Oracle® Identity Manager

Connector Guide for PeopleSoft User Management

Release 9.1.0

E11206-04

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for PeopleSoft User Management, Release 9.1.0

E11206-04

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

3 Extending the Functionality of the Connector

Preface

This guide provides information about integrating Oracle Identity Manager with PeopleSoft User Management.

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 User Management?

This chapter provides an overview of the updates made to the software and documentation for release 9.1.0.2 of the PeopleSoft User Management connector.

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

- Software Updates

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

- Documentation-Specific Updates

  This section describes major changes made 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 Remote Manager has been added to the connector to support provisioning operations for multiple target systems. Information specific to the connector with the Remote Manager have been added to the relevant sections in this guide. The architecture of the connector with the Remote Manager is described in "Architecture of the Connector With the Remote Manager" on page 1-4.

- New files have been added to the installation media directory for the connector with the Remote Manager. These files are listed in "Files and Directories That Comprise the Connector" on page 2-1.
- 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 2-9.
- The Delete Reconciliation scheduled task has been added to the connector. Through this scheduled task, the data of deleted users is reconciled into Oracle Identity Manager. See "Configuring the Reconciliation Scheduled Tasks" on page 4-6 for more information about this scheduled task and its attributes.
- You can configure SSL connectivity between Oracle Identity Manager and the target system for this release of the connector. However, SSL is not supported for Oracle Application Server. For instructions to configure SSL, see "Postinstallation" on page 2-30.
- Information about the files in which you set the log levels has changed. This information is available in "Enabling Logging" on page 2-31.

Software Updates in Release 9.1.0.1

The following software update has been made in release 9.1.0.1:

- Support for Oracle Identity Manager Release 9.1.0.1

Support for Oracle Identity Manager Release 9.1.0.1

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

Software Updates in Release 9.1.0.2

The following table lists issues resolved in release 9.0.4.2:

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

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 Updated 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 functionality of the connector is described in Chapter 3, "Extending the Functionality of the Connector".

- The architecture of the connector has been included in this guide. This information is provided in "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. The field mappings for lookup field synchronization, target resource reconciliation, and provisioning are described in the following sections, respectively:
  - "Lookup Field Synchronization" on page 1-5
  - "User Fields for Target Resource Reconciliation" on page 1-7
- The reconciliation matching and action rules for target resource reconciliation have been added to the guide. This information is available at the following section:
  - "Target Resource Reconciliation" on page 1-6

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 peopleSoftUMApp.war file into the deployment directory of Oracle WebLogic Server have been modified.

Documentation-Specific Updated in Release 9.1.0.2

The following are documentation-specific updates in release 9.1.0.2:

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

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of resources to various target systems. Oracle Identity Manager Connectors are used to integrate Oracle Identity Manager with target applications. This guide discusses the connector that enables you to use PeopleSoft Enterprise Applications as a managed (target) source of user data for Oracle Identity Manager.

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

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

In the target resource configuration, information about user accounts created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

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

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:

- Roadmap for Deploying and Using the Connector

Note: Information for the connector with the Remote Manager has been included in this guide wherever applicable. You can refer to this information if you use the connector with the Remote Manager.

1.1 Certified Deployment Configurations

Table 1–1 lists the certified deployment configurations.

Table 1–1 Certified Deployment Configurations

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 9.1.0 and later
	If your Oracle Identity Manager installation is running on JDK 1.5, then deploy the connector without the Remote Manager. If your Oracle Identity Manager installation does not run on JDK 1.5, then you must deploy the connector with the Remote Manager. See *Oracle Identity Manager Release Notes* for details about certified JDKs.
Target systems	This release of the connector supports PeopleTools 8.49. **Note:** The connector does not support the association of PeopleSoft CRM users with the EMP ID type.
	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 version of PeopleTools and the target system you are using to check if you are using the combination supported by this connector. To do so, perform the following steps:

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

   `http://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:

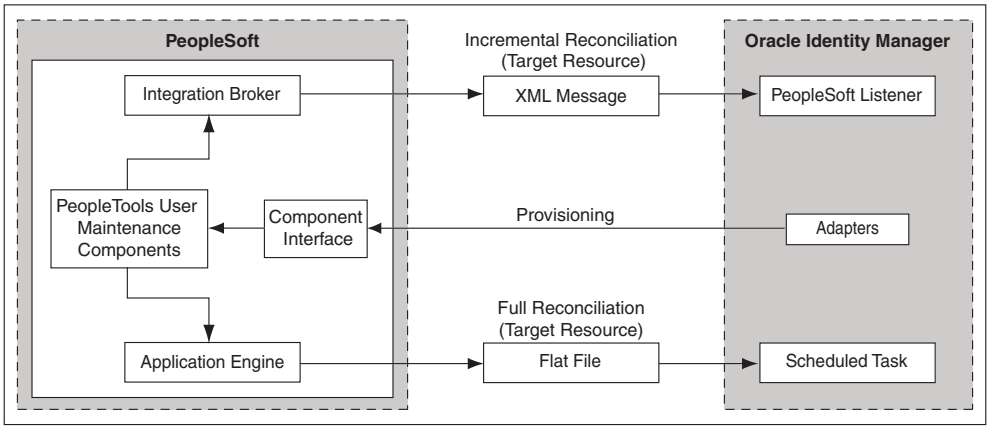
- The "Connector Architecture" section on page 1-3 describes the architecture of the connector.

- If you want to configure the connector for target resource reconciliation and provisioning, then see the following sections:
  - Lookup Field Synchronization
  - Target Resource Reconciliation
  - Provisioning

1.2.1 Connector Architecture

Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of the Connector



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

- Reconciliation
- Provisioning

1.2.1.1 Reconciliation

This connector supports 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 user 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 reconciliation at periodic intervals to ensure that all user records are reconciled into Oracle Identity Manager. "Configuring Full Reconciliation" on page 4-4 describes the procedure to configure full reconciliation.

- **Incremental reconciliation**

Incremental reconciliation involves real-time reconciliation of newly created or modified user 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. "Configuring Incremental Reconciliation" on page 4-13 describes the procedure to configure incremental reconciliation.

Incremental reconciliation involves the following steps:

1. When user 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 user 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 the Oracle Identity Manager host computer.
3. The PeopleSoft listener parses the XML message and sends a reconciliation event to Oracle Identity Manager.

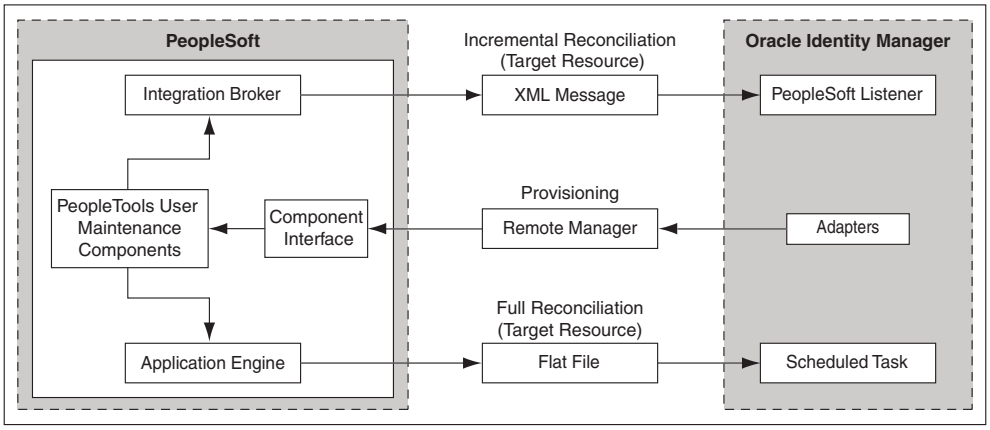
1.2.1.2 Provisioning

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

1.2.1.3 Architecture of the Connector With the Remote Manager

Figure 1–2 shows the architecture of the connector with the Remote Manager.

Figure 1–2 Architecture of the Connector with the Remote Manager



PeopleSoft does not support JDK versions earlier than 1.5. Your Oracle Identity Manager installation might be running on JDK 1.4.2. To make your Oracle Identity Manager installation compatible with the target system, you must use the connector with the Remote Manager. If the Oracle Identity Manager environment does not match the target system environment, then the Remote Manager provides an environment that is compatible for both, in this case, JDK 1.5.

Another reason for using the Remote Manager is that you might be running different versions of the target system in which the target libraries vary between the versions. As a result, the different versions of the API conflict with each other. In this scenario,

the Remote Manager is used to provide individual JVMs, each containing only a single version of the conflicting libraries.

Note: This release of the connector supports only one version, PeopleTools 8.49.

When the connector supports multiple versions of a target system, it must be able to support all versions simultaneously. If this is not possible (for example, because of conflicting target libraries), Oracle recommends that you use the Remote Manager in such a way that each Remote Manager can manage one specific target version.

1.2.2 Lookup Field Synchronization

During a provisioning operation, you use a lookup field to specify a single value from a set of values. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

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

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

Table 1–2 Lookup Fields That Are Synchronized

Lookup Definition	Target System Lookup Field	Synchronization Method
Lookup.PSFTUM.LanguageCode For the connector with the Remote Manager: Lookup.PSFTUM_RM.LanguageCode	LanguageCode	You use the PSFT UM LookUp Reconciliation scheduled task to synchronize this lookup definition. For the connector with the Remote Manager, you use the PSFT UM_RM LookUp Reconciliation scheduled task to synchronize this lookup definition.
Lookup.PSFTUM.CurrencyCode For the connector with the Remote Manager: Lookup.PSFTUM_RM.CurrencyCode	CurrencyCode	You use the PSFT UM LookUp Reconciliation scheduled task to synchronize this lookup definition. For the connector with the Remote Manager, you use the PSFT UM_RM LookUp Reconciliation scheduled task to synchronize this lookup definition.

Table 1–2 (Cont.) Lookup Fields That Are Synchronized

Lookup Definition	Target System Lookup Field	Synchronization Method
Lookup.PSFTUM.PermissionList For the connector with the Remote Manager: Lookup.PSFTUM_RM.PermissionList	PermissionList	You use the PSFT UM LookUp Reconciliation scheduled task to synchronize this lookup definition. For the connector with the Remote Manager, you use the PSFT UM_RM LookUp Reconciliation scheduled task to synchronize this lookup definition.
Lookup.PSFTUM.EmailType For the connector with the Remote Manager: Lookup.PSFTUM_RM.EmailType	EmailTypes	You use the PSFT UM LookUp Reconciliation scheduled task to synchronize this lookup definition. For the connector with the Remote Manager, you use the PSFT UM_RM LookUp Reconciliation scheduled task to synchronize this lookup definition.
Lookup.PSFTUM.Roles For the connector with the Remote Manager: Lookup.PSFTUM_RM.Roles	UserRoles	You use the PSFT UM LookUp Reconciliation scheduled task to synchronize this lookup definition. For the connector with the Remote Manager, you use the PSFT UM_RM LookUp Reconciliation scheduled task to synchronize this lookup definition.

1.2.3 Target Resource Reconciliation

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

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

Note: If you delete a user from the target system, then the data of the deleted user is reconciled into Oracle Identity Manager through the Delete Reconciliation scheduled task.

This section discusses the following topics:

- User Fields for Target Resource Reconciliation
- Reconciliation Rules
- Reconciliation Action Rules

1.2.3.1 User Fields for Target Resource Reconciliation

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

Table 1–3 Fields Used for Target Resource Reconciliation

OIM PeopleSoft UM Resources Process Form Field	Target System Field	Description
Single-Valued Fields		
User Id	PSOPRDEFN.OPRID	Login ID of the user profile This is a mandatory field.
Employee Id	PSOPRDEFN.EMPLID	Employee ID of the employee to which the user profile will be assigned
User Description	PSOPRDEFN.OPRDEFNDESC	Description of the user profile
Multi Language Code	PSOPRDEFN.MULTILANG	Multilanguage code
Language Code	PSOPRDEFN.LANGUAGE_CD	Language code
Currency Code	PSOPRDEFN.CURRENCY_CD	Currency code
User Id Alias	PSOPRDEFN.USERIDALIAS	Alias of user login ID
Row Security Permission List	PSOPRDEFN.ROWSECCLASS	Row security parameter
Process Profile Permission List	PSOPRDEFN.PRCSPRFLCLS	Process profile parameter
Navigator Home Permission List	PSOPRDEFN.DEFAULTNAVHP	Navigator home page address
Primary Permission List	PSOPRDEFN.OPRCLASS	Primary permission list
Primary Email Address	PSUSEREMAIL.EMAILID	E-mail address (primary e-mail account)
Primary Email Type	PSUSEREMAIL.EMAILTYPE	Email type (primary e-mail account)
Multivalued Field		
RoleName	PSROLEUSER_VW.ROLENAME	The role name that is assigned to the user profile
Email Address	PSUSEREMAIL.EMAILID	E-mail address
Email Type **Note:** To specify the e-mail address for an account, you must also specify the e-mail type of that e-mail address.	PSUSEREMAIL.EMAILTYPE	E-mail type

Note: The name of the process form in the first column of the preceding table is UD_PSFT_BAS. For the connector with the Remote manager, the name of this process form is UD_PSFT_RM.

