Contents

Preface ............................................................................................................................................................ ix
  Audience ............................................................................................................................................. ix
  Documentation Accessibility ............................................................................................................ ix
  Related Documents ............................................................................................................................ ix
  Documentation Updates ........................................................................................................................ ix
  Conventions ............................................................................................................................................ x

What’s New in the Oracle Identity Manager Connector for PeopleSoft Employee Reconciliation? .......................................................... xi
  Software Updates ............................................................................................................................... xi
  Documentation-Specific Updates ....................................................................................................... xii

1 About the Connector
  1.1 Certified Components .................................................................................................................... 1-1
  1.2 Usage Recommendation ............................................................................................................... 1-3
  1.3 Connector Architecture .............................................................................................................. 1-3
    1.3.1 Full Reconciliation ............................................................................................................. 1-4
    1.3.2 Incremental Reconciliation ............................................................................................... 1-4
  1.4 Features of the Connector ............................................................................................................ 1-5
    1.4.1 Dedicated Support for Trusted Source Reconciliation ....................................................... 1-5
    1.4.2 Full and Incremental Reconciliation .................................................................................. 1-5
    1.4.3 Support for Major Person Lifecycle Events ...................................................................... 1-5
    1.4.4 Reconciliation of Effective-Dated Lifecycle Events .......................................................... 1-6
    1.4.5 Support for Standard PeopleSoft Messages ..................................................................... 1-7
    1.4.6 Support for Resending Messages That Are Not Processed ............................................... 1-8
    1.4.7 Validation and Transformation of Person Data ................................................................. 1-8
    1.4.8 Reconciliation of the Manager ID Attribute ....................................................................... 1-8
      1.4.8.1 Full Reconciliation of the Manager ID Attribute .......................................................... 1-8
      1.4.8.2 Dynamic Reconciliation of the Manager ID Attribute .................................................... 1-9
      1.4.8.3 Steps in the Manager ID Reconciliation Process ........................................................ 1-9
    1.4.9 Target Authentication .......................................................................................................... 1-10
    1.4.10 Support for Specifying Persons to Be Excluded from Reconciliation Operation ......... 1-10
  1.5 Connector Objects Used During Reconciliation ............................................................................ 1-10
    1.5.1 User Attributes for Reconciliation ....................................................................................... 1-11
    1.5.2 Reconciliation Rules ............................................................................................................ 1-11
1.5.2.1 Overview of the Reconciliation Rule ..................................................... 1-11
1.5.2.2 Viewing the Reconciliation Rule in the Design Console ..................... 1-12
1.5.3 Reconciliation Action Rules ....................................................................... 1-12
1.5.3.1 Overview of the Reconciliation Action Rules ........................................ 1-13
1.5.3.2 Viewing the Reconciliation Action Rules in the Design Console .......... 1-13
1.5.4 Predefined Lookup Definitions ................................................................ 1-14
1.5.4.1 Lookup.PSFT.HRMS.Configuration ..................................................... 1-14
1.5.4.2 Lookup.PSFT.HRMS.ManagerRecon.Configuration ............................ 1-16
1.5.4.3 Lookup Definitions Used to Process PERSON_BASIC_SYNC Messages ... 1-17
1.5.4.3.1 Lookup.PSFT.Message.PersonBasicSync.Configuration .................. 1-17
1.5.4.3.2 Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping ................. 1-19
1.5.4.3.3 Lookup.PSFT.HRMS.PersonBasicSync.Recon ................................... 1-23
1.5.4.3.4 Lookup.PSFT.HRMS.PersonBasicSync.EmpType ............................. 1-25
1.5.4.3.5 Lookup.PSFT.HRMS.PersonBasicSync.Validation .......................... 1-25
1.5.4.3.6 Lookup.PSFT.HRMS.PersonBasicSync.Transformation .................... 1-25
1.5.4.4 Lookup Definitions Used to Process WORKFORCE_SYNC Messages .... 1-25
1.5.4.4.1 Lookup.PSFT.Message.WorkForceSync.Configuration .................... 1-25
1.5.4.4.2 Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping .................... 1-28
1.5.4.4.3 Lookup.PSFT.HRMS.WorkForceSync.Recon ..................................... 1-30
1.5.4.4.4 Lookup.PSFT.HRMS.WorkForceSync.EmpStatus .............................. 1-32
1.5.4.4.5 Lookup.PSFT.HRMS.WorkForceSync.EmpType ................................ 1-33
1.5.4.4.6 Lookup.PSFT.HRMS.WorkForceSync.Validation ............................. 1-34
1.5.4.4.7 Lookup.PSFT.HRMS.WorkForceSync.Transformation ....................... 1-34
1.5.4.5 Other Lookup Definitions ................................................................. 1-34
1.5.4.5.1 Lookup.PSFT.HRMS.ExclusionList ............................................... 1-35
1.5.4.5.2 Lookup.PSFT.HRMS.CustomQuery .................................................. 1-35
1.5.6 Roadmap for Deploying and Using the Connector ............................... 1-35

2 Deploying the Connector

2.1 Preinstallation .......................................................................................... 2-1
2.1.1 Preinstallation on Oracle Identity Manager .......................................... 2-1
2.1.1.1 Files and Directories on the Installation Media ................................... 2-1
2.1.2 Preinstallation on the Target System .................................................... 2-3
2.1.2.1 Importing a Project from Application Designer ................................... 2-3
2.1.2.2 Creating a Target System User Account for Connector Operations .... 2-3
2.1.2.2.1 Creating a Permission List .............................................................. 2-5
2.1.2.2.2 Creating a Role for a Limited Rights User ....................................... 2-7
2.1.2.2.3 Assigning the Required Privileges to the Target System Account .... 2-8
2.2 Installation ................................................................................................ 2-9
2.2.1 Installation on Oracle Identity Manager ............................................... 2-9
2.2.1.1 Running the Connector Installer ......................................................... 2-9
2.2.1.2 Copying the Connector Files and External Code Files ......................... 2-11
2.2.1.3 Configuring the IT Resource ............................................................... 2-11
2.2.1.4 Deploying the PeopleSoft Listener ..................................................... 2-12
2.2.1.4.1 Deploying the PeopleSoft Listener on WebSphere Application Server 2-14
2.2.1.4.2 Importing Oracle Identity Manager CA Root Certificate into PeopleSoft WebServer 2-16
3 Using the Connector

3.1 Summary of Steps to Use the Connector ................................................................. 3-1
3.2 Performing Full Reconciliation .............................................................................. 3-2
3.2.1 Generating XML Files ....................................................................................... 3-2
3.2.1.1 Running the PERSON_BASIC_FULLSYNC Message .................................................. 3-2
3.2.1.2 Running the WORKFORCE_FULLSYNC Message ....................................................... 3-4
3.2.2 Importing XML Files into Oracle Identity Manager .............................................. 3-5
3.2.2.1 Configuring the Scheduled Task for Person Data Reconciliation .................. 3-5
3.2.2.2 Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task .... 3-6
3.3 Performing Incremental Reconciliation .................................................................. 3-8
3.4 Limited Reconciliation ......................................................................................... 3-8
3.5 Resending Messages That Are Not Received by the PeopleSoft Listener .................. 3-10
3.6 Configuring Scheduled Tasks ................................................................................ 3-11
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–1</td>
<td>Architecture of the Connector</td>
<td>1-3</td>
</tr>
<tr>
<td>1–2</td>
<td>Reconciliation Rule</td>
<td>1-12</td>
</tr>
<tr>
<td>1–3</td>
<td>Reconciliation Action Rules</td>
<td>1-14</td>
</tr>
<tr>
<td>1–4</td>
<td>Sample XML File for PERSON_BASIC_SYNC Message</td>
<td>1-23</td>
</tr>
<tr>
<td>1–5</td>
<td>Sample XML File for WORKFORCE_SYNC Message</td>
<td>1-30</td>
</tr>
</tbody>
</table>
List of Tables

1–1 Certified Components ............................................................................................................ 1-1
1–2 User Attributes for Reconciliation ......................................................................................... 1-11
1–3 Action Rules for Trusted Source Reconciliation ................................................................. 1-13
2–1 Files and Directories on the Installation Media ............................................................... 2-1
2–2 Files to Be Copied to the Oracle Identity Manager Host Computer ............................... 2-11
2–3 IT Resource Parameters ..................................................................................................... 2-12
2–4 Log Levels and ODL Message Type:Level Combinations .................................................. 2-63
3–1 Attributes of the Peoplesoft HRMS Trusted Reconciliation Scheduled Task .................. 3-6
3–2 Attributes of the PeopleSoft HRMS Manager Reconciliation Scheduled Task ............... 3-7
3–3 Scheduled Tasks for Reconciliation ................................................................................... 3-11
4–1 Connector Objects and Their Associations .......................................................................... 4-14
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:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><code>monospace</code></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
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 Section 1.4.8, "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 Section 2.2.1.4, "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 Section 1.5.4.1, "Lookup.PSFT.HRMS.Configuration" and Section 2.3.1.3, "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 Section 1.5.4.2, "Lookup.PSFT.HRMS.ManagerRecon.Configuration" and Section 3.2.2.2, "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:

<table>
<thead>
<tr>
<th>Bug Number</th>
<th>Issue Description</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>13091034</td>
<td>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.</td>
<td>This issue has been resolved. The Manager ID value is now updated when the User ID attribute is reconciled into a UDF.</td>
</tr>
</tbody>
</table>

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 "21" of this guide:

- The "Target System" row of Table 1–1, "Certified Components" 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:
  - Section 2.1.2.2.1, "Creating a Permission List"
  - Section 2.1.2.2.2, "Creating a Role for a Limited Rights User"
  - Section 2.1.2.2.3, "Assigning the Required Privileges to the Target System Account"
  - Section 2.2.2.1.1, "Configuring the PeopleSoft Integration Broker"
  - Section 2.2.2.1.2, "Configuring the PERSON_BASIC_FULLSYNC 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 Section 2.3.1.2, "Setting Up the Lookup.PSFT.HRMS.ExclusionList Lookup Definition" have been modified.
- The "Note" in Step 5c of Section 2.1.2.2, "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, "Certified Components" 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, "Certified Components" 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:
  - Section 2.1.2.2.1, "Creating a Permission List"
  - Section 2.1.2.2.2, "Creating a Role for a Limited Rights User"
  - Section 2.1.2.2.3, "Assigning the Required Privileges to the Target System Account"
  - Section 2.1.2.2.3, "Assigning the Required Privileges to the Target System Account"
  - Section 2.2.2.1.1, "Configuring the PeopleSoft Integration Broker"
  - Section 2.2.2.1.2, "Configuring the PERSON_BASIC_FULLSYNC Service Operation"
  - Section 2.2.2.1.3, "Configuring the WORKFORCE_FULLSYNC Service Operation"
  - Section 2.2.2.1.3, "Configuring the WORKFORCE_FULLSYNC Service Operation"
  - Section 2.2.2.2.1, "Configuring PeopleSoft Integration Broker"
  - Section 2.2.2.2.2, "Configuring the PERSON_BASIC_SYNC Service Operation"
  - Section 2.2.2.2.3, "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 Section 2.2.1.4, "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_SYNC 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, "Certified Components" 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 Section 1.4.4, "Reconciliation of Effective-Dated Lifecycle Events."
- Information regarding PeopleSoft HRMS 9.2 with PeopleTools 8.55 has been added to the following sections:
  - Section 2.1.2.2.1, "Creating a Permission List"
  - Section 2.1.2.2.2, "Creating a Role for a Limited Rights User" Section 2.1.2.2.3, "Assigning the Required Privileges to the Target System Account"
  - Section 2.1.2.2.3, "Assigning the Required Privileges to the Target System Account"
  - Section 2.2.2.1.2, "Configuring the PERSON_BASIC_FULLSYNC Service Operation"
  - Section 2.2.2.1.3, "Configuring the WORKFORCE_FULLSYNC Service Operation"
  - Section 2.2.2.1.3, "Configuring the WORKFORCE_SYNC Service Operation"
  - Section 2.2.2.2.1, "Configuring the PERSON_BASIC_SYNC Service Operation"
  - Section 2.2.2.2.2, "Configuring the PERSON_BASIC_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, "Certified Components" 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, "Certified Components".
- The "JDK" row of Table 1–1, "Certified Components" has been renamed to "Connector Server JDK".
- All instances of WLS_HOME have been replaced with WL_HOME in Section 2.2.1.4, "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:
  - Section 2.2.2.1.2, "Configuring the PERSON_BASIC_FULLSYNC Service Operation"
  - Section 2.2.2.1.3, "Configuring the WORKFORCE_FULLSYNC Service Operation"
- Section 2.2.2.2.2, "Configuring the PERSON_BASIC_SYNC Service Operation"
- Section 2.2.2.2.3, "Configuring the WORKFORCE_SYNC Service Operation"

- The first "Note" present in Section 2.2.2.1.3, "Configuring the WORKFORCE_FULLSYNC Service Operation" has been modified.
- The "Target systems" row of Table 1–1, "Certified Components" has been updated.
- The "Note" in Step 3 of the Activating the PERSON_BASIC_SYNC Service Operation area of Section 2.2.2.2, "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_SYNC Service Operation area of Section 2.2.2.2, "Configuring the PERSON_BASIC_SYNC Service Operation" has been added.
- An issue related to workforce incremental reconciliation has been added to Section 5.2, "Troubleshooting."

