# Oracle® Identity Manager Connector Guide for PeopleSoft Campus



ORACLE

Oracle Identity Manager Connector Guide for PeopleSoft Campus, 11.1.1

E36940-11

Copyright © 2012, 2020, Oracle and/or its affiliates.

Primary Author: Gowri.G.R

Contributing Authors: Alankrita Prakash

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

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

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

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

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

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

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

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

# Contents

#### Preface

Audience	Х
Documentation Accessibility	Х
Related Documents	Х
Conventions	Х

# What's New in the Oracle Identity Manager Connector for PeopleSoft Campus?

Software Updates	xii
Documentation-Specific Updates	xii

#### 1 About the Connector

1.1 Cert	fied Components	1-1
1.2 Con	nector Architecture	1-2
1.3 Med	ium of Data Interchange	1-5
1.3.1	Full Reconciliation	1-5
1.3.2	Incremental Reconciliation	1-6
1.4 Feat	ures of the Connector	1-7
1.4.1	Dedicated Support for Trusted Source Reconciliation	1-8
1.4.2	Seeding Roles into Oracle Identity Manager	1-8
1.4.3	Full and Incremental Reconciliation	1-9
1.4.4	Reconciliation of Effective-Dated Lifecycle Events	1-9
1.4.5	Support for Standard PeopleSoft Messages	1-10
1.4.6	Support for Resending Messages That Are Not Processed	1-11
1.4.7	Validation and Transformation of Person Data	1-11
1.4.8	Target Authentication	1-11
1.4.9	Support for Specifying Persons to Be Excluded from Reconciliation	
	Operation	1-11
1.5 Con	nector Objects Used During Reconciliation	1-12
1.5.1	Reconciliation Rules	1-12
1.5	5.1.1 Overview of the Reconciliation Rule	1-12



	1.5.1.2	Viewing the Reconciliation Rule in the Design Console	1-13
:	1.5.2 Reco	onciliation Action Rules	1-14
	1.5.2.1	Overview of the Reconciliation Action Rules	1-14
	1.5.2.2	Viewing the Reconciliation Action Rules in the Design Console	1-15
:	1.5.3 Pred	lefined Lookup Definitions	1-16
	1.5.3.1	Lookup.PSFT.Campus.Configuration	1-16
	1.5.3.2	Lookup Definitions Used to Process SCC_CONSTITUENT_FULLSYNC Messages	1-17
	1.5.3.3	Lookup Definitions Used to Process SCC_CONSTITUENT_SYNC Messages	1-25
	1.5.3.4	Lookup.PSFT.Campus.CustomQuery	1-29
	1.5.3.5	Lookup.PSFT.Campus.ExclusionList	1-30
1.6	Roadmap	for Deploying and Using the Connector	1-30

# 2 Deploying the Connector

2.1	Preir	nstalla	tion	2-1
:	2.1.1	Dete	ermining the Version of PeopleTools and the Target System	2-1
:	2.1.2	Files	and Directories on the Installation Media	2-1
:	2.1.3	Preii	nstallation on the Target System	2-3
	2.1	L.3.1	Creating a Target System User Account for Connector Operations	2-3
2.2	Insta	llatior	1	2-7
:	2.2.1	Insta	allation on Oracle Identity Manager	2-8
	2.2	2.1.1	Running the Connector Installer	2-8
	2.2	2.1.2	Copying the Connector Files and External Code Files	2-9
	2.2	2.1.3	Configuring the IT Resource	2-10
	2.2	2.1.4	IT Resource Parameters	2-12
	2.2	2.1.5	Deploying the PeopleSoft Listener	2-13
	2.2	2.1.6	Removing the PeopleSoft Listener	2-16
:	2.2.2	Insta	allation on the Target System	2-18
	2.2	2.2.1	Configuring the Target System for Full Reconciliation	2-18
	2.2	2.2.2	Enabling Content-based Filtering for Full Reconciliation in SCC_CONSTITUENT_FULLSYNC Message	2-31
	2.2	2.2.3	Configuring the Target System for Incremental Reconciliation	2-35
	2.2	2.2.4	Enabling Content-based Routing for Incremental Reconciliation in SCC_CONSTITUENT_SYNC Message	2-60
:	2.2.3	Insta	allation with Other PeopleSoft Connectors	2-62
2.3	Post	install	ation	2-62
:	2.3.1	Con	figuring Oracle Identity Manager	2-62
	2.3	3.1.1	Enabling Logging	2-63
	2.3	3.1.2	Setting Up the Lookup.PSFT.Campus.Configuration Lookup Definition	2-66



2.3.1.3	Setting Up the Lookup.PSFT.Campus.ExclusionList Lookup	
	Definition	2-66
2.3.1.4	Configuring SSL	2-67
2.3.1.5	Creating an Authorization Policy for Campus ID	2-76
2.3.1.6	Displaying UDFs in Oracle Identity Manager 11.1.2 or Later	2-76
2.3.1.7	Localizing Field Labels in UI Forms	2-77
2.3.2 Conf	iguring the Target System	2-78
Postcloning	g Steps	2-79

## 3 Using the Connector

2.4

01 0			0.1
	2	of Steps to Use the Connector	3-1
3.2 See	ding R	oles into Oracle Identity Manager	3-2
3.2.1	Gen	erating CSV File	3-2
3.2.2	Impo	orting CSV File into Oracle Identity Manager to Create Roles	3-3
3.3 Verif	iying th	ne Affiliation Status Code	3-3
3.3.1	Abou	ut Affiliation Status	3-4
3.3.2	Verif	ying the Affiliation Status Code on PeopleSoft Campus	3-4
3.4 Verif	iying th	ne Entries in Attribute Mapping Lookup Definitions	3-6
3.5 Perf	orming	Full Reconciliation	3-6
3.5.1	Gen	erating XML Files	3-7
3.5.2	Impo	orting XML Files into Oracle Identity Manager	3-8
3.5	5.2.1	Configuring the Scheduled Task for Person Data Reconciliation	3-8
3.5	5.2.2	Configuring the Scheduled Task for Processing Affiliation Effective Date	3-9
3.6 Perf	orming	Incremental Reconciliation	3-9
3.7 Limi	ted Re	conciliation	3-9
3.7.1	Abou	ut Limited Reconciliation	3-10
3.7.2	Conf	iguring Limited Reconciliation	3-10
3.8 Res	ending	Messages That Are Not Received by the PeopleSoft Listener	3-11
3.8.1	Send	ling Messages Manually	3-12
3.8.2	Rese	ending Messages Manually in Error or TimeOut Status	3-12
3.9 Con	figurin	g Scheduled Jobs	3-13
3.9.1	Conf	ïgurable Scheduled Tasks	3-13
3.9.2	Conf	ïguring a Scheduled Task	3-13

## 4 Extending the Functionality of the Connector

4.1 Adding New User Attributes for Reconciliation	4-1
4.1.1 Adding a New User Attribute for Reconciliation	4-1
4.1.2 Creating a User-Defined Field	4-3
4.2 Adding New Affiliation Attributes for Reconciliation	4-3



	4.2.1	About Affiliation Attributes	4-3
	4.2.2	Adding the New Field to the List of Reconciliation Fields	4-4
	4.2.3	Creating a New Version of the Process Form	4-5
	4.2.4	Adding a New Field on the Process Form	4-5
	4.2.5	Creating a Reconciliation Field Mapping for the New Field	4-6
	4.2.6	Creating an Entry for the Field in the Lookup Definition for Attribute Mapping	4-7
	4.2.7	Creating an Entry for the Field in the Lookup Definition for Reconciliation	4-8
	4.2.8	Creating an Entry for the Field in the Configuration Lookup Definition	4-9
	4.2.9	Verifying the Affiliation Rank Attribute	4-10
4.3	Addi	ng Support for Primary Affiliations	4-10
4.4	Mod	ifying Field Lengths on the OIM User Form	4-11
4.5	Con	figuring Validation of Data During Reconciliation	4-11
	4.5.1	Implementing the Validation Logic in a Java Class	4-12
	4.5.2	Uploading the JAR File to Oracle Identity Manager	4-13
	4.5.3	Updating the Message-Specific Configuration Lookup Definition	4-14
	4.5.4	Redeploying the PeopleSoftOIMListener.ear File on the Application	
		Server	4-14
4.6		figuring Transformation of Data During Reconciliation	4-15
	4.6.1	Implementing the Transformation Logic in a Java Class	4-15
	4.6.2	Uploading the JAR File to Oracle Identity Manager	4-17
	4.6.3	Updating the Message-Specific Configuration Lookup Definition	4-17
	4.6.4	Redeploying the PeopleSoftOIMListener.ear File on the Application Server	4-18
4.7	Setti	ng Up the Lookup.PSFT.Campus.CustomQuery Lookup Definition	4-18
4.8	Con	figuring the Connector for Multiple Installations of the Target System	4-19
	4.8.1	About Configuring the Connector for Multiple Installations of the Target System	4-19
	4.8.2	Creating Copies of the Connector Objects	4-21
To	ctina	and Troublochooting	
	_	and Troubleshooting	
5.1		ing Reconciliation	5-1
5.2	Irou	bleshooting	5-2
De	eterm	ining the Root Audit Action Details	
A.1	The	PSCAMA Subnode	A-1
A.2	Roo	t Audit Action	A-2
Se	etting	Up SSL on Oracle WebLogic Server	
B.1	Gen	erating Signed Public Encryption Key and CSR	B-1



Α

В

B.2	Submitting CSRs to CAs for Signing	B-4
B.3	Downloading the Root Certificate	B-6
B.4	Importing a Server-Side Public Key into a Keystore	B-6
B.5	Generating and Importing Public Keys	B-8
B.6	Configuring Oracle WebLogic Server to Use the Keystore	B-9
B.7	Adding the Root Certificate	B-12
B.8	Configuring the PeopleSoft Certificates	B-12

# C Message Structure

# D Authorization Policy

Index



## List of Figures

1-1	Architecture of the Connector	1-3
1-2	Storing Data in Oracle Identity Manager	1-4
1-3	Full Reconciliation	1-6
1-4	Incremental Reconciliation	1-7
1-5	Seeding Roles in Oracle Identity Manager	1-9
1-6	Reconciliation Rule	1-13
1-7	Affiliation Reconciliation Rule	1-14
1-8	Reconciliation Action Rules	1-15
1-9	Sample XML File for SCC_CONSTITUENT_SYNC Message	1-24
4-1	Adding a New Affiliation Field for Reconciliation	4-5
4-2	Adding a New Version of Process Form	4-6
4-3	Adding a Affiliation Field Mapping	4-7
4-4	Adding an Entry to Attribute Mapping Lookup	4-8
4-5	Adding an Entry to Reconciliation Lookup	4-9
4-6	Adding an Entry to Configuration Lookup	4-10



#### List of Tables

1-1	Certified Components	1-1
1-2	Action Rules for Trusted Source Reconciliation	1-14
2-1	Files and Directories on the Installation Media	2-2
2-2	Files to Be Copied to the Oracle Identity Manager Host Computer	2-10
2-3	IT Resource Parameters	2-12
2-4	Log Levels and ODL Message Type:Level Combinations	2-63
3-1	Attributes of the PeopleSoft Campus Role Creation Scheduled Task	3-3
3-2	Attributes of the PeopleSoft Campus Trusted Full Reconciliation Scheduled Task	3-8
3-3	Attributes of the PeopleSoft Campus Affiliation Effective Date Processor Scheduled Task	3-9
4-1	Connector Objects and Their Associations	4-20



# Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with PeopleSoft Campus.

## Audience

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

# **Documentation Accessibility**

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup? ctx=acc&id=docacc.

#### Access to Oracle Support

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

# **Related Documents**

For information about installing and using Oracle Identity Manager, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E52734\_01/index.html

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

http://docs.oracle.com/cd/E22999\_01/index.htm

## Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.



Convention	Meaning
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 Campus?

