Oracle® Identity Manager

Connector Guide for PeopleSoft Employee Reconciliation

Release 9.1.0

E11205-05

July 2009

Oracle Identity Manager Connector Guide for PeopleSoft Employee Reconciliation, Release 9.1.0

E11205-05

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

Audience vii
Documentation Accessibility vii
Related Documents viii
Documentation Updates viii
Conventions viii
Software Updates ix
Documentation-Specific Updates x

1 About the Connector

1.1 Certified Deployment Configurations 1-2
1.1.1 Determining the Version of PeopleTools and the Target System 1-2
1.2 Features of the Connector 1-2
1.2.1 Connector Architecture 1-3
1.2.2 Trusted Source Reconciliation 1-4
1.2.2.1 User Fields for Trusted Source Reconciliation 1-4
1.2.2.2 Valid Person Types 1-5
1.2.2.3 Reconciliation Rule 1-6
1.2.2.4 Reconciliation Action Rules 1-6
1.2.2.5 Person Termination Events 1-7
1.2.2.6 Effective Date Feature of the Target System 1-7
1.3 Certified Languages 1-8
1.4 Roadmap for the Connector Deployment Procedure 1-8

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 That Comprise the Connector 2-1
2.1.1.2 Determining the Release Number of the Connector 2-3
2.1.2 Preinstallation on the Target System 2-3
2.1.2.1 Creating a Target System Account for Connector Operations 2-3
2.1.2.1.1 Creating a Permission List 2-4
2.1.2.1.2 Creating a Role for a Limited Rights User 2-6
2.1.2.1.3 Assigning Limited Rights to a User 2-6
2.2 Installation 2-7
2.2.1 Installation on Oracle Identity Manager 2-7

2.2.1.1 Running the Connector Installer 2-7
2.2.1.2 Copying the Connector Files and External Code Files 2-8
2.2.1.3 Configuring the IT Resource 2-9
2.2.1.4 Deploying the PeopleSoft Listener 2-9
2.2.2 Installation on the Target System 2-15
2.2.2.1 Configuring the Target System for Full Reconciliation 2-15
2.2.2.1.1 Creating the Application Engine Program 2-15
2.2.2.1.2 Configuring the Record Delimiter 2-17
2.2.2.2 Configuring the Target System for Incremental Reconciliation 2-18
2.2.2.2.1 Creating the Queues 2-19
2.2.2.2.2 Creating the Messages 2-20
2.2.2.2.3 Publishing the Messages 2-20
2.2.2.2.4 Configuring PeopleSoft Integration Broker 2-23
2.2.2.2.5 Configuring the EOP_PUBLISHE Application Engine Program 2-27
2.3 Postinstallation 2-30
2.3.1 Postinstallation on Oracle Identity Manager 2-30
2.3.1.1 Enabling Logging 2-30
2.3.1.2 Configuring SSL 2-32
2.3.1.2.1 Configuring SSL on Oracle WebLogic Server 2-32
2.3.1.2.2 Configuring SSL on IBM WebSphere Application Server 2-38
2.3.1.2.3 Configuring SSL on JBoss Application Server 2-40
2.3.2 Postinstallation on the Target System 2-43
2.3.2.1 Configuring SSL 2-43

3 Extending the Functionality of the Connector

3.1 Adding New Fields for Full Reconciliation 3-1
3.2 Adding New Fields for Incremental Reconciliation 3-3

4 Using the Connector

4.1 Configuring Full Reconciliation 4-1
4.1.1 Specifying the Number of Records to Be Reconciled 4-1
4.1.2 Determining the Last Record Reconciled 4-1
4.1.3 Limited Reconciliation 4-2
4.1.4 Configuring the Reconciliation Scheduled Task 4-4
4.1.4.1 Managing Scheduled Tasks 4-4
4.1.5 Running the Application Engine Program 4-10
4.2 Configuring Incremental Reconciliation 4-11
4.2.1 Limited Reconciliation 4-11
4.3 Multiple Trusted Source Reconciliation 4-13
4.4 Guidelines on Using the Connector 4-13

5 Testing the Connector

5.1 Testing Full Reconciliation 5-1
5.2 Testing Incremental Reconciliation 5-2
5.2.1 Prerequisites for Testing the PeopleSoft Listener 5-2
5.2.2 Testing the PeopleSoft Listener 5-2

6 Known Issues

Index

Preface

This guide provides information about integrating Oracle Identity Manager with PeopleSoft Human Resources Management Systems (HRMS) and PeopleSoft Human Capital Management (HCM).

Audience

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

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at `http://www.fcc.gov/cgb/consumerfacts/trs.html`, and a list of phone numbers is available at `http://www.fcc.gov/cgb/dro/trsphonebk.html`.

Related Documents

To access the Oracle Identity Manager documents mentioned as references in this guide, visit Oracle Technology Network.

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

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

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

`http://www.oracle.com/technology/documentation/index.html`

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://www.oracle.com/technology/documentation/index.html`

Conventions

The following text conventions are used in this document:

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

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

This chapter provides an overview of the updates made to the software and documentation for release 9.1.0.2 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. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

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

Software Updates

This section discusses the software updates made to the connector:

- Software Updates in Release 9.1.0
- Software Updates in Release 9.1.0.1
- Software Updates in Release 9.1.0.2

Software Updates in Release 9.1.0

The following software updates have been made in release 9.1.0:

- From this release onward, PeopleTools 8.22, 8.45, 8.46, 8.47, and 8.48 are not supported. Information specific to these releases has been removed from the guide. The modified target system requirements information is documented in "Certified Deployment Configurations" on page 1-2.
- The list of target system fields that are reconciled has changed. This is described in "User Fields for Trusted Source Reconciliation" on page 1-4.
- The list of person types that are supported in this release of the connector has been modified. See "Valid Person Types" on page 1-5 for details.
- The connector supports the Effective Dating feature of the target system. See "Effective Date Feature of the Target System" on page 1-7 for details.

- The connector supports person termination events. See "Person Termination Events" on page 1-7 for details.
- Information about the files in which you set the log levels has changed. This information is available in "Enabling Logging" on page 2-30.
- From this release onward, the connector is installed through the Connector Installer feature of the Oracle Identity Manager Administrative and User Console. Instructions to perform the installation are provided in "Running the Connector Installer" on page 2-7.
- You can configure SSL connectivity between Oracle Identity Manager and the target system for this release of the connector. However, SSL is not supported for Oracle Application Server. For instructions to configure SSL, see "Postinstallation" on page 2-30.

Software Updates in Release 9.1.0.1

The following software updates have been made in release 9.1.0.1:

- Support for Oracle Identity Manager Release 9.1.0.1
- Resolved Issues in Release 9.1.0.1

Support for Oracle Identity Manager Release 9.1.0.1

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

Resolved Issues in Release 9.1.0.1

The following table lists the issues resolved in this release:

Bug Number	Issue	Resolution
8246283	The deployment.properties file is bundled in the listener (peopleSoftERApp.war) file. The default message name in this properties file was the one used during testing. You had to change the message name and redeploy the listener while testing the connector and again before you started using it in your production environment.	This issue has been resolved. The message name for both testing and production environments has been set to `PSFT_OIM_ER_MSG`.

Software Updates in Release 9.1.0.2

There are no software updates in release 9.1.0.2.

Documentation-Specific Updates

The following documentation-specific updates made to the guide:

- Documentation-Specific Updates in Release 9.1.0
- Documentation-Specific Updates in Release 9.1.0.1
- Documentation-Specific Updates in release 9.1.0.2

Documentation-Specific Updates in Release 9.1.0

The following are documentation-specific updates in release 9.1.0:

- Information about connector deployment has been modified in this document based on the different stages of connector deployment. This information is provided in Chapter 2, "Deploying the Connector".
- The extended functionalities of the connector are described in Chapter 4, "Using the Connector".
- The architecture of the connector has been included in this guide. This information is located at "Connector Architecture" on page 1-3.
- The field mappings between the target system and Oracle Identity Manager have been moved from the appendix to the first chapter. For information on the field mappings for reconciliation, see "User Fields for Trusted Source Reconciliation" on page 1-4.
- The reconciliation rules and the corresponding actions for these rules have been added to the guide. For information on these rules, see "Trusted Source Reconciliation" on page 1-4.

Documentation-Specific Updates in Release 9.1.0.1

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

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

Documentation-Specific Updates in release 9.1.0.2

There are no documentation-specific updates in release 9.1.0.2.

1 About the Connector

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

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

Table 1–1 lists the functions that are supported by this connector.

Table 1–1 Functions Supported by this Connector

Function	Type	Description
Create Employee	Reconciliation	Creates OIM Users corresponding to newly created employee records in the target system.
Update Employee	Reconciliation	Modifies OIM Users corresponding to updates made to existing employees in the target system.
Disable Employee	Reconciliation	Performs the global disabling of an OIM User in Oracle Identity Manager.
Enable Employee	Reconciliation	Enables a disabled OIM User.

> **Note:**
>
> - This connector does not support target resource reconciliation or provisioning operations.
>
> - See *Oracle Identity Manager Connector Concepts* for detailed information about connector deployment configurations.

The connector supports reconciliation in two ways:

- Full reconciliation: This involves fetching all existing target system records into Oracle Identity Manager.
- Incremental reconciliation: This involves real-time reconciliation of changes in the target system records into Oracle Identity Manager.

The "Connector Architecture" section on page 1-3 discusses full and incremental reconciliation in detail.

This chapter contains the following sections:

- Certified Deployment Configurations
- Features of the Connector
- Certified Languages
- Roadmap for the Connector Deployment Procedure

1.1 Certified Deployment Configurations

Table 1–2 lists the certified deployment configurations.

Table 1–2 Certified Deployment Configurations

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 9.1.0 and later
Target system	The following are the supported target systems and the PeopleTools versions for each: ■ PeopleSoft HRMS 8.8 SP1 with PeopleTools 8.49 ■ PeopleSoft Enterprise HCM 8.9 with PeopleTools 8.49 ■ PeopleSoft Enterprise HCM 9.0 with PeopleTools 8.49
	You must ensure that the following components are installed and configured in the target system environment: ■ Tuxedo and Jolt (the application server) ■ PeopleSoft Internet Architecture ■ PeopleSoft Application Designer (2-tier mode)

1.1.1 Determining the Version of PeopleTools and the Target System

Before you deploy the connector you might want to determine the versions of PeopleTools and the target system you are using to check if this release of the connector supports that combination. To do so, perform the following steps:

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

   ```
   http://SERVER_NAME/psp/ps/DATABASE_NAME/?cmd=login
   ```

   For example:

   ```
   http://psftserver.example.com/psp/ps/TestDB/?cmd=login
   ```

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

1.2 Features of the Connector

This section discusses the following topics:

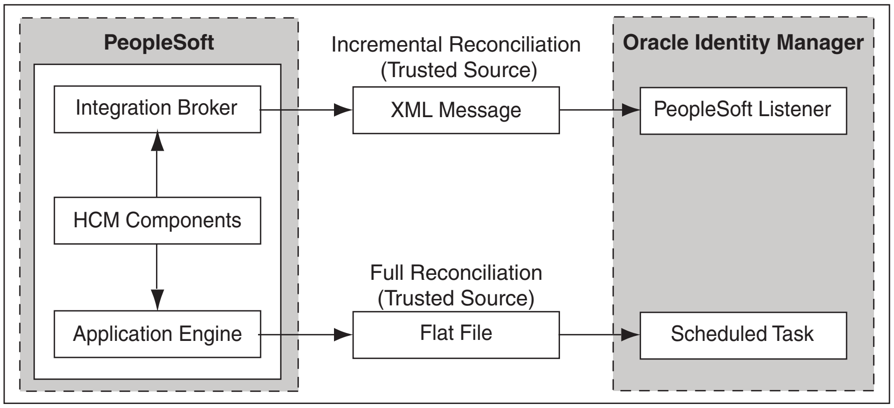
- The "Connector Architecture" section on page 1-3 describes the architecture of the connector.

- The "Trusted Source Reconciliation" section on page 1-4 describes the reconciliation features of the connector.

1.2.1 Connector Architecture

Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of the Connector



This connector supports trusted source reconciliation in two ways.

- **Full reconciliation**

  A full reconciliation run involves fetching all the records in the target system and using them for reconciliation in Oracle Identity Manager by using a flat file. The PeopleSoft Application Engine program populates the flat file that contains all the employee data separated by the specified delimiter (*). The flat file is then read by an Oracle Identity Manager scheduled task that generates reconciliation events.

  The PeopleSoft Application Engine program is run using PeopleSoft Internet Architecture.

  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. Oracle recommends that you run full reconciliations at periodic intervals to ensure that all the user records are reconciled into Oracle Identity Manager. "Configuring Full Reconciliation" on page 4-1 describes the procedure to configure full reconciliation.

- **Incremental reconciliation**

  Incremental reconciliation involves real-time reconciliation of newly created or modified employee data. You use incremental reconciliation to reconcile individual data changes after an initial, full reconciliation run has been performed. Incremental reconciliation is performed using PeopleSoft application messaging. The "Configuring Incremental Reconciliation" on page 4-11 describes the procedure to configure incremental reconciliation.

  Incremental reconciliation involves the following steps:

  1. When employee data is added, updated, or deleted in the target system, a PeopleCode event is activated.

2. The PeopleCode event generates an XML message containing the modified employee data and sends it in real time to the PeopleSoft listener by using HTTP. If SSL is configured, then the PeopleSoft listener can also use HTTPS. The PeopleSoft listener is a Web application that is deployed on an Oracle Identity Manager host computer.
3. The PeopleSoft listener parses the XML message and sends a reconciliation event to Oracle Identity Manager.

1.2.2 Trusted Source Reconciliation

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

> **See Also:** "Trusted Source Reconciliation" in *Oracle Identity Manager Connector Concepts* for conceptual information about trusted source reconciliation

This section discusses the following topics:

- User Fields for Trusted Source Reconciliation
- Valid Person Types
- Reconciliation Rule
- Reconciliation Action Rules
- Person Termination Events

1.2.2.1 User Fields for Trusted Source Reconciliation

Table 1–3 lists the identity fields whose values are fetched from the target system during reconciliation.