1.2.3.2 Reconciliation Rules

The following are the reconciliation rules for target resource reconciliation:

Rule Name: PSFT UM Target Res rule

Rule Element: User Login Equals Users.Oprid

For the connector with the **Remote Manager**:

Rule Name: PSFT UM Remote Recon Rule

Rule Element: User Login Equals Users.Oprid

In these rules:

- User Login is the User Id field on the OIM User form.
- Users.Oprid is the User Id field of the user profile on the target system.

To access the reconciliation rules:

> **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 UM Target Res rule**. For the connector with the Remote Manager, locate **PSFT UM Remote Recon Rule**.

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

1.2.3.3 Reconciliation Action Rules

Table 1–4 lists the reconciliation action rules for target resource reconciliation:

Table 1–4 Action Rules for Target Resource Reconciliation

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

To access the reconciliation action rules for target resource reconciliation:

> **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_UM_RO** resource object. For the connector with the Remote Manager, locate the **PSFTUM_RM** 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.

1.2.4 Provisioning

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

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

This section discusses the following topics:

- User Provisioning Functions Supported by the Connector
- User Fields for Provisioning

1.2.4.1 User Provisioning Functions Supported by the Connector

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

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

Table 1–5 User Provisioning Functions Supported by the Connector

Function	Adapter
Create a user	adp PSFTUM CREATE USER For the connector with the Remote manager: adp PSFT_RM CREATE USER
Update the password of a user	adp PSFTUM Reset Password For the connector with the Remote Manager: adp PSFT_RM Reset Password
Update the description of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Update the multilanguage code of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Update the primary e-mail address of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Update the primary e-mail address type of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser

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

Function	Adapter
Update the language code of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Update the currency code of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Update the Employee Id of a user	adp PSFTUM Update User EmpId For the connector with the Remote Manager: adp PSFT_RM Update User EmpId
Update the Primary Permission list of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Update the Process Profile Permission list of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Update the Navigator Home Permission list of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Update the Row Security Permission list of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Update the User Id alias of a user	adp PSFTUM UpdateUser For the connector with the Remote Manager: adp PSFT_RM UpdateUser
Add a role to a user	adp PSFTUM addORDeleteRole For the connector with the Remote Manager: adp PSFT_RM addORDeleteRole
Delete a role from a user	adp PSFTUM addORDeleteRole For the connector with the Remote Manager: adp PSFT_RM addORDeleteRole
Add an e-mail address to a user	adp PSFTUM addOrDeleteEmail For the connector with the Remote Manager: adp PSFT_RM addOrDeleteEmail
Delete the e-mail address of a user	adp PSFTUM addOrDeleteEmail For the connector with the Remote Manager: adp PSFT_RM addOrDeleteEmail
Unlock a user	adp PSFTUM UnLock User For the connector with the Remote Manager: adp PSFT_RMUnLock User

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

Function	Adapter
Lock a user	adp PSFTUM Lock User For the connector with the Remote Manager: adp PSFT_RM Lock User
Delete a user at the target system	adp PSFTUM Delete User For the connector with the Remote Manager: adp PSFT_RM Delete User
Prepopulate the User Id on the process form with the User Id of the OIM User **Note:** If the PeopleSoft Employee Reconciliation and the PeopleSoft User Management connectors are deployed on a single Oracle Identity Manager installation, then the User Id field of the OIM User is populated with the value of the Employee Id of the employee reconciled from PeopleSoft.	adp PSFTUM Prepopulate UserID For the connector with the Remote Manager: adp PSFT_RM Prepopulate UserID
Prepopulate the Employee Id on the process form with the User Id of the OIM User **Note:** The Employee Id is used to link a user profile to the employee.	adp PSFTUM Prepopulate EmployeeID UM For the connector with the Remote Manager: adp PSFT_RM Prepopulate EmployeeID UM

1.2.4.2 User Fields for Provisioning

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

Table 1–6 User Fields for Provisioning

OIM PeopleSoft UM Resources Process Form Field	Target System Field	Description	Adapter
Single-Valued Fields			
User Id	PSOPRDEFN.OPRID	Login Id of the user profile	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
User Description	PSOPRDEFN.OPRDEFNDESC	Description of the user profile	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
Employee Id	PSOPRDEFN.EMPLID	Employee Id of the employee to which the user profile will be assigned	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER

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

OIM PeopleSoft UM Resources Process Form Field	Target System Field	Description	Adapter
Multi Language Code	PSOPRDEFN.MULTILANG	Multilanguage code	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
Language Code	PSOPRDEFN.LANGUAGE_CD	Language code	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
Currency Code	PSOPRDEFN.CURRENCY_CD	Currency code	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
User Id Alias	PSOPRDEFN.USERIDALIAS	Alias of user login Id	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
Row Security Permission List	PSOPRDEFN.ROWSECCLASS	Row security parameter	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
Process Profile Permission List	PSOPRDEFN.PRCSPRFLCLS	Process profile parameter	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
Navigator Home Permission List	PSOPRDEFN.DEFAULTNAVHP	Navigator home page address	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER

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

OIM PeopleSoft UM Resources Process Form Field	Target System Field	Description	Adapter
Primary Permission List	PSOPRDEFN.OPRCLASS	Primary permission list	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
Primary Email Address	PSUSEREMAIL.EMAILID	E-mail address (primary e-mail account)	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
Primary Email Type	PSUSEREMAIL.EMAILTYPE	E-mail type (primary e-mail account)	adp PSFTUM CREATE USER For the connector with the Remote Manager: adp PSFT_RM CREATE USER
Multivalued Fields			
RoleName	PSROLEUSER_VW.ROLENAME	The role name that is assigned to the user profile	adp PSFTUM addORDeleteRole For the connector with the Remote Manager: adp PSFT_RM addORDeleteRole
Email Address	PSUSEREMAIL.EMAILID	E-mail address (e-mail account)	adp PSFTUM addOrDeleteEmail For the connector with the Remote Manager: adp PSFT_RM addOrDeleteEmail
Email Type	PSUSEREMAIL.EMAILTYPE	Email type (e-mail account)	adp PSFTUM addOrDeleteEmail For the connector with the Remote Manager: adp PSFT_RM addOrDeleteEmail

Note: (The name of the process form in the first column of the preceding table is UD_PSFT_BAS. For the connector with the Remote manager, the name of this process form is UD_PSFT_RM.

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 Deploying and Using the Connector

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 and Troubleshooting" 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:

- Preinstallation
- Installation
- Postinstallation

This chapter provides information about each stage of connector deployment.

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
configuration/PeopleSoft User Management-CI.xml For the connector with the Remote Manager: configuration/PeopleSoft User ManagementRM-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/PSFTUMReconciliation.jar	This JAR file contains the class files that are used to implement full reconciliation.
lib/PSFTUMProvisioning.jar For the connector with the Remote Manager: lib/PSFTUM_RMProvisioning.jar	This JAR file contains the class files that are required for provisioning.

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

File in the Installation Media Directory	Description
lib/PSFTUM_RMProvisioning.ear	This EAR file is used for running the testing utility for provisioning on IBM WebSphere Application Server.
lib/peopleSoftUMApp.war	This Web Archive (WAR) file contains the classes and configuration files required to implement incremental reconciliation.
The following files in the peoplecode directory: CurrencyCode.txt EmailType.txt LanguageCode.txt PermissionList.txt UserRoles.txt	These files contain the PeopleCode for the steps that you define for the Application Engine program. This is explained in "Creating the Application Engine Program" on page 2-19.
peoplecode/UserMgmtCBRecon_8.49.txt peoplecode/UserMgmtBulkRecon_8.49.txt peoplecode/DeleteUsrProfileCBRecon_8.49.txt	These files contain the code that you must add to the PeopleCode for the SavePostChange event while performing the procedure described in "Publishing the Messages" on page 2-23.
test/cbrecon/psft-xel-test.vbs	You can use this VBScript file to test the incremental reconciliation functionality of the connector. This file creates a dummy XML message similar to the ones created by PeopleSoft Enterprise Applications when a user account is created or modified in the target system. For information about testing incremental reconciliation, see "Testing Incremental Reconciliation" on page 5-2.
test/cbrecon/psft-del-xel-test.vbs	You can use this VBScript file to test the delete reconciliation functionality during incremental reconciliation. This file creates a dummy XML message similar to the ones created by PeopleSoft Enterprise Applications when a user is deleted from 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 used by the psft-xel-test.vbs file to communicate with the connector by using XML over HTTP.
test/cbrecon/USR_MGMT_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 when a user is created or modified on the target system.
test/cbrecon/USR_DEL_MSG.xml	This XML file is used by the psft-del_xel-test.vbs file to define the template of the XML message that is received from the target system when a user is deleted from the target system.
test/config/config.properties	This file is used to specify the parameters and settings required to connect, create, update, and delete users in the target system by using the testing utility for provisioning.
test/config/config_Recon.properties	This file is used to specify the parameters required to perform a reconciliation run. This file stores the scheduled task attributes and the IT resource parameters.

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

File in the Installation Media Directory	Description
test/config/attribute_prov.properties **Note:** This file is used only for the connector without the Remote Manager.	This file stores the attribute mappings used during provisioning. This file is used by the testing utility.
test/config/attributeMap_Recon.properties	This file stores the attribute mappings used during reconciliation. This file is used by the testing utility.
test/config/attributeChildMap_Recon.properties	This file stores the attribute mappings used during reconciliation for child tables. This file is used by the testing utility.
test/config/log.properties	This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility.
test/scripts/psftUM.bat test/scripts/psftUM.sh For the connector with the Remote Manager: test/scripts/psftUM_RM.bat test/scripts/psftUM_RM.sh	The BAT file or UNIX shell script calls the testing utility for provisioning.
For the connector with the Remote Manager: test/scripts/was_psftUM_RM.bat test/scripts/was_psftUM_RM.sh	This batch file or shell script is used to run the testing utility for provisioning running on IBM WebSphere Application Server.
For the connector with the Remote Manager: test/scripts/wasBasecp.bat test/scripts/wasBasecp.sh	This batch file or shell script is used by was_psftUM_RM.bat or was_psftUM_RM.sh for setting the classpath.
test/scripts/psftUM_Recon.bat test/scripts/psftUM_Recon.sh	The BAT file or UNIX shell script calls the testing utility for reconciliation.
The files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied into the following directory: *OIM_HOME*/connectorResources **Note:** A resource bundle is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
xml/PSFTUM-ConnectorConfig.xml For the connector with the Remote Manager: xml/PSFTUM_RM-ConnectorConfig.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ Scheduled tasks ■ IT resource ■ Resource objects (this file contains the configurations of the resource objects for the target resource) ■ Process definition ■ Process tasks ■ Adapters ■ Process form

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

File in the Installation Media Directory	Description
For the connector with the Remote Manager: config/attribute_RMprov.properties	This properties file contains the attribute mappings used during provisioning if you are using the connector with the Remote Manager.

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/ScheduleTask/PSFTUMReconciliation.jar

2. Open the manifest.mf file in a text editor. The manifest.mf file is one of the files bundled inside the PSFTUMReconciliation.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 the flat file generation. 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 Definition Security for a Group
- 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, `OIMUM`, and then click **Add**.
4. On the General tab, enter a description for the permission list in the **Description** field.
5. On the Component Interfaces tab, click the search icon for the Name field and perform the following:
   a. In the Name lookup, enter `USER_PROFILE` and then click **Lookup**. From the list, select **USER_PROFILE**. The application returns to the Component Interfaces tab. Click the **Edit** link.
   b. On the Component Interface 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 **Name** field and repeat Steps a through c for the DELETE_USER_PROFILE component interface.
6. On the Pages tab, click the search icon for Menu Name and perform the following:
   a. In the Menu Name lookup, enter `APPLICATION_ENGINE` and then click **Lookup**. From the list, select **APPLICATION_ENGINE**. The application returns to the Pages tab. Click 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.

