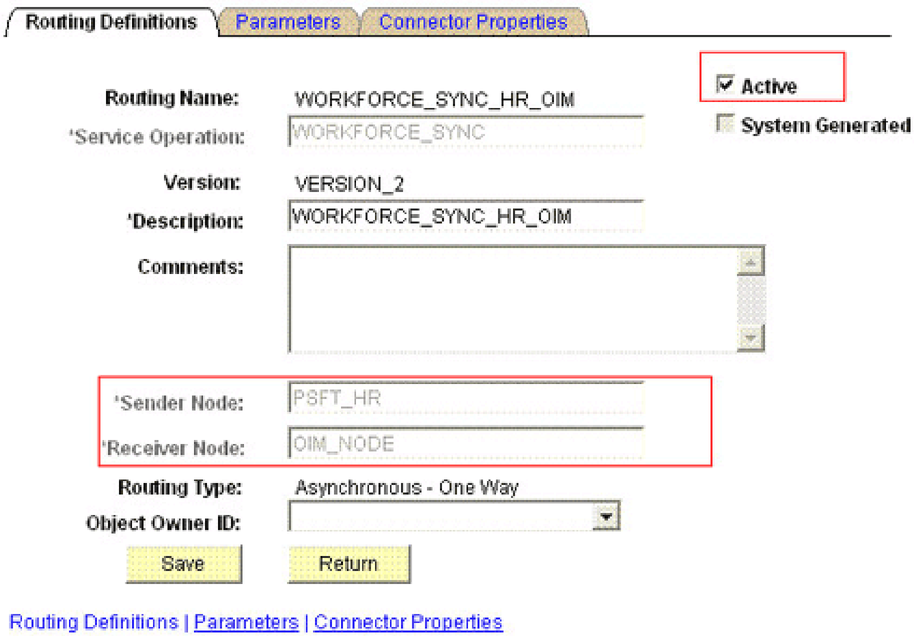
1. On the Routing tab, enter `WORKFORCE_SYNC_HR_OIM` as the routing name and then click **Add.**
2. On the Routing Definitions tab, enter the following:

   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:



☑ Active
□ System Generated

Routing Name: WORKFORCE_SYNC_HR_OIM
*Service Operation: WORKFORCE_SYNC
Version: VERSION_2
*Description: WORKFORCE_SYNC_HR_OIM
Comments:
*Sender Node: PSFT_HR
*Receiver Node: OIM_NODE
Routing Type: Asynchronous - One Way
Object Owner ID:

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

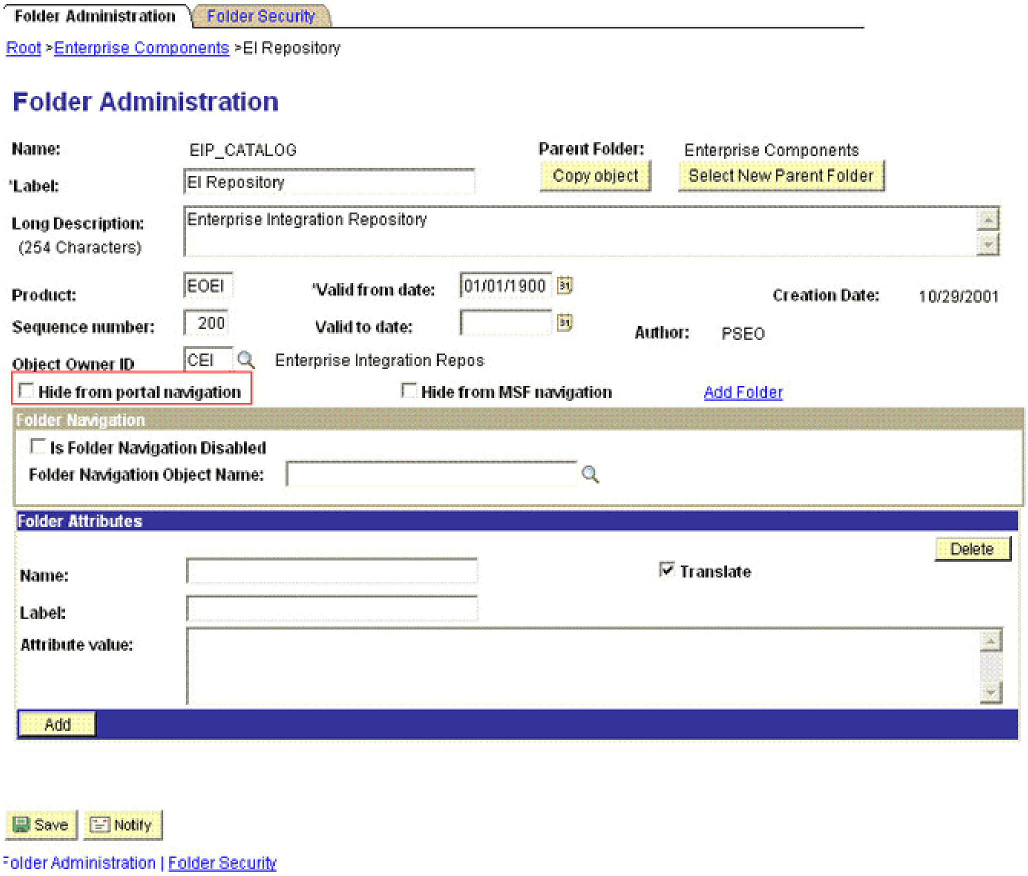
2.2.2.2.3.5 Displaying the EI Repository Folder

To display the EI Repository folder:

> **Note:**
>
> - If you are using PeopleTools 8.53, then do not perform the procedure described in this section.
> - If you have performed this procedure as described in "Displaying the EI Repository Folder", then you can skip this section.
> - Perform this procedure using the PeopleSoft administrator credentials.

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

   The following screenshot displays the Hide from portal navigation check box:



Root >Enterprise Components >EI Repository

Folder Administration

Name:	EIP_CATALOG	Parent Folder:	Enterprise Components
*Label:	EI Repository		
Long Description: (254 Characters)	Enterprise Integration Repository		
Product:	EOEI	*Valid from date:	01/01/1900
Sequence number:	200	Valid to date:	
Object Owner ID	CEI Enterprise Integration Repos		
Creation Date:	10/29/2001	Author:	PSEO

□ Hide from portal navigation
□ Hide from MSF navigation

Folder Navigation

□ Is Folder Navigation Disabled
Folder Navigation Object Name:

Folder Attributes

Name:
Label:
Attribute value:
☑ Translate

Folder Administration | Folder Security

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

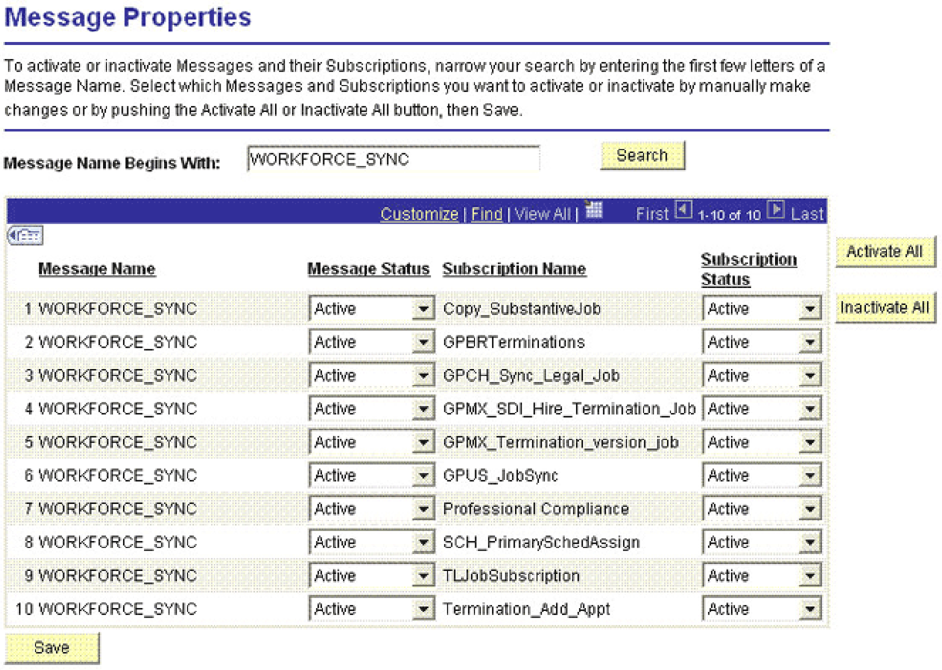
2.2.2.2.3.6 Activating the WORKFORCE_SYNC Message

To activate the WORKFORCE_SYNC message:

> **Note:**
>
> If you are using PeopleTools 8.53, then do not perform the procedure described in this section

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

   The following screenshot displays the message to be activated:



Message Properties

To activate or inactivate Messages and their Subscriptions, narrow your search by entering the first few letters of a Message Name. Select which Messages and Subscriptions you want to activate or inactivate by manually make changes or by pushing the Activate All or Inactivate All button, then Save.

Message Name Begins With: WORKFORCE_SYNC

	Message Name	Message Status	Subscription Name	Subscription Status
1	WORKFORCE_SYNC	Active	Copy_SubstantiveJob	Active
2	WORKFORCE_SYNC	Active	GPBRTerminations	Active
3	WORKFORCE_SYNC	Active	GPCH_Sync_Legal_Job	Active
4	WORKFORCE_SYNC	Active	GPMX_SDI_Hire_Termination_Job	Active
5	WORKFORCE_SYNC	Active	GPMX_Termination_version_job	Active
6	WORKFORCE_SYNC	Active	GPUS_JobSync	Active
7	WORKFORCE_SYNC	Active	Professional Compliance	Active
8	WORKFORCE_SYNC	Active	SCH_PrimarySchedAssign	Active
9	WORKFORCE_SYNC	Active	TLJobSubscription	Active
10	WORKFORCE_SYNC	Active	Termination_Add_Appt	Active

4. Click the **Subscription** tab, and activate the Subscription PeopleCode.

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

2.2.2.2.4 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 below for more information on removing unwanted fields at the message level.
  – 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 below for more information on removing unwanted fields at the message level.
  – 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.

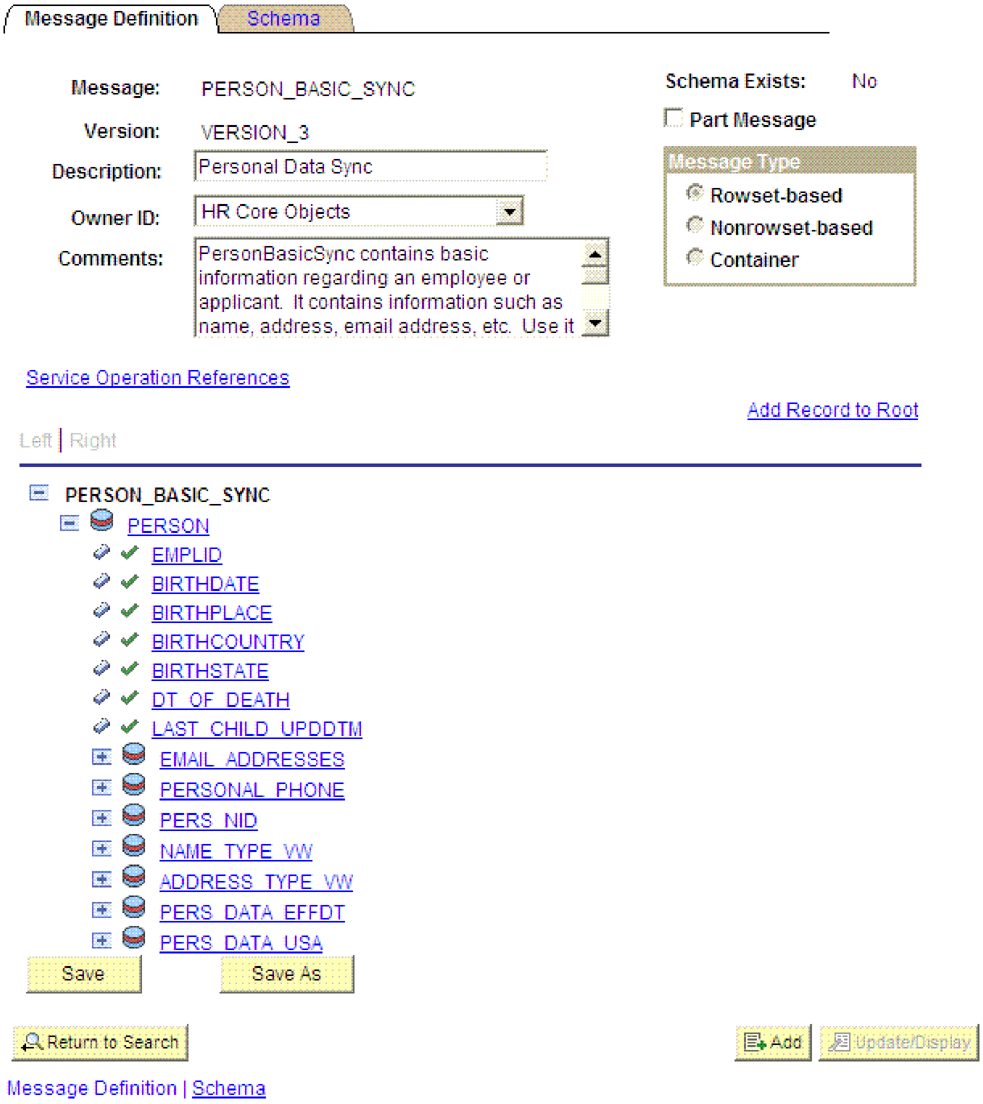
    For more information about implementing transformation, refer to Chapter 21 of Integration Broker PeopleBook on Oracle Technology Network at the following location http://download.oracle.com/docs/cd/E13292_01/pt849pbr0/eng/psbooks/tibr/book.htm

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

- Remove unwanted fields at the message level. To do so:

  1. Expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Messages.**
  2. Search for and open the desired message, for example, PERSON_BASIC_SYNC.VERSION_3 used for incremental reconciliation.
  3. Expand the message.



Message: PERSON_BASIC_SYNC

Version: VERSION_3

Description: Personal Data Sync

Owner ID: HR Core Objects

Comments: PersonBasicSync contains basic information regarding an employee or applicant. It contains information such as name, address, email address, etc. Use it

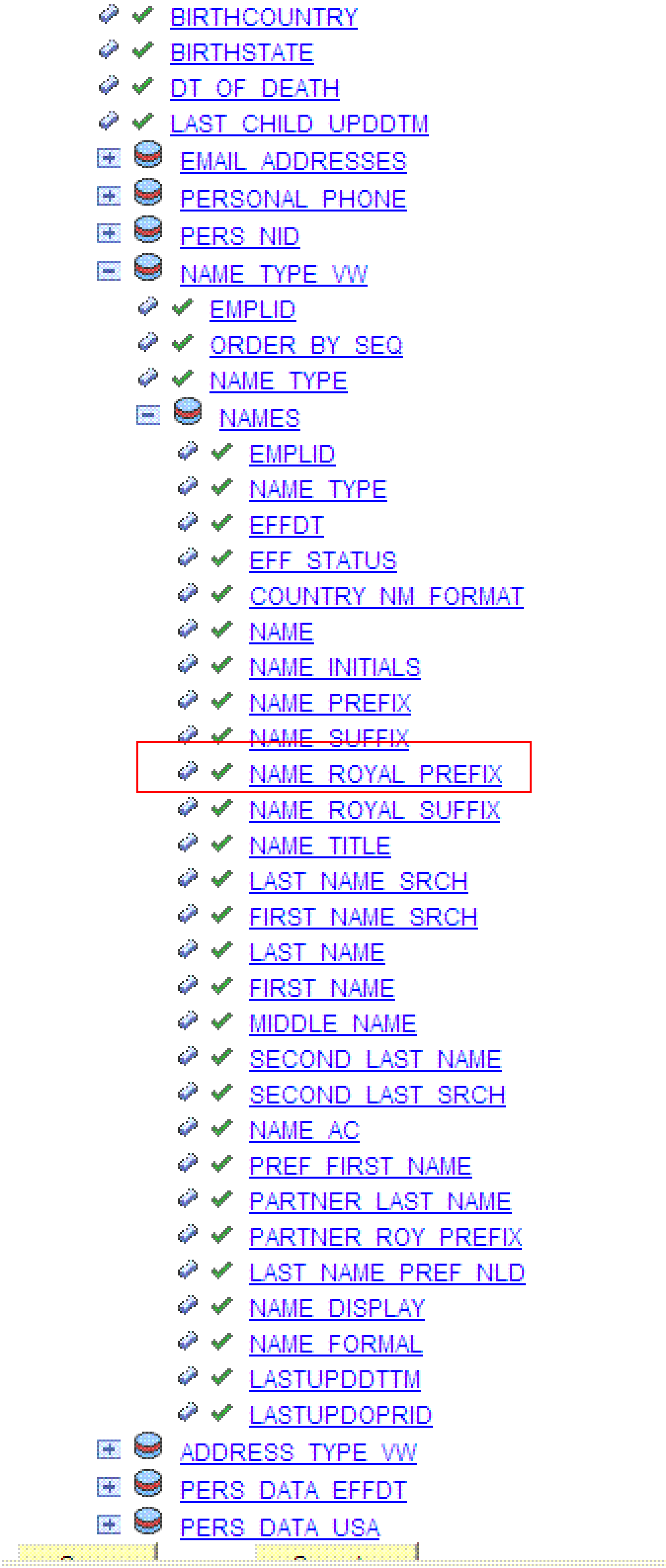
Schema Exists: No

□ Part Message

Message Type
● Rowset-based
○ Nonrowset-based
○ Container

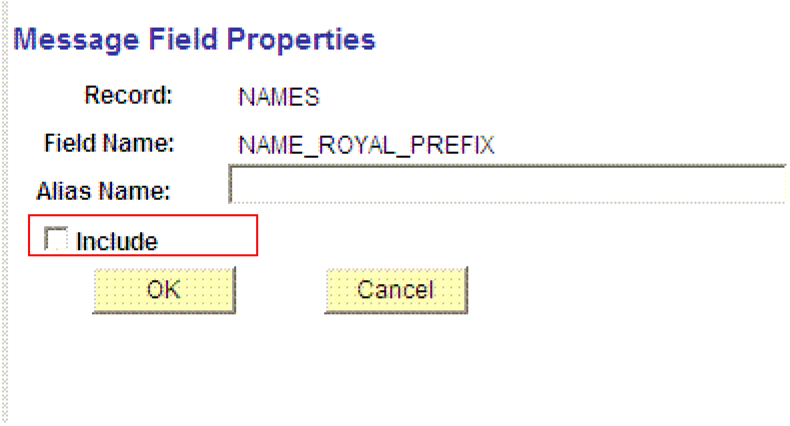
PERSON_BASIC_SYNC
- PERSON
  - ✓ EMPLID
  - ✓ BIRTHDATE
  - ✓ BIRTHPLACE
  - ✓ BIRTHCOUNTRY
  - ✓ BIRTHSTATE
  - ✓ DT_OF_DEATH
  - ✓ LAST_CHILD_UPDDTM
  - EMAIL_ADDRESSES
  - PERSONAL_PHONE
  - PERS_NID
  - NAME_TYPE_VW
  - ADDRESS_TYPE_VW
  - PERS_DATA_EFFDT
  - PERS_DATA_USA

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



- ✓ BIRTHCOUNTRY
- ✓ BIRTHSTATE
- ✓ DT_OF_DEATH
- ✓ LAST_CHILD_UPDDTM
- ⊞ EMAIL_ADDRESSES
- ⊞ PERSONAL_PHONE
- ⊞ PERS_NID
- ⊟ NAME_TYPE_VW
  - ✓ EMPLID
  - ✓ ORDER_BY_SEQ
  - ✓ NAME_TYPE
  - ⊟ NAMES
    - ✓ EMPLID
    - ✓ NAME_TYPE
    - ✓ EFFDT
    - ✓ EFF_STATUS
    - ✓ COUNTRY_NM_FORMAT
    - ✓ NAME
    - ✓ NAME_INITIALS
    - ✓ NAME_PREFIX
    - ✓ NAME_SUFFIX
    - ✓ NAME_ROYAL_PREFIX
    - ✓ NAME_ROYAL_SUFFIX
    - ✓ NAME_TITLE
    - ✓ LAST_NAME_SRCH
    - ✓ FIRST_NAME_SRCH
    - ✓ LAST_NAME
    - ✓ FIRST_NAME
    - ✓ MIDDLE_NAME
    - ✓ SECOND_LAST_NAME
    - ✓ SECOND_LAST_SRCH
    - ✓ NAME_AC
    - ✓ PREF_FIRST_NAME
    - ✓ PARTNER_LAST_NAME
    - ✓ PARTNER_ROY_PREFIX
    - ✓ LAST_NAME_PREF_NLD
    - ✓ NAME_DISPLAY
    - ✓ NAME_FORMAL
    - ✓ LASTUPDDTTM
    - ✓ LASTUPDOPRID
- ⊞ ADDRESS_TYPE_VW
- ⊞ PERS_DATA_EFFDT
- ⊞ PERS_DATA_USA

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



Message Field Properties

Record:	NAMES
Field Name:	NAME_ROYAL_PREFIX
Alias Name:	

□ Include

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

2.3 Postinstallation

Postinstallation information is divided across the following sections:

- Configuring Oracle Identity Manager
- Configuring the Target System

2.3.1 Configuring Oracle Identity Manager

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

- Enabling Logging
- Setting Up the Lookup.PSFT.HRMS.ExclusionList Lookup Definition
- Setting Up the Lookup.PSFT.HRMS.Configuration Lookup Definition
- Configuring SSL
- Creating an Authorization Policy for Job Code
- Displaying UDFs in Oracle Identity Manager 11.1.2.x or Later

2.3.1.1 Enabling Logging

This section contains the following topics:

- Log Levels and Message Types
- Enabling Logging on Oracle WebLogic Server

2.3.1.1.1 Log Levels and Message Types

Oracle Identity Manager uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.
- SEVERE

  This level enables logging of information about errors that 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

2.3.1.1.2 Enabling Logging on Oracle WebLogic Server

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

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

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

To enable logging on Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

```
<log_handler name='psft-er-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="ORACLE.IAM.CONNECTORS.PSFT" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="psft-er-handler"/>
     <handler name="console-handler"/>
   </logger>

<logger name="ORACLE.IAM.CONNECTORS.PSFT.HRMS" level="[LOG_LEVEL]"
useParentHandlers="false">
<handler name="psft-er-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-er-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_se
rver1\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="ORACLE.IAM.CONNECTORS.PSFT" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="psft-er-handler"/>
     <handler name="console-handler"/>
   </logger>

<logger name="ORACLE.IAM.CONNECTORS.PSFT.HRMS" level="NOTIFICATION:1"
useParentHandlers="false">
<handler name="psft-er-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 actual name of the file to which you want to redirect the output.
4. Restart the application server.

2.3.1.2 Setting Up the Lookup.PSFT.HRMS.ExclusionList Lookup Definition

In the Lookup.PSFT.HRMS.ExclusionList lookup definition, enter the user IDs of target system accounts for which you do not want to perform reconciliation. See Lookup.PSFT.HRMS.ExclusionList for more information about this lookup definition.

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the **Lookup.PSFT.HRMS.ExclusionList** lookup definition.
3. Click **Add.**

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

4. In the Code Key and Decode columns, enter the first user ID to exclude.
5. Repeat Steps 3 and 4 for all the user IDs you want to exclude.

   For example, if you do not want to reconcile users with 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

6. Click the Save icon.

2.3.1.3 Setting Up the Lookup.PSFT.HRMS.Configuration Lookup Definition

Every standard PeopleSoft message has a message-specific configuration defined in the Lookup.PSFT.HRMS.Configuration lookup definition. See Lookup.PSFT.HRMS.Configuration for more information about this lookup definition.

For example, the mapping for the PERSON_BASIC_SYNC message in this lookup definition is defined as follows:

Code Key: PERSON_BASIC_SYNC

Decode: Lookup.PSFT.Message.PersonBasicSync.Configuration

You can configure the message names, such as PERSON_BASIC_SYNC, WORKFORCE_SYNC, PERSON_BASIC_FULLSYNC, and WORKFORCE_FULLSYNC defined in this lookup definition.

Consider a scenario in which the target system sends the PERSON_BASIC_SYNC.VERSION_3 message. You must change the Code Key value in this lookup definition to implement the message sent by the target system.

To modify or set the Code Key value:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the **Lookup.PSFT.HRMS.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: PERSON_BASIC_SYNC.VERSION_3

   Decode: Lookup.PSFT.Message.PersonBasicSync.Configuration
5. Repeat Steps 3 and 4 to modify the Code Key values for all the standard PeopleSoft messages you want to rename in this lookup definition.
6. Click the Save icon.

2.3.1.4 Configuring SSL

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

2.3.1.4.1 Configuring SSL on IBM WebSphere Application Server

You can configure SSL connectivity on IBM WebSphere Application Server with either a self-signed certificate or a CA certificate. Perform the procedure described in one of the following sections:

- Configuring SSL on IBM WebSphere Application Server with a Self-Signed Certificate
- Configuring SSL on IBM WebSphere Application Server with a CA Certificate

2.3.1.4.1.1 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.**

2.3.1.4.1.2 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:

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.

17. To receive a signed certificate issued by a CA, perform the following tasks:

a. 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.**
b. Click **Receive a certificate from a certificate authority.**
c. Enter the full path and name of the certificate file.
d. Select the default data type from the list.
e. Click **Apply** and then **Save.**

The keystore contains a new personal certificate that is issued by a CA. The SSL configuration is ready to use the new CA-signed personal certificate.

2.3.1.4.2 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. Perform the procedure described in one of the following sections:

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

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

2.3.1.4.2.1 Configuring SSL on Oracle WebLogic Server with a Self-Signed Certificate

To configure SSL connectivity between Oracle Identity Manager on Oracle WebLogic Server and the target system with a self-signed certificate, you must perform the following tasks:

To generate the keystore:

1. Run the following command:

   ```
   keytool -genkey -keystore ABSOLUTE_KEYSTORE_PATH -alias ALIAS_NAME -keyalg
   KEY_ALGORITHM -storepass KEYSTORE_PASSWORD -keypass PRIVATE_KEY_PASSWORD
   ```

   For example:

   ```
   keytool -genkey -keystore c:\temp\keys\keystore.jks -alias example088196 -
   keyalg RSA -storepass example1234 -keypass example1234
   ```

> **Note:**
>
> - The keystore password and the private key password must be the same.
>
> - Typically, the alias is the name or the IP address of the computer on which you are configuring SSL.
>
> - The alias used in the various commands of this procedure must be the same.

2. When prompted, enter information about the certificate. This information is displayed to persons attempting to access a secure page in the application. This is illustrated in the following example:

   ```
   keytool -genkey -keystore c:\temp\keys\keystore.jks -alias example088196    -
   keyalg RSA -storepass example1234 -keypass example1234
   What is your first and last name?
     [Unknown]: Must be the name or IP address of the computer
   What is the name of your organizational unit?
     [Unknown]:  example
   What is the name of your organization?
     [Unknown]:  example
   What is the name of your City or Locality?
     [Unknown]:  New York
   What is the name of your State or Province?
     [Unknown]:  New York
   What is the two-letter country code for this unit?
     [Unknown]:  US
   Is <CN=Name or IP address of the computer, OU=example, O=example, L=New York,
   ST=New York, C=US> correct?
     [no]:  yes
   ```

   When you enter yes in the last line of the preceding example, the keystore.jks file is created in the c:\temp\keys\directory.

3. Export the keystore to a certificate file by running the following command:

   ```
   keytool -export -alias ALIAS_NAME -keystore ABSOLUTE_KEYSTORE_PATH -file
   CERTIFICATE_FILE_ABSOLUTE_PATH
   ```

   For example:

   ```
   keytool -export -alias example088196 -keystore c:\temp\keys\keystore.jks -file
   c:\temp\keys\keystore.cert
   ```

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

5. Import the keystore by running the following command:

   ```
   keytool -import -alias ALIAS_NAME -keystore NEW_KEYSTORE_ABSOLUTE_PATH -file
   CERTIFICATE_FILE_ABSOLUTE_PATH
   ```

   For example:

   ```
   keytool -import -alias example088196 -keystore c:\temp\keys\new.jks -file
   c:\temp\keys\keystore.cert
   ```

   When you run this command, it prompts for the keystore password, as shown in the following example:

```
Enter keystore password:  example1234 [Enter]
Trust this certificate? [no]:  yes [Enter]
Certificate was added to keystore
```

In this example, the instances when you can press Enter are shown in bold.

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

1. Log in to the Oracle WebLogic Server console at `http://`*`localhost`*`:7001/console` and perform the following:
    1. Expand the servers node and select the **oim** server instance.
    2. Select the **General** tab.
    3. Select the **SSL Listen Port Enabled** option.
    4. Ensure that a valid port is specified in the SSL Listen Port field. The default port is 7002.
    5. Click **Apply** to save your changes.
2. Click the **Keystore & SSL** tab, and then click **Change.**
3. From the Keystores list, select **Custom identity And Java Standard Trust,** and then click **Continue.**
4. Configure the keystore properties. To do so:
    1. In the Custom Identity Key Store File Name column, specify the full path of the keystore generated in Step 1 of generating the keystore, 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.
    2. Provide the Java standard trust keystore pass phrase and the Confirm Java standard trust keystore pass phrase. The default password is `changeit`, unless you change the password.
    3. Click **Continue.**
5. Specify the private key alias, pass phrase and the confirm pass phrase as the keystore password. Click **Continue.**
6. Click **Finish.**
7. Restart Oracle WebLogic Server. If the server starts successfully with the SSL configuration, then lines similar to the following are recorded in the startup log:

```
<Apr 21, 2008 2:35:43 PM GMT+05:30> <Notice> <WebLogicServer> <BEA-000355>
<Thread "ListenThread.Default" listening on port 7001, ip address *.*>
<Apr 21, 2008 2:35:43 PM GMT+05:30> <Notice> <WebLogicServer> <BEA-000355>
<Thread "SSLListenThread.Default" listening on port 7002, ip address *.*>
```

> **Note:**
>
> 7002 is the default SSL port for Oracle WebLogic Server.

2.3.1.4.2.2 Configuring SSL on Oracle WebLogic Server with a CA Certificate

To configure SSL connectivity between Oracle Identity Manager on Oracle WebLogic Server and the target system with a CA certificate, you must perform the following tasks:

> **Note:**
>
> Although this is an optional step in the deployment procedure, Oracle strongly recommends that you configure SSL communication between the target system and Oracle Identity Manager.

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

1. Run the following command:

   ```
   keytool -genkey -keystore ABSOLUTE_KEYSTORE_PATH -alias ALIAS_NAME -keyalg
   KEY_ALGORITHM -storepass KEYSTORE_PASSWORD -keypass PRIVATE_KEY_PASSWORD
   ```

   For example:

   ```
   keytool -genkey -keystore c:\temp\keys\keystore.jks -alias example088196 -keyalg
   RSA -storepass example1234 -keypass example1234
   ```

   > **Note:**
   >
   > The keystore password and the private key password must be the same.
   >
   > Typically, the alias name is the name or the IP address of the computer on which you are configuring SSL.

2. When prompted, enter the information about the certificate. This information is displayed to persons attempting to access a secure page in the application. This is illustrated in the following example:

   ```
   keytool -genkey -keystore c:\temp\keys\keystore.jks -alias example088196    -
   keyalg RSA -storepass example1234 -keypass example1234
   What is your first and last name?
     [Unknown]:  Must be the name or IP address of the computer
   What is the name of your organizational unit?
     [Unknown]:  example
   What is the name of your organization?
     [Unknown]:  example
   What is the name of your City or Locality?
     [Unknown]:  New York
   What is the name of your State or Province?
     [Unknown]:  New York
   What is the two-letter country code for this unit?
     [Unknown]:  US
   Is <CN=Name or IP address of the computer, OU=example, O=example, L=New York,
   ST=New York, C=US> correct?
     [no]:  yes
   ```

When you enter yes in the last line of the preceding example, the keystore.jks file is created in the c:\temp\keys\directory.

3. Generate the certificate signing request by running the following command:

   ```
   keytool -certreq -keystore ABSOLUTE_KEYSTORE_PATH -alias ALIAS_NAME -keyalg
   KEY_ALGORITHM -file CERTIFICATE_FILE_ABSOLUTE_PATH
   ```

   For example:

   ```
   keytool -certreq -keystore c:\temp\keys\keystore.jks -alias example088196 -
   keyalg RSA -file c:\temp\keys\keystore.cert
   ```

   When prompted for the keystore password, enter the same password used for the keystore in Step 1, for example `example1234`. This stores a certificate request in the file that you specified in the preceding command.

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

5. Export the keystore generated in Step 1 to a new certificate file, for example, myCert.cer, by running the following command:

   ```
   keytool –export –keystore ABSOLUTE_KEYSTORE_PATH -alias alias-name specified
   in step 1 -file CERTIFICATE_FILE_ABSOLUTE_PATH
   ```

   For example:

   ```
   keytool –export –keystore c:\temp\keys\keystore.jks -alias example088196 -
   file c:\temp\keys\myCert.cer
   ```

6. Import the CA certificate to a new keystore by running the following command:

   ```
   keytool -import -alias ALIAS_NAME -file CERTIFICATE_FILE_ABSOLUTE_PATH -
   keystore NEW_KEYSTORE_ABSOLUTE_PATH -storepass KEYSTORE_PASSWORD generated
   in Step 1
   ```

   For example:

   ```
   keytool -import -alias example088196 -file c:\temp\keys\rootCert.cert -
   keystore c:\temp\keys\rootkeystore.jks
   ```

   When you run this command, it prompts for the keystore password, as shown:

   ```
   Enter keystore password:  example1234 [Enter]
   Trust this certificate? [no]:  yes [Enter]
   Certificate was added to keystore
   ```

   In this example, the instances when you can press Enter are shown in bold.

After creating and importing the keystore to the system, start Oracle WebLogic Server. To configure Oracle WebLogic Server:

1. Log in to the Oracle WebLogic Server console ((http://*localhost*:7001/console) and perform the following:

   a. Expand the server node and select the server instance.

   b. Select the **General** tab.

   c. Select the **SSL Port Enabled** option.

   d. Ensure that a valid port is specified in the SSL Listen Port field. The default port is 7002.

   e. Click **Apply** to save your changes.

2. Click the **Keystore & SSL** tab, and click the **Change** link.
3. From the Keystores list, select **Custom Identity And Custom Trust,** and then click **Continue.**
4. Configure the keystore properties. To do so:
   a. In the Custom Identity Key Store File Name column, specify the full path of the keystore generated in Step 1 of generating the keystore, for example, `c:\temp\keys\keystore.jks`. In the Custom Identity Key Store Type column, specify the type of keystore, for example, `JKS`. In the Custom Identity Key Store Pass Phrase and Confirm Custom Identity Key Store Pass Phrase columns, specify the keystore password.
   b. In the Custom Trust and Custom Trust Key Store File Name column, specify the full path of the keystore generated in Step 1 of generating the keystore, 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`, unless you change the password.
   d. Click **Continue.**
5. Specify the alias name and private key password. Click **Continue.**
6. Click **Finish.**
7. Restart Oracle WebLogic Server. If the server starts successfully with the SSL configuration, then lines similar to the following are recorded in the startup log:

```
<Apr 21, 2008 2:35:43 PM GMT+05:30> <Notice> <WebLogicServer> <BEA-000355> <Thread
"ListenThread.Default" listening on port 7001, ip address *.*>
<Apr 21, 2008 2:35:43 PM GMT+05:30> <Notice> <WebLogicServer> <BEA-000355> <Thread
"SSLListenThread.Default" listening on port 7002, ip address *.*>
```

> **Note:**
>
> 7002 is the default SSL port for Oracle WebLogic Server.

2.3.1.5 Creating an Authorization Policy for Job Code

> **Note:**
>
> Perform this procedure only if you are using Oracle Identity Manager release 11*g* R1 (11.1.1.*x*). You must configure the authorization policy for Supervisor ID if you want to use PeopleSoft HRMS Manager Reconciliation scheduled task.

The following instructions are specific to individual steps of the procedure described in the "Creating an Authorization Policy for User Management" section of that chapter:

- When you reach Step 3, then:

  In the Policy Name field, enter `Job Code Authorization Policy.`

- When you reach Step 4, then:

  In the Description field, enter `Job Code Authorization Policy.`

- When you reach Step 7, then:

  In the Permissions table, select the following check boxes in the Enable column:

  – Modify User Profile

  – Search User

  – View User Details

  Click **Edit Attributes.**

  On the Attribute Settings page, clear all the check boxes and select **Job Code**.

- When you reach Step 14 c, then:

  From the Available Roles list, select **System Administrator,** and then click the **Move** button to move the selected role to the **Organizations to Add** list.

> **Note:**
>
> Perform the preceding steps to create an authorization policy for any user-defined field that you want to add, for example Supervisor ID, Department, and so on.

2.3.1.6 Displaying UDFs in Oracle Identity Manager 11.1.2.x or Later

In Oracle Identity Manager release 11.1.2.*x* or later, some user attributes (UDFs) such as Department, Job Code, and Supervisor ID are not displayed after running the reconciliation for the WORKFORCE_FULLSYNC message. If you want to display these attributes as form fields in the Oracle Identity Manager user interface, then you must customize the associated pages on the interface to add the custom form fields. To do so:

1. Perform reconciliation for the WORKFORCE_FULLSYNC message.
2. Log in to Oracle Identity System Administration.
3. Create and activate a sandbox.
4. From the Identity System Administration Console, in the Upgrade region, click **Upgrade User Form.**

   All the UDFs are listed.
5. Click **Upgrade now.**
6. Publish the sandbox.

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

2.3.2 Configuring the Target System

Postinstallation on the target system consists of configuring SSL. To do so:

1. Copy the certificate to the computer on which PeopleSoft HRMS/HCM 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 to import.

   > **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.

2.4 Upgrading the Connector

You can upgrade the PeopleSoft Employee Reconciliation 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 Employee Reconciliation connector from release 9.1.1.6 to this release of the connector, perform the following procedures:

- Prerequisites for Upgrading the Connector
- Re-defining the Connector
- Running the Upgrade Wizard
- Upgrading the Connector Files and External Code Files
- Upgrading the PeopleSoft Listener
- Upgrading the Customizations
- Updating the PeopleSoft Target System
- Compiling the Adapters

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

2.4.1 Prerequisites for Upgrading the Connector

Before you perform the upgrade procedures:

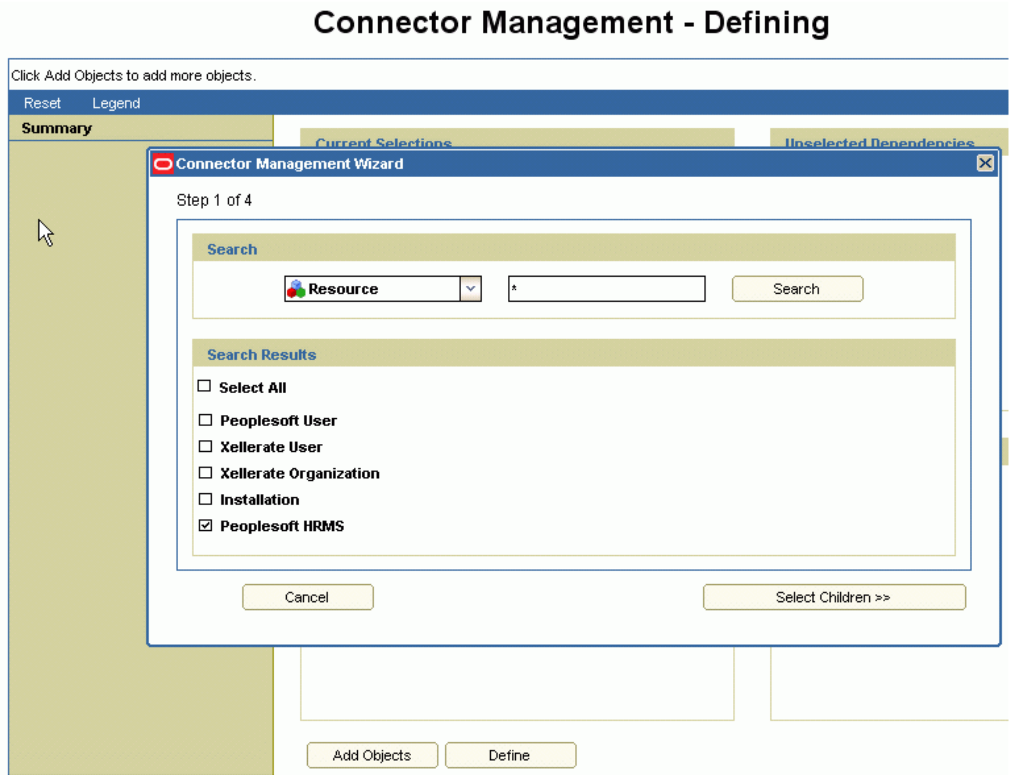
- It is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
- As a best practice, first perform the upgrade procedure in a test environment.

2.4.2 Re-defining the Connector

The upgrade process of the connector must not include IT resource. Therefore, you must re-define the connector to exclude IT resource.

To re-define the connector to exclude IT resource:

1. Add the Peoplesoft HRMS resource. To do so:
   a. Log in to the Administrative and User Console.
   b. On the Welcome to Identity Manager Advanced Administration page, under the System Management section, click **Manage Connector.**
   c. Click **Define.**
   d. In Step 1 of the Connector Management Wizard, select **Resource** from the drop-down box and search for `Peoplesoft HRMS`.
   e. In the Search Results region, select the Peoplesoft HRMS check box and click **Select Children,** as shown in the following screenshot.



Connector Management - Defining

Click Add Objects to add more objects.

Connector Management Wizard

Step 1 of 4

Search

Resource | * | Search

Search Results

☐ Select All

☐ Peoplesoft User

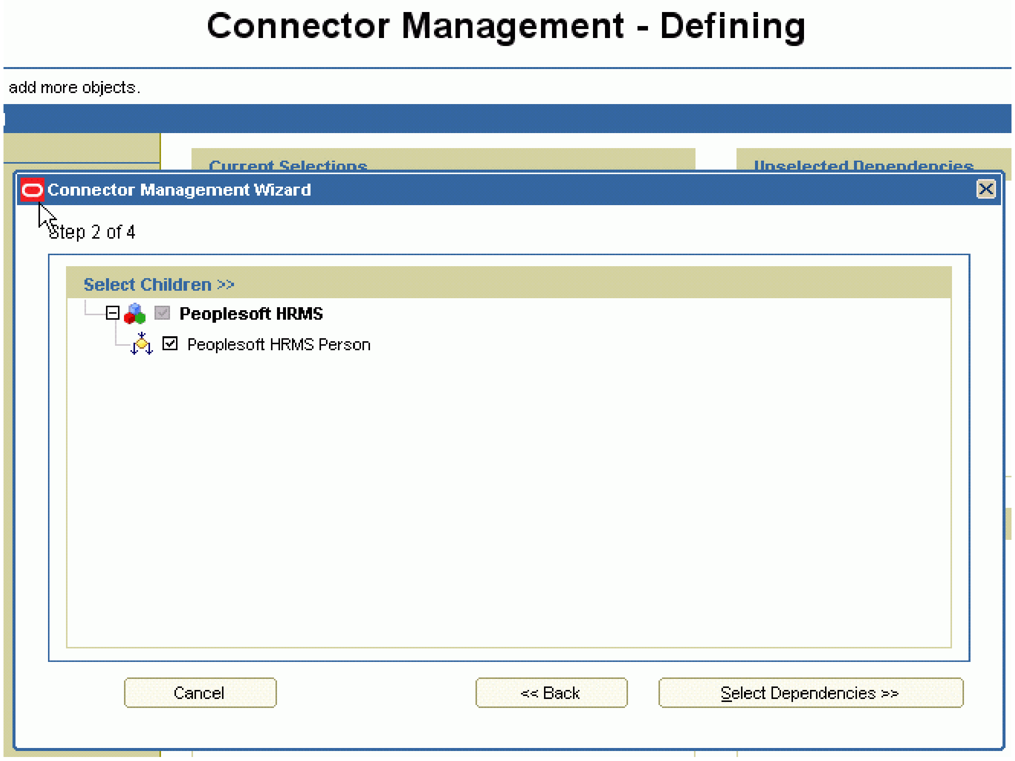
☐ Xellerate User

☐ Xellerate Organization

☐ Installation

☑ Peoplesoft HRMS

f. In Step 2, in the Select Children region, ensure the Peoplesoft HRMS Person check box is selected. Click **Select Dependencies,** as shown in the following screenshot.



Connector Management - Defining

add more objects.

Connector Management Wizard

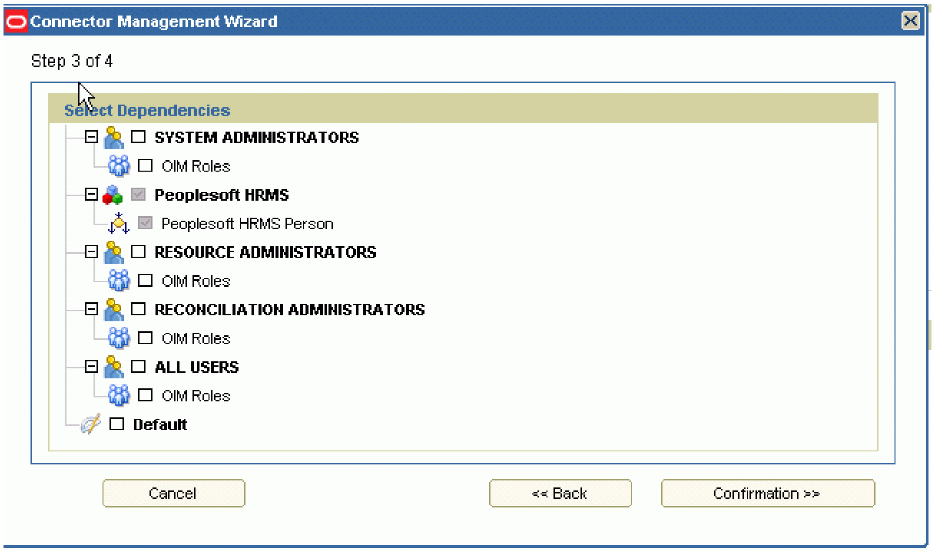
Step 2 of 4

Select Children >>

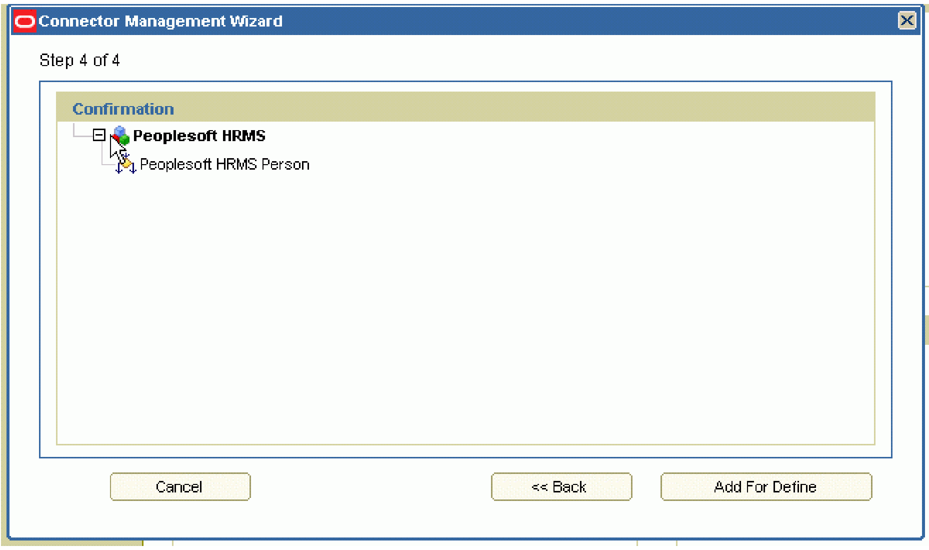
☑ Peoplesoft HRMS

☑ Peoplesoft HRMS Person

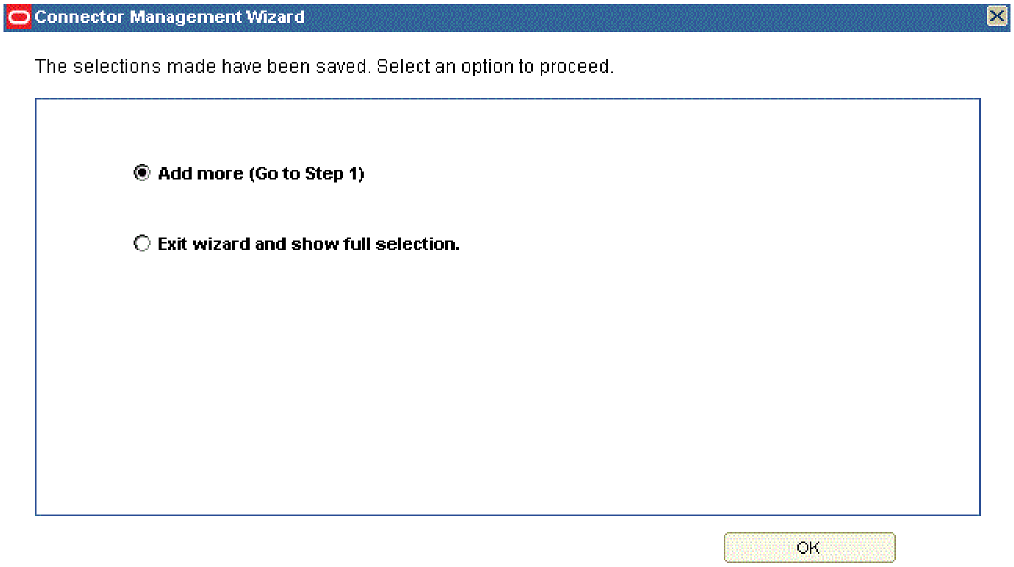
g. In Step 3, in the Select Dependencies region, ensure the Peoplesoft HRMS and the Peoplesoft HRMS Person check boxes are selected. Click **Confirmation,** as shown in the following screenshot.



h. In Step 4, click **Add For Define,** as shown in the following screenshot.



i. On the next page, select Add more (Go to Step 1) to add Peoplesoft HRMS scheduled tasks, and click OK, as shown in the following screenshot.



Connector Management Wizard

The selections made have been saved. Select an option to proceed.

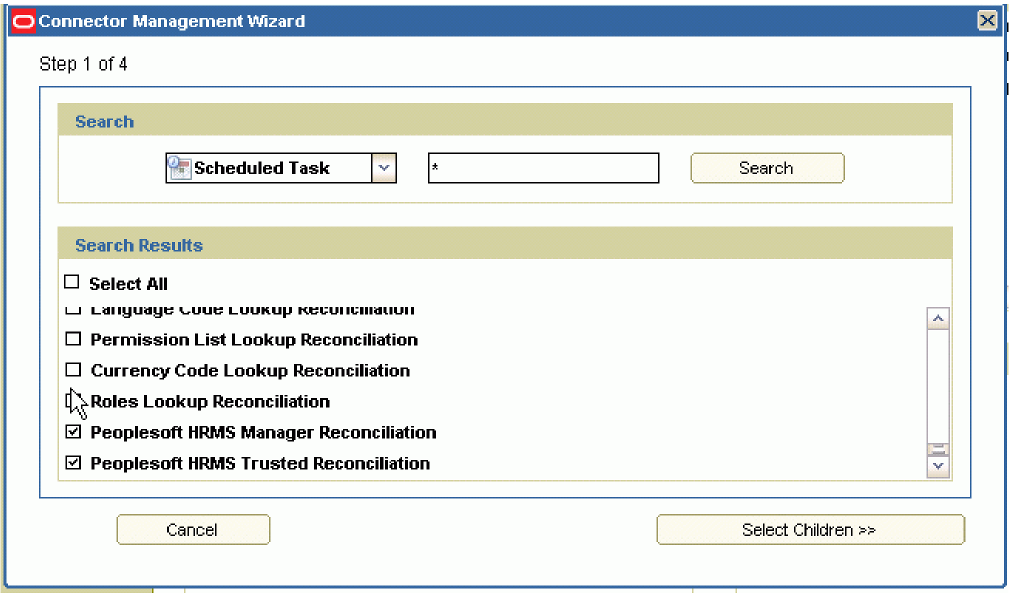
● Add more (Go to Step 1)

○ Exit wizard and show full selection.

2. Add the Peoplesoft HRMS scheduled tasks. To do so:

   a. In Step 1 of the Connector Management Wizard, select **Scheduled Task** from the drop-down box and search for the Peoplesoft HRMS tasks.

   b. In the Search Results region, select the Peoplesoft HRMS Manager Reconciliation and the Peoplesoft HRMS Trusted Reconciliation check boxes. Then, click **Select Children,** as shown in the following screenshot.



Connector Management Wizard

Step 1 of 4

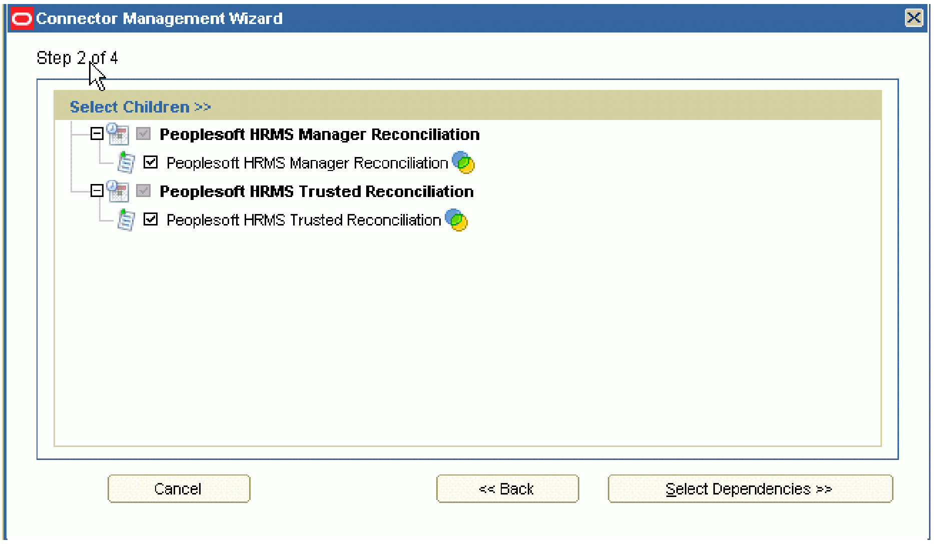
Search

Scheduled Task | *

Search Results

□ Select All
□ Language Code Lookup Reconciliation
□ Permission List Lookup Reconciliation
□ Currency Code Lookup Reconciliation
□ Roles Lookup Reconciliation
☑ Peoplesoft HRMS Manager Reconciliation
☑ Peoplesoft HRMS Trusted Reconciliation

   c. In Step 2, in the Select Children region, ensure the Peoplesoft HRMS scheduled tasks are selected, as shown in the following screenshot. Click **Select Dependencies.**

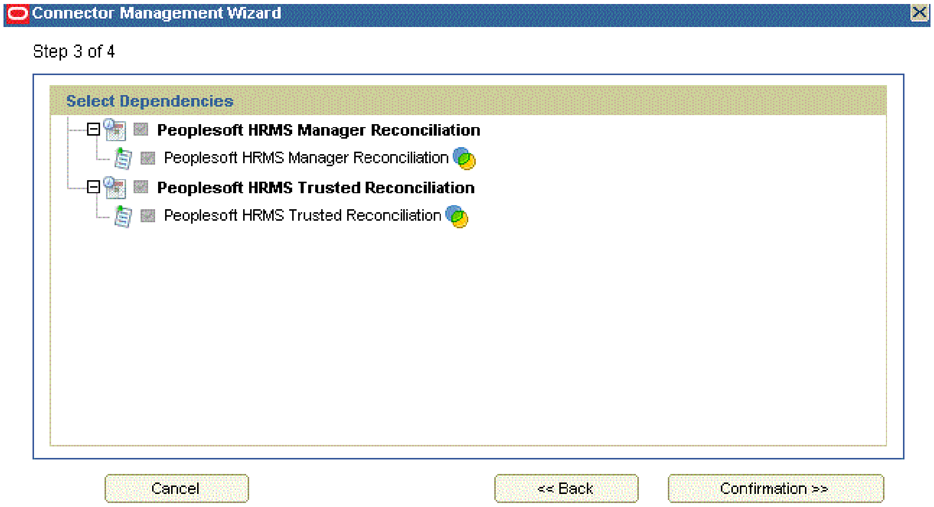


Step 2 of 4

Select Children >>

- ☑ **Peoplesoft HRMS Manager Reconciliation**
  - ☑ Peoplesoft HRMS Manager Reconciliation
- ☑ **Peoplesoft HRMS Trusted Reconciliation**
  - ☑ Peoplesoft HRMS Trusted Reconciliation

d. In Step 3, in the Select Dependencies region, ensure the Peoplesoft HRMS scheduled tasks are selected, as shown in the following screenshot. Click **Confirmation.**



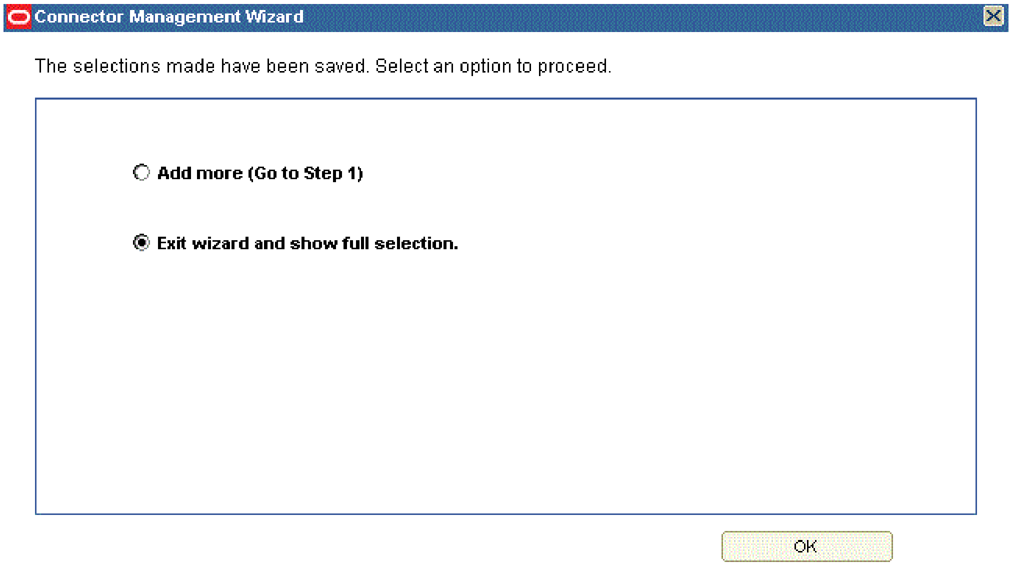
Step 3 of 4

Select Dependencies

- ☑ **Peoplesoft HRMS Manager Reconciliation**
  - ☑ Peoplesoft HRMS Manager Reconciliation
- ☑ **Peoplesoft HRMS Trusted Reconciliation**
  - ☑ Peoplesoft HRMS Trusted Reconciliation

e. In Step 4, click **Add For Define.**

f. On the next page, select Exit wizard and show full selection, and click OK, as shown in the following screenshot.



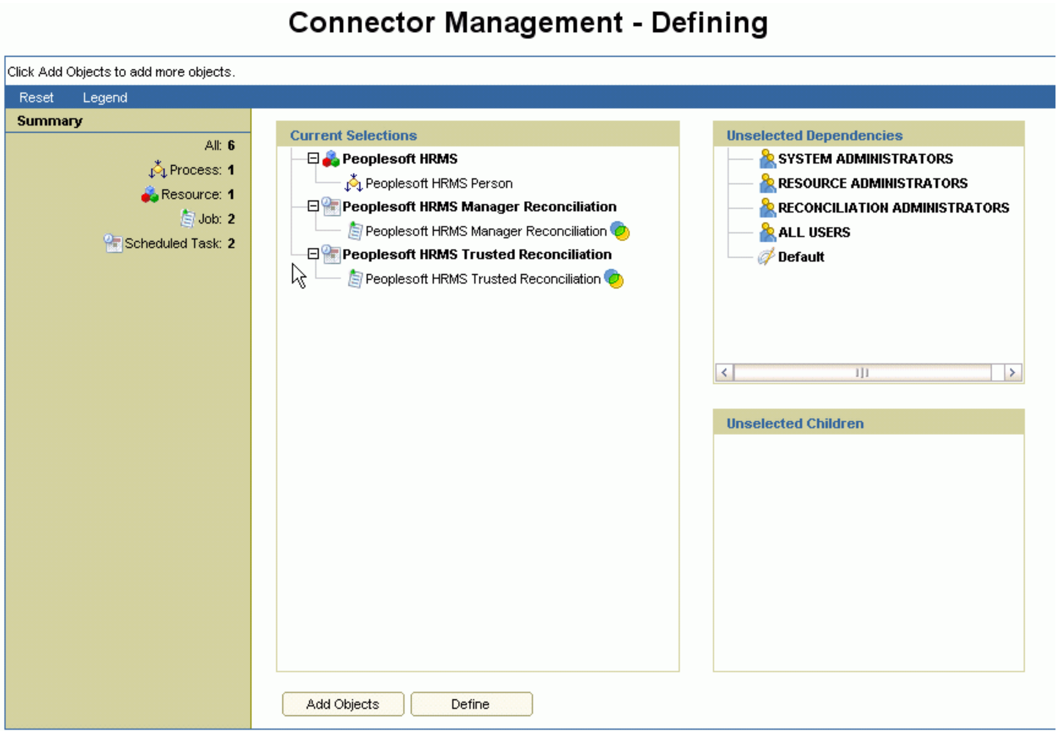
Connector Management Wizard

The selections made have been saved. Select an option to proceed.

○ Add more (Go to Step 1)

● Exit wizard and show full selection.

3. On the Summary page, verify the objects added in the preceding steps, as shown in the following screenshot. Then, click **Define.**



Connector Management - Defining

Click Add Objects to add more objects.

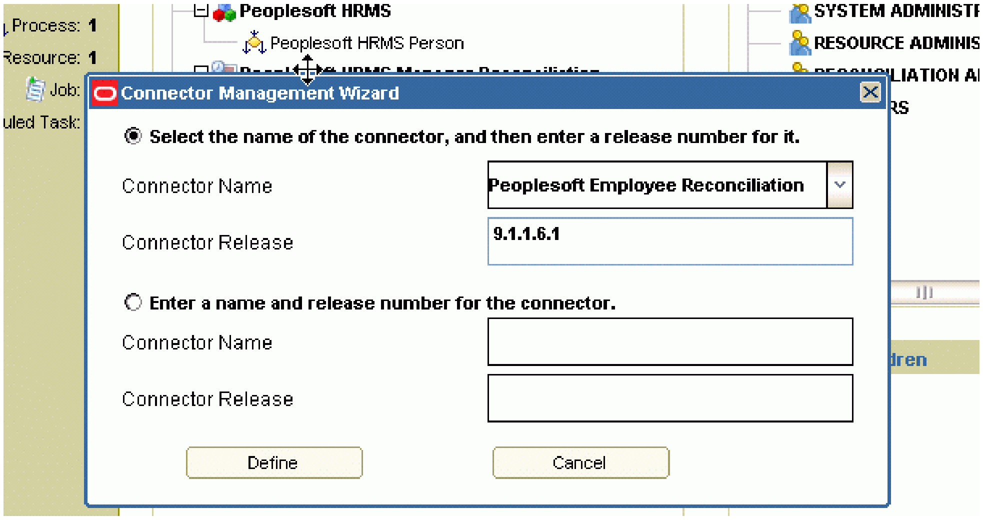
All: 6
Process: 1
Resource: 1
Job: 2
Scheduled Task: 2

Current Selections
- Peoplesoft HRMS
  - Peoplesoft HRMS Person
- Peoplesoft HRMS Manager Reconciliation
  - Peoplesoft HRMS Manager Reconciliation
- Peoplesoft HRMS Trusted Reconciliation
  - Peoplesoft HRMS Trusted Reconciliation

Unselected Dependencies
- SYSTEM ADMINISTRATORS
- RESOURCE ADMINISTRATORS
- RECONCILIATION ADMINISTRATORS
- ALL USERS
- Default

Unselected Children

4. Select Peoplesoft Employee Reconciliation in the Connector Name drop-down box, and enter a new version in the Connector Release field, as shown in the following sample screenshot. Then, click **Define.**



Connector Management Wizard

● Select the name of the connector, and then enter a release number for it.

Connector Name: Peoplesoft Employee Reconciliation

Connector Release: 9.1.1.6.1

○ Enter a name and release number for the connector.

Connector Name:

Connector Release:

2.4.3 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`:

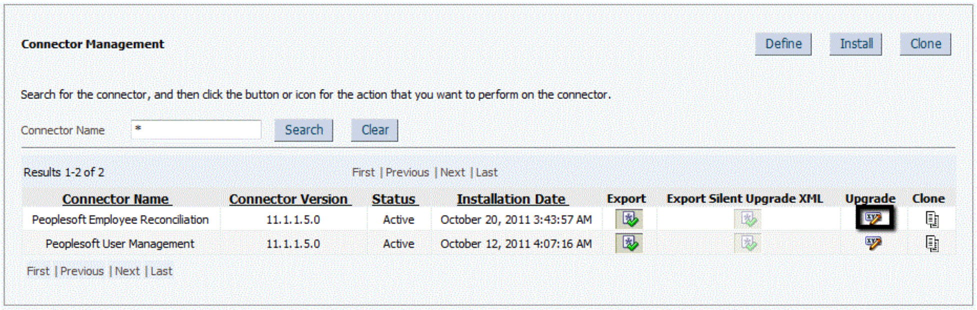
   OIM_HOME/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/xml/PeoplesoftHRMS-ConnectorConfig.xml

   The PeoplesoftHRMS-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 Employee Reconciliation connector and click the upgrade icon, as highlighted in the following screenshot.



Connector Management

Search for the connector, and then click the button or icon for the action that you want to perform on the connector.

Connector Name: *

Results 1-2 of 2

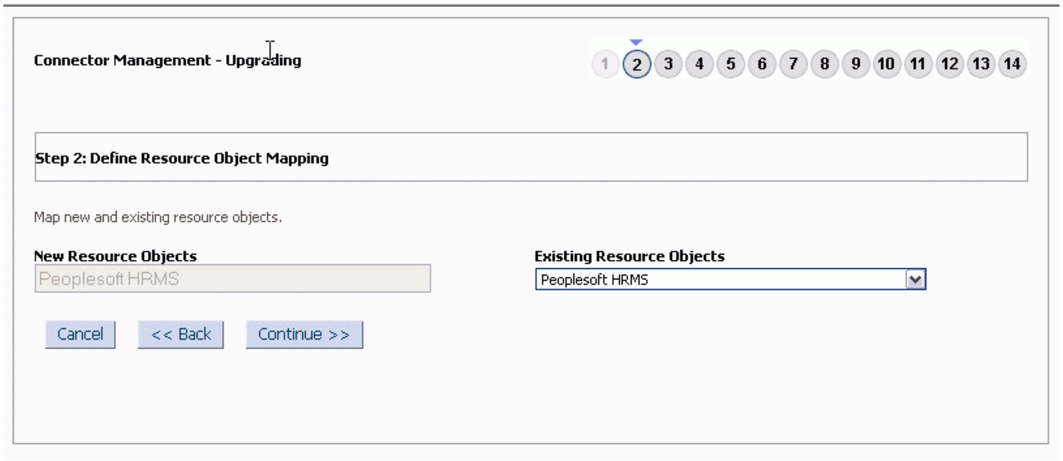
Connector Name	Connector Version	Status	Installation Date	Export	Export Silent Upgrade XML	Upgrade	Clone
Peoplesoft Employee Reconciliation	11.1.1.5.0	Active	October 20, 2011 3:43:57 AM				
Peoplesoft User Management	11.1.1.5.0	Active	October 12, 2011 4:07:16 AM				

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 PeoplesoftHRMS-ConnectorConfig.xml file created in Step 1.

   For example, `c:\tmp\PeoplesoftHRMS-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.**



Connector Management - Upgrading

Step 2: Define Resource Object Mapping

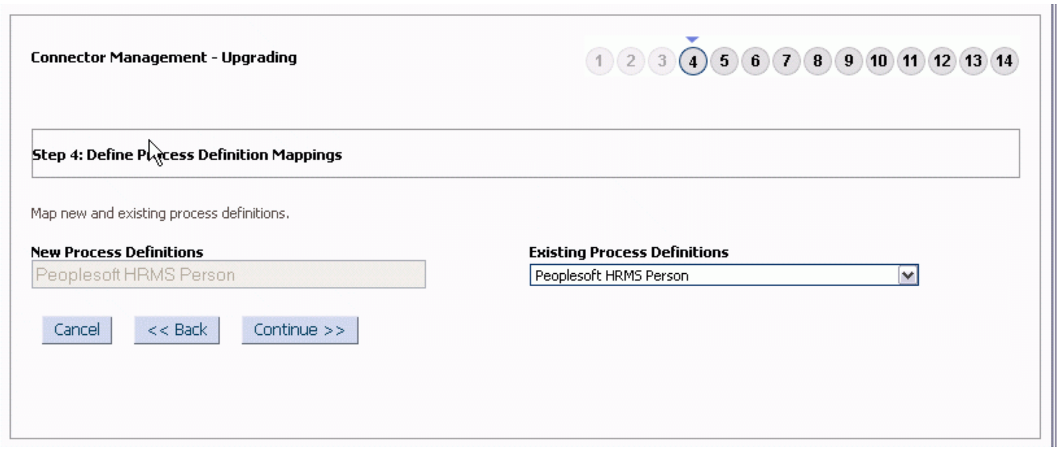
Map new and existing resource objects.

New Resource Objects: Peoplesoft HRMS

Existing Resource Objects: Peoplesoft HRMS

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 screenshot.



Connector Management - Upgrading

Step 4: Define Process Definition Mappings

Map new and existing process definitions.

New Process Definitions: Peoplesoft HRMS Person

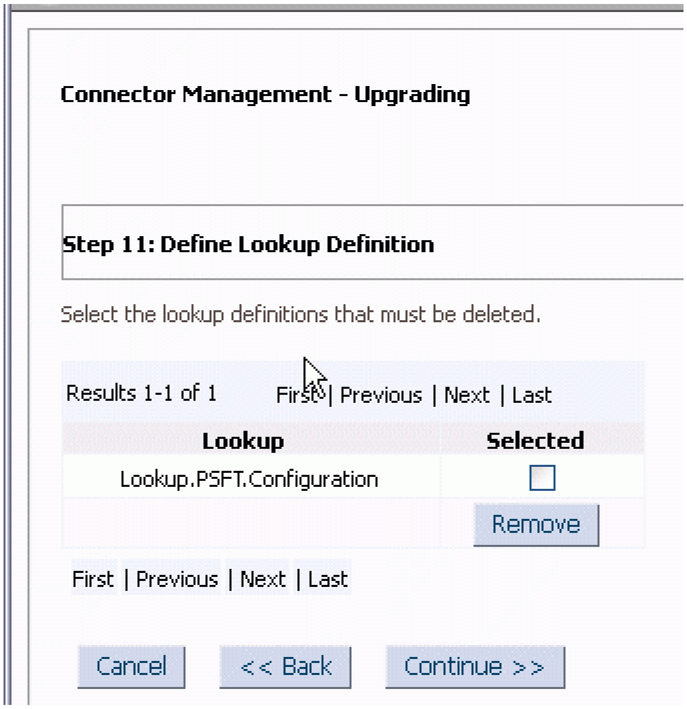
Existing Process Definitions: Peoplesoft HRMS Person

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.**

> **Note:**
>
> Steps 6 to 10 of the upgrade wizard require no changes and are skipped. This behavior is expected.

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



Connector Management - Upgrading

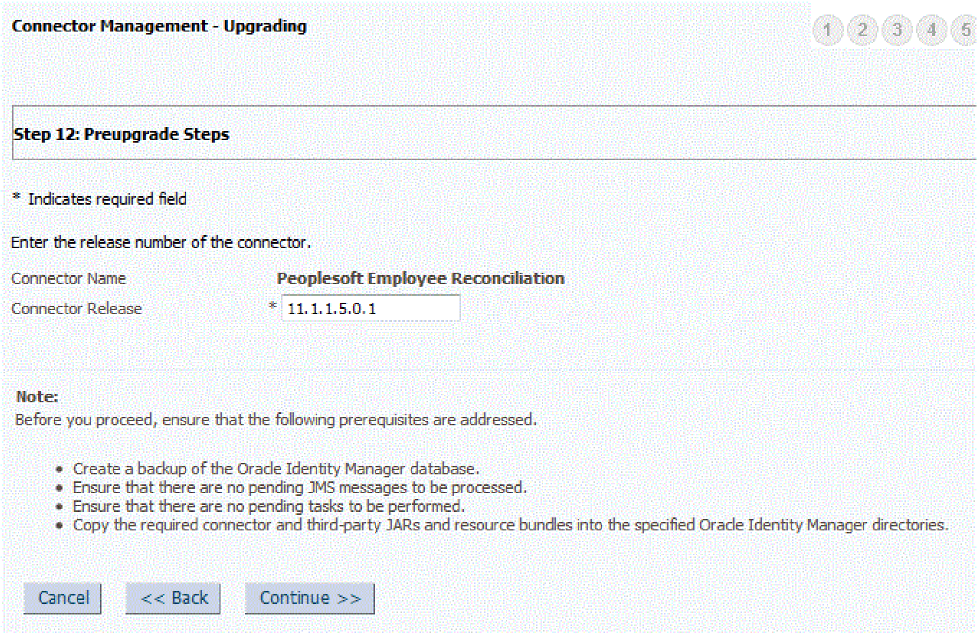
Step 11: Define Lookup Definition

Select the lookup definitions that must be deleted.

Results 1-1 of 1 First | Previous | Next | Last

Lookup	Selected
Lookup.PSFT.Configuration	□

11. 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.**



Connector Management - Upgrading

Step 12: Preupgrade Steps

* Indicates required field

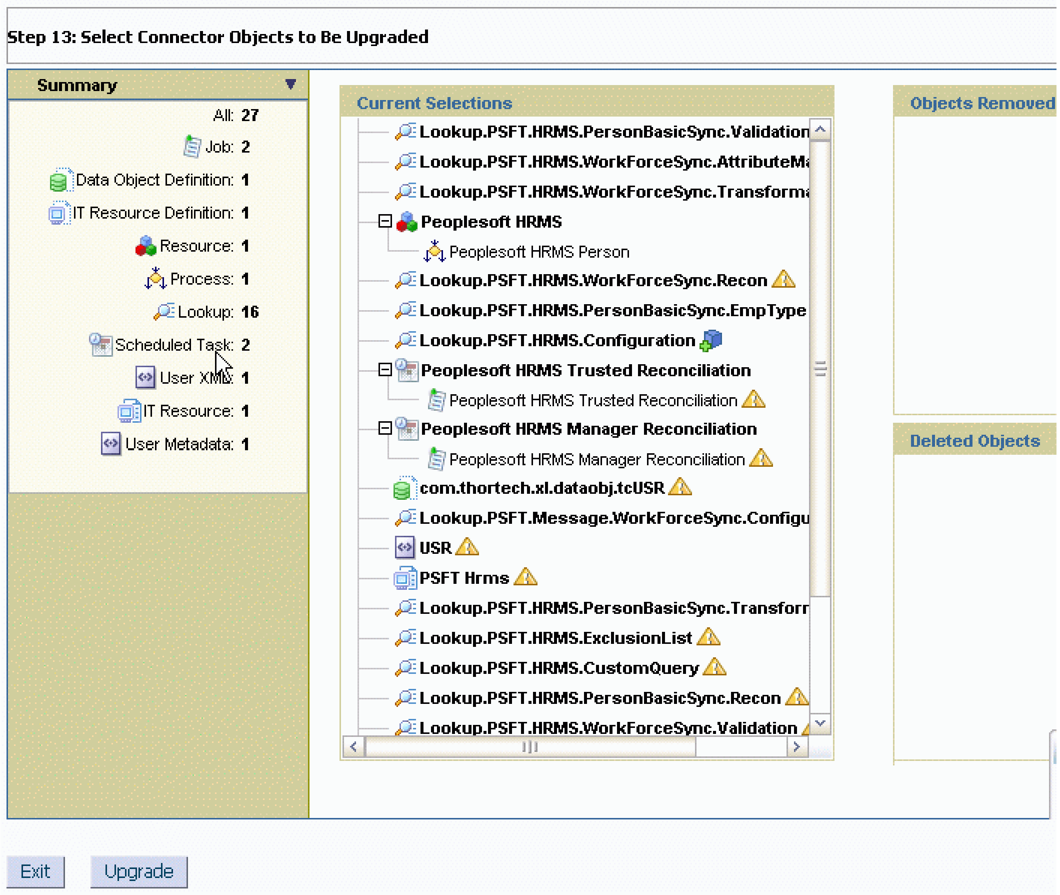
Enter the release number of the connector.

Connector Name	Peoplesoft Employee Reconciliation
Connector Release	* 11.1.1.5.0.1

Note:
Before you proceed, ensure that the following prerequisites are addressed.

- Create a backup of the Oracle Identity Manager database.
- Ensure that there are no pending JMS messages to be processed.
- Ensure that there are no pending tasks to be performed.
- Copy the required connector and third-party JARs and resource bundles into the specified Oracle Identity Manager directories.

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



Step 13: Select Connector Objects to Be Upgraded

Summary

All:	27
Job:	2
Data Object Definition:	1
IT Resource Definition:	1
Resource:	1
Process:	1
Lookup:	16
Scheduled Task:	2
User XML:	1
IT Resource:	1
User Metadata:	1

Current Selections

- Lookup.PSFT.HRMS.PersonBasicSync.Validation
- Lookup.PSFT.HRMS.WorkForceSync.AttributeMa
- Lookup.PSFT.HRMS.WorkForceSync.Transforma
- Peoplesoft HRMS
  - Peoplesoft HRMS Person
- Lookup.PSFT.HRMS.WorkForceSync.Recon
- Lookup.PSFT.HRMS.PersonBasicSync.EmpType
- Lookup.PSFT.HRMS.Configuration
- Peoplesoft HRMS Trusted Reconciliation
  - Peoplesoft HRMS Trusted Reconciliation
- Peoplesoft HRMS Manager Reconciliation
  - Peoplesoft HRMS Manager Reconciliation
- com.thortech.xl.dataobj.tcUSR
- Lookup.PSFT.Message.WorkForceSync.Configu
- USR
- PSFT Hrms
- Lookup.PSFT.HRMS.PersonBasicSync.Transforr
- Lookup.PSFT.HRMS.ExclusionList
- Lookup.PSFT.HRMS.CustomQuery
- Lookup.PSFT.HRMS.PersonBasicSync.Recon
- Lookup.PSFT.HRMS.WorkForceSync.Validation

13. 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. Then, click **Exit.**

2.4.4 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
PSFTER.jar	2 - ScheduledTask
PSFTCommon.jar	1 - JavaTasks
Common.jar Remove this file only if no other connector is using it.	1 - JavaTasks

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. 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 from the *OIM_HOME*/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/lib directory and indicate the JAR types as specified in the following table:

JAR File Name	JAR Type
PSFTCommon.jar Add this file only if it was not added while upgrading the PeopleSoft User Management connector.	2 - ScheduledTask
PSFT_ER-oim-integration.jar	2 - ScheduledTask

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

2.4.5 Upgrading the PeopleSoft Listener

> **Note:**
>
> - If you have already deployed a listener for the PeopleSoft User Management connector, then you can skip this procedure.
>
>   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 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 and Configuring Transformation of Data During Reconciliation for more information.

2.4.6 Upgrading the Customizations

To upgrade the connector customizations:

1. Update the validation customizations.

   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.
2. Update the transformation customizations

   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.
3. Update the entries in the connector configuration lookup, Lookup.PSFT.HRMS.Configuration.

See Lookup.PSFT.HRMS.Configuration for information about this step.

4. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then you must create a new UI form and attach it to an existing application instance so view the user-defined fields (UDFs or custom attributes).

   See Displaying UDFs in Oracle Identity Manager 11.1.2.x or Later for more information.

2.4.7 Updating the PeopleSoft Target System

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.

Configure a new node, for example, OIM_ER_NODE, and configure routings from the PERSON_BASIC_SYNC and WORKFORCE_SYNC service operations.

See Configuring the Target System for Full Reconciliation and Configuring the Target System for Full Reconciliation for more information.

2.4.8 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

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

- Summary of Steps to Use the Connector
- Performing Full Reconciliation
- Performing Incremental Reconciliation
- Limited Reconciliation
- Resending Messages That Are Not Received by the PeopleSoft Listener
- Configuring Scheduled Tasks

3.1 Summary of Steps to Use the Connector

The following is a summary of the steps to use the connector for full reconciliation:

> **Note:**
>
> It is assumed that you have performed all the procedures described in the preceding chapter.

1. Generate XML files for the PERSON_BASIC_FULLSYNC message for all persons. See Running the PERSON_BASIC_FULLSYNC Message for more information.
2. Generate XML files for the WORKFORCE_FULLSYNC message for the same set of persons. See Running the WORKFORCE_FULLSYNC Message for more information.

   > **Note:**
   >
   > The XML files that you generate in Steps 1 and 2 must reside in different directories.

3. Copy these XML files to a directory on the Oracle Identity Manager host computer.
4. Configure the Peoplesoft HRMS Trusted Reconciliation scheduled task for the PERSON_BASIC_FULLSYNC message. The XML files are read by this scheduled task to generate reconciliation events. See Configuring the Scheduled Task for Person Data Reconciliation for more information.
5. Configure the Peoplesoft HRMS Trusted Reconciliation scheduled task for the WORKFORCE_FULLSYNC message. The XML files are read by this scheduled task to generate reconciliation events. See Configuring the Scheduled Task for Person Data Reconciliation for more information.

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

3.2 Performing Full Reconciliation

Full reconciliation involves reconciling all existing person records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

The following sections discuss the procedures involved in full reconciliation:

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

3.2.1 Generating XML Files

You must generate XML files for all existing persons in the target system.

> **Note:**
>
> Before performing the procedure to generate XML files, you must ensure that you have configured the PERSON_BASIC_FULLSYNC and WORKFORCE_FULLSYNC messages. See Importing XML Files into Oracle Identity Manager for more information.

To generate XML files for full reconciliation perform the procedures described in the following topics:

> **Note:**
>
> If you are using PeopleTools 8.50 and HCM 9.0, then before running Full Data Publish, you must apply the patch that addresses Bug 824529. This patch can be downloaded from Oracle Metalink.

- Running the PERSON_BASIC_FULLSYNC Message
- Running the WORKFORCE_FULLSYNC Message

3.2.1.1 Running the PERSON_BASIC_FULLSYNC Message

To run the PERSON_BASIC_FULLSYNC 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:

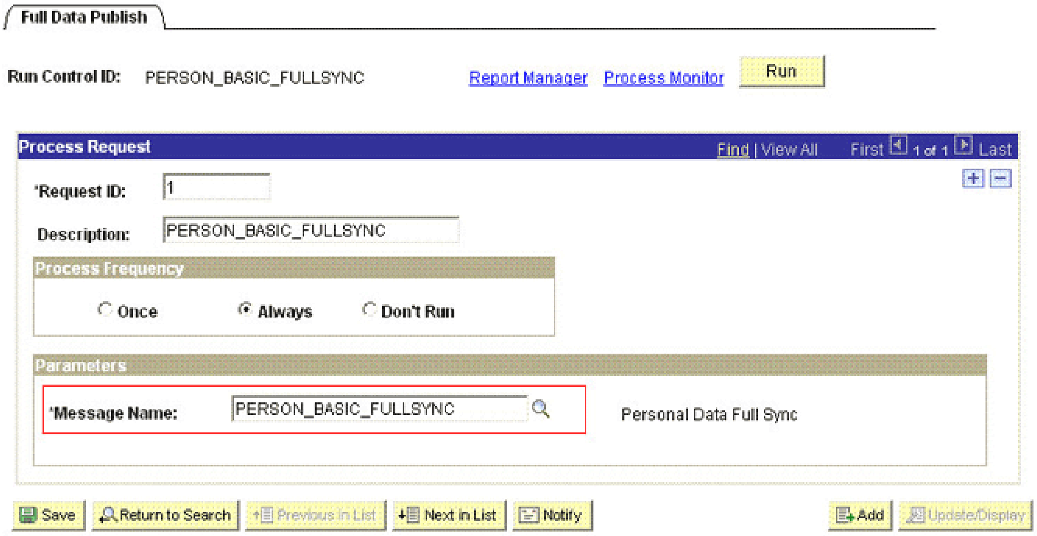
Request ID: Enter a request ID.

Description: Enter a description for the process request.

Process Frequency: Select **Always.**

Message Name: Select **PERSON_BASIC_FULLSYNC.**

The following screenshot displays the preceding steps:



Run Control ID: PERSON_BASIC_FULLSYNC

Process Request

*Request ID: 1

Description: PERSON_BASIC_FULLSYNC

Process Frequency

○ Once ● Always ○ Don't Run

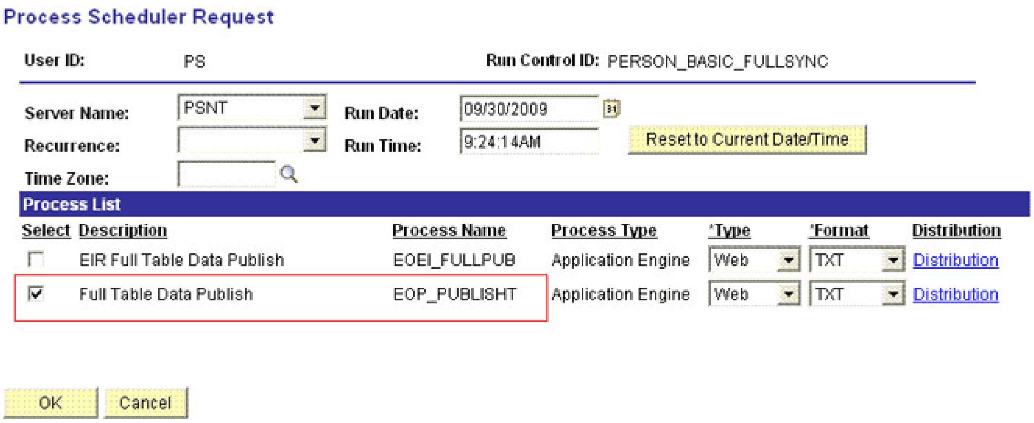
Parameters

*Message Name: PERSON_BASIC_FULLSYNC Personal Data Full Sync

5. Click **Save** to save the configuration.
6. Click **Run.**

   The Process Scheduler Request page appears.
7. From the **Server Name** list, select the appropriate server.
8. Select **Full Table Data Publish** process list, and click **OK.**

   The following screenshot displays the process list:



Process Scheduler Request

User ID: PS Run Control ID: PERSON_BASIC_FULLSYNC

Server Name: PSNT Run Date: 09/30/2009

Recurrence: Run Time: 9:24:14AM

Time Zone:

Process List

Select	Description	Process Name	Process Type	*Type	*Format	Distribution
☐	EIR Full Table Data Publish	EOEI_FULLPUB	Application Engine	Web	TXT	Distribution
☑	Full Table Data Publish	EOP_PUBLISHT	Application Engine	Web	TXT	Distribution

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 PERSON_BASIC_FULLSYNC message are generated at a location that you specified in the FilePath property while creating the OIM_FILE_NODE node for PeopleSoft Web Server. See Configuring the PeopleSoft Integration Broker on page 2-19 section for more information.

Copy these XML files to a directory 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 PERSON_BASIC_FULLSYNC Service Operation on page 2-23 section. This is for security purposes.

3.2.1.2 Running the WORKFORCE_FULLSYNC Message

To run the WORKFORCE_FULLSYNC 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:

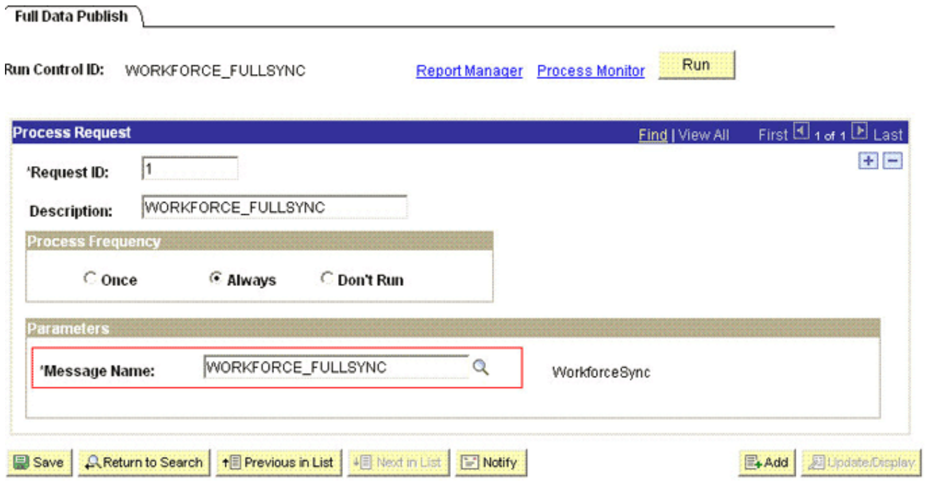
   Request ID: Enter a request ID.

   Description: Enter a description for the process request.

   Process Frequency: Select **Always.**

   Message Name: Select **WORKFORCE_FULLSYNC.**

   The following screenshot displays the preceding steps:



Full Data Publish

Run Control ID: WORKFORCE_FULLSYNC

Process Request

*Request ID: 1

Description: WORKFORCE_FULLSYNC

Process Frequency

○ Once ● Always ○ Don't Run

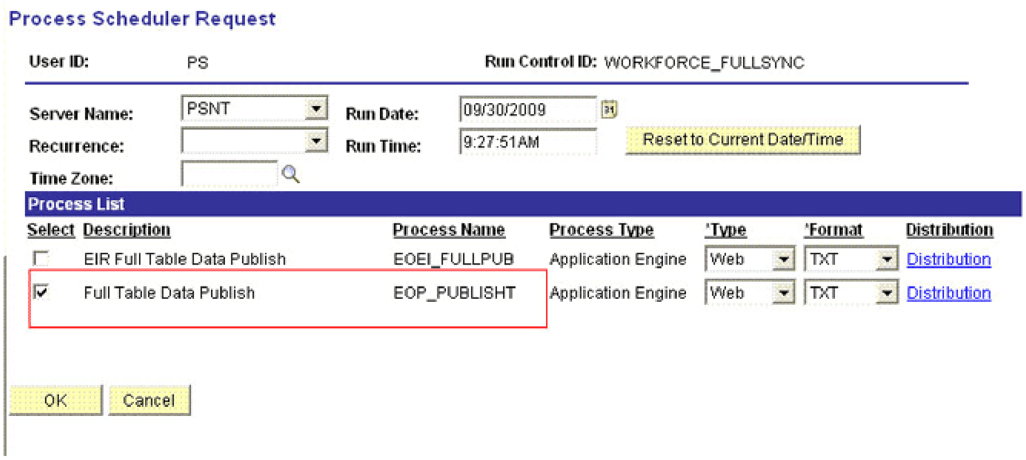
Parameters

*Message Name: WORKFORCE_FULLSYNC WorkforceSync

5. Click **Save** to save the configuration.
6. Click **Run.**

   The Process Scheduler Request page appears.
7. From the **Server Name** list, select the appropriate server.
8. Select the **Full Table Data Publish** process list, and click **OK.**

   The following screenshot displays the process list:



Process Scheduler Request

User ID: PS   Run Control ID: WORKFORCE_FULLSYNC

Server Name: PSNT   Run Date: 09/30/2009

Recurrence: Run Time: 9:27:51AM

Time Zone:

Process List

Select	Description	Process Name	Process Type	*Type	*Format	Distribution
☐	EIR Full Table Data Publish	EOEI_FULLPUB	Application Engine	Web	TXT	Distribution
☑	Full Table Data Publish	EOP_PUBLISHT	Application Engine	Web	TXT	Distribution

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 WORKFORCE_FULLSYNC message are generated at a location that you specified in the FilePath property while creating the OIM_FILE_NODE node for PeopleSoft Web Server. See"Configuring the PeopleSoft Integration Broker" section for more information.

   You must copy these XML files to a directory on the Oracle Identity Manager host computer.

> **Note:**
>
> After you have performed this procedure, remove the permission list created in "Setting Up the Security for the WORKFORCE_FULLSYNC Service Operation" section. This is for security purposes.

3.2.2 Importing XML Files into Oracle Identity Manager

Configuring the Scheduled Task for Person Data Reconciliation section describes the procedure to configure the scheduled task.

Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task describes the procedure to configure the scheduled task for reconciliation of Manager ID values.

3.2.2.1 Configuring the Scheduled Task for Person Data Reconciliation

When you run the Connector Installer, the PeopleSoft HRMS Trusted Reconciliation scheduled task is automatically created in Oracle Identity Manager.

To perform a full reconciliation run, you must configure the scheduled task to reconcile all person data into Oracle Identity Manager depending on the values that you specified in the scheduled task attributes. Table 3-1 describes the attributes of this scheduled task. See Configuring Scheduled Tasks for instructions on running the scheduled task.

> **Note:**
>
> Before you configure the scheduled task, you must ensure that the mapping for all Actions to be performed on the target system is defined in the Lookup.PSFT.HRMS.WorkForceSync.EmpStatus lookup definition. See Lookup.PSFT.HRMS.WorkForceSync.EmpStatus for more information.

The Peoplesoft HRMS Trusted Reconciliation scheduled task is used to transfer XML file data from the file to the parser. The parser then converts this data into reconciliation events.

Table 3-1 Attributes of the Peoplesoft HRMS Trusted Reconciliation Scheduled Task

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`, the XML file is not archived.
Archive Path	Enter the full path and name of the directory in which you want XML files used during full reconciliation to be archived. You must enter a value for the Archive Path attribute only if you specify `yes` as the value for the Archive Mode attribute. Sample value: `/usr/archive`
File Path	Enter the path of the directory on the Oracle Identity Manager host computer into which you copy 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 Configuring the IT Resource. Default value: `PSFT HRMS`
Message Name	Use this attribute to specify the name of the delivered message used for full reconciliation. Sample value: `PERSON_BASIC_FULLSYNC or WORKFORCE_FULLSYNC`
Task Name	This attribute holds the name of the scheduled task. Value: `Peoplesoft HRMS Trusted Reconciliation`

In Oracle Identity Manager release 11.1.2.*x* or later, some user attributes (UDFs) such as Department are not displayed after running the reconciliation for the WORKFORCE_FULLSYNC message. To display these attributes as form fields in the

Oracle Identity Manager user interface, see Displaying UDFs in Oracle Identity Manager 11.1.2.x or Later.

3.2.2.2 Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task

Manager ID values are not reconciled during full reconciliation run.

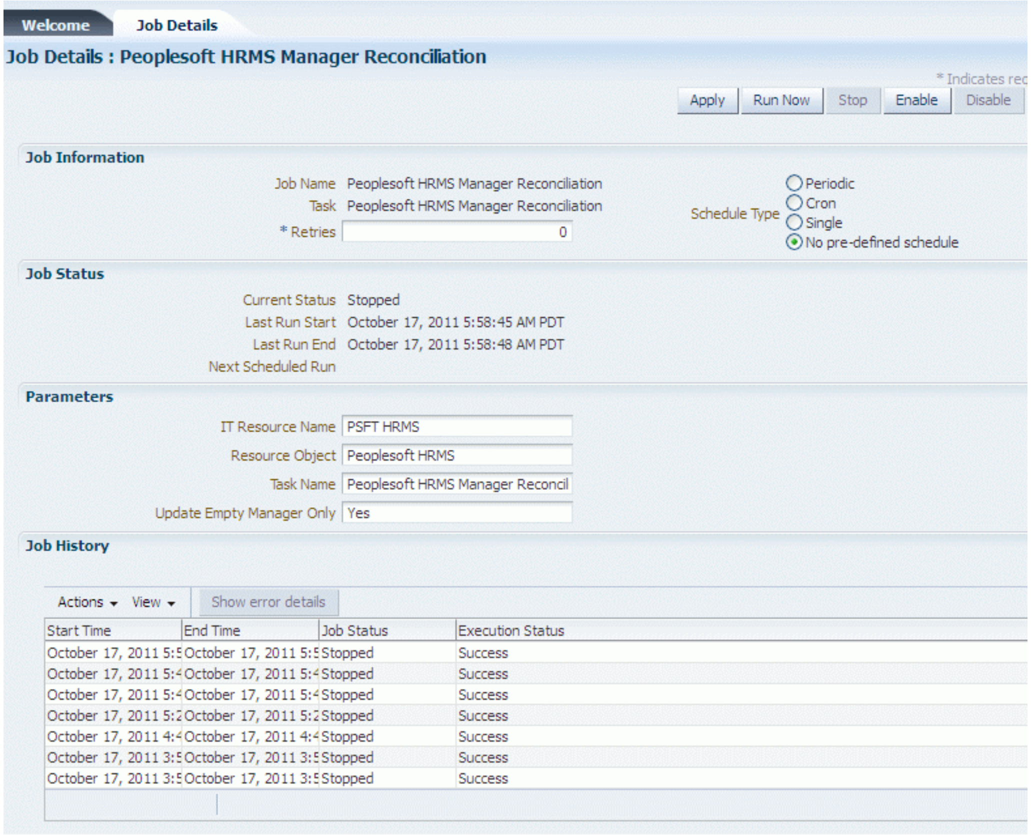
You must configure and run the PeopleSoft HRMS Manager Reconciliation scheduled task. Table 3-2 describes the attributes of this scheduled task.

Table 3-2 Attributes of the PeopleSoft HRMS Manager Reconciliation Scheduled Task

Attribute	Description
IT Resource Name	Enter the name of the IT resource. Default value: `PSFT HRMS`
Resource Object	Enter the name of the resource object. Default value: `Peoplesoft HRMS`
Task Name	This attribute holds the name of the scheduled task. Default value: `Peoplesoft HRMS Manager Reconciliation`
Update Empty Manager Only	Set this value to `Yes` to update empty Manager ID of a Person. Default value: `No`

Before you run this scheduled task, you must specify a value for the Update Empty Manager Only attribute.

The attributes of the PeopleSoft HRMS Manager Reconciliation scheduled task are shown in the following screenshot:



Job Details : Peoplesoft HRMS Manager Reconciliation

Job Information

Job Name Peoplesoft HRMS Manager Reconciliation
Task Peoplesoft HRMS Manager Reconciliation
* Retries 0

Schedule Type ○ Periodic ○ Cron ○ Single ● No pre-defined schedule

Job Status

Current Status Stopped
Last Run Start October 17, 2011 5:58:45 AM PDT
Last Run End October 17, 2011 5:58:48 AM PDT
Next Scheduled Run

Parameters

IT Resource Name PSFT HRMS
Resource Object Peoplesoft HRMS
Task Name Peoplesoft HRMS Manager Reconcil
Update Empty Manager Only Yes

Job History

Start Time	End Time	Job Status	Execution Status
October 17, 2011 5:5	October 17, 2011 5:5	Stopped	Success
October 17, 2011 5:4	October 17, 2011 5:4	Stopped	Success
October 17, 2011 5:4	October 17, 2011 5:4	Stopped	Success
October 17, 2011 5:2	October 17, 2011 5:2	Stopped	Success
October 17, 2011 4:4	October 17, 2011 4:4	Stopped	Success
October 17, 2011 3:5	October 17, 2011 3:5	Stopped	Success
October 17, 2011 3:5	October 17, 2011 3:5	Stopped	Success

- Enter `yes` if you want the scheduled task to populate Manager ID values in OIM User records that do not have this value. Existing Manager ID values in other OIM User records are not modified.
- Enter `no` if you want the scheduled task to fetch and populate Manager ID values for all OIM User records, regardless of whether the Manager ID attribute in these records currently contains a value.

This scheduled task uses the Lookup.PSFT.HRMS.ManagerRecon.Configuration lookup definition to read the values required to run the task. If you want to modify this scheduled task, for example, when the Employee ID field is mapped to a UDF, then you must modify the values in this lookup as per the changes made to the task. See Lookup.PSFT.HRMS.ManagerRecon.Configuration for information about this lookup.

When it is run, this scheduled task performs the process described inSteps in the Manager ID Reconciliation Process

3.3 Performing Incremental Reconciliation

You do not require additional configuration for incremental reconciliation.

It is assumed that you have deployed the PeopleSoft listener as described in Deploying the PeopleSoft Listener.

> **Note:**
>
> You must ensure that you have defined the mapping for all Actions to be performed on the target system in the Lookup.PSFT.HRMS.WorkForceSync.EmpStatus lookup definition. See Lookup.PSFT.HRMS.WorkForceSync.EmpStatus for more information.

3.4 Limited Reconciliation

This section contains the following topics:

- About Limited Reconciliation
- Configuring Limited Reconciliation

3.4.1 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 configure segment filtering to specify the attributes whose values you want to fetch into Oracle Identity Manager. Similarly, 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 in the message-specific configuration lookup.

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:

```
Last Name=Doe
```

With this query condition, only records for persons whose last name is Doe 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 persons whose first name is John and last name is Doe:

```
First Name=John  & Last Name=Doe
```

You can limit reconciliation to the records of those persons whose first name is either John or their User ID is 219786 using the following query:

```
First Name=John | User ID=219786
```

3.4.2 Configuring Limited Reconciliation

To configure limited reconciliation:

1. Ensure that the OIM User attribute to use in the query exists in the Lookup.PSFT.HRMS.CustomQuery lookup definition. This lookup definition maps the resource object attributes with OIM User form fields.

   > **See Also:**
   >
   > Lookup.PSFT.HRMS.CustomQuery for a listing of the default contents of this lookup definition

   You must add a new row in this lookup definition whenever you add a new UDF in the process form. See Setting Up the Lookup.PSFT.HRMS.CustomQuery Lookup Definition for adding an entry in this lookup definition and Adding New Attributes for Incremental Reconciliation for adding a UDF.

2. 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 used in the query condition. For example:

     ```
     First Name=John & Last Name=Doe
     ```

     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:

     ```
     First Name=John & Last Name=Doe
     ```

     ```
     First Name= John & Last Name= Doe
     ```

     In the second query condition, the reconciliation engine would look for first name and last name 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 values in the Lookup.PSFT.HRMS.CustomQuery lookup definitions. For example, the following query condition would fail:

     fiRst Name = John

3. 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 PERSON_BASIC_FULLSYNC message, search and open the **Lookup.PSFT.Message.PersonBasicSync.Configuration** lookup. Specify the query condition in the Decode column of the **Custom Query** attribute.

3.5 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 or not. Reconciliation events are not created for the messages that are sent to Oracle Identity Manager while the WAR file is unavailable. To ensure that all the messages generated on the target system reach Oracle Identity Manager, perform the following procedure:

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 queue. When you check the details of a specific message, the status is listed as `Timeout` or `Error`.

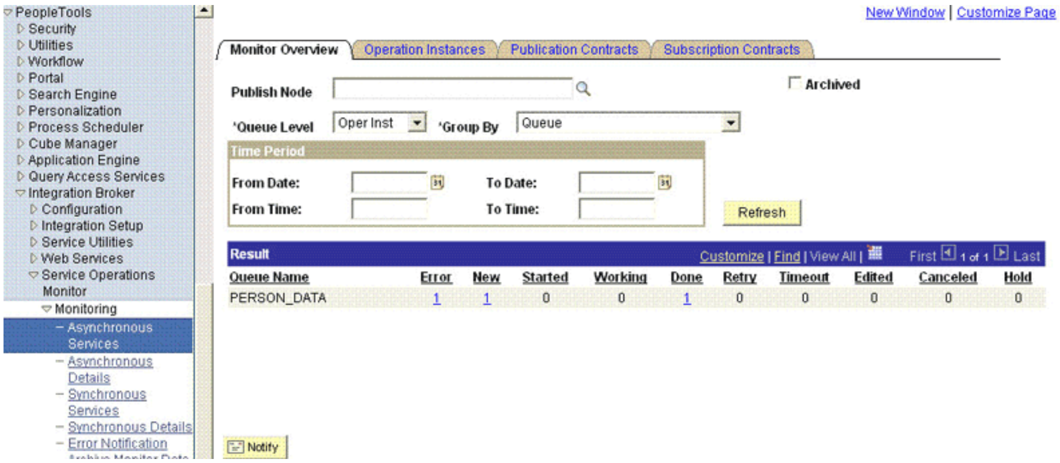
To publish a message in the queue to Oracle Identity Manager, resubmit the message when Oracle Identity Manager is running.

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 created in Creating a Role for a Limited Rights User. But, you can specify persons who have rights to perform this task based on the security policy of your organization.

To manually resend messages in Error or TimeOut status:

1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Service Operations Monitor, Monitoring,** and then click **Asynchronous Services.**
2. From the Group By list, select **Service Operation** or **Queue** to view the number of messages in Error, TimeOut, Done, and so on.



Publish Node
□ Archived

*Queue Level: Oper Inst
*Group By: Queue

Time Period
From Date:
To Date:
From Time:
To Time:

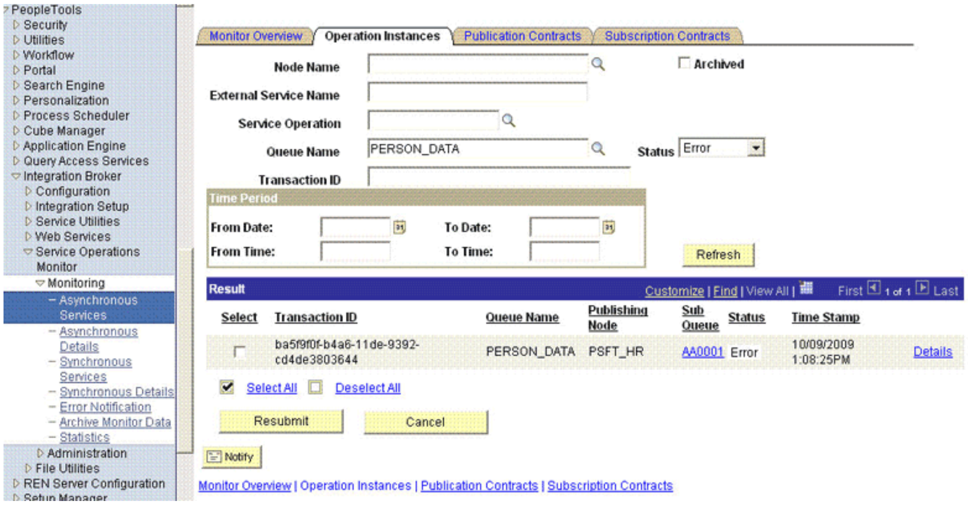
Result

Queue Name	Error	New	Started	Working	Done	Retry	Timeout	Edited	Canceled	Hold
PERSON_DATA	1	1	0	0	1	0	0	0	0	0

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.



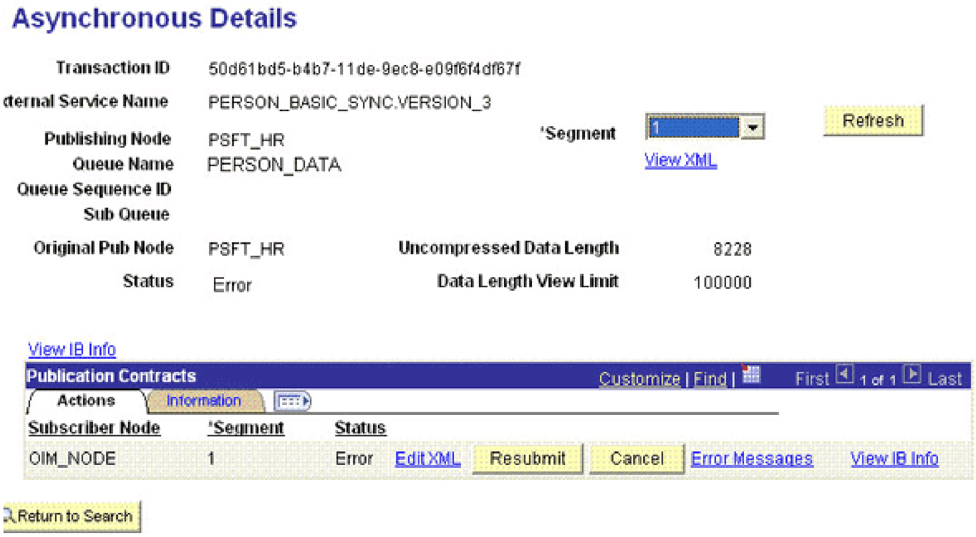
Node Name ☐ Archived
External Service Name
Service Operation
Queue Name PERSON_DATA Status Error
Transaction ID

Time Period
From Date: To Date:
From Time: To Time:

Result

Select	Transaction ID	Queue Name	Publishing Node	Sub Queue	Status	Time Stamp	
☐	ba5f9f0f-b4a6-11de-9392-cd4de3803644	PERSON_DATA	PSFT_HR	AA0001	Error	10/09/2009 1:08:25PM	Details

4. Click the **Details** link of the message to be resent. A new window appears.



Asynchronous Details

Transaction ID 50d61bd5-b4b7-11de-9ec8-e09f6f4df67f
xternal Service Name PERSON_BASIC_SYNC.VERSION_3
Publishing Node PSFT_HR
Queue Name PERSON_DATA
Queue Sequence ID
Sub Queue
*Segment 1
Original Pub Node PSFT_HR
Status Error
Uncompressed Data Length 8228
Data Length View Limit 100000

Publication Contracts

Subscriber Node	*Segment	Status					
OIM_NODE	1	Error	Edit XML	Resubmit	Cancel	Error Messages	View IB Info

5. Click the **Error Messages** link to check the error description.

6. Click **Resubmit** after you have resolved the issue.

3.6 Configuring Scheduled Tasks

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

This section contains the following topics:

- Scheduled Tasks for Reconciliation
- Configuring a Scheduled Task

3.6.1 Scheduled Tasks for Reconciliation

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

Table 3-3 Scheduled Tasks for Reconciliation

Scheduled Task	Description
PeopleSoft HRMS Trusted Reconciliation	This scheduled task is used during full reconciliation. It parses the contents of the XML files and then creates reconciliation events for each record. See Configuring the Scheduled Task for Person Data Reconciliation for information about this scheduled task.
PeopleSoft HRMS Manager Reconciliation	This scheduled task is used for reconciling Manager ID values during full reconciliation. See Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task for information about this scheduled task.

3.6.2 Configuring a Scheduled Task

To configure a scheduled task:

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 task. To do so:

   - On the Job Details tab, under the Parameters section, specify values for the attributes of the scheduled task. See Table 3-1 for more information about the attributes of the scheduled task.

> **Note:**
>
> - Attribute values are predefined in the connector XML that is imported during the installation of the connector. Specify values only for the attributes to change.
> - If you want to stop a scheduled task while it is running, the process is terminated only after the complete processing of the file that is being run. For instance, you want to reconcile data from five XML files. But, if you stop the scheduled task when it is reconciling data from the third file, then the reconciliation will stop only after processing the third file completely.

5. After specifying the attributes, 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 task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

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 Full Reconciliation
- Adding New Attributes for Incremental Reconciliation
- Modifying Field Lengths on the OIM User Form
- Configuring Validation of Data During Reconciliation
- Configuring Transformation of Data During Reconciliation
- Setting Up the Lookup.PSFT.HRMS.CustomQuery Lookup Definition
- Setting Up the Lookup.PSFT.HRMS.WorkForceSync.EmpStatus Lookup Definition
- Configuring the Connector for Multiple Installations of the Target System

4.1 Adding New Attributes for Full Reconciliation

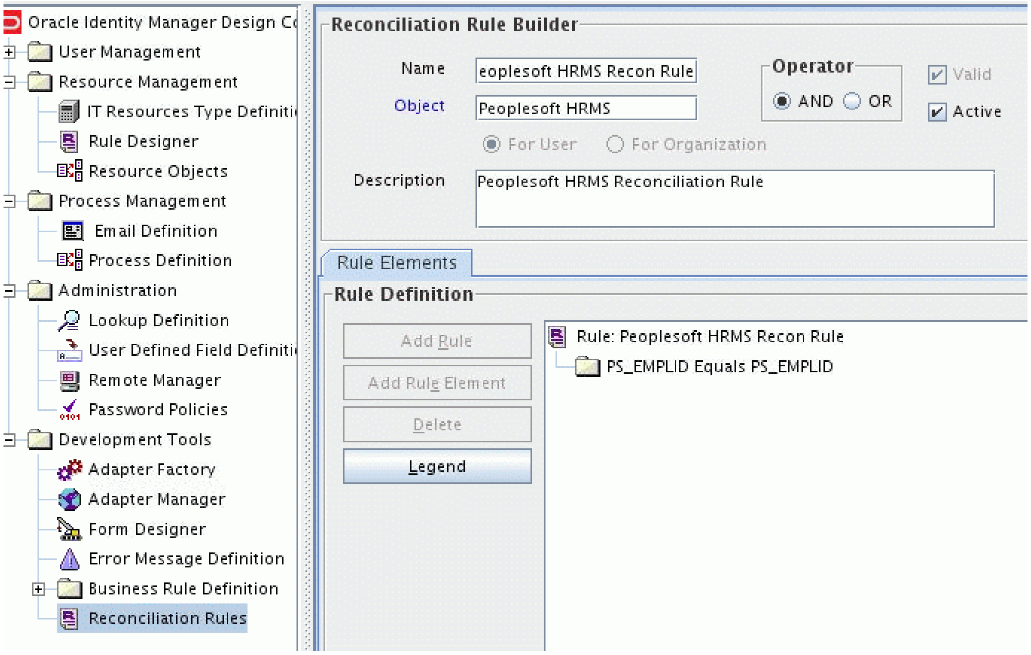
This section contains the following topics:

- About New Attributes for Full Reconciliation
- Adding New Attributes for Full Reconciliation

4.1.1 About New Attributes for Full Reconciliation

You can modify the default field mappings between Oracle Identity Manager and the PeopleSoft target system. For example, the Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping lookup definition for the PERSON_BASIC_FULLSYNC message holds the default attribute mappings. If required, you can add to this predefined set of attribute mappings.

By default, the Employee ID field in the target system is mapped to the User Login field in Oracle Identity Manager. Suppose you change this mapping, for example, Employee ID is mapped to PS_EMPLID. To match profiles based on this field, you must also change the reconciliation rule before creating a new reconciliation profile. For the described example, see the following screenshot of the sample reconciliation:



Reconciliation Rule Builder

Name: eoplesoft HRMS Recon Rule

Object: Peoplesoft HRMS

Operator: ● AND ○ OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: Peoplesoft HRMS Reconciliation Rule

Rule Definition

Rule: Peoplesoft HRMS Recon Rule
PS_EMPLID Equals PS_EMPLID

4.1.2 Adding New Attributes for Full Reconciliation

To add a new attribute for full reconciliation:

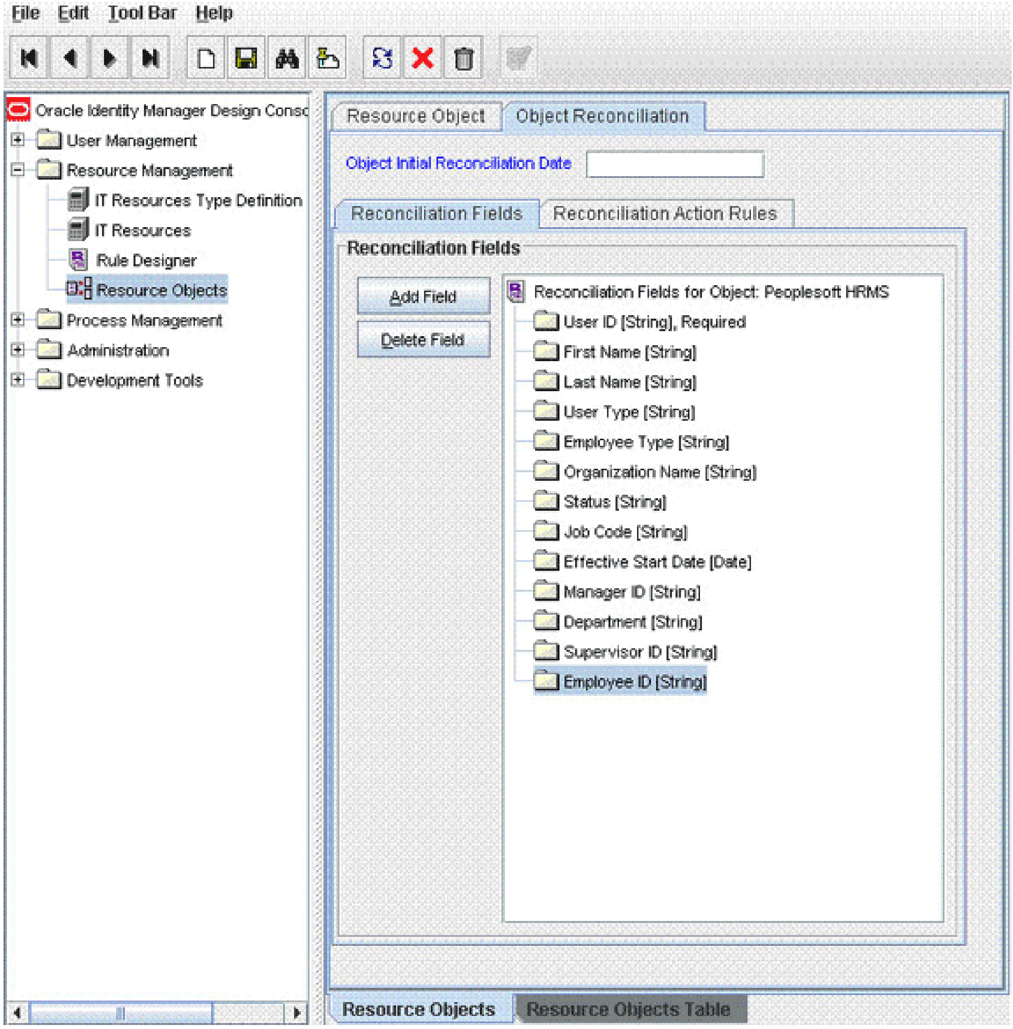
> **Note:**
>
> If you do not want to add new attributes for full reconciliation, then you need not perform this procedure.

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. Create a new user-defined field. For the procedure to create a user-defined field, see step 5 of Adding New Attributes for Incremental Reconciliation.

   b. Add a reconciliation field corresponding to the new attribute in the Peoplesoft HRMS resource object. For example, you can add the `Employee ID` reconciliation field.



c. Modify the PeopleSoft HRMS Person process definition to include the mapping between the newly added field and the corresponding reconciliation field. For the example described earlier, the mapping is as follows:

```
Employee ID = Employee ID
```

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

2. Add the new attribute in the message-specific attribute mapping lookup definition. For example, the Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping lookup definition for the PERSON_BASIC_FULLSYNC 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*

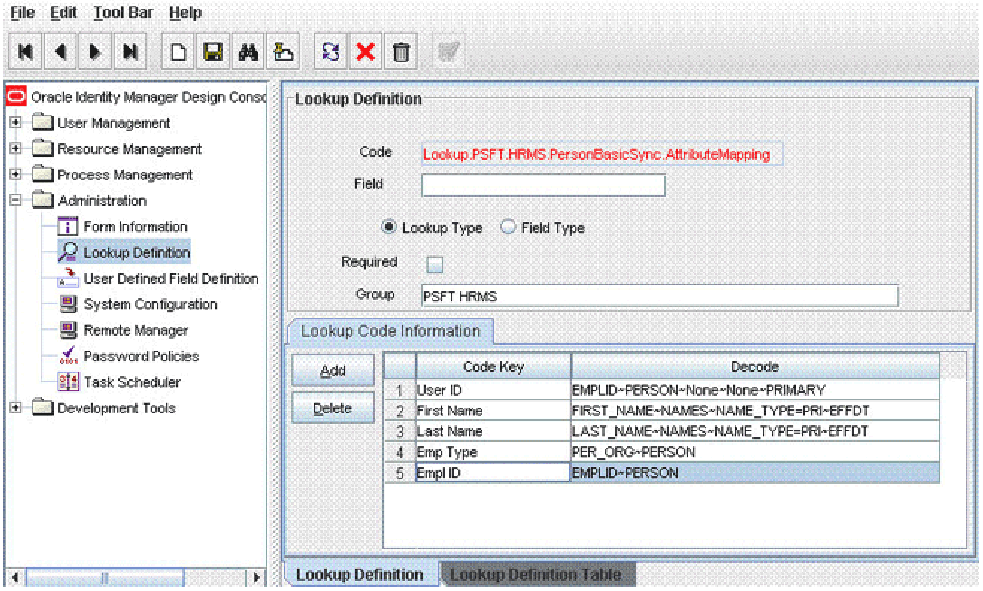
   For example:

   Code Key: Empl ID

   Decode: EMPLID~PERSON

In this example, `Empl ID` is the reconciliation field and its equivalent target system field is `EMPLID.`

The mapping is shown in the following screenshot:



Lookup Definition

Code: Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping

Field:

● Lookup Type ○ Field Type

Required □

Group: PSFT HRMS

	Code Key	Decode
1	User ID	EMPLID~PERSON~None~None~PRIMARY
2	First Name	FIRST_NAME~NAMES~NAME_TYPE=PRI~EFFDT
3	Last Name	LAST_NAME~NAMES~NAME_TYPE=PRI~EFFDT
4	Emp Type	PER_ORG~PERSON
5	Empl ID	EMPLID~PERSON

3. Add the new attribute in the Resource Object attribute reconciliation lookup definition. For example, the Lookup.PSFT.HRMS.PersonBasicSync.Recon lookup for the PERSON_BASIC_FULLSYNC message.

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

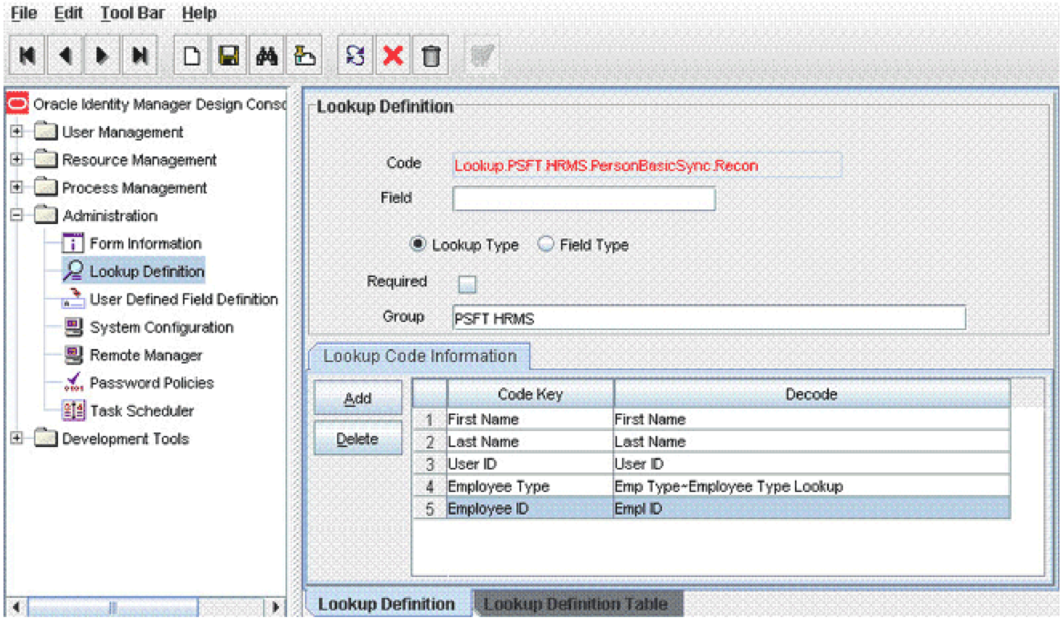
Code Key	Decode
RO Attribute	*`ATTRIBUTE FIELD~LOOKUP NAME`*

   For example:

   Code Key: Employee ID

   Decode: Empl ID

   The following screenshot displays the mapping:



Code: Lookup.PSFT.HRMS.PersonBasicSync.Recon

Field:

● Lookup Type ○ Field Type

Required □

Group: PSFT HRMS

	Code Key	Decode
1	First Name	First Name
2	Last Name	Last Name
3	User ID	User ID
4	Employee Type	Emp Type~Employee Type Lookup
5	Employee ID	Empl ID

In this example, RO Attribute refers to the resource object attribute name added in the preceding steps. The decode value is the code key value in the message-specific attribute mapping lookup definition.

4. Add the new attribute in the Custom Query lookup definition. See Setting Up the Lookup.PSFT.HRMS.CustomQuery Lookup Definition for more information.

4.2 Adding New Attributes for Incremental Reconciliation

Standard incremental reconciliation involves the reconciliation of predefined attributes. If required, you can add new attributes to the list of attributes that are reconciled.

> **Note:**
>
> If you do not want to add new attributes for incremental reconciliation, then you can skip this section.

To add a new attribute for incremental reconciliation:

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 Developer's Guide for Oracle Identity Manager* for detailed instructions on performing the following steps

a. Create a new user-defined field. For the procedure to create a user-defined field, see step 5 in this procedure.

b. Add a reconciliation field corresponding to the new attribute in the Peoplesoft HRMS resource object. For the example described earlier, you can add the Employee ID reconciliation field.

c. Modify the PeopleSoft HRMS Person process definition to include the mapping between the newly added field and the corresponding reconciliation field. For the example described earlier, the mapping is as follows:

```
Employee ID = Employee ID
```

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

2. Add the new attribute in the message-specific attribute mapping lookup definition, for example, the Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping lookup definition for the PERSON_BASIC_SYNC 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*

   For example:

   Code Key: Empl ID

   Decode: EMPLID~PERSON

   In this example, `Empl ID` is the reconciliation field and its equivalent target system field is EMPLID.

3. Add the new attribute in the Resource Object attribute reconciliation lookup definition, for example the Lookup.PSFT.HRMS.PersonBasicSync.Recon lookup for the PERSON_BASIC_SYNC message.

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

Code Key	Decode
RO Attribute	*ATTRIBUTE FIELD~LOOKUP NAME*

   For example:

   Code Key: Employee ID

   Decode: Empl ID

   In this example, RO Attribute refers to the resource object attribute name added in the preceding steps. The Decode value is the Code Key value defined in the message-specific attribute mapping lookup definition.

4. Add the new attribute in the Custom Query lookup definition. See Setting Up the Lookup.PSFT.HRMS.CustomQuery Lookup Definition for more information.

5. To create a user-defined field (UDF) on Oracle Identity Manager:

   a. Log in to the Oracle Identity Management Administration Console.

   b. Click **Advanced**.

c. On the Configuration tab, click **User Configuration**.

d. From the Actions menu, select **User Attributes**.

e. Click **Create Attribute**.

f. Enter details of the attribute (UDF) that you want to create. From the Category list, select **Custom Attributes**.

g. Set values for the attribute properties.

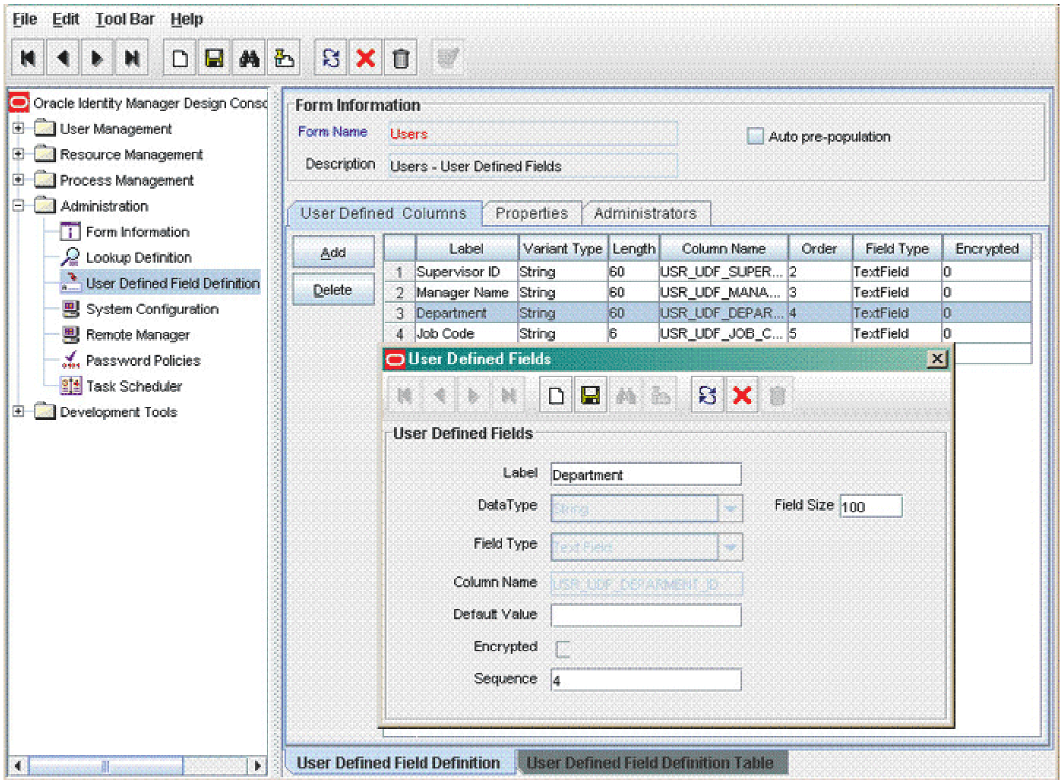
h. Review the data that you have entered, and then save the attribute.

4.3 Modifying Field Lengths on the OIM User Form

You might want to modify the lengths of the fields (attributes) on the OIM User form. For example, if you use the Japanese locale, then you might want to increase the lengths of OIM User form fields to accommodate multibyte data from the target system.

If you want to modify the length of a field on the OIM User form, then:

1. Log in to the Design Console.
2. Expand **Administration,** and double-click **User Defined Field Definition.**



Form Information

Form Name: Users

Description: Users - User Defined Fields

□ Auto pre-population

	Label	Variant Type	Length	Column Name	Order	Field Type	Encrypted
1	Supervisor ID	String	60	USR_UDF_SUPER...	2	TextField	0
2	Manager Name	String	60	USR_UDF_MANA...	3	TextField	0
3	Department	String	60	USR_UDF_DEPAR...	4	TextField	0
4	Job Code	String	6	USR_UDF_JOB_C...	5	TextField	0

User Defined Fields

User Defined Fields

Label: Department

DataType: String

Field Size: 100

Field Type: Text Field

Column Name: USR_UDF_DEPARMENT_ID

Default Value:

Encrypted: □

Sequence: 4

3. Search for and open the **Users** form.
4. Modify the length of the required field.
5. Click the Save icon.

4.4 Configuring Validation of Data During Reconciliation

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

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 First Name attribute contains the number sign (#):

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

   public boolean validate(HashMap hmUserDetails,
            HashMap hmEntitlementDetails, String field) {
               /*
            * You must write code to validate attributes. Parent
            * data values can be fetched by using hmUserDetails.get(field)
            * For child data values, loop through the
            * ArrayList/Vector fetched by hmEntitlementDetails.get("Child
   Table")
            * Depending on the outcome of the validation operation,
            * the code must return true or false.
            */
            /*
            * In this sample code, the value "false" is returned if the field
            * contains the number sign (#). Otherwise, the value "true" is
            * returned.
            */
   ```

```
      boolean valid=true;
      String sFirstName=(String) hmUserDetails.get(field);
      for(int i=0;i<sFirstName.length();i++){
        if (sFirstName.charAt(i) == '#'){
              valid=false;
              break;
        }
      }
      return valid;
  }
} /* End */
```

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

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

   - **For Microsoft Windows:**

     OIM_HOME/server/bin/UploadJars.bat

   - **For UNIX:**

     OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.
4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.

   b. Search for and open the message-specific configuration lookup definition.

      For example, locate the **Lookup.PSFT.Message.WorkForceSync.Configuration** lookup definition for the WORKFORCE_SYNC message. See Lookup.PSFT.Message.WorkForceSync.Configuration for information about this lookup definition. Check for the parameter Validation Lookup Definition in this lookup definition. The Decode value specifies the name of the validation lookup. In this example, the Decode value is Lookup.PSFT.HRMS.WorkForceSync.Validation.

   c. Search for and open the **Lookup.PSFT.HRMS.WorkForceSync.Validation** lookup definition.

   d. In the Code Key column, enter `First Name`. 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.WorkForceSync.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 directory:

   CONN_HOME/listener/deployable-archive/PeoplSoftOIMListener.ear/PeoplSoftOIMListener.war/WEB-INF/lib

7. Redeploy the PeopleSoftOIMListener.ear file on the application server. To do so, run the following command:

   ```
   ant redeploy
   ```

   See Deploying the PeopleSoft Listener for information about the deployment tool.

4.5 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 directory in which Oracle WebLogic Server is installed.

   - **For Microsoft Windows:**

     OIM_HOME/server/bin/UploadJars.bat

   - **For UNIX:**

     OIM_HOME/server/bin/UploadJars.sh

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

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

   a. Log in to the Design Console.

   b. Search for and open the message-specific configuration lookup definition, in this example, the **Lookup.PSFT.Message.WorkForceSync.Configuration** lookup definition for the WORKFORCE_SYNC message.

      See Lookup.PSFT.Message.WorkForceSync.Configuration for information about this lookup definition. Check for the parameter Transformation Lookup Definition in this lookup definition. The Decode value specifies the name of the transformation lookup. In this example, the Decode value is Lookup.PSFT.HRMS.WorkForceSync.Transformation.

   c. Search for and open the **Lookup.PSFT.HRMS.WorkForceSync.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.WorkForceSync.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 in Step 2 to the following directory:

   CONN_HOME/listener/deployable-archive/PeoplSoftOIMListener.ear/PeoplSoftOIMListener.war/WEB-INF/lib
7. Redeploy the PeopleSoftOIMListener.ear file on the application server. To do so, run the following command:

   ```
   ant redeploy
   ```

   See Deploying the PeopleSoft Listener for information about the deployment tool.

4.6 Setting Up the Lookup.PSFT.HRMS.CustomQuery Lookup Definition

You configure limited reconciliation by specifying a query condition as the value of the Custom Query attribute in the message-specific configuration lookup. See Lookup.PSFT.HRMS.CustomQuery for more information about this lookup definition.

You must ensure that the OIM User attribute to use in the query exists in the Lookup.PSFT.HRMS.CustomQuery lookup definition. You must add a row in this lookup definition whenever you add a UDF in the user form.

To add a new UDF to this lookup definition:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the **Lookup.PSFT.HRMS.CustomQuery** lookup definition.
3. Click **Add.**

   > **Note:**
   >
   > The Code Key value represents the resource object field name and the Decode value specifies the column name of the USR table.

4. In the Code Key and Decode columns, enter the values for the UDF.

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

Code Key	Decode
RO Attribute Name	Column name of the USR table

If you have added a UDF Empl ID with column name as USR_UDF_EMPLOYEE_ID, then define the following entry in this lookup definition:

Code Key: Empl ID

Decode: USR_UDF_EMPLOYEE_ID

5. Click the Save icon.

4.7 Setting Up the Lookup.PSFT.HRMS.WorkForceSync.EmpStatus Lookup Definition

The Lookup.PSFT.HRMS.WorkForceSync.EmpStatus lookup definition maps the value retrieved from the ACTION node in the WORKFORCE_SYNC message XML with the status to be shown on Oracle Identity Manager for the employee. See Lookup.PSFT.HRMS.WorkForceSync.EmpStatus for more information about this lookup definition.

The following section describes how to add an action, for example Suspension in this lookup definition.

To add an action in the Lookup.PSFT.HRMS.WorkForceSync.EmpStats lookup definition:

1. Obtain the Code Key and the description for the action to be added from your PeopleSoft functional resource.

   The Code Key is usually a three-character string.

   The path to obtain the Action values and its description in PeopleSoft HRMS 9.0 is as follows:

   From the Main Menu, select **Set Up HRMS, Product Related, Workforce Administration,** and then **Actions.**
2. Log in to the Design Console of Oracle Identity Manager.
3. Expand **Administration,** and then double-click **Lookup Definition.**
4. Search for and open the **Lookup.PSFT.HRMS.WorkForceSync.EmpStats** lookup definition.
5. Click **Add.**

> **Note:**
>
> The following is the format of the values stored in this lookup definition:
>
> Code Key: ACTION value retrieved from the WORKFORCE_SYNC message XML
>
> Decode: `Active` or `Disabled` in Oracle Identity Manager

6. In the Code Key and Decode columns, enter the values for the following values:

   Code Key: SUS

   Decode: Disabled

   In this example, SUS is retrieved from the ACTION node of the WORKFORCE_SYNC message XML for the action suspension. The corresponding mapping for this action is defined as Disabled in Oracle Identity Manager.

   > **Note:**
   >
   > You must define the mapping for all Actions to be performed on the target system in this lookup definition.

7. Click the Save icon.

4.8 Configuring the Connector for Multiple Installations of the Target System

This section contains the following topics:

- Connector Objects and Their Associations
- Creating Copies of the Connector Objects

4.8.1 Connector Objects and Their Associations

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

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

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

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

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

Note:

A single listener is sufficient for multiple installations of the target system. You can configure the nodes to point to the same listener with different IT resource names.

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.HRMS.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 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 HRMS	• Scheduled Task: Peoplesoft HRMS Trusted Reconciliation • Resource Object: Peoplesoft HRMS	You need to create a copy of IT Resource with a different name.
Resource Object	Peoplesoft HRMS	Message-specific configuration lookup definitions: • Lookup.PSFT.Message.PersonBasicSync.Configuration • Lookup. PSFT.Message.WorkForceSync.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 the two installations of the target system.
Common Configuration Lookup Definition	Lookup.PSFT.HRMS.Configuration	Message-specific configuration lookup definitions: • Lookup.PSFT.Message.PersonBasicSync.Configuration • Lookup. PSFT.Message.WorkForceSync.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 the 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.PersonBasicSync.Configuration • Lookup.PSFT.Message.WorkForceSync.Configuration	Attribute mapping lookup definitions: • Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping • Lookup.PSFT.HRMS.WorkForceSync.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 the two installations of the target system.
Attribute Mapping Lookup Definition	• Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping • Lookup.PSFT.HRMS.WorkForceSync.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 the two installations of the target system.
Recon Map Lookup Definition	• Lookup.PSFT.HRMS.PersonBasicSync.Recon • Lookup.PSFT.HRMS.WorkForceSync.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 the two installations of the target system.