Table 1–3 User Fields for Reconciliation

OIM User Form Field	PeopleSoft HRMS/HCM Field	Description
User ID	PS_PERSON.EMPLID	Employee ID of the employee to which the user profile will be assigned This is a mandatory field for the creation of an OIM User.
Last Name	PS_NAMES.LAST_NAME	Last name This is a mandatory field for the creation of an OIM User.
First Name	PS_NAMES.FIRST_NAME	First name This is a mandatory field for the creation of an OIM User.
Employee Type	PS_JOB.REG_TEMP PS_JOB.FULL_PART_TIME PS_JOB.PER_ORG	The Employee Type of the OIM User. The combination of the values of the PS_JOB.REG_TEMP, PS_JOB.FULL_PART_TIME, and the PS_JOB.PER_ORG fields are used to specify the Employee Type of the OIM User. This is a mandatory field for the creation of an OIM User.
Status	PS_JOB.HR_STATUS	Specifies whether the employee is active or terminated

1.2.2.2 Valid Person Types

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.PSFTER.EmpType.Map.Recon 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 will be reconciled into the corresponding Employee Type field of Oracle Identity Manager.

The Lookup.PSFTER.EmpType.Map.Recon lookup definition has the following default combinations:

> **Note:** You can modify the values of the lookup definition based on your requirement.

Code Key	Decode
CWR##TEMP##FT	Temp
CWR##TEMP##PT	Intern
CWR##REG##FT	Consultant
CWR##REG##PT	Part-Time
EMP##TEMP##FT	Part-Time
EMP##TEMP##PT	Temp
EMP##REG##FT	Full-Time
EMP##REG##PT	Temp
For HRMS 8.8 SP1, the following combinations are available in addition to the preceding list:	
NON##TEMP##FT	Part-Time
NON##TEMP##PT	Consultant
NON##REG##FT	Temp
NON##REG##PT	Full-Time
For all HRMS versions, the following combination is available in addition to the preceding list:	
###### **Note:** This Code key is for a situation in which the PS_JOB.REG_TEMP, PS_JOB.FULL_PART_TIME, and PS_JOB.PER_ORG fields on the target system are empty.	Consultant

Note: The Decode values are case-sensitive.

In the preceding table:

- CWR represents Contingent Worker.
- EMP represents Employee.
- TEMP represents Temporary.
- REG represents Regular.
- FT represents Full-Time.
- PT represents Part-Time.
- NON represents employees who do not belong to any of the predefined employee types. This value is applicable only for HRMS 8.8 SP1.
- The last row in the table represents a scenario in which no job is assigned to an employee.

1.2.2.3 Reconciliation Rule

The following is the reconciliation rule for trusted source reconciliation:

Rule Name: PSFT ER

Rule Element: User Login Equals Users.EmplId

In this rule:

- User Login represents the User ID field on the OIM User form.
- Users.EmplId 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.

To access the reconciliation rule:

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Locate **PSFT ER**.

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

1.2.2.4 Reconciliation Action Rules

The following table lists the reconciliation action rules for this connector:

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

To access the reconciliation action rules for this connector:

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Locate the **PSFT_ER_RO** 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.

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

Note: For any rule condition that is not predefined for this connector, Oracle Identity Manager will neither perform any action nor log an error.

1.2.2.5 Person Termination Events

The connector reconciles records of terminated employees. If the status of an employee is INACTIVE, then it means that the employee is terminated. The employee account is disabled in the target system, and globally deprovisioned in Oracle Identity Manager through the Disable User function of the connector.

1.2.2.6 Effective Date Feature of the Target System

On the target system, you can use the Effective Date feature to assign a future date to changes that you want to make to a user account. The following example illustrates how this feature works:

Suppose the system date is 02-May-2008. On the target system, the current designation of user John Doe is Systems Analyst. You want to change John's designation to Senior Systems Analyst and set 16-May-08 as the date on which the change will take place. To achieve this, you have set 16-May-08 as the effective date for the change in John's account information.

Oracle Identity Manager stores current data. In this context, current data is the most recent data in which the effective date is not later than the current system date. In other words, the date on which data is created or changed cannot be a date in the future.

The connector can recognize and ignore target system records with effective dates that are later than the system date. This feature of the connector is aimed at reconciling only target system changes that are already effective. The following extension to the example illustrates this feature of the connector:

After you set the effective date for John's designation change, suppose a reconciliation run takes place at 11:30 p.m. on 05-May-2008. During this reconciliation run, John's latest record with the effective date set to 16-May-08 is ignored because it is set in the future.

When a reconciliation run takes place on 16-May-08, John's data becomes current. When this happens, the Effective Date feature changes John's data and this change is reconciled into Oracle Identity Manager.

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

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

1.3 Certified Languages

The connector supports the following languages:

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

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

1.4 Roadmap for the Connector Deployment Procedure

The following is the organization of information 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, "Extending the Functionality of the Connector" describes the extended functions of the connector.
- Chapter 4, "Using the Connector" provides information on the tasks that must be performed each time you want to run reconciliation.
- Chapter 5, "Testing the Connector" provides information on testing the connector.
- Chapter 6, "Known Issues" lists the known issues that you may encounter while using the connector.

2

Deploying the Connector

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

> **Note:** This connector does not support target resource reconciliation or provisioning operations.

- Preinstallation
- Installation
- Postinstallation

This chapter provides information about each stage of connector deployment.

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

2.1 Preinstallation

Preinstallation information is divided across the following sections:

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

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Files and Directories That Comprise the Connector
- Determining the Release Number of the Connector

2.1.1.1 Files and Directories That Comprise the Connector

The contents of the connector installation media are described in Table 2–1.

Table 2–1 Files and Directories That Comprise the Connector

File in the Installation Media Directory	Description
config/configureReconciliation.properties	This file is used to specify the date format used for full reconciliation. The date format is used in both the PeopleSoft server and Oracle Identity Manager.
configuration/PeopleSoft Employee Recon-CI.xml	This is the connector installer content file.
ext/csv.jar	This JAR file is a library that is used to parse and read the flat file used for full reconciliation.
lib/xlPSFTERRecon.jar	This JAR file contains the class files that are used to implement full reconciliation.
lib/peopleSoftERApp.war	This Web Archive (WAR) file contains the classes and configuration files required to implement incremental reconciliation.
The following files in the peopleCode directory: For PeopleTools 8.49 on HRMS 8.8 SP1*:* JOB_DATA_ADD_NEE_component_8.49&8.8.txt JOB_DATA_HIRE_component_8.49&8.8.txt OIMConnector_appclass_8.49&8.8.txt OIMPublicationMgr_appclass_8.49&8.8.txt OIMSubscriptionMgr_appclass_8.49&8.8.txt For PeopleTools 8.49 on HCM 8.9/9.0: JOB_DATA_component_8.49.txt JOB_DATA_CONCUR_component_8.49.txt JOB_DATA_CWR_component_8.49.txt JOB_DATA_EMP_component_8.49.txt OIMConnector_appclass_8.49.txt OIMPublicationMgr_appclass_8.49.txt OIMSubscriptionMgr_appclass_8.49.txt PERSONAL_DATA_component_8.49.txt	These files contain the PeopleCode that you must add to the SavePostChange event while performing the procedure described in "Publishing the Messages" on page 2-20.
The following files in the peopleCode directory: For PeopleTools 8.49 on HRMS 8.8 SP1: HRMSFullRecon_8.49&8.8.txt For PeopleTools 8.49 on HCM 8.9 and 9.0: HRMSFullRecon_8.49.txt	These files contain the PeopleCode that generates the flat file during full reconciliation.
test/cbrecon/psft-xel-test.vbs	This VBScript file is used to test the incremental reconciliation functionality of the connector by creating a dummy XML message similar to the ones created by the target system. For information about testing incremental reconciliation, see "Testing Incremental Reconciliation" on page 5-2.
The following files in the test/cbrecon directory: pingRequest.xml pingResponse.xml publishRequest.xml publishResponse.xml	These XML files are required by the psft-xel-test.vbs file for communicating with the connector by using XML over HTTP.

Table 2–1 (Cont.) Files and Directories That Comprise the Connector

File in the Installation Media Directory	Description
test/cbrecon/psft_xellerate_msg.xml	This XML file is used by the psft-xel-test.vbs file to define the template of the XML message that is received from the target system.
test/scripts/psftER_Recon.bat test/scripts/psftER_Recon.sh	The BAT file or UNIX shell script calls the testing utility for reconciliation.
test/config/attributeMap_Recon.properties test/config/config_Recon.properties test/config/log.properties	These files are used by the psftER_Recon.bat file. The attributeMap_Recon.properties file contains the field mappings between the Oracle Identity Manager fields and the target system fields. The config_Recon.properties file contains the configurations for running the psftER_Recon.bat file. The log.properties file contains the logger information.
xml/PSFTER-ConnectorConfig.xml	This XML file contains definitions for the following components of the connector: ■ Resource object ■ Process definition ■ IT resource type ■ Reconciliation rules ■ Scheduled tasks

2.1.1.2 Determining the Release Number of the Connector

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

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

   OIM_HOME/JavaTasks/xlPSFTERRecon.jar

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

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

2.1.2 Preinstallation on the Target System

Preinstallation on the target system consists of creating a target system account with appropriate privileges for connector operations. This special account created on the target system will be able to perform all the configurations required for connector operations. This includes configuring the PeopleSoft Integration Broker for incremental reconciliation, and configuring and running the Application Engine for bulk file generation and publishing effective-dated data. This account will not have access to any other pages or components that are not required by the connector. For creating this account, you must log in to PeopleSoft Internet Architecture with administrator credentials. The procedure to create a target system account is provided in the following section:

2.1.2.1 Creating a Target System Account for Connector Operations

Note: If a target system account with the required privileges exists, then you can skip this section.

Creating a target system account for connector operations involves the procedures described in the following sections:

- Creating a Permission List
- Creating a Role for a Limited Rights User
- Assigning Limited Rights to a User

2.1.2.1.1 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://SERVER_NAME/psp/ps/DATABASE_NAME/?cmd=login
   ```

   For example:

   ```
   http://psftserver.example.com/psp/ps/TestDB/?cmd=login
   ```

2. In the PeopleSoft Internet Architecture window, click **PeopleTools**, **Security**, **Permissions & Roles**, and then click **Permission Lists**.
3. Click **Add a new Value**. On the Add a New Value tab, enter the permission list name, for example, `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. In the Menu Name lookup, enter `APPLICATION_ENGINE` and then click **Lookup**. From the list, select **APPLICATION_ENGINE**. The application returns to the Pages tab. Click the **Edit Components** link.

   b. On the Component Permissions page, click **Edit Pages** for the AE_REQUEST component name.

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

   d. Click on 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 the **Edit Components** link.

   e. On the Component Permissions page, click **Edit Pages** for each of the following component names:

      IB_GATEWAY

      IB_MESSAGE_BUILDER

      IB_MONITOR_QUEUES

      IB_NODE

      IB_OPERATION

      IB_QUEUEDEFN

      IB_ROUTINGDEFN

      IB_SERVICE

      IB_SERVICEDEFN

f. Click **Select All**, and then click **OK** for each of the components. Click **OK** on the Components Permissions page. The application returns to the Pages tab.

g. Click on the plus sign (+) to add another row for **Menu Name**.

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

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

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

k. Click on the plus sign (+) to add another row for **Menu Name**.

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

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

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

o. Click on the plus sign (+) to add another row for **Menu Name**.

p. 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 the **Edit Components** link.

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

r. 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**. The application returns to the Process Group Permission page.
13. Click on 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 on 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.

2.1.2.1.2 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://SERVER_NAME/psp/ps/DATABASE_NAME/?cmd=login
   ```

   For example:

   ```
   http://psftserver.example.com/psp/ps/TestDB/?cmd=login
   ```

2. In the PeopleSoft Internet Architecture window, click **PeopleTools**, **Security**, **Permissions & Roles**, and then click **Roles**.
3. Click **Add a new Value**. On the Add a New Value tab, enter the role name, for example, `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 **Save**.

2.1.2.1.3 Assigning Limited Rights to a User

To assign limited rights to a user:

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

   ```
   http://SERVER_NAME/psp/ps/DATABASE_NAME/?cmd=login
   ```

   For example:

   ```
   http://psftserver.example.com/psp/ps/TestDB/?cmd=login
   ```

2. In the PeopleSoft Internet Architecture window, click **PeopleTools**, **Security**, **User Profiles**, and then click **User Profiles**.
3. Click **Add a new Value**. On the Add a New Value tab, enter the user profile name, for example, `OIMER`, and then click **Add**.
4. On the General tab, perform the following:
   1. From the Symbolic ID list, select the value that is displayed, for example, SYSADM1.
   2. Enter valid values for the **Password** and **Confirm Password** fields.
   3. Click the search icon for the Process Profile permission list.
   4. 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 and perform the following:
   1. In the Roles lookup, enter `OIMER` and then click **Lookup**. From the list, select **OIMER**.
   2. Click on the plus sign (+) to add another row.
   3. In the Roles lookup, enter `ProcessSchedulerAdmin` and then click **Lookup**. From the list, select **ProcessSchedulerAdmin**.
   4. Click **Save** to save this user profile. This user profile is used as a limited rights user at the target system for performing all reconciliation-related configurations.

2.2 Installation

Installation information is divided across the following sections:

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

2.2.1 Installation on Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

- Running the Connector Installer
- Copying the Connector Files and External Code Files
- Configuring the IT Resource

2.2.1.1 Running the Connector Installer

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

To run the Connector Installer, refer to the instructions given in the "Installing Predefined Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*. The following instructions are specific to individual steps of the procedure described in the "Installing a Predefined Connector" section of that chapter:

- When you reach Step 3 of that procedure, apply the following instructions:

  The following is the default connector installation directory:

  OIM_HOME/ConnectorDefaultDirectory

  If you have copied the installation files into this directory, then select **PeopleSoft Employee Recon 9.1.0** from the **Connector List** list.

- Perform Steps 1 through 5 of that procedure. When you reach Step 6 of that procedure, see "Configuring the IT Resource" on page 2-9 in this guide. Instructions to Step 6 of that procedure are described in detail in this section.

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

Table 2–2 Files Copied to Oracle Identity Manager

File in the Installation Media Directory	Destination Directory
ext/csv.jar	*OIM_HOME*/ThirdParty
lib/xlPSFTERRecon.jar	*OIM_HOME*/ScheduleTask

> **Note:** For a clustered environment, copy the files listed in Table 2–2 into their respective destination directories on each node of the cluster.