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

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

Software Updates

This section describes updates made to the connector software.

Documentation-Specific Updates

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

# Software Updates

The following section discusses the software updates:

## Software Updates in Release 11.1.1.5.0

There are no software updates in this release of the connector.

# **Documentation-Specific Updates**

The following section discusses the documentation-specific updates:

## Documentation-Specific Updates in Release 11.1.1.5.0

The following is a documentation-specific updates in revision "11" of this guide:

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

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

- The "Target Systems" row in Table 1-1 has been modified to include support for PeopleSoft Campus Solutions Maintenance Pack 9.2 with PeopleTools 8.54 through 8.56.
- The description of the ORACLE\_COMMON environment variable in Deploying the PeopleSoft Listener has been modified.

The following are documentation-specific updates in revision "9" of this guide:



- The "Target Systems" row in Table 1-1 has been modified to include support for PeopleSoft Campus Solutions Maintenance Pack 9.0 with PeopleTools 8.51 through 8.53.
- An issue related to the creation of two CREATE user events has been added to Troubleshooting.

The following are documentation-specific updates in revision "8" of this guide:

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

The following is a documentation-specific update in revision "7" of this guide:

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

The following is a documentation-specific update in revision "6" of this guide:

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

The following are documentation-specific updates in revision "5" of this guide:

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

The following is a documentation-specific update in revision "4" of this guide:

Figure 1-1 has been updated.

The following are documentation-specific updates in revision "3" of this guide:

- The "Oracle Identity Manager" row in Table 1-1 has been modified.
- Displaying UDFs in Oracle Identity Manager 11.1.2 or Later has been added.
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added in the following sections:
  - Running the Connector Installer
  - Configuring the IT Resource
  - Configuring Scheduled Jobs



# 1 About the Connector

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

#### Note:

In this guide, PeopleSoft Campus has been referred to as the **target system**.

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

This chapter contains the following sections:

- Certified Components
- Connector Architecture
- Features of the Connector
- Connector Objects Used During Reconciliation
- Roadmap for Deploying and Using the Connector

# **1.1 Certified Components**

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

#### Table 1-1 Certified Components

Item	Requirement		
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:		
	• Oracle Identity Governance 12c (12.2.1.4.0)		
	• Oracle Identity Governance 12c (12.2.1.3.0)		
	<ul> <li>Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0)</li> </ul>		
	Oracle Identity Manager 11g Release 2 (11.1.2.0.0) or later		
	<ul> <li>Oracle Identity Manager 11g Release 1 (11.1.1.5.0) BP06 or later</li> </ul>		



Item	Requirement
Target systems	<ul> <li>The target system can be any one of the following:</li> <li>PeopleSoft Campus Solutions Maintenance Pack 9.0 Bundle 27 with PeopleTools 8.50</li> <li>PeopleSoft Campus Solutions Maintenance Pack 9.0 with PeopleTools 8.51</li> <li>PeopleSoft Campus Solutions Maintenance Pack 9.0 with PeopleTools 8.52</li> <li>PeopleSoft Campus Solutions Maintenance Pack 9.0 with PeopleTools 8.53</li> <li>PeopleSoft Campus Solutions Maintenance Pack 9.2 with PeopleTools 8.54</li> <li>PeopleSoft Campus Solutions Maintenance Pack 9.2 with PeopleTools 8.55</li> <li>PeopleSoft Campus Solutions Maintenance Pack 9.2</li> </ul>
0	with PeopleTools 8.56
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 or later, or JRockit 1.6 or later
Other software	You must ensure that the following components are installed and configured in the target system environment
	<ul> <li>Tuxedo and Jolt (the application server)</li> <li>PeopleSoft Internet Architecture</li> <li>PeopleSoft Application Designer (2-tier mode)</li> <li>The following standard PeopleSoft messages are available:</li> <li>SCC_CONSITTUENT_SYNC</li> </ul>

Table 1-1	(Cont.) C	Certified	Components
-----------	-----------	-----------	------------

# **1.2 Connector Architecture**

Figure 1-1 shows the architecture of the connector.



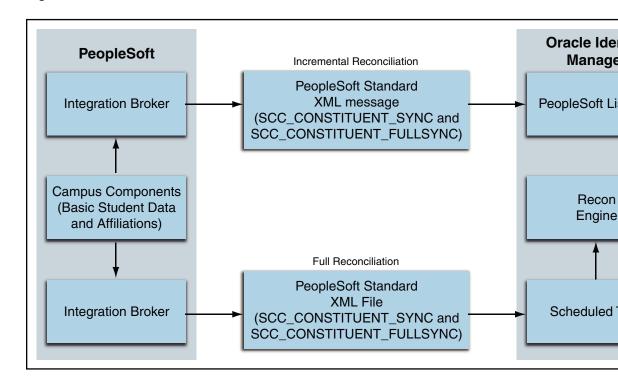


Figure 1-1 Architecture of the Connector

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

The connector reconciles basic student (person) data and affiliations into Oracle Identity Manager. Basic student data is used in Oracle Identity Manager to create the necessary identities. Affiliations are used to define access policies. Student academic program data is not reconciled into Oracle Identity Manager.

Figure 1-2 shows how data is stored in Oracle Identity Manager.



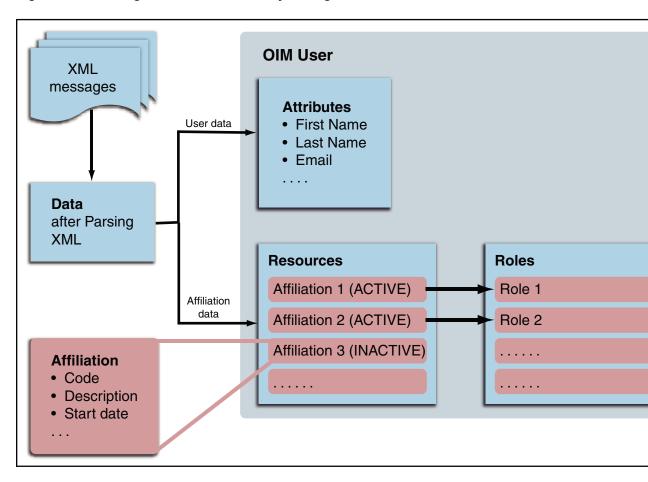


Figure 1-2 Storing Data in Oracle Identity Manager

The data is obtained after parsing the XML messages (which can be SCC\_CONSTITUENT\_FULLSYNC or SCC\_CONSTITUENT\_SYNC messages) received from the target system. This data contains both the user data (such as First Name and Email) and the affiliation data (such as Affiliation Code and Affiliation Start Date).

The user data is stored in the OIM User form. The affiliation data goes into the Affiliation resource form.

In OIM, the affiliations are modeled as resources. The affiliation resource form has the following fields:

- Affiliation Code
- Affiliation Status
- Affiliation Description
- Affiliation Start Date
- Affiliation End Date
- Institution

Based on the values of the Affiliation Status and Affiliation Start Date fields, the affiliation resource is in Enabled or Disabled state. If the Affiliation Status is Active



and the current date lies between Affiliation Start Date and Affiliation End Date, then the resource is in Enabled state. Otherwise, the resource is in Disabled state.

The roles are created in Oracle Identity Manager corresponding to each unique affiliation. For more information about the roles, see Seeding Roles into Oracle Identity Manager. For each enabled affiliation, the corresponding role is assigned to the user. This enables the use of access policies based on the type of affiliations that the user has.

# 1.3 Medium of Data Interchange

Standard PeopleSoft XML files and messages are the medium of data interchange between PeopleSoft Campus and Oracle Identity Manager. The method by which person data is sent to Oracle Identity Manager depends on the type of reconciliation that you configure. It is listed as follows:

- Full Reconciliation
- Incremental Reconciliation

## 1.3.1 Full Reconciliation

#### Note:

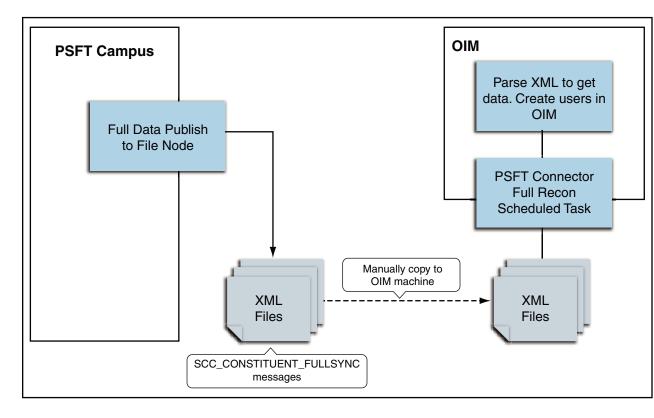
To reconcile all existing target system records into Oracle Identity Manager, you must run full reconciliation the first time you perform a reconciliation run after deploying the connector. This is to ensure that the target system and Oracle Identity Manager contain the same data.

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

Figure 1-3 shows full reconciliation between PeopleSoft Campus and Oracle Identity Manager.







Full reconciliation involves the following steps:

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

- The PeopleSoft Integration Broker populates the XML files for the SCC\_CONSTITUENT\_FULLSYNC messages with all the person data, such as biographical information and student information.
- 2. Copy these XML files to a directory on the Oracle Identity Manager host computer.
- 3. Configure the PeopleSoft Campus Trusted Full Reconciliation scheduled task. The XML files are read by this scheduled task to generate reconciliation events.

#### 1.3.2 Incremental Reconciliation

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

Figure 1-4 shows incremental reconciliation between PeopleSoft Campus and Oracle Identity Manager.



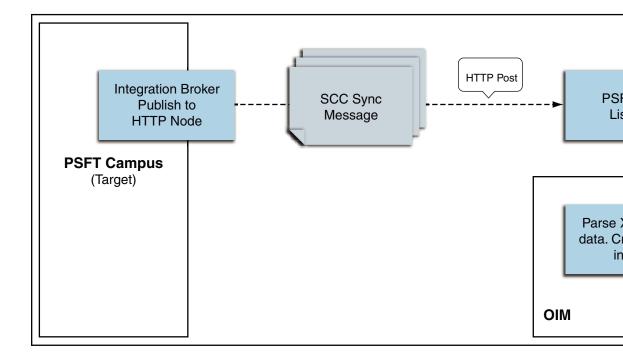


Figure 1-4 Incremental Reconciliation

Incremental reconciliation involves the following steps:

Performing Incremental Reconciliation describes the procedure to configure incremental reconciliation.

- **1.** When person data is added or updated in the target system, a PeopleCode event is generated.
- The PeopleCode event generates an XML message, SCC\_CONSTITUENT\_SYNC, containing the modified person data and sends it in real time to the PeopleSoft listener over HTTP. The PeopleSoft listener is a Web application that is deployed on an Oracle Identity Manager host computer. If SSL is configured, then the message is sent to the PeopleSoft listener over HTTPS.
- 3. The PeopleSoft listener parses the XML message and creates a reconciliation event in Oracle Identity Manager.

#### Note:

During connector deployment, the PeopleSoft listener is deployed as an EAR file.

# 1.4 Features of the Connector

The following are the features of the connector:

- Dedicated Support for Trusted Source Reconciliation
- Seeding Roles into Oracle Identity Manager



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

## 1.4.1 Dedicated Support for Trusted Source Reconciliation

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

## 1.4.2 Seeding Roles into Oracle Identity Manager

The connector supports seeding roles into Oracle Identity Manager corresponding to each unique affiliation in PeopleSoft Campus. This is done so that when a particular affiliation (a resource in Oracle Identity Manager) is assigned to a user, then if the affiliation is active, the corresponding role is assigned to the user. You can write access policies on those roles, which are access policies effectively based on affiliations such as student, prospect, employee, alumni, and so on. There is a separate scheduled task, called PeopleSoft Campus Role Creation, for seeding the roles into Oracle Identity Manager. You must run this task before using the connector for reconciliation. See Seeding Roles into Oracle Identity Manager for more information.