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

- The "Oracle Identity Manager" row of Table 1–1, "Certified Components" has been updated.
- Information specific to Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) has been added to Section 1.2, "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 Chapter 4, "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 Section 2.1.2.2.2, "Creating a Role for a Limited Rights User."
- A "Note" has been added to Step 6.e of Section 2.1.2.2.3, "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, "Certified Components" has been modified to include Oracle Identity Manager 11g 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, "Certified Components" 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 Section 5.1, "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, "Certified Components".
- HRMS 9.2 has been added to the first note in Section 2.2.2.1.3, "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 Section 2.2.2.1.1, "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:
- Section 2.2.2.1.2, "Configuring the PERSON_BASIC_FULLSYNC Service Operation"
- Section 2.2.2.1.3, "Configuring the WORKFORCE_FULLSYNC Service Operation"
- Section 2.2.2.2.2, "Configuring the PERSON_BASIC_SYNC Service Operation"
- Section 2.2.2.2.3, "Configuring the WORKFORCE_SYNC Service Operation"

A note has been added to the procedure for Activating the WORKFORCE_FULLSYNC Message in the following sections:
- Section 2.2.2.1.2, "Configuring the PERSON_BASIC_FULLSYNC Service Operation"
- Section 2.2.2.1.3, "Configuring the WORKFORCE_FULLSYNC Service Operation"
- Section 2.2.2.2.2, "Configuring the PERSON_BASIC_SYNC Service Operation"
- Section 2.2.2.2.3, "Configuring the WORKFORCE_SYNC Service Operation"

The name of the "Known Issues" chapter has been changed to "Known Issues and Workarounds". In addition, Chapter 6, "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, "Certified Components" has been modified.
- Section 2.3.1.6, "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:
  - Section 2.2.1.1, "Running the Connector Installer"
  - Section 2.2.1.3, "Configuring the IT Resource"
  - Section 3.6, "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 Section 2.2.1.4.1, "Deploying the PeopleSoft Listener on WebSphere Application Server."
  Added a procedure to display UDFs in Oracle Identity Manager release 11.1.2 in Section 3.2.2.1, "Configuring the Scheduled Task for Person Data Reconciliation."
  Added bug 13497967 to Chapter 6, "Known Issues and Workarounds"
- Revision "4"
  In Table 1–1, "Certified Components" the PeopleSoft HRMS 9.1 with PeopleTools 8.52 has been added as a newly certified target system.
Revision “3”

In Table 1–1, "Certified Components" the Oracle Identity Manager version has been updated to Release 11.1.1.5 BP02.
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:

- Section 1.1, "Certified Components"
- Section 1.2, "Usage Recommendation"
- Section 1.3, "Connector Architecture"
- Section 1.4, "Features of the Connector"
- Section 1.5, "Connector Objects Used During Reconciliation"
- Section 1.6, "Roadmap for Deploying and Using the Connector"

### 1.1 Certified Components

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Identity Governance or Oracle Identity Manager</td>
<td>You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:</td>
</tr>
<tr>
<td></td>
<td>- Oracle Identity Governance 12c (12.2.1.3.0)</td>
</tr>
<tr>
<td></td>
<td>- Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0)</td>
</tr>
<tr>
<td></td>
<td>- Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0)</td>
</tr>
<tr>
<td></td>
<td>- Oracle Identity Manager release 11.1.1.5 BP02</td>
</tr>
</tbody>
</table>
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

### Table 1–1 (Cont.) Certified Components

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target systems</td>
<td>The target system can be any one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 8.9 with PeopleTools 8.49</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 8.9 with PeopleTools 8.50</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.0 with PeopleTools 8.49</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.0 with PeopleTools 8.50</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.0 with PeopleTools 8.52</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.1 with PeopleTools 8.50</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.1 with PeopleTools 8.51</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.1 with PeopleTools 8.52</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.1 with PeopleTools 8.53</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.2 with PeopleTools 8.53</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.2 with PeopleTools 8.54</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.2 with PeopleTools 8.55</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.2 with PeopleTools 8.56</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft HRMS 9.2 with PeopleTools 8.57</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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:</td>
</tr>
<tr>
<td></td>
<td><a href="https://support.oracle.com/">https://support.oracle.com/</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connector Server</th>
<th>11.1.2.1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector Server JDK</td>
<td>JDK 1.6 or later, or JRockit 1.6 or later</td>
</tr>
<tr>
<td>Other Software</td>
<td>You must ensure that the following components are installed and configured in the target system environment:</td>
</tr>
<tr>
<td></td>
<td>■ Tuxedo and Jolt (the application server)</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft Internet Architecture</td>
</tr>
<tr>
<td></td>
<td>■ PeopleSoft Application Designer (2-tier mode)</td>
</tr>
<tr>
<td></td>
<td>The following standard PeopleSoft messages are available:</td>
</tr>
<tr>
<td></td>
<td>■ PERSON_BASIC_FULLSYNC</td>
</tr>
<tr>
<td></td>
<td>■ WORKFORCEFULLSYNC</td>
</tr>
<tr>
<td></td>
<td>■ PERSON_BASIC_SYNC</td>
</tr>
<tr>
<td></td>
<td>■ WORKFORCE_SYNC</td>
</tr>
</tbody>
</table>

**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:


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

### 1.2 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 11g 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 11g Release 1 BP02 (11.1.1.5.2) or later, Oracle Identity Manager 11g Release 2 BP04 (11.1.2.0.4) or later, or Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.x version of this connector.

### 1.3 Connector Architecture

Figure 1–1 shows the architecture of the connector.

**Figure 1–1 Architecture of the Connector**

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

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:

- Section 1.3.1, "Full Reconciliation"
- Section 1.3.2, "Incremental Reconciliation"
1.3.1 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 Section 1.4.5, "Support for Standard PeopleSoft Messages" for more information about these messages.

Full reconciliation involves the following steps:

See Section 3.2, "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.

1.3.2 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 Section 1.4.5, "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:

Section 3.3, "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.
1.4 Features of the Connector

The following are the features of the connector:

- Section 1.4.1, "Dedicated Support for Trusted Source Reconciliation"
- Section 1.4.2, "Full and Incremental Reconciliation"
- Section 1.4.3, "Support for Major Person Lifecycle Events"
- Section 1.4.4, "Reconciliation of Effective-Dated Lifecycle Events"
- Section 1.4.5, "Support for Standard PeopleSoft Messages"
- Section 1.4.6, "Support for Resending Messages That Are Not Processed"
- Section 1.4.7, "Validation and Transformation of Person Data"
- Section 1.4.8, "Reconciliation of the Manager ID Attribute"
- Section 1.4.9, "Target Authentication"
- Section 1.4.10, "Support for Specifying Persons to Be Excluded from Reconciliation Operation"

1.4.1 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.

1.4.2 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.

1.4.3 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 Section 1.5.4.4.4, "Lookup.PSFT.HRMS.WorkForceSync.EmpStatus" for more information.

1.4.4 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 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 Section 1.4.5, "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 Section 1.5.4.3.1, "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: HIR
Decode: Active

See Section 1.5.4.4.4, "Lookup.PSFT.HRMS.WorkForceSync.EmpStatus." for more information about this lookup definition.
1.4.5 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:** 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.
1.4.6 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 Section 3.5, "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:


1.4.7 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.

- Section 4.4, "Configuring Validation of Data During Reconciliation" provides information about setting up the validation feature.
- Section 4.5, "Configuring Transformation of Data During Reconciliation" provides information about setting up the transformation feature.

1.4.8 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.

1.4.8.1 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 Section 3.2.2.2, "Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task" for instructions on how to reconcile Manager ID values in this scenario.

1.4.8.2 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.

1.4.8.3 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:

   ![Supervisor_ID_node](image)

   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 Section 3.2.2.2, "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.

1.4.9 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 Section 2.2.2.2.1, "Configuring PeopleSoft Integration Broker" for setting up the node. In addition, the flag IsActive is used to verify whether the IT Resource is active or not. The value of this flag is Yes, by default. When this value is Yes, target authentication is carried out. Target authentication fails if it is set to No.

1.4.10 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 Section 1.5.4.5.1, "Lookup.PSFT.HRMS.ExclusionList" for more information.

1.5 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:

- Section 1.5.1, "User Attributes for Reconciliation"
- Section 1.5.2, "Reconciliation Rules"
1.5.1 User Attributes for Reconciliation

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

<table>
<thead>
<tr>
<th>OIM User Form Field</th>
<th>PeopleSoft HRMS/HCM Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>PS_PERSON.EMPLID</td>
<td>The employee ID of the user. This is a mandatory field for the creation of an OIM User.</td>
</tr>
<tr>
<td>Last Name</td>
<td>PS_NAMES.LAST_NAME</td>
<td>The last name of the user. This is a mandatory field for the creation of an OIM User.</td>
</tr>
<tr>
<td>First Name</td>
<td>PS_NAMES.FIRST_NAME</td>
<td>The first name of the user. This is a mandatory field for the creation of an OIM User.</td>
</tr>
<tr>
<td>Employee Type</td>
<td>PS_JOB.REG_TEMP, PS_JOB.FULL_PART_TIME, PS_JOB.PER_ORG</td>
<td>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.</td>
</tr>
<tr>
<td>Status</td>
<td>PS_JOB.ACTION</td>
<td>The action to be taken for a person. It could be HIRE, TRANSFER, and so on.</td>
</tr>
<tr>
<td>Start Date</td>
<td>PS_JOB.EFFDT</td>
<td>The effective date of a person's job record.</td>
</tr>
<tr>
<td>Supervisor ID</td>
<td>PS_JOB.SUPERVISOR_ID</td>
<td>The supervisor ID of a person.</td>
</tr>
<tr>
<td>Department</td>
<td>PS_JOB.DEPTID</td>
<td>The department ID of a person.</td>
</tr>
<tr>
<td>Job ID</td>
<td>PS_JOB.JOBCODE</td>
<td>The job ID of a person.</td>
</tr>
</tbody>
</table>

1.5.2 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:

- Section 1.5.2.1, "Overview of the Reconciliation Rule"
- Section 1.5.2.2, "Viewing the Reconciliation Rule in the Design Console"

1.5.2.1 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.