2.2.1.2 Copying the Connector Files and External Code Files

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

> **Note:** The directory paths given in the first column of this table correspond to the location of the connector files in the PeopleSoft Employee Reconciliation directory on the installation media. See "Files and Directories That Comprise the Connector" on page 2-1 for more information about these files.
>
> - If a particular destination directory does not already exist on the Oracle Identity Manager host computer, then create it.

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

File in the Installation Media Directory	Destination Directory
Files in the config directory	*OIM_HOME*/XLIntegrations/PSFTER/config
lib/peopleSoftERApp.war	*OIM_HOME*/XLIntegrations/PSFTER/cbrecon_webapp
Files in the test/cbrecon directory	*OIM_HOME*/XLIntegrations/PSFTER/cbrecon
Files in the test/scripts directory	*OIM_HOME*/XLIntegrations/PSFTER/scripts
Files in the test/config directory	*OIM_HOME*/XLIntegrations/PSFTER/config
Files in the xml directory	*OIM_HOME*/XLIntegrations/PSFTER/connectorXML
Files in the peopleCode directory	*OIM_HOME*/XLIntegrations/PSFTER/peopleCode

Note: While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. 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_Employee IT resource is automatically created in Oracle Identity Manager. You must specify values for the parameters of this IT resource as follows:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `PSFT_Employee` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2–4 describes each parameter:

Table 2–4 Parameters of the IT Resource for the Target System

Parameter	Description
NumberOfRetries	Use this parameter to specify the number of times Oracle Identity Manager must try connecting to the target system. Default value: `2` **Note:** The timeout feature is enabled only for full reconciliation.
DelayBetweenRetries	Use this parameter to specify the time difference between consecutive retries (in milliseconds). Default value: `20000`

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

2.2.1.4 Deploying the PeopleSoft Listener

To deploy the PeopleSoft listener:

1. Copy the *OIM_HOME*/XLIntegrations/PSFTER/cbrecon_webapp/peopleSoftERApp.war file into a temporary folder. Enter the following command to extract the contents of the peopleSoftERApp.war file.

```
jar -xvf peopleSoftERApp.war
```

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

2. Edit the xlsession.properties file. This file contains the **UserName** Oracle Identity Manager connection parameter. The value that you specify for this parameter is the user name for logging in to Oracle Identity Manager. The default value is `xelsysadm.`

3. Edit the xlConnection.properties file. This file contains the following system properties that enable an API client to communicate with Oracle Identity Manager:

   - **XL.HomeDir:** Use this property to specify the full path and name of the *OIM_HOME* directory. Specify the following value for this parameter:

     ```
     -DXL.HomeDir=OIM_HOME
     ```

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

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

     Each application server uses a different authentication configuration file:

     IBM WebSphere Application Server: `authws.conf`

     Oracle WebLogic Server: `authwl.conf`

     JBoss Application Server: `auth.conf`

     Oracle Application Server: `auth.conf`

   - **java.naming.provider.url:** Use this property to specify the JNP URL of the application server. This URL is located in the `<Discovery><CoreServer><java.naming.provider.url>` tag of the *OIM_HOME*/config/xlconfig.xml file. Each application server uses a different JNP URL:

     – Oracle WebLogic Server: `t3://localhost:7001`

     – IBM WebSphere Application Server: `corbaloc:iiop:localhost:2809`

     – JBoss Application Server: `jnp://localhost:1099`

     – Oracle Application Server: `ormi://localhost:12401/Xellerate`

4. Edit the following properties in the configureReconciliation.properties file:

   Note: This file is different from the configureReconciliation.properties file specified in Table 2–1.

   - **Serverdateformat:** Use this property to specify the date format that is used by the target system. You can select one of the following date formats:

     – `dd-mmm-yy`

     – `ddmmyy`

     – `yyddmm`

     – `yymmdd`

     – `dd.mm.yy` (if the PeopleSoft installation uses Microsoft SQL Server)

     – `dd.mm.yyyy` (if the PeopleSoft installation uses IBM DB2 UDB)

- **OrganizationName:** Use this property to specify the name of an Oracle Identity Manager organization. This property specifies the organization to which all OIM Users will be assigned. The default value of this property is `Xellerate Users`.
- **XelServerDate:** Use this property to specify the date format that is used in Oracle Identity Manager.

  The current format of the XelServerDate property is: `yyyy/MM/dd hh:mm:ss z`.

  Note: You must not change this date format if you are using Oracle Database. However, if you are using Microsoft SQL Server, then you might need to change this date format.

- **User Type**: Use this property to specify the Oracle Identity Manager user types. The default value of this property is `End-User`.
- **ReconcilingRO**: Use this property to specify the name of the trusted resource object. The default value is `PSFT_ER_RO`.
- **LookupName**: Use this property to specify the name of the lookup definition in which the person types are mapped to OIM employee types.
- **FiltersToBeApplied**: Use this property to specify the comma-separated list of filters that are applied on the target system field names during reconciliation.
- **FiltersValues**: Use this property to specify the comma-separated list of values for the filters that you specify as the values of the FiltersToBeApplied property.

  Note: In the FiltersValues property, data is separated by a comma. However, if a comma is part of the values specified, then it will be treated as a different value. Consider the following example:

  ```
  IsFilterApplied = yes, FiltersToBeApplied =
  Users.EMPLID,Users.ADDRESS, and FiltersValues =SFC1001,San
  Jose,California
  ```

  In this scenario, you have entered the value of `Users.ADDRESS` as `"San Jose, California"`. The reconciliation engine will consider it as two different values, `"San Jose"`, and `"California"`. The FiltersToBeApplied property contains two filters while the FiltersValues property contains three. As a result of this inconsistency, the "Filters are not synchronized" error message will be displayed.

  For information about how these filters are applied during reconciliation, see Chapter 4, "Using the Connector".

- **IsFilterApplied**: Use this property to specify whether or not filters must be applied during reconciliation. Valid values are `yes` and `no`. If invalid values are provided, then the default value `no` is used.
- **SearchCriteria**: Use this property to specify the search algorithm to be applied on the filters that you enter. Valid values are `INDEX_OF`, `EXACT_MATCH`. Consider the following example.

  You specify a filter in which the value of Users.FirstName must contain "JO" and you also set a value for the SearchCriteria property. If you specify

INDEX_OF, then all records containing "JO" will be reconciled. If you specify EXACT_MATCH, then only those records in which the value of Users.FirstName is "JO" will be reconciled.

If invalid values are provided, then by default the value of this property is considered as INDEX_OF.

- **CaseSensitive**: Use this property to specify if the filters that search the records are case sensitive or not. Consider the following example:

  You specify the value of this property as yes. In this case, if the filter specifies that Users.FirstName=JOHN, then only JOHN will match. The values John or john will be ignored. If you specify the value as no, then the value will be accepted regardless of the case in which it is specified.

  If invalid values are provided, then the default value no is used.

- **Operator**: Use this property to specify the operator that you want to apply to the filters. Valid values are AND or OR. Depending on the value specified, data is joined accordingly for any combination of the target system fields specified in the FiltersToBeApplied property. However, if invalid values are provided, then the "Invalid Operators" error message is displayed and no records are reconciled.

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

   Note: Before you copy these files from the OIM_HOME/lib directory, check if these files exist in the WEB-INF/lib directory of the temporary folder. If these files exist, then first delete them from the WEB-INF/lib directory.

   - xlAPI.jar
   - xlAuthentication.jar
   - xlBackOfficeBeans.jar
   - xlBackofficeClient.jar
   - xlCache.jar
   - xlCrypto.jar
   - xlDataObjectBeans.jar (for IBM WebSphere Application Server, copy this file from the *OIM_CLIENT*/xlclient/lib directory)
   - xlDataObjects.jar
   - xlLogger.jar
   - xlUtils.jar
   - xlVO.jar
   - xlAdapterUtilities.jar
   - xlRemoteManager.jar
   - xlScheduler.jar

   Copy the following files from the *OIM_HOME*/ext directory to the WEB-INF/lib directory:

- oscache.jar
- javagroups-all.jar
- commons-collections.jar
- commons-digester.jar
- commons-logging.jar
- commons-validator.jar
- commons-beanutils.jar
- jdbcpool-0.99.jar
- log4j-1.2.8.jar
- struts.jar
- xerces.jar
- xercesImpl.jar
- velocity-dep.jar (only for UNIX)

6. Delete the peopleSoftERApp.war file from the temporary directory into which you extract it, and then use the following command to re-create the file:

   ```
   jar -cvf peopleSoftERApp.war .
   ```

7. Ensure that the old version of the peopleSoftERApp.war file is removed from the application server deployment directory.

8. Deploy the newly created peopleSoftERApp.war file into the deployment directory of the application server as follows:

   For Oracle WebLogic Server:

   a. Log in to the Oracle WebLogic admin console.

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

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

   c. Click the **Deployments** tab

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

   e. Click **Install**.

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

   g. Select the WAR file that you want to install.

   h. Click **Next**.

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

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

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

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

m. Click **Finish**.

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

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

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

   Success Settings updated successfully.

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

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

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

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

For IBM WebSphere Application Server:

a. Log in to the WebSphere Admin console.

b. Expand **Applications**.

c. Click **Install New Application**.

d. Locate the WAR file by using the Browse button.

e. Specify the Context root as `peopleSoftERApp`.

f. Click **Next**.

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

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

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

j. Click **Finish**.

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

l. Click **Enterprise Applications**.

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

For JBoss Application Server:

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

b. Restart JBoss Application Server.

For Oracle Application Server:

a. Log in to the Oracle Application Server Administrative Console.

b. Select the name of the instance on which the Oracle Identity Manager server is running.

c. Select the Applications tab.

d. Click Deploy.

e. Locate the WAR file by using the Browse button.

f. Click **Next**.

g. Specify the application name as `peopleSoftERApp`.

h. Click **Next**.

i. To accept the default deployment settings, click **Deploy**.

j. When the WAR file is successfully deployed, restart Oracle Application Server.

9. Restart Oracle Identity Manager and the Design Console.

> **Note:** You can add new fields to be reconciled during incremental reconciliation. However, you must complete the deployment procedure before you can add new fields.
>
> See "Adding New Fields for Incremental Reconciliation" on page 3-3 for information about the procedure to add new fields for reconciliation.

2.2.2 Installation on the Target System

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

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

2.2.2.1 Configuring the Target System for Full Reconciliation

As described in Chapter 1, "About the Connector", full reconciliation is used to reconcile all data that are added, modified, or deleted in the target system into Oracle Identity Manager. The PeopleCode that is activated extracts the required employee data through the following components:

- For PeopleSoft HRMS 8.8 SP1

  PERSONAL_DATA, JOB_DATA, JOB_DATA_NEE, JOB_DATA_CONCUR, and JOB_DATA_HIRE

- For PeopleSoft HCM 8.9 and 9.0:

  PERSONAL_DATA, JOB_DATA, JOB_DATA_EMP, JOB_DATA_CONCUR, and JOB_DATA_CWR

Configuring the target system for full reconciliation involves preparing the flat file for full reconciliation by performing the following procedures:

1. Creating the Application Engine Program

   This is a one-time procedure.

2. Configuring the Record Delimiter

   Depending on your requirements, you may configure the record delimiter once, or each time you want to perform full reconciliation.

2.2.2.1.1 Creating the Application Engine Program

Note: The PeopleCode in an Application Engine program calls a method defined in the OIMConnector application class of the OIM_PUBLICATION_RULES Application Package. Ensure that you create the OIM_PUBLICATION_RULES application package before saving the Application Engine program. See "Creating the Application Package" on page 2-22 for details about creating the application package.

The Application Engine program populates a flat file with employee data that requires reconciliation. To create the Application Engine program:

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

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

   ---

2. From the File menu, click **New**.
3. In the New Definition dialog box, select **App Engine Program** from the **Definition** list.
4. On the App Engine Program page, a plus sign (+) is displayed besides the `MAIN` section. The `MAIN` section may contain multiple steps. Expand **MAIN**. A step named `Step01` is added to `MAIN`.
5. Rename `Step01` to `Populate.`
6. Click **Action** in the **Insert** menu. An action is added to the `Populate` step.
7. Select **PeopleCode** from the list in the new action.
8. Click **Save** in the **File** menu, and save the Application Engine program as `BLKPRCS_ER`.
9. Double-click the **PeopleCode** action. A new PeopleCode window is displayed.
10. Copy the code from the following file into the PeopleCode window:

    On PeopleSoft HRMS 8.8 SP1:

    OIM_HOME/XLIntegrations/PSFTER/peopleCode/HRMSFullRecon_8.49&8.8.txt

    On PeopleSoft HCM 8.9 or HCM 9.0:

    OIM_HOME/XLIntegrations /PSFTER/peopleCode/HRMSFullRecon_8.49.txt
11. You must make the following changes in the code that you copied in Step 10:

    Replace *`ABSOLUTE_PATH_OF_THE_FILE`* with the directory path at which you want the flat file to be created.
12. Save the PeopleCode action, and close the window.
13. On the App Engine Program page, right-click on the PeopleCode folder and select **Insert Action**.

14. An action is added. Select **SQL** from the list in the new action.
15. Double-click the **SQL** action. A new SQL window is displayed. Enter `COMMIT` in the window and click **Save**.
16. If the target system is using Microsoft SQL Server, then you may need to change the value of the XelServerDate property in the following file:

    ```
    OIM_HOME/XLIntegrations/PSFTER/config/configureReconciliation.properties
    ```

    Set the value of this property to the following:

    ```
    dd.mm.yy
    ```

    If the target system is using Oracle Database, then you need not change the value of the XelServerDate property.
17. Save the Application Engine program.

2.2.2.1.2 Configuring the Record Delimiter If the record delimiter is part of any data that is reconciled, then you must configure the record delimiter to specify an appropriate value:

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

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

2. From the File menu, click **Open**.
3. In the Open Definition dialog box, select **App Engine Program** from the **Definition** list, and enter BLKPRCS_ER as the name of the Application Engine program.
4. On the App Engine Program page, a plus sign (+) is displayed besides the MAIN section. The MAIN section may contain multiple steps. Expand **MAIN**. A step named Step01 is added to MAIN.
5. Double-click the **PeopleCode** action. A new PeopleCode window is displayed.
6. In the PeopleCode window, search for the following string:

    &Sepratr = Left("*",1)

    In this string, the asterisk character (*) represents the source string and 1 represents the numerical character.
7. In the Left (*source_str*, *num_chars*) function, change the first parameter to a new delimiter value. For example, if you want to change the delimiter value from the asterisk character (*), to the ampersand (&), then change the line to the following:

    &Sepratr = Left("&",1);
8. Click **Save**.