Figure 1-5 shows seeding PeopleSoft Campus roles in Oracle Identity Manager.



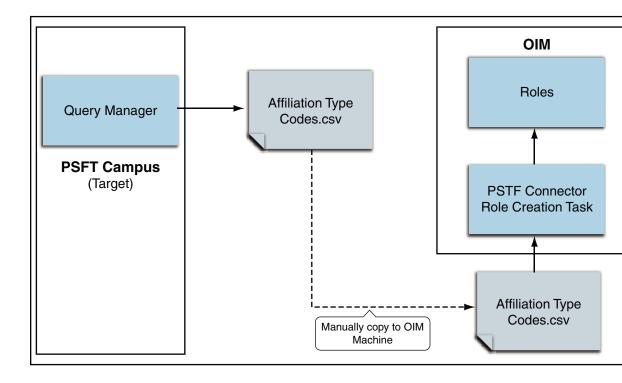


Figure 1-5 Seeding Roles in Oracle Identity Manager

#### 1.4.3 Full and Incremental Reconciliation

The connector supports reconciliation in two ways:

In a full reconciliation run, all records are fetched from the target system to Oracle Identity Manager in the form of XML files. In incremental reconciliation, records that are added or modified are directly sent to the listener deployed on the Oracle Identity Manager host computer. The listener parses the records and sends reconciliation events to Oracle Identity Manager.

## 1.4.4 Reconciliation of Effective-Dated Lifecycle Events

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

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

PeopleSoft uses two standard messages to reconcile a record. These are the SCC\_CONSTITUENT\_SYNC messages. See Support for Standard PeopleSoft Messages for more information about these messages.



You run the SCC\_CONSTITUENT\_SYNC message to create an OIM User. The default status of an OIM User is **Active**. See the **Employee Status** Code Key in the lookup definition described in Lookup.PSFT.Message.SccConstituentFullSync.Configuration.

#### Note:

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

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

#### 1.4.5 Support for Standard PeopleSoft Messages

PeopleSoft provides standard messages to send biographical data (Campus ID, Email ID, First Name, Last Name, Home Phone, User ID, and Start Date) and student-related data to external applications, such as Oracle Identity Manager. These messages also contain affiliation information (Affiliation Code, Affiliation Status, Affiliation Description, Affiliation Start Date, Affiliation End Date, and Institution). Affiliations are defined as the relationship between and an individual and an institution, such as STUDENT, PROSPECT, and so on. The connector uses the following standard PeopleSoft messages that are delivered as part of PeopleSoft Campus installation to achieve full reconciliation and incremental reconciliation:

SCC\_CONSTITUENT\_FULLSYNC

During full reconciliation, these messages are sent to Oracle Identity Manager.

SCC\_CONSTITUENT\_SYNC

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

#### Note:

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



## 1.4.6 Support for Resending Messages That Are Not Processed

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

If the connector is not able to process a message successfully, then it sends an error code and PeopleSoft Integration Broker marks that message as Failed. A message marked as Failed can be resent to the listener. See Resending Messages That Are Not Received by the PeopleSoft Listener for details.

#### See Also:

Resubmitting and Canceling Service Operations for Processing topic in the PeopleBook Enterprise PeopleTools 8.49 PeopleBook: PeopleSoft Integration Broker available on Oracle Technology Network:

http://download.oracle.com/docs/cd/E13292\_01/pt849pbr0/eng/
psbooks/tibr/book.htm

## 1.4.7 Validation and Transformation of Person Data

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

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

## 1.4.8 Target Authentication

Target authentication is done to validate whether Oracle Identity Manager should accept messages from the target system or not. It is done by passing the name of the IT resource in the Integration Broker node. You must ensure that the correct value of the IT resource name is specified in the node. See Configuring PeopleSoft Integration Broker for setting up the node. In addition, the flag IsActive is used to verify whether the IT Resource is active or not. The value of this flag is Yes, by default. When this value is Yes, target authentication is carried out. Target authentication fails if it is set to No.

# 1.4.9 Support for Specifying Persons to Be Excluded from Reconciliation Operation

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



# 1.5 Connector Objects Used During Reconciliation

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

#### See Also:

Reconciliation Metadata in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for conceptual information about trusted source reconciliation.

This section discusses the following topics:

- Reconciliation Rules
- Reconciliation Action Rules
- Predefined Lookup Definitions

### 1.5.1 Reconciliation Rules

#### 🖍 See Also:

Reconciliation Engine in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager for generic information about reconciliation matching and action rules

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

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

#### 1.5.1.1 Overview of the Reconciliation Rule

The following are the process-matching rules:

Rule Name: PeopleSoft Campus Reconciliation Rule

Rule Name: PSFT Campus Affiliation Rule

Rule Element: User Login Equals User ID

In this rule:

- User Login represents the User ID field on the OIM User form.
- User ID represents the Employee ID field of the employee on the target system.



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

#### 1.5.1.2 Viewing the Reconciliation Rule in the Design Console

After you deploy the connector, you can view the reconciliation rule by performing the following steps:

#### Note:

Perform the following procedure only after the connector is deployed.

- **1.** Log in to the Oracle Identity Manager Design Console.
- 2. Expand Development Tools.
- 3. Double-click Reconciliation Rules.
- 4. Search for and open **PSFT Campus.** Figure 1-6 shows this reconciliation rule and Figure 1-7 shows affiliation reconciliation rule.

Figure 1-6 Reconciliation Rule

Reconciliation	Rule Builder
Name	Peoplesoft Campus Recon F Valid
Object	Peoplesoft Campus       Active
	For User O For Organization
Description	Peoplesoft Campus Reconciliation Rule
Rule Elements	
-Rule Definition	1
Add <u>R</u> ule	📳 Rule: Peoplesoft Campus Recon Rule
Add Rul <u>e</u> Elei	ment User Login Equals User ID
<u>D</u> elete	
<u>L</u> egend	



_					
	– Reconciliation Rule Builder				
		itait bai			
	Name	PSET Ca	mpus Affiliation Rul	Operator	✓ Valid
					In a la cana
	Object	Affiliatio	on	🖲 AND 🔾 OR	🖌 Active
		🔘 For l	User 🔿 For Organia	zation	
	Description	PSFT Car	mpus Affiliation Rule		
L					
ſ	Rule Elements	1			
ŕ					
	-Rule Definition	1			
	Add Rule		📳 Rule: PSFT Campus	s Affiliation Rule	
	Add <u>R</u> ule	-			
	Add Rule Element				
	_				
	<u>D</u> elete				
	Legend				

Figure 1-7 Affiliation Reconciliation Rule

## 1.5.2 Reconciliation Action Rules

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

#### Note:

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

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

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

#### 1.5.2.1 Overview of the Reconciliation Action Rules

Table 1-2 lists the reconciliation action rules for this connector:

#### Table 1-2 Action Rules for Trusted Source Reconciliation

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



#### 1.5.2.2 Viewing the Reconciliation Action Rules in the Design Console

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

#### Note:

Perform the following procedure only after the connector is deployed.

- **1.** Log in to the Oracle Identity Manager Design Console.
- 2. Expand Resource Management.
- 3. Double-click Resource Objects.
- 4. Search for and open the PeopleSoft Campus resource object.
- Click the Object Reconciliation tab and then the Reconciliation Action Rules tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1-8 shows these reconciliation action rules.

	2 8 ×			
Oracle Identity Manager Design Consc	Resource	Object Object Reconciliati	on	
Oser Management     Resource Management	Object Initial	Reconciliation Date		
IT Resources Type Definition	Reconcilia	ation Fields Reconciliation	Action Rules	
Rule Designer	Add	Rule Condition	Action	User
Resource Objects	Delete	1 No Matches Found	Create User	
Process Management	Peiere	2 One Entity Match Found	Establish Link	

Figure 1-8 Reconciliation Action Rules



## 1.5.3 Predefined Lookup Definitions

The predefined lookup definitions can be categorized as follows:

- Lookup.PSFT.Campus.Configuration
- Lookup Definitions Used to Process SCC\_CONSTITUENT\_FULLSYNC Messages
- Lookup Definitions Used to Process SCC\_CONSTITUENT\_SYNC Messages
- Lookup.PSFT.Campus.CustomQuery
- Lookup.PSFT.Campus.ExclusionList

#### 1.5.3.1 Lookup.PSFT.Campus.Configuration

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

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

Code Key	Decode	Description
Campus Resource Exclusion List Lookup	Lookup.PSFT.Campus.ExclusionL ist	Name of the Resource Exclusion lookup for PeopleSoft Campus
		See Lookup.PSFT.Campus.Exclu sionList for more information about this lookup definition.
Ignore Root Audit Action	No	Use this value if the Root PSCAMA audit action is required to be considered while parsing the XML message.
		Enter Yes if PSCAMA Audit Action is not taken into account. Here, the Root Audit Action is considered as a Change event.
		Enter No if PSCAMA Audit Action is taken into account. If Root PSCAMA Audit Action is NULL or Empty, then the Root Audit Action is considered as an ADD event.
		See Also: Determining the Root Audit Action Details



Code Key	Decode	Description
SCC_CONSTITUENT_FUL LSYNC	Lookup.PSFT.Message.SccConsti tuentFullSync.Configuration	Name of the lookup definition for SCC_CONSTITUENT_FULL SYNC message
		See Lookup.PSFT.Message.SccC onstituentFullSync.Configurat ion for more information about this lookup definition.
SCC_CONSTITUENT_SYN C.v1	Lookup.PSFT.Message.SccConsti tuentSync.Configuration	Name of the lookup definition for SCC_CONSTITUENT_SYNC message
		See Lookup.PSFT.Message.SccC onstituentSync.Configuration for more information about this lookup definition.
Target Date Format	yyyy-MM-dd	Data format of the Date type data in the XML file and messages Do <i>not</i> modify this value.

You can configure the message names, such as the SCC\_CONSTITUENT\_SYNC and SCC\_CONSTITUENT\_FULLSYNC defined in this lookup definition. Setting Up the Lookup.PSFT.Campus.Configuration Lookup Definition describes the procedure to configure these message names.

1.5.3.2 Lookup Definitions Used to Process SCC\_CONSTITUENT\_FULLSYNC Messages

The following lookup definitions are used to process SCC\_CONSTITUENT\_FULLSYNC messages:

#### 1.5.3.2.1 Lookup.PSFT.Message.SccConstituentFullSync.Configuration

The Lookup.PSFT.Message.SccConstituentFullSync.Configuration lookup definition provides the configuration-related information for the SCC\_CONSTITUENT\_FULLSYNC messages.

The lookup definition has the following entries:

Code Key	Decode	Description
Affiliation Resource Object	Affiliation	Name of the Affiliation Resource Object



Code Key	Decode	Description
Affiliations	Affiliation Code~Affiliation Status~Affiliation Description~Affiliation Start Date~Affiliation End Date~Institution	The code key value should be the same as the decode key value for the Affiliation Attribute Name entry (the next entry in this table). The decode key value lists all the attributes which are part of the Affiliation Resource form. The values should be separated by tilde (~) character. If a new affiliation attribute has to be added for reconciliation, the new attribute must be added to this decode key value.
Affiliations Attribute Name	Affiliations	Name of the Affiliations Attribute Default value: Affiliations
Attribute Mapping Lookup	Lookup.PSFT.Campus.SccCo nstituentFullSync.AttributeMa pping	Name of the lookup definition that maps Oracle Identity Manager attributes with the attributes in the SCC_CONSTITUENT_FULLSY NC message XML See Lookup.PSFT.Campus.SccConst tuentFullSync.AttributeMapping for more information about this lookup definition.
Custom Query	Enter a Value	If you want to implement limited reconciliation, then enter the query condition that you create by following the instructions given in the Limited Reconciliation.
Custom Query Lookup Definition	Lookup.PSFT.Campus.Custo mQuery	This entry holds the name of the lookup definition that maps resource object fields with OIM User form fields. This lookup definition is used during application of the custom query. See Limited Reconciliation for more information.
Data Node Name	Transaction	Name of the node in the XML files to execute a transaction Default value: Transaction
		You must not change the default value.
Employee Status	Enabled	Default status of an employee during the creation of an OIM User
		<b>Note:</b> You can change the status to Disabled, if you want the status to be Inactive when the OIM User is created.