### 1.5.2.2 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.
4. Search for and open PSFT ER. Figure 1–2 shows this reconciliation rule.

---

**Figure 1–2 Reconciliation Rule**

---

### 1.5.3 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.
The following sections provide information about the reconciliation action rules for this connector:

- **Section 1.5.3.1, "Overview of the Reconciliation Action Rules"
- **Section 1.5.3.2, "Viewing the Reconciliation Action Rules in the Design Console"

### 1.5.3.1 Overview of the Reconciliation Action Rules

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

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Matches Found</td>
<td>Create User</td>
</tr>
<tr>
<td>One Entity Match Found</td>
<td>Establish Link</td>
</tr>
</tbody>
</table>

### 1.5.3.2 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.
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.
1.5.4 Predefined Lookup Definitions

The predefined lookup definitions can be categorized as follows:

- Section 1.5.4.1, "Lookup.PSFT.HRMS.Configuration"
- Section 1.5.4.2, "Lookup.PSFT.HRMS.ManagerRecon.Configuration"
- Section 1.5.4.3, "Lookup Definitions Used to Process PERSON_BASIC_SYNC Messages"
- Section 1.5.4.4, "Lookup Definitions Used to Process WORKFORCE_SYNC Messages"
- Section 1.5.4.5, "Other Lookup Definitions"

1.5.4.1 Lookup.PSFT.HRMS.Configuration

The Lookup.PSFT.HRMS.Configuration lookup definition is used to store configuration information that is used by the connector. See Section 2.2.1.3, "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:
## Connector Objects Used During Reconciliation

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager Recon Config Lookup</td>
<td>Lookup.PSFT.HRMS.ManagerRecon.Configuration</td>
<td>Name of the lookup used by the PeopleSoft HRMS Manager Reconciliation scheduled task to read the required values. See Section 1.5.4.2, &quot;Lookup.PSFT.HRMS.ManagerRecon.Configuration&quot; for more information about this lookup definition.</td>
</tr>
<tr>
<td>HRMS Resource Exclusion List Lookup</td>
<td>Lookup.PSFT.HRMS.ExclusionList</td>
<td>Name of the Resource Exclusion lookup for PeopleSoft Employee Reconciliation. See Section 1.5.4.1, &quot;Lookup.PSFT.HRMS.Configuration&quot; for more information about this lookup definition.</td>
</tr>
<tr>
<td>Ignore Root Audit Action</td>
<td>No</td>
<td>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: Appendix A, &quot;Determining the Root Audit Action Details&quot;.</td>
</tr>
<tr>
<td>PERSON_BASIC_FULLSYNC NC</td>
<td>Lookup.PSFT.Message.PersonBasicSync.Configuration</td>
<td>Name of the lookup definition for PERSON_BASIC_FULLSY NC message. See Section 1.5.4.3.1, &quot;Lookup.PSFT.Message.PersonBasicSync.Configuration&quot; for more information about this lookup definition. <strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>
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. Section 2.3.1.3, "Lookup.PSFT.Message.PersonBasicSync.Configuration" describes the procedure to configure these message names.

1.5.4.2 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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERSON_BASIC_SYNC</td>
<td>Lookup.PSFT.Message.PersonBasicSync.Configuration</td>
<td>Name of the lookup definition for the PERSON_BASIC_SYNC message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Section 1.5.4.3.1, &quot;Lookup.PSFT.Message.PersonBasicSync.Configuration&quot; for more information about this lookup definition.</td>
</tr>
<tr>
<td>Target Date Format</td>
<td>yyyy-MM-dd</td>
<td>Data format of the Date type data in the XML file and messages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must not change this value.</td>
</tr>
<tr>
<td>WORKFORCE_FULLSYNC</td>
<td>Lookup.PSFT.Message.WorkForceSync.Configuration</td>
<td>Name of the lookup definition for the WORKFORCE_FULLSYNC message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Section 1.5.4.4.1, &quot;Lookup.PSFT.Message.WorkForceSync.Configuration&quot; for more information about this lookup definition.</td>
</tr>
<tr>
<td></td>
<td>Note: The Decode value is the same as that of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WORKFORCE_SYNC, because the data to be reconciled is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the same for both messages.</td>
<td></td>
</tr>
<tr>
<td>WORKFORCE_SYNC</td>
<td>Lookup.PSFT.Message.WorkForceSync.Configuration</td>
<td>Name of the lookup definition for the WORKFORCE_SYNC message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Section 1.5.4.2, &quot;Lookup.PSFT.HRMS.ManagerRecon.Configuration&quot; for more information about this lookup definition.</td>
</tr>
</tbody>
</table>

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. Section 2.3.1.3, "Setting Up the Lookup.PSFT.HRMS.Configuration Lookup Definition" describes the procedure to configure these message names.
See Section 3.2.2.2, "Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task" for instructions on how to configure and run the PeopleSoft HRMS Manager Reconciliation scheduled task.

1.5.4.3 Lookup Definitions Used to Process PERSON_BASIC_SYNC Messages

The following lookup definitions are used to process PERSON_BASIC_SYNC messages:

1.5.4.3.1 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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee ID RO</td>
<td>Name of the Resource Object field for Employee ID of a person.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sample value: User ID</td>
<td></td>
</tr>
<tr>
<td>Employee ID UDF</td>
<td>Metadata of the field of the person form with which EMPL ID from the target system is mapped.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sample value: Users.User ID</td>
<td></td>
</tr>
<tr>
<td>Manager UDF</td>
<td>Metadata of the Supervisor ID field of the person form.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sample value: USR_UDF_SUPERVISOR_ID</td>
<td></td>
</tr>
</tbody>
</table>

See Section 1.5.4.3.2, "Lookup.PSFT.HRMS.PersonBasicSync.AttributeMapping" for more information about this lookup definition.
## Custom Query Lookup Definition

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 Section 3.4, "Limited Reconciliation" for more information.

### 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

Name of the lookup definition that maps Oracle Identity Manager attributes with employee type attributes obtained from XML message. See Section 1.5.4.3.4, "Lookup.PSFT.HRMS.PersonBasicSync.EmpType" for more information about this lookup definition.

### Message Handler Class

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: Appendix B, "Configuring the Connector Messages".

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Query Lookup Definition</td>
<td>Lookup.PSFT.HRMS.Custom Query</td>
<td>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 Section 3.4, &quot;Limited Reconciliation&quot; for more information.</td>
</tr>
<tr>
<td>Data Node Name Transaction</td>
<td>Transaction</td>
<td>Name of the node in the XML files to execute a transaction. Default value: Transaction. You must not change the default value.</td>
</tr>
<tr>
<td>Employee Status Active</td>
<td>Active</td>
<td>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.</td>
</tr>
<tr>
<td>Employee Type Lookup</td>
<td>Lookup.PSFT.HRMS.PersonBasicSync.EmpType</td>
<td>Name of the lookup definition that maps Oracle Identity Manager attributes with employee type attributes obtained from XML message. See Section 1.5.4.3.4, &quot;Lookup.PSFT.HRMS.PersonBasicSync.EmpType&quot; for more information about this lookup definition.</td>
</tr>
<tr>
<td>Message Handler Class</td>
<td>oracle.iam.connectors.psft.common.handler.impl.PSFTPPersonSyncReconMessageHandlerImpl</td>
<td>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: Appendix B, &quot;Configuring the Connector Messages&quot;.</td>
</tr>
</tbody>
</table>
1.5.4.3.2 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 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: Appendix B, "Configuring the Connector Messages"
message. The following table provides the format of the values stored in this lookup definition:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emp Type</td>
<td>PER_ORG~PERSON</td>
</tr>
<tr>
<td>First Name</td>
<td>FIRST_NAME<del>NAMES</del>NAME_TYPE=PRI~EFFDT</td>
</tr>
<tr>
<td>Last Name</td>
<td>LAST_NAME<del>NAMES</del>NAME_TYPE=PRI~EFFDT</td>
</tr>
<tr>
<td>User ID</td>
<td>EMPLID<del>PERSON</del>None<del>None</del>PRIMARY</td>
</tr>
</tbody>
</table>

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:
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:
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.
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

1.5.4.3.3 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:
### Connector Objects Used During Reconciliation

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Type</td>
<td>Emp Type~Employee Type Lookup</td>
</tr>
<tr>
<td>First Name</td>
<td>First Name</td>
</tr>
<tr>
<td>Last Name</td>
<td>Last Name</td>
</tr>
<tr>
<td>User ID</td>
<td>User ID</td>
</tr>
</tbody>
</table>

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

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

\[ATTRIBUTE \sim LOOKUP~DEF\]

**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 Section 1.5.4.3.2, "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.

### 1.5.4.3.4 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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMP</td>
<td>Full-Time</td>
</tr>
<tr>
<td>CWR</td>
<td>Part-Time</td>
</tr>
<tr>
<td>POI</td>
<td>Temp</td>
</tr>
</tbody>
</table>

In the preceding table:

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

### 1.5.4.3.5 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 Section 4.4, "Configuring Validation of Data During Reconciliation" for more information about adding entries in this lookup definition.

### 1.5.4.3.6 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 Section 4.5, "Configuring Transformation of Data During Reconciliation" for more information about adding entries in this lookup definition.

### 1.5.4.4 Lookup Definitions Used to Process WORKFORCE_SYNC Messages

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

### 1.5.4.4.1 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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Mapping Lookup</td>
<td>Lookup.PSFT.HRMS.WorkForceSync.AttributeMapping</td>
<td>Name of the lookup definition that maps Oracle Identity Manager attributes with attributes in the WORKFORCE_SYNC and WORKFORCE_FULLSYNC message XML. See Section 1.5.4.4.2, “Lookup.PSFT.HRMS.WorkForce Sync.AttributeMapping” for more information about this lookup definition.</td>
</tr>
<tr>
<td>Custom Query</td>
<td>Enter a Value</td>
<td>If you want to implement limited reconciliation, then enter the query condition that you create by following the instructions given in Section 3.4, “Limited Reconciliation.”</td>
</tr>
<tr>
<td>Custom Query Lookup Definition</td>
<td>Lookup.PSFT.HRMS.Custom Query</td>
<td>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 Section 3.4, “Limited Reconciliation” for more information.</td>
</tr>
<tr>
<td>Data Node Name</td>
<td>Transaction</td>
<td>Name of the node in the XML files to run a transaction.</td>
</tr>
<tr>
<td>Employee Status Lookup</td>
<td>Lookup.PSFT.HRMS.WorkForceSync.EmpStatus</td>
<td>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 Section 1.5.4.4.4, “Lookup.PSFT.HRMS.WorkForce Sync.EmpStatus” for more information about this lookup definition.</td>
</tr>
<tr>
<td>Code Key</td>
<td>Decode</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Employee Type Lookup</td>
<td>Lookup.PSFT.HRMS.WorkForceSync.EmpType</td>
<td>Name of the lookup definition that stores all valid person types and components of the Employee person type in the target system. Is a lookup definition. See Section 1.5.4.4.5, “Lookup.PSFT.HRMS.WorkForce Sync.EmpType” for more information about this lookup definition.</td>
</tr>
<tr>
<td>Message Handler Class</td>
<td>oracle.iam.connectors.psft.common.handler.impl.PSFTWorkForceSyncReconMessageHandlerImpl</td>
<td>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: Appendix B, &quot;Configuring the Connector Messages.&quot;</td>
</tr>
<tr>
<td>Message Parser</td>
<td>oracle.iam.connectors.psft.common.parser.impl.JobMessageParser</td>
<td>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: Appendix B, &quot;Configuring the Connector Messages.&quot;</td>
</tr>
<tr>
<td>Recon Lookup Definition</td>
<td>Lookup.PSFT.HRMS.WorkForceSync.Recon</td>
<td>Name of the lookup definition that maps Oracle Identity Manager attribute with Resource Object attribute. See Section 1.5.4.4.3, “Lookup.PSFT.HRMS.WorkForce Sync.Recon” for more information about this lookup definition.</td>
</tr>
<tr>
<td>Resource Object</td>
<td>Peoplesoft HRMS</td>
<td>Name of the resource object</td>
</tr>
</tbody>
</table>
1.5.4.4.2 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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformation Lookup Definition</td>
<td>Lookup.PSFT.HRMS.WorkForceSync.Transformation</td>
<td>Name of the transformation lookup definition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It is empty by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Section 1.5.4.4.7, &quot;Lookup.PSFT.HRMS.WorkForceSync.Transformation&quot; for more information about this lookup definition.</td>
</tr>
<tr>
<td>Use Transformation</td>
<td>No</td>
<td>Enter yes to implement transformation while reconciling records. Otherwise, enter no.</td>
</tr>
<tr>
<td>Use Validation</td>
<td>No</td>
<td>Enter yes to implement validation while reconciling records. Otherwise, enter no.</td>
</tr>
<tr>
<td>Validation Lookup Definition</td>
<td>Lookup.PSFT.HRMS.WorkForceSync.Validation</td>
<td>Name of the validation lookup definition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It is empty by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Section 1.5.4.4.6, &quot;Lookup.PSFT.HRMS.WorkForceSync.Validation&quot; for more information about this lookup definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPTID</td>
<td>DEPTID<del>JOB</del>None~EFFDT</td>
</tr>
<tr>
<td>FULL_PART_TIME</td>
<td>FULL_PART_TIME<del>JOB</del>None~EFFDT</td>
</tr>
<tr>
<td>JOBCODE</td>
<td>JOBCODE<del>JOB</del>None~EFFDT</td>
</tr>
<tr>
<td>PER_ORG</td>
<td>PER_ORG<del>JOB</del>None~EFFDT</td>
</tr>
<tr>
<td>REG_TEMP</td>
<td>REG_TEMP<del>JOB</del>None~EFFDT</td>
</tr>
<tr>
<td>EFFDT</td>
<td>EFFDT<del>JOB</del>None~EFFDT</td>
</tr>
<tr>
<td>ACTION</td>
<td>ACTION<del>JOB</del>None~EFFDT</td>
</tr>
<tr>
<td>SUPERVISOR_ID</td>
<td>SUPERVISOR_ID<del>JOB</del>NONE~EFFDT</td>
</tr>
<tr>
<td>EMPLID</td>
<td>EMPLID<del>PER_ORG_ASGN</del>None<del>None</del>PRIMARY</td>
</tr>
</tbody>
</table>