2.2.2.2 Configuring the Target System for Incremental Reconciliation

Configuring the target system for incremental reconciliation involves creating messages and queues, publishing messages by writing PeopleCode that is used to populate and send messages from PeopleSoft Integration Broker to other systems, and configuring PeopleSoft Integration Broker.

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.

After messages are created and associated with their respective queue, they must be published. Publishing a message involves adding the required PeopleCode in Application Designer. This is because PeopleSoft Integration Broker and Oracle Identity Manager communicate through the exchange of XML messages and a message can only be generated by using specific instructions in the PeopleCode.

For this connector, the PSFT_OIM_ER_MSG message that is published to Oracle Identity Manager contains the current and effective employee data including Personal and Job details.

To publish the message for future-dated rows (publishing PSFT_OIM_ER_MSG on the day when the future employee data has become current), the following messages are created:

- For Personal data:

  OIM_PERSON_SYNC

  OIM_PERSON_SYNC_EFF

- For Job data:

  OIM_JOB_SYNC

  OIM_JOB_SYNC_EFF

The publishing of a message for the Effective Date feature is done in three steps as follows:

For Current-dated changes:

1. The application publishes the OIM_PERSON_SYNC or the OIM_JOB_SYNC (in the case of Job changes) message. This message is published internally to PeopleSoft. It contains all the data changes (past, current, and future). This message calls a PeopleSoft function that checks if the table rows contain current or future data.
2. Then the OIM_PERSON_SYNC_EFF or the OIM_JOB_SYNC_EFF message is published internally to PeopleSoft and contains only current data.
3. After the two preceding messages are published, the PSFT_OIM_ER_MSG is created. It contains the data from either the OIM_PERSON_SYNC_EFF or the OIM_JOB _SYNC_EFF message (current data only) and is formatted and sent to Oracle Identity Manager.

For Future-dated changes:

1. The application publishes the OIM_PERSON_SYNC or the OIM_JOB _SYNC (in the case of Job changes) message internally to PeopleSoft. It contains all the data changes (past, current, and future). This message calls a PeopleSoft function that checks if the table rows contain current or future data. If the row contains data that

is future-dated, it is stored in the PS_EO_EFFDELAY table, which is available in PeopleSoft.

2. Then the OIM_PERSON_SYNC_EFF or the OIM_JOB _SYNC_EFF message is published internally to PeopleSoft. The future changes need to be published on the day they become current by using the EOP_PUBLISHE Application Engine program. Because of this, Oracle recommends that you must schedule the EOP_PUBLISHE Application Engine program to run **daily**. For information about configuring the EOP_PUBLISHE Application Engine Program, see "Configuring the EOP_PUBLISHE Application Engine Program" on page 2-27.

3. The application checks all the rows in the PS_EO_EFFDELAY table containing data that becomes current on a particular date and creates the corresponding PSFT_OIM_ER_MSG message for each row in the table. The PSFT_OIM_ER message is then formatted and sent to Oracle Identity Manager.

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 passed among systems through PeopleSoft Integration Broker.

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

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

1. Creating the Queues
2. Creating the Messages
3. Publishing the Messages
4. Configuring PeopleSoft Integration Broker

2.2.2.2.1 Creating the Queues

To create queues:

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

   ```
   http://SERVER_NAME/psp/ps/DATABASE_NAME/?cmd=login
   ```

   For example:

   ```
   http://psftserver.example.com/psp/ps/TestDB/?cmd=login
   ```

2. In the PeopleSoft Internet Architecture window, expand **People Tools**, **Integration Broker**, and **Integration Setup**, and then click **Queues**.

3. On the Add a New Value tab, enter the queue name, for example, `OIM_ER_QUEUE`, and then click **Add**.

4. On the Queue Definitions tab, select **archive**.

5. Select **Run** from the **Queue Status** list.

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

2.2.2.2.2 Creating the Messages

To create messages:

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

   ```
   http://SERVER_NAME/psp/ps/DATABASE_NAME/?cmd=login
   ```

   For example:

   ```
   http://psftserver.example.com/psp/ps/TestDB/?cmd=login
   ```

2. In the PeopleSoft Internet Architecture window, expand **People Tools**, **Integration Broker**, and **Integration Setup**, and then click **Messages**.
3. On the Find an Existing Value tab:

   a. Enter `PERSON_BASIC_SYNC` as the message name and `VERSION_3` as the version. Click **Search**.

   > **Note:** The version that you specify for PERSON_BASIC_SYNC is applicable for PeopleSoft HCM 8.9 and 9.0. For PeopleSoft HRMS 8.8 SP1, you must enter `VERSION_2` as the version.

   b. Click **Save As**. Save the message with the name as OIM_PERSON_SYNC and the version as VERSION_1.

   c. Click **OK**.

   d. Repeat Steps b and c to save another message with the name OIM_PERSON_SYNC_EFF and the version as VERSION_1.

4. Repeat Step 2 to open the WORKFORCE_SYNC message with the version VERSION_2. Save the message as OIM_JOB_SYNC and OIM_JOB_SYNC_EFF with the versions as VERSION_1.

   > **Note:** The version that you specify for WORKFORCE_SYNC is applicable for PeopleSoft HCM 8.9 and 9.0. For PeopleSoft HRMS 8.8 SP1, you must enter `VERSION_1` as the version.

5. In the PeopleSoft Internet Architecture window, expand **People Tools**, **Integration Broker**, and **Integration Setup**, and then click **Messages**.
6. On the Add a New Value tab, enter `PSFT_OIM_ER_MSG` as the message name and `VERSION_1` as the version.
7. On the Message Definition tab, select **Nonrowset-based** as the message type.
8. Click **Save** to save the changes.

2.2.2.2.3 Publishing the Messages

Publishing messages involves the following procedures:

- Writing the PeopleCode for Components
- Creating the Application Package

Writing the PeopleCode for Components

To write the PeopleCode for components:

1. Click **Start**, **Programs**, **Peoplesoft8.x**, and then **Application Designer**. The Application Designer window is displayed in 2-tier mode

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

2. From the File menu, click **Open**. The Open Definition dialog box is displayed.
3. Select **Component** from the Definition list, enter `PERSONAL_DATA` in the **Name Selection Criteria** field, and then press **Enter**. All component names starting with the text `PERSONAL_DATA` are displayed.
4. Select **PERSONAL_DATA** from the list, and then click **Open.** The details of the PERSONAL_DATA component are displayed.
5. Click the **Structure** tab, right-click **PERSONAL_DATA,** and then select **View PeopleCode** from the list. The PeopleCode window for the PERSONAL_DATA component is displayed.
6. Select the **SavePostChange** event from the list in the upper-right corner of the window. The PeopleCode for this event is displayed.
7. In the *OIM_HOME*/XLIntegrations/PSFTER/peopleCode/PERSONAL_DATA_component_8.49.txt file, perform the following:

   Copy the following import definition and paste it at the beginning of the PeopleCode for the SavePostChange event:

   ```
   /* OIM */
   import OIM_PUBLICATION_RULES:OIMPublicationMgr;
   /* OIM end */
   ```

   Copy the rest of the code and paste it at the end of the PeopleCode for the SavePostChange event.

8. From the **File** menu, click **Save** to save the changes to the component.
9. Repeat Steps 2 through 8 if you also want to publish messages for the following components:

   - For **PeopleSoft HRMS 8.8 SP1**:

     – JOB_DATA: In Step 7 of the procedure, copy the code provided in the following file:

     OIM_HOME/XLIntegrations/PSFTER/peopleCode/JOB_DATA_component_8.49.txt

     – JOB_DATA_HIRE: In Step 7 of the procedure, copy the code provided in the following file:

     OIM_HOME/XLIntegrations/PSFTER/peopleCode/JOB_DATA_HIRE_component_8.49&8.8.txt

  - JOB_DATA_ADD_NEE: In Step 7 of the procedure, copy the code provided in the following file:

    OIM_HOME/XLIntegrations/PSFTER/people-Code/JOB_DATA_ADD_NEE_component_8.49&8.8.txt

  - JOB_DATA_CONCUR: In Step 7 of the procedure, copy the code provided in the following file:

    OIM_HOME/XLIntegrations/PSFTER/people-Code/JOB_DATA_CONCUR_component_8.49.txt

- For **PeopleSoft HCM 8.9 and 9.0**:

  - JOB_DATA: In Step 7 of the procedure, copy the code provided in the following file:

    OIM_HOME/XLIntegrations/PSFTER/people-Code/JOB_DATA_component_8.49.txt

  - JOB_DATA_EMP: In Step 7 of the procedure, copy the code provided in the following file:

    OIM_HOME/XLIntegrations/PSFTER/people-Code/JOB_DATA_EMP_component_8.49.txt

  - JOB_DATA_CWR: In Step 7 of the procedure, copy the code provided in the following file:

    OIM_HOME/XLIntegrations/PSFTER/people-Code/JOB_DATA_CWR_component_8.49.txt

  - JOB_DATA_CONCUR: In Step 7 of the procedure, copy the code provided in the following file:

    OIM_HOME/XLIntegrations/PSFTER/people-Code/JOB_DATA_CONCUR_component_8.49.txt

Creating the Application Package

To create the application package:

1. Click **Start**, **Programs**, **Peoplesoft8.x**, and then **Application Designer**. The Application Designer window is displayed in 2-tier mode.

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

2. From the File menu, click **New**. The New Definition dialog box is displayed.
3. Select **application package** from the Definition list, and save the package as OIM_PUBLICATION_RULES.
4. Right-click OIM_PUBLICATION_RULES and select **Insert App Class**. Enter `OIMConnector`.
5. Repeat Step 4 to enter two more application classes: `OIMPublicationMgr` and `OIMSubscriptionMgr`.

6. From the File menu, click **Save All**.
7. Double-click the application classes and copy the code from the following text files into the application classes:
   - In the OIMConnector application class:
     - For **PeopleSoft HRMS 8.8 SP1**:

       OIMConnector_appclass_8.49&8.8.txt
     - For **PeopleSoft HCM 8.9 and 9.0**:

       OIMConnector_appclass_8.49.txt
   - In the OIMPublicationMgr application class:
     - For **PeopleSoft HRMS 8.8 SP1**:

       OIMPublicationMgr_appclass_8.49&8.8.txt
     - For **PeopleSoft HCM 8.9 and 9.0**:

       OIMPublicationMgr_appclass_8.49.txt
   - In the OIMSubscriptionMgr application class:
     - For **PeopleSoft HRMS 8.8 SP1**:

       OIMSubscriptionMgr_appclass_8.49&8.8.txt
     - For **PeopleSoft HCM 8.9 and 9.0**:

       OIMSubscriptionMgr_appclass_8.49.txt

2.2.2.2.4 Configuring PeopleSoft Integration Broker The following sections explain the procedures to configure PeopleSoft Integration Broker on PeopleTools 8.49:

- Configuring PeopleSoft Integration Broker Gateway
- Configuring PeopleSoft Integration Broker

Configuring PeopleSoft Integration Broker Gateway

To configure the PeopleSoft Integration Broker gateway:

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

   ```
   http://SERVER_NAME/psp/ps/DATABSE_NAME/?cmd=login
   ```

   For example:

   ```
   http://psftserver.example.com/psp/ps/TestDB/?cmd=login
   ```

2. Expand **PeopleTools, Integration Broker, Configuration,** and then **Gateways**. The Gateway component details are displayed.
3. Enter `LOCAL` in the **Integration Gateway ID** field, 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 hostname specified in the URL of the PeopleSoft listener are that of the computer on which the target system is installed. The URL of the PeopleSoft listener is in the following format:

   ```
   http://HOST_NAME or IP_ADDRESS:PORT/PSIGW/PeopleSoftListeningConnector
   ```

For example:

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

5. To load all target connectors that are registered with the `LOCAL` gateway, click **Load Gateway Connectors**. A window is displayed mentioning that the loading process is successful. Click **OK**.
6. Click **Save**.
7. Click **Ping Gateway** to check if 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

To configure PeopleSoft Integration Broker:

1. Create a remote node by performing the following steps:

   a. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Nodes**.

   b. On the Add a New Value tab, enter the node name, for example, `OIM_ER_NODE`, and then click **Add**.

   c. On the Node Definition tab, enter a description for the node in the **Description** field. In addition, enter `PS` in the **Default User ID** field.

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

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

   Gateway ID: **LOCAL**

   Connector ID: **HTTPTARGET**

   f. On the **Properties** subpage in the Connectors tab, enter the following information:

   Property ID: **PRIMARYURL**

   Property Name: **URL**

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

   ```
   http://ORACLE_IDENTITY_MANAGER_SERVER_IP_ADDRESS:PORT/peopleSoftERApp/do/pe
   opleSoftER
   ```

   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 Oracle WebLogic Server:

   ```
   http://10.121.16.42:7001/peopleSoftERApp/do/peopleSoftER
   ```

   For IBM WebSphere Application Server:

   ```
   http://10.121.16.42:9080/peopleSoftERApp/do/peopleSoftER
   ```

   For JBoss Application Server:

   ```
   http://10.121.16.42:8080/peopleSoftERApp/do/peopleSoftER
   ```

For Oracle Application Server:

```
http://10.121.16.42/peopleSoftERApp/do/peopleSoftER
```

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

```
https://COMMON_NAME:PORT/peopleSoftERApp/do/peopleSoftER
```

For Oracle WebLogic Server:

```
https://example088196:7002/peopleSoftERApp/do/peopleSoftER
```

For IBM WebSphere Application Server:

```
https://example088196:9443/peopleSoftERApp/do/peopleSoftER
```

For JBoss Application Server:

```
https://example088196:8443/peopleSoftERApp/do/peopleSoftER
```

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

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

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

2. Create a service by performing the following steps:

   a. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Services**.

   b. On the Add a New Value tab, enter the service name `PSFT_OIM_ER_MSG`, and then click **Add**.

   c. Enter a description for the service in the **Description** field.

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

   e. Repeat Steps b through d to create the following services for the messages you created:

   OIM_PERSON_SYNC

   OIM_PERSON_SYNC_EFF

   OIM_JOB_SYNC

   OIM_JOB_SYNC_EFF

3. Create a service operation for each of the messages that you create. All these service operations must be associated with their corresponding services created in Step 2. To do so, perform the following steps:

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

   b. On the Add Service Operation tab, enter the service name for which you are creating the service operation. In addition, enter the service operation name.