Code Key	Decode	Description
Message Handler Class	oracle.iam.connectors.psft.co mmon.handler.impl.PSFTCa mpusSyncReconMessageHa ndlerImpl	Name of the Java class that accepts the XML payload, configuration information, and a handle to Oracle Identity Manager. Depending on the message type, it retrieves the appropriate configuration from Oracle Identity Manager and processes the message. To parse a specific message type, it relies on a Message Parser factory. If you want a customized
		implementation of the message, then you must extend the MessageHandler.java class.
Message Parser	oracle.iam.connectors.psft.co mmon.parser.impl.CampusM essageParser	Name of the parser implementation class that contains the logic for message parsing
		If you want a customized implementation of the message then you must extend the MessageParser.java class.
Organization	Xellerate Users	Default organization in Oracle Identity Manager
Recon Lookup Definition	Lookup.PSFT.Campus.SccCo nstituentSync.Recon	Name of the lookup definition that maps Oracle Identity Manager attributes with the Resource Object attributes See Lookup.PSFT.Campus.SccCons tuentSync.Recon for more information about this lookup definition.
Resource Object	PeopleSoft Campus	Name of the resource object
Transformation Lookup Definition	Lookup.PSFT.Campus.SccCo nstituentSync.Transformation	lookup definition See Configuring Transformation
		of Data During Reconciliation fo more information about adding entries in this lookup definition.
		<b>Note:</b> The default value for transformation lookups for both SCC_CONSTITUENT_SYNC and
		SCC_CONSTITUENT_FULLSY NC messages is the same.
		You can use different lookups by changing the decode key value.



Code Key	Decode	Description
User Type	End-User	It specifies the value with which a person is created in Oracle Identity Manager using the SCC_CONSTITUENT_FULLSY NC message.
Use Transformation	No	Enter yes to implement transformation while reconciling records. Otherwise, enter no.
Use Validation	No	Enter yes to implement validation while reconciling records. Otherwise, enter no.
Validation Lookup Definition	Lookup.PSFT.Campus.SccCo nstituentSync.Validation	Name of the validation lookup definition
		See Configuring Validation of Data During Reconciliation for more information about adding entries in this lookup definition.
		Note: The default value for validation lookups for both SCC_CONSTITUENT_SYNC and SCC_CONSTITUENT_FULLSY NC messages is the same.
		You can use different lookups by changing the decode key value.

#### 1.5.3.2.2 Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping

The Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping lookup definition maps OIM User attributes with the attributes defined in the SCC\_CONSTITUENT\_FULLSYNC message.

The Decode entries of this lookup definition are based on the message structure shown in Message Structure. All full data publish XML files contain this message structure at the beginning of the files. If the message structure changes (if the node names in the XML file are different), then the Decode entries in the lookup definition need to be updated as per the new message structure.

The following table provides the format of the values stored in this lookup definition:

Code Key	Decode
Affiliation Code	SCC_AFL_CODE~SCC_AFL_PERSON~None~None~RESOURCE= Affiliations
Affiliation Description	SCC_AFL_STS_DESCR~SCC_AFL_PERSON~None~None~RESOU RCE=Affiliations
Affiliation End Date	END_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliation s
Affiliation Start Date	START_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliati ons



Code Key	Decode
Affiliation Status	SCC_AFL_STATUS~SCC_AFL_PERSON~None~None~RESOURCE =Affiliations
Campus ID	CAMPUS_ID~PERSON_SA
Email	EMAIL_ADDR~SCC_PER_EMAIL_I
First Name	FIRST_NAME~SCC_PER_NAME_I2~NAME_TYPE=PRI~EFFDT
Home Phone	PHONE~SCC_PER_PHONE_I
Institution	INSTITUTION~SCC_AFL_PERSON~None~None~RESOURCE=Affili ations
Last Name	LAST_NAME~SCC_PER_NAME_I2~NAME_TYPE=PRI~EFFDT
Start Date	EFFDT~SCC_PER_NAME_I2~None~EFFDT
User ID	EMPLID~SCC_CM_PERSON_I~None~None~PRIMARY

Code Key: Name of the OIM User field

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

NODE~PARENT NODE~TYPE NODE=Value~EFFECTIVE DATED NODE~PRIMARY or RESOURCE=Resource Name

In this format:

NODE: Name of the node in the SCC\_CONSTITUENT\_SYNC message XML file from which the value is read. You must specify the name of the NODE in the lookup definition. It is a mandatory field.

PARENT NODE: Name of the parent node for the NODE. You must specify the name of the parent node in the lookup definition. It is a mandatory field.

TYPE NODE=Value: Type of the node associated with the Node value. Value defines the type of the Node.

For example, in the SCC\_CONSTITUENT\_SYNC message, the rowset NAME\_TYPE\_VW lists the names assigned to a person. The names assigned could be primary, secondary, or nickname, depending on how it is configured in PeopleSoft.

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

FIRST\_NAME~NAMES~NAME\_TYPE=PRI~EFFDT

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

The NAME\_TYPE node with PRI value is shown in the following screenshot:



) 🚅 🚽 🕺 🖻 💼 🗠 어 어 👬 😫 🏎 들	🗖 🦉 🚛 🜉 📮 xml->SCC_CONSTITUENT_DS->MsgData->Transaction(2)->SCC_CM_PERSON_I->NAME_TY
	191 <dt_of_death></dt_of_death>
	192 <name_type_vw2 class="R"></name_type_vw2>
±KTS BIRTHDATE	193 <emplid ischanged="Y">EXCLUDE2</emplid>
	194 <name_type lschanged="Y">PRI</name_type>
	195 <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre>ORDER_BY_SEQ IsChanged="Y"&gt;1</pre>
	196 SCC_PER_NAME_I class="R">
	197 CEMPLID IsChanged="Y">EXCLUDE2
	198 <name_type ischanged="Y">PRI</name_type>
ia w NAME_TYPE_VW2	199 <effdt ischanged="Y">2000-01-01</effdt>
	200 <eff_status ischanged="Y">A</eff_status>
EMPLID	201 <country_nm_format ischanged="Y">001</country_nm_format>
AME_TYPE	202 <name ischanged="Y">last2,Joshua</name>
- IsChanged = "Y"	203 <name_initials>/NAME_INITIALS&gt;</name_initials>
	204 <name_prefix ischanged="Y">Mr</name_prefix> 205 <name_suffix></name_suffix>
	205 <name_suffix></name_suffix> 206 <name_royal_prefix></name_royal_prefix>
E-<>SCC_PER_NAME_I	207 <name_royal_prefix></name_royal_prefix>
- E class = "R"	208 <name_itile></name_itile>
ti di tanàn amin'ny fisiana a	209 <last name_srchischanged="Y">EASTON</last>
I I I I I I I I I I I I I I I I I I I	210 <first_name_srch ischanged="Y">JOSHUA</first_name_srch>
tiere the second secon	211 <last_name ischanged="Y">last2</last_name>
EFF_STATUS	212 <first_name ischanged="Y">Joshua</first_name>
	213 <middle name=""></middle>
ti- ti- <ti>↓</ti>	214 <second last="" name=""></second>
NAME_INITIALS	215 <second last="" srch=""></second>
THAT NAME_PREFIX	216 <name ac=""></name>
NAME SUFFIX	217 <pref first="" name=""></pref>
NAME ROYAL PREF	218 <partner last="" name=""></partner>
NAME ROYAL SUFF	219 <partner prefix="" roy=""></partner>
NAME TITLE	220 <last ischanged="Y" name="" nld="" pref="">1</last>
EKT LAST NAME SRCH	221 <name_display ischanged="Y">Joshua last2</name_display>
FIRST_NAME_SRCH	222 <name_formal ischanged="Y">Mr Joshua last2</name_formal>
LAST NAME	223 <name_display_srch ischanged="Y">JOSHUAEASTON</name_display_srch>
	224
	225 <pscama class="R"></pscama>
	226 <audit_actn ischanged="Y">A</audit_actn>
SECOND_LAST_NAM	227
	228
NAME_AC	229 <pscama class="R"></pscama>
	230 <audit_actn ischanged="Y">A</audit_actn>
	231
Tree View 0 warning(s), 0 error(s)	<pre>232 <address_type_v2 class="R"></address_type_v2></pre>
,	233

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

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

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

The EFFDT node is shown in the following screenshot:



🗅 🚅 🖬 🐰 🖻 💼 🗠 બ 🛤 🔄 🛶 1		🔳 💂 🔽 🛛 xml->SCC_CONSTITUENT_DS->MsgData->Transaction(2)->SCC_CM_PERSON_I-
	191	<pre></pre>
	192	<name_type_vw2 class="R"></name_type_vw2>
	193	<emplid ischanged="Y">EXCLUDE2</emplid>
	194	<name_type ischanged="Y">PRI</name_type>
> BIRTHPLACE	195	<pre><order_by_seq lschanged="Y">1</order_by_seq></pre>
BIRTHCOUNTRY	196	<scc_per_name_i class="R"></scc_per_name_i>
> BIRTHSTATE	197	<emplid ischanged="Y">EXCLUDE2</emplid>
> DT_OF_DEATH	198	<name_type ischanged="Y">PRI</name_type>
E NAME_TYPE_VW2	199	<effdt ischanged="Y">2000-01-01</effdt>
- E class = "R"	200	EFF_STATUS IsChanged="Y">A
ti-     tip-     tip- <t< td=""><td>201</td><td><country_nm_format ischanged="Y">001</country_nm_format></td></t<>	201	<country_nm_format ischanged="Y">001</country_nm_format>
□ □ <t name_type<="" td=""><td>202</td><td><name ischanged="Y">last2,Joshua</name></td></t>	202	<name ischanged="Y">last2,Joshua</name>
- IsChanged = "Y"	203	<name_initial s=""></name_initial>
	204	<name_prefix ischanged="Y">Mr</name_prefix>
	205	<name_suffix></name_suffix>
	206	<name_royal_prefix></name_royal_prefix>
Lass = "R"	207	<name_royal_suffix></name_royal_suffix>
	208	<name_title></name_title>
	209	<last_name_srch ischanged="Y">EASTON</last_name_srch>
EFFDT	210	<first_name_srch ischanged="Y">JOSHUA</first_name_srch>
	211	<last_name ischanged="Y">last2</last_name>
	212	<first_name ischanged="Y">Joshua</first_name>
terts NAME	213	<middle_name></middle_name>
	214	<second_last_name></second_last_name>
	215	<second_last_srch></second_last_srch>
	216	<name_ac></name_ac>
NAME_SUFFIX	217	<pref_first_name></pref_first_name>
NAME_ROYAL_PREF	218	<partner_last_name></partner_last_name>
NAME_ROYAL_SUFF	219	<partner_roy_prefix></partner_roy_prefix>
NAME_TITLE	220	<last_name_pref_nld changed="Y" is="">1</last_name_pref_nld>
EAST_NAME_SRCH	221	<name_display ischanged="Y">Joshua last2</name_display>
FIRST_NAME_SRCH	222	<name_formal ischanged="Y">Mr Joshua last2</name_formal>
EAST_NAME	223	<pre><name_display_srch ischanged="Y">JOSHUAEASTON</name_display_srch></pre>
	224	
MIDDLE_NAME	225	<pscama class="R"></pscama>
SECOND_LAST_NAM	226 227	<audit_actn ischanged="Y">A</audit_actn>
SECOND_LAST_SRC	227	 
	228	<pscama class="R"></pscama>
PREF_FIRST_NAME	229	<pscama class="R"> <audit_actn ischanged="Y">A</audit_actn></pscama>
	230	
	231	 <address_type_v2 class="R"></address_type_v2>
Tree View 🛛 🔽 0 warning(s), 0 error(s)	232	<emplid ischanged="Y">EXCLUDE2</emplid>
able Ostastina Desuran	233	<address_type ischanged="Y">HOME</address_type>
able Selection Browser	234	<pre><abbress_fifeeischanged=fifemes abbress_fifeeischanged="fifemes/Abbress_fifeeischanged=fifemes/Abbress_fifeeischanged=fifemes/Abbress_fifeeischanged=fifemes/Abbress_fifeeischanged=fifemes/Abbress_fifeeischanged=fifemes/Abbress_fifeeischanged=fifemes/Abbress_fifeeischanged=fifemes/Abbress_fifeeischanged=fifemes/Abbress_fifeeischanged=fifemes/Abbress_fifeeischanged=fifeeischan&lt;/td"></abbress_fifeeischanged=fifemes></pre>
This Tree Coloction Browcer is empty	200	-onben_br_seq roonanged= r - r -onben_br_seq.