4.8.2 Creating Copies of the Connector Objects

To create copies of the connector objects:

> **Note:**
>
> See Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the steps in this procedure.

1. Create a copy of the IT resource. See Configuring the IT Resource for information about this IT resource.
2. Create a copy of the Peoplesoft HRMS resource object.
3. Create copy of the PERSON_BASIC_SYNC and WORKFORCE_SYNC message-specific configuration lookup.
4. Create a copy of the Lookup.PSFT.HRMS.Configuration lookup definition. Add the new lookup to the Configuration Lookup parameter of the new IT resource created in Step 1. See Lookup.PSFT.HRMS.Configuration for information about this lookup definition.

5. Create a copy of the message-specific attribute mapping and Recon lookup definition, for example, the Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping and the Lookup.PSFT.HRMS.PersonBasicSync.Recon for PERSON_BASIC_SYNC message. Similarly, the Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping and the Lookup.PSFT.HRMS.WorkForceSync.Recon for WORKFORCE_SYNC message.
6. Create a copy of the Peoplesoft HRMS Trusted Reconciliation scheduled task. See Configuring the Scheduled Task for Person 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.

5
Testing and Troubleshooting

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

> **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 topics related to connector testing.

- Testing Reconciliation
- Troubleshooting

5.1 Testing Reconciliation

The testing utility enables you to test the functionality of the connector. The testing utility takes as input the XML file or message generated by the target system. It can be used for testing full and incremental reconciliation.

The testing utility is located in the test directory on the installation media. See 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:

   i) Enter the PeopleSoftOIMListener servlet URL as the value of ListenerURL in following syntax:

   ```
   http://HOSTNAME:PORT/PeopleSoftOIMListener
   ```

   For example:

   ```
   ListenerURL=http://10.1.6.83:8080/PeopleSoftOIMListener
   ```

   ii) Enter the absolute XML message file path as the value of XMLFilePath as shown in the following example:

   ```
   XMLFilePath=c:/xmlmessages/person_basic_sync.xml
   ```

   > **Note:**
   >
   > Ensure that there is no blank or white-space character in the directory path and file name that you specify.

iii) Enter a value for the MessageType. For a ping message, specify `Ping, None,` or `otherwise` as shown in the following example:

```
MessageType=None
```

iv) Enter a value for **ITResourceName.** This value must match the active IT resource in Oracle Identity Manager.

For example:

```
ITResourceName=PSFT HRMS
```

v) Enter the name of the message for which you run the testing utility.

For example:

```
MessageName=PERSON_BASIC_SYNC
```

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 directory.

3. Open a command window, and navigate to the scripts directory.

   You must run the testing utility from the *OIM_HOME*/server/ConnectorDefaultDirectory/*CONN_HOME*/test/scripts directory, where *CONN_HOME* is the connector directory.

   For example:

   OIM_HOME/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/test/scripts

4. Run the following script:

   - For Microsoft Windows:

     ```
     InvokeListener.bat
     ```

   - For UNIX:

     ```
     InvokeListener.sh
     ```

Verify that a reconciliation event is created in Oracle Identity Manager and that the event contains the data specified in the message-specific XML file.

5.2 Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the PeopleSoft Employee Reconciliation connector:

Problem Description	Solution

You might receive the following error message while reconciling job data:
`ERROR [PSFTCOMMON]`
`===============================`
`ERROR [PSFTCOMMON]`
`oracle.iam.connectors.psft.common.hand`
`ler.HandlerFactory:`
`getMessageHandler:`
`No Lookup defined for`
`message WORKFORCE_SYNC.VERSION_2`
`ERROR [PSFTCOMMON]`
`===============================`
 	
`ERROR [PSFTCOMMON]`
`===============================`
`ERROR [PSFTCOMMON]`
`oracle.iam.connectors.psft.common.list`
`ener.PeopleSoftOIMListener:`
`process: Message specific handler`
`couldn'tbe initialized.`
`Please check if lookup definition has`
`been`
`specified for the message`
`"WORKFORCE_SYNC.VERSION_2".`
`ERROR [PSFTCOMMON]`
`================================`
 	
This indicates that the target system is sending the WORKFORCE_SYNC message with the name WORKFORCE_SYNC.VERSION_2.
	You must modify the Code Key value of the WORKFORCE_SYNC attribute in the Lookup.PSFT.HRMS.Configuration lookup definition as follows:
	Code Key: WORKFORCE_SYNC.VERSION_2
	Decode: Lookup.PSFT.Message.WorkForceSync.Configuration

If the WORKFORCE_FULLSYNC message is processed before the PERSON_BASIC_FULLSYNC message, then the Oracle Identity Manager stores the data for all those events in the Event Received state. You might receive an event in the Event Received state with an empty Status field.	You must check the value of the Action applicable for the Person in the Lookup.PSFT.HRMS.WorkForceSync.EmpStatus lookup definition. This lookup definition stores the mapping between the Action applicable for a Person and the OIM User status.
Workforce incremental reconciliation fails or the updates on the target system are not transmitted to Oracle Identity Manager.	You must update the Lookup.PSFT.HRMS.Configuration lookup definition on the Design Console. To update, modify the `WORKFORCE_SYNC.VERSION_3` value to `WORKFORCE_SYNC.INTERNAL.`

6
Known Issues and Workarounds

The following is an issue and workaround associated with this release of the connector:

6.1 Deletion Of Person Records Not Supported By The Connector

The connector does not support direct deletion of person records.

There is no workaround available for this issue.

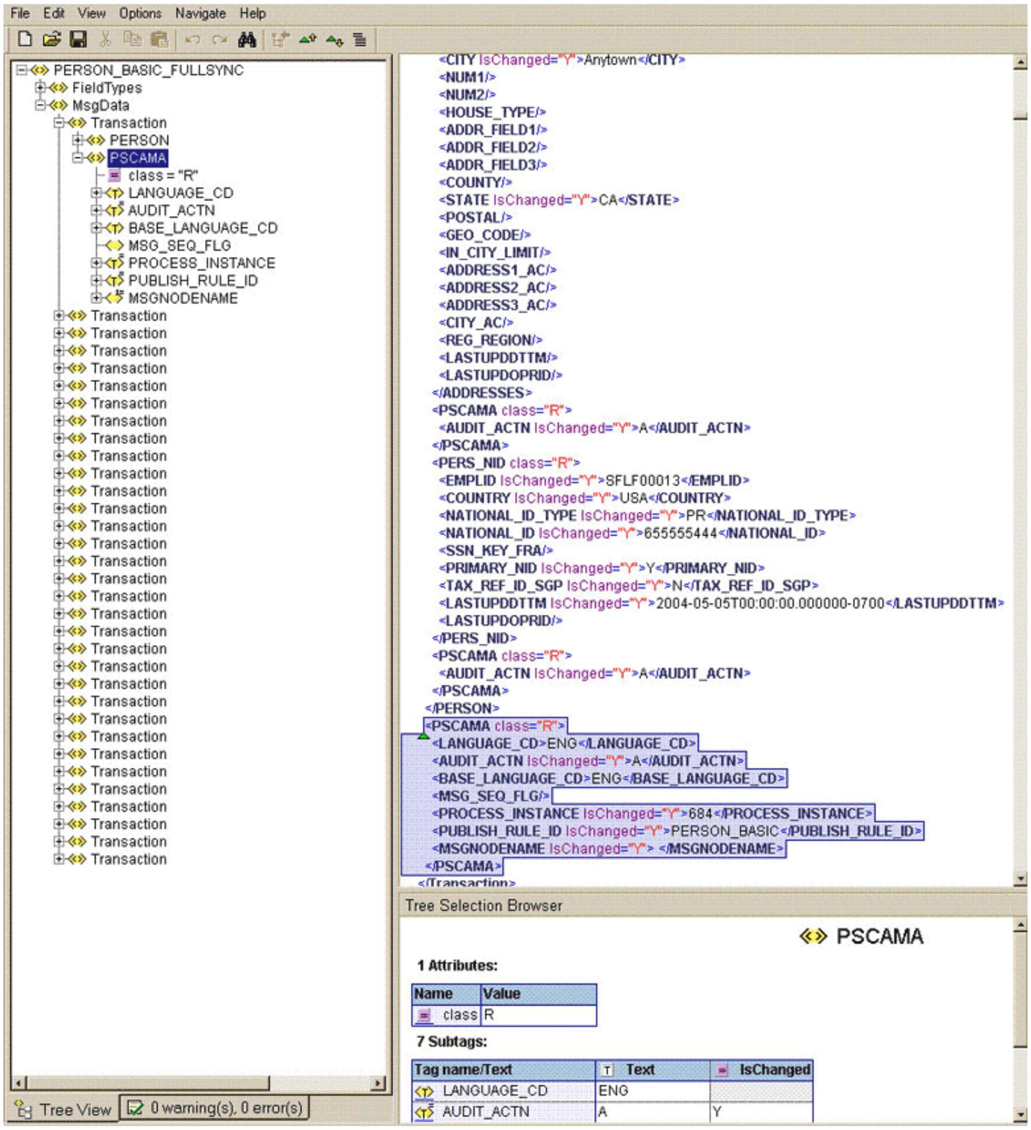
A

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 files for PERSON_BASIC_FULLSYNC and WORKFORCE_FULLSYNC messages have multiple transaction nodes. However, in case of incremental reconciliation, the XML messages PERSON_BASIC_SYNC and WORKFORCE_SYNC have only one transaction node.

Every transaction node has a PeopleSoft Common Application Messaging Attributes (PSCAMA) subnode.

The following screenshot shows the PSCAMA node:



```
PERSON_BASIC_FULLSYNC
  FieldTypes
  MsgData
    Transaction
      PERSON
      PSCAMA
        class = "R"
        LANGUAGE_CD
        AUDIT_ACTN
        BASE_LANGUAGE_CD
        MSG_SEQ_FLG
        PROCESS_INSTANCE
        PUBLISH_RULE_ID
        MSGNODENAME
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
```

```
      <CITY IsChanged="Y">Anytown</CITY>
      <NUM1/>
      <NUM2/>
      <HOUSE_TYPE/>
      <ADDR_FIELD1/>
      <ADDR_FIELD2/>
      <ADDR_FIELD3/>
      <COUNTY/>
      <STATE IsChanged="Y">CA</STATE>
      <POSTAL/>
      <GEO_CODE/>
      <IN_CITY_LIMIT/>
      <ADDRESS1_AC/>
      <ADDRESS2_AC/>
      <ADDRESS3_AC/>
      <CITY_AC/>
      <REG_REGION/>
      <LASTUPDDTTM/>
      <LASTUPDOPRID/>
    </ADDRESSES>
    <PSCAMA class="R">
      <AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
    </PSCAMA>
    <PERS_NID class="R">
      <EMPLID IsChanged="Y">SFLF00013</EMPLID>
      <COUNTRY IsChanged="Y">USA</COUNTRY>
      <NATIONAL_ID_TYPE IsChanged="Y">PR</NATIONAL_ID_TYPE>
      <NATIONAL_ID IsChanged="Y">655555444</NATIONAL_ID>
      <SSN_KEY_FRA/>
      <PRIMARY_NID IsChanged="Y">Y</PRIMARY_NID>
      <TAX_REF_ID_SGP IsChanged="Y">N</TAX_REF_ID_SGP>
      <LASTUPDDTTM IsChanged="Y">2004-05-05T00:00:00.000000-0700</LASTUPDDTTM>
      <LASTUPDOPRID/>
    </PERS_NID>
    <PSCAMA class="R">
      <AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
    </PSCAMA>
  </PERSON>
  <PSCAMA class="R">
    <LANGUAGE_CD>ENG</LANGUAGE_CD>
    <AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
    <BASE_LANGUAGE_CD>ENG</BASE_LANGUAGE_CD>
    <MSG_SEQ_FLG/>
    <PROCESS_INSTANCE IsChanged="Y">684</PROCESS_INSTANCE>
    <PUBLISH_RULE_ID IsChanged="Y">PERSON_BASIC</PUBLISH_RULE_ID>
    <MSGNODENAME IsChanged="Y"> </MSGNODENAME>
  </PSCAMA>
</Transaction>
```

Tree Selection Browser

PSCAMA

1 Attributes:

Name	Value
class	R

7 Subtags:

Tag name/Text	Text	IsChanged
LANGUAGE_CD	ENG	
AUDIT_ACTN	A	Y

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:

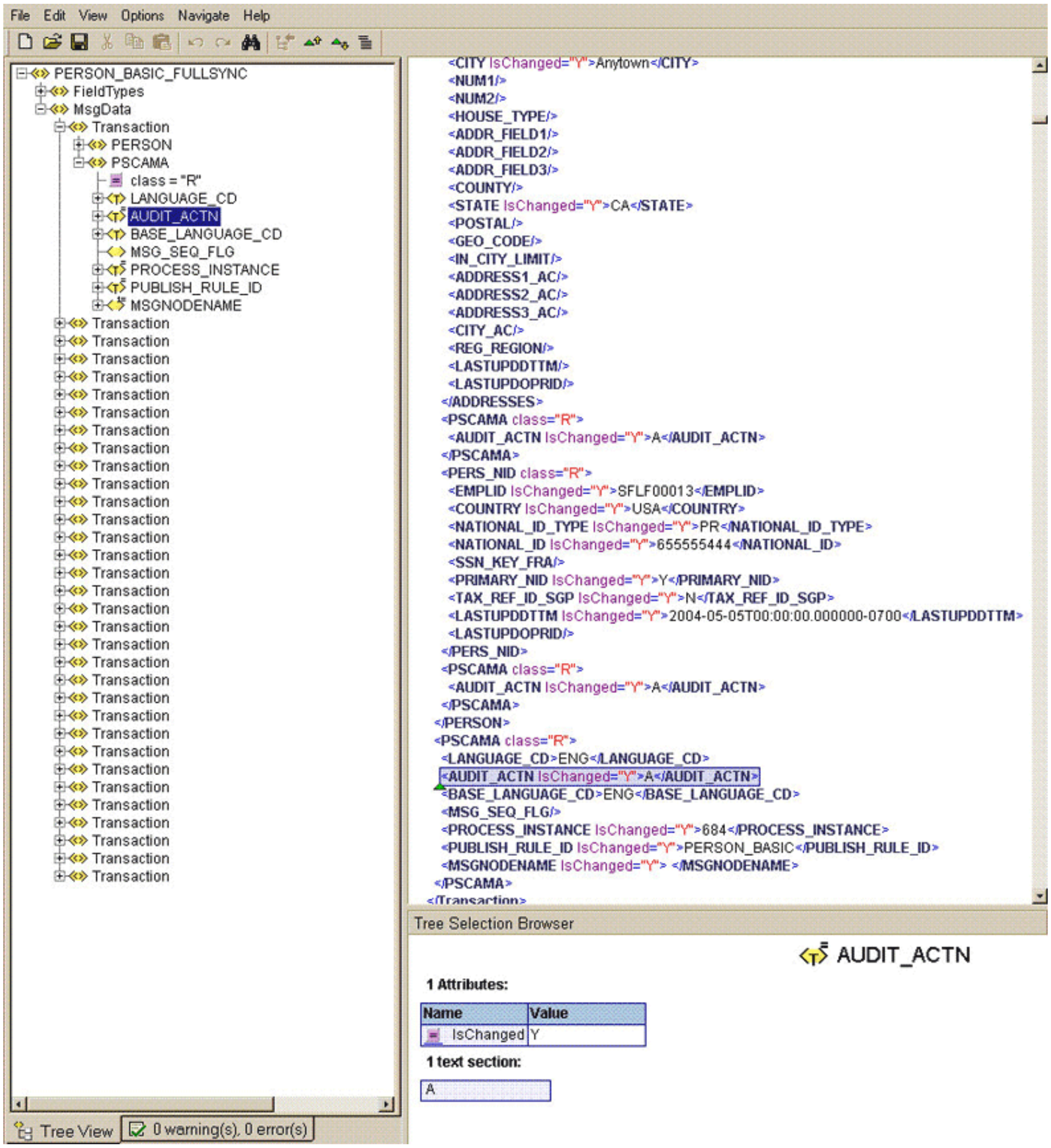
- Language in which the data is written
- Type of transaction the row represents, such as add or update

When receiving a message, PeopleCode inspects the PSCAMA node for this information and responds accordingly.

The AUDIT_ACTN subnode of PSCAMA, known as Root Audit Action, filters the data records in an XML message. It indicates the action taken against a person, such as Add or Change in Oracle Identity Manager.

If the biographical information is changed for a person on the target system, then the Root Audit Action value is C. If a person is added, then the Root Audit Action is either A or empty.

The Add Root Audit Action is shown in the following screenshot:



```
PERSON_BASIC_FULLSYNC
  FieldTypes
  MsgData
    Transaction
      PERSON
      PSCAMA
        class = "R"
        LANGUAGE_CD
        AUDIT_ACTN
        BASE_LANGUAGE_CD
        MSG_SEQ_FLG
        PROCESS_INSTANCE
        PUBLISH_RULE_ID
        MSGNODENAME
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
```

```
    <CITY IsChanged="Y">Anytown</CITY>
    <NUM1/>
    <NUM2/>
    <HOUSE_TYPE/>
    <ADDR_FIELD1/>
    <ADDR_FIELD2/>
    <ADDR_FIELD3/>
    <COUNTY/>
    <STATE IsChanged="Y">CA</STATE>
    <POSTAL/>
    <GEO_CODE/>
    <IN_CITY_LIMIT/>
    <ADDRESS1_AC/>
    <ADDRESS2_AC/>
    <ADDRESS3_AC/>
    <CITY_AC/>
    <REG_REGION/>
    <LASTUPDDTTM/>
    <LASTUPDOPRID/>
   </ADDRESSES>
   <PSCAMA class="R">
    <AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
   </PSCAMA>
   <PERS_NID class="R">
    <EMPLID IsChanged="Y">SFLF00013</EMPLID>
    <COUNTRY IsChanged="Y">USA</COUNTRY>
    <NATIONAL_ID_TYPE IsChanged="Y">PR</NATIONAL_ID_TYPE>
    <NATIONAL_ID IsChanged="Y">655555444</NATIONAL_ID>
    <SSN_KEY_FRA/>
    <PRIMARY_NID IsChanged="Y">Y</PRIMARY_NID>
    <TAX_REF_ID_SGP IsChanged="Y">N</TAX_REF_ID_SGP>
    <LASTUPDDTTM IsChanged="Y">2004-05-05T00:00:00.000000-0700</LASTUPDDTTM>
    <LASTUPDOPRID/>
   </PERS_NID>
   <PSCAMA class="R">
    <AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
   </PSCAMA>
  </PERSON>
  <PSCAMA class="R">
   <LANGUAGE_CD>ENG</LANGUAGE_CD>
   <AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
   <BASE_LANGUAGE_CD>ENG</BASE_LANGUAGE_CD>
   <MSG_SEQ_FLG/>
   <PROCESS_INSTANCE IsChanged="Y">684</PROCESS_INSTANCE>
   <PUBLISH_RULE_ID IsChanged="Y">PERSON_BASIC</PUBLISH_RULE_ID>
   <MSGNODENAME IsChanged="Y"> </MSGNODENAME>
  </PSCAMA>
 </Transaction>
```

AUDIT_ACTN

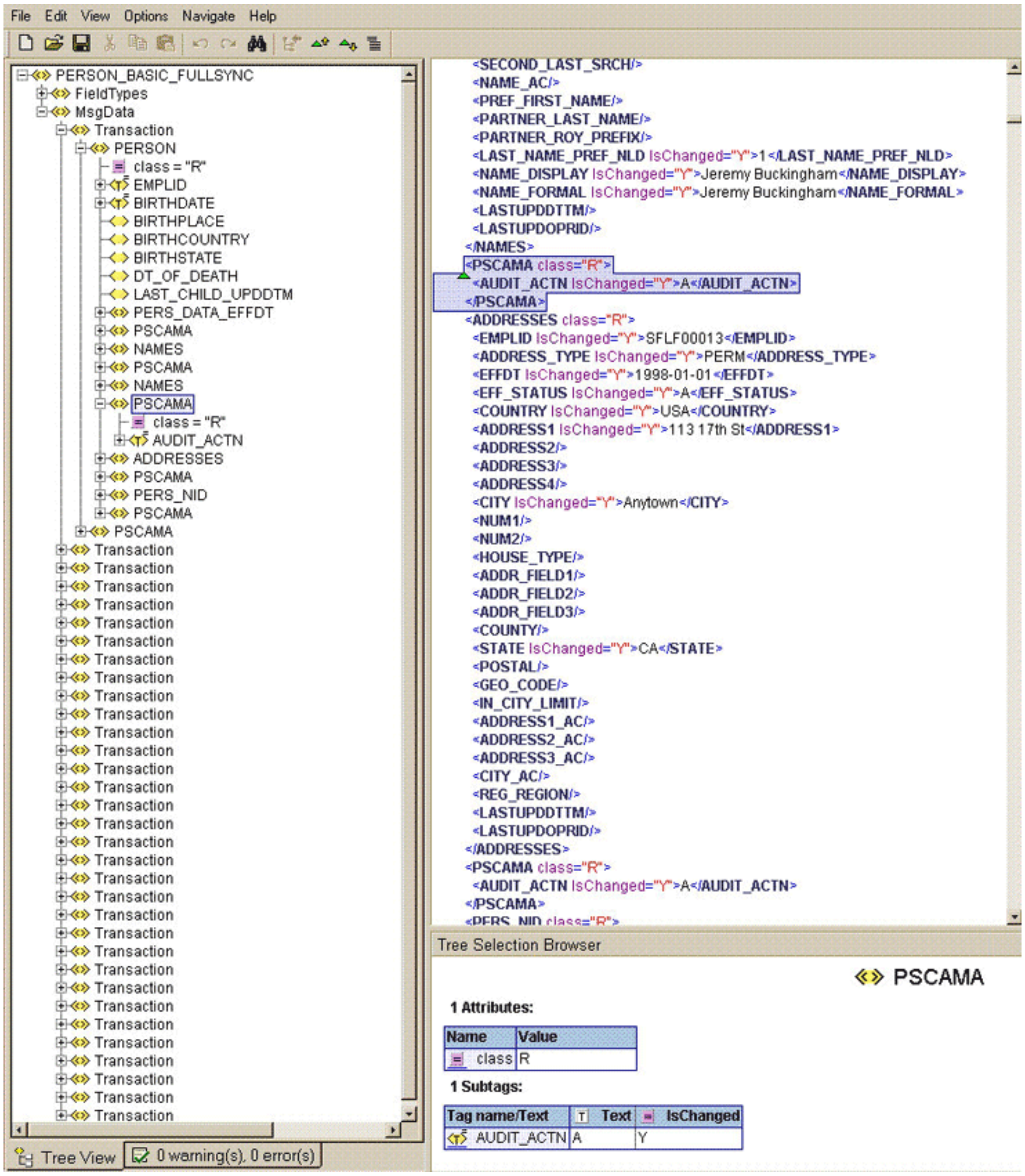
1 Attributes:

Name	Value
IsChanged	Y

1 text section:

A

The nonzero level PSCAMA node and its Root Audit Action are shown in the following screenshot:



```
PERSON_BASIC_FULLSYNC
  FieldTypes
  MsgData
    Transaction
      PERSON
        class = "R"
        EMPLID
        BIRTHDATE
        BIRTHPLACE
        BIRTHCOUNTRY
        BIRTHSTATE
        DT_OF_DEATH
        LAST_CHILD_UPDDTM
        PERS_DATA_EFFDT
        PSCAMA
        NAMES
        PSCAMA
        NAMES
        PSCAMA
          class = "R"
          AUDIT_ACTN
        ADDRESSES
        PSCAMA
        PERS_NID
        PSCAMA
      PSCAMA
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
    Transaction
```

```
  <SECOND_LAST_SRCH/>
  <NAME_AC/>
  <PREF_FIRST_NAME/>
  <PARTNER_LAST_NAME/>
  <PARTNER_ROY_PREFIX/>
  <LAST_NAME_PREF_NLD IsChanged="Y">1</LAST_NAME_PREF_NLD>
  <NAME_DISPLAY IsChanged="Y">Jeremy Buckingham</NAME_DISPLAY>
  <NAME_FORMAL IsChanged="Y">Jeremy Buckingham</NAME_FORMAL>
  <LASTUPDDTTM/>
  <LASTUPDOPRID/>
</NAMES>
<PSCAMA class="R">
  <AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
</PSCAMA>
<ADDRESSES class="R">
  <EMPLID IsChanged="Y">SFLF00013</EMPLID>
  <ADDRESS_TYPE IsChanged="Y">PERM</ADDRESS_TYPE>
  <EFFDT IsChanged="Y">1998-01-01</EFFDT>
  <EFF_STATUS IsChanged="Y">A</EFF_STATUS>
  <COUNTRY IsChanged="Y">USA</COUNTRY>
  <ADDRESS1 IsChanged="Y">113 17th St</ADDRESS1>
  <ADDRESS2/>
  <ADDRESS3/>
  <ADDRESS4/>
  <CITY IsChanged="Y">Anytown</CITY>
  <NUM1/>
  <NUM2/>
  <HOUSE_TYPE/>
  <ADDR_FIELD1/>
  <ADDR_FIELD2/>
  <ADDR_FIELD3/>
  <COUNTY/>
  <STATE IsChanged="Y">CA</STATE>
  <POSTAL/>
  <GEO_CODE/>
  <IN_CITY_LIMIT/>
  <ADDRESS1_AC/>
  <ADDRESS2_AC/>
  <ADDRESS3_AC/>
  <CITY_AC/>
  <REG_REGION/>
  <LASTUPDDTTM/>
  <LASTUPDOPRID/>
</ADDRESSES>
<PSCAMA class="R">
  <AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
</PSCAMA>
<PERS_NID class="R">
```

Tree Selection Browser

PSCAMA

1 Attributes:

Name	Value
class	R

1 Subtags:

Tag name/Text	Text	IsChanged
AUDIT_ACTN	A	Y

B

Configuring the Connector Messages

You can configure the connector messages of release 9.1.0.*x*.*y* with that of the current release.

This appendix contains the following topics:

- Configuring the Connector Messages
- Lookup Definitions to Configure the Messages

B.1 Configuring the Connector Messages

To configure the messages:

1. Add the following lookup definitions:
   - Lookup.PSFT.Message.XellerateUser.Configuration
   - Lookup.PSFT.HRMS.XellerateUser.EmpStatus
   - Lookup.PSFT.HRMS.XellerateUser.EmpType
   - Lookup.PSFT.HRMS.XellerateUser.AttributeMapping
   - Lookup.PSFT.HRMS.XellerateUser.Recon

   To add a lookup definition:

   a. Log in to the Oracle Identity Manager Design Console.

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

   c. In the **Code** field, enter the name of the lookup definition, for example, `Lookup.PSFT.Message.XellerateUser.Configuration.`

   d. In the **Group** field, enter the name with which you want to associate the lookup definition, for example, `PSFT HRMS.`

   e. Click the Save icon.

   f. Add the Code Key and Decode values specified in "Lookup Definitions to Configure the Messages" section. To do so:

      i) Click **Add**.

      A new row is added.

      ii) Enter the following values:

      Code Key: Attribute Mapping Lookup

      Decode: Lookup.PSFT.HRMS.XellerateUser.AttributeMapping

      iii) Repeat Steps i) and ii) to add the remaining entries in the lookup definition.

      iv) Click the Save icon.

2. Modify the Lookup.PSFT.HRMS.Configuration lookup definition as follows:

   a. Add the following entry in the lookup definition:

Code Key: Name of the message sent by PeopleSoft, for example, XELLERATE_USR_MSG

Decode: Lookup.PSFT.Message.XellerateUser.Configuration

b. Modify the value of the following entry in the lookup definition:

Code Key: Ignore Root Audit Action

Decode: Yes

c. Click the Save icon.

3. Write code that implements the required message handler or message parser logic in a Java class. See the following files in the /samples directory of the installation media for more information about the Java code.

- PSFTXellerateUserReconMessageHandlerImpl.java
- XellerateUserMessageParser.java

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

5. Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 4 to the Oracle Identity Manager database.

> **Note:**
>
> See Upload JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for steps to import the contents of JavaTasks directory into the Oracle Identity Manager database.

6. Remove PeopleSoftOIMListener.ear file from the application server. See Removing the PeopleSoft Listener for the procedure.

7. Copy the validation JAR file created in Step 4 to the following directory:

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

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

9. Modify the PeopleSoft Integration Broker configuration as follows:

a. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Nodes.**

b. On the Find an Existing Value tab, enter the node name, for example, `OIM_ER_NODE,` and then click **Search.**

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

Gateway ID: LOCAL

Connector ID: HTTPTARGET

d. 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 IT Resource name as configured for PeopleSoft HRMS

Sample value: PSFT HRMS

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://ORACLE_IDENTITY_MANAGER_SERVER_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 Oracle WebLogic Server:

```
http://10.121.16.42:7001/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 Oracle WebLogic Server:

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

> **Note:**
>
> The ports may vary depending on the installation that you are using.

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

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

B.2 Lookup Definitions to Configure the Messages

You must add the following lookup definitions to configure the messages of this release of the connector:

- Lookup.PSFT.Message.XellerateUser.Configuration
- Lookup.PSFT.Message.XellerateUser.Configuration
- Lookup.PSFT.HRMS.XellerateUser.EmpStatus
- Lookup.PSFT.HRMS.XellerateUser.AttributeMapping
- Lookup.PSFT.HRMS.XellerateUser.Recon

B.2.1 Lookup.PSFT.Message.XellerateUser.Configuration

Code Key	Decode
Attribute Mapping Lookup	Lookup.PSFT.HRMS.XellerateUser.AttributeMapping
Custom Query	Enter a Value
Custom Query Lookup Definition	Lookup.PSFT.HRMS.CustomQuery
Data Node Name	Transaction
Employee Status Lookup	Lookup.PSFT.HRMS.XellerateUser.EmpStatus
Employee Type Lookup	Lookup.PSFT.HRMS.XellerateUser.EmpType
Recon Lookup Definition	Lookup.PSFT.HRMS.XellerateUser.Recon
Message Handler Class	oracle.iam.connectors.psft.common.handler.impl.PSFTXellerateUserReconMessageHandlerImpl
Message Parser	oracle.iam.connectors.psft.common.parser.impl.XellerateUserMessageParser
Organization	Xellerate Users
Resource Object	Peoplesoft HRMS
Transformation Lookup Definition	Lookup.PSFT.HRMS.XellerateUser.Transformation
User Type	End-User
Use Transformation	No
Use Validation	No
Validation Lookup Definition	Lookup.PSFT.HRMS.XellerateUser.Validation

B.2.2 Lookup.PSFT.Message.XellerateUser.Configuration

Code Key	Decode
Attribute Mapping Lookup	Lookup.PSFT.HRMS.XellerateUser.AttributeMapping
Custom Query	Enter a Value
Custom Query Lookup Definition	Lookup.PSFT.HRMS.CustomQuery
Data Node Name	Transaction
Employee Status Lookup	Lookup.PSFT.HRMS.XellerateUser.EmpStatus
Employee Type Lookup	Lookup.PSFT.HRMS.XellerateUser.EmpType
Recon Lookup Definition	Lookup.PSFT.HRMS.XellerateUser.Recon
Message Handler Class	oracle.iam.connectors.psft.common.handler.impl.PSFTXellerateUserReconMessageHandlerImpl

Code Key	Decode
Message Parser	oracle.iam.connectors.psft.common.parser.impl.XellerateUserMessageParser
Organization	Xellerate Users
Resource Object	Peoplesoft HRMS
Transformation Lookup Definition	Lookup.PSFT.HRMS.XellerateUser.Transformation
User Type	End-User
Use Transformation	No
Use Validation	No
Validation Lookup Definition	Lookup.PSFT.HRMS.XellerateUser.Validation

B.2.3 Lookup.PSFT.HRMS.XellerateUser.EmpStatus

Code Key	Decode
A	Active
I	Inactive

B.2.4 Lookup.PSFT.HRMS.XellerateUser.AttributeMapping

Code Key	Decode
Department	DEPTID~JOB
Emp Type	EMPLOYEETYPE~JOB
First Name	FIRST_NAME~PERSONAL_DATA
Last Name	LAST_NAME~PERSONAL_DATA
Job ID	JOBCODE~JOB
Status	STATUS~JOB
User ID	EMPLID~PERSONAL_DATA~None~None~PRIMARY

B.2.5 Lookup.PSFT.HRMS.XellerateUser.Recon

Code Key	Decode
Department	Department
Employee Type	Emp Type~Employee Type Lookup
First Name	First Name
Last Name	Last Name
Job Code	Job ID
Status	Status~Employee Status Lookup
User ID	User ID

C

Setting Up SSL on Oracle WebLogic Server

This appendix describes how to configure SSL on Oracle WebLogic Server for PeopleTools 8.50.

Setting up SSL on Oracle WebLogic Server involves the following steps:

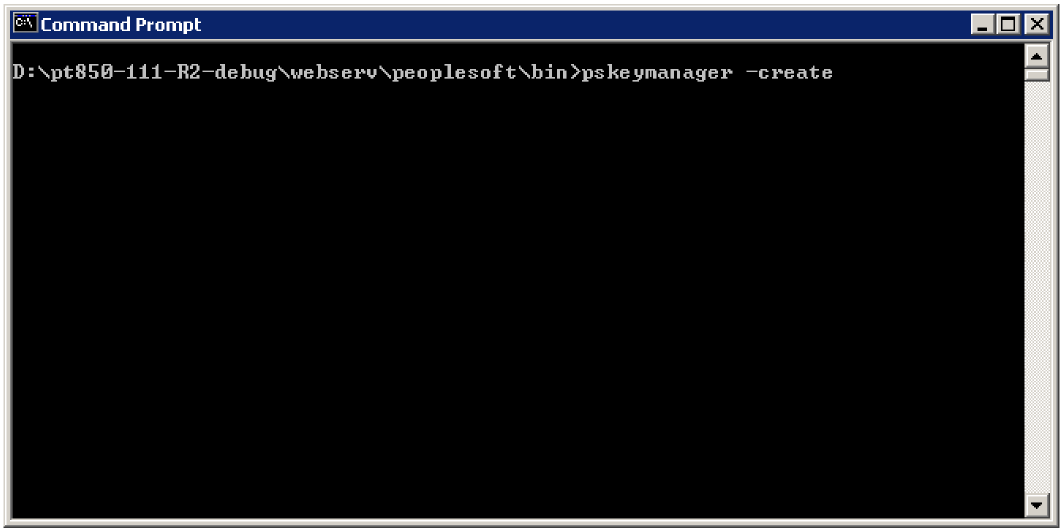
- Generating Signed Public Encryption Key and CSR
- Submitting CSRs to CAs for Signing
- Downloading the Root Certificate
- Importing a Server-Side Public Key into a Keystore
- Generating and Importing Public Keys
- Configuring Oracle WebLogic Server to Use the Keystore
- Adding the Root Certificate
- Configuring the PeopleSoft Certificates

C.1 Generating Signed Public Encryption Key and CSR

To generate signed public encryption key and certificate signing request (CSR):

1. Start PSKeyManager by navigating to the appropriate directory on the MS-DOS command prompt.
2. Enter the following at the command line:

```
pskeymanager -create
```



```
D:\pt850-111-R2-debug\webserv\peoplesoft\bin>pskeymanager -create
```

The PSKeyManager opens.

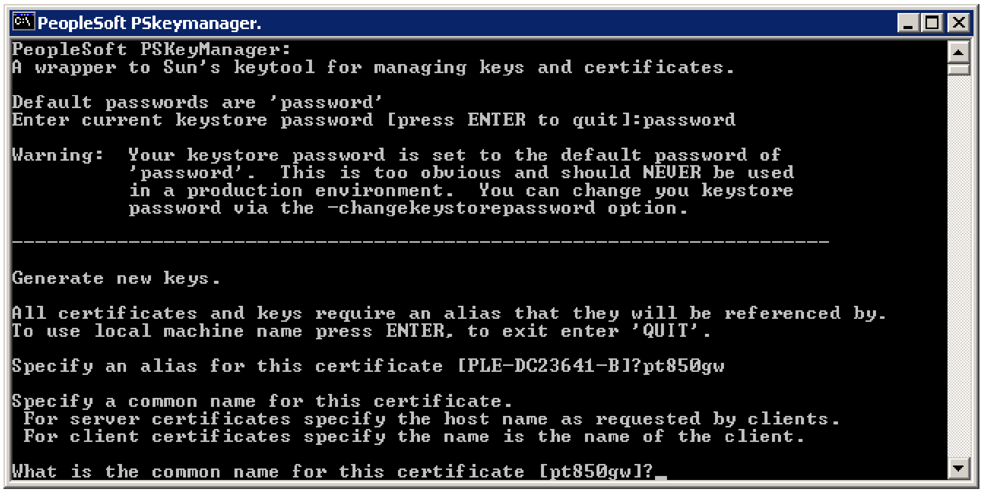
3. Enter the following at the command line:

   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.**



```
PeopleSoft PSKeyManager:
A wrapper to Sun's keytool for managing keys and certificates.