The name of the service operation must be the same as that of the service that you created in Step 2.

Note: Each service is associated with a corresponding service operation. The name of the service operation is the same as that of the messages created.

---

c. From the Operation type list, select **Asynchronous-Oneway**, and then click **Add**.

d. On the General tab of the Service Operation Definition page, enter a description for the Operation type in the **Operation Description** field. In addition, enter `PSFT_OIM_ER_MSG.VERSION_1` in the **Message.Version** field, `VERSION_1` in the **Version** field, and `OIM_ER_QUEUE` in the **Queue Name** field.

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

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

g. On the Routing Definition tab, enter `PSFT_HR` in the **Sender Node** field and `OIM_ER_NODE` in the **Receiver Node** field.

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

i. Repeat Steps b through h to create the following service operations. For these service operations, enter `PSFT_HR` in both **Sender Node** and **Receiver Node** fields.

Note: You must enter `PSFT_HR` in *both* fields.

OIM_PERSON_SYNC

OIM_PERSON_SYNC_EFF

OIM_JOB_SYNC

OIM_JOB_SYNC_EFF

j. On the handlers tab of the service operations, for each service operation, except for the PSFT_OIM_ER_MSG service operation:

i. Enter the following values for the service operation:

Name: `OIM_PUBLICATION_RULES`

Type: `OnNotify`

Implementation: `Application Class`

Status: `Active`

ii. Click the **Details** link and enter the following values:

For **OIM_JOB_SYNC** and **OIM_PERSON_SYNC**:

Package Name: `OIM_PUBLICATION_RULES`

Path: `:`

Class ID: `OIMSubscriptionMgr`

Method: `OnNotify`

For **OIM_JOB_SYNC_EFF** and **OIM_PERSON_SYNC_EFF**:

Package Name: `OIM_PUBLICATION_RULES`

Path: `:`

Class ID: `OIMConnector`

Note: You must enter `OIMConnector` in the **Class ID** field. This value is not present in the list.

Method: `OnNotify`

iii. Click **OK**, and then click **Save**.

Before the XML messages are sent from the target system to Oracle Identity Manager, you must verify if 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**.

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 the particular message, you will find the status 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. See "Publishing the Messages" on page 2-20 for more information.

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.

2.2.2.2.5 Configuring the EOP_PUBLISHE Application Engine Program To manage the Effective Date feature, you must configure the EOP_PUBLISHE Application Engine Program. You must perform the procedures described in the following sections for PeopleTools and the target system.

This section describes the following topics:

- Updating the EOP_PUBLISHE Application Engine Program
- Running the EOP_PUBLISHE Application Engine Program

Updating the EOP_PUBLISHE Application Engine Program

To update the EOP_PUBLISHE Application Engine program in PeopleSoft Internet Architecture:

1. Click **Start**, **Programs**, and then **Application Designer**. The Application Designer window is displayed in 2-tier mode.

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

2. From the **File** menu, click **Open**.
3. In the Open Definition dialog box, select **App Engine Program**, enter `EOP_PUBLISHE` as the name of the program, and then click **Open**.
4. In "Section 3100, Step15" of the PeopleCode block that is displayed, you must replace the code for the IsChildRow() function with the following code:

```
/* ******************************** */
/* Is Child Row */
/* ******************************** */
Function IsChildRow(&REC_PARENT As Record, &REC_CHILD As Record, &IDXP As
number, &IDXC As number, &PARENT_EFFDT As string, &CHILD_EFFDT As string)
Returns number;
   If &ARY_RECSTAT [&IDXC] = "B" Then
      Return - 1;
   Else
      If &ARY_RECSTAT [&IDXC] = "E" Then
         Return 1;
      End-If;
   End-If;
   &ARY_KEYFLD = &ARY_ARY_KEYFLD [&IDXP];
   If EO_EFFDTPUB_AET.MSGNAME = "OIM_JOB_SYNC_EFF" Or
         EO_EFFDTPUB_AET.MSGNAME = "OIM_PERSON_SYNC_EFF" Then
      &BAISMOD = 1;
   Else
      &BAISMOD = &ARY_KEYFLD.Len;
   End-If;
   REM For &I = 1 To &ARY_KEYFLD.Len;
   For &I = 1 To &BAISMOD
      &FIELD_PARENT = &REC_PARENT.GetField(@("FIELD." | &ARY_KEYFLD [&I]));
      &FIELD_CHILD = &REC_CHILD.GetField(@("FIELD." | &ARY_KEYFLD [&I]));
      If &FIELD_PARENT.Value > &FIELD_CHILD.Value Then
         Return - 1;
      Else
         If &FIELD_PARENT.Value < &FIELD_CHILD.Value Then
            Return 1;
         End-If;
      End-If;
   End-For;



   /*   IF PARENT RECORD DOES NOT CONTAIN EFFDT,  */
   /*   CHECK TO SEE IF CHILD RECORD CONTAINS     */
   /*   EFFDT AND IT FALLS WITHIN FROM-TO RANGE   */

   If &PARENT_EFFDT = "N" And
         &CHILD_EFFDT = "Y" Then
      &ARY_KEYFLD = &ARY_ARY_KEYFLD [&IDXC];

      For &I = 1 To &ARY_KEYFLD.Len;
         &FIELD_CHILD = &REC_CHILD.GetField(@("FIELD." | &ARY_KEYFLD [&I]));

         If &FIELD_CHILD.Name = "EFFDT" Then
            Evaluate &FIELD_CHILD.Value
            When < &EFFDT_FROM
               Return - 1;
            When > &EFFDT_TO
               Return 1;
            End-Evaluate;
         End-If;
      End-For;
   End-If;


   Return 0;

End-Function;
```

> **Note:** The two messages that contain data with an effective date are used in this code. Therefore, the message names in the code must be the same as the names of the messages created in "Creating the Messages" on page 2-20.

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

Running the EOP_PUBLISHE Application Engine Program

The program checks for all the data rows in the table that have become current and effective and creates the corresponding third message for each current and effective data row.

To run the EOP_PUBLISHE Application Engine Program in PeopleSoft Internet Architecture:

1. Click **Enterprise Components**, **Integration Definitions**, **Initiate Processes**, and then click **Effective Date Publish**. The Connector tab is displayed.
2. Click the **Add a new value** tab and provide a new value for Run Control Id, and then click **Add**.
3. In the Description tab, enter a value for Request ID, Message Name, and End Date. This will result in all effective dated messages being triggered before the specified end date.

> **Note:** The message name can be either OIM_PERSON_SYNC_EFF or OIM_JOB_SYNC_EFF. These have to be same as that created in "Creating the Messages" on page 2-20. Remember to use different Run Control ID's for the two messages.

4. Click **Save**.
5. Click the **Run** tab on the top right corner, and then click **OK**. This action publishes the messages. For verification, search for the initiated process in the Process Monitor tab. A **Success** status must be displayed.

2.3 Postinstallation

Postinstallation information is divided across the following sections:

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

2.3.1 Postinstallation on Oracle Identity Manager

> **Note:** In a clustered environment, you must perform these procedures on each node of the cluster.

- Enabling Logging
- Configuring SSL

2.3.1.1 Enabling Logging

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

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

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

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

- **Oracle WebLogic Server**

  To enable logging:

  1. Make the following changes in the *OIM_HOME*/config/log.properties:

     – Search for the following line:

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

Make this line a comment and uncomment the line preceding this line.

– Locate and uncomment the following lines:

```
#log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
#log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
#log4j.appender.logfile.File=c:/oracle/xellerate/logs/xel.log
#log4j.appender.logfile.MaxBackupIndex=20
#log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
#log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
```

2. Specify the name and the location of the file to which the preceding logs will be written. You can do this by changing the value of the following line:

```
log4j.appender.logfile.File=DIRECTORY_PATH/xel.log
```

3. Add the following line in the *OIM_HOME*/config/log.properties file:

```
log4j.logger.OIMCP.PSFTER=LOG_LEVEL
```

4. In this line, replace *LOG_LEVEL* with the log level that you want to set.

   For example:

```
log4j.logger.OIMCP.PSFTER=DEBUG
```

After you enable logging, the log information is written to the following file:

```
DIRECTORY_PATH/xel.log
```

- **IBM WebSphere Application Server**

  To enable logging:

1. Make the following changes in the *OIM_HOME*/config/log.properties:

   – Search for the following line:

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

Make this line a comment and uncomment the line preceding this line.

– Locate and uncomment the following lines:

```
#log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
#log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
#log4j.appender.logfile.File=c:/oracle/xellerate/logs/xel.log
#log4j.appender.logfile.MaxBackupIndex=20
#log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
#log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
```

2. Specify the name and the location of the file to which the preceding logs will be written. You can do this by changing the value of the following line:

```
log4j.appender.logfile.File=DIRECTORY_PATH/xel.log
```

3. Add the following line in the *OIM_HOME*/config/log.properties file:

```
log4j.logger.OIMCP.PSFTER=LOG_LEVEL
```

4. In this line, replace *LOG_LEVEL* with the log level that you want to set.

   For example:

```
log4j.logger.OIMCP.PSFTER=DEBUG
```

After you enable logging, the log information is written to the following file:

```
DIRECTORY_PATH/xel.log
```

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines:

     ```
     <category name="OIMCP.PSFTER">
        <priority value="LOG_LEVEL"/>
     </category>
     ```

  2. In these lines, replace *log_level* with the log level that you want to set. For example:

     ```
     <category name="OIMCP.PSFTER">
        <priority value="DEBUG"/>
     </category>
     ```

  After you enable logging, the log information is written to the following file:

  ```
  JBOSS_HOME/server/default/log/server.log
  ```

- **Oracle Application Server**

  To enable logging:

  1. Add the following line in the *OIM_HOME*/config/log.properties file:

     ```
     log4j.logger.OIMCP.PSFTER=LOG_LEVEL
     ```

  2. In these lines, replace *LOG_LEVEL* with the log level that you want to set.

     For example:

     ```
     log4j.logger.OIMCP.PSFTER=DEBUG
     ```

  After you enable logging, the log information is written to the following file:

  ```
  ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log
  ```

2.3.1.2 Configuring SSL

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

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

2.3.1.2.1 Configuring SSL on Oracle WebLogic Server You can configure SSL connectivity on Oracle WebLogic Server with either a self-signed certificate or a CA certificate. The following sections describe the procedures:

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

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

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

- Generating Keystore
- Configuring Oracle WebLogic Server

Generating Keystore

To generate the keystore:

1. Run the following command:

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

   For example:

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

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

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

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

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

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

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

For example:

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

4. When prompted for the private key password, enter the same password used for the keystore, for example, `example1234`.
5. Import the keystore by running the following command:

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

For example:

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

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

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

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

Configuring Oracle WebLogic Server

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

1. Log in to the Oracle WebLogic Server console at `http://localhost:7001/console` and perform the following:
   a. Expand the servers node and select the server instance.
   b. Select the **General** tab.
   c. Select the **SSL Listen Port Enabled** option.
   d. Ensure that a valid port is specified in the SSL Listen Port field. The default port is 7002.
   e. Click **Apply** to save your changes.
2. Click the **Keystore & SSL** tab, and then click **Change**.
3. From the Keystores list, select **Custom identity And Java Standard Trust**, and then click **Continue**.
4. Configure the keystore properties. To do so:
   a. In the Custom Identity Key Store File Name column, specify the full path of the keystore generated in Step 1 of "Generating Keystore" on page 2-33, 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 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:

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

- Generating Keystore
- Configuring Oracle WebLogic Server

Generating Keystore

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

1. Run the following command:

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

For example:

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

Note:

The keystore password and the private key password must be the same.

Typically, the alias name is the name or the IP address of the computer on which you are configuring SSL.

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

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

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

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

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

   For example:

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

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

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

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

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

   For example:

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

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

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

   For example:

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

When you run this command, it will prompt 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 2-35, 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 2-35, 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.

2.3.1.2.2 Configuring SSL on IBM WebSphere Application Server You can configure SSL connectivity on IBM WebSphere Application Server with either a self-signed certificate or a CA certificate. The following sections describe this:

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

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

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

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

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

2. Click **Security**, **SSL certificate and key management**, **Related items**, **Key stores and certificates**, **NodeDefaultKeyStore**, and then click **Personal certificates**.
3. Click **Create a self-signed certificate**.
4. In the **Alias** field, enter an alias name. You specify the alias name to identify the certificate request in the keystore.
5. In the CN field, enter a value for common name. The common name must be the fully-qualified DNS host name or the name of the computer. The CN of the certificate must match the domain name or the name of the computer. For example, if the name of your domain is us.example.com, then the CN of the SSL certificate that you create for your domain must also be us.example.com.
6. In the **Organization** field, enter an organization name.
7. In the **Organization unit** field, specify the organization unit.
8. In the **Locality** field, enter the locality.
9. In the **State or Province** field, enter the state.
10. In the **Zip Code** field, enter the zip code.
11. From the **Country or region** list, select the country code.
12. Click **Apply** and then **Save**.
13. Click **Security**, **SSL certificate and key management**, **Related items**, **Key stores and certificates**, **NodeDefaultKeyStore**, and then click **Personal certificates**.
14. Select the check box for the new alias name.
15. Click **Extract.**
16. Specify the absolute file path where you want to extract the certificate under the certificate file name. For example, C:\SSLCerts\sslcert.cer.
17. Click **Apply** and then click **OK**.

Configuring SSL on IBM WebSphere Application Server with a CA Certificate

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

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

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

2. Click **Security**, **SSL certificate and key management**, **Related items**, **Key stores and certificates**, **NodeDefaultKeyStore**.
3. On the Additional Properties tab, click **Personal certificate requests**.
4. Click **New**.
5. In the File for certificate request field, enter the full path where the certificate request is to be stored, and a file name. For example: `c:\servercertreq.arm` (for a computer running on Microsoft Windows).
6. In the **Key label** field, enter an alias name. You specify the alias name to identify the certificate request in the keystore.
7. In the CN field, enter a value for common name. The common name must be the fully-qualified DNS host name or the name of the computer. The CN of the certificate must match the domain name of your community. For example, if the name of your domain is us.example.com, then the CN of the SSL certificate that you create for your community must also be us.example.com.
8. In the **Organization** field, enter an organization name.
9. In the **Organization unit** field, specify the organization unit.
10. In the **Locality** field, enter the locality.
11. In the **State or Province** field, enter the state.
12. In the **Zip Code** field, enter the zip code.
13. From the **Country or region** list, select the country code.
14. Click **Apply** and then **Save**. The certificate request is created in the specified file location in the keystore. This request functions as a temporary placeholder for the signed certificate until you manually receive the certificate in the keystore.