Primary or RESOURCE=Resource Name: Specifies if the node is a mandatory field or a resource field. For example, in case of a resource field, RESOURCE=Affiliations specifies that it is a field in the Affiliations resource object.

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

If you want to retrieve the value for the Code Key, First Name, then the name of the NODE will be FIRST\_NAME as depicted in the XML file. See the sample XML file in Figure 1-9 for more information about each node in the SCC\_CONSTITUENT\_SYNC message.



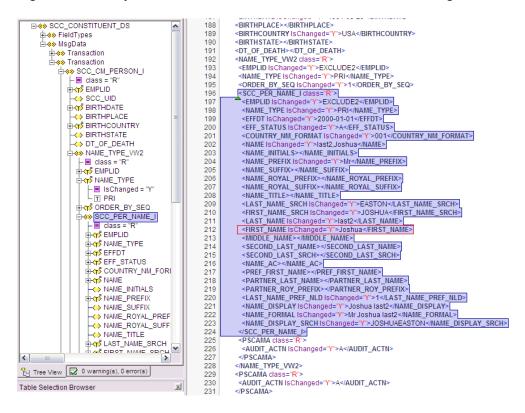


Figure 1-9 Sample XML File for SCC\_CONSTITUENT\_SYNC Message

The PARENT NODE for the NODE FIRST\_NAME will be SCC\_PER\_NAME\_I. Now suppose, you have a scenario where you have multiple FIRST\_NAME nodes in the XML file to support the effective-dated feature for this attribute. In this case, you must identify the TYPE NODE for the PARENT NODE that has the value PRI. In this example, the TYPE NODE is NAME\_TYPE with the value PRI.

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

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

If you do not want to provide any element in the Decode column, then you must specify None. This is implemented for the User ID attribute.

Now, you can concatenate the various elements of the syntax using a tilde (~) to create the Decode entry for First Name as follows:

NODE: FIRST\_NAME

PARENT NODE: SCC\_PER\_NAME\_I

TYPE NODE=Value: NAME\_TYPE=PRI

EFFECTIVE DATED NODE: EFFDT

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

FIRST\_NAME~SCC\_PER\_NAME\_I~NAME\_TYPE=PRI~EFFDT



# 1.5.3.3 Lookup Definitions Used to Process SCC\_CONSTITUENT\_SYNC Messages

The following lookup definitions are used to process the SCC\_CONSTITUENT\_SYNC messages:

# 1.5.3.3.1 Lookup.PSFT.Message.SccConstituentSync.Configuration

The Lookup.PSFT.Message.SccConstituentSync.Configuration lookup definition provides the configuration-related information for the SCC\_CONSTITUENT\_SYNC messages for reconciliation.

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

Code Key	Decode	Description
Affiliation Resource Object	Affiliation	Name of the Affiliation Resource Object
Affiliations	Affiliation Code~Affiliation Status~Affiliation Description~Affiliation Start Date~Affiliation End Date~Institution	The code key value should be the same as the decode key value for the Affiliation Attribute Name entry (the next entry in this table). The decode key value lists all the attributes which are part of the Affiliation Resource form. The values should be separated by tilde (~) character. If a new affiliation attribute has to be added for reconciliation, the new attribute must be added to this decode key value.
Affiliations Attribute Name	Affiliations	Name of the Affiliations Attribute
Attribute Mapping Lookup	Lookup.PSFT.Campus.SccCo nstituentSync.AttributeMappi ng	Name of the lookup definition that maps Oracle Identity Manager attributes with attributes in the SCC_CONSTITUENT_SYNC message XML
		See Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping for more information about this lookup definition.
Custom Query	Enter a Value	If you want to implement limited reconciliation, then enter the query condition that you create by following the instructions given in Limited Reconciliation.



Code Key	Decode	Description
Custom Query Lookup Definition	Lookup.PSFT.Campus.Custo mQuery	This entry holds the name of the lookup definition that maps resource object fields with OIM User form fields. This lookup definition is used during application of the custom query. See Limited Reconciliation for more information.
Data Node Name	Transaction	Name of the node in the XML files to run a transaction
Employee Status	Enabled	Default status of an employee during the creation of an OIM User
		<b>Note:</b> You can change the status to Disabled, if you want the status to be Inactive when the OIM User is created.
Message Handler Class	oracle.iam.connectors.psft.co mmon.handler.impl.PSFTCa mpusSyncReconMessageHa ndlerImpl	Name of the Java class that accepts the XML payload, configuration information, and a handle to Oracle Identity Manager. Depending on the message type, it retrieves the appropriate configuration from Oracle Identity Manager and processes the message. To parse a specific message type, it relies on a Message Parser factory.
		If you want a customized implementation of the message, then you must extend the MessageHandler.java class.
Message Parser	oracle.iam.connectors.psft.co mmon.parser.impl.CampusM essageParser	Name of the parser implementation class that contains the logic for message parsing
		If you want a customized implementation of the message, then you must extend the MessageParser.java class.
Organization	Xellerate Users	Default organization in Oracle Identity Manager
Recon Lookup Definition	Lookup.PSFT.Campus.SccCo nstituentSync.Recon	Name of the lookup definition that maps Oracle Identity Manager attribute with Resource Object attribute See Lookup.PSFT.Campus.SccConst tuentSync.Recon for more
		information about this lookup definition.



Code Key	Decode	Description
Transformation Lookup Definition	Lookup.PSFT.Campus.SccCo nstituentSync.Transformation	Name of the transformation lookup definition
		It is empty by default.
		Note: The default value for transformation lookups for both SCC_CONSTITUENT_SYNC and SCC_CONSTITUENT_FULLSY NC messages is the same.
		You can use different lookups b changing the decode key value
User Type	End-User	It specifies the value with which a person is created in Oracle Identity Manager using the SCC_CONSTITUENT_SYN message.
Use Transformation	No	Enter yes to implement transformation while reconciling records. Otherwise, enter no.
Use Validation	No	Enter yes to implement validation while reconciling records. Otherwise, enter no.
Validation Lookup Definition	Lookup.PSFT.Campus.SccCo nstituentSync.Validation	Name of the validation lookup definition
		It is empty by default.
		Note: The default value for validation lookups for both SCC_CONSTITUENT_SYNC and SCC_CONSTITUENT_FULLS' NC messages is the same.
		You can use different lookups b changing the decode key value

# 1.5.3.3.2 Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping

The Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping lookup definition maps OIM User attributes with the attributes defined in the SCC\_CONSTITUENT\_SYNC message XML. The following is the format of the values stored in this lookup definition:

Code Key	Decode
Affiliation Code	SCC_AFL_CODE~SCC_AFL_PERSON~None~None~RESOURCE=A ffiliations
Affiliation Description	SCC_AFL_STS_DESCR~SCC_AFL_PERSON~None~None~RESOU RCE=Affiliations
Affiliation End Date	END_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations
Affiliation Start Date	START_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliatio ns



Code Key	Decode
Affiliation Status	SCC_AFL_STATUS~SCC_AFL_PERSON~None~None~RESOURCE= Affiliations
Campus ID	CAMPUS_ID~PERSON_SA
Email	EMAIL_ADDR~SCC_PER_EMAIL_I
First Name	FIRST_NAME~SCC_PER_NAME_I~NAME_TYPE=PRI~EFFDT
Home Phone	PHONE~SCC_PER_PHONE_I
Institution	INSTITUTION~SCC_AFL_PERSON~None~None~RESOURCE=Affilia tions
Last Name	LAST_NAME~SCC_PER_NAME_I~NAME_TYPE=PRI~EFFDT
Start Date	EFFDT~SCC_PER_NAME_I~None~EFFDT
User ID	EMPLID~SCC_CM_PERSON_I~None~None~PRIMARY

For the description and format of the Code Key and Decode entries, see Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping.

# 1.5.3.3.3 Lookup.PSFT.Campus.SccConstituentSync.Recon

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

Code Key	Decode
Affiliation Code	Affiliation Code~None~Resource
Affiliation Description	Affiliation Description~None~None~Resource
Affiliation End Date	Affiliation End Date~None~None~Resource
Affiliations	Affiliations
Affiliation Start Date	Affiliation Start Date~None~None~Resource
Affiliation Status	Affiliation Status~None~None~Resource
Campus ID	Campus ID
Effective Start Date	Start Date
Email	Email
First Name	First Name
Home Phone	Home Phone
Institution	Institution~None~None~Resource
Last Name	Last Name
User ID	User ID
User Type	User Type

Code Key: Name of the resource object field in Oracle Identity Manager Decode: Combination of the following elements separated by a tilde (~) character: ATTRIBUTE~LOOKUP DEF~LKF~Resource



In this format:

ATTRIBUTE: Refers to the Code Key of the Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping lookup definition

LOOKUP DEF: If the field is not a resource field, provide the value for ATTRIBUTE. If it is a resource field, provide None for LOOKUP DEF and LKF as they are not used in PeopleSoft Campus.

Resource: It indicates that this field is a resource field, which is an Affiliation form field.

In the following example, if the field is a user form field, such as Email, then:Code Key: Email

This is the resource object field name.Decode: Email

This is the Code Key entry in the attribute mapping lookup definition.

In the following example, if the field is an Affiliations resource form field, such as Affiliation Code, then:Code Key: Affiliation Code

Decode: Affiliation Code~None~Resource

The two values in the middle are None because they are not used in this connector. However, they are used in the PeopleSoft Employee Reconciliation and PeopleSoft User Management connectors.

# 1.5.3.4 Lookup.PSFT.Campus.CustomQuery

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

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

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

Code Key: Resource object field name

Decode: Column name of the USR table

Code Key	Decode	
Campus ID	USR_UDF_CAMPUS_ID	
Effective Start Date	Users.Start Date	
Email	Users.Email	
First Name	Users.First Name	
Last Name	Users.Last Name	
User ID	Users.User ID	



# 1.5.3.5 Lookup.PSFT.Campus.ExclusionList

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

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

Code Key: User ID resource object field name

Decode: List of user IDs separated by the pipe character (|)

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

# 1.6 Roadmap for Deploying and Using the Connector

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

- Deploying the Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Using the Connector provides information about the tasks that must be performed each time you want to run reconciliation.
- Extending the Functionality of the Connector describes procedures that you can perform to extend the functionality of the connector.
- Testing and Troubleshooting provides information about testing the connector.
- Determining the Root Audit Action Details provides information about root audit action.
- Setting Up SSL on Oracle WebLogic Server describes how to configure SSL on Oracle WebLogic Server for PeopleTools.
- Message Structure contains the message structure that is part of all full data publish XML files.



# 2 Deploying the Connector

Deploying the connector involves the following steps:

## Note:

In this guide, PeopleSoft Campus is referred to as the target system.