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.
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.

1.5.4.4.3 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 Used During Reconciliation

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Department</td>
</tr>
<tr>
<td>Effective Start Date</td>
<td>Start Date</td>
</tr>
<tr>
<td>Employee Type</td>
<td>PER ORG##REG TEMP##FULL PART TIME-EMPLOYEE TYPE LOOKUP</td>
</tr>
<tr>
<td>Job Code</td>
<td>Job ID</td>
</tr>
<tr>
<td>Status</td>
<td>STATUS-EMPLOYEE STATUS LOOKUP</td>
</tr>
<tr>
<td>Supervisor ID</td>
<td>Supervisor ID</td>
</tr>
<tr>
<td>User ID</td>
<td>User ID</td>
</tr>
</tbody>
</table>

**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 Section 1.5.4.4.2, "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
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.

### 1.5.4.4.4 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.

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADD</td>
<td>Active</td>
</tr>
<tr>
<td>ADL</td>
<td>Active</td>
</tr>
<tr>
<td>ASG</td>
<td>Disabled</td>
</tr>
<tr>
<td>BON</td>
<td>Active</td>
</tr>
<tr>
<td>COM</td>
<td>Disabled</td>
</tr>
<tr>
<td>DEM</td>
<td>Disabled</td>
</tr>
<tr>
<td>DTA</td>
<td>Disabled</td>
</tr>
<tr>
<td>FSC</td>
<td>Disabled</td>
</tr>
<tr>
<td>HIR</td>
<td>Active</td>
</tr>
<tr>
<td>JED</td>
<td>Disabled</td>
</tr>
<tr>
<td>JRC</td>
<td>Active</td>
</tr>
<tr>
<td>LOA</td>
<td>Disabled</td>
</tr>
<tr>
<td>LOF</td>
<td>Disabled</td>
</tr>
<tr>
<td>LTO</td>
<td>Disabled</td>
</tr>
<tr>
<td>PAY</td>
<td>Active</td>
</tr>
<tr>
<td>PLA</td>
<td>Disabled</td>
</tr>
<tr>
<td>POI</td>
<td>Active</td>
</tr>
<tr>
<td>POS</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
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 Section 4.7, “Setting Up the Lookup.PSFT.HRMS.WorkForceSync.EmpStatus Lookup Definition” for adding an entry in this lookup definition.

1.5.4.4.5 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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRB</td>
<td>Disabled</td>
</tr>
<tr>
<td>PRO</td>
<td>Active</td>
</tr>
<tr>
<td>REC</td>
<td>Active</td>
</tr>
<tr>
<td>STD</td>
<td>Disabled</td>
</tr>
<tr>
<td>SUB</td>
<td>Disabled</td>
</tr>
<tr>
<td>TDL</td>
<td>Disabled</td>
</tr>
<tr>
<td>TER</td>
<td>Disabled</td>
</tr>
<tr>
<td>TWB</td>
<td>Disabled</td>
</tr>
<tr>
<td>TWP</td>
<td>Disabled</td>
</tr>
<tr>
<td>XFR</td>
<td>Active</td>
</tr>
</tbody>
</table>

Note: The Decode values are case-sensitive.
### Code Key

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWR##T##D</td>
<td>Consultant</td>
</tr>
<tr>
<td>CWR##T##F</td>
<td>Temp</td>
</tr>
<tr>
<td>CWR#T##P</td>
<td>Intern</td>
</tr>
<tr>
<td>EMP##R##D</td>
<td>Consultant</td>
</tr>
<tr>
<td>EMP##R##F</td>
<td>Full-Time</td>
</tr>
<tr>
<td>EMP##R##P</td>
<td>Temp</td>
</tr>
<tr>
<td>EMP##T##D</td>
<td>Consultant</td>
</tr>
<tr>
<td>EMP##T##F</td>
<td>Part-Time</td>
</tr>
<tr>
<td>EMP##T##P</td>
<td>Temp</td>
</tr>
<tr>
<td>POI##R##D</td>
<td>Consultant</td>
</tr>
<tr>
<td>POI##R##F</td>
<td>Full-Time</td>
</tr>
<tr>
<td>POI##R##P</td>
<td>Temp</td>
</tr>
<tr>
<td>POI##T##D</td>
<td>Consultant</td>
</tr>
<tr>
<td>POI##T##F</td>
<td>Part-Time</td>
</tr>
<tr>
<td>POI##T##P</td>
<td>Temp</td>
</tr>
</tbody>
</table>

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.

#### 1.5.4.6 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.

#### 1.5.4.7 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.

#### 1.5.4.5 Other Lookup Definitions

The following are the predefined generic lookup definitions:
1.5.4.5.1 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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID resource object field name</td>
<td>List of user IDs separated by the tilde character (~)</td>
</tr>
</tbody>
</table>

See Section 2.3.1.2, "Setting Up the Lookup.PSFT.HRMS.ExclusionList Lookup Definition" for more information.

1.5.4.5.2 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 Section 3.4, "Limited Reconciliation" for more information. Section 4.6, "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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource object field name</td>
<td>Column name of the USR table</td>
</tr>
</tbody>
</table>

1.6 Roadmap for Deploying and Using the Connector

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

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" provides information about the tasks that must be performed each time you want to run reconciliation.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform to extend the functionality of the connector.
- Chapter 5, "Testing and Troubleshooting" provides information about testing the connector.
- Chapter 6, "Known Issues and Workarounds" lists the known issues associated with this release of the connector.
- Appendix A, "Determining the Root Audit Action Details" provides information about root audit action.
- Appendix B, "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.
- Appendix D, "Changing Default Message Versions" describes how to activate and deactivate message versions.
Deploying the connector involves the following steps:

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

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"
- Section 2.4, "Upgrading the Connector"

## 2.1 Preinstallation

Preinstallation information is divided across the following sections:

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

### 2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following 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>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration/PSFT_Employee_Reconciliation-CI.xml</td>
<td>This XML file contains configuration information that is used during connector installation.</td>
</tr>
<tr>
<td>JavaDoc</td>
<td>This directory contains information about the Java APIs used by the connector.</td>
</tr>
<tr>
<td>lib/PSFT_ER-oim-integration.jar</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 2–1 (Cont.) Files and Directories on the Installation Media

<table>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lib/PSFTCommon.jar</td>
<td>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.</td>
</tr>
</tbody>
</table>

The following files and directories in the listener directory:

- 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:

- 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.

<table>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>test/config/reconConfig.properties</td>
<td>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.</td>
</tr>
<tr>
<td>test/config/log.properties</td>
<td></td>
</tr>
<tr>
<td>test/lib/PSFTTest.jar</td>
<td>This JAR file is used by the testing utility for reconciliation.</td>
</tr>
<tr>
<td>test/scripts/InvokeListener.bat</td>
<td>This BAT file and the UNIX shell script call the testing utility for reconciliation.</td>
</tr>
<tr>
<td>test/scripts/InvokeListener.sh</td>
<td></td>
</tr>
<tr>
<td>xml/PeoplesoftHRMS-ConnectorConfig.xml</td>
<td>This XML file contains definitions for the connector components.</td>
</tr>
</tbody>
</table>
  - Resource object
  - Process definition
  - IT resource type
  - Reconciliation rules
  - Scheduled tasks
  - Lookup definitions

<table>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files in the resources directory</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note:** A resource bundle is a file containing localized versions of the text strings that include GUI element labels and messages.
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:

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

2.1.2.1 Importing a Project from Application Designer

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

You can import the OIM_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 Section 2.1.2.2.1, "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.
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:

- Section 2.1.2.2.1, "Creating a Permission List"
- Section 2.1.2.2.2, "Creating a Role for a Limited Rights User"
- Section 2.1.2.2.3, "Assigning the Required Privileges to the Target System Account"

2.1.2.2.1 Creating a Permission List

To create a permission list:

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:


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 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:
   

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**.
   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:
   

2. In the PeopleSoft Internet Architecture window:
   a. For PeopleTools 8.54 and earlier releases, expand **PeopleTools, Security, User Profiles**, and then click **User Profiles**.
   b. 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.

---

**Note:** Permission list **EOEI9000** is not available in PeopleTools 8.53 and above, and is hence not applicable.
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:

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

### 2.2.1 Installation on Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

- Section 2.2.1.1, "Running the Connector Installer"
- Section 2.2.1.2, "Copying the Connector Files and External Code Files"
- Section 2.2.1.3, "Configuring the IT Resource"
- Section 2.2.1.4, "Deploying the PeopleSoft Listener"
- Section 2.2.1.5, "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 Section 2.2.1.3, "Configuring the IT Resource" for more information.
   b. Configuring the scheduled tasks
      See Section 3.6, "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.

<table>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Destination for Oracle Identity Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>lib/PeopleSoftOIMListener.ear</td>
<td>$OIM_HOME/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/listener$</td>
</tr>
<tr>
<td>Files in the test/scripts directory</td>
<td>$OIM_HOME/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/scripts$</td>
</tr>
<tr>
<td>Files in the test/config directory</td>
<td>$OIM_HOME/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/config$</td>
</tr>
</tbody>
</table>

**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 Section 2.1.1.1, "Files and Directories on the Installation Media" for more information about these files.

If a particular destination directory does not exist on the Oracle Identity Manager host computer, then create it.

- 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.

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.