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

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

   - App Engine Program
   - Message
   - Component
   - Project

9. Click **OK**.

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

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

12. On the Process tab, click the **Process Group Permissions** link. The Process Group Permission page is displayed.

13. In the Process Group lookup, click the search icon. From the list, select **TLSALL**. The application will return to the Process Group Permission page.

14. Click on the plus sign (+) to add another row for **Process Group**.

15. In the Process Group lookup, click the search icon. From the list, select **STALL**. The application will return to the Process Group Permission page.

16. Click **OK**.

17. 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 Definition Security for a Group

For the USERMAINT and PURGE_USR_PROFILE components, you must create a definition security for a group. To do so:

1. Log in to the Application Designer in 2 tier mode with administrator credentials.
2. On the Go tab, select Definition Security.
3. On the PS Definition Security page, click **File** and then click **New Group**.
4. On the window that is displayed, select **Components** from the list.
5. From the Excluded Components list on the right side, select **USERMAINT** and **PURGE_USR_PROFILE**, and then click the left arrow button. This will add these components for your group.
6. From the File menu, click **Save As** and save this group as **OIMUM**.
7. From the File menu, click **Open** and then click **Permission List**. All the existing permission lists are displayed.
8. Select **OIMUM** as the permission list and click **OK**. Details of the permission list along with the groups are displayed on the right side in the Excluded Group ID list.
9. From the list, select the group that you created in Step 6. Click the left arrow to include this group in your permission list.
10. From the File menu, click **Save**.

2.1.2.1.3 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, `OIMUM`, and then click **Add**.
4. On the General tab, enter a description for the role in the **Description** field.
5. On the Permission Lists tab, click the search icon and perform the following:

   a. In the Permission Lists lookup, enter `OIMUM` and then click **Lookup**. From the list, select **OIMUM**.

   b. Click **Save**.

2.1.2.1.4 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, `OIMUM`, and then click **Add**.
4. On the General tab, perform the following:
   a. From the Symbolic ID list, select the value that is displayed, for example, SYSADM1.
   b. Enter valid values for the **Password** and **Confirm Password** fields.
   c. Click the search icon for the Process Profile permission list.
   d. In the Process Profile lookup, enter `OIMUM` and then click **Lookup**. From the list, select **OIMUM**. The application returns to the General tab.
5. On the ID tab, select **none** as the value of the ID type.
6. On the Roles tab, click the search icon and perform the following:
   a. In the Roles lookup, enter `OIMUM` and then click **Lookup**. From the list, select **OIMUM**.
   b. Click on the plus sign (+) to add another row.
   c. In the Roles lookup, enter `ProcessSchedulerAdmin` and then click **Lookup**. From the list, select **ProcessSchedulerAdmin**.
   d. Click **Save** to save this user profile. This user profile is used by Oracle Identity Manager as an admin user in the IT resource to enable the connector to perform provisioning operations. This user profile is also 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

- Deploying the PeopleSoft Listener

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 User Management 9.1.0** from the **Connector List** list.

  For the connector with the Remote Manager, select **PeopleSoft User Management RM 9.1.0** from the list.

  Note: The connector with the Remote Manager and the connector without the Remote Manager can exist together in a single deployment environment. If you want to support multiple versions of the target system, then you can deploy the connector with the Remote Manager along with the connector without the Remote Manager.

  If you have copied the installation files into a different directory, then:

  1. In the **Alternative Directory** field, enter the full path and name of that directory.
  2. To repopulate the list of connectors in the Connector List list, click **Refresh**.
  3. From the **Connector List** list, select the connector that you want to install.

- Perform Steps 1 through 5 of that procedure. When you reach Step 6 of that procedure, see "Configuring the IT Resource" on page 2-11 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/PSFTUMProvisioning.jar	*OIM_HOME*/JavaTasks
For the connector with the Remote Manager: lib/PSFTUM_RMProvisioning.jar	*OIM_HOME*/JavaTasks
lib/PSFTUMReconciliation.jar	*OIM_HOME*/ScheduleTask

Table 2–2 (Cont.) Files Copied to Oracle Identity Manager

File in the Installation Media Directory	Destination Directory
Files in the resources directory	*OIM_HOME*/connectorResources

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 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
lib/peopleSoftUMApp.war	*OIM_HOME*/cbrecon_webapp/lib
For the connector with the Remote Manager: lib/PSFTUM_RMProvisioning.jar	*RM_HOME*/JavaTasks
Files in the peoplecode directory	*OIM_HOME*/XLIntegrations/PSFTUM/peoplecode
Files in the test/cbrecon directory	*OIM_HOME*/XLIntegrations/PSFTUM/cbrecon
Files in the test/scripts directory	*OIM_HOME*/XLIntegrations/PSFTUM/scripts
Files in the test/config directory	*OIM_HOME*/XLIntegrations/PSFTUM/config
For the connector with the Remote Manager: Files in the config directory	*RM_HOME*/XLIntegrations/PSFTUM/config
For the connector with the Remote Manager and if your Oracle Identity Manager installation is running on IBM WebSphere Application Server: lib/PSFTUM_RMProvisioning.ear	*OIM_HOME*/JavaTasks

After you copy the connector files, copy the following files from the *PEOPLESOFT_HOME*/web/psjoa directory on the target system computer into the *OIM_HOME*/ThirdParty directory and into the *RM_HOME*/JavaTasks directory for the connector with the Remote Manager.

- psjoa.jar

  This is the PeopleSoft Java object adapter file containing the compiled Java classes required by Oracle Identity Manager to remotely connect to the target system.

- peoplesoft.jar

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

  The "Configuring the Target System for Provisioning" section on page 2-28 provides information about the procedure to generate this file for the specific release of PeopleTools (8.49) that you are using.

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

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 provisioning and reconciliation.

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

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `PSFT UM Server` 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:

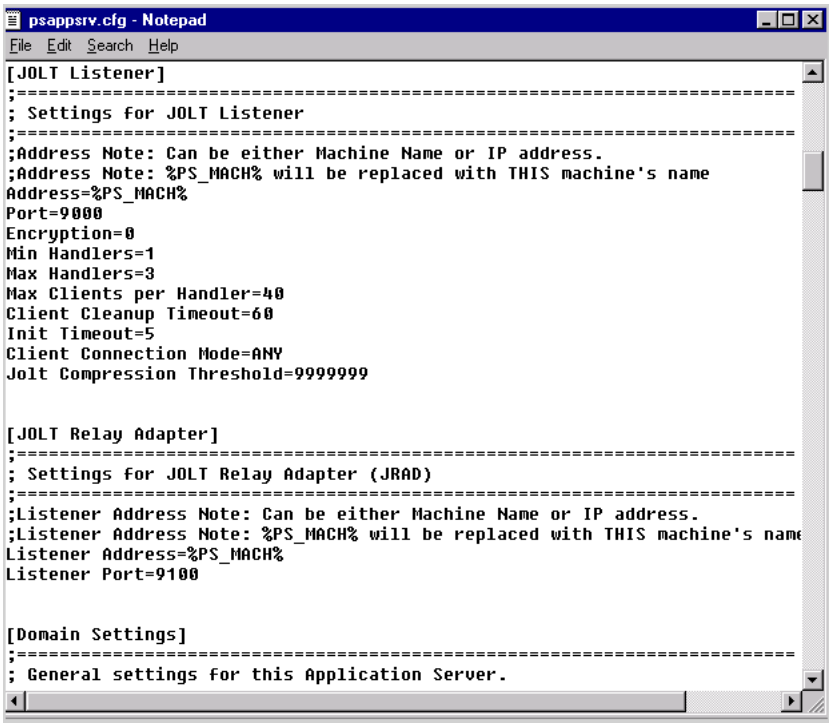
Table 2–4 Parameters of the IT Resource for the Target System

Parameter	Description
Admin	User ID of the PeopleSoft Enterprise Applications limited rights user profile. Oracle Identity Manager uses this target system account to connect to and exchange data with the target system. Sample value: `OIMUM`
AdminCredentials	Enter the password of the PeopleSoft Enterprise Applications administrator.
AttributeMapLookUpForProv **Note:** This parameter is used only in the connector without the Remote Manager.	This parameter holds the name of the lookup definition containing attribute field mappings between Oracle Identity Manager and the target system. This mapping information is used during provisioning. Default value: `Lookup.PSFTUM.Attr.Map.Prov` **Note:** You must not change the value of this parameter.

Table 2–4 (Cont.) Parameters of the IT Resource for the Target System

Parameter	Description
ComponentInterfaceName	Component interface used to load user data in PeopleSoft Enterprise Applications Default value: `USER_PROFILE`
ServerName	Enter the IP address or host name of the computer hosting the PeopleSoft application server. Sample value: `ServerName = 172.21.109.48`
ServerPort	JOLT Listener port: BEA JOLT acts as the communication layer between the Web server and the application server installed on the target system. Default value: `9000` **Note:** The JOLT Port can be determined by either using the PSADMIN utility or by locating the Port parameter in the JOLT Listener section in the psappsrv.cfg file. Figure 2–1 shows the psappsrv.cfg file.
IsSecure	This parameter is deprecated in the current release. Modifying the values for this parameter will not affect the functionality of the connector.
SymbolicId	Enter the AccessId associated with the PeopleSoft Enterprise Applications limited rights user profile. The AccessId specifies whether or not the user has sufficient privileges on the PeopleSoft Enterprise Applications database. Sample value: `SYSADM1`
NumberOfRetries	Enter the number of times Oracle Identity Manager must try connecting to the target system before the `InvocationTargetException` error is thrown. Default value: `2` **Note:** The timeout feature is enabled only for full reconciliation and provisioning. It is not applied during incremental reconciliation.
DelayBetweenRetries	Use this parameter to specify the time difference (in milliseconds) between consecutive retries. Default value: `20000`
RecordName	Use this parameter to add the Employee ID for a new user profile or update the Employee ID for an existing a user profile. Default value: `PERSONAL_DATA`
UnsupportedCharacters	List of characters or strings that are not supported by PeopleSoft in the value specified for any user profile field Default value: `,##;## ##:##&##(##)##\##[##]##/##<##>##PPLSOFT` These characters are separated by ## (two number sign characters).
PIAServerName	Enter the IP address or host name of the computer hosting the PeopleSoft Internet Architecture. **Note:** The IP address or the host name must be followed by the port number on which PeopleSoft Internet Architecture is running. Sample value: `172.21.109.48:90`

Figure 2–1 PSAPPSRV.CFG File



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

> **Note:** The procedure to configure the IT resource for the connector with the Remote Manager is described later in this chapter.

2.2.1.4 Deploying the PeopleSoft Listener

To deploy the PeopleSoft Listener:

1. Copy the *OIM_HOME*/cbrecon_webapp/lib/peopleSoftUMApp.war file into a temporary directory. Enter the following command to extract the contents of the peopleSoftUMApp.war file.

   ```
   jar -xvf peopleSoftUMApp.war
   ```

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

2. Edit the deployment.properties file. This file contains the message property that corresponds to the name of the XML message sent by the target system. The default value of this property is `USR_MGMT_MSG`.
3. 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`.
4. 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:host:2809`
  - JBoss Application Server: `jnp://localhost:1099`
  - Oracle Application Server: `ormi://localhost:12401/Xellerate`

5. Edit the following properties in the configureReconciliation.properties file:
   - **reconciliationMode:** Use this property to specify the mode of reconciliation that you want to use. Set value of this property to `target`.
   - **ITResourceType**: Use this property to fetch IT Resource instances. The default value is `PSFT UM`. For the connector with the Remote Manager, this value is `PSFTUM_RM`. The XML message generated by PeopleSoft contains the IP and the PORT of the computer on which the message is generated.

     Note: This information is compared against all the IT resources that match the value you provide for this property. The PIAServerName attribute is compared with the PeopleSoft IP. The value of the PIAServerName attribute must be in the following format:

     `PIA_SRVR_IP_ADDRESS``:`*`PIA_PORT`*

     For example, 172.21.109.62:90

   - **ReconcilingRO:** Use this property to specify the name of the resource object used for reconciliation:

     `ReconcilingRO=PSFT_UM_RO` (by default)

     For the connector with the Remote Manager:

     `ReconcilingRO=PSFTUM_RM`

- **PIA_IP**: Use this property to specify the Xpath to fetch the IP address of the target system, which generates the XML message. The default value is `//Transaction/PSOPRDEFN/PIA_IP`.