Default passwords are 'password'
Enter current keystore password [press ENTER to quit]:password

Warning:  Your keystore password is set to the default password of
          'password'.  This is too obvious and should NEVER be used
          in a production environment.  You can change you keystore
          password via the -changekeystorepassword option.

----------------------------------------------------------------------

Generate new keys.

All certificates and keys require an alias that they will be referenced by.
To use local machine name press ENTER, to exit enter 'QUIT'.

Specify an alias for this certificate [PLE-DC23641-B]?pt850gw

Specify a common name for this certificate.
 For server certificates specify the host name as requested by clients.
 For client certificates specify the name is the name of the client.

What is the common name for this certificate [pt850gw]?_
```

   Enter the appropriate information at the following command prompts:

   Organization unit

   Organization

   City or Locality

   State or Province

   Country code

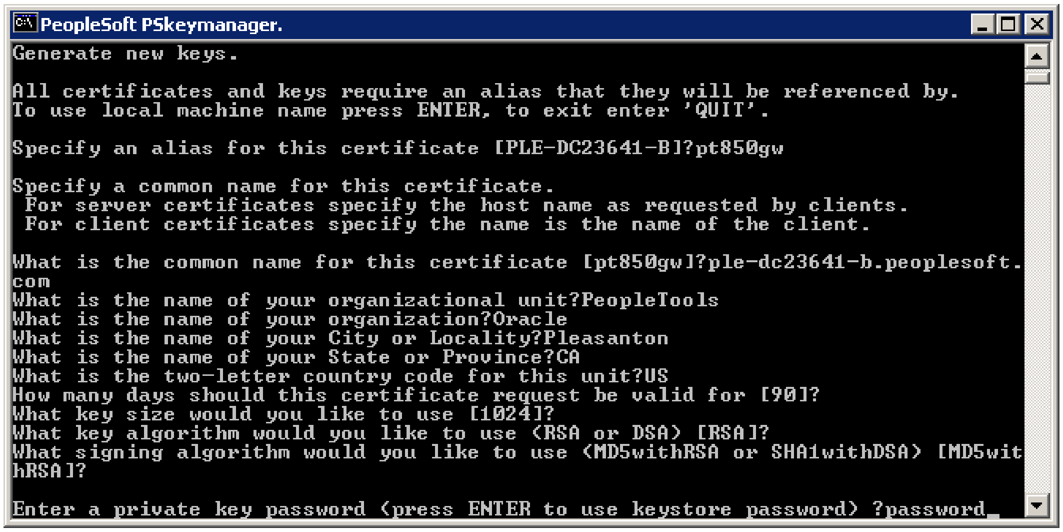
   Number of days the certificate should be valid (Default is 90.)

   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.**



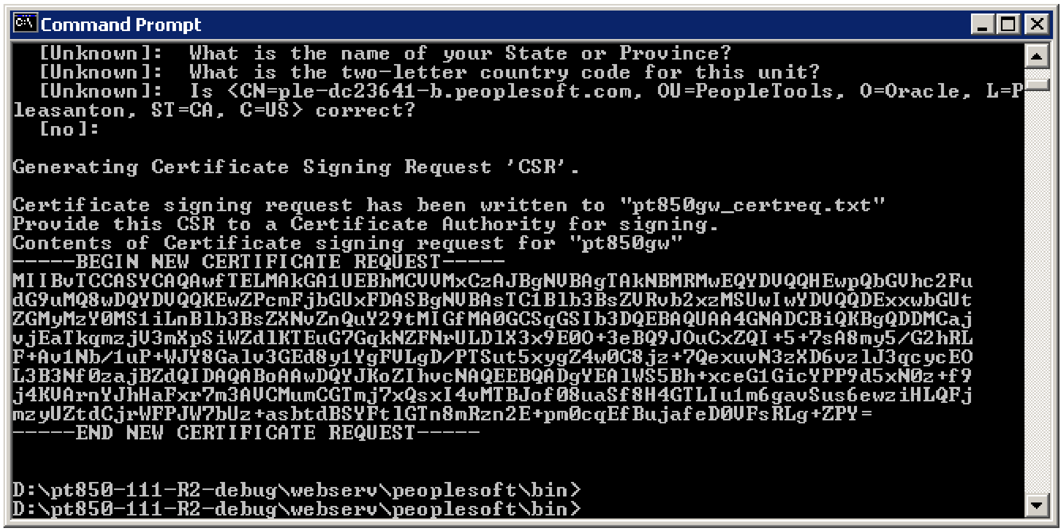
```
Generate new keys.

All certificates and keys require an alias that they will be referenced by.
To use local machine name press ENTER, to exit enter 'QUIT'.

Specify an alias for this certificate [PLE-DC23641-B]?pt850gw

Specify a common name for this certificate.
 For server certificates specify the host name as requested by clients.
 For client certificates specify the name is the name of the client.

What is the common name for this certificate [pt850gw]?ple-dc23641-b.peoplesoft.
com
What is the name of your organizational unit?PeopleTools
What is the name of your organization?Oracle
What is the name of your City or Locality?Pleasanton
What is the name of your State or Province?CA
What is the two-letter country code for this unit?US
How many days should this certificate request be valid for [90]?
What key size would you like to use [1024]?
What key algorithm would you like to use (RSA or DSA) [RSA]?
What signing algorithm would you like to use (MD5withRSA or SHA1withDSA) [MD5wit
hRSA]?

Enter a private key password (press ENTER to use keystore password) ?password_
```

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-----
```



```
  [Unknown]:  What is the name of your State or Province?
  [Unknown]:  What is the two-letter country code for this unit?
  [Unknown]:  Is <CN=ple-dc23641-b.peoplesoft.com, OU=PeopleTools, O=Oracle, L=P
leasanton, ST=CA, C=US> correct?
  [no]:

Generating Certificate Signing Request 'CSR'.

Certificate signing request has been written to "pt850gw_certreq.txt"
Provide this CSR to a Certificate Authority for signing.
Contents of Certificate signing request for "pt850gw"
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBvTCCASYCAQAwfTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMRMwEQYDVQQHEwpQbGVhc2Fu
dG9uMQ8wDQYDVQQKEwZPcmFjbGUxFDASBgNVBAsTC1Blb3BsZVRvb2xzMSUwIwYDVQQDExxwbGUt
ZGMyMzY0MS1iLnBlb3BsZXNvZnQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDMCaj
vjEaTkqmzjV3mXpSiWZdlKTEuG7GqkNZFNrULDlX3x9E0O+3eBQ9JOuCxZQI+5+7sA8my5/G2hRL
F+Av1Nb/1uP+WJY8Galv3GEd8y1YgFVLgD/PTSut5xygZ4w0C8jz+7QexuvN3zXD6vzlJ3qcycEO
L3B3Nf0zajBZdQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAlWS5Bh+xceG1GicYPP9d5xN0z+f9
j4KVArnYJhHaFxr7m3AVCMumCGTmj7xQsxI4vMTBJof08uaSf8H4GTLIu1m6gavSus6ewziHLQFj
mzyUZtdCjrWFPJW7bUz+asbtdBSYFtlGTn8mRzn2E+pm0cqEfBujafeD0VFsRLg+ZPY=
-----END NEW CERTIFICATE REQUEST-----


D:\pt850-111-R2-debug\webserv\peoplesoft\bin>
D:\pt850-111-R2-debug\webserv\peoplesoft\bin>
```

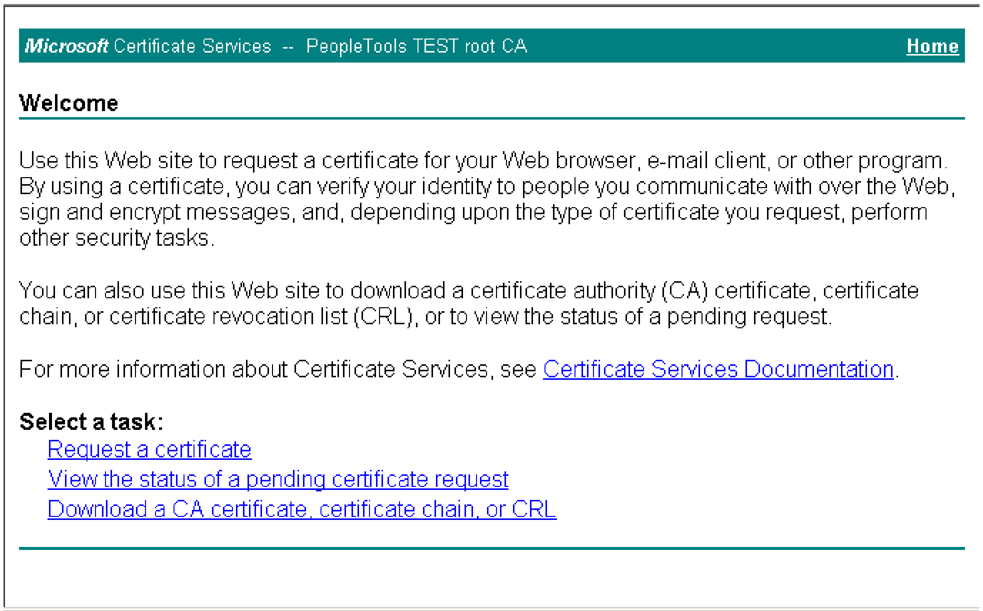
The CSR is a text file, and is written to the <*PSFT_HOME*>\webserv\peoplesoft directory. The file name is <host_name>_certreq.txt.

C.2 Submitting CSRs to CAs for Signing

To 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**.



Microsoft Certificate Services -- PeopleTools TEST root CA **Home**

Welcome

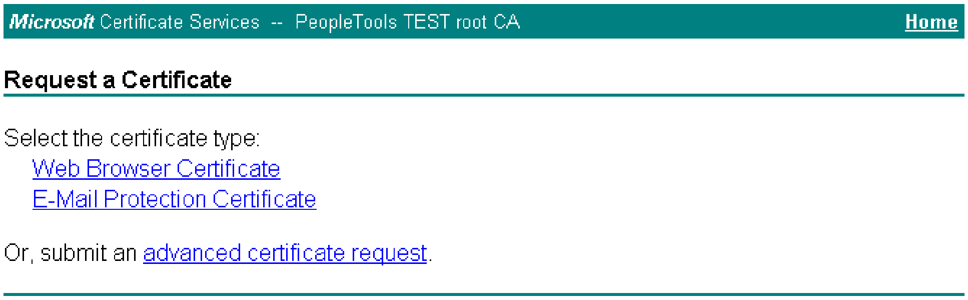
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

2. Click **advanced certificate request.**



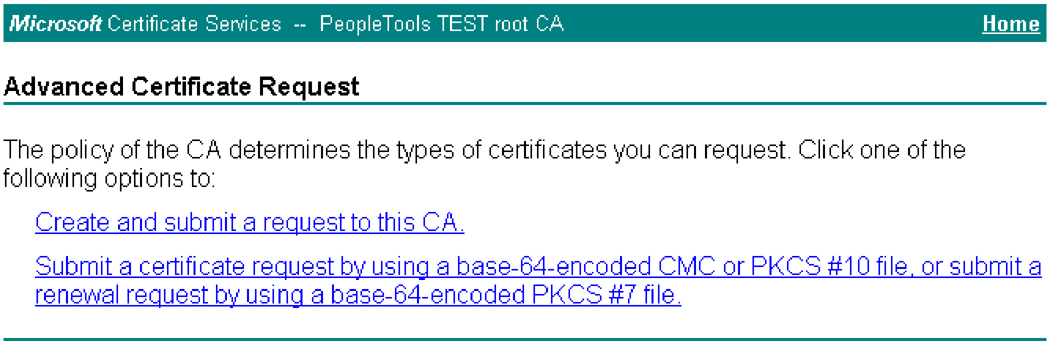
Microsoft Certificate Services -- PeopleTools TEST root CA **Home**

Request a Certificate

Select the certificate type:
Web Browser Certificate
E-Mail Protection Certificate

Or, submit an 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.**



Microsoft Certificate Services -- PeopleTools TEST root CA — **Home**

Advanced Certificate Request

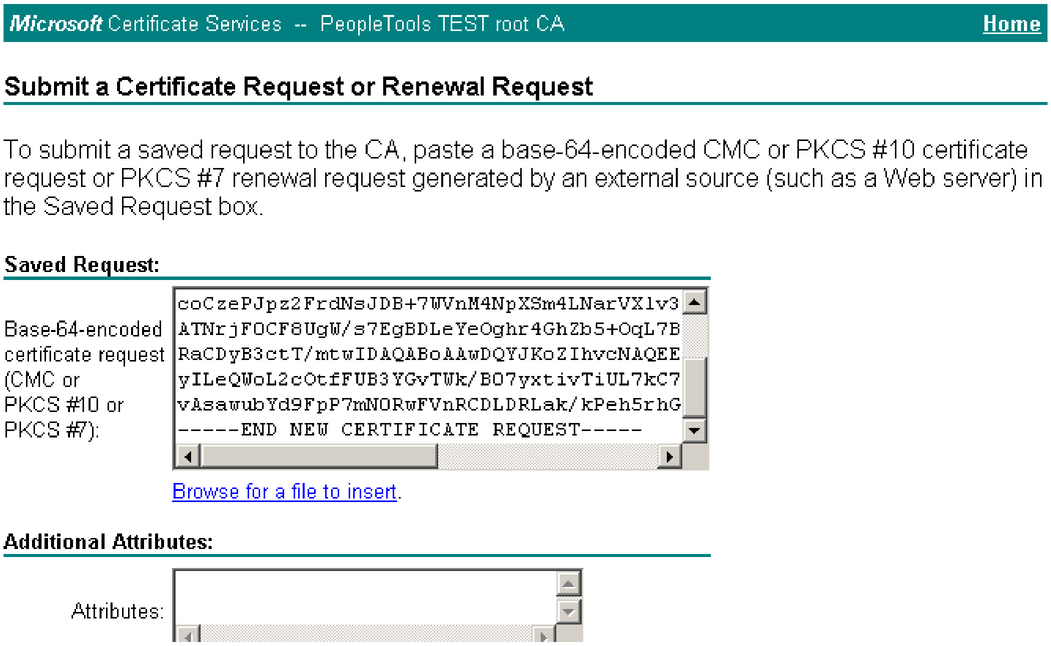
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

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.



Microsoft Certificate Services -- PeopleTools TEST root CA — **Home**

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
coCzePJpz2FrdNsJDB+7WVnM4NpXSm4LNarVXlv3
ATNrjFOCF8UgW/s7EgBDLeYeOghr4GhZb5+OqL7B
RaCDyB3ctT/mtwIDAQABoAAwDQYJKoZIhvcNAQEE
yILeQWoL2cOtfFUB3YGvTWk/BO7yxtivTiUL7kC7
vAsawubYd9FpP7mNORwFVnRCDLDRLak/kPeh5rhG
-----END NEW CERTIFICATE REQUEST-----
```

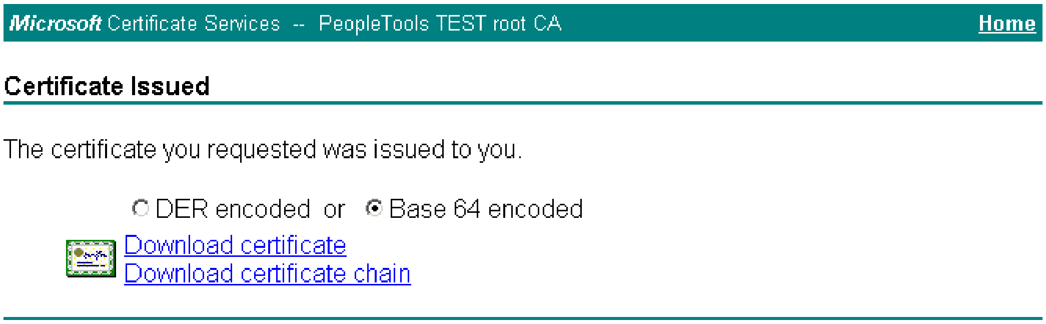
Browse for a file to insert.

Additional Attributes:

Attributes:

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.



Microsoft Certificate Services -- PeopleTools TEST root CA — **Home**

Certificate Issued

The certificate you requested was issued to you.

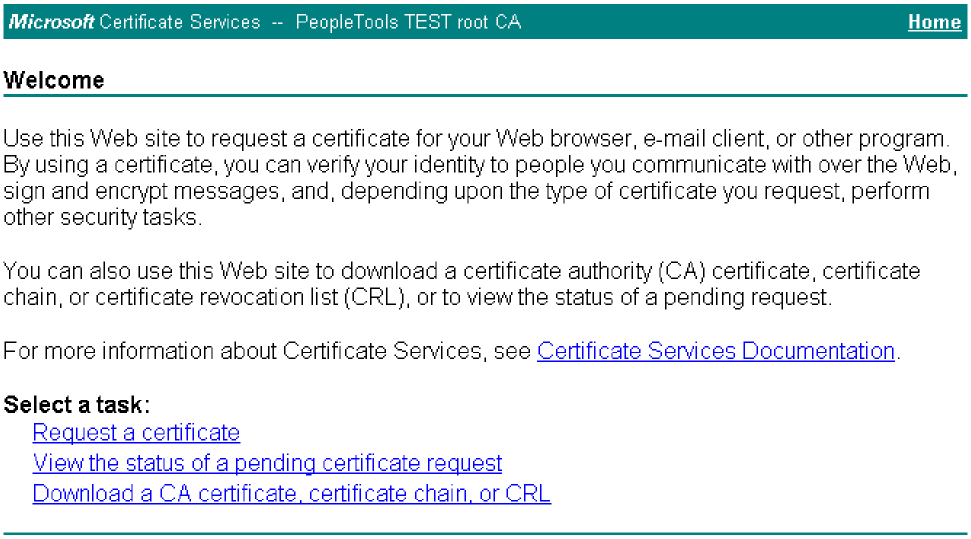
○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

C.3 Downloading the Root Certificate

To download the root certificate:

1. Click **Download a CA certificate, certificate chain, or CRL.**



Welcome

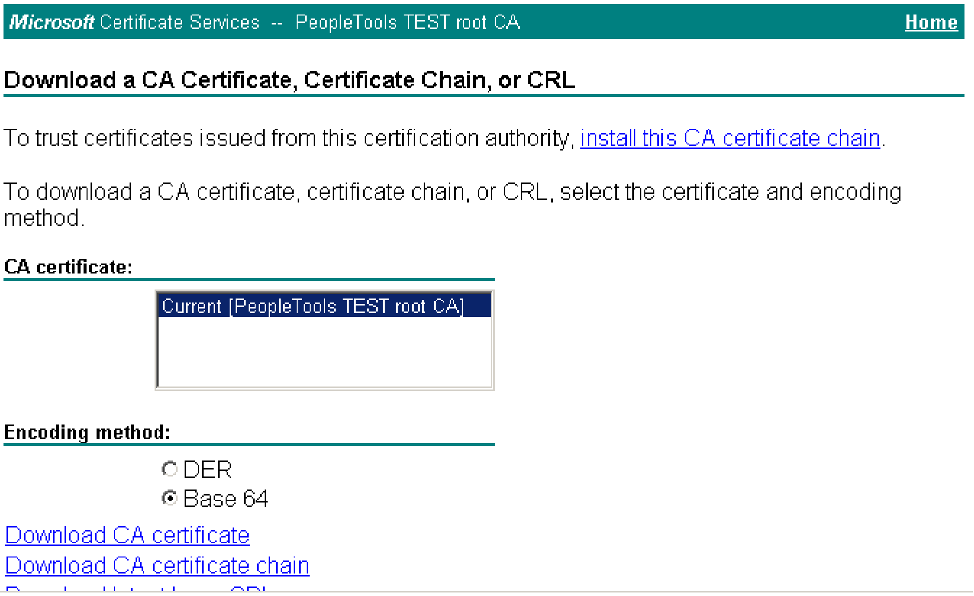
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

2. From the **CA certificate** list, select the certificate.



Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:
Current [PeopleTools TEST root CA]

Encoding method:
○ DER
● Base 64

Download CA certificate
Download CA certificate chain

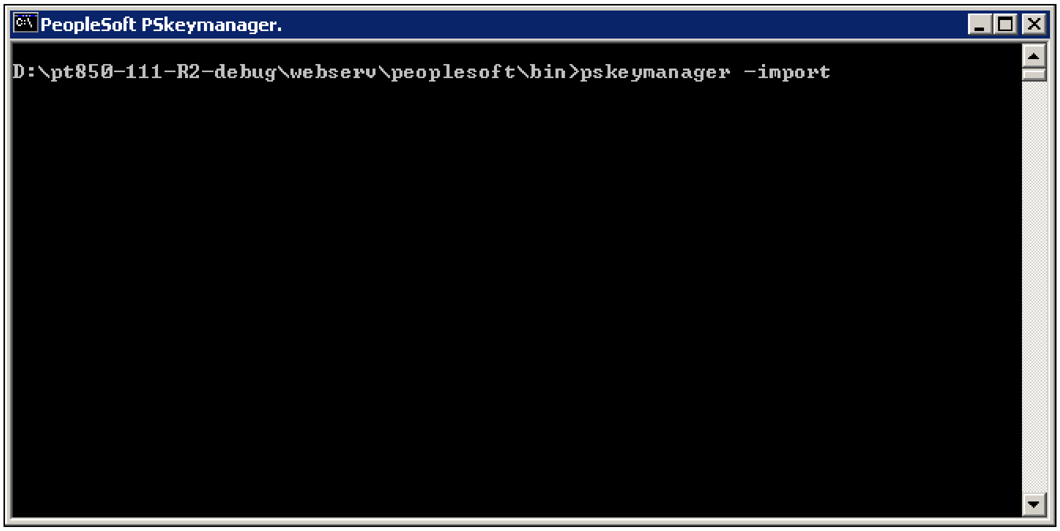
3. Download and save the root certificate on your local drive.

C.4 Importing a Server-Side Public Key into a Keystore

To import a server-side public key into a keystore:

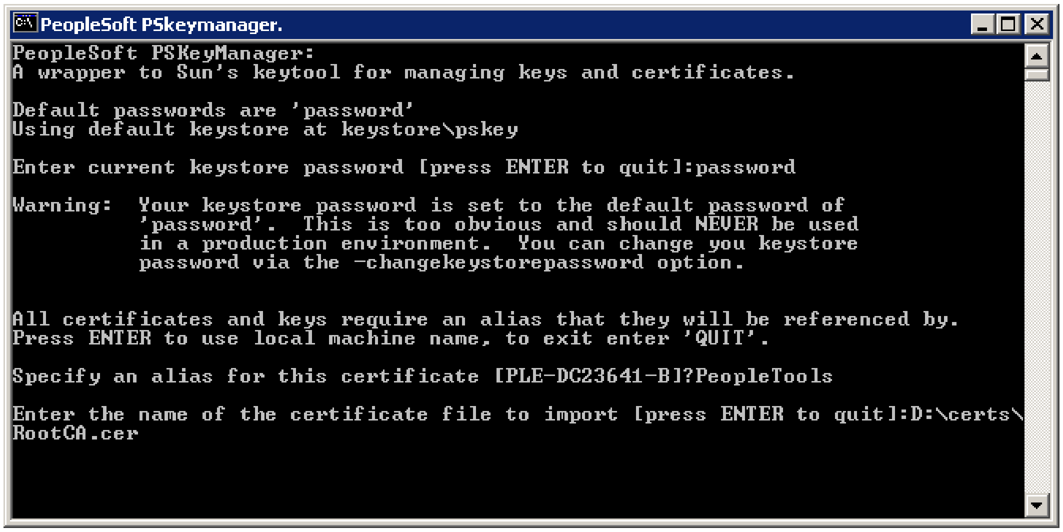
1. Open PSKeyManager.
2. Navigate to the required directory on the MS-DOS command prompt.
3. Enter the following at the command line:

   ```
   pskeymanager -import
   ```



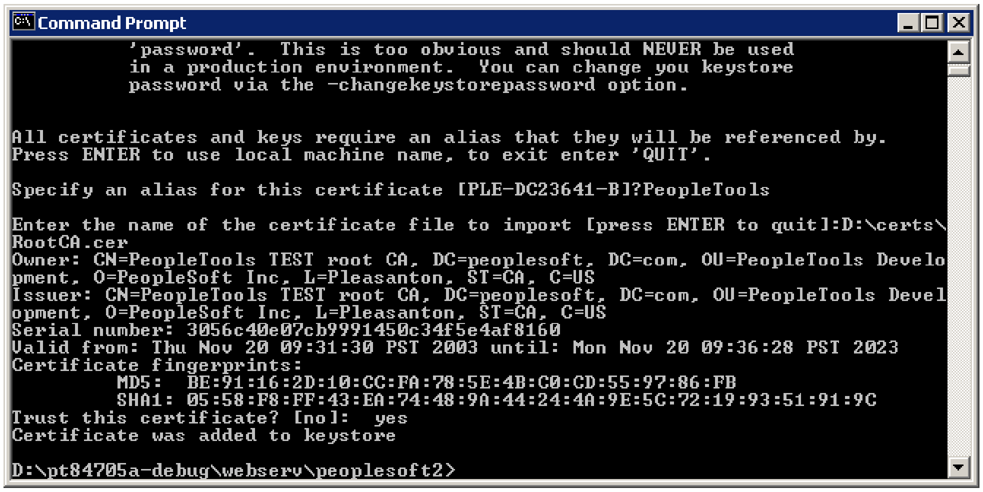
```
D:\pt850-111-R2-debug\webserv\peoplesoft\bin>pskeymanager -import
```

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.



```
PeopleSoft PSKeyManager:
A wrapper to Sun's keytool for managing keys and certificates.

Default passwords are 'password'
Using default keystore at keystore\pskey

Enter current keystore password [press ENTER to quit]:password

Warning:  Your keystore password is set to the default password of
          'password'.  This is too obvious and should NEVER be used
          in a production environment.  You can change you keystore
          password via the -changekeystorepassword option.


All certificates and keys require an alias that they will be referenced by.
Press ENTER to use local machine name, to exit enter 'QUIT'.

Specify an alias for this certificate [PLE-DC23641-B]?PeopleTools

Enter the name of the certificate file to import [press ENTER to quit]:D:\certs\
RootCA.cer
```

7. At the `Trust this certificate` command prompt, enter **Yes** and press **Enter.**



```
          'password'.  This is too obvious and should NEVER be used
          in a production environment.  You can change you keystore
          password via the -changekeystorepassword option.


All certificates and keys require an alias that they will be referenced by.
Press ENTER to use local machine name, to exit enter 'QUIT'.

Specify an alias for this certificate [PLE-DC23641-B]?PeopleTools

Enter the name of the certificate file to import [press ENTER to quit]:D:\certs\
RootCA.cer
Owner: CN=PeopleTools TEST root CA, DC=peoplesoft, DC=com, OU=PeopleTools Develo
pment, O=PeopleSoft Inc, L=Pleasanton, ST=CA, C=US
Issuer: CN=PeopleTools TEST root CA, DC=peoplesoft, DC=com, OU=PeopleTools Devel
opment, O=PeopleSoft Inc, L=Pleasanton, ST=CA, C=US
Serial number: 3056c40e07cb9991450c34f5e4af8160
Valid from: Thu Nov 20 09:31:30 PST 2003 until: Mon Nov 20 09:36:28 PST 2023
Certificate fingerprints:
         MD5:  BE:91:16:2D:10:CC:FA:78:5E:4B:C0:CD:55:97:86:FB
         SHA1: 05:58:F8:FF:43:EA:74:48:9A:44:24:4A:9E:5C:72:19:93:51:91:9C
Trust this certificate? [no]:  yes
Certificate was added to keystore

D:\pt84705a-debug\webserv\peoplesoft2>
```

C.5 Generating and Importing Public Keys

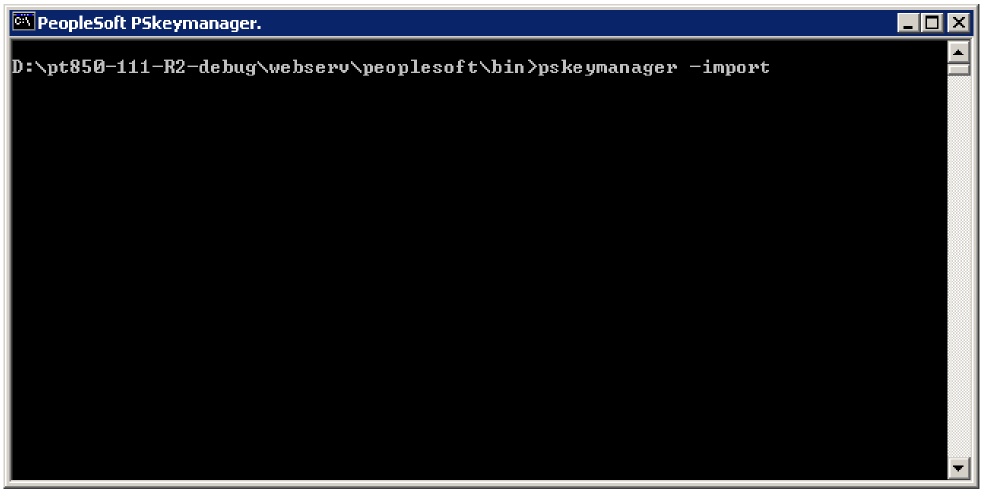
To generate and import public keys:

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
   ```

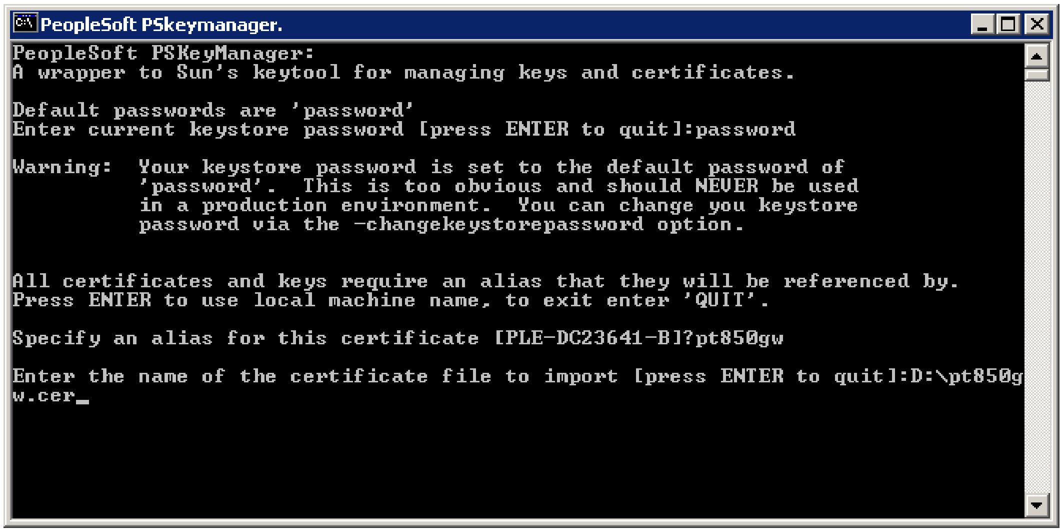


```
D:\pt850-111-R2-debug\webserv\peoplesoft\bin>pskeymanager -import
```

3. At the `Enter current keystore password` command prompt, enter the password and press **Enter.**

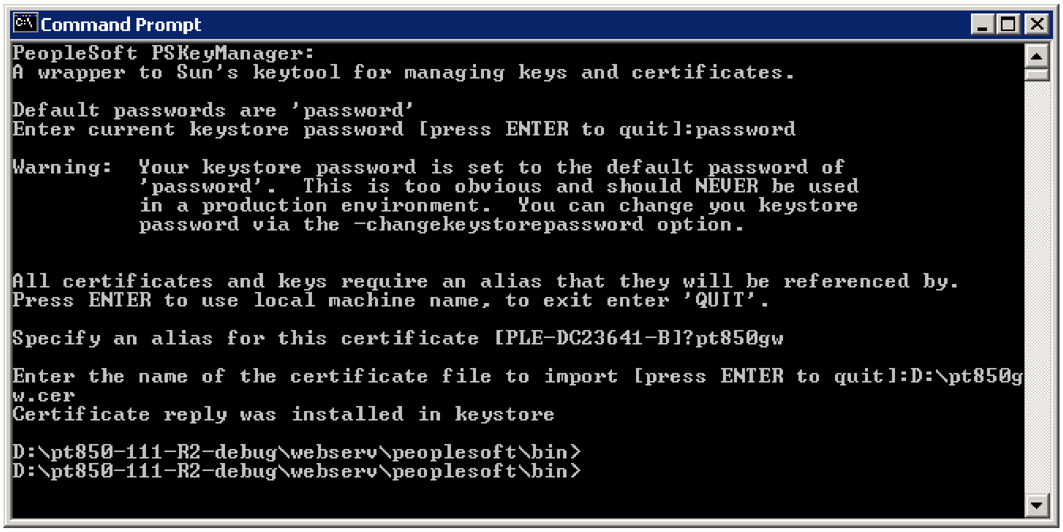
4. At the `Specify an alias for this certificate <host_name>?` command prompt, enter the certificate alias and press **Enter.**

5. At the `Enter the name of the certification file to import` command prompt, enter the path and name of the certificate to import.



```
PeopleSoft PSKeyManager:
A wrapper to Sun's keytool for managing keys and certificates.

Default passwords are 'password'
Enter current keystore password [press ENTER to quit]:password

Warning:  Your keystore password is set to the default password of
          'password'.  This is too obvious and should NEVER be used
          in a production environment.  You can change you keystore
          password via the -changekeystorepassword option.


All certificates and keys require an alias that they will be referenced by.
Press ENTER to use local machine name, to exit enter 'QUIT'.

Specify an alias for this certificate [PLE-DC23641-B]?pt850gw

Enter the name of the certificate file to import [press ENTER to quit]:D:\pt850g
w.cer_
```

Certificate is successfully installed in the keystore.