### Table 2–3  IT Resource Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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` |

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

### 2.2.1.4 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.
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:
  2. Run the following command:

```bash
java -jar ..///..//modules/com.bea.core.jarbuilder_1.3.0.0.jar
```
Start Oracle Identity Manager and the Admin Server.

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: 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.

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.

---

2.2.1.4.1 Deploying the PeopleSoft Listener on WebSphere Application Server

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

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

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

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

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

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

- Create the listener EAR file in listener directory. To do so:
a. Change directories to
$OIM_ORACLE_HOME/server/ConnectorDefaultDirectory/PSFT_ER-11.1.1.5.0/listener.

b. 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
rm -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
```

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.

```bash
$WAS_HOME/profiles/<Custom01>/bin/stopNode.sh
```
12. 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`.

### 2.2.1.4.2 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. Identify 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. Identify 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.

---

Installation

\$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`.

---

Oracle Identity Manager Connector Guide for PeopleSoft Employee Reconciliation
2.2.1.5 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:** Section 2.4.5, "Upgrading the PeopleSoft Listener" for information about upgrading the listener

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.

**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.


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:

- Section 2.2.2.1, "Configuring the Target System for Full Reconciliation"
- Section 2.2.2.2, "Configuring the Target System for Incremental Reconciliation"

#### 2.2.2.1 Configuring the Target System for Full Reconciliation

As described in Chapter 1, "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:

- Section 2.2.2.1.1, "Configuring the PeopleSoft Integration Broker"
- Section 2.2.2.1.2, "Configuring the PERSON_BASIC_FULLSYNC Service Operation"
- Section 2.2.2.1.3, "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**

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:

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.

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.
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: FTPTARGET
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.

Configuring the PERSON_BASIC_FULLSYNC Service Operation

To configure the PERSON_BASIC_FULLSYNC service operation perform the following procedures:


- 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
Deploying the Connector

- Displaying the EI Repository Folder
- Activating the PERSON_BASIC_FULLSYNC Message
- Activating the Full Data Publish Rule
- Publishing Messages With VERSION_5

**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:

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

---

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

5. Click Save.

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:

1. From the Queue Status list, select Run.

2. Click Save.
The queue status is highlighted in the following screenshot:

4. Click Return to Search.

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.

The link is highlighted in the following screenshot:
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 Appendix 2.1.2.2.1, "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:

d. Click Save.

e. Click Return to Search.
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: PSPT_HR
   - Receiver Node: OIM_FILE_NODE
   
   The following screenshot displays the Sender and Receiver nodes:

3. Click Save.

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

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

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

1. Click the Look up icon.
2. Click Default to sort the results in descending order.
   
The default active local node should meet the following criteria:
   - Local Node: 1
   - Default Local Node: Y
   - Node Type: PIA
   
Only one node can meet all the above conditions at a time.

3. Select the node.
4. Click Save.
To display the EI Repository folder:

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

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

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

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:
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:

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

   **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.

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

---

**Activating the Full Data Publish Rule**

You must define and activate 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:
4. Click Save.

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.
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**.
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.
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.

Configuring the WORKFORCE_FULLSYNC Service Operation

To configure the WORKFORCE_FULLSYNC service operation perform the following procedures:
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 Appendix D, “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:

---

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

5. Click **Save**.

**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:

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

2. Click **Save**.

---

The queue status is shown in the following screenshot:
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.

   
The link is shown in the following screenshot:
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 Appendix 2.1.2.2.1, "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
```

```
<table>
<thead>
<tr>
<th>Permission</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>OIMER</td>
<td>Full Access</td>
</tr>
</tbody>
</table>
```

d. Click Save.

e. Click Return to Search.

**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:
   
   1. Click the Look up icon.
   2. Click Default to sort the results in descending order.
      
      The default active local node should meet the following criteria:
      
      Local Node: 1
      Default Local Node: Y
      Node Type: PIA
      
      Only one node can meet all the above conditions at a time.

3. Select the node.

4. Click Save.

   **Receiver Node:** OIM_FILE_NODE

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

   ![Routing Definitions](image)

3. Click Save.

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

**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" on page 2-27, 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:

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

Activating the WORKFORCE_FULLSYNC Message

To activate the WORKFORCE_FULLSYNC message:
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:

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

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

Activating the Full Data Publish Rule

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:

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.
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.

- Section 2.2.2.2.1, "Configuring PeopleSoft Integration Broker"
- Section 2.2.2.2.2, "Configuring the PERSON_BASIC_SYNC Service Operation"
- Section 2.2.2.2.3, "Configuring the WORKFORCE_SYNC Service Operation"
- Section 2.2.2.2.4, "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:

Configuring PeopleSoft Integration Broker Gateway
Section "Configuring PeopleSoft Integration Broker Gateway" on page 2-18 describes the procedure to configure the PeopleSoft Integration Broker gateway.

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:

```properties
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:
   ```plaintext
   <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 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.

**Configuring the PERSON_BASIC_SYNC Service Operation**

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

**Activating the PERSON_BASIC_SYNC Service Operation**

To activate the PERSON_BASIC_SYNC 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. 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:
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:

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

The queue status is shown in the following screenshot:
4. Click Return to Search.

Setting Up the Security for the 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.

   The link is shown in the following screenshot:
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 Section 2.1.2.2.1, “Creating a Permission List.”

To attach the permission list:

**Note:** This procedure describes how to grant access to the 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

<table>
<thead>
<tr>
<th>Service</th>
<th>PERSON_BASIC_SYNC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>PERSON_BASIC_SYNC</td>
</tr>
</tbody>
</table>

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:

The following screenshot displays the preceding steps:

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

**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:
   1. Click the Look up icon.
   2. Click Default to sort the results in descending order.
      The default active local node should meet the following criteria:
      - Local Node: 1
      - Default Local Node: Y
      - Node Type: PIA
      Only one node can meet all the above conditions at a time.
   3. Select the node.
   4. Click Save.

   **Receiver Node:** OIM_NODE

   The following screenshot displays the Sender and Receiver nodes:

3. 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 Definitions Parameters Connector Properties]

- **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
- **Message.Ver into Transform 1:** PERSON_BASIC_SYNC.INTERNAL
- **Transform Program 1:** HMTF_TR_OA
- **Message.Ver out of Transforms:** PERSON_BASIC_SYNC.VERSION_3

- **Save**
- **Return**

---

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

---

**Out Req Transform**

**Default Message:** PERSON_BASIC_SYNC.INTERNAL  
**Out Message:** PERSON_BASIC_SYNC.VERSION_3
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" on page 2-27, 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](image)

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

Activating the PERSON_BASIC_SYNC Message
To activate PERSON_BASIC_SYNC messages:
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:

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

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:

   "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"

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

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

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

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

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 Message"

Activating the WORKFORCE_SYNC Service Operation
To activate the WORKFORCE_SYNC service operation:

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

2. On the Find Service Operation tab, enter 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:

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

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:

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

---

The queue status is shown in the following screenshot:

![Queue Status Screenshot]

4. Click Return to Search.

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.

The following screenshot displays the link:
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 Section 2.1.2.2.1, “Creating a Permission List.”

To attach the permission list:

**Note:** This procedure describes how to grant access to the 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:
d. Click Save.
e. Click Return to Search.

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
   - Receiver Node: OIM_NODE

   **Note:** The Sender Node is the default active local node. To locate the sender node:
   1. Click the Look up icon.
   2. Click Default to sort the results in descending order.
      The default active local node should meet the following criteria:
      - Local Node: 1
      - Default Local Node: Y
      - Node Type: PIA
      Only one node can meet all the above conditions at a time.
   3. Select the node.
   4. Click Save.

   Receiver Node: OIM_NODE

   The following screenshot displays the Sender and Receiver nodes:
3. Click **Save**.

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

**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:
4. Click Save.

5. Log out, and then log in.

**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:
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.

2.2.2.4 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 "Removing Unwanted Fields at Message Level" section for more information.

■ If active routings exist, analyze the subscription or handler code of the routing to determine the fields they are utilizing and the ones not needed in Oracle Identity Manager. If so, remove the unwanted fields at message level. See "Removing Unwanted Fields at Message Level" section for more information.

■ Lastly, if there are active routings that use these sensitive fields that you do not want to transmit to Oracle Identity Manager, then you need to write a transformation.

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


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

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

2. Search for and open the desired message, for example, PERSON_BASIC_SYNC.VERSION_3 used for incremental reconciliation.

3. Expand the message.

4. Navigate to the field that you do not want to transmit to Oracle Identity Manager, for example, NAME_ROYAL_PREFIX.
5. Click the field and clear the **Include** check box.

![Message Field Properties](image)

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

### 2.3 Postinstallation

Postinstallation information is divided across the following sections:
- Section 2.3.1, "Configuring Oracle Identity Manager"
- Section 2.3.2, "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.

- Section 2.3.1.1, "Enabling Logging"
- Section 2.3.1.2, "Setting Up the Lookup.PSFT.HRMS.ExclusionList Lookup Definition"
- Section 2.3.1.3, "Setting Up the Lookup.PSFT.HRMS.Configuration Lookup Definition"
- Section 2.3.1.4, "Configuring SSL"
- Section 2.3.1.5, "Creating an Authorization Policy for Job Code"
- Section 2.3.1.6, "Displaying UDFs in Oracle Identity Manager 11.1.2.x or Later"

2.3.1.1 Enabling Logging

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>
<thead>
<tr>
<th>Java Level</th>
<th>ODL Message Type:Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEVERE.intValue()+100</td>
<td>INCIDENT_ERROR:1</td>
</tr>
<tr>
<td>SEVERE</td>
<td>ERROR:1</td>
</tr>
<tr>
<td>WARNING</td>
<td>WARNING:1</td>
</tr>
</tbody>
</table>

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster.
The configuration file for OJDL is logging.xml, which is located at the following path:

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

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

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:
   a. Add the following blocks in the file:
      ```xml
      <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]`:
      ```xml
      <log_handler name='psft-er-handler' level='NOTIFICATION:1' class='oracle.core.ojdl.logging.ODLHandlerFactory'>
        <property name='logreader:' value='off'/>
        <property name='path'
      ```

<table>
<thead>
<tr>
<th>Java Level</th>
<th>ODL Message Type:Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO</td>
<td>NOTIFICATION:1</td>
</tr>
<tr>
<td>CONFIG</td>
<td>NOTIFICATION:16</td>
</tr>
<tr>
<td>FINE</td>
<td>TRACE:1</td>
</tr>
<tr>
<td>FINER</td>
<td>TRACE:16</td>
</tr>
<tr>
<td>FINEST</td>
<td>TRACE:32</td>
</tr>
</tbody>
</table>

Table 2–4 (Cont.) Log Levels and ODL Message Type:Level Combinations
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 Section 1.5.4.5.1, "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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID [PATTERN]</td>
<td>User001</td>
</tr>
</tbody>
</table>

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 Section 1.5.4.1, "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:

- Section 2.3.1.4.1, "Configuring SSL on IBM WebSphere Application Server"
- Section 2.3.1.4.2, "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

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

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

1. Log in to the WebSphere Integrated Solutions Console. The URL may be similar to the following:
   
   https://localhost:9043/ibm/console/logon.jsp

2. Click Security, SSL certificate and key management, Related items, Key stores and certificates, NodeDefaultKeyStore, and then click Personal certificates.

3. Click Create a self-signed certificate.

4. In the Alias field, enter an alias name. You specify the alias name to identify the certificate request in the keystore.

5. In the CN field, enter a value for common name. The common name must be the fully qualified DNS host name or the name of the computer. The CN of the certificate must match the domain name or the name of the computer. For example, if the name of your domain is us.example.com, then the CN of the SSL certificate that you create for your domain must also be us.example.com.