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

15. Send the certification request arm file to a CA for signing.
16. Create a backup of your keystore file. You must create this backup before receiving the CA-signed certificate into the keystore. The default password for the keystore is WebAS. The Integrated Solutions Console contains the path information for the keystore's location. The path to the NodeDefaultKeyStore is listed in the Integrated Solutions Console as:

    ```
    was_profile_root\config\cells\cell_name\nodes\node_name\key.p12
    ```

Now you can receive the CA-signed certificate into the keystore to complete the process of generating a signed certificate for IBM WebSphere Application Server.

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

1. In the WebSphere Integrated Solutions Console, click **Security**, **SSL certificate and key management**, **Related items**, **Key stores and certificates**, **NodeDefaultKeyStore**, and then click **Personal Certificates**.
2. Click **Receive a certificate from a certificate authority**.
3. Enter the full path and name of the certificate file.
4. Select the default data type from the list.
5. Click **Apply** and then **Save**.

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

2.3.1.2.3 Configuring SSL on JBoss Application Server Before configuring SSL on JBoss Application Server, ensure the following:

- JBoss Application Server is installed on the Oracle Identity Manager host computer
- Java Developer's Kit is installed on the JBoss Application Server host

You can configure SSL connectivity on JBoss Application Server with either a self-signed certificate or a CA certificate. The following sections describe this. If you are configuring SSL on JBoss Application Server with a self-signed certificate, then perform the following tasks:

- Creating the Self-Signed Certificate
- Moving the Keystore
- Updating the Configuration File

If you are configuring SSL on JBoss Application Server with a CA certificate, then perform the following tasks:

- Importing a CA Certificate
- Moving the Keystore
- Updating the Configuration File

Creating the Self-Signed Certificate

To create the self-signed certificate, see "Generating Keystore" on page 2-33.

Importing a CA Certificate

To import a CA certificate, perform the following tasks:

1. Run the following command:

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

   For example:

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

Note:

- The keystore password and the private key password must be the same.

- Typically, the alias is the name or IP address of the computer on which you are configuring SSL.

- The alias used in the various command of this procedure must be the same.

2. When prompted, enter the information about the certificate, such as company and contact name. This information is displayed to employees attempting to access a secure page in the application. This is illustrated in the following example:

   ```
   What is your first and last name?
     [Unknown]:  Must be the name or IP address of the computer
   What is the name of your organizational unit?
     [Unknown]:  example
   What is the name of your organization?
     [Unknown]:  example
   What is the name of your City or Locality?
     [Unknown]:  New York
   What is the name of your State or Province?
     [Unknown]:  New York
   What is the two-letter country code for this unit?
     [Unknown]:  US
   Is <CN=Name or IP address of the computer, OU=example, O=example, L=New York,
   ST=New York, C=US> correct?
     [no]:  yes
   ```

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

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

   ```
   keytool -certreq -alias ALIAS_NAME -file ABSOLUTE_CSR_PATH  -keystore
   ABSOLUTE_KEYSTORE_PATH
   ```

   For example:

   ```
   keytool -certreq -alias example088196 -file c:\temp\keys\certReq.csr -keystore
   c:\temp\keys\custom.keystore
   ```

4. Submit the certReq.csr file on a CA Web site for downloading the CA certificate.

   Ensure that your %JAVA_HOME%\jre\lib\security\cacerts has the root certificate of the CA that has generated the CA certificate.

   To check all the root certificates that %JAVA_HOME%\jre\lib\security\cacerts contains, run the following command:

   ```
   keytool -list -keystore %JAVA_HOME%\jre\lib\security\cacerts -storepass
   cacerts_store_password
   ```

   For example:

   ```
   %JAVA_HOME%\jre\bin\keytool -list -keystore
   %JAVA_HOME%\jre\lib\security\cacerts -storepass changeit
   ```

If the %JAVA_HOME%\jre\lib\security\cacerts keystore does not contain the root certificate of CA that has generated the CA certificate, then you must import the root certificate of CA into %JAVA_HOME%\jre\lib\security\cacerts.

Run the following command to import the root certificate of CA:

```
keytool -import  -alias <cacerts_key_entry_alias> -file <CARootCertificate.cer>
-keystore %JAVA_HOME%\jre\lib\security\cacerts  -storepass
cacerts_store_password
```

For example:

```
keytool -import -alias cakey -file "C:\temp\Thawte Test Root.cer" -keystore
%JAVA_HOME%\jre\lib\security\cacerts -storepass changeit
```

You will see that the certificate has been added to the keystore.

5. Import the CA certificate by running the following command:

```
keytool -import -alias ALIAS_NAME -keystore ABSOLUTE_KEYSTORE_PATH
-trustcacerts -file ABSOLUTE_CACERT_PATH
```

ABSOLUTE_CACERT_PATH represents the path in which you have stored the certificate downloaded from CA.

For example:

```
keytool -import -alias example088196 -keystore c:\temp\keys\custom.keystore
 -trustcacerts -file c:\temp\keys\CACert.cer
```

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

```
Enter keystore password:  example1234 [Enter]
Owner: CN=Thawte Test CA Root, OU=TEST TEST TEST, O=Thawte Certification,
ST=FOR TESTING PURPOSES ONLY, C=ZA
Issuer: CN=Thawte Test CA Root, OU=TEST TEST TEST, O=Thawte Certification,
ST=FOR TESTING PURPOSES ONLY, C=ZA
Serial number: 0
Valid from: Thu Aug 01 05:30:00 GMT+05:30 1996 until: Fri Jan 01 03:29:59
GMT+05:30 2021
Certificate fingerprints:
         MD5:  5E:E0:0E:1D:17:B7:CA:A5:7D:36:D6:02:DF:4D:26:A4
         SHA1: 39:C6:9D:27:AF:DC:EB:47:D6:33:36:6A:B2:05:F1:47:A9:B4:DA:EA
Trust this certificate? [no]:  yes [Enter]
```

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

Moving the Keystore

To move the certificate to a JBoss Application Server directory, copy the generated keystore to the conf directory of your JBoss installation. For example, the directory can be C:\Program Files\jboss-4.0.3\server\default\conf\.

Updating the Configuration File

Before updating the configuration file, shut down JBoss Application Server. The *JBOSS_HOME*/server/default/deploy/jbossweb-tomcat55.sar/server.xml file contains information about what web features to turn on when the server starts up. Inside this file, there is a part that looks similar to the following:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore
<Connector port="8443" address="${jboss.bind.address}"
  maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
  emptySessionPath="true"
  scheme="https" secure="true" clientAuth="false"
  keystoreFile="${jboss.server.home.dir}/conf/chap08.keystore"
  keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
```

In the code, make the following changes:

- Uncomment the block of code.
- Change the value of `Connector port` to `443` (default SSL port).
- Change the value of `keystoreFile` to the absolute path of the keystore generated in "Generating Keystore" on page 2-33.
- Change the value of `keystorePass` to the password of the keystore.

After making the changes, the code block will look similar to the following:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="443" address="${jboss.bind.address}"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/ custom.keystore"
keystorePass=" example1234 " sslProtocol = "TLS" />
<!-- -->
```

SSL is now enabled. You can restart JBoss Application Server and browse to the following URL to verify if SSL is enabled:

```
https://localhost:443
```

2.3.2 Postinstallation on the Target System

Postinstallation on the target system consists of the following procedure:

2.3.2.1 Configuring SSL

To configure SSL:

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

   Note: If you are using IBM WebSphere Application Server, then you must download the root certificate from a CA.

2. Run the following command:

   ```
   PEOPLESOFT_HOME/webserv/peoplesoft/bin/pskeymanager.cmd -import
   ```

3. When prompted, enter the current keystore password.
4. When prompted, enter the alias of the certificate that you want 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.

3 Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

- Adding New Fields for Full Reconciliation
- Adding New Fields for Incremental Reconciliation

3.1 Adding New Fields for Full Reconciliation

To add new fields for full reconciliation:

> **Note:** If you do not want to add new fields for full reconciliation, then you need not perform this procedure.

1. In PeopleSoft Application Designer:

   a. From the File menu, click **Open**. The Open Definition dialog box is displayed.

   b. Select **App Engine Program** from the **Definition** list.

   c. Enter `BLKPRCS_ER` in the **Name Selection Criteria** field.

   d. Click **Open**.

2. Modify the header and queries in the application engine code (BLKPRCS_ER).

   For example, suppose you want to add the alternate city field, ALT_CITY, to the list of fields that are reconciled. You must first identify the table in which this field is located. This field is located in the ADDRESSES table. The required changes are as follows:

   a. Define this field as a variable. To do so, add the code highlighted in bold in the following sample:

   ```
   Local string &city_ac;
   ```

   b. Modify the header variable to include the new variable, which you want to reconcile. Add the lines highlighted in bold in the following code sample:

   ```
   &hdr = "EMPLID" | &Sepratr | "LASTNAME" | &Sepratr | "FIRSTNAME" | &Sepratr
   | "SEX" | &Sepratr | "POSTAL" | &Sepratr | "CITY" | &Sepratr | "PHONE" |
   &Sepratr | "BIRTHDATE" | &Sepratr | "COUNTRY" | &Sepratr | "ADDRESS" |
   &Sepratr | "STATE" | &Sepratr | "HIRE_DATE" | &Sepratr | "DEPTID" |
   &Sepratr | "JOBCODE" | &Sepratr | "EMPLOYEETYPE" | &Sepratr | "STATUS" |
   &Sepratr | "ALT_CITY";
   ```

c. At the end of the SQL statements section, add a SQL statement to retrieve and store the column values of the new field in a local variable as follows:

```
/* ALTERNATE CITY */
   &Sel = CreateSQL("select CITY_AC from %table(ADDRESSES) where EMPLID =
:1", &emplid);
   &f = &Sel.Fetch(&city_ac);
```

d. Add data fields that are retrieved to the XML message. For example, to add the data fields of the CITY_AC column to the ALT_CITY tag, add the lines highlighted in bold in the following code sample:

```
&datarow = &datarow | &phone | &Sepratr | &bdate | &Sepratr | &cnty |
&Sepratr | &address | &Sepratr | &state | &Sepratr | &hdate | &Sepratr |
&deptid | &Sepratr | &jobcode | &Sepratr | &emptype | &Sepratr | &hrstatus
| &Sepratr | &city_ac;
```

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

> **See Also:** *Oracle Identity Manager Design Console* for detailed instructions on performing the following steps

a. Create a new user-defined field. For the procedure to create a new user-defined field, see "Creating a New User-Defined Field" on page 3-5.

b. Add a reconciliation field corresponding to the new field in the PSFT_ER_RO resource object. For the example described earlier, you can add the Users.ALTCITY reconciliation field

c. Modify the PSFT_ER 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:

```
Users.ALTCITY = Alternate City
```

4. Add the new field in the Lookup.PSFTER.Attr.Map.Recon lookup definition. The format that you must use is as follows:

Code Key	Decode Key
TargetAttribute	*Users.OimAttributeName*

> **Note:** You must ensure that the *TargetAttribute* value that you specify does not contain spaces.

For example:

```
Code Key value: ALT_CITY
Decode: Users.ALTCITY
```

In this example, ALTCITY is the reconciliation field and its equivalent target system field is CITY_AC. As a standard, the prefix "Users." is added at the start of all reconciliation field names.

5. Restart Oracle Identity Manager.

3.2 Adding New Fields for Incremental Reconciliation

> **Note:** If you do not want to add new fields for incremental reconciliation, then you can skip this section.

Standard incremental reconciliation involves the reconciliation of predefined fields. If required, you can add new fields to the list of fields that are reconciled.

To add new fields for incremental reconciliation:

1. Modify the PeopleCode given in the following files. These files are in the *OIM_HOME*/XLIntegrations/PSFTER/peopleCode directory.

   - For HRMS 8.8 SP1

     OIMConnector_appclass_8.49&8.8.txt

   - For HCM 8.9 and 9.0

     OIMConnector_appclass_8.49.txt

   For example, suppose you want to add the alternate city field, ALT_CITY, to the list of fields that are reconciled. You must first identify the table in which this field is located. This field is located in the ADDRESSES table. The required changes are as follows:

   a. Define this field as a variable. To do so, add the code highlighted in bold in the following sample:

   ```
   Local string &EMPLID, &lname, &fname, &sex, &postal, &city, &phone, &cnty,
   &address, &state, &bdate, &hrstatus, &reg_temp, &per_org, &full_part_time,
   &emptype, &address1, &address2, &address3, &city_ac;
   ```

   Then, you must initialize it. To do so, add the code highlighted in bold in the following sample:

   ```
   &Hrstat = "";
   &date = "";
   &city_ac = "";
   ```

   b. At the end of the SQL statements section, add a SQL statement to retrieve and store the column values of the new field in a local variable.

   ```
   If (&city_ac = "") Then
     &Sel = CreateSQL("select A.CITY_AC from %table(ADDRESSES) A where
   A.EMPLID = :1", &EMPLID);
     &f = &Sel.Fetch(&city_ac);
   End-If;
   ```

   c. Add data fields that are retrieved to the XML message. For example, to add the data fields of the CITY_AC column to the ALT_CITY tag, add the lines highlighted in bold in the following code sample:

   ```
   &recnode = &fieldtypenode.AddElement("DEPT_TBL");
   &recnode.AddAttribute("class", "R");
   &fields = &recnode.AddElement("DEPTNAME");
   &fields.AddAttribute("type", "CHAR");
   &fields = &recnode.AddElement("ALT_CITY");
   &fields.AddAttribute("type", "CHAR");
   ```

d. Add the data text that are retrieved to the XML message. For example, to add the data text of the CITY_AC column to the ALT_CITY tag, add the lines highlighted in bold in the following code sample:

```
&datarecnode = &transnode.AddElement("DEPT_TBL");
&datarecnode.AddAttribute("class", "R");
&datafldnode = &datarecnode.AddElement("DEPTNAME");
&textnode = &datafldnode.AddText(&deptname);
&datafldnode = &datarecnode.AddElement("ALT_CITY");
&textnode = &datafldnode.AddText((&city_ac);
```

2. Extract the contents of the peopleSoftERApp.war file into a temporary directory by using the following command:

```
jar -xvf peopleSoftERApp.war
```

Copies of this file are in the application server deployment directory.