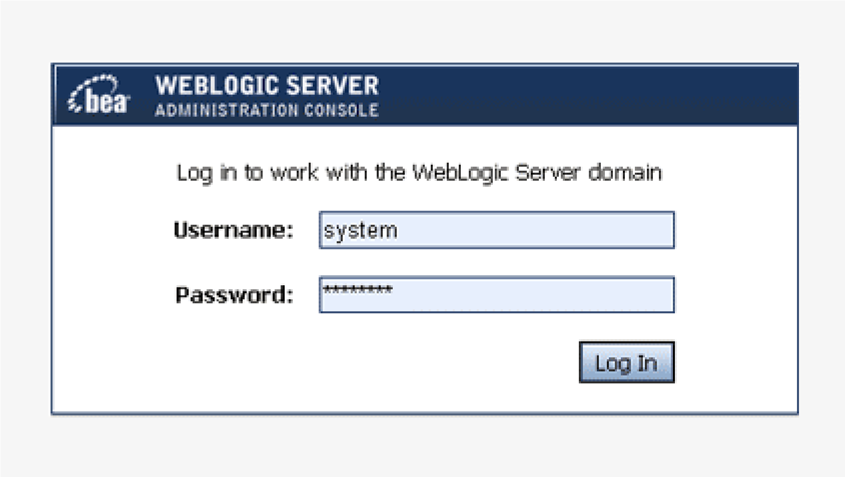


```
PeopleSoft PSKeyManager:
A wrapper to Sun's keytool for managing keys and certificates.

Default passwords are 'password'
Enter current keystore password [press ENTER to quit]:password

Warning:  Your keystore password is set to the default password of
          'password'.  This is too obvious and should NEVER be used
          in a production environment.  You can change you keystore
          password via the -changekeystorepassword option.


All certificates and keys require an alias that they will be referenced by.
Press ENTER to use local machine name, to exit enter 'QUIT'.

Specify an alias for this certificate [PLE-DC23641-B]?pt850gw

Enter the name of the certificate file to import [press ENTER to quit]:D:\pt850g
w.cer
Certificate reply was installed in keystore

D:\pt850-111-R2-debug\webserv\peoplesoft\bin>
D:\pt850-111-R2-debug\webserv\peoplesoft\bin>
```

C.6 Configuring Oracle WebLogic Server to Use the Keystore

To configure the Oracle WebLogic Server to use the keystore:

1. Log in to Oracle WebLogic Administration Console.

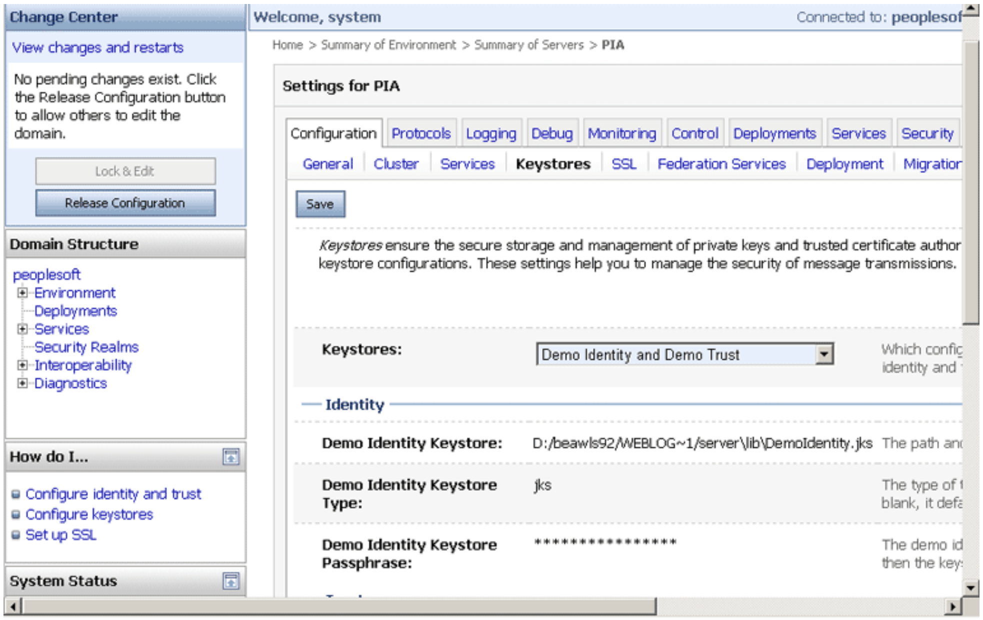


Log in to work with the WebLogic Server domain

Username: system

Password: ********

2. Expand **PeopleSoft, Environment, Servers, PIA** to setup the SSL configuration for the PIA server.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Settings for PIA

Keystores ensure the secure storage and management of private keys and trusted certificate author keystore configurations. These settings help you to manage the security of message transmissions.

Keystores: Demo Identity and Demo Trust — Which config identity and

Identity

Demo Identity Keystore: D:/beawls92/WEBLOG~1/server\lib\DemoIdentity.jks — The path an

Demo Identity Keystore Type: jks — The type of blank, it defa

Demo Identity Keystore Passphrase: **************** — The demo id then the key

3. Click the **Keystores** tab.

4. From the **Keystores** list, select **Custom Identity and Custom Trust.**

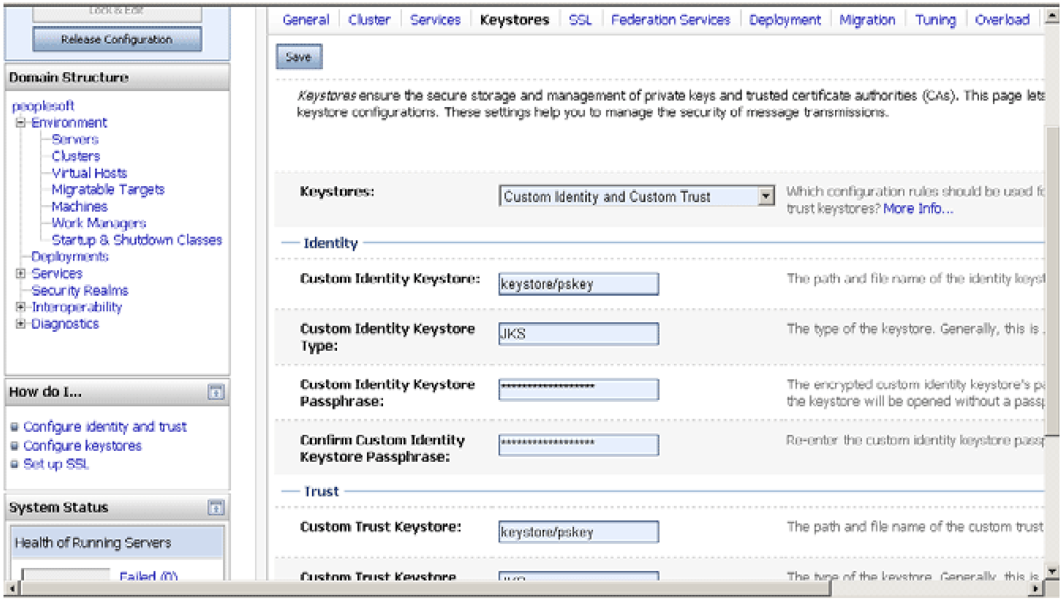
5. In the **Identity** region, complete the following fields:

- 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.



Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets
keystore configurations. These settings help you to manage the security of message transmissions.

Keystores: Custom Identity and Custom Trust — Which configuration rules should be used fo
trust keystores? More Info...

Custom Identity Keystore: keystore/pskey — The path and file name of the identity keyst

Custom Identity Keystore Type: JKS — The type of the keystore. Generally, this is .

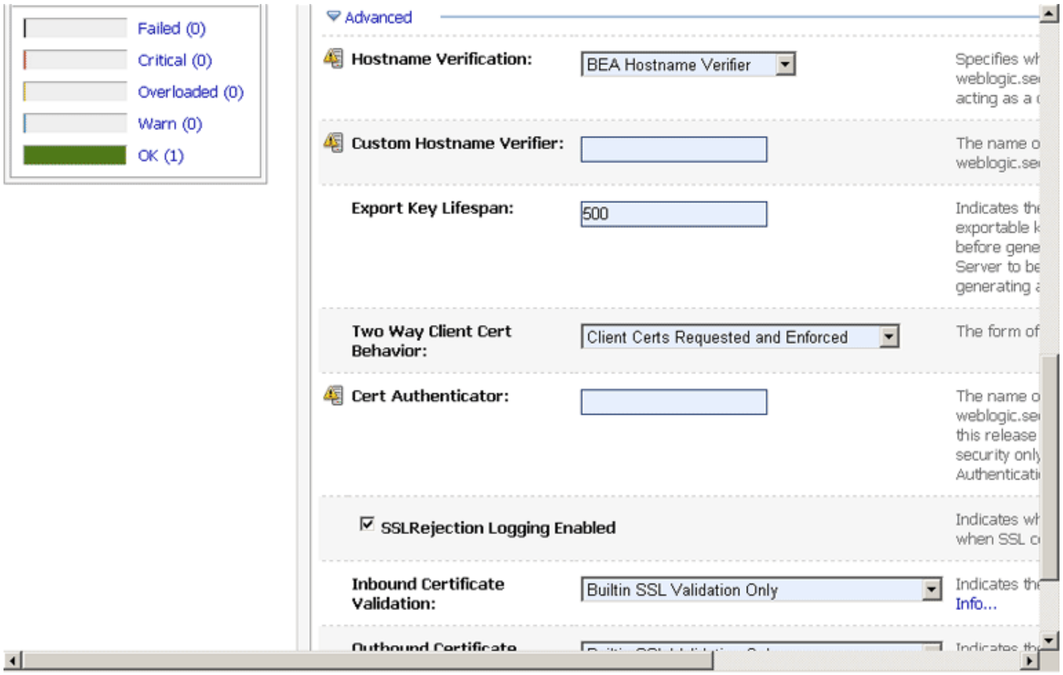
Custom Identity Keystore Passphrase: •••••••••••••••••• — The encrypted custom identity keystore's pa
the keystore will be opened without a passp

Confirm Custom Identity Keystore Passphrase: •••••••••••••••••• — Re-enter the custom identity keystore passp

Custom Trust Keystore: keystore/pskey — The path and file name of the custom trust

Custom Trust Keystore — The type of the keystore. Generally, this is

6. On the SSL tab, ensure that the parameter **Two Way Client Cert Behavior** is set to **Client Certs Requested and Enforced.**



Hostname Verification: BEA Hostname Verifier — Specifies wh
weblogic.se
acting as a c

Custom Hostname Verifier: — The name o
weblogic.se

Export Key Lifespan: 500 — Indicates the
exportable k
before gene
Server to be
generating a

Two Way Client Cert Behavior: Client Certs Requested and Enforced — The form of

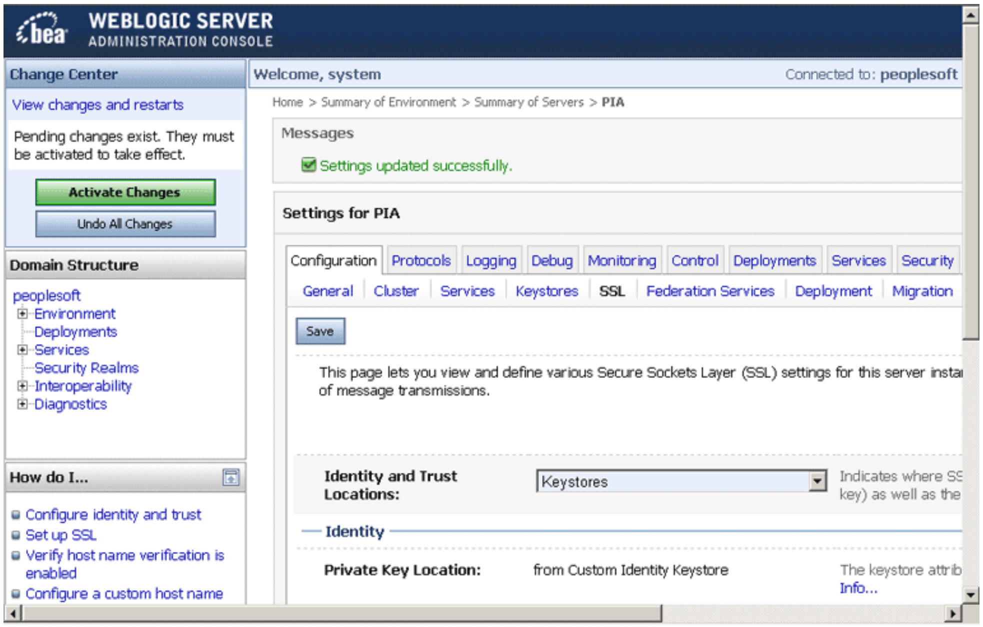
Cert Authenticator: — The name o
weblogic.se
this release
security only
Authenticati

☑ SSLRejection Logging Enabled — Indicates wh
when SSL c

Inbound Certificate Validation: Builtin SSL Validation Only — Indicates the
Info...

Outbound Certificate — Indicates th

7. Click the **Activate Changes** button.



Pending changes exist. They must be activated to take effect.

Messages

✓ Settings updated successfully.

Settings for PIA

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instai of message transmissions.

Identity and Trust Locations: Keystores ▾ Indicates where SS key) as well as the

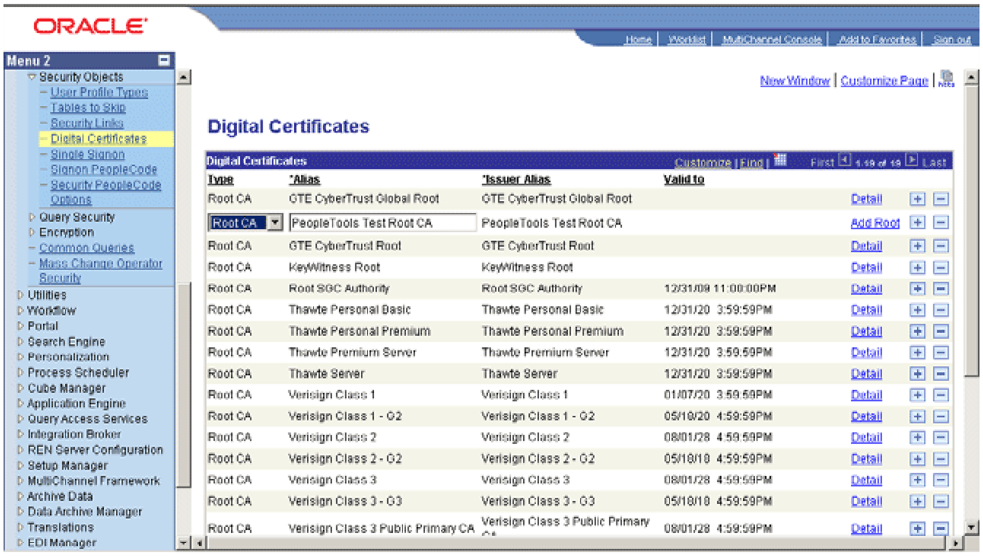
Identity

Private Key Location: from Custom Identity Keystore The keystore attrib Info...

C.7 Adding the Root Certificate

To add the root certificate:

1. Expand **Security, Security Objects,** and then click **Digital Certificates.**



Digital Certificates

Digital Certificates

Type	*Alias	*Issuer Alias	Valid to			
Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail	+	−
Root CA ▾	PeopleTools Test Root CA	PeopleTools Test Root CA		Add Root	+	−
Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail	+	−
Root CA	KeyWitness Root	KeyWitness Root		Detail	+	−
Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	Detail	+	−
Root CA	Thawte Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Server	Thawte Server	12/31/20 3:59:59PM	Detail	+	−
Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	Detail	+	−
Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	Detail	+	−
Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	Detail	+	−
Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	05/18/18 4:59:59PM	Detail	+	−
Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	Detail	+	−
Root CA	Verisign Class 3 - G3	Verisign Class 3 - G3	05/18/18 4:59:59PM	Detail	+	−
Root CA	Verisign Class 3 Public Primary CA	Verisign Class 3 Public Primary CA	08/01/28 4:59:59PM	Detail	+	−

2. Click **Add Root.**

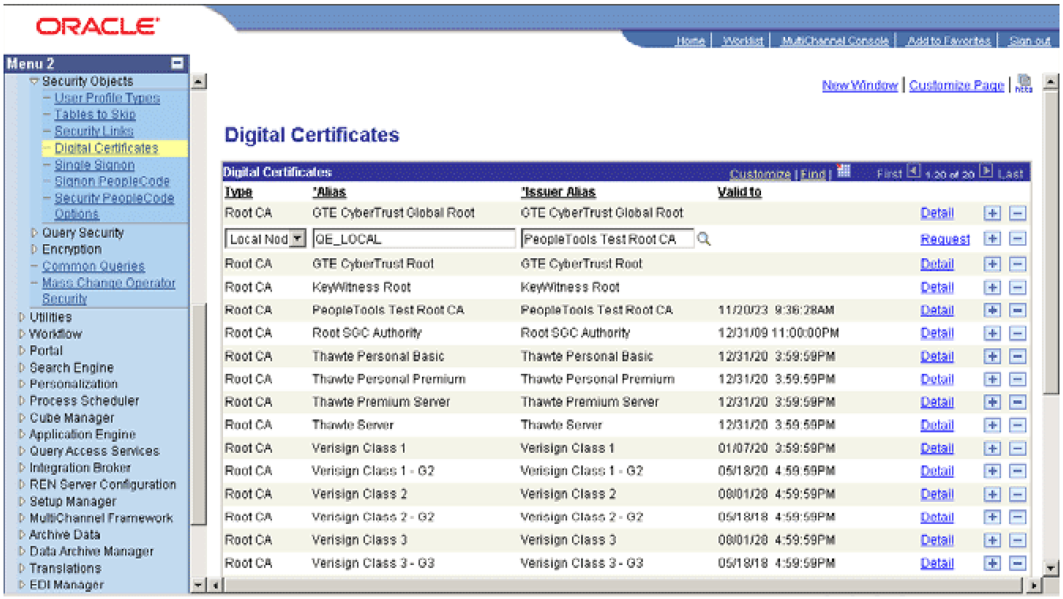
C.8 Configuring the PeopleSoft Certificates

To 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.

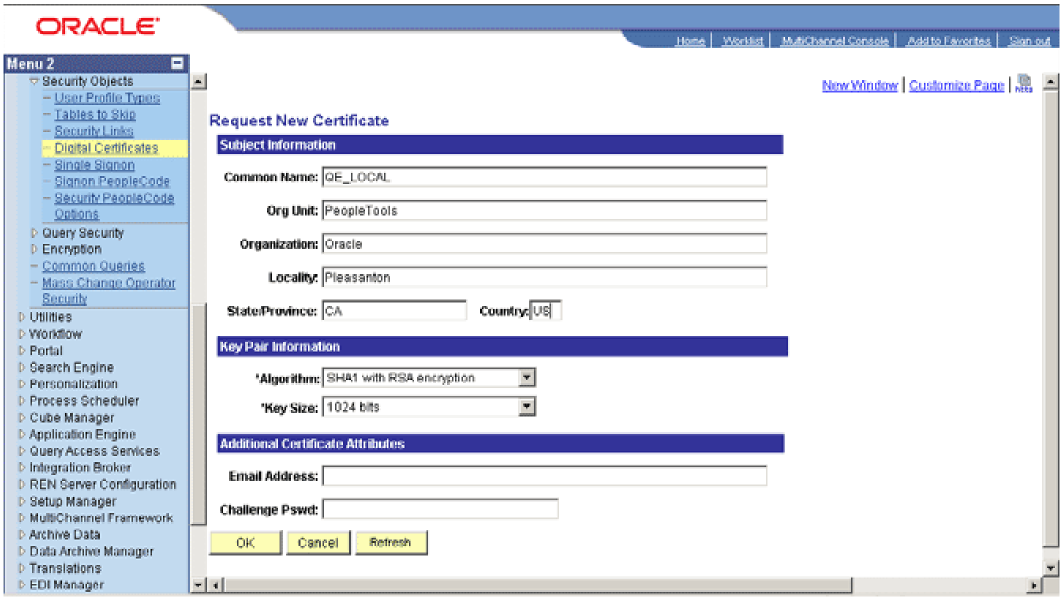


Digital Certificates

Digital Certificates

Type	*Alias	*Issuer Alias	Valid to			
Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail	+	−
Local Nod	QE_LOCAL	PeopleTools Test Root CA		Request	+	−
Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail	+	−
Root CA	KeyWitness Root	KeyWitness Root		Detail	+	−
Root CA	PeopleTools Test Root CA	PeopleTools Test Root CA	11/20/23 9:36:28AM	Detail	+	−
Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	Detail	+	−
Root CA	Thawte Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Server	Thawte Server	12/31/20 3:59:59PM	Detail	+	−
Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	Detail	+	−
Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	Detail	+	−
Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	Detail	+	−
Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	05/18/18 4:59:59PM	Detail	+	−
Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	Detail	+	−
Root CA	Verisign Class 3 - G3	Verisign Class 3 - G3	05/18/18 4:59:59PM	Detail	+	−

4. Click **Request.**
5. Send this certificate request to the CA to get a new certificate.



Request New Certificate

Subject Information

Common Name: QE_LOCAL

Org Unit: PeopleTools

Organization: Oracle

Locality: Pleasanton

State/Province: CA   Country: US

Key Pair Information

*Algorithm: SHA1 with RSA encryption

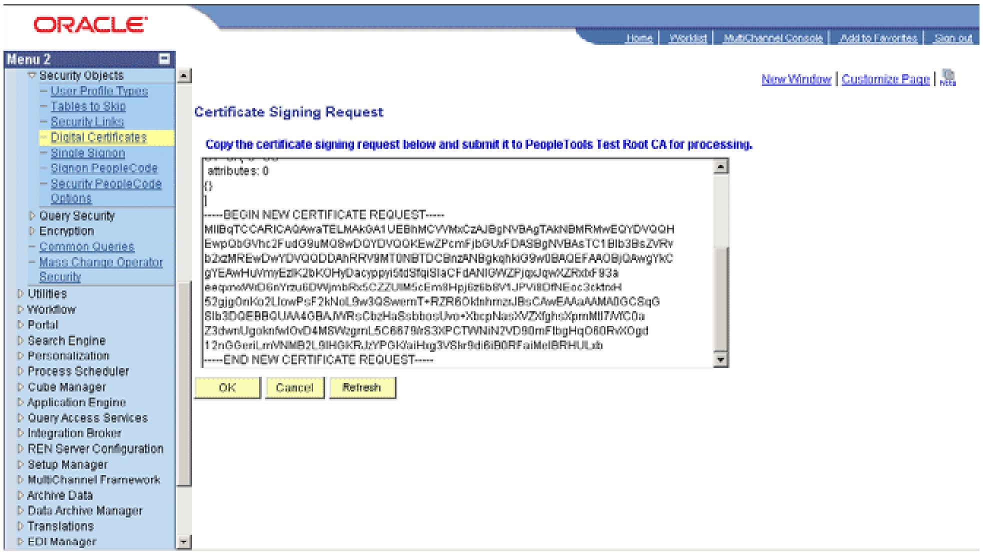
*Key Size: 1024 bits

Additional Certificate Attributes

Email Address:

Challenge Pswd:

6. Click **OK.**

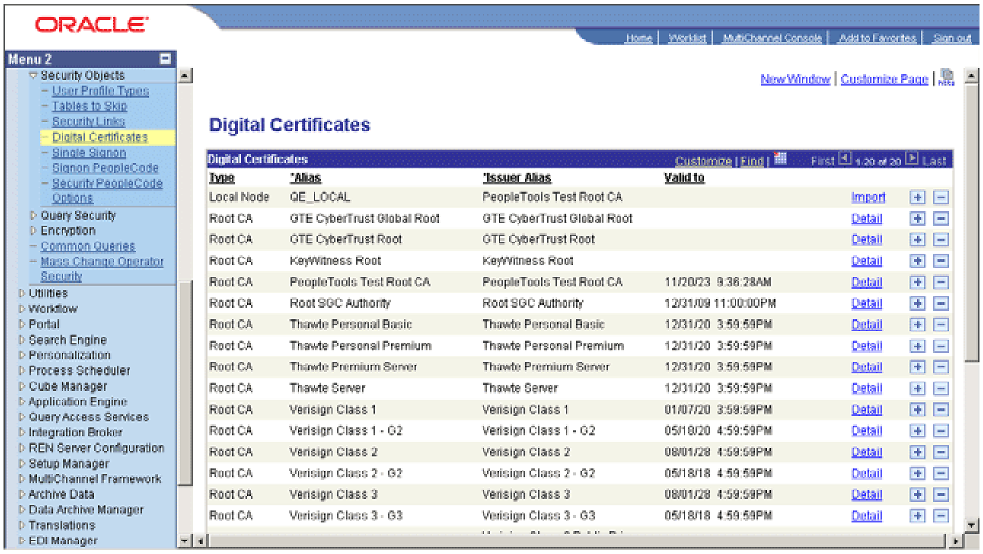


Certificate Signing Request

Copy the certificate signing request below and submit it to PeopleTools Test Root CA for processing.

```
 attributes: 0
{}
]
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBqTCCARICAQAwaTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMRMwEQYDVQQH
EwpQbGVhc2FudG9uMQ8wDQYDVQQKEwZPcmFjbGUxFDASBgNVBAsTC1BlB3BsZVRv
b2xzMREwDwYDVQQDDAhRRV9MT0NBTDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAwHuVmyEzlK2bKOHyDacyppyi5tdSfqiSIaCFdANIGWZPjqxJqwXZRxtxF93a
eeqrxWrD6nYrzu6DWjmbRx5CZZUlM5cEm8Hpj6z6b8V1JPVi8DfNEoc3cktnxH
52gjg0nKo2LlowPsF2kNoL9w3QSwemT+RZR6OktnhmzJBsCAwEAAaAAMA0GCSqG
SIb3DQEBBQUAA4GBAJWRsCbzHaSsbbosUvo+XbcpNasXVZXfghsXpmMlI7MC0a
Z3dwnUgoknfwIOvD4MSWzgmL5C6879rS3XPCTWNiN2VD90mFIbgHqO80RvXOgd
12nGGeriLmVNMB2L9IHGKRJzYPGK/aiHxg3VSkr9di6iB0RFaiMeIBRHULxb
-----END NEW CERTIFICATE REQUEST-----
```

7. Ensure that the local node appears on the Digital Certificates list.



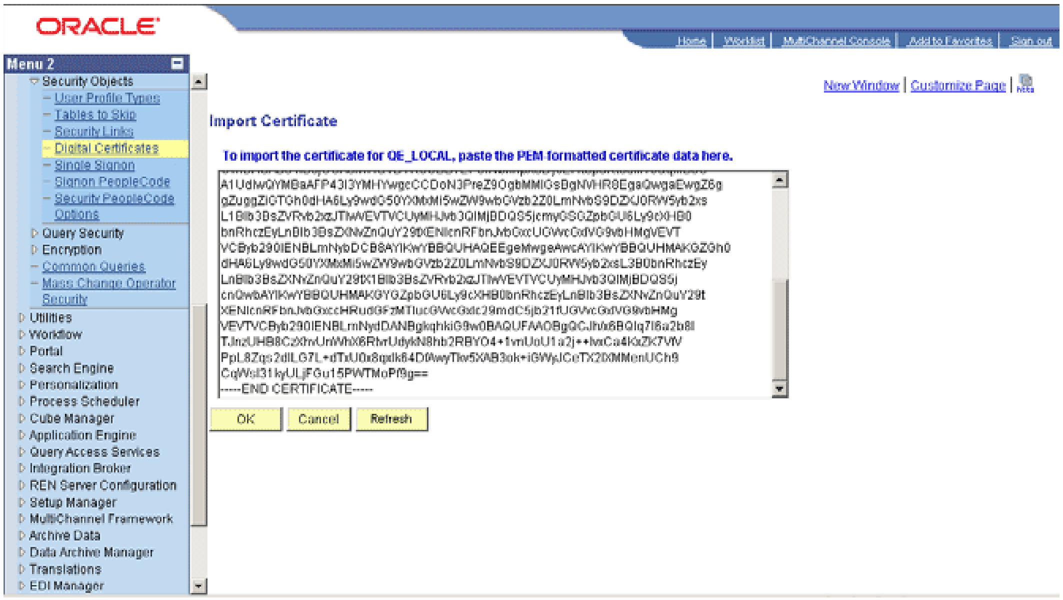
Digital Certificates

Digital Certificates

Type	*Alias	*Issuer Alias	Valid to			
Local Node	QE_LOCAL	PeopleTools Test Root CA		Import	+	−
Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail	+	−
Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail	+	−
Root CA	KeyWitness Root	KeyWitness Root		Detail	+	−
Root CA	PeopleTools Test Root CA	PeopleTools Test Root CA	11/20/23 9:36:28AM	Detail	+	−
Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	Detail	+	−
Root CA	Thawte Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Server	Thawte Server	12/31/20 3:59:59PM	Detail	+	−
Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	Detail	+	−
Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	Detail	+	−
Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	Detail	+	−
Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	05/18/18 4:59:59PM	Detail	+	−
Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	Detail	+	−
Root CA	Verisign Class 3 - G3	Verisign Class 3 - G3	05/18/18 4:59:59PM	Detail	+	−

8. Click **Import.**

The Import Certificate page appears.