6. In the Organization field, enter an organization name.

7. In the Organization unit field, specify the organization unit.

8. In the Locality field, enter the locality.

9. In the State or Province field, enter the state.

10. In the Zip Code field, enter the zip code.

11. From the Country or region list, select the country code.

12. Click Apply and then Save.

13. Click Security, SSL certificate and key management, Related items, Key stores and certificates, NodeDefaultKeyStore, and then click Personal certificates.

14. Select the check box for the new alias name.

15. Click Extract.

16. Specify the absolute file path where you want to extract the certificate under the certificate file name, for example, C:\SSLCerts\sslcert.cer.
17. Click **Apply** and then click **OK**.

**Configuring SSL on IBM WebSphere Application Server with a CA Certificate**

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

1. Log in to the WebSphere Integrated Solutions Console. The URL may be similar to the following:

   ```
   https://localhost:9043/ibm/console/logon.jsp
   ```

2. Click **Security, SSL certificate and key management, Related items, Key stores and certificates, NodeDefaultKeyStore**.

3. On the Additional Properties tab, click **Personal certificate requests**.

4. Click **New**.

5. In the **File for certificate request** field, enter the full path where the certificate request is to be stored, and a file name. For example: `c:\servercertreq.arm` (for a computer running on Microsoft Windows).

6. In the **Key label** field, enter an alias name. You specify the alias name to identify the certificate request in the keystore.

7. In the **CN** field, enter a value for common name. The common name must be the fully-qualified DNS host name or the name of the computer. The CN of the certificate must match the domain name of your community. For example, if the name of your domain is `us.example.com`, then the CN of the SSL certificate that you create for your community must also be `us.example.com`.

8. In the **Organization** field, enter an organization name.

9. In the **Organization unit** field, specify the organization unit.

10. In the **Locality** field, enter the locality.

11. In the **State or Province** field, enter the state.

12. In the **Zip Code** field, enter the zip code.

13. From the **Country or region** list, select the country code.

14. Click **Apply** and then **Save**. The certificate request is created in the specified file location in the keystore. This request functions as a temporary placeholder for the signed certificate until you manually receive the certificate in the keystore.

   **Note:** Keystore tools such as iKeyman and keyTool cannot receive signed certificates that are generated by certificate requests from IBM WebSphere Application Server. Similarly, IBM WebSphere Application Server cannot accept certificates that are generated by certificate requests from other keystore utilities.

15. Send the certification request arm file to a CA for signing.

16. Create a backup of your keystore file. You must create this backup before receiving the CA-signed certificate into the keystore. The default password for the keystore is WebAS. The Integrated Solutions Console contains the path information for the location of the keystore. The path to the NodeDefaultKeyStore is listed in the Integrated Solutions Console as:
Now you can receive the CA-signed certificate into the keystore to complete the process of generating a signed certificate for IBM WebSphere Application Server.

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

1. In the WebSphere Integrated Solutions Console, click **Security, SSL certificate and key management, Related items, Key stores and certificates, NodeDefaultKeyStore**, and then click **Personal Certificates**.

2. Click **Receive a certificate from a certificate authority**.

3. Enter the full path and name of the certificate file.

4. Select the default data type from the list.

5. Click **Apply** and then **Save**.

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

### 2.3.1.4.2 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:

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

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

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

- Generating Keystore
- Configuring Oracle WebLogic Server

#### Generating Keystore

To generate the keystore:

1. Run the following command:

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

   For example:

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

   See Also: Appendix C, "Setting Up SSL on Oracle WebLogic Server"
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:

```bash
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:

```bash
keytool -export -alias ALIAS_NAME -keystore ABSOLUTE_KEYSTORE_PATH -file CERTIFICATE_FILE.Absolute_PATH
```

For example:

```bash
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:

```bash
keytool -import -alias ALIAS_NAME -keystore NEW_KEYSTORE.Absolute_PATH -file CERTIFICATE_FILE.Absolute_PATH
```

For example:

```bash
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:

---

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

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

**Configuring Oracle WebLogic Server**

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

1. Log in to the Oracle WebLogic Server console at [http://localhost:7001/console](http://localhost:7001/console) and perform the following:
   a. Expand the servers node and select the oim server instance.
   b. Select the General tab.
   c. Select the SSL Listen Port Enabled option.
   d. Ensure that a valid port is specified in the SSL Listen Port field. The default port is 7002.
   e. Click Apply to save your changes.

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

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

4. Configure the keystore properties. To do so:
   a. In the Custom Identity Key Store File Name column, specify the full path of the keystore generated in Step 1 of Generating Keystore, for example, `c:\temp\keys\keystore.jks`. In the Custom Identity Key Store Type column, specify the type of keystore, for example, JKS. In the Custom Identity Key Store Pass Phrase and Confirm Custom Identity Key Store Pass Phrase columns, specify the keystore password.
   b. Provide the Java standard trust keystore pass phrase and the Confirm Java standard trust keystore pass phrase. The default password is changeit, unless you change the password.
   c. Click Continue.

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

6. Click Finish.

7. Restart Oracle WebLogic Server. If the server starts successfully with the SSL configuration, then lines similar to the following are recorded in the startup log:

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

---

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

- Generating Keystore
- Configuring Oracle WebLogic Server

### Generating Keystore

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

1. Run the following command:

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

   For example:

   ```shell
   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:

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

   **Note:**

   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:

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

For example:

```bash
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:

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

For example:

```bash
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:

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

For example:

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

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

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

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

**Configuring Oracle WebLogic Server**

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

1. Log in to the Oracle WebLogic Server console ((http://localhost:7001/console) and perform the following:
   a. Expand the server node and select the server instance.
   b. Select the **General** tab.
   c. Select the **SSL Port Enabled** option.
d. Ensure that a valid port is specified in the SSL Listen Port field. The default port is 7002.
e. Click Apply to save your changes.

2. Click the Keystore & SSL tab, and click the Change link.
3. From the Keystores list, select Custom Identity And Custom Trust, and then click Continue.
4. Configure the keystore properties. To do so:
   a. In the Custom Identity Key Store File Name column, specify the full path of the keystore generated in Step 1 of "Generating Keystore" on page 2-72, for example, c:\temp\keys\keystore.jks. In the Custom Identity Key Store Type column, specify the type of keystore, for example, JKS. In the Custom Identity Key Store Pass Phrase and Confirm Custom Identity Key Store Pass Phrase columns, specify the keystore password.
   b. In the Custom Trust and Custom Trust Key Store File Name column, specify the full path of the keystore generated in Step 1 of "Generating Keystore" on page 2-72, 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 11g 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 the following procedure:

**Configuring SSL**

To configure SSL:

1. Copy the certificate to the computer on which PeopleSoft HRMS/HCM is installed.
2. Run the following command:
   ```bash
   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:

- Section 2.4.1, "Prerequisites for Upgrading the Connector"
- Section 2.4.2, "Re-defining the Connector"
- Section 2.4.3, "Running the Upgrade Wizard"
- Section 2.4.4, "Upgrading the Connector Files and External Code Files"
- Section 2.4.5, "Upgrading the PeopleSoft Listener"
- Section 2.4.6, "Upgrading the Customizations"
- Section 2.4.7, "Updating the PeopleSoft Target System"
- Section 2.4.8, "Compiling the Adapters"
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:
   1. Log in to the Administrative and User Console.
   2. On the Welcome to Identity Manager Advanced Administration page, under the System Management section, click Manage Connector.
   3. Click Define.
   4. In Step 1 of the Connector Management Wizard, select Resource from the drop-down box and search for Peoplesoft HRMS.
   5. In the Search Results region, select the Peoplesoft HRMS check box and click Select Children, as shown in the following screenshot.
6. 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.

7. 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.
8. In Step 4, click **Add For Define**, as shown in the following screenshot.

9. 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.
2. Add the Peoplesoft HRMS scheduled tasks. To do so:

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

2. 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](image)

3. 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**.

![Connector Management Wizard](image)

4. In Step 3, in the Select Dependencies region, ensure the Peoplesoft HRMS scheduled tasks are selected, as shown in the following screenshot. Click **Confirmation**.
5. In Step 4, click **Add For Define**.

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

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

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/People softHRMS-ConnectorConfig.xml

   The PeoplesoftHRMS-ConnectorConfig.xml file contains definitions for the connector components. See Section 2.1.1.1, "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.

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.

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.
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**.

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**.
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.

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:

<table>
<thead>
<tr>
<th>JAR File Name</th>
<th>JAR Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSFTER.jar</td>
<td>2 - ScheduledTask</td>
</tr>
<tr>
<td>PSFTCommon.jar</td>
<td>1 - JavaTasks</td>
</tr>
<tr>
<td>Common.jar</td>
<td>1 - JavaTasks</td>
</tr>
</tbody>
</table>

Remove this file only if no other connector is using it.

**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:
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 Section 2.2.1.5, "Removing the PeopleSoft Listener."

2. Deploy the new PeopleSoft listener by performing the procedure described in Section 2.2.1.4, "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 Section 4.4, "Configuring Validation of Data During Reconciliation" and Section 4.5, "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 Section 4.4, "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 Section 4.5, "Configuring Transformation of Data During Reconciliation."
3. Update the entries in the connector configuration lookup, Lookup.PSFT.HRMS.Configuration.

   See Section 1.5.4.1, "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 Section 2.3.1.6, "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 Section 2.2.2.1, "Configuring the Target System for Full Reconciliation" and Section 2.2.2.1, "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.
After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

- Section 3.1, "Summary of Steps to Use the Connector"
- Section 3.2, "Performing Full Reconciliation"
- Section 3.3, "Performing Incremental Reconciliation"
- Section 3.4, "Limited Reconciliation"
- Section 3.5, "Resending Messages That Are Not Received by the PeopleSoft Listener"
- Section 3.6, "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:

1. Generate XML files for the PERSON_BASIC_FULLSYNC message for all persons. See Section 3.2.1.1, "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 Section 3.2.1.2, "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 Section 3.2.2.1, "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
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:

- Section 3.2.1, "Generating XML Files"
- Section 3.2.2, "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 Section 3.2.2, "Importing XML Files into Oracle Identity Manager" for more information.

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

Running the Messages for Full Data Publish

This section describes the procedures for generating XML files.

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.

- Section 3.2.1.1, "Running the PERSON_BASIC_FULLSYNC Message"
- Section 3.2.1.2, "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.
Performing Full Reconciliation

Using the Connector

Process Frequency: Select Always.

Message Name: Select PERSON_BASIC_FULLSYNC.

The following screenshot displays the preceding steps:

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:

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 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.
Performing Full Reconciliation

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:

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:

---

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.
Performing Full Reconciliation

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 PeopleSoft Integration Broker" on page 2-19 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" on page 2-36 section. This is for security purposes.

### 3.2.2 Importing XML Files into Oracle Identity Manager

Section 3.2.2.1, "Configuring the Scheduled Task for Person Data Reconciliation" section describes the procedure to configure the scheduled task.

Section 3.2.2.2, "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 Section 3.6, "Configuring Scheduled Tasks" for instructions on running the scheduled task.
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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive Mode</td>
<td>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.</td>
</tr>
<tr>
<td>Archive Path</td>
<td>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</td>
</tr>
<tr>
<td>File Path</td>
<td>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</td>
</tr>
<tr>
<td>IT Resource Name</td>
<td>Enter the name of the IT resource that you create by performing the procedure described in Section 2.2.1.3, &quot;Configuring the IT Resource.&quot; Default value: PSFT HRMS</td>
</tr>
<tr>
<td>Message Name</td>
<td>Use this attribute to specify the name of the delivered message used for full reconciliation. Sample value: PERSON_BASIC_FULLSYNC or WORKFORCE_FULLSYNC</td>
</tr>
<tr>
<td>Task Name</td>
<td>This attribute holds the name of the scheduled task. Value: Peoplesoft HRMS Trusted Reconciliation</td>
</tr>
</tbody>
</table>

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 Section 2.3.1.6, "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.
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:

- 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 Section 1.5.4.2, "Lookup.PSFT.HRMS.ManagerRecon.Configuration" for information about this lookup.

When it is run, this scheduled task performs the process described in Section 1.4.8.3, "Steps 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 Section 2.2.1.4, "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 Section 1.5.4.4.4, "Lookup.PSFT.HRMS.WorkForceSync.EmpStatus” for more information.

---

### 3.4 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current incremental reconciliation run. For full reconciliation, all target system records are fetched into Oracle Identity Manager.

You 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
```
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:** Section 1.5.4.5.2, "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 Section 4.6, "Setting Up the Lookup.PSFT.HRMS.CustomQuery Lookup Definition" for adding an entry in this lookup definition and Section 4.2, "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:

Manually Sending Messages

If Oracle Identity Manager is not running when a message is published, then the message is added to a queue. You can check the status of the message in the queue in the Message Instance tab. This tab lists all the published messages in 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 Section 2.1.2.2, "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.