- Preinstallation
- Installation
- Postinstallation
- Postcloning Steps

# 2.1 Preinstallation

Preinstallation information is divided across the following sections:

- Determining the Version of PeopleTools and the Target System
- Files and Directories on the Installation Media
- Preinstallation on the Target System

# 2.1.1 Determining the Version of PeopleTools and the Target System

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

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

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

For example:

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

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

# 2.1.2 Files and Directories on the Installation Media

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



File in the Installation Media Directory	Description
configuration/PSFT_Campus_Reconciliation- Cl.xml	This XML file contains configuration information that is used during connector installation.
javadoc	This directory contains information about the Java APIs used by the connector.
lib/PSFT_CS-oim-integration.jar	This JAR file contains the class files that are specific to integration of the connector with PeopleSoft target systems.
	During connector deployment, this file is copied to the Oracle Identity Manager database.
lib/PSFTCommon.jar	This JAR file contains PeopleSoft-specific files common to Campus, Employee Reconciliation, and User Management versions of the connector.
	During connector deployment, this file is copied to the Oracle Identity Manager database.
The following files and directories in the listener directory: base directory lib/deploytool.jar	The base directory contains the class files for the PeopleSoftOIMListener.ear file. This Enterprise Archive (EAR) file contains one or more entries representing the modules of the Web application to be deployed onto an application server.
build.xml deploy.properties README.txt	During connector deployment, the PeopleSoft listener is deployed as an EAR file.
	The deploytool.jar file contains the class files required for deploying the listeners.
	The build.xml file is the deployment script, which contains configurations to deploy the listener.
	The deploy.properties file contains Oracle Identity Manager connection details.
	The README.txt file contains instructions to deploy, remove, and redeploy the listener.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector.
	During connector deployment, this file is copied to the Oracle Identity Manager database.
	<b>Note:</b> A <b>resource bundle</b> is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
test/config/log.properties	These files are used by the InvokeListener.bat file. The reconConfig.properties file contains configuration information for
test/config/reconConfig.properties	running the InvokeListener.bat file. The log.properties file contains logger information.
test/lib/PSFTTest.jar	This JAR file is used by the testing utility for reconciliation.
test/scripts/InvokeListener.bat	This BAT file and the UNIX shell script call the testing utility for
test/scripts/InvokeListener.sh	reconciliation.

## Table 2-1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
xml/PeoplesoftCampus-ConnectorConfig.xml	This XML file contains definitions for the connector components.
	Resource object
	Process definition
	IT resource type
	Reconciliation rules
	Scheduled tasks
	Lookup definitions

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

# 2.1.3 Preinstallation on the Target System

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

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

The preinstallation steps consist of creating a user account with limited rights. Permission lists may contain any number of accesses, such as the Web libraries permission, Web services permissions, page permissions, and so on. You attach this permission list to a role, which in turn is linked to a user profile.

This section describes the following procedure, which has to be performed on the target system to create a user account with limited rights:

# 2.1.3.1 Creating a Target System User Account for Connector Operations

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

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

# Note:

For creating the target system account, you must log in to PeopleSoft Internet Architecture with administrator credentials.

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



# 2.1.3.1.1 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://IPADDRESS:PORT/psp/ps/?cmd=login

For example:

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

- 2. In the PeopleSoft Internet Architecture window, 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, OIMCS, and then click Add.
- 4. On the General tab, enter a description for the permission list in the **Description** field.
- 5. On the Pages tab, click the search icon for Menu Name and perform the following:
  - a. Click the plus sign (+) to add a row for Menu Name. Click the search icon for Menu Name. In the Menu Name lookup, enter IB\_PROFILE and then click Lookup. From the list, select IB\_PROFILE. The application returns to the Pages tab. Click Edit Components.
  - **b.** On the Component Permissions page, click **Edit Pages** for each of the following component names:

**IB\_GATEWAY** 

IB\_MESSAGE\_BUILDER

**IB\_MONITOR\_QUEUES** 

**IB\_NODE** 

- **IB\_OPERATION**
- IB\_QUEUEDEFN

IB\_ROUTINGDEFN

**IB\_SERVICE** 

IB\_SERVICEDEFN

**IB\_MONITOR** 

- c. Click Select All, and then click OK for each of the components. Click OK on the Components Permissions page.
- d. On the Pages tab, click the plus sign (+) to add another row for Menu Name.
- e. In the Menu Name lookup, enter PROCESSMONITOR and then click Lookup. From the list, select PROCESSMONITOR. The application returns to the Pages tab. Click Edit Components.
- f. On the Component Permissions page, click **Edit Pages** for the PROCESSMONITOR component name.



- g. Click Select All, and then click OK. Click OK on the Components Permissions page.
- h. On the Pages tab, click the plus sign (+) to add another row for Menu Name.
- i. In the Menu Name lookup, enter PROCESS\_SCHEDULER and then click Lookup. From the list, select PROCESS\_SCHEDULER. The application returns to the Pages tab. Click Edit Components.
- j. On the Component Permissions page, click **Edit Pages** for the PRCSDEFN component name.
- k. Click Select All, and then click OK. Click OK on the Components Permissions page.
- I. On the Pages tab, click the plus sign (+) to add another row for Menu Name.
- m. In the Menu Name lookup, enter MANAGE\_INTEGRATION\_RULES and then click Lookup. From the list, select MANAGE\_INTEGRATION\_RULES. The application returns to the Pages tab. Click Edit Components.
- n. On the Component Permissions page, click **Edit Pages** for the EO\_EFFDTPUB component name.
- Click Select All, and then click OK. Click OK on the Components Permissions page. The application returns to the Pages tab.
- On the People Tools tab, select the Application Designer Access check box and click the Definition Permissions link. The Definition Permissions page is displayed.
- On this page, grant full access to the following object types by selecting Full Access from the Access list:
  - App Engine Program
  - Message
  - Component
  - Project
  - Application Package
- 8. Click OK.
- Click the Tools Permissions link. The Tools Permissions page is displayed. On this page, grant full access to the SQL Editor tool by selecting Full Access from the Access list.
- 10. Click **OK**. The application returns to the People Tools tab.
- **11.** On the Process tab, click the **Process Group Permissions** link. The Process Group Permission page is displayed.
- 12. In the Process Group lookup, click the search icon. From the list, select **TLSALL.**
- **13.** On the Process Group Permission page, click the plus sign (+) to add another row for **Process Group.**
- **14.** In the Process Group lookup, click the search icon. From the list, select **STALL.** The application returns to the Process Group Permission page.
- **15.** Click **OK.**
- **16.** On the Web Libraries tab, click the search icon for the Web Library Name field and perform the following:



- a. In the Web Library Name lookup, enter WEBLIB\_PORTAL and then click Lookup. From the list, select WEBLIB\_PORTAL. The application returns to the Web Libraries tab. Click the Edit link.
- b. On the WebLib Permissions page, click Full Access(All).
- c. Click OK and then click Save.
- d. Click the plus sign (+) to add a row for the **Web Library Name** field and repeat Steps a through c for the WEBLIB\_PT\_NAV library.
- e. Click Save to save all the settings specified for the permission list.

## 2.1.3.1.2 Creating a Role for a Limited Rights User

To create a role for a limited rights user:

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

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

For example:

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

- 2. In the PeopleSoft Internet Architecture window, 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, OIMCS, 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 OIMCS and then click Lookup. From the list, select OIMCS.
  - **b.** Click the plus sign (+) to add another row.
  - c. In the Permission Lists lookup, enter EOEI9000 and then click Lookup. From the list, select EOEI9000.

## Note:

Permission list EOEI9000 is not available in PeopleTools 8.53, and is hence not applicable.

- d. Click the plus sign (+) to add another row.
- e. In the Permission Lists lookup, enter EOCO9000 and then click Lookup. From the list, select EOCO9000.
- 6. Click Save.

## 2.1.3.1.3 Assigning the Required Privileges to the Target System Account

To assign the required privileges to the target system account:



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

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

For example:

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

- 2. In the PeopleSoft Internet Architecture window, 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, OIMCS, 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 OIMCS and then click **Lookup**. From the list, select **OIMCS**. The application returns to the General tab.
- 5. On the ID tab, select **none** as the value of the ID type.
- 6. On the Roles tab, click the search icon:
  - a. In the Roles lookup, enter OIMCS and then click Lookup. From the list, select OIMCS.
  - b. Click the plus sign (+) to add another row.
  - c. In the Roles lookup, enter ProcessSchedulerAdmin and then click Lookup. From the list, select ProcessSchedulerAdmin.
  - d. Click the plus sign (+) to add another row.
  - e. In the Roles lookup, enter EIR Administrator and then click Lookup. From the list, select EIR Administrator.

#### Note:

Role EIR Administrator is not available in PeopleTools 8.53, and is hence not applicable.

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

# 2.2 Installation

Installation information is divided across the following sections:

- Installation on Oracle Identity Manager
- Installation on the Target System
- Installation with Other PeopleSoft Connectors



# 2.2.1 Installation on Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

- Running the Connector Installer
- Copying the Connector Files and External Code Files
- Configuring the IT Resource
- IT Resource Parameters
- Deploying the PeopleSoft Listener
- Removing the PeopleSoft Listener

# 2.2.1.1 Running the Connector Installer

## Note:

In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Administrative and User Console.

To run the Connector Installer:

- 1. Create a directory for the connector, for example, PSFT\_CS-11.1.1.5.0, in the OIM\_HOME/server/ConnectorDefaultDirectory directory.
- 2. Copy the contents of the connector installation media directory into directory created in Step 1.
- 3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
  - For Oracle Identity Manager release 11.1.1:
    - a. Log in to the Administrative and User Console by using the user account described in Creating the User Account for Installing Connectors in Oracle Fusion Middleware Administering Oracle Identity Manager.
    - **b.** On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector**.
  - For Oracle Identity Manager release 11.1.2.x:
    - a. Log in to Oracle Identity System Administration by using the user account described in Creating the User Account for Installing Connectors in Oracle Fusion Middleware Administering Oracle Identity Manager.
    - b. In the left pane, under System Management, click Manage Connector.
- 4. In the Manage Connector page, click **Install**.
- 5. From the Connector List list, select **PeopleSoft Campus 11.1.1.5.0.** This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

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



- a. In the Alternative Directory field, enter the full path and name of that directory.
- b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
- c. From the Connector List list, select PeopleSoft Campus 11.1.1.5.0.
- 6. Click Load.
- 7. To start the installation process, click **Continue**.

The following tasks are performed, in sequence:

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

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

- Retry the installation by clicking **Retry**.
- Cancel the installation and begin again from Step 1.
- 8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of steps that you must perform after the installation is displayed. These steps are as follows:
  - a. Configuring the IT resource for the connector

See Configuring the IT Resource for more information.

b. Configuring the scheduled tasks

See Configuring Scheduled Jobs for more information.

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

# 2.2.1.2 Copying the Connector Files and External Code Files

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

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



### Note:

 The directory paths given in the first column of this table correspond to the location of the connector files in the PeopleSoft Campus directory on the installation media. See Files and Directories on the Installation Media for more information about these files.

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

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

File in the Installation Media Directory	Destination for Oracle Identity Manager
lib/PeopleSoftOIMListener.ear	OIM_HOME/server/ConnectorDefaultDirectory/ PSFT_CS-11.1.1.5.0/listener
Files in the test/scripts directory	OIM_HOME/server/ConnectorDefaultDirectory/ PSFT_CS-11.1.5.0/scripts
Files in the test/config directory	OIM_HOME/server/ConnectorDefaultDirectory/ PSFT_CS-11.1.1.5.0/config

# 2.2.1.3 Configuring the IT Resource

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

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

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

Log in to the Administrative and User Console

• For Oracle Identity Manager release 11.1.2.x:

Log in to Oracle Identity System Administration

- 2. If you are using Oracle Identity Manager release 11.1.1, then:
  - a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
  - **b.** On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
- **3.** If you are using Oracle Identity Manager release 11.1.2.*x*, and if you want to create a sandbox, then create application instance as follows:



#### See Also:

Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager for more information about application instance and sandbox

- a. On the upper navigation bar, click **Sandboxes.** The Manage Sandboxes page is displayed.
- b. On the toolbar, click **Create Sandbox.** The Create Sandbox dialog box is displayed.
- c. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.
- d. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.
- e. Click **Save and Close.** A message is displayed with the sandbox name and creation label.
- f. Click **OK**. The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.
- g. Select the sandbox that you created.
- h. On the toolbar, click Activate Sandbox.