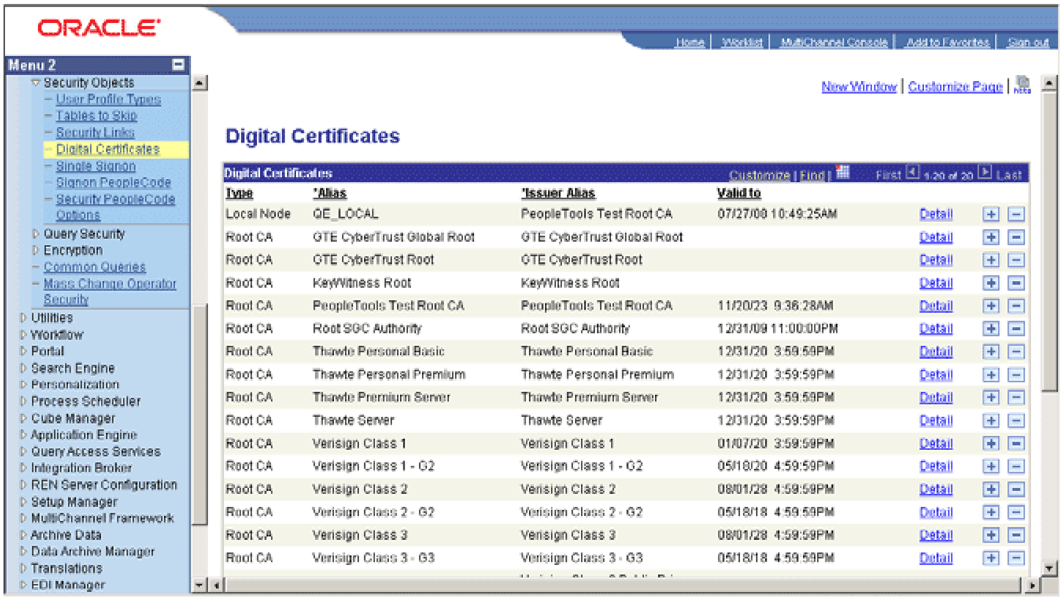


Import Certificate

To import the certificate for QE_LOCAL, paste the PEM formatted certificate data here.

```
A1UdIwQYMBaAFP43I3YMHYwgcCCDoN3PreZ9OgbMMIGsBgNVHR8EgaQwgaEwgZ6g
gZuggZiGTGh0dHA6Ly9wdG50YXMxMi5wZW9wbGVzb2Z0LmNvbS9DZXJ0RW5yb2xs
L1Blb3BsZVRvb2xzJTIwVEVTVCUyMHJvb3QlMjBDQS5jcmyGSGZpbGU6Ly9cXHB0
bnRhczEyLnBlb3BsZXNvZnQuY29tXENlcnRFbnJvbGxcUGVvcGxlVG9vbHMgVEVT
VCByb290IENBLmNybDCB8AYIKwYBBQUHAQEEgeMwgeAwcAYIKwYBBQUHMAKGZGh0
dHA6Ly9wdG50YXMxMi5wZW9wbGVzb2Z0LmNvbS9DZXJ0RW5yb2xsL3B0bnRhczEy
LnBlb3BsZXNvZnQuY29tX1Blb3BsZVRvb2xzJTIwVEVTVCUyMHJvb3QlMjBDQS5j
cnQwbAYIKwYBBQUHMAKGYGZpbGU6Ly9cXHB0bnRhczEyLnBlb3BsZXNvZnQuY29t
XENlcnRFbnJvbGxccHRudGFzMTIucGVvcGxlc29mdC5jb21fUGVvcGxlVG9vbHMg
VEVTVCByb290IENBLmNydDANBgkqhkiG9w0BAQUFAAOBgQCJh/x6BQIq7I6a2b8I
TJnzUHB8CzXhvUnWhX6RlvrUdykN8hb2RBYO4+1vnUoU1a2j++lwCa4KxZK7VlV
PpL8Zqs2dlLG7L+dTxU0x8qdk84D0wyTlv5XAB3ok+iGWjJCeTX2OXMMenUCh9
CqWsl31kyULjFGu15PWTMoPf9g==
-----END CERTIFICATE-----
```

9. Click **OK**.

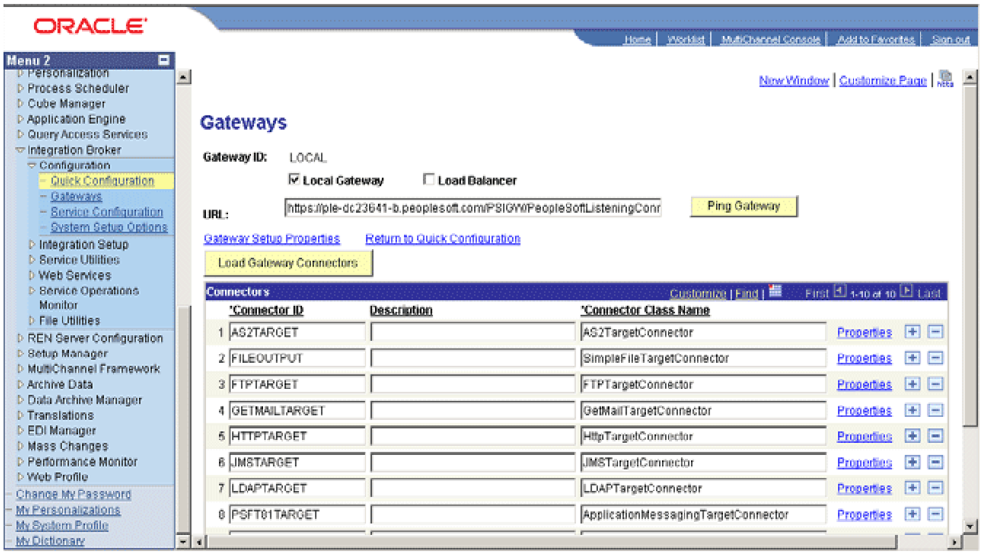


Digital Certificates

Digital Certificates

Type	*Alias	*Issuer Alias	Valid to			
Local Node	QE_LOCAL	PeopleTools Test Root CA	07/27/08 10:49:25AM	Detail	+	−
Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail	+	−
Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail	+	−
Root CA	KeyWitness Root	KeyWitness Root		Detail	+	−
Root CA	PeopleTools Test Root CA	PeopleTools Test Root CA	11/20/23 9:36:28AM	Detail	+	−
Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	Detail	+	−
Root CA	Thawte Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	Detail	+	−
Root CA	Thawte Server	Thawte Server	12/31/20 3:59:59PM	Detail	+	−
Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	Detail	+	−
Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	Detail	+	−
Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	Detail	+	−
Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	05/18/18 4:59:59PM	Detail	+	−
Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	Detail	+	−
Root CA	Verisign Class 3 - G3	Verisign Class 3 - G3	05/18/18 4:59:59PM	Detail	+	−

10. Click **Load Gateway Connectors.**



Gateways

Gateway ID: LOCAL

☑ Local Gateway □ Load Balancer

URL: https://ple-dc23641-b.peoplesoft.com/PSIGW/PeopleSoftListeningConr

Connectors

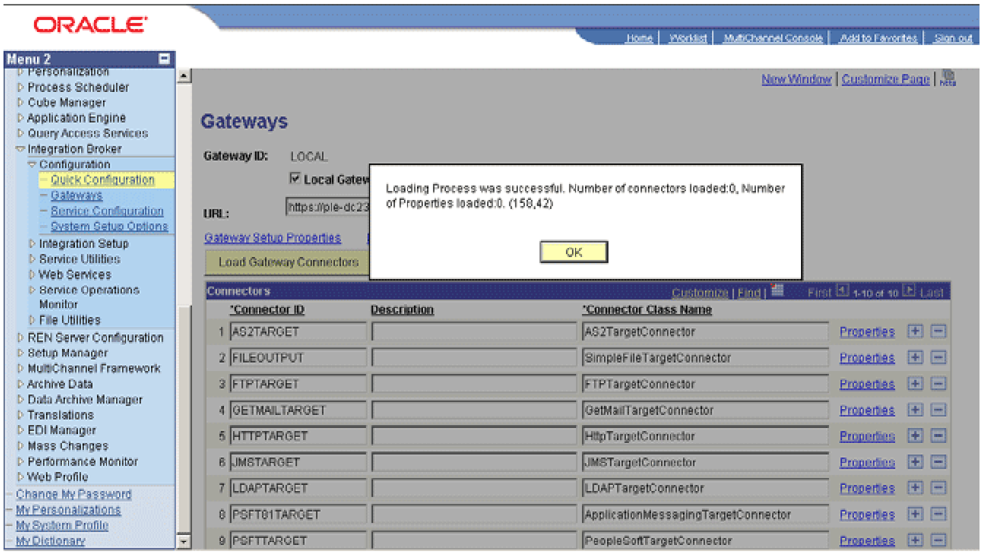
	*Connector ID	Description	*Connector Class Name	
1	AS2TARGET		AS2TargetConnector	Properties
2	FILEOUTPUT		SimpleFileTargetConnector	Properties
3	FTPTARGET		FTPTargetConnector	Properties
4	GETMAILTARGET		GetMailTargetConnector	Properties
5	HTTPTARGET		HttpTargetConnector	Properties
6	JMSTARGET		JMSTargetConnector	Properties
7	LDAPTARGET		LDAPTargetConnector	Properties
8	PSFT81TARGET		ApplicationMessagingTargetConnector	Properties

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.



Gateways

Gateway ID: LOCAL

☑ Local Gatew

URL: https://ple-dc23

Loading Process was successful. Number of connectors loaded:0, Number of Properties loaded:0. (158,42)

Connectors

	*Connector ID	Description	*Connector Class Name	
1	AS2TARGET		AS2TargetConnector	Properties
2	FILEOUTPUT		SimpleFileTargetConnector	Properties
3	FTPTARGET		FTPTargetConnector	Properties
4	GETMAILTARGET		GetMailTargetConnector	Properties
5	HTTPTARGET		HttpTargetConnector	Properties
6	JMSTARGET		JMSTargetConnector	Properties
7	LDAPTARGET		LDAPTargetConnector	Properties
8	PSFT81TARGET		ApplicationMessagingTargetConnector	Properties
9	PSFTTARGET		PeopleSoftTargetConnector	Properties

D

Changing Default Message Versions

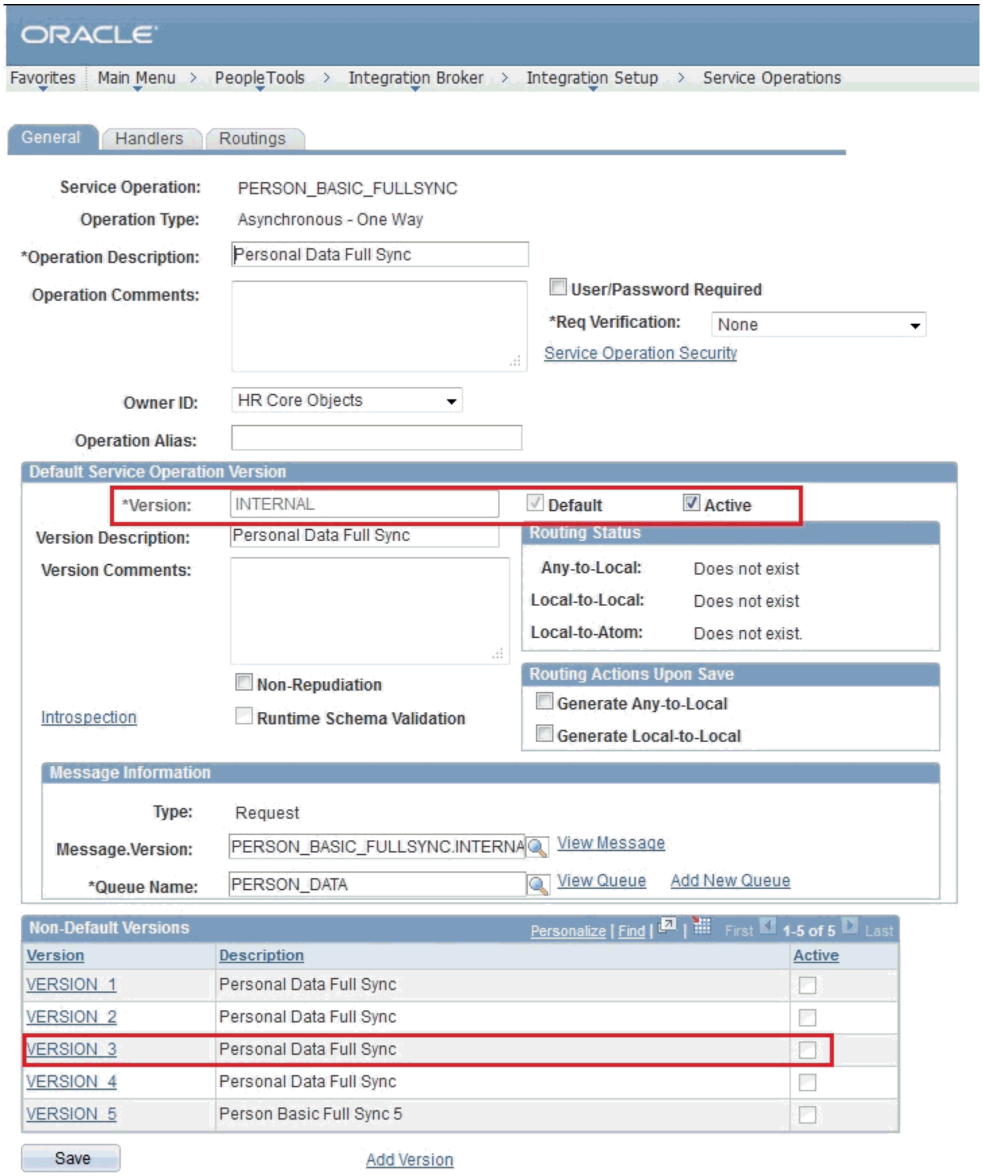
This appendix describes the following procedures:

- Activating a Message Version
- Deactivating a Message Version

D.1 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 PERSON_BASIC_FULLSYNC, in the **Service Operation** field. Then, click **Search.**
3. The following screenshot displays INTERNAL message set as active and default. To set VERSION_3 as Default and Active, click the VERSION_3 link.



Service Operation: PERSON_BASIC_FULLSYNC

Operation Type: Asynchronous - One Way

*Operation Description: Personal Data Full Sync

Operation Comments:

□ User/Password Required

*Req Verification: None

Service Operation Security

Owner ID: HR Core Objects

Operation Alias:

Default Service Operation Version

*Version: INTERNAL ☑ Default ☑ Active

Version Description: Personal Data Full Sync

Version Comments:

□ Non-Repudiation

Introspection □ Runtime Schema Validation

Routing Status

Any-to-Local: Does not exist

Local-to-Local: Does not exist

Local-to-Atom: Does not exist.

Routing Actions Upon Save

□ Generate Any-to-Local

□ Generate Local-to-Local

Message Information

Type: Request

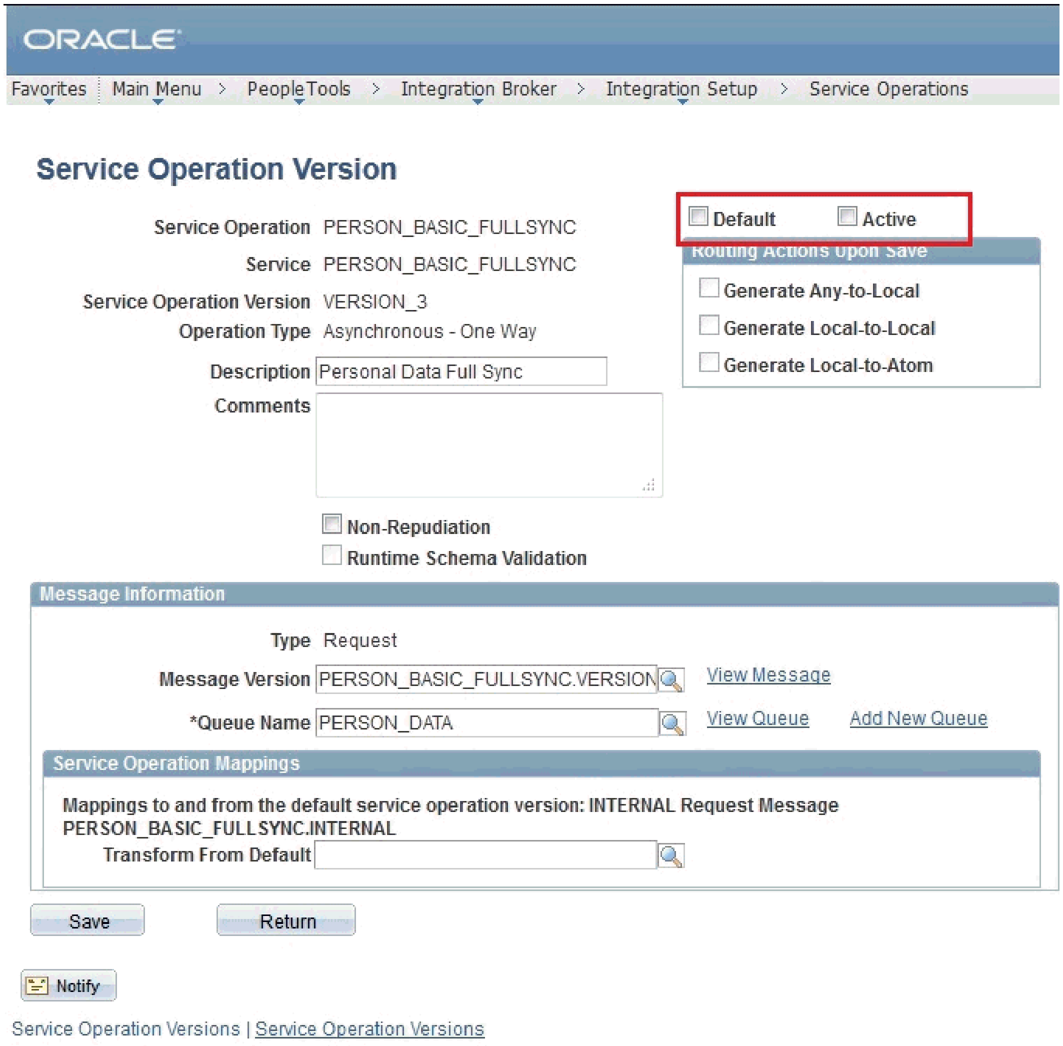
Message.Version: PERSON_BASIC_FULLSYNC.INTERNA View Message

*Queue Name: PERSON_DATA View Queue Add New Queue

Non-Default Versions Personalize | Find | First 1-5 of 5 Last

Version	Description	Active
VERSION_1	Personal Data Full Sync	□
VERSION_2	Personal Data Full Sync	□
VERSION_3	Personal Data Full Sync	□
VERSION_4	Personal Data Full Sync	□
VERSION_5	Person Basic Full Sync 5	□

4. Select the **Default** and **Active** checkboxes highlighted in the following screenshot and click **Save.**



Service Operation Version

□ Default □ Active

Service Operation PERSON_BASIC_FULLSYNC

Service PERSON_BASIC_FULLSYNC

Service Operation Version VERSION_3

Operation Type Asynchronous - One Way

Description Personal Data Full Sync

Comments

Routing Actions Upon Save

□ Generate Any-to-Local

□ Generate Local-to-Local

□ Generate Local-to-Atom

□ Non-Repudiation

□ Runtime Schema Validation

Message Information

Type Request

Message Version PERSON_BASIC_FULLSYNC.VERSION

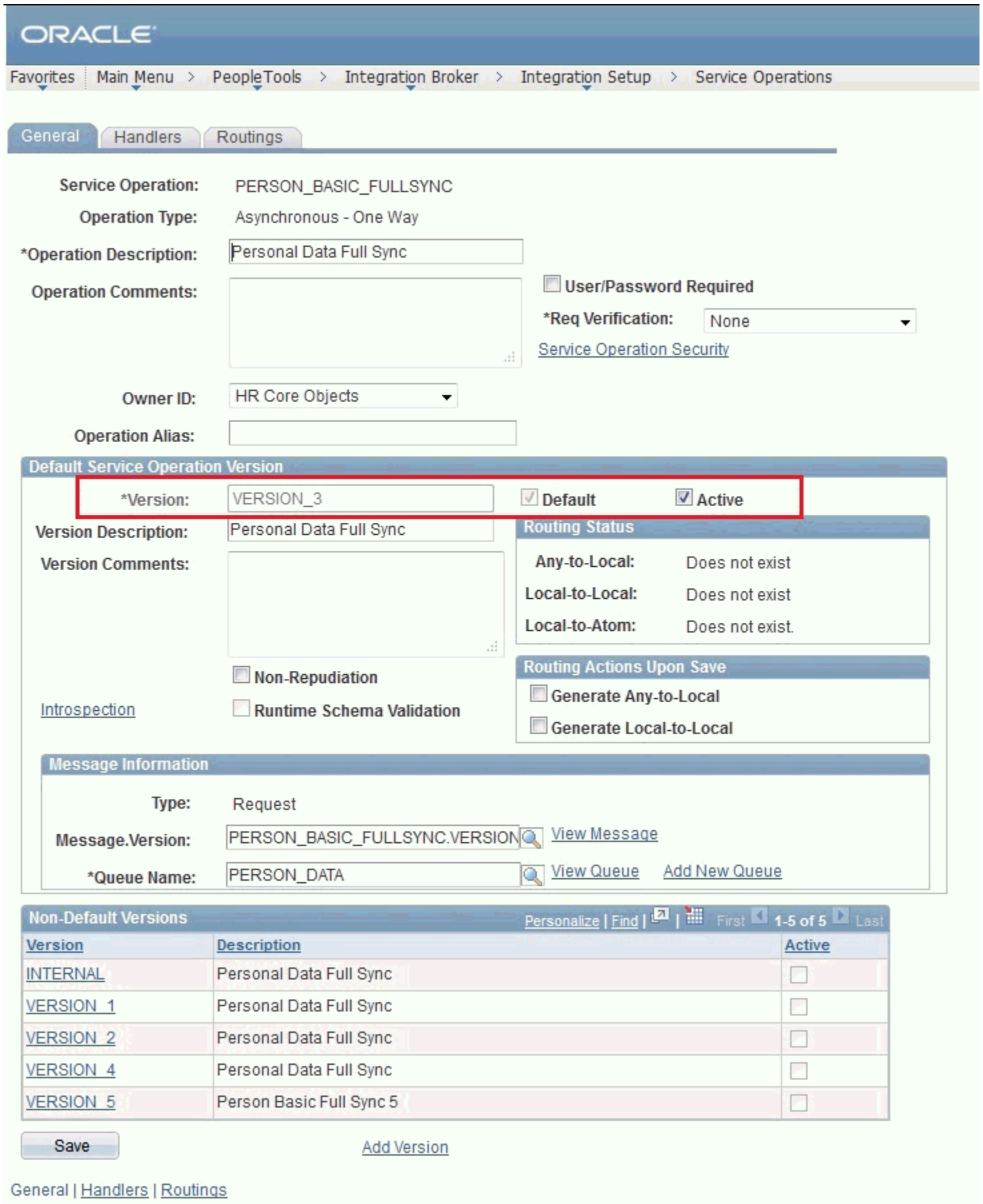
*Queue Name PERSON_DATA

Service Operation Mappings

Mappings to and from the default service operation version: INTERNAL Request Message PERSON_BASIC_FULLSYNC.INTERNAL

Transform From Default

Then, the VESRION_3 message is activated and set as default.


ORACLE
Favorites
Main Menu > PeopleTools > Integration Broker > Integration Setup > Service Operations
General
Handlers
Routings
Service Operation Security
Introspection
View Message
View Queue
Add New Queue
Personalize | Find |
First 1-5 of 5 Last
Save
Add Version
General | Handlers | Routings

Service Operation:	PERSON_BASIC_FULLSYNC
Operation Type:	Asynchronous - One Way
*Operation Description:	Personal Data Full Sync
Operation Comments:	
☐ User/Password Required	
*Req Verification:	None
Owner ID:	HR Core Objects
Operation Alias:	

Default Service Operation Version

*Version:	VERSION_3
☑ Default	☑ Active
Version Description:	Personal Data Full Sync
Version Comments:	
☐ Non-Repudiation	
☐ Runtime Schema Validation	

Routing Status

Any-to-Local:	Does not exist
Local-to-Local:	Does not exist
Local-to-Atom:	Does not exist

Routing Actions Upon Save

☐ Generate Any-to-Local

☐ Generate Local-to-Local

Message Information

Type:	Request
Message.Version:	PERSON_BASIC_FULLSYNC.VERSION
*Queue Name:	PERSON_DATA

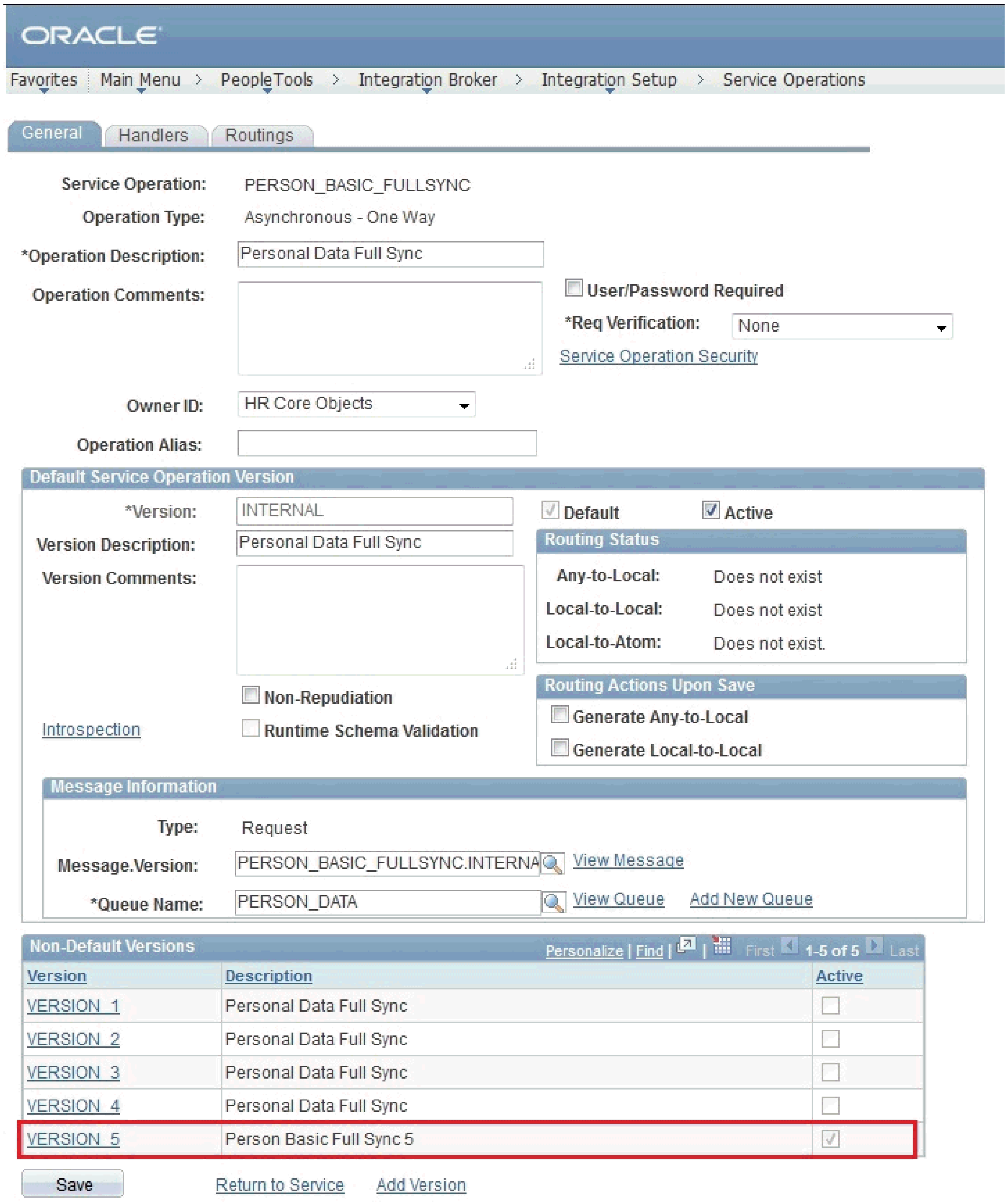
Non-Default Versions

Version	Description	Active
INTERNAL	Personal Data Full Sync	☐
VERSION_1	Personal Data Full Sync	☐
VERSION_2	Personal Data Full Sync	☐
VERSION_4	Personal Data Full Sync	☐
VERSION_5	Person Basic Full Sync 5	☐

D.2 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 PERSON_BASIC_FULLSYNC, in the **Service Operation** field. Then, click **Search.**
3. The following screenshot displays INTERNAL message set as active and default. To deactivate the non-default VERSION_5 message, click the VERSION_5 link in the Non-Default Versions region.


ORACLE
Favorites | Main Menu > PeopleTools > Integration Broker > Integration Setup > Service Operations
General | Handlers | Routings

Service Operation: PERSON_BASIC_FULLSYNC

Operation Type: Asynchronous - One Way

*Operation Description: Personal Data Full Sync

Operation Comments:

□ User/Password Required

*Req Verification: None

Service Operation Security

Owner ID: HR Core Objects

Operation Alias:

Default Service Operation Version

*Version: INTERNAL

☑ Default ☑ Active

Version Description: Personal Data Full Sync

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

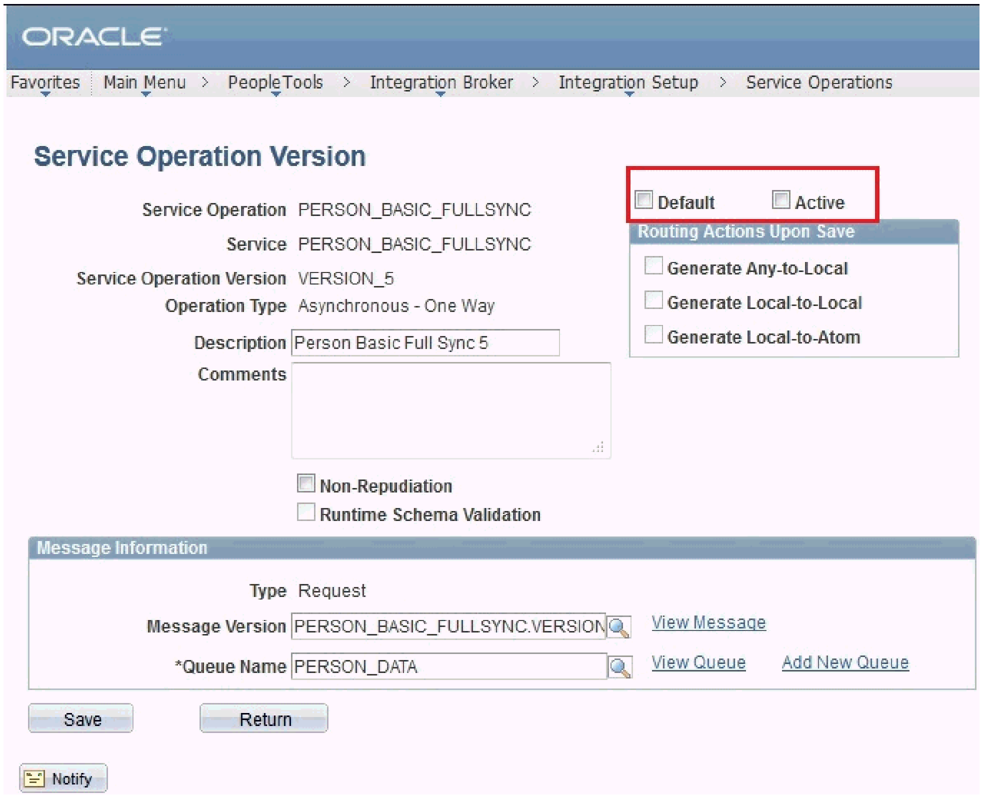
Message.Version: PERSON_BASIC_FULLSYNC.INTERNA View Message

*Queue Name: PERSON_DATA View Queue Add New Queue

Non-Default Versions Personalize | Find | | First 1-5 of 5 Last

Version	Description	Active
VERSION_1	Personal Data Full Sync	□
VERSION_2	Personal Data Full Sync	□
VERSION_3	Personal Data Full Sync	□
VERSION_4	Personal Data Full Sync	□
VERSION_5	Person Basic Full Sync 5	☑

4. Deselect the **Default** and **Active** checkboxes highlighted in the following screenshot and click **Save.**


ORACLE
Favorites | Main Menu > PeopleTools > Integration Broker > Integration Setup > Service Operations
Save
Return
Notify
View Message
View Queue
Add New Queue

Service Operation Version

Service Operation PERSON_BASIC_FULLSYNC

Service PERSON_BASIC_FULLSYNC

Service Operation Version VERSION_5

Operation Type Asynchronous - One Way

Description Person Basic Full Sync 5

Comments

□ Non-Repudiation

□ Runtime Schema Validation

□ Default □ Active

Routing Actions Upon Save

□ Generate Any-to-Local

□ Generate Local-to-Local

□ Generate Local-to-Atom

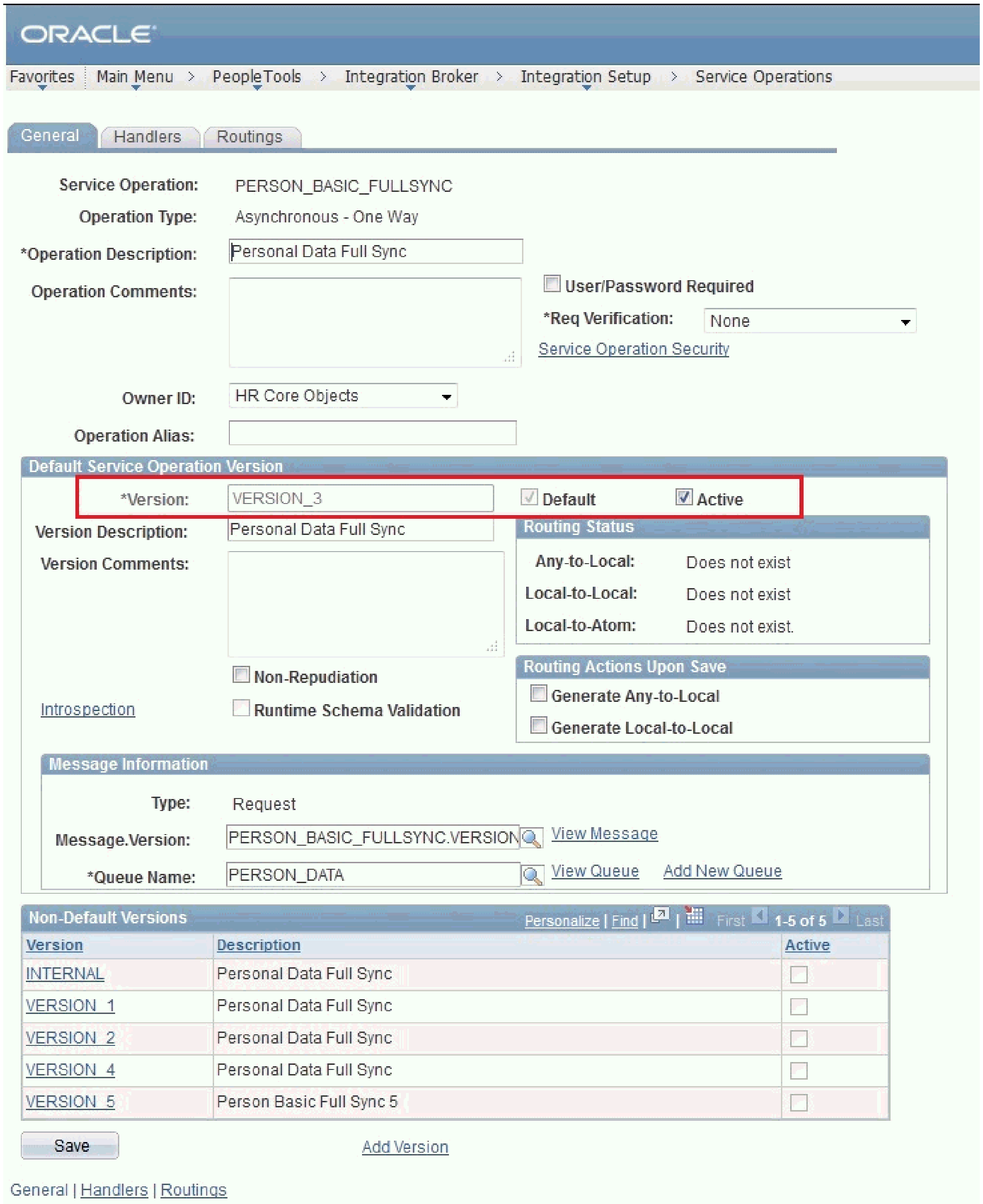
Message Information

Type Request

Message Version PERSON_BASIC_FULLSYNC.VERSION

*Queue Name PERSON_DATA

Then, the VESRION_5 message is deactivated.


ORACLE
Favorites | Main Menu > PeopleTools > Integration Broker > Integration Setup > Service Operations
General | Handlers | Routings

Service Operation: PERSON_BASIC_FULLSYNC

Operation Type: Asynchronous - One Way

*Operation Description: Personal Data Full Sync

Operation Comments:

□ User/Password Required

*Req Verification: None

Service Operation Security

Owner ID: HR Core Objects

Operation Alias:

Default Service Operation Version

*Version: VERSION_3 ☑ Default ☑ Active

Version Description: Personal Data Full Sync

Version Comments:

□ Non-Repudiation

Introspection □ Runtime Schema Validation

Routing Status

Any-to-Local: Does not exist

Local-to-Local: Does not exist

Local-to-Atom: Does not exist.

Routing Actions Upon Save

□ Generate Any-to-Local

□ Generate Local-to-Local

Message Information

Type: Request

Message.Version: PERSON_BASIC_FULLSYNC.VERSION View Message

*Queue Name: PERSON_DATA View Queue Add New Queue

Non-Default Versions Personalize | Find | First 1-5 of 5 Last

Version	Description	Active
INTERNAL	Personal Data Full Sync	□
VERSION_1	Personal Data Full Sync	□
VERSION_2	Personal Data Full Sync	□
VERSION_4	Personal Data Full Sync	□
VERSION_5	Person Basic Full Sync 5	□

Save   Add Version

General | Handlers | Routings

Index