3. In the attributemap.properties file, add the XPath (key-value entry) of the new field. For example, add the following XPath for the ALT_CITY attribute:

```
Users.ALTCITY=//Transaction/PERSONAL_DATA/ALT_CITY
```

Note: In the attributemap.properties file, the key part of each line is the text to the left of the equal (=) sign. You must ensure that the key part of the lines does not contain spaces. For example, `Users . ALTCITY`, `Users. ALTCITY`, and `Users.ALT CITY` are all invalid key values because they contain spaces.

4. Delete the existing peopleSoftERApp.war file from the temporary directory into which you extracted it, and then enter the following command to re-create the file that contains the new attribute:

```
jar -cvf peopleSoftERApp.war .
```

5. Delete the old version of the peopleSoftERApp.war file from the application server deployment directory.

6. Copy the newly created peopleSoftERApp.war file into the application server deployment directory.

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

See Also: *Oracle Identity Manager Design Console* for detailed instructions on performing the following steps

a. Create a new user-defined field. For the procedure to create a new user-defined field, see "Creating a New User-Defined Field" on page 3-5.

b. Add a reconciliation field corresponding to the new field in the PSFT_ER_RO resource object. For the example described earlier, you can add the Users.ALTCITY reconciliation field.

c. Modify the PSFT_ER process definition to include the mapping between the newly added attribute and the corresponding reconciliation field. For the example described earlier, the mapping is as follows:

```
Users.ALTCITY = Alternate City
```

In this example, `ALTCITY` is the reconciliation field and also the equivalent target system field. As a standard, the prefix "`Users.`" is added at the start of all reconciliation field names.

8. Restart Oracle Identity Manager.

Creating a New User-Defined Field

To create a new user-defined field, perform the following:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand the Administration folder.
3. Double-click **User Defined Field Definition**.
4. Search for and open the Users form.
5. Click **Add**.
6. Enter the details of the field.

   For example, if you are adding the Alternate City field, then enter Alternate City in the Label field, set the data type to String, enter USR_UDF_ALT_CITY as the column name, and enter a field size value.
7. Click **Save**.

4

Using the Connector

This chapter contains the following topics:

- Configuring Full Reconciliation
- Configuring Incremental Reconciliation

You can also configure the connector for multiple trusted source reconciliation, as described in "Multiple Trusted Source Reconciliation" on page 4-13.

The guidelines for using this connector are described in the following section:

- Guidelines on Using the Connector

4.1 Configuring Full Reconciliation

This section discusses the following topics:

- Specifying the Number of Records to Be Reconciled
- Determining the Last Record Reconciled
- Limited Reconciliation
- Configuring the Reconciliation Scheduled Task
- Running the Application Engine Program

4.1.1 Specifying the Number of Records to Be Reconciled

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can specify the number of records to be reconciled at a time by using the NoOfRecordsToBeReconciled scheduled task attribute. You must enter any integer value greater than zero. The default value of this attribute is `5`.

4.1.2 Determining the Last Record Reconciled

You use the IndexOfLastReconciledRecord scheduled task attribute during a full reconciliation run to determine the last record reconciled. At the start of the first full reconciliation run, the value of this attribute is `-1`. At the end of each subsequent full reconciliation run, this attribute stores the index number of the last record reconciled during the previous reconciliation run.

Whenever you want to perform a full reconciliation run, change the value of the IndexOfLastReconciledRecord attribute to `-1`.

> **Note:** During limited reconciliation, if the IsFilterApplied=Yes condition is specified, then this attribute will not be updated during a reconciliation.

4.1.3 Limited Reconciliation

By default, all target system records that are added or modified after the previous reconciliation run are reconciled during the current reconciliation run. You can customize the reconciliation process by specifying the subset of newly added or modified records that must be reconciled. You implement this form of **limited reconciliation** by creating **customized queries** for reconciliation. You do this by creating filters for reconciliation.

Creating a filter involves specifying a value for the IsFilterApplied, FiltersToBeApplied, FiltersValues, SearchCriteria, CaseSensitive, and the Operator scheduled task attributes.

When performing limited reconciliation for this connector, you can specify one or a combination of the following target system fields as values of the scheduled task attributes mentioned earlier:

- EMPLID
- LASTNAME
- FIRSTNAME
- SEX
- POSTAL
- CITY
- SSN
- PHONE
- BIRTHDATE
- COUNTRY
- ADDRESS
- STATE
- HIRE_DATE
- DEPTID
- JOBCODE
- STATUS

If you want to use multiple target system fields to filter records, then you must also specify the logical operator (`AND` or `OR`) that you want to apply to the combination of target system fields that you select.

Consider the filters applied through the scheduled task attributes in the following examples of limited reconciliation:

> **See Also:** The "Configuring the Reconciliation Scheduled Task" section on page 4-4 for information about these scheduled task attributes used for filtering records.

Example 1:

```
IsFilterApplied=yes
FiltersToBeApplied=EMPLID,LASTNAME,FIRSTNAME
FiltersValues=SFCA001,Doe,John
CaseSensitive=yes
SearchCriteria= INDEX_OF
Operator=and
```

This example will reconcile all the records in which the EMPLID, LASTNAME, and FIRSTNAME fields contain the values SFCA001, Doe, and John, respectively. The search criteria INDEX_OF has been specified. Therefore, the query will search within a string and reconcile all the records that contain these values.

If you specify SearchCriteria= EXACT_MATCH, then the query will match the full string instead of searching within the string.

Example 2:

```
IsFilterApplied=yes
FiltersToBeApplied=FIRSTNAME,SEX,POSTAL
FiltersValues=John,M,1920
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=and
```

This example will reconcile all the records in which the FIRSTNAME, SEX, and POSTAL fields contain the values John, M, and 1920, respectively. The case of the values will not be considered. The values of SearchCriteria and CaseSensitive are specified as EXAMPLE. Therefore, by default, INDEX_OF and NO are used as the values of these attributes.

Example 3:

```
IsFilterApplied=EXAMPLE
FiltersToBeApplied=FIRSTNAME,SEX,POSTAL
FiltersValues=John,M,1920
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=AND
```

This example will reconcile all the records. The value of IsFilterApplied is specified as EXAMPLE. Therefore, by default, the value `nodata` is used as the value and all the records are reconciled.

Example 4:

```
IsFilterApplied=EXAMPLE
FiltersToBeApplied=FIRSTNAME,SEX,Postal
FiltersValues=John,,
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=NODATA
```

This example will reconcile all the records in which the value of FIRSTNAME is `John`, and the values of SEX and POSTAL are not specified. You must provide a space in the search criteria if you want to reconcile all records in which no values have been specified.

Example 5:

```
IsFilterApplied=YES
FiltersToBeApplied=FIRSTNAME,SEX,POSTAL
FiltersValues=John,M,1920
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=NODATA
```

The value of Operator is invalid. As a result of this, no records will be reconciled. The valid values are AND or OR.

4.1.4 Configuring the Reconciliation Scheduled Task

When you run the Connector Installer, the PSFTERTrustedUserRecon scheduled task is automatically created in Oracle Identity Manager.

To perform a full reconciliation run, you must configure the scheduled task to reconcile all employee data into Oracle Identity Manager depending on the values that you have specified in the scheduled task attributes.

To configure the reconciliation scheduled tasks for this connector, perform the procedure described in the following section.

The employee reconciliation scheduled task has been defined only for trusted source employee reconciliation.

4.1.4.1 Managing Scheduled Tasks

> **Note:** This feature is in the process of being migrated from the Design Console to the Administrative and User Console. For the current Oracle Identity Manager release, this feature is available in both consoles.

To locate a scheduled task:

1. Expand **Resource Management**.
2. Click **Manage Scheduled Task**.
3. On the Scheduled Task Management page, you can use any one or a combination of the search options provided to locate a scheduled task. Click **Search** after you specify the search criteria.

Each row of the search results table displays the following information about a scheduled task:

- Scheduled Task: This column displays the name of the scheduled task. If you want to view the details of the scheduled task, then click its name in this column.
- Status: This column displays the status of the scheduled task. The status can be one of the following:
  - INACTIVE: The scheduled task has been run successfully, and it is set to run again at the date and time specified in the Next Start field.
  - RUNNING: The scheduled task is currently running.

  - COMPLETED: The scheduled task has been run successfully, but will not run again (the frequency is set at the **Once** option).
  - ERROR: An error was encountered due to which the task could not be started.
  - FAILED: The scheduled task failed while running.
- Frequency: This column displays the frequency at which the scheduled task has been set to run.
- Last Start: This column displays the date and time at which the scheduled task began its last run.
- Last Stop: This column displays the date and time at which the scheduled task ended its last run.
- Next Start: This column displays the date and time at which the scheduled task will begin its next run.
- Edit: This column displays the edit icon for each scheduled task. Click the edit icon if you want to modify the task.
- Enable: For a particular scheduled task, if the Enable link is displayed in this column, then it means that the scheduled task is currently disabled and you can enable the task by clicking the **Enable** link. If `Enabled` is displayed, then it means that the task is already enabled.
- Disable: For a particular scheduled task, if the Disable link is displayed in this column, then it means that the scheduled task is currently enabled and you can disable the task by clicking the **Disable** link. If `Disabled` is displayed, then it means that the task is already disabled.
- Run Now: For a particular scheduled task, if the Status column displays `INACTIVE` and if the gray button is displayed in the Enable column (implying that the task is in the enabled state), then you can run the task by clicking the button in the Run Now column. This button cannot be used if any one of the following conditions is true:
  - The Status column displays `RUNNING`, which means that the task is currently running.
  - The Enable column displays the green button (and the Disable column displays the gray button), which means that the task must be enabled before it can be run.

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.

The following sections describe the procedures that you can perform by using the features of the Scheduled Task Management page:

- Viewing Scheduled Tasks
- Modifying Scheduled Tasks

Viewing Scheduled Tasks

To view the details of a scheduled task, click the task name in the Scheduled Task column of the search results table displayed on the Scheduled Task Management page.

After viewing the scheduled task details, click **Edit** if you want to modify the scheduled task. Alternatively, you can click **Run now** if you want to run the scheduled task. As mentioned earlier, only a scheduled task that is currently `ENABLED` can be run.

Modifying Scheduled Tasks

To modify the details of a scheduled task:

1. In the search results table displaying the list of scheduled tasks, click the edit icon in the Edit column of the table.

   Note: If you want to run the task, click the task name in the first column of the search results table and then click **Run now**. After you click **Run now**, you need not perform the rest of the steps in this procedure.

   If you want to stop a scheduled task while it is running, then use the Stop Execution feature of the Design Console. See "The Task Scheduler Form" in *Oracle Identity Manager Design Console Guide* for information about this feature.

2. On the Scheduled Task Details page, you can modify all the details of the scheduled task, except for the task name and class name.
3. Click **Continue**.
4. If required, modify the attributes of the scheduled task. You can modify values of existing attributes, delete attributes, or add new ones.

   You must specify values for the attributes of the user reconciliation scheduled tasks. Table 4–1 describes 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 that you want to change.

Table 4–1 Attributes of the Scheduled Tasks for Reconciliation of Employee Data

Attribute Name	Description
FilePath	Enter the full path of the location in which the flat file is stored on Oracle Identity Manager. The operating system of a remote computer must be able to access this file path. **Note**: The file path must contain the path of only the flat file that is generated when you run the Application Engine program, because the scheduled task searches for text files. See "Configuring the Target System for Full Reconciliation" on page 2-15 for information about generating the delimiter-separated flat file. Default value: `C:\OIM_HCM_BulkRecon.txt`
ReconcilingRO	Enter the name of the resource object Default value: `PSFT_ER_RO`
OrganizationName	Enter the default name of the Oracle Identity Manager organization. This value is used while creating an OIM User. The value that you specify must exist in Oracle Identity Manager. Default value: `Xellerate Users`
NoOfRecordsToBeReconciled	Enter the number of records to be reconciled See "Specifying the Number of Records to Be Reconciled" on page 4-1 for more information about this attribute. Default value: `5`
ServerName	Enter the name of the IT resource. Default value: PSFT_Employee
IndexOfLastReconciledRecord	Use this attribute to specify the index of the last successfully reconciled record. This attribute is applicable only for full reconciliation. See "Determining the Last Record Reconciled" on page 4-1 for more information about this attribute. Default value: `-1`
IsFilterApplied	Specify whether or not filters must be applied during reconciliation. The value can be `Yes`, `No`, or `NoData`. However, if invalid values are provided, then by default the value of this attribute will be considered as `No`. See "Limited Reconciliation" on page 4-2 for more information about using this attribute. Default value: `NoData`
FiltersToBeApplied	Specify the comma-separated list of filters (for target system user fields) that you want to apply during reconciliation. See "Limited Reconciliation" on page 4-2 for more information about using this attribute. Default value: `NoData`

Table 4–1 (Cont.) Attributes of the Scheduled Tasks for Reconciliation of Employee Data

Attribute Name	Description
FiltersValues	Specify the comma-separated values for the filter attributes that you specify as values for the FiltersToBeApplied attribute. See "Limited Reconciliation" on page 4-2 for more information about using this attribute. The filtering process is controlled by the IsFilterApplied attribute. Based on the value specified (Yes, No, or Nodata), the filtering is performed. Consider the following test cases: Consider the following test cases in which the two filter conditions are SFCA001, JOHN: Case 1: IsFilterApplied = yes, FiltersToBeApplied = nodata, and FiltersValues = nodata This case is equivalent to IsFilterApplied = no, and all the records will be reconciled. Case 2: IsFilterApplied = yes, FiltersToBeApplied =, and FiltersValues = This case is equivalent to IsFilterApplied = no, and all the records will be reconciled. Case 3: IsFilterApplied = yes, FiltersToBeApplied = EMPLID,LASTNAME, and FiltersValues = In this case, the "Filters are not synchronized" error message is displayed. **Note:** In the FiltersValues attribute, the data is separated by a comma. However, if a comma is part of values, then it will be treated as a different value. Consider the following example: IsFilterApplied = yes, FiltersToBeApplied = EMPLID,ADDRESS, and FiltersValues = SFC1001,San Jose,California In this scenario, the user has entered the value of ADDRESS as "San Jose, California". The filtering engine will consider it as two different values, "San Jose", and "California". The FiltersToBeApplied attribute contains two filters while the FiltersValues attribute contains three. As a result of this inconsistency, the "Filters are not synchronized" error message will be displayed..
CaseSensitive	Enter Yes as the value of this attribute if you want to search records on the basis of the case (uppercase and lowercase letters). When the filters are applied, a case-sensitive search is applied for records that match the filter criteria. The values can be Yes, No, or Nodata. Default value: Nodata
SearchCriteria	Specify the search algorithm to be applied on the filters that you enter. The values can be INDEX_OF, EXACT_MATCH, or NoData. However, if invalid values are provided, then by default the value of this attribute will be considered as INDEX_OF. Default value: NoData See "Limited Reconciliation" on page 4-2 for more information.