  Note: XPath describes how to locate specific elements in a document. It allows you to locate specific content within an XML document. XPATH treats an XML document as a logical ordered tree.

- **PIA_PORT**: Use this property to specify the Xpath to fetch the port on which PeopleSoft Internet Architecture is running. The default value is `//Transaction/PSOPRDEFN/PIA_PORT`.
- **DEL_USER_OPRID**: Use this property to specify the Xpath to fetch the deleted User ID. The default value is `//Transaction/PRG_USR_PROFILE/OPERID`.
- **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.OPRID,Users.DESCRIPTION`, and `FiltersValues = SFCA001, This is a, test`

  In this scenario, you have entered the value of `Users.DESCRIPTION` as `"This is a, test"`. The reconciliation engine will consider it as two different values, `"This is a"`, and `"test"`. 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.OPRID 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.OPRID 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.Name=`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.

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

   Note: Before you copy these files from the *OIM_HOME*/lib directory, check if these files exist in the WEB-INF/lib directory. 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)

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

- peoplesoft.jar
- psjoa.jar

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

```
jar -cvf  peopleSoftUMApp.war .
```

8. Ensure that the old version of the peopleSoftUMApp.war file is deleted from the application server deployment directory.
9. Deploy the newly created peopleSoftUMApp.war file in 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 `peopleSoftUMApp`.
   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. In the Context root field, enter peopleSoftUMApp.

f. Click **Next**.

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

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

i. On the Map virtual hosts page, select **peopleSoftUMApp.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 **peopleSoftUMApp** 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 **peopleSoftUMApp**.

h. Click **Next**.

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

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

10. 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 3-2 for information about the procedure to add new fields for incremental reconciliation.

2.2.2 Installation on the Target System

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

- Configuring the Target System for Full Reconciliation
- Configuring the Target System for Incremental Reconciliation
- Configuring the Target System for Provisioning
- Installing the Remote Manager
- Enabling Logging in the Remote Manager
- Enabling Client-Side Authentication for the Remote Manager

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 user data through the USERMAINT and PURGE_USR_PROFILE components.

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

- Creating the Application Engine Program

  This is a one-time procedure.

- 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 The Application Engine program populates a flat file with user 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 `BLKRecon`.
6. Click **Action** in the **Insert** menu. An action is added to the BLKRecon step.
7. Select **PeopleCode** from the list for the new action.
8. Click **Save** in the **File** menu, and save the Application Engine program as BLKPRCS_USER.
9. Double-click the **PeopleCode** action. A new PeopleCode window is displayed.
10. Copy the code from the *OIM_HOME*/XLIntegrations/PSFTUM/peoplecode/UserMgmtBulkRecon_8.49.txt file into the PeopleCode window.

    Note: You must create the BLKRecon step before creating the other steps. This will help you set the delimiter value only once in the code. Otherwise, the delimiter value will be set to "*"(asterisk) by default.

11. Change the path to a directory location on the PeopleSoft server as follows:

    ```
    &DataFile = GetFile("path where you want to generate the comma-separated flat
    file\BulkRecon.txt", "w", %FilePath_Absolute);
    &LOGFile = GetFile("path where you want to generate the comma-separated flat
    file\BulkRecon.log", "w", "a", %FilePath_Absolute);
    ```

    For example:

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

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

Step Name	File Containing the Required PeopleCode
`language`	LanguageCode.txt
`Currency`	CurrencyCode.txt
`userrole`	UserRoles.txt
`permiss`	PermissionList.txt
`EmailType`	EmailType.txt
`BLKRecon` (already created in Step 5.)	UserMgmtBulkRecon_8.49.txt

15. 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_USER as the name of the Application Engine program.

   See Also: "Configuring the Target System for Full Reconciliation" on page 2-19 for the procedure to create and run an 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.

Note: For this connector, two messages must be created, USR_MGMT_MSG, and OIM_DEL_MESSAGE. USR_MGMT_MSG contains information of user accounts that are created or modified. OIM_DEL_MESSAGE contains information of user accounts that are deleted.

The two separate messages are created because USR_MGMT_MSG contains all information about a user account. However, when a user account is deleted, only OPRID of the user is required to be sent to Oracle Identity Manager.

After messages are created and associated with their respective queues, 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.

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

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

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

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

---

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_UM_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 Add a New Value tab, enter USR_MGMT_MSG as the message name `VERSION_1` or `v1` as the version.
4. Click **Add**.
5. On the Message Definition tab, select **Nonrowset-based** as the message type.
6. Click **Save** to save the changes.
7. Repeat Steps 1 through 5 to create the OIM_DEL_MESSAGE message.

2.2.2.2.3 Publishing the Messages To publish messages:

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 `USERMAINT` in the **Name Selection Criteria** field, and then click **Enter**. All component names starting with the text USERMAINT are displayed.

4. Select **USERMAINT** from the list, and then click **Open**. The details of the USERMAINT component are displayed.
5. Click the **Structure** tab, right-click **USERMAINT**, and then select **View PeopleCode**. The PeopleCode for the USERMAINT 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. Copy the code given in the following file and paste it after the import definitions in the PeopleCode for the SavePostChange event:

   OIM_HOME/XLIntegrations/PSFTUM/peopleCode/UserMgmtCBRecon_8.49.txt

   Note: While creating the message by following the procedures described in the "Creating the Messages" section on page 2-23, if you change the name of the message to something other than USR_MGMT_MSG, then you must use the same name in the code that you copy.

8. Add the following function call at the end of the PeopleCode for the SavePostChange event:

   Note: Perform this step only after you copy the code from the text file.

```
/**********************************************************************/
/* Calling the GENERATEUSER function to generate the
USR_MGMT_MSG message*/
/**********************************************************************/
If Len(%CompIntfcName) = 0 Then
Local string &OPID;
&OPID = PSOPRDEFN.OPRID;
&s_ipadd = %Request.ServerName;
&n_port = %Request.ServerPort;
GENERATEUSR(&OPID);
End-If;
```

9. From the File menu, click **Save** to save the changes to the USERMAINT component.
10. Repeat Steps 1 through 6 for the PURGE_USR_PROFILE component, and then perform the following:
    a. Copy the code given in the following file and paste it in the PeopleCode for the SavePostChange event:

       OIM_HOME/XLIntegrations/PSFTUM/peopleCode/DeleteUsrProfileCBRecon_8.49.txt

       Note: While creating the message by following the procedures described in the "Creating the Messages" section on page 2-23, if you change the name of the message to something other than OIM_DEL_MESSAGE, then you must use the same name in the code that you copy.

b. Add the following function call at the end of the PeopleCode for the SavePostChange event:

Note: Perform this step only after you copy the code from the text file.

```
/*********************************************************************/
/* Calling the DELETEUSR function to generate the
OIM_DEL_MESSAGE message*/
/*********************************************************************/
If Len(%CompIntfcName) = 0 Then
Local string &OPID;
&OPID = PSOPRDEFN.OPRID;
&s_ipadd = %Request.ServerName;
&n_port = %Request.ServerPort;
DELETEUSR(&OPID);
End-If;
```

c. From the File menu, click **Save** to save the changes to the PURGE_USR_PROFILE component.

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

- 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://servername/psp/ps/Databasename/?cmd=login`

   For example:

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

2. To display the Gateway component details, 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 host name 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://computer_name_of_the_PeopleSoft_Web_server or IP_address:port/PSIGW/PeopleSoftListeningConnector`

   For example:

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

5. To load all target connectors that are registered with the LOCAL gateway, click **Load Gateway Connectors**. A window is displayed mentioning that the loading process is successful. Click **OK**.
6. Click **Save**.
7. Click **Ping Gateway** to check 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_UM_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://*computer_name_of_OIM_SERVER or IP address:port*/peopleSoftUMApp/do/peopleSoftUM

      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/peopleSoftUMApp/do/peopleSoftUM

      For IBM WebSphere Application Server:

      http://10.121.16.42:9080/peopleSoftUMApp/do/peopleSoftUM

      For JBoss Application Server:

      http://10.121.16.42:8080/peopleSoftUMApp/do/peopleSoftUM

      For Oracle Application Server:

      http://10.121.16.42/peopleSoftUMApp/do/peopleSoftUM

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

`https://COMMON_NAME:PORT/peopleSoftUMApp/do/peopleSoftUM`

For Oracle WebLogic Server:

`https://example088196:7002/peopleSoftUMApp/do/peopleSoftUM`

For IBM WebSphere Application Server:

`https://example088196:9443/peopleSoftUMApp/do/peopleSoftUM`

For JBoss Application Server:

`https://example088196:8443/peopleSoftUMApp/do/peopleSoftUM`

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

h. Click **Ping Node** 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, for example, `OIM_UM_SERVICE`, and then click **Add**.

c. On the Service Definition tab, enter a description for the service in the **Description** field.

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

3. Create a service operation by performing the following steps:

a. In PeopleSoft Internet Architecture, 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 messages you created in Step 2 of the "Creating the Messages" section on page 2-23, for example, `USR_MGMT_MSG` and `OIM_DEL_MESSAGE`.

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 `USR_MGMT_MSG.VERSION_1` in the **Message.Version** field and `OIM_UM_QUEUE` in the **Queue Name** field.

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

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

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

Sender Node: `PSFT_HR`

Receiver Node: `OIM_UM_NODE`

Service Operation: USR_MGMT_MSG

h. Add another routing definition for OIM_DEL_MESSAGE and enter the following:

Sender Node: PSFT_HR

Receiver Node: OIM_UM_NODE

Service Operation: OIM_DEL_MESSAGE

Note: PSFT_HR is the default local node for PeopleSoft HCM applications. If you are using other PeopleSoft applications, verify the default local node by using the procedure described in Step 1a. For example, if you are using PeopleSoft CRM applications, then the default local node is PSFT_CR.

---

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

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 2-23 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 the Oracle Identity Manager server.

2.2.2.3 Configuring the Target System for Provisioning

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

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

   All the component interfaces with names that start with USER_PROFILE are displayed in the Open Definition dialog box.
5. Select the **USER_PROFILE** entry, and then click **Open.**
6. Click **Yes** in the message that is displayed. The properties of the USER_PROFILE component interface are displayed.

7. In the window for the USER_PROFILE component interface, select **PeopleSoft APIs** from the **Build** menu. The Build PeopleSoft API Bindings dialog box is displayed.
8. In the Java Classes region, select **Build**.
9. From the **Select APIs to Build** list, select **CompIntfc.CompIntfcPropertyInfo**, **CompIntfc.CompIntfcPropertyInfoCollection**, **CompIntfc.DELETE_USER_PROFILE**, **CompIntfc.DELETE_USER_PROFILECollection**, and the APIs with names that start with **CompIntfc.USER_PROFILE**.
10. In the **Target Directory** field, specify the path of the directory in which you want the Java API classes to be created, and then click **OK.**
11. Ensure that the psjoa.jar file is included in the CLASSPATH environment variable. This file is located in the *PEOPLESOFT_HOME*/web/psjoa directory.
12. Compile the APIs from the target directory specified in the preceding step. To do so:
    a. Specify the JAVA_HOME environment variable.
    b. In the command prompt, run the following command in the directory that you specified in Step 10 of this procedure:

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

13. Bundle the compiled class files in a JAR named peoplesoft.jar as follows:

    jar -cvf peoplesoft.jar PeopleSoft/Generated/CompIntfc/*.class

2.2.2.4 Installing the Remote Manager

Note: Ensure that the Remote Manager is installed on JRE version 1.5.x. By default, the Remote Manager uses bundled JRE version 1.4.2_11.

In this guide, the directory in which you install the Remote Manager is referred to as *RM_HOME*.

The procedures to configure the Remote Manager are described in "Configuring the Remote Manager" on page 2-45.