The table refreshes and a marker in the Active column is displayed. In addition, the Sandboxes link on the upper navigation bar also displays the active sandbox name in parentheses.

- i. In the left pane, under Configuration, click **Application Instances.** The Application Instances page is displayed.
- j. From the Actions menu, select **Create.** Alternatively, click **Create** on the toolbar. The Create Application Instance page is displayed.
- k. Enter the values of the attributes. For example:

Name: PeopleSoftInstance

Display Name: PeopleSoftInstance

Resource Object: Affiliation

IT Resource Instance: PSFT Campus

- I. Click **Save.** The application instance is created, and the details of the application instance is displayed in a page.
- m. To create a form to be associated with the application instance, open the Create Application Instance page or the Attributes tab of the Application Instance details page.
- n. Adjacent to the Forms field, click Create. The Create Form page is displayed.
- o. Enter values for the form attributes. For example:

Resource Type: Affiliation

Form Name: CampusForm

p. Click Create. A message is displayed stating that the form is created.



- q. In the Create Application Instance page or the Attributes tab of the Application Instance details page, click **Refresh** adjacent to the Form field. The newly created form is available for selection in the Form list.
- r. Select the new form from the drop-down list and click Apply.

The application instance is created.

- s. Before publishing the sandbox, close all the open tabs and pages.
- t. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created.
- **u.** On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.
- v. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.
- w. Search for and run the Catalog Synchronization Job scheduled job to sync the application instance with the catalog. See Configuring Scheduled Jobs for more information about configuring and running scheduled jobs.
- 4. In the left pane, under Configuration, click **IT Resource.**
- 5. In the IT Resource Name field on the Manage IT Resource page, enter PSFT Campus and then click **Search.** Alternatively, from the IT Resource Type menu, select **PSFT Campus**, and then click **Search**.
- 6. Click the edit icon for the IT resource.
- 7. From the list at the top of the page, select Details and Parameters.
- 8. Specify values for the parameters discussed in Table 2-3. The remaining parameters of IT resource are not applicable for this connector.
- 9. To save the values, click **Update**.

# 2.2.1.4 IT Resource Parameters

Specify values for the parameters discussed in Table 2-3.s

 Table 2-3
 IT Resource Parameters

Parameter	Description
Configuration Lookup	This parameter holds the name of the lookup definition that contains configuration information.
	Default value: Lookup.PSFT.Campus.Configuration
	<b>Note:</b> You must not change the value of this parameter. However, if you create a copy of all the connector objects, then you can specify the unique name of the copy of this lookup definition as the value of the Configuration Lookup Name parameter in the copy of the IT resource.



Parameter	Description
IsActive	This parameter is used to specify whether the specified IT Resource is in use or not. Enter one of the following as the value of the IsActive parameter:
	Enter yes as the value to specify that the target system installation represented by this IT resource is active. If you specify yes as the value, then the connector processes messages sent from this target system installation.
	Enter $no$ as the value if you do not want the connector to process messages sent from this target system installation.
	Default value: Yes

#### Table 2-3 (Cont.) IT Resource Parameters

# 2.2.1.5 Deploying the PeopleSoft Listener

The PeopleSoft listener is a Web application that is deployed on an Oracle Identity Manager host computer. The PeopleSoft listener parses the XML message and creates a reconciliation event in Oracle Identity Manager.

# Note:

- If you have already deployed a listener for the PeopleSoft User Management or Employee Reconciliation connector, then you must remove that listener and deploy the listener from the installation media of the PeopleSoft Campus connector.
- The PeopleSoft Campus, PeopleSoft Employee Reconciliation, and PeopleSoft User Management connectors have different IT resources. Therefore, you must configure separate HTTP nodes for messages of the Campus, Employee Reconciliation, and User Management connectors.

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

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

This section contains the following topics:

- Setting the Prerequisites of Deploying the PeopleSoft Listener
- Deploying the PeopleSoft Listener on Oracle Identity Manager
- Setting the Prerequisites of Deploying the PeopleSoft Listener on WebSphere
   Application Server
- Deploying the PeopleSoft Listener on WebSphere Application Server
- Importing Oracle Identity Manager CA Root Certificate into PeopleSoft WebServer



# 2.2.1.5.1 Setting the Prerequisites of Deploying the PeopleSoft Listener

Before deploying the PeopleSoft listener, perform the following steps:

- Ensure Apache Ant 1.7 or later and JDK 1.6 or later are installed.
- Set the following environment values in ant.properties:
  - ORACLE\_HOME maps to the Oracle Identity Manager installation directory. For example, /ps1/beahome/Oracle\_IDM1
  - ORACLE\_COMMON maps to the common directory in ORACLE\_HOME. For example, /ps1/beahome/Oracle\_IDM1/common
  - WLS\_HOME maps to the WebLogic Server directory. For example, / middleware/wlserver\_10.3
  - JAVA\_HOME maps to your JDK environment. For example, /usr/local/ packages/jdk16/
  - *PATH* must include the *JAVA\_HOME*/bin directory. You can set the *PATH* variable using the SET PATH=\$JAVA\_HOME/bin:\$PATH command.
- Build the **wlfullclient.jar** file in Oracle WebLogic server, for example, in the *WLS\_HOME*/server/lib directory:
  - 1. Change directories to WLS\_HOME/server/lib.
  - 2. Run the following command:

java -jar ../../modules/com.bea.core.jarbuilder\_1.3.0.0.jar

## Note:

The exact jar file version can be different based on the WebLogic Server. Use the corresponding file with the name as com.bea.core.jarbuilder at the WLS\_HOME/../modules/ directory.

• Start Oracle Identity Manager and the Admin Server.

#### 2.2.1.5.2 Deploying the PeopleSoft Listener on Oracle Identity Manager

To deploy the PeopleSoft listener on Oracle Identity Manager:

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

The listener directory is located in the connector package directory, for example, *OIM\_HOME/*server/ConnectorDefaultDirectory/PSFT\_CS-11.1.1.5.0.

2. Run the following command:

ant setup-listener



### Note:

If you need to deploy the listener in an Oracle Identity Manager cluster, then:

- Specify the name of the cluster for the oim.server.name property in the listener/deploy.properties file.
- Update the following configurations appropriately with the URL of the listener, /PeopleSoftOIMListener:
  - Front-end web server
  - Load balancer
  - PeopleSoft nodes
- Copy the connector package into the OIM\_HOME/server/ ConnectorDefaultDirectory directory of every node.

2.2.1.5.3 Setting the Prerequisites of Deploying the PeopleSoft Listener on WebSphere Application Server

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

• *OIM\_ORACLE\_HOME* maps to the Oracle Identity Manager installation directory. For example, /ps1/was/Oracle\_IDM1

You can set this variable using the setenv OIM\_ORACLE\_HOME <value> command.

 JAVA\_HOME maps to your JDK environment. For example, /usr/local/ packages/jdk16/

You can set this variable using the setenv JAVA\_HOME <value> command.

• *PATH* must include the *JAVA\_HOME*/bin directory. You can set this variable using the setenv PATH \$JAVA\_HOME/bin:\$PATH command.

## 2.2.1.5.4 Deploying the PeopleSoft Listener on WebSphere Application Server

To deploy the PeopleSoft listener on IBM WebSphere Application Server:

1. Copy the listener EAR creation scripts to the following directory:

*OIM\_ORACLE\_HOME*/server/ConnectorDefaultDirectory/PSFT\_CS-11.1.1.5.0/ listener

- 2. Set the Oracle Identity Manager connection details in the listener/deploy.properties file.
- 3. Run the following command:

ant setup-listener

4. The listener EAR will be created in the following directory:

*OIM\_ORACLE\_HOME*/server/ConnectorDefaultDirectory/PSFT\_CS-11.1.1.5.0/ listener/deployear



- 5. Log in to the WebSphere Admin console.
- 6. Expand Applications.
- 7. Select Enterprise Applications from the list.
- 8. Click Install and browse for the listener EAR directory.
- 9. Select Fast Path and click Next.
- **10.** Under **Map modules to servers,** select **oim\_server1** to map the listener EAR file.
- **11.** Save the listener EAR application and start the service.

# 2.2.1.5.5 Importing Oracle Identity Manager CA Root Certificate into PeopleSoft WebServer

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

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

- For Oracle WebLogic Server:
  - **1.** Identity the certificate of issuing authority, the root CA for Oracle Identity Manager.

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

#### MW\_HOME/wlserver\_10.3/server/lib/CertGenCA.der

If the certificate is issued by an external entity, then you must import the corresponding root certificate.

2. Use **pskeymanager** to import the root certificate into PeopleSoft WebServer keystore.

#### • For IBM WebSphere Application Server:

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

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

If the certificate is issued by a different entity, then you must import the corresponding root certificate.

2. Use **pskeymanager** to import the root certificate into PeopleSoft WebServer keystore.

# 2.2.1.6 Removing the PeopleSoft Listener

This section contains the following topics:

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



## Note:

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

## 2.2.1.6.1 Removing the PeopleSoft Listener for IBM WebSphere Application Server

To remove the PeopleSoft listener:

- 1. Log in to the WebSphere Admin console.
- 2. Expand Applications.
- 3. Select Enterprise Applications from the list.

A list of deployed applications is shown in the right pane.

- 4. Select the PeopleSoftOIMListener.ear check box.
- 5. Specify the Context root as PeopleSoftOIMListener.
- 6. Click Uninstall.

An Uninstall Application confirmation screen appears with the name of the application to be uninstalled. In this scenario, the application would be PeopleSoftOIMListener.

7. Click OK.

## 2.2.1.6.2 Removing the PeopleSoft Listener for Oracle WebLogic Server

From the listener directory, run the following command:

ant undeploy

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

- 1. Log in to the Oracle WebLogic admin console.
- 2. From the Domain Structure list, select **OIM\_DOMAIN.**

Where **OIM\_DOMAIN** is the domain on which Oracle Identity Manager is installed.

- 3. Click the **Deployments** tab.
- 4. On Microsoft Windows, in the Change Centre window, click Lock & Edit.
- 5. Select **PeopleSoftOIMListener.ear.** This enables the Delete button of the Control tab in the Summary Of Deployments region.
- 6. Click **Stop.** A list appears.
- 7. Select Force Stop Now.

The Force Stop Application confirmation screen appears.



- 8. Click Yes.
- 9. On the Control tab in the Summary Of Deployments region, select **PeopleSoftOIMListener.ear.**
- 10. Click Delete.

A confirmation message appears on successful deletion of the WAR file.

**11**. On the left pane, click the **Active Changes** button.

# 2.2.2 Installation on the Target System

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

- Configuring the Target System for Full Reconciliation
- Enabling Content-based Filtering for Full Reconciliation in SCC\_CONSTITUENT\_FULLSYNC Message
- Configuring the Target System for Incremental Reconciliation
- Enabling Content-based Routing for Incremental Reconciliation in SCC\_CONSTITUENT\_SYNC Message

# 2.2.2.1 Configuring the Target System for Full Reconciliation

As described in About the Connector, full reconciliation is used to reconcile all existing person data into Oracle Identity Manager.