Table 4–1 (Cont.) Attributes of the Scheduled Tasks for Reconciliation of Employee Data

Attribute Name	Description
Operator	Specify the operator that you want to apply to the filter attributes for which you specify a value other than `nodata`. Depending on the value specified (`AND` or `OR`), data is joined accordingly for any combination of the target system attributes specified in the FiltersToBeApplied scheduled task attribute. During reconciliation, only those target system records that contain the specified combination are reconciled. However, if an invalid value is provided, then the "Invalid Operators" error message is displayed and no records are reconciled. Default value: `OR`
ScheduledTaskName	Enter the name of the scheduled task. This attribute is used to update the IndexOfLastReconciledRecord attribute.
LookupForAttributeMapping	Enter a value for this attribute to specify the name of the lookup definition that maps reconciliation fields used during a reconciliation run. The name of this lookup definition cannot be changed. Default value: Lookup.PSFTER.Attr.Map.Recon
LookupForEmployeeTypeMapping	Enter the name of the lookup definition that maps the PeopleSoft person types with the OIM employee types. Default value: Lookup.PSFTER.EmpType.Map.Recon
UserType	Enter the user type for Oracle Identity Manager. This value is used to create OIM Users. The value that you specify must exist in Oracle Identity Manager. Default value: `End-User`
RecordDelimiter	Specify a value for this attribute to configure the delimiter. If you do not enter any value, then the asterisk character (*) will be used as the delimiter character. Valid values are all special characters except the following: ■ Hash (`#`) ■ Semicolon (`;`) ■ Period (`.`) ■ At sign (`@`) ■ Comma (`,`) Consider the following sample scenarios: Sample scenario 1: `RecordDelimiter = myDelimiter` In this case, `m` will be considered as the delimiter but the records will not be reconciled because the delimiter must be a special character. Sample scenario 2: `RecordDelimiter = $myDelimiter` In this case, `$` will be set as a new delimiter. Sample scenario 3: `RecordDelimiter =` In this case, the default value "`*`" (asterisk) will be set as the delimiter. **Note:** Ensure that the value that you enter for this attribute is the same as that mentioned in the flat file. See "Configuring the Target System for Full Reconciliation" on page 2-15 for instructions to configure the record delimiter.

5. Click **Save Changes** to commit all the changes to the database.

4.1.5 Running the Application Engine Program

You can run the Application Engine program by using PeopleSoft Internet Architecture as follows:

> **Note:** You must run the Application Engine program each time you want to perform full reconciliation.

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

   ```
   http://SERVER_NAME/psp/ps/DATABASE_NAME/?cmd=login
   ```

   For example:

   ```
   http://psftserver.example.com/psp/ps/TestDB/?cmd=login
   ```

2. Click **People Tools**, **Process Scheduler**, **Processes**, and then click **Add a new Value**.
3. Select **Application Engine** as the process type, and enter `BLKPRCS_ER` as the process name.
4. Click **Add**.
5. In the Process Definition Options tab, enter the following values for **Component** and **Process Groups**, and click **Save**:

   Component: `AE_REQUEST`

   Process Groups: `TLSALL`, `STALL`

6. To make the Application Engine program run in PeopleSoft Internet Architecture, click **People Tools**, **Application Engine**, **Request AE**, and then click **Add a new Value**.
7. Enter values for the following and then click **Add**:

   User ID: Enter your OIM User ID

   Run Control ID: Enter a unique run control value

   Program Name: Enter `BLKPRCS_ER`

8. Click **Run**.
9. From the list that is displayed, select the BLKPRCS_ER process, which you created in Step 3.
10. Click **OK**.
11. To determine the progress status of the Application Engine program, click **People Tools**, **Process Scheduler**, and then **Process Monitor**. Click **Refresh** until the `Success` message is displayed as the status.

> **Note:** If the Status is displayed as "Queued", then you must check the status of the process scheduler. To do so, click **People Tools**, **Process Scheduler**, and then **Process Monitor**. Click the **Server List** tab and check the status of server. If no status is displayed, then start the process scheduler.

4.2 Configuring Incremental Reconciliation

> **Note:** In this section, the term "field" refers to the identity attributes that store employee data.

This section discusses the following topic:

4.2.1 Limited Reconciliation

By default, all target system records that are added or modified after the previous reconciliation run are reconciled during the current reconciliation run. You can customize the reconciliation process by specifying the subset of newly added or modified records that must be reconciled. You implement this form of **limited reconciliation** by creating **customized queries** for reconciliation. You do this by creating filters for reconciliation.

Creating a filter involves specifying a value for a target system attribute, which will be used in the `SELECT` query criteria to retrieve the records to be reconciled. This can be done by editing the configureReconciliation.properties file.

When performing limited reconciliation for this connector, you can specify one or a combination of the following resource object attributes as the criteria for filtering records:

- Users.EmplId
- Users.LastName
- Users.FirstName
- Users.Sex
- Users.Postal
- Users.City
- Users.Phone
- Users.BirthDate
- Users.Country
- Users.Address
- Users.State
- Users.SSN
- Users.HIRE_DATE
- Users.DeptId
- Users.JobCode
- Users.Status

If you want to use multiple resource object attributes to filter records, then you must also specify the logical operator (`AND` or `OR`) that you want to apply to the combination of target system attributes that you select.

Consider the filters applied in the following examples of limited reconciliation:

Example 1:

```
IsFilterApplied=yes
```

```
FiltersToBeApplied=Users.EmplId,Users.LastName,Users.FirstName
FiltersValues=SFCA001,Doe,John
CaseSensitive=yes
SearchCriteria= INDEX_OF
Operator=and
```

This example will reconcile all the records in which Users.EmplId, Users.LastName, and Users.FirstName contain the values SFCA001, Doe, and John, respectively. The search criteria INDEX_OF has been specified. Therefore, the search will be conducted within a string and all the records that contain these values will be reconciled.

If you specify SearchCriteria= EXACT_MATCH, then the query will search the full string instead of searching within the string.

Example 2:

```
IsFilterApplied=yes
FiltersToBeApplied=Users.FirstName,Users.Sex,Users.Postal
FiltersValues=John,M,1920
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=and
```

This example will reconcile all the records in which Users.FirstName, Users.Sex, and Users.Postal contain the values John, M, and 1920, respectively. The case (uppercase or lowercase) of the values will not be considered. The values of SearchCriteria and CaseSensitive are specified as EXAMPLE. Therefore, by default, INDEX_OF and NODATA are used as valid values, respectively.

Example 3:

```
IsFilterApplied=EXAMPLE
FiltersToBeApplied=Users.FirstName,Users.Sex,Users.Postal
FiltersValues=John,M,1920
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=or
```

This example will reconcile all the records. The value of IsFilterApplied is an invalid value. Therefore, by default, the value `No` is used and all the records are reconciled.

Example 4:

```
IsFilterApplied=EXAMPLE
FiltersToBeApplied=Users.FirstName,Users.DeptId,Users.Postal
FiltersValues=John,,
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=NODATA
```

This example will reconcile all the records in which the value of Users.FirstName is `John`, and the values of Users.DeptId and Users.Postal are not specified. You must provide a space in the search criteria if you want to reconcile all records in which no values have been specified.

Example 5:

```
IsFilterApplied=YES
FiltersToBeApplied=Users.FirstName,Users.Sex,Users.Postal
FiltersValues=John,M,1920
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
```

```
Operator=NODATA
```

The value specified for Operator is invalid. As a result of this, no records will be reconciled. The valid values are `AND` or `OR`.

4.3 Multiple Trusted Source Reconciliation

Note:

- At some places in this guide, multiple trusted source is referred to as MTS.

- This connector is MTS-compatible.

In the operating environment of your organization, multiple target systems might act as trusted sources for the various attributes that constitute the employee account. For example, employees' first names and last names might come from one target system, and employees' e-mail addresses might come from another. In such a scenario, you can configure each target system as a trusted source for a specific attribute or set of attributes of the employee accounts. By doing this, you configure multiple trusted source reconciliation, which is a special implementation of trusted source reconciliation.

In another form of multiple trusted source reconciliation, you designate multiple target systems as trusted sources for employees belonging to specific user types.

See Also:

- *Oracle Identity Manager Connector Concepts* for more information

- *Oracle Identity Manager Design Console Guide* for information about implementing multiple trusted source reconciliation

4.4 Guidelines on Using the Connector

Some Asian languages use multibyte character sets. If the character limit for the fields in the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you were using the Japanese language and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

5 Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- Testing Full Reconciliation
- Testing Incremental Reconciliation

5.1 Testing Full Reconciliation

The testing utility allows you to test the functionality of the connector without using Oracle Identity Manager. The testing utility takes as input a text file generated by the target system. This file contains comma-separated values.

To run the testing utility:

1. Open the *OIM_HOME*/XLIntegrations/PSFTER/config/config_Recon.properties file, and specify values for the following properties:
   - FiltersToBeApplied:
   - FiltersValues:
   - IsFilterApplied:
   - Operator:
   - SearchCriteria:
   - CaseSensitive:
   - FilePath:
   - NoOfRecordsToBeReconciled
   - UserType
   - EmployeeType
   - Organization
   - TrustedRO
   - IndexOfLastReconciledRecord
   - RecordDelimiter
   - AppendMode: If the value is `yes`, then the data is added to the end of the file. If the value is `no`, then the data is written from the beginning and the previous contents of the file are overwritten. The default value is `no`.

- DestinationFileName: Specify the file name with path where the text file will be generated.
- DelayBetweenRetries
- NumberOfRetries

2. After you specify the values in the properties file, run the following file.

   For UNIX:

   ```
   OIM_HOME/XLIntegrations/PSFTER/scripts/psftER_Recon.sh
   ```

   For Microsoft Windows:

   ```
   OIM_HOME/XLIntegrations/PSFTER/scripts/psftER_Recon.bat
   ```

3. After the testing utility completes the run, a text file is created in the location specified in the DestinationFileName property. This file contains all the records that satisfy the filter condition, if required.

5.2 Testing Incremental Reconciliation

Testing incremental reconciliation involves verifying that the PeopleSoft listener can reconcile employee data into Oracle Identity Manager. The following sections provide information about this procedure:

- Prerequisites for Testing the PeopleSoft Listener
- Testing the PeopleSoft Listener

5.2.1 Prerequisites for Testing the PeopleSoft Listener

The following are prerequisites for testing the PeopleSoft listener:

- Ensure that the Microsoft Windows scripting engine is installed. This is required to run VBScript files.
- Ensure that the PeopleSoft XML message template is described in the psft_xellerate_msg.xml file, which is in the *OIM_HOME*/XLIntegrations/PSFTER/cbrecon directory.

5.2.2 Testing the PeopleSoft Listener

> **Note:** The procedure described in this section requires a restart of Oracle Identity Manager. After you perform this procedure, you must reverse the change made in the deployment.properties file and then restart Oracle Identity Manager again.

To test the PeopleSoft listener:

1. In the *OIM_HOME*/XLIntegrations/PSFTER/cbrecon/psft-xel-test.vbs file:
   - Modify the value of the ps_server_url variable so that it points to the URL for the PeopleSoft listener.
   - Specify the required PeopleSoft attributes and employee data values in the ExecuteATM function.
2. Run the psft-xel-test.vbs file.

When the script is run, it creates a reconciliation event. Verify that the reconciliation event is created in Oracle Identity Manager and that the event contains the data that you specify in the VBScript file.

If the reconciliation event is successful, then an OIM User account is created or updated containing the values specified in the psft-xel-test.vbs file.

6

Known Issues

The following is a known issue associated with this release of the connector:

Bug 7191933

SSL configuration between the target system and the PeopleSoft listener is not supported if the PeopleSoft listener is deployed on Oracle Application Server.

Index

A

adding custom attributes, 4-11
Application Engine program, creating, 2-15

C

change-based reconciliation, 2-9
configuring
  PeopleSoft Internet Architecture, 2-23
  PeopleSoft listener, 2-9
connector
  installing, 2-7
connector customization, 3-1
connector files and directories
  copying, 2-8
  description, 2-1
  destination directories, 2-8
  installation media file, 2-1
connector testing, 5-1
connector version number, determining, 2-3
creating
  Application Engine program, 2-15
creating scheduled tasks, 4-4
custom attributes, adding, 4-11
customizing connector, 3-1

D

defining
  IT resources, 2-9
  scheduled tasks, 4-4
deployment configurations, 1-2
determining version number of connector, 2-3

E

enabling logging, 2-30

F

files and directories of the connector
  See connector files and directories
full reconciliation, 1-3

G

globalization features, 1-8

I

incremental reconciliation, 1-3
issues, 6-1
IT resources
  defining, 2-9
  parameters, 2-9

L

logging enabling, 2-30

M

managing scheduled tasks, 4-4
modifying scheduled tasks, 4-6
multilanguage support, 1-8

P

parameters of IT resources, 2-9
PeopleSoft Internet Architecture, configuring, 2-23
`PERSONAL_DATA` component, 2-21
problems, 6-1
publishing message, 2-20

R

reconciliation
  trusted source mode, 2-3, 2-8
reconciliation type
  full, 1-3
  incremental, 1-3
requirements for deploying, 1-2

S

scheduled tasks
  defining, 4-4
scheduled tasks, managing, 4-4
scheduled tasks, modifying, 4-6
scheduled tasks, viewing, 4-5
subscribing message, 2-22

supported
    languages, 1-8
    releases of Oracle Identity Manager, 1-2
    target systems, 1-2

T

target systems supported, 1-2
testing, 5-1, 5-2
trusted source reconciliation, 2-3, 2-8

V

version number of connector, determining, 2-3
viewing
    scheduled tasks, 4-5

X

XML files
    description, 2-3, 2-8
    for trusted source reconciliation, 2-3, 2-8