To install the Remote Manager:

1. The Remote Manager installation files are shipped along with the Oracle Identity Manager installation files. Depending on the application server that you use, perform the procedure to install the Remote Manager on the target system computer by following the instructions given in one of the following guides:
   - *Oracle Identity Manager Installation and Configuration Guide for Oracle WebLogic Server*
   - *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*
   - *Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server*
   - *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*

2. Copy the following JAR files into the *RM_HOME*/JavaTasks directory:
   - *OIM_HOME*/lib/xlVO.jar
   - *OIM_HOME*/lib/xlAPI.jar

2.2.2.5 Enabling Logging in the Remote Manager

To enable logging in the Remote Manager:

1. Add the following lines in the *RM_HOME*/config/log.properties file:

   ```
   log4j.logger.OIMCP.PSFTUM=LOG_LEVEL
   ```

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

   For example:

   ```
   log4j.logger.OIMCP.PSFTUM=DEBUG
   ```

After you enable logging, when you start using the connector, the log information is written to the file whose name and location you specify in the log.properties file.

2.2.2.6 Enabling Client-Side Authentication for the Remote Manager

To enable client-side authentication for the Remote Manager:

1. Open the *RM_HOME*/xlremote/config/xlconfig.xml file in a text editor.
2. Set the ClientAuth property to `true` as follows:

   ```
   <ClientAuth>true</ClientAuth>
   ```

3. Ensure that the RMIOverSSL property is set to true as follows:

   ```
   <RMIOverSSL>true</RMIOverSSL>
   ```

4. Perform Steps 2 through 3 in the *OIM_HOME*/config/xlconfig.xml file.

2.3 Postinstallation

Postinstallation information is divided across the following sections:

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

2.3.1 Postinstallation on Oracle Identity Manager

Postinstallation on Oracle Identity Manager consists of the following procedures:

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

- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging
- Configuring SSL

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

While you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/connectorResources directory. Whenever you add a new resource bundle in the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

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

   OIM_HOME/bin/*script_file_name*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

   OIM_HOME/config/xlconfig.xml

2.3.1.2 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=DIRECTORY_PATH/xel.log
       #log4j.appender.logfile.MaxBackupIndex=20
       #log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
       #log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
       ```

  2. Specify the name and the location of the file to which the preceding logs 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.PSFTUM=log_level
     ```

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

     For example:

     ```
     log4j.logger.OIMCP.PSFTUM=DEBUG
     ```

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

  ```
  DIRECTORY_PATH/xel.log
  ```

- **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=DIRECTORY_PATH/xel.log
#log4j.appender.logfile.MaxBackupIndex=20
#log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
#log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
```

2. Specify the name and the location of the file to which the preceding logs 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.PSFTUM=log_level
   ```

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

   For example:

   ```
   log4j.logger.OIMCP.PSFTUM=DEBUG
   ```

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

```
DIRECTORY_PATH/xel.log
```

- **JBoss Application Server**

  To enable logging:

  1. In the *OIM_HOME*/config/log.properties file, add the following lines:

     ```
     <category name="OIMCP.PSFTUM">
        <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.PSFTUM">
        <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.PSFTUM=log_level
     ```

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

     For example:

     ```
     log4j.logger.OIMCP.PSFTUM=DEBUG
     ```

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

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

2.3.1.3 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

2.3.1.3.1 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 2-34, 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 2-36, 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 2-36, 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.

2.3.1.3.2 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.

2.3.1.3.3 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 Runtime Environment is installed on the JBoss Application Server host

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

- Creating 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 2-34.

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 2-34.
- 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 procedures:

- Configuring SSL
- Installing the Remote Manager

2.3.2.1 Configuring SSL

To configure SSL on the target system:

1. Copy the certificate to the computer on which PeopleSoft Enterprise Applications is installed.

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

2. Run the following command:

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

3. When prompted, enter the current keystore password.
4. When prompted, enter the alias of the certificate that you imported while performing the application server specific procedures listed in "Configuring SSL" on page 2-34.

   Note: The alias must be the same as the one created when the keystore was generated.

   If you are using IBM WebSphere Application Server, then enter `root` as the alias.

5. When prompted, enter the full path and name of the certificate and press **Enter**.

   Note: If you are using IBM WebSphere Application Server, then enter the path of the root certificate.

6. When prompted for the following:

   ```
   Trust this certificate? [no]: yes
   ```

   Select `yes` and press **Enter**.

7. Restart the Web server of the target system.

2.3.3 Configuring the Remote Manager

This section discusses the following topics:

- Configuring the IT Resource for the Connector with the Remote Manager
- Configuring Oracle Identity Manager to Trust the Remote Manager
- Verifying That the Remote Manager Is Running

2.3.3.1 Configuring the IT Resource for the Connector with the Remote Manager

The IT resource for the connector with the Remote Manager contains connection information about the Remote Manager. Oracle Identity Manager uses this information during provisioning.

When you deploy the connector with the Remote Manager, two IT resource instances, PSFTUM_849_RM and PSFT_RM_849, are automatically created in Oracle Identity Manager.

The PSFTUM_849_RM IT resource instance contains the following fields:

- service name

  Sample value: `ServiceName= RManager`

- url

  The syntax of the url is: rmi://*REMOTE_MANGER_HOST*:*BINDING_PORT*

  Sample value: `url = rmi://172.21.109.95:12346`

  The service name and the binding port of the url are available in the *RM_HOME*/config/xlconfig.xml file.

You must specify values for the parameters of the PSFT_RM_849 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 `PSFTUM_RM_849` 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 2–5 describes each parameter:

Table 2–5 Parameters of the IT Resource for the Connector with the Remote Manager

Parameter	Description
Admin	User ID of the PeopleSoft Enterprise Applications limited rights user profile. Oracle Identity Manager uses this target system account to connect to and exchange data with the target system. Sample value: `OIMUM`
AdminCredentials	Enter the password of the PeopleSoft Enterprise Applications administrator.
ComponentInterfaceName	Component interface used to load user data in PeopleSoft Enterprise Applications Default value: `USER_PROFILE`
ServerName	Enter the IP address or host name of the computer hosting the PeopleSoft application server. Note: The IP address or the host name must be followed by the port number on which PeopleSoft Internet Architecture is running. Sample value: `ServerName = 172.21.109.48:90`
ServerPort	JOLT Listener port: BEA JOLT acts as the communication layer between the Web server and the application server installed on the target system. Default value: `9000`
IsSecure	This parameter is deprecated in the current release. Modifying the values for this parameter will not affect the functionality of the connector.
SymbolicId	Enter the AccessId associated with the PeopleSoft Enterprise Applications limited rights user profile. The AccessId specifies whether or not the limited rights user has sufficient privileges on the PeopleSoft Enterprise Applications database. Sample value: `SYSADM1`

Table 2–5 (Cont.) Parameters of the IT Resource for the Connector with the Remote Manager

Parameter	Description
NumberOfRetries	Enter the number of times Oracle Identity Manager must try connecting to the target system before the `InvocationTargetException` error is thrown. Default value: `2` **Note:** The timeout feature is enabled only for full reconciliation and provisioning. It is not applied during incremental reconciliation.
DelayBetweenRetries	Use this parameter to specify the time difference (in milliseconds) between consecutive retries. Default value: `20000`
RecordName	Use this parameter to add the Employee ID for a new user profile or update the Employee ID for an existing user profile. Default value: `PERSONAL_DATA`
UnsupportedCharacters	List of characters or strings that are not supported by PeopleSoft in the value specified for any user profile field Default value: `,##;## ##:##&##(##)##\##[##]##/##<##>##PPLSOFT` These characters are separated by ## (two number sign characters).
PIAServerName	Enter the IP address or host name of the computer hosting PeopleSoft Internet Architecture. **Note:** The IP address or the host name must be followed by the port number on which PeopleSoft Internet Architecture is running. Sample value: `172.21.109.48:90`

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

2.3.3.2 Configuring Oracle Identity Manager to Trust the Remote Manager

To configure Oracle Identity Manager to trust the Remote Manager you have installed:

1. From the computer hosting the Remote Manager, copy the *RM_HOME*/xlremote/config/xlserver.cert file to a temporary directory on the Oracle Identity Manager host computer.

   Note: The server certificate in the *OIM_HOME* directory is also named xlserver.cert. Ensure that you do not overwrite that certificate.

2. To import the certificate by using the keytool utility, run the following command:

   ```
   JAVA_HOME/jre/bin/keytool -import -alias ALIAS -file
   RM_CERT_LOCATION/xlserver.cert -keystore OIM_HOME/xellerate/config/.xlkeystore
   -storepass PASSWORD
   ```

   In the preceding command, replace:

   - *JAVA_HOME* with the location of the Java directory for your application server.
   - *ALIAS* with an alias for the certificate in the store.
   - *RM_CERT_LOCATION* with the full path of the temporary directory where you copied the certificate.
   - *PASSWORD* with the password of the keystore.

3. Copy the *OIM_HOME*/xellerate/config/xlserver.cert file to a temporary directory on the Remote Manager host computer.
4. To import the certificate by using the keytool utility on the Remote Manager host computer, run the following command:

   ```
   JAVA_HOME/jre/bin/keytool -import -alias ALIAS -file
   OIM_CERT_LOCATION/xlserver.cert -keystore RM_HOME/xlremote/config/.xlkeystore
   -storepass PASSWORD
   ```

   In the preceding command, replace:

   - *JAVA_HOME* with the location of the Java directory for your application server.
   - *ALIAS* with an alias for the certificate in the store.
   - *OIM_CERT_LOCATION* with the full path of the temporary directory where you copied the certificate.
   - *PASSWORD* with the password of the keystore.

   Note: It is recommended that you follow security best practices and change the default passwords used for the Remote Manager keystore. To change the Remote Manager keystore password, follow the instructions given in *Oracle Identity Manager Installation and Configuration Guide* for your application server.

2.3.3.3 Verifying That the Remote Manager Is Running

To ensure that the Remote Manager is running:

1. Use the following script to start the Remote Manager:

   RM_HOME/xlremote/remotemanager.bat

2. Log in to the Design Console.
3. Expand **Administration**, and double-click **Remote Manager**.
4. Search for and open the Remote Manager that you have created.
5. Click the Refresh icon. The screen displays details of the Remote Manager that you have configured. The running check box should be selected for the Remote Manager. This implies that the status of the Remote Manager is active.

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
- Adding New Fields for Provisioning
- Adding New Fields for Provisioning for the Connector with the Remote Manager

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 can skip this section.

1. Modify the header and queries in the application engine code (BLKPRCS_UM).

   For example, if you want to reconcile a new column with the name ROLEUSER_ALT, then make the following changes in the application engine code:

```
Local String &ROLEUSER_ALT;
&hdr = "OPRID" | &Sepratr | "OPRDEFNDESC" | &Sepratr | "ALIAS" | &Sepratr |
"EMPLID" | &Sepratr | "PRIEMAILID" | &Sepratr | "LANGUAGE_CD" | &Sepratr |
"MULTILANG" | &Sepratr | "CURRENCY_CD" | &Sepratr | "OPRCLASS" | &Sepratr |
"ROWSECCLASS" | &Sepratr | "PRCSPRFLCLS" | &Sepratr | "DEFAULTNAVHP" | &Sepratr
| "ROLES" | &Sepratr | "EMAILIDS" | &Sepratr | "USERTYPE" | &Sepratr | "STATUS"
| &Sepratr |  "ROLEUSER_ALT";
```

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

```
/*ALTERNATE ROLE*/
   &sel = CreateSQL("select ROLEUSER_ALT from %TABLE(PSROLEXLATOPRVW) where
oprid=:1", &oprid);
   &f = &sel.fetch(&ROLEUSER_ALT);
```

   Add data fields to the file by using the following command:

```
/*WRITING DATA IN FILE*/
&data_row = &oprid | &Sepratr  | &desc | &Sepratr  | &alias | &Sepratr  |
&empid | &Sepratr  | &email | &Sepratr  | &lng_cd | &Sepratr  | &multilang |
&Sepratr  | &currency | &Sepratr  | &oprclass | &Sepratr  | &rowsec | &Sepratr
| &prcsprf | &Sepratr  | &navhp | &Sepratr  | &roles | &Sepratr  | &othmail |
&Sepratr  | &usertype | &Sepratr  | &acctlock | &Sepratr  | &roleuser_alt;
```

```
&DataFile.WriteLine(&data_row);
End-While;
```

3. Log in to the Oracle Identity Manager Design Console.
4. Expand **Development Tools** and then double-click **Form Designer**.
5. Enter `UD_PSFT_BAS` in the Table Name field and click the **Query for records** button. For the connector with the Remote Manager, enter UD_PSFT_RM as the table name.