3. Click the link pertaining to the message to be resent, for example, the link under the Error or the TimeOut column.

You are taken to the Operation Instance tab.
4. Click the Details link of the message to be resent. A new window appears.

**Asynchronous Details**

<table>
<thead>
<tr>
<th>Transaction ID</th>
<th>Internal Service Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5098513c-4867-11da-84e6-a9f58d55f97f</td>
<td>PERSON_DATA</td>
</tr>
</tbody>
</table>

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.

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

**Table 3–3  Scheduled Tasks for Reconciliation**

<table>
<thead>
<tr>
<th>Scheduled Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeopleSoft HRMS Trusted Reconciliation</td>
<td>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 Section 3.2.2.1, &quot;Configuring the Scheduled Task for Person Data Reconciliation&quot; for information about this scheduled task.</td>
</tr>
<tr>
<td>PeopleSoft HRMS Manager Reconciliation</td>
<td>This scheduled task is used for reconciling Manager ID values during full reconciliation. See Section 3.2.2.2, &quot;Running the PeopleSoft HRMS Manager Reconciliation Scheduled Task&quot; for information about this scheduled task.</td>
</tr>
</tbody>
</table>
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:
   a. 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.

---
Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

- Section 4.1, "Adding New Attributes for Full Reconciliation"
- Section 4.2, "Adding New Attributes for Incremental Reconciliation"
- Section 4.3, "Modifying Field Lengths on the OIM User Form"
- Section 4.4, "Configuring Validation of Data During Reconciliation"
- Section 4.5, "Configuring Transformation of Data During Reconciliation"
- Section 4.6, "Configuring the Lookup.PSFT.HRMS.CustomQuery Lookup Definition"
- Section 4.7, "Configuring the Lookup.PSFT.HRMS.WorkForceSync.EmpStatus Lookup Definition"
- Section 4.8, "Configuring the Connector for Multiple Installations of the Target System"

4.1 Adding 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:

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.
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 Creating a User-Defined Field on page 4-6.

   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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttributeName</td>
<td>NODE<del>PARENT NODE</del>NODE</td>
</tr>
<tr>
<td></td>
<td>TYPE=Value~EFFECTIVE DATED</td>
</tr>
<tr>
<td></td>
<td>NODE~PRIMARY</td>
</tr>
</tbody>
</table>

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:
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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>RO Attribute</td>
<td>ATTRIBUTE FIELD-LOOKUP NAME</td>
</tr>
</tbody>
</table>

For example:
Code Key: Employee ID
Decode: Empl ID
The following screenshot displays the mapping:
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 Section 4.6, "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 Creating a User-Defined Field on page 4-6.

   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:

      \[ \text{Employee ID} = \text{Employee ID} \]
Adding New Attributes for Incremental Reconciliation

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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttributeName</td>
<td>NODE<del>PARENT NODE</del>NODE</td>
</tr>
<tr>
<td></td>
<td>TYPE=Value~EFFECTIVE DATED</td>
</tr>
<tr>
<td></td>
<td>NODE~PRIMARY</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>RO Attribute</td>
<td>ATTRIBUTE FIELD~LOOKUP NAME</td>
</tr>
</tbody>
</table>

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 Section 4.6, "Setting Up the Lookup.PSFT.HRMS.CustomQuery Lookup Definition" for more information.

Creating a User-Defined Field
To create a UDF on Oracle Identity Manager:

1. Log in to the Oracle Identity Management Administration Console.
2. Click **Advanced**.
3. On the Configuration tab, click **User Configuration**.
4. From the Actions menu, select **User Attributes**.
5. Click **Create Attribute**.
6. Enter details of the attribute (UDF) that you want to create. From the Category list, select Custom Attributes.

7. Set values for the attribute properties.

8. 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.

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 (#):

```java
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.
         */
        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;
    }
}
```

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:
Configuring Validation of Data During Reconciliation

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:
  
  \textit{OIM\_HOME/server/bin/UploadJars.bat}

- For UNIX:
  
  \textit{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 \textit{Lookup.PSFT.Message.WorkForceSync.Configuration} lookup definition for the WORKFORCE\_SYNC message. See Section 1.5.4.4.1, "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 \textit{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:

   \textit{CONN\_HOME/listener/deployable-archive/PeopleSoftOIMListener.ear/PeopleSoftOIMListener.war/WEB-INF/lib}

7. Redeploy the PeopleSoftOIMListener.ear file on the application server. To do so, run the following command:

   \texttt{ant redeploy}
See Section 2.2.1.4, "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:

   ```java
   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:
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 Section 1.5.4.4.1, "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.

   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/PeopleSoftOIMListener.ear/PeopleSoft OIMListener.war/WEB-INF/lib

7. Redeploy the PeopleSoftOIMListener.ear file on the application server. To do so, run the following command:

   ant redeploy

---

**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.

---
See Section 2.2.1.4, "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 Section 1.5.4.5.2, "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.
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:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>RO Attribute Name</td>
<td>Column name of the USR table</td>
</tr>
</tbody>
</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 Section 1.5.4.4.4, "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:

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.
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

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**

<table>
<thead>
<tr>
<th>Connector Object</th>
<th>Name</th>
<th>Referenced By</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Resource</td>
<td>PSFT HRMS</td>
<td>• Scheduled Task: Peoplesoft HRMS Trusted Reconciliation&lt;br&gt;• Resource Object: Peoplesoft HRMS</td>
<td>You need to create a copy of IT Resource with a different name.</td>
</tr>
<tr>
<td>Resource Object</td>
<td>Peoplesoft HRMS</td>
<td>Message-specific configuration lookup definitions: &lt;br&gt;• Lookup.PSFT.Message.PersonBasicSync.Configuration&lt;br&gt;• Lookup.PSFT.Message.WorkForceSync.Configuration</td>
<td>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. <strong>Note:</strong> Create copies of this resource object only if there are differences in attributes between the two installations of the target system.</td>
</tr>
<tr>
<td>Common Configuration</td>
<td>Lookup.PSFT.HRMS</td>
<td>Message-specific configuration lookup definitions: &lt;br&gt;• Lookup.PSFT.Message.PersonBasicSync.Configuration&lt;br&gt;• Lookup.PSFT.Message.WorkForceSync.Configuration</td>
<td>It is optional to create a copy of the common configuration lookup definition. <strong>Note:</strong> Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.</td>
</tr>
</tbody>
</table>
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 Section 2.2.1.3, "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 Section 1.5.4.1, "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.

6. Create a copy of the Peoplesoft HRMS Trusted Reconciliation scheduled task. See Section 3.2.2.1, "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.
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.

- Section 5.1, "Testing Reconciliation"
- Section 5.2, "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 Section 2.1.1.1, "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
      ```
i) 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:

---

**Note:** Ensure that there is no blank or white-space character in the directory path and file name that you specify.
**Problem Description**

You might receive the following error message while reconciling job data:

```
ERROR [PSFTCOMMON]
================================
ERROR [PSFTCOMMON]
oracle.iam.connectors.psft.common.handler.HandlerFactory:
getMessageHandler:
No Lookup defined for 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.

**Solution**

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:


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.
The following is an issue and workaround associated with this release of the connector:

6.1 Connector Issues

The following is an issue and workaround associated with the connector:

6.1.1 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.
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:
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:
The nonzero level PSCAMA node and its Root Audit Action are shown in the following screenshot:
Configuring the Connector Messages

You can configure the connector messages of release 9.1.0.x.y with that of the current release as follows:

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 Section 2.2.1.5, "Removing the PeopleSoft Listener" for the procedure.

7. Copy the validation JAR file created in Step 4 to the following directory:
   PeopleSoftOIMListener.ear/PeopleSoftOIMListener.war/WEB-INF/lib

8. Redeploy the PeopleSoftOIMListener.ear file on the application server. See Section 2.2.1.4, "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.

**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.HRMS.XellerateUser.EmpStatus
- `Lookup.PSFT.HRMS.XellerateUser.EmpType`
- `Lookup.PSFT.HRMS.XellerateUser.AttributeMapping`
- `Lookup.PSFT.HRMS.XellerateUser.Recon`

**Lookup.PSFT.Message.XellerateUser.Configuration**

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Mapping Lookup</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.AttributeMapping</code></td>
</tr>
<tr>
<td>Custom Query</td>
<td>Enter a Value</td>
</tr>
<tr>
<td>Custom Query Lookup Definition</td>
<td><code>Lookup.PSFT.HRMS.CustomQuery</code></td>
</tr>
<tr>
<td>Data Node Name</td>
<td>Transaction</td>
</tr>
<tr>
<td>Employee Status Lookup</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.EmpStatus</code></td>
</tr>
<tr>
<td>Employee Type Lookup</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.EmpType</code></td>
</tr>
<tr>
<td>Recon Lookup Definition</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.Recon</code></td>
</tr>
<tr>
<td>Message Handler Class</td>
<td><code>oracle.iam.connectors.psft.common.handler.impl.PSFTXellerateUserReconMessageHandlerImpl</code></td>
</tr>
<tr>
<td>Message Parser</td>
<td><code>oracle.iam.connectors.psft.common.parser.impl.XellerateUserMessageParser</code></td>
</tr>
<tr>
<td>Organization</td>
<td>Xellerate Users</td>
</tr>
<tr>
<td>Resource Object</td>
<td>Peoplesoft HRMS</td>
</tr>
<tr>
<td>Transformation Lookup Definition</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.Transformation</code></td>
</tr>
<tr>
<td>User Type</td>
<td>End-User</td>
</tr>
<tr>
<td>Use Transformation</td>
<td>No</td>
</tr>
<tr>
<td>Use Validation</td>
<td>No</td>
</tr>
<tr>
<td>Validation Lookup Definition</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.Validation</code></td>
</tr>
</tbody>
</table>

**Lookup.PSFT.Message.XellerateUser.Configuration**

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Mapping Lookup</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.AttributeMapping</code></td>
</tr>
<tr>
<td>Custom Query</td>
<td>Enter a Value</td>
</tr>
<tr>
<td>Custom Query Lookup Definition</td>
<td><code>Lookup.PSFT.HRMS.CustomQuery</code></td>
</tr>
<tr>
<td>Data Node Name</td>
<td>Transaction</td>
</tr>
<tr>
<td>Employee Status Lookup</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.EmpStatus</code></td>
</tr>
<tr>
<td>Employee Type Lookup</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.EmpType</code></td>
</tr>
<tr>
<td>Recon Lookup Definition</td>
<td><code>Lookup.PSFT.HRMS.XellerateUser.Recon</code></td>
</tr>
<tr>
<td>Message Handler Class</td>
<td><code>oracle.iam.connectors.psft.common.handler.impl.PSFTXellerateUserReconMessageHandlerImpl</code></td>
</tr>
<tr>
<td>Message Parser</td>
<td><code>oracle.iam.connectors.psft.common.parser.impl.XellerateUserMessageParser</code></td>
</tr>
<tr>
<td>Organization</td>
<td>Xellerate Users</td>
</tr>
</tbody>
</table>
### Configuring the Connector Messages