   See Also: *Oracle Identity Manager Design Console Guide* for more information about this step and the remaining steps of this procedure

6. Click **Create New Version**.
7. In the Create a New Version dialog box, specify the version name in the **Label** field. Save the changes, and then close the dialog box.
8. From the **Current Version** list, select the newly created version.
9. On the Additional Columns tab, click **Add**. Add a column corresponding to the new field in the UD_PSFT_BAS User Defined process form. For the connector with the Remote Manager, add the column to the UD_PSFT_RM User Defined process form. For the example described earlier, you can add the UD_PSFT_BAS_ALTROLE column.
10. Add a reconciliation field corresponding to the new field in the PSFT_UM_RO resource object. For the connector with the Remote Manager, you can add the field to the PSFTUM_RM resource object. For the example described earlier, you can add the Users.RoleUser_Alt reconciliation field.
11. Modify the Lookup.PSFTUM.Attr.Map.Recon lookup definition and add a new row with the target field ROLEUSER_ALT in the Code key and the RO field Users.RoleUser_Alt in Decode. For the connector with the Remote Manager, modify the Lookup.PSFTUM_RM.Attr.Map.Recon lookup definition.
12. Modify the PSFTUM process definition to include the mapping between the newly added attribute and the corresponding reconciliation field. For the connector with the Remote Manager, modify the PSFTUM_RM process definition. For the example described earlier, the mapping is as follows:

    ```
    Users.RoleUser_Alt=UD_PSFT_BAS_ALTROLE
    ```

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

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 in the UserMgmtCBRecon_8.49.txt file inside the *OIM_HOME*/XLIntegrations/PSFTUM/peopleCode directory. The required changes are as follows:

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

      For example, suppose you want to add the alternate user role field, ROLEUSER_ALT, to the list of fields that are reconciled. Then, performing this step involves adding the following SQL statement to retrieve the values of the ROLEUSER_ALT column from the PSROLEXLATOPRVW table:

      ```
      Local String &ROLEUSER_ALT;
      /*ALTERNATE ROLE*/
         &sel = CreateSQL("select ROLEUSER_ALT from %TABLE(PSROLEXLATOPRVW) where
      oprid=:1", &oprid);
         &f = &sel.fetch(&ROLEUSER_ALT);
      ```

   b. Add data fields that are retrieved to the XML message. For example, to add the alternate user role column to the PSROLEXLATOPRVW tag, add the lines highlighted in bold in the following code sample:

      ```
      &recnode = &fieldtypenode.AddElement("PSROLEXLATOPRVW");
      &recnode.AddAttribute("class", "R");
      &fields = &recnode.AddElement("ROLEUSER_ALT");
      &fields.AddAttribute("type", "CHAR");
      ```

   c. Add the data text that are retrieved to the XML message. For example, to add the ROLEUSER_ALT column to the PSROLEXLATOPRVW tag, add the lines highlighted in bold in the following code sample:

      ```
      &datarecnode = &transnode.AddElement("PSROLEXLATOPRVW");
      &datarecnode.AddAttribute("class", "R");
      &datafldnode = &datarecnode.AddElement("ROLEUSER_ALT");
      &textnode = &datafldnode.AddText(&roleuser_alt);
      ```

2. In PeopleSoft Application Designer, copy the contents of the UserMgmtCBRecon_8.49.txt file into the savePostChange event for the USERMAINT component.

3. To extract the contents of the peopleSoftUMApp.war file into a temporary directory, enter the following command:

   ```
   jar -xvf peopleSoftUMApp.war
   ```

4. In the attributemap.properties file, add the XPath (key-value entry) of the new field. For example, you can add the following XPath for the ROLEUSER_ALT field:

   ```
   Users.ROLEUSER_ALT =//Transaction/PSROLEXLATOPRVW/ROLEUSER_ALT
   ```

   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 . ROLEUSER_ALT`, `Users. ROLEUSER_ALT`, and `Users.ROLEUSER ALT` are all invalid key values because they contain spaces.

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

```
jar -cvf peopleSoftUMApp.war .
```

6. Delete the old version of the peopleSoftUMApp.war file from the application server deployment directory.
7. Copy the newly created peopleSoftUMApp.war file into the application server deployment directory.
8. Log in to the Oracle Identity Manager Design Console.
9. Expand **Development Tools** and then double-click **Form Designer**.
10. Enter `UD_PSFT_BAS` in the Table Name field and click the **Query for records** button. For the connector with the Remote Manager, enter UD_PSFT_RM as the table name.

    See Also: *Oracle Identity Manager Design Console Guide* for more information about this step and the remaining steps of this procedure

11. Click **Create New Version**.
12. In the Create a New Version dialog box, specify the version name in the **Label** field. Save the changes, and then close the dialog box.
13. From the **Current Version** list, select the newly created version.
14. On the Additional Columns tab, click **Add**. Add a column corresponding to the new field in the UD_PSFT_BAS user-defined process form. For the connector with the Remote Manager, add the column to the UD_PSFT_RM user-defined process form. For the example described earlier, you can add the UD_PSFT_BAS_ALTROLE column.
15. Add a reconciliation field corresponding to the new field in the resource object, PSFT_UM_RO. For the connector with the Remote Manager, you add the field to the PSFTUM_RM resource object. For the example described earlier, you can add the Users.RoleUser_Alt reconciliation field.
16. Modify the PSFTUM process definition to include the mapping between the newly added field and the corresponding reconciliation field. For the connector with the Remote Manager, modify the PSFTUM_RM process definition. For the example described earlier, the mapping is as follows:

    ```
    Users.RoleUser_Alt=UD_PSFT_BAS_ALTROLE
    ```

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

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

17. Restart Oracle Identity Manager and the Design Console.

3.3 Adding New Fields for Provisioning

Note: If you do not want to add new fields for provisioning, then you can skip this section.

If you want to add new fields for provisioning for the connector with the Remote Manager, proceed to the next section.

To add a new field for provisioning:

See Also: *Oracle Identity Manager Design Console Guide*

Note: Only those fields that have their corresponding SET API's in IUserProfile.class in the peoplesoft.jar file can be provisioned. For example, if you want to provision the Worklist field, then the peoplesoft.jar file must also contain the setWorklistUser (String s) API.

The datatype of the argument in setWorklistUser (String s) must be the same or compatible with the datatype of the corresponding Worklist field in Oracle Identity Manager.

1. Add a mapping for the new field. To do so:
   a. Log in to the Oracle Identity Manager Design Console.
   b. Expand **Administration** and then double-click **Lookup Definition**.
   c. Enter Lookup.PSFTUM.Attr.Map.Prov as the name of the lookup definition in the Code field and click the **Query for records** button.
   d. Modify the Lookup.PSFTUM.Attr.Map.Prov lookup definition and add a new row with the form column name as `code` and target field name as `decode`.

      The format that you must use is as follows:

      ```
      FORM Column Name=TargetAttributeName
      ```

      For example:

      If you want to add the Worklist field, then add the following code key and decode in the Lookup.PSFTUM.Attr.Map.Prov lookup definition:

Code Key	Decode
UD_PSFT_BAS_WORKLIST	WorklistUser

Note: The peoplesoft.jar file must contain a setWorklistUser API for the attribute in the Decode of the look up. For example, for the decode value WorklistUser, the peoplesoft.jar file must also contain a setWorklistUser API. This decode value is case sensitive.

2. Add a new column in the process form by performing the following:
   a. Expand **Development Tools** and then double-click **Form Designer**.

b. Enter `UD_PSFT_BAS` in the Table Name field and click the **Query for records** button.

c. Click **Create New Version**.

d. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.

e. From the **Current Version** list, select the newly created version.

f. On the Additional Columns tab, click **Add**.

g. Specify the new field name and other values.

See Also: *Oracle Identity Manager Design Console* for more information about this step and the remaining steps of this procedure

h. Click the **Make Version Active** button.

Note: If you want to enable the new fields to be updated, then follow the procedure provided in "Enabling Update on a New Field for Provisioning" on page 3-9.

3.4 Adding New Fields for Provisioning for the Connector with the Remote Manager

---

Note: If you do not want to add new fields for provisioning for the connector with the Remote Manager, then you can skip this section.

To add a new field for provisioning for the connector with the Remote Manager:

Note: Only those fields that have their corresponding SET API's in IUserProfile.class in the peoplesoft.jar file can be provisioned. For example, if you want to provision the Worklist field, then the peoplesoft.jar file must also contain the setWorklistUser (String s) API.

The datatype of the argument in setWorklistUser (String s) must be the same or compatible with the datatype of the corresponding Worklist field in Oracle Identity Manager.

---

1. Add a mapping for the new field. To do so:

   a. Add a mapping for the new field. To do so, modify the attribute_RMprov.properties file located in the *RM_HOME*/XLIntegrations/PSFTUM/config directory. At the end of this file, some of the field definitions are preceded by comment characters. You can uncomment these definitions that you want to use to make them a part of the provisioning fields. You can add new fields to this file. The format that you must use is as follows:

   ```
   OIMAttributeName=TargetAttributeName
   ```

   For example:

If you want to add the Worklist field, then add the following line in the attribute_RMprov.properties file:

Worklist=WorklistUser

Note: The peoplesoft.jar file must contain a setWorklistUser API for the attribute in the Decode of the look up. For example, for the decode value WorklistUser, the peoplesoft.jar file must also contain a setWorklistUser API. This decode value is case sensitive.

b. Restart the Remote Manager.

2. Add a new column in the process form by performing the following:
   a. Log in to the Oracle Identity Manager Design Console.
   b. Expand **Development Tools** and then double-click **Form Designer**.
   c. Enter `UD_PSFT_RM` in the Table Name field and click the **Query for records** button.

   See Also: *Oracle Identity Manager Design Console Guide* for more information about this step and the remaining steps of this procedure

   d. Click **Create New Version**.
   e. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.
   f. From the **Current Version** list, select the newly created version.
   g. On the Additional Columns tab, click **Add**.
   h. Specify the new field name and other values.
   i. From the Current Version list, select the newly created version and click **Make Version Active**.
3. Add a new variable in the variable list by performing the following:
   a. Open the Adapter Factory form. This form is in the **Development Tools** folder of the Oracle Identity Manager Design Console.
   b. Click **Query for Records**.
   c. On the Adapter Factory Table tab, double-click the **adp PSFT_RM CREATEUSER** adapter from the list.
   d. On the Variable List tab, click **Add**.
   e. In the Add a Variable dialog box, add a variable Worklist and specify the Type and Description. From the Map To list, select **Resolve at run time**, save the changes, and close the dialog box.
4. Define an additional adapter task for the newly added variable in the adp PSFT_RM CreateUser adapter. To do so:
   a. On the Adapter Tasks tab of the Adapter Factory form, click **IF(connect == SUCCESS)**.
   b. On the Adapter Tasks tab of the Adapter Factory form, click **Add**.
   c. In the Adapter Task Selection dialog box, select **Functional Task**, select **Java** from the list of functional task types, and then click **Continue**.

d. In the Object Instance Selection dialog box, select the **New Object** instance and then click **Continue**.

e. In the Add an Adapter Factory Task dialog box, specify the task name. From the API Source list, select **JavaTaskJar: PSFTUM_RMProvisioning.jar**, and from the Application API list, select **com.thortech.xl.um.integration.hostAccess.PropertySetter()**.

f. Select the **setProperty** method from the Methods list, and then click **Save**.

g. Map the application method parameters, save the changes, and close the dialog box. To map the application method parameters:

For the Output: String:

i. From the Map to list, select **Adapter Variables**.

ii. From the Name list, select **Return variable**.

iii. Click **Set**.

For the Input: String input:

i. From the Map to list, select **Adapter Variables**.

ii. From the Name list, select **Input**.

iii. Click **Set**.

For the Input: String:

i. From the Map to list, select **Literal**.

ii. From the Type list, select **String**.

iii. In the Value field, enter `Worklist`.

iv. Click **Set**.

For the Input: String:

i. From the Map to list, select **Adapter Variables**.

ii. From the Name list, select **Worklist**.

iii. Click **Set**.

5. Create an additional adapter task to set the input variable. To do so:

a. Open the Adapter Factory form. This form is in the Development Tools folder in the Oracle Identity Manager Design Console.

b. On the Adapter Tasks tab of the Adapter Factory form, click **Logical task IF(connect == SUCCESS)**.

c. On the Adapter Tasks tab, click **Add**.

d. In the Adapter Task Selection dialog box, select **Logic Task**, select **SET VARIABLE** from the list, and then click **Continue**.

e. In the Edit Set Variable Task Parameters dialog box, select **input** from the Variable Name list, select **Adapter Task** from the Operand Type list, and the **Operand Qualifier** as the Adapter Task that you have created in Step 4. Then, click **Save**.

Note: Ensure that this newly created variable task is located immediately after the Javatask created in step 4.

---

f. Click **Build** to compile the adp PSFT_RM CreateUser adapter. The Compile Status will be displayed as **OK**.

6. Map the process form columns and adapter variables for the Create User process task as follows:

   a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.

   b. Click **Query for Records**.

   c. On the Process Definition Table tab, double-click the **PSFTUM_RM** process.

   d. On the Tasks tab, double-click the **Create User** task.

   e. In the Closing Form dialog box, click **Yes**.

   f. On the Integration tab of the Editing Task Columns Create User dialog box, map the unmapped variables, save the changes, and close the dialog box. To map an unmapped variable:

      i. Double-click the row in which **N** is displayed in the Status column. The value N signifies that the variable is not mapped.

      ii. From the Map to list in the Edit Data Mapping for Variables dialog box, select **Process Data**.

      iii. From the Qualifier list, select the process form label for the newly added column in the process form.

      iv. Repeat Steps i through iii for all unmapped variables.

7. Repeat Steps 1 through 6 if you want to add more fields.

Note: If you want to enable the new fields to be updated, then follow the procedure provided in "Enabling Update on a New Field for Provisioning" on page 3-9.

3.5 Enabling Update on a New Field for Provisioning

To enable the new provisioning fields to be updated, perform the following steps:

Note:

Some of the steps in the following procedure are specific to the values that have been used. If you use other values, then these steps might need to be performed differently.

To add new fields for provisioning, see "Adding New Fields for Provisioning" on page 3-5, and "Adding New Fields for Provisioning for the Connector with the Remote Manager" on page 3-6.

---

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Process Management** and then double-click **Process definition**.
3. Enter `PSFTUM` in the Name field, and then click the **Query for records** button.

   For the connector with the Remote Manager, enter `PSFTUM_RM`.
4. Add a new task, for example, `Worklist Updated`, and save the task.

5. Click the **Integration** tab of the Worklist Updated task, and then click **Add**.
6. Select **Adapter** as the handler type and then perform the following:
   a. Select **ADPPSFTUMUPDATEUSER** and click **Save**. For the connector with the Remote Manager, select **ADPPSFT_RMUPDATEUSER**.
   b. In Adapter Variables, double click **attrName**. A window is displayed for editing the data mapping of the variable.
   c. From the Map To list, select **Literal**.
   d. In Literal Value, enter `UD_PSFT_BAS_Worklist` as the column name for the new field that was added in the Lookup.PSFTUM.Attr.Map.Prov lookup definition.

      For the connector with the Remote Manager, in Literal Value, enter `Worklist` as the value of OIMAttributeName. This value should be same as that specified in the attribute_RMprov.properties file.
7. In the adapter variables tab, double-click **attrValue**. A window is displayed for editing the data mapping of the variable. From the Map To list, select **Process Data** and from the Qualifier list, select form field label for the newly added column in the form.

   Perform this step for the connector with the Remote Manager also.
8. Perform all mappings and save.
9. Click the **Responses** tab of the Worklist Updated task. Add the SUCCESS and ERROR responses. Enter C for the SUCCESS response and R for the ERROR response.

Note: You must enter Y or N in the WorklistUser field because only these values are accepted by PeopleSoft.

4

Using the Connector

This chapter contains the following sections:

- Configuring the Scheduled Tasks for Lookup Field Synchronization
- Configuring Reconciliation
- Performing Provisioning Operations

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

- Guidelines on Using the Connector

4.1 Configuring the Scheduled Tasks for Lookup Field Synchronization

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

- PSFT UM LookUp Reconciliation

  This scheduled task is used to synchronize the values of the lookup fields between the target system and Oracle Identity Manager.

- PSFT UM_RM LookUp Reconciliation

  This scheduled task is used to synchronize the values of the lookup fields between the target system and Oracle Identity Manager if you are using the connector with the Remote Manager.

Table 4–1 describes the attributes of both scheduled tasks.

Note:

- Default attribute values are predefined in the connector XML file that is imported during the installation of the connector. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Table 4–1 Scheduled Task Attributes For Lookup Field Synchronization

Attribute	Description
ServerName	Enter the name of the IT resource
LookupType	Enter any one of the following values for this attribute to specify the type of data that is searched for in the target system; ■ `LanguageCode` ■ `EmailTypes` ■ `CurrencyCode` ■ `PermissionList` ■ `UserRoles` Default value: `UserRoles`

Table 4–1 (Cont.) Scheduled Task Attributes For Lookup Field Synchronization

Attribute	Description
FilePath	Enter the full path of the file in which the lookup data to be reconciled is stored. The operating system of the computer on which Oracle Identity Manager is installed must be able to access this file path. The data extracted from this file is stored in the LookupName attribute. Sample value: `C:\PSFTUM\LookupRecon\Roles.txt`
LookupName	Enter the name of the lookup definitions created in Oracle Identity Manager that corresponds to the lookup fields in the target system. The value can be any one of the following: ▪ `Lookup.PSFTUM.LanguageCode` ▪ `Lookup.PSFTUM.EmailType` ▪ `Lookup.PSFTUM.CurrencyCode` ▪ `Lookup.PSFTUM.PermissionList` ▪ `Lookup.PSFTUM.Roles` Default value: `Lookup.PSFTUM.Roles` For the connector with the Remote Manager, the value can be any one of the following: ▪ `Lookup.PSFTUM_RM.LanguageCode` ▪ `Lookup.PSFTUM_RM.EmailType` ▪ `Lookup.PSFTUM_RM.CurrencyCode` ▪ `Lookup.PSFTUM_RM.PermissionList` ▪ `Lookup.PSFTUM_RM.Roles` Default value: `Lookup.PSFTUM_RM.Roles`
RecordDelimiter	Enter a value for this attribute to configure the delimiter. If you do not enter any value, then the delimiter will be set as "`*`" (asterisk) by default. Valid values are all special characters except the following: `#, ;, ., @, ,` Default value: `*` Case 1: `RecordDelimiter = myDelimiter` In this case, `m` will be considered as the delimiter but the records will not be reconciled because the valid delimiter can only be a special character. Case 2: RecordDelimiter = `$myDelimiter` In this case, `$` will be set as a new delimiter. Case 3: RecordDelimiter = In this case, the default value "*" (asterisk) will be set as the delimiter. See "Configuring the Target System for Full Reconciliation" on page 2-19 for instructions to configure the record delimiter in PeopleCode. **Note:** Ensure that the value that you enter for this attribute is the same as that mentioned in the flat file.

4.2 Configuring Reconciliation

This section describes the following topics:

4.2.1 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 Tasks
- Running the Application Engine Program

4.2.1.1 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`.

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

4.2.1.2 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`.

4.2.1.3 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, Operator, SearchCriteria, and CaseSensitive 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:

- OPRID
- OPRDEFNDESC
- ALIAS

- EMPLID
- PRIEMAILID
- LANGUAGE_CD
- MULTILANG
- CURRENCY_CD
- OPRCLASS
- ROWSECCLASS
- PRCSPRFLCLS
- DEFAULTNAVHP
- ROLES
- EMAILIDS
- USERTYPE
- 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 Tasks" section on page 4-6 for information about these scheduled task attributes used for filtering records.

Example 1:

```
IsFilterApplied=yes
FiltersToBeApplied=OPRID,OPRDEFNDESC,ALIAS
FiltersValues=SFCA001,Application User,John
CaseSensitive=yes
SearchCriteria=INDEX_OF
Operator=AND
```

This example will reconcile all the records in which the OPRID, OPRDEFNDESC, and ALIAS fields contain the values SFCA001, Application User, 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=OPRID,OPRDEFNDESC,ALIAS
FiltersValues=SFCA001,Application User,John
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=AND
```

This example will reconcile all the records in which the OPRID, OPRDEFNDESC, and ALIAS fields contain the values SFCA001, Application User, and John, respectively.

The case (uppercase or lowercase) of the values is not considered. The values of SearchCriteria and CaseSensitive are specified as EXAMPLE. Therefore, by default, INDEX_OF and Nodata are used as the values of these attributes, respectively.

Example 3:

```
IsFilterApplied=EXAMPLE
FiltersToBeApplied=OPRID,OPRDEFNDESC,ALIAS
FiltersValues=SFCA001,Application User,John
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=NODATA
```

This example will reconcile all the records. The value of IsFilterApplied is specified as EXAMPLE. Therefore, by default, NO is used as the value and all the records are reconciled.

Example 4:

```
IsFilterApplied=YES
FiltersToBeApplied=OPRID,OPRDEFNDESC,ALIAS
FiltersValues=SFCA001,Application User,John
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`.

4.2.1.4 Configuring the Reconciliation Scheduled Tasks

When you run the Connector Installer, reconciliation scheduled tasks are automatically created in Oracle Identity Manager. Table 4–2 describes these scheduled tasks.

Table 4–2 Reconciliation Scheduled Tasks

Schedule Task Name	Description
PSFT UM Target Resource User Reconciliation	This scheduled task is used for target resource reconciliation.
PSFT UM_RM Target Resource User Reconciliation	This scheduled task is used for target resource reconciliation if you are using the connector with the Remote Manager.
PSFT UM Target Resource Delete Reconciliation	This scheduled task is used to reconcile data of deleted users from a target resource into Oracle Identity Manager.
PSFT UM_RM Target Resource Delete Reconciliation	This scheduled task is used to reconcile data of deleted users from a target resource into Oracle Identity Manager if you are using the connector with the Remote Manager.

To perform a full reconciliation run, you must configure the scheduled tasks to reconcile the users in 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.

4.2.1.4.1 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 4–3 describes the attributes of the scheduled tasks.

Note: Attribute values are predefined in the connector XML file that is imported during the installation of the connector. Specify values only for the attributes that you want to change.

Table 4–3 Attributes of the Scheduled Tasks for Reconciliation of User Data

Attribute	Description
MultiValueSeperator	Enter ## as the multivalue separator in the flat file.
ServerName	Enter the name of the IT resource Default value: `PSFT UM Server`
FilePath	Enter the full path of the directory in which the flat file is stored on Oracle Identity Manager. The operating system of the computer on which Oracle Identity Manager is installed 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. Sample value: `C:\bulkrecon.txt` See "Configuring the Target System for Full Reconciliation" on page 2-19 for information about generating the flat file.
ReconcilingRO	Enter the name of the resource object that is used for reconciliation. For target resource reconciliation: Default value: `PSFT_UM_RO` For the connector with the Remote Manager: Default value: `PSFTUM_RM`.
NoOfRecordsToBeReconciled	Enter the number of records to be reconciled See "Specifying the Number of Records to Be Reconciled" on page 4-4 for more information about this attribute. Default value: `5`
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`
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 is considered as `No`. Default value: `Nodata`

Table 4–3 (Cont.) Attributes of the Scheduled Tasks for Reconciliation of User Data

Attribute	Description
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 4-4 for more information about using this attribute.

FiltersValues	Enter the comma-separated list of values for the filter attributes that you specify as the value of the FiltersToBeApplied attribute
	See "Limited Reconciliation" on page 4-4 for more information.
	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:
	Case 1: `IsFilterApplied = yes`
	Only if the value of the IsFilterApplied attribute is `yes`, will data be fetched for filtering.
	Case 2: `IsFilterApplied = yes`, `FiltersToBeApplied =`, and `FiltersValues = JOHN`
	In this case, the "Filters not synchronized" error message is displayed.
	Case 3: `IsFilterApplied = yes`, `FiltersToBeApplied = OPRID`, and `FiltersValues =`
	In this case, the "Filters not synchronized" error message is displayed.
	Case 4: `IsFilterApplied = yes`, `FiltersToBeApplied = ,` and `FiltersValues =`
	or
	`IsFilterApplied = yes`, `FiltersToBeApplied = Nodata`, and `FiltersValues = Nodata`
	These cases are equivalent to `IsFilterApplied = No`.
	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 = OPRID,DESCRIPTION,` and `FiltersValues = SFCA001, This is a, test`
	In this scenario, the user has entered the value of `DESCRIPTION` as "This is a, test". The filtering engine will consider it as two different values, "This is a", and "test". 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 value 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 4-4 for more information.