**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

#### Lookup.PSFT.HRMS.XellerateUser.EmpStatus

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Active</td>
</tr>
<tr>
<td>I</td>
<td>Inactive</td>
</tr>
</tbody>
</table>

#### Lookup.PSFT.HRMS.XellerateUser.AttributeMapping

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>DEPTID~JOB</td>
</tr>
<tr>
<td>Emp Type</td>
<td>EMPLOYEETYPE~JOB</td>
</tr>
<tr>
<td>First Name</td>
<td>FIRST_NAME~PERSONAL_DATA</td>
</tr>
<tr>
<td>Last Name</td>
<td>LAST_NAME~PERSONAL_DATA</td>
</tr>
<tr>
<td>Job ID</td>
<td>JOBCODE~JOB</td>
</tr>
<tr>
<td>Status</td>
<td>STATUS~JOB</td>
</tr>
<tr>
<td>User ID</td>
<td>EMPLID<del>PERSONAL_DATA</del>None<del>None</del>PRIMARY</td>
</tr>
</tbody>
</table>

#### Lookup.PSFT.HRMS.XellerateUser.Recon

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Department</td>
</tr>
<tr>
<td>Employee Type</td>
<td>Emp Type~Employee Type Lookup</td>
</tr>
<tr>
<td>First Name</td>
<td>First Name</td>
</tr>
<tr>
<td>Last Name</td>
<td>Last Name</td>
</tr>
<tr>
<td>Job Code</td>
<td>Job ID</td>
</tr>
<tr>
<td>Status</td>
<td>Status~Employee Status Lookup</td>
</tr>
<tr>
<td>User ID</td>
<td>User ID</td>
</tr>
</tbody>
</table>
Setting Up SSL on Oracle WebLogic Server

This section describes how to configure SSL on Oracle WebLogic Server for PeopleTools 8.50.

To set up SSL on Oracle WebLogic Server:

1. Generate signed public encryption key and certificate signing request (CSR).
   a. Start PSKeyManager by navigating to the appropriate directory on the MS-DOS command prompt.
   b. Enter the following at the command line:
      pskeymanager -create

      The PSKeyManager opens.

   c. Enter the following at the command line:
      
      At the Enter current keystore password [press ENTER to quit] command prompt, enter the password. The default password is password.

      At the Specify an alias for this certificate <host_name>? command prompt, enter the certificate alias and press Enter. The default certificate alias is the local machine name.

      At the What is the common name for this certificate <host_name>? command prompt, enter the host name for the certificate, for example <host_name>.corp.myorg.com.

      Press Enter.
Enter the appropriate information at the following command prompts:

- **Organization unit**
- **Organization**
- **City or Locality**
- **State or Province**
- **Country code**
- **Number of days the certificate should be valid** (Default is 90.)
- **Key size to use** (Default is 1024.)
- **Key algorithm** (Default is RSA.)
- **Signing algorithm** (Default is MD5withRSA or SHA1withDSA.)

**d.** At the **Enter a private key password <press ENTER to use keystore password>** prompt, specify the password or press **Enter.**

**e.** Verify that the values you entered are correct, and press **Enter.**

The PSKeyManager generates a public key and provides the CSR that you must submit to the Certificate Authority (CA) for signing.

The following example shows a sample CSR:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBtDCCAR0CAQAwdDELMAkGA1UEBhMCVVMxEDAOBgNVBAgTB0FyaXpvbmExEDAOBgNVBAcTB1B
```
The CSR is a text file, and is written to the \<PSFT_HOME>\webserv\peoplesoft directory. The file name is <host_name>_certreq.txt.

2. Submit CSRs to CAs for signing:

   a. Click Download a CA certificate, certificate chain, or CRL.

   b. Click advanced certificate request.
c. Click Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

d. Paste the content of the CSR in the Saved Request list box.

e. Download and save the signed public key on your local drive.
3. Download the root certificate.
   a. Click Download a CA certificate, certificate chain, or CRL.
   b. From the CA certificate list, select the certificate.
   c. Download and save the root certificate on your local drive.

4. Import a server-side public key into a keystore.
   a. Open PSKeyManager.
   b. Navigate to the required directory on the MS-DOS command prompt.
c. Enter the following at the command line:

```
pskeymanager -import
```

d. At the `Enter current keystore password` command prompt, enter the password and press **Enter**.

e. At the `Specify an alias for this certificate <host_name>?` command prompt, enter the certificate alias and press **Enter**.

f. At the `Enter the name of the certification file to import` command prompt, enter the path and name of the certificate to import.

g. At the `Trust this certificate` command prompt, enter **Yes** and press **Enter**.
5. Generate and import public keys.
   
a. Place the public key from your CA in the keystore. The location of the keystore is as follows:
   
   `<PSFT_HOME>\webserv\peoplesoft\keystore`

   b. Install the certificate for server authentication SSL on Oracle WebLogic Server using the following command:
   
   `pskeymanager -import`

   c. At the `Enter current keystore password` command prompt, enter the password and press Enter.

   d. At the `Specify an alias for this certificate <host_name>?` command prompt, enter the certificate alias and press Enter.

   e. At the `Enter the name of the certification file to import` command prompt, enter the path and name of the certificate to import.
Certificate is successfully installed in the keystore.

6. Configuring the Oracle WebLogic Server to use the keystore.
   a. Log in to Oracle WebLogic Administration Console.

   ![Oracle WebLogic Administration Console]

   b. Expand PeopleSoft, Environment, Servers, PIA to setup the SSL configuration for the PIA server.
c. Click the Keystores tab.
d. From the Keystores list, select Custom Identity and Custom Trust.
e. In the Identity region, complete the following fields:
   - In the Custom Identity Keystore field, enter keystore/pskey.
   - In the Custom Identity Keystore Type field, enter JKS.
   - In the Custom Identity Keystore Passphrase field, enter password.
   - In the Confirm Custom Identity Keystore Passphrase field, enter password again.
f. On the SSL tab, ensure that the parameter **Two Way Client Cert Behavior** is set to **Client Certs Requested and Enforced**.

![SSL Tab Screenshot]

- **Two Way Client Cert Behavior**: Option to select the type of client certificate handling.
- **Client Certs Requested and Enforced**: Indicates the client certificate must be requested and enforced during the SSL connection.

![Activate Changes Button]

- **Activate Changes**: Button to apply the changes made to the SSL settings.

![WebLogic Server Console]

- **WebLogic Server Administration Console**: Interface for managing SSL settings and other configurations.
- **Settings updated successfully**: Message confirming the successful application of changes.

- **Domain Structure**: Section for configuring domain-level settings.

- **Identity and Trust Locations**: Area for specifying locations for identity and trust information.

- **Private Key Location**: Field to specify the location of the private key.

- **Configuration**: Tab for setting various aspects like protocols, logging, debug, monitoring, control, deployments, services, and security.
7. Add root certificate.
   a. Expand Security, Security Objects, and then click Digital Certificates.

   ![Digital Certificates](image1)

   b. Click Add Root.

8. Configure the Peoplesoft certificates.

   ![Digital Certificates](image2)

   **Note:** You can use the same root certificate generated in Step 2.

   a. Expand Security, Security Objects, and then click Digital Certificates.
   b. Add a local node type certificate.
   c. Set Alias to the default local node.

   d. Click Request.
   e. Send this certificate request to the CA to get a new certificate.
f. Click OK.

g. Ensure that the local node appears on the Digital Certificates list.

h. Click Import.
The Import Certificate page appears.

1. Click OK.

j. Click Load Gateway Connectors.
The following message appears:

Loading Process was successful. Number of connectors loaded: 0. Number of Properties loaded: 0. (158.42)

Click OK.

k. Click Ping Node to ping your local node.
Changing Default Message Versions

This appendix describes the following procedures:

- Appendix D.1, "Activating a Message Version"
- Appendix D.2, "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.
4. Select the **Default** and **Active** checkboxes highlighted in the following screenshot and click **Save**.
Then, the VESRION_3 message is activated and set as default.
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.
4. Deselect the **Default** and **Active** checkboxes highlighted in the following screenshot and click **Save**.
Then, the VESRION_5 message is deactivated.
Index

A
adding new attributes
   for full reconciliation, 4-1
   for incremental reconciliation, 4-5
Application Designer
   importing a project, 2-3
   architecture, 1-3

C
certified components, 1-1
   clones, 4-13
   cloning connector, 4-13
   configuring
      full reconciliation, 3-2
      PeopleSoft Internet Architecture, 2-42
      PeopleSoft listener, 2-12, 2-14
   scheduled task
      Manager ID recon, 3-6
      PeopleSoft HRMS Trusted Reconciliation, 3-5
   transformation
      for reconciliation, 4-10
      validation
      for reconciliation, 4-7
Configuring Scheduled Tasks, 3-11
connector architecture, 1-3
connector clones, 4-13
connector customization, 4-1
connector features, 1-5
connector files and directories
   copying, 2-11
   description, 2-1
   destination directories, 2-11
Connector Installer, 2-9
connector testing, 5-1
connector, copies, 4-13
copies of connector, 4-13
   customizing connector, 4-1

D
   defining
      IT resources, 2-11

E
   enabling logging, 2-63
   errors, 5-2

F
   features of connector, 1-5
   files and directories of the connector
      See connector files and directories
   full reconciliation, 1-5, 3-2
      configuring, 3-2

G
   generating
      XML files for full reconciliation, 3-2

I
   incremental reconciliation, 1-4, 1-5, 2-12, 2-14, 3-8
   installation, 2-9
      Oracle Identity Manager, 2-9
      Target System, 2-18
   installing connector, 2-1, 2-9, 2-62
   issues, 6-1
   IT resources
      defining, 2-11
      parameters, 2-11

L
   limited reconciliation, 3-8
   logging enabling, 2-63
   lookup definitions
      exclusion list, 1-34
      Lookup.PSFT.HRMS.Configuration, 1-14
      Lookup.PSFT.HRMS.ManagerRecon.Configuration, 1-16
      predefined, 1-14

M
   modifying field length
      on OIM User form, 4-7
Index-2

P
parameters of IT resources, 2-11
PeopleSoft Internet Architecture, configuring, 2-42
Person lifecycle events, 1-5
postinstallation
Oracle Identity Manager, 2-63
Target System, 2-75
preinstallation
Oracle Identity Manager, 2-1
Target System, 2-3
problems, 5-2, 6-1

R
reconciliation
full, 1-5, 3-2
incremental, 1-5
trusted source mode, 2-2
reconciliation action rules, 1-12
reconciliation rule, 1-11
reconciliation type
full reconciliation, 1-4
incremental, 1-4
removing
PeopleSoft Listener, 2-17
requirements for deploying, 1-1
resending messages
PeopleSoft Listener, 3-10

S
setting up
Lookup.PSFT.HRMS.CustomQuery, 4-12
Lookup.PSFT.HRMS.WorkForceSync.EmpStats, 4-12
stages of connector deployment
postinstallation, 2-62
summary of steps
full reconciliation, 3-1
supported
releases of Oracle Identity Manager, 1-1
target systems, 1-2

T
target system
configuring full reconciliation, 2-18
configuring incremental reconciliation, 2-41
target system, multiple installations, 4-13
target systems supported, 1-2
testing, 5-1
reconciliation, 5-1
troubleshooting, 5-2
trusted source reconciliation, 1-10, 2-2
user fields, 1-11

U
upgrading
PeopleSoft Listener, 2-87
upgrading the connector, 2-76
customizations, 2-87
redefining, 2-77
target system, 2-88
upgrade wizard, 2-82

X
XML files
description, 2-2
for trusted source reconciliation, 2-2