Table 4–3 (Cont.) Attributes of the Scheduled Tasks for Reconciliation of User Data

Attribute	Description
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 4-4 for more information about this attribute. Default value: `-1`
ScheduledTaskName	The name of the scheduled task. This attribute is used to update the `IndexOfLastReconciledRecord` attribute. Default value: `PSFT UM Target Resource User Reconciliation` For the connector with the Remote Manager, the default value is `PSFT UM_RM Target Resource User Reconciliation`.
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. For target resource reconciliation: Default value: `Lookup.PSFTUM.Attr.Map.Recon` For a target resource reconciliation run on the connector with the Remote Manager: Default value: `Lookup.PSFTUM_RM.Attr.Map.Recon`
ChildAttributeMapLookUpForRecon	Enter a value for this attribute to specify the mappings of child tables reconciled during reconciliation. Default value: `Lookup.PSFTUM.Child.Attr.Map.Recon`
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 (`,`) Default value: `*` 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 Record Delimiter" on page 2-21 for instructions to configure the record delimiter in PeopleCode.

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

4.2.1.5 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_USER` 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 employee ID

   Run Control ID: Enter a unique run control value

   Program Name: Enter `BLKPRCS_USER`

8. Click **Run**.
9. From the list that is displayed, select the BLKPRCS_USER 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.

4.2.2 Configuring Incremental Reconciliation

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

This section discusses the following topic:

4.2.2.1 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.OprId
- Users.OprDefnDesc
- Users.Alias
- Users.EmployeeId
- Users.Multilanguage
- Users.PrimaryPermission
- Users.RowSecurityPermission
- Users.LanguageCD
- Users.CurrencyCode
- Users.AccountStatus
- Users.ProcessProfilePermission
- Users.NavigatorHomePagePermission
- Users.PrimaryEmailId
- Users.EmailIds
- Users.Roles
- Users.EmailId

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.OprId,Users.OprDefnDesc,Users.Alias
FiltersValues=SFCA001,Application User,John
CaseSensitive=yes
SearchCriteria= INDEX_OF
Operator=and
```

This example will reconcile all the records in which Users.OprId, Users.OprDefnDesc, and Users.Alias contain the values SFCA001, Application User, 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.OprId,Users.OprDefnDesc,Users.Alias
FiltersValues=SFCA001,Application User,John
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=and
```

This example will reconcile all the records in which Users.OprId, Users.OprDefnDesc, and Users.Alias contain the values SFCA001, Application User, and John, 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 the valid values, respectively.

Example 3:

```
IsFilterApplied=EXAMPLE
FiltersToBeApplied=Users.OprId,Users.OprDefnDesc,Users.Alias
FiltersValues=SFCA001,Application User,John
CaseSensitive=EXAMPLE
SearchCriteria=EXAMPLE
Operator=NODATA
```

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

Example 4:

```
IsFilterApplied=YES
FiltersToBeApplied=Users.OprId,Users.OprDefnDesc,Users.Alias
FiltersValues=SFCA001,Application User,John
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 Performing Provisioning Operations

Note: The "Unable to access pstools.properties" message might be recorded in the server logs during provisioning operations. You can ignore this message.

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user. To provision a resource:

Note: The following procedure is performed using the direct provisioning approach.

1. Log in to the Administrative and User Console.
2. From the Users menu:
   - Select **Create** if you want to first create the OIM User and then provision a PeopleSoft User Management account to the user.
   - Select **Manage** if you want to provision a PeopleSoft User Management account to an existing OIM User.
3. If you select Create, on the Create User page, enter values for the OIM User fields, and then click **Create User**.
4. If you select Manage, then search for the OIM User and select the link for the user from list of users displayed in the search results.
5. On the User Detail page, select **Resource Profile** from the list at the top of the page.
6. On the Resource Profile page, click **Provision New Resource**.
7. On the Step 1: Select a Resource page, select **PSFT_UM_RO** from the list, and then click **Continue**.

   If you are using the connector with the Remote Manager, then select **PSFTUM_RM**.
8. On the Step 2: Verify Resource Selection page, click **Continue**.
9. On the Step 5: Provide Process Data page, enter the details of the account that you want to create on the target system and then click **Continue**.
10. On the Step 6: Verify Process Data page, verify the data that you entered and then click **Continue**.

    The account is created on the target system and provisioned as a resource to the OIM User. The page that is displayed provides options to disable or revoke the resource from the OIM User.

See Also: "Provisioning" on page 1-9 for more information about the provisioning functions supported by this connector and the process form fields used for provisioning

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 and Troubleshooting

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

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/PSFTUM/config/config_Recon.properties file, and specify values for the following properties:
   - FiltersToBeApplied
   - FiltersValues
   - IsFilterApplied
   - Operator
   - SearchCriteria
   - CaseSensitive
   - FilePath
   - RecordDelimiter
   - NoOfRecordsToBeReconciled
   - UserType
   - EmployeeType
   - OrganizationName
   - IndexOfLastReconciledRecord
   - 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/PSFTUM/scripts/psftUM_Recon.sh

   For Microsoft Windows:

   OIM_HOME/XLIntegrations/PSFTUM/scripts/psftUM_Recon.bat

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 user profiles 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 USR_MGMT_MSG.xml file, which is in the *OIM_HOME*/XLIntegrations/PSFTUM/cbrecon directory.

5.2.2 Testing the PeopleSoft Listener

To test the PeopleSoft listener:

1. In the *OIM_HOME*/XLIntegrations/PSFTUM/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 user data values in the ExecuteATM function.
2. Run psft-xel-test.vbs. Ensure that the script runs without any errors.

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 psft-xel-test.vbs file.

If the reconciliation event is successful, an event is displayed with the status as either Event Linked or No Match Found.

5.3 Testing Provisioning

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

There are two modes in which the testing utility runs:

- File Mode: In this mode, all the connectivity information will be read from the config file and it will prompt you to enter target credentials, which consist of the username and password.
- OIM Mode: While running in OIM mode, the testing utility will read only the connectivity information from the IT Resource and rest of the information will be read from the file. It will prompt you to enter Oracle Identity Manager credentials, which consist of the username and password to log in to Oracle Identity Manager.

  While running the testing utility in OIM mode, you must copy the following files to the *OIM_HOME*/ThirdParty directory:

  – For Oracle WebLogic Server:

    Copy weblogic.jar from *BEA_HOME*/weblogic81/server/lib

  – For IBM WebSphere Application Server, copy the following files:

    com.ibm.ws.admin.client_6.1.0.jar from *WAS_HOME*/AppServer/runtimes

    ibmorb.jar from *WAS_HOME*/AppServer/java/jre/lib

    xlDataObjectBeans.jar from *OIM_CLIENT*/xlclient/lib

  – For JBoss Application Server:

    Copy jbossall-client.jar and ejb.jar from *OIM_CLIENT*/xlclient/ext

  – For Oracle Application Server:

    Copy oc4jclient.jar and ejb.jar from *OIM_CLIENT*/xlclient/ext, and javagroups-all.jar from *OIM_HOME*/ext.

For the connector with the Remote Manager, before the testing utility prompts you for either the target or Oracle Identity Manager credentials, it will prompt you for the Remote Manager credentials. You must provide the following details:

- service name

  Sample value: `ServiceName= RManager`

- url

  The syntax of the url is: rmi://*REMOTE_MANGER_HOST*:*BINDING_PORT*

  Sample value: `url = rmi://172.21.109.95:12346`

  The service name and the binding port of the url are available in the *RM_HOME*/config/xlconfig.xml file.

Before you use the testing utility, you must set the required values in the config.properties file. This file is located in the *OIM_HOME*/XLIntegrations/PSFTUM/config directory.

Use the information in the following table to modify the default attributes of the config.properties file.

Name	Description	Sample Value
Mode	Specifies the mode (File/OIM) in which the testing utility will run.	FILE
ITResourceType	The IT resource type of the IT resource instance, which is used to fetch the connectivity information when running in OIM mode.	PSFTUM_RM
ITResourceName	The name of the IT resource instance which is used to fetch the connectivity information when running in OIM mode.	PSFTUM_RM_849
serverName	IP address or host name of the PeopleSoft Enterprise Applications server	172.21.109.95
serverPort	Port at which the PeopleSoft Enterprise Applications server is listening	9000
ciName	Component interface used to load user data in PeopleSoft Enterprise Applications	USER_PROFILE
NumberOfRetries	Number of times the connection to the target system must be retried before the `InvocationTargetException` is thrown	2
DelayBetweenRetries	Time difference between subsequent retries (in milliseconds)	10000
action	Action to be performed	You can specify one of the following values: CONNECT CREATE DELETE UPDATEUSERINFO UPDATEUSER_EMPID UPDATEPASSWORD
userId	User login ID	PSFTTEST
userDescription	Description of the user	PSFTTEST
primaryEmailAddress	Primary e-mail address	PSFTTEST@psft.com
primaryEmailType	E-mail type of the primary e-mail account	BUS
password	Password of the user	password
languageCode	Language code for the user	ENG
currencyCode	Currency code for the user	USD
recName	Used to validate the employee ID during user provisioning in PeopleSoft Enterprise Applications	PERSONAL_DATA
empId	Employee ID for the user	A10000
primaryPermissionList	Primary permission list for the user	HCCPAM1
userIdAlias	User ID alias	PSFTTEST1
symbId	Specifies the AccessId associated with the user profile The AccessId specifies whether or not the user has sufficient privileges on the PeopleSoft Enterprise Applications database.	PS89

Name	Description	Sample Value
attrName	Name of the attribute to be updated	You can specify one of the following values. These are the column names of the fields to be updated. UD_PSFT_BAS_EMPLID UD_PSFT_BAS_OPRDEFNDESC UD_PSFT_BAS_OPERPSWD
attrValue	Value of the attribute to be updated	The value that you provide must correspond to the attribute name that you specify as the value of the attrName parameter.

After you specify values in the config.properties file, run one of the following files:

For UNIX:

OIM_HOME/XLIntegrations/PSFTUM/scripts/PSFTUM.sh

For Microsoft Windows

OIM_HOME/XLIntegrations/PSFTUM/scripts/PSFTUM.bat

For the connector with the Remote Manager:

For UNIX:

OIM_HOME/XLIntegrations/PSFTUM/scripts/PSFTUM_RM.sh

For Microsoft Windows

OIM_HOME/XLIntegrations/PSFTUM/scripts/PSFTUM_RM.bat

If your Oracle Identity Manager installation is running on IBM WebSphere Application Server, then run the following file:

For UNIX:

OIM_HOME/XLIntegrations/PSFTUM/scripts/was_psftUM_RM.sh

For Microsoft Windows

OIM_HOME/XLIntegrations/PSFTUM/scripts/was_PSFTUM_RM.bat

5.4 Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the PeopleSoft User Management connector.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with the PeopleSoft Enterprise Applications server.	■ Ensure that the PeopleSoft Enterprise Applications server is running. ■ Ensure that Oracle Identity Manager is running. ■ Ensure that all the adapters have been compiled. ■ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that the IP address, admin ID, and admin password are correct. ■ Ensure that the correct JOLT port has been specified. See Table 2–4, " Parameters of the IT Resource for the Target System" for information about locating and determining a JOLT port. ■ Ensure that the server on which Oracle Identity Manager is running can communicate with the JOLT listener over the JOLT port.
The Operation Fail message is displayed on the Oracle Identity Manager Administrative and User Console.	■ Ensure that the values for the attributes do not contain delimiter characters, such as white space and commas. ■ Ensure that the attribute values do not exceed allowable length.
The Create User adapter is triggered even when the pre-populate adapter is run successfully.	Set the property associated with the user ID attribute in the process form as required.

6

Known Issues

The following are known issues associated with this release of the connector:

- **Bug 7165853**

  Adding new multivalued fields for either reconciliation or provisioning is not supported.

- **Bug 6685642**

  The Remote Manager functions as expected after the certificate import and trust configuration between Oracle Application Server and the Remote Manager is completed. However, the status of the Remote Manager in the Oracle Identity Manager Design Console does not get updated to "Running".

- **Bug 7191873**

  If your Oracle Identity Manager installation is deployed on IBM WebSphere Application Server, you must use the connector with the Remote Manager to implement provisioning from Oracle Identity Manager to PeopleSoft.

- **Bug 7191922**

  SSL configuration during provisioning from Oracle Identity Manager to PeopleSoft is supported only when you are using the connector with the Remote Manager. The Remote Manager should be deployed on the same computer on which PeopleSoft is installed.

- **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

R

S

T

V