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

- Configuring the PeopleSoft Integration Broker
- Configuring the SCC\_CONSTITUENT\_FULLSYNC Service Operation

## 2.2.2.1.1 Configuring the PeopleSoft Integration Broker

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

- Configuring PeopleSoft Integration Broker Gateway
- Configuring PeopleSoft Integration Broker

#### 2.2.2.1.1.1 Configuring PeopleSoft Integration Broker Gateway

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

To configure the PeopleSoft Integration Broker gateway:

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

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



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

For example:

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

- 2. To display the Gateway component details, expand **PeopleTools**, **Integration Broker**, **Configuration**, and then **Gateways**. The Gateway component details are displayed.
- 3. In the Integration Gateway ID field, enter LOCAL, and then click Search. The LOCAL gateway is a default gateway that is created when you install PeopleSoft Internet Architecture.
- 4. Ensure that the IP address and host name specified in the URL of the PeopleSoft listener are those on which the target system is installed. The URL of the PeopleSoft listener is in one of the following formats:

http://HOSTNAME\_of\_the\_PeopleSoft\_Web\_server or IPADDRESS:PORT/PSIGW/PeopleSoftListeningConnector

For example:

http://10.121.16.42:80/PSIGW/PeopleSoftListeningConnector

- To load all target connectors that are registered with the LOCAL gateway, click Load Gateway Connectors. A window is displayed mentioning that the loading process is successful. Click OK.
- 6. Click Save.
- 7. Click **Ping Gateway** to check whether the gateway component is active. The PeopleTools version and the status of the PeopleSoft listener are displayed. The status should be ACTIVE.

#### 2.2.2.1.1.2 Configuring PeopleSoft Integration Broker

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

To configure PeopleSoft Integration Broker:

- **1.** Create a remote node as follows:
  - 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\_FILE\_NODE, and then click **Add.**
  - c. On the Node Definition tab, provide the following values:

In the Description field, enter a description for the node.

In the Default User ID field, enter PS.

- d. Make this node a remote node by deselecting the **Local Node** check box and selecting the **Active Node** check box.
- e. Ensure that the Node Type is PIA.



f. On the Connectors tab, search for the following information by clicking the Lookup icon:

Gateway ID: LOCAL

Connector ID: FILEOUTPUT

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

Property ID: HEADER

Property Name: sendUncompressed

Required value: Y

Property ID: PROPERTY

Property Name: Method

Required value: PUT

Property ID: PROPERTY

Property Name: FilePath

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

Property ID: PROPERTY

Property Name: Password

Required value: Same value as of **ig.fileconnector.password** in the integrationGateway.properties file

## Note:

To locate the intergrationGateway.properties file, perform the following steps using the PeopleSoft administrator credentials:

- i. In PeopleSoft Internet Architecture, expand **PeopleTools**, Integration Broker, Configuration, and then click Gateways.
- ii. In the Integration Gateway ID field, enter LOCAL, and then click Search.
- iii. Click the Gateway Setup Properties link.

You are prompted to enter the user ID and password.

iv. Specify the following values:

In the UserID field, enter the appropriate user ID.

In the Password field, enter the appropriate password.

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

2.2.2.1.2 Configuring the SCC\_CONSTITUENT\_FULLSYNC Service Operation

The SCC\_CONSTITUENT\_FULLSYNC message contains the basic personal information about all the persons. This information includes the ID, First Name, Last Name, Affiliation Type, and other contact information.

To configure the SCC\_CONSTITUENT\_FULLSYNC service operation, perform the following procedures:

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

#### 2.2.2.1.2.1 Activating the SCC\_CONSTITUENT\_FULLSYNC Service Operation

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

To activate the SCC\_CONSTITUENT\_FULLSYNC service operation:

- 1. In PeopleSoft Internet Architecture, expand PeopleTools, Integration Broker, Integration Setup, and then click Service Operations.
- 2. On the Find Service Operation tab, enter SCC\_CONSTITUENT\_FULLSYNC in the Service field, and then click Search.
- 3. Click the SCC\_CONSTITUENT\_FULLSYNC link.

#### Note:

In PeopleSoft Campus, there are two versions of the message (INTERNAL and VERSION\_1) associated with this service operation. But, when you integrate PeopleSoft Campus 9.0 and Oracle Identity Manager, you must use the default version INTERNAL.

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



General Handlers	Routings	
Service Operation:	SCC_CONSTITUENT_FULLSYNC	
Operation Type:	Asynchronous - One Way	
*Operation Description:	Constituent Full Sync	
Operation Comments:		User/Password Required
		*Req Verification: None
		Service Operation Security
Owner ID:	Campus Community	
Operation Alias:		
Default Service Operation	1 Version	
*Version:	INTERNAL	Default Active
Version Description:	Internal Version	Routing Status
Version Comments:	Same as the latest version but with real table names	Any-to-Local: Does not exist
	real table hames.	Local-to-Local: Does not exist
		Local-to-Atom: Does not exist.
	Non-Repudiation	Routing Actions Upon Save
Introspection	.  Runtime Schema Validation	Generate Any-to-Local
macoposition		Generate Local-to-Local
Message Information		
Type:	Request	
Message.Version:	SCC_CONSTITUENT_FULLSYNC.IN	ITEQ View Message
*Queue Name:	PERSON_DATA	Q View Queue Add New Queue
	_	
Non-Default Versions	Description	Personalize   Find   🖾   🗰 First 🚺 1 of 1 💟 Last Active
	Version 1	
Save	Return to Service Add Version	

General | <u>Handlers</u> | <u>Routings</u>

- 4. In the Default Service Operation Version region, click Active.
- 5. Click Save.
- 6. In the Non-Default Versions region, click the VERSION\_1 link, as shown in the following screenshot.



Service Service Operation Version Operation Type Description Comments	Asynchronous - One Way	_	Default couting Actions I Generate An Generate Lo Generate Lo	y-to-Local cal-to-Local
Message Information				
Туре	Request			
Message Version	SCC_CONSTITUENT_FULLSYNC.VER	Q	View Message	
*Queue Name	PERSON_DATA	Q	View Queue	Add New Queue
Save Return				
Service Operation Versions   Service	Operation Versions			

Service Operation Version

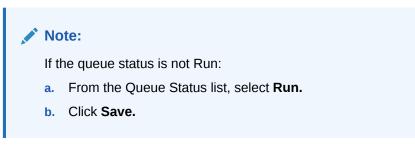
- 7. Click Active.
- 8. Click Save.
- 9. Click Return.

2.2.2.1.2.2 Verifying the Queue Status for the SCC\_CONSTITUENT\_FULLSYNC Service Operation

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

To ensure that the status of the queue for the SCC\_CONSTITUENT\_FULLSYNC service operation is Run:

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



The queue status is highlighted in the following screenshot:



#### Queue Definitions

	PERSON_DATA MaintainPersonalD	ata		Archive	Unordered		
Comments	HR Message Char Message Objects o Employee and Nor	containing	×	Queue Status Owner ID	Run HR Core Objec	ts	<b>v</b>
Operations Assigne	d to Queue		Define Partit	ioning Fields			
Service Vie	w All   🖾 🛛 First 🖡	1-10 of	Common Fie	elds	View All 🛛 🖾	First 🚺	1-3 of 3 🔽 Last
Operations	90	▶ Last	Include	<u>Field</u>	Alia	<u>as Name</u>	
Service Operation		Version		OPERATIONNAME	=		
CS ADM APPL DA	ATA FULLSYNC	VERSION_1		PUBLISHER			
CS ADM PRSPCT	DATA FULLSYNC	VERSION_1					
CS TEST SCORE	S FULLSYNC	VERSION_1		PUBPROC			
HCR ADD JOB		VERSION_1					
HCR ADD JOB A	<u>CK</u>	VERSION_1					
HCR ADD PERSO	<u>N</u>	VERSION_1					
HCR ADD PERSO	<u>DN ACK</u>	VERSION_1					
HCR CAN JOB		VERSION_1					
PERSON ACCOMP	P FULLSYNC	VERSION_1					
PERSON ACCOMP	SYNC	VERSION_1					
Save			Add Field	d			

#### 4. Click Return to Search.

2.2.2.1.2.3 Setting Up the Security for the SCC\_CONSTITUENT\_FULLSYNC Service Operation

A person on the target system who has permission to modify or add personal or job information of a person might not have access to send messages regarding these updates. Therefore, it is imperative to explicitly grant security to enable operations.

To set up the security for SCC\_CONSTITUENT\_FULLSYNC service operation:

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

The link is highlighted in the following screenshot:



General Handlers	Routings		
Service Operation:	SCC CONSTITUENT FULLSYNC		
Operation Type:	Asynchronous - One Way		
*Operation Description:	Constituent Full Sync		
Operation Comments:		User/Passwo	rd Required
		*Req Verification	n: None 💌
		: Service Operation	<u>i Security</u>
Owner ID:	Campus Community		
Operation Alias:			
Default Service Operation	Version		
*Version:	INTERNAL	✓ Default	Active
Version Description:	Internal Version	Routing Status	
Version Comments:	Same as the latest version but with real table names.	Any-to-Local:	Does not exist
	real table names.	Local-to-Local:	Does not exist
		Local-to-Atom:	Does not exist.
	Non-Repudiation	Routing Actions Up	on Save
Introspection	Runtime Schema Validation	Generate Any-t	to-Local
maopoolon		Generate Loca	I-to-Local
Message Information			
Type:	Request		
Message.Version:	SCC CONSTITUENT FULLSYNC.IN	JTFQ View Message	
_	PERSON_DATA		Add New Queue
*Queue Name:	PERSON_DAIX		
Non-Default Versions		Personalize   Find   🖾	
·	Description /ersion 1		Active
			<u>v</u>
Save	eturn to Service Add Version		

General | Handlers | Routings

4. Attach the **OIMCS** permission list to the SCC\_CONSTITUENT\_FULLSYNC service operation. This list is created in Step 3 of the preinstallation procedure discussed in Creating a Permission List.

To attach the permission list:

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

The **OIMCS** permission list appears.

c. From the Access list, select Full Access.

The following screenshot displays the preceding steps:



# Web Service Access

#### Operation:

## SCC\_CONSTITUENT\_FULLSYNC

Permission	Personalize   Find   🖟	0   🖩 🗌	First 🚺	1-2 of 2	🕨 La	ast
Permission List		Access				
HCSPSERVICE		Full Acc	ess	~	+	-
OIMCS	٩	Full Acc	ess	~	+	-

- d. Click Save.
- e. Click Return to Search.

2.2.2.1.2.4 Defining the Routing for the SCC\_CONSTITUENT\_FULLSYNC Service Operation

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

To define the routing for SCC\_CONSTITUENT\_FULLSYNC service operation:

- 1. On the Routing tab, enter SCC\_CONSTITUENT\_FULLSYNC\_CS\_FILE as the routing name and then click Add.
- 2. On the Routing Definitions tab, enter the following:

Sender Node: PSFT\_CS

#### Note:

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

- a. Click the Look up icon.
- b. Click **Default** to sort the results in descending order.

The default active local node should meet the following criteria:

Local Node: 1

Default Local Node: Y

Node Type: PIA

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

- c. Select the node.
- d. Click Save.

Receiver Node: OIM\_FILE\_NODE

The following screenshot displays the Sender and Receiver nodes:



Routing Definitions Parar	neters	Connector	Properties	Routi	ng Properties
Routing Name *Service Operation					Active System Generated
Version	INTERNA	L			
*Description	Fullsyncf	for constituer	nt msg		Graphical View
Comments					
*Sender Node	CS900IM	IA			
*Receiver Node	OIM_FILE	E_NODE			
Operation Type	Asynchro	onous - One	Way	_	
Owner ID				*	
Save	Returi	n			

Routing Definitions | Parameters | Connector Properties | Routing Properties

- 3. Click the **Parameters** tab and enter the following details in the fields:
  - External Alias: SCC\_CONSTITUENT\_FULLSYNC.VERSION\_1
  - Message.Ver into Transform 1: SCC\_CONSTITUENT\_FULLSYNC.INTERNAL
  - Transform Program 1: HMTF\_TR\_OA

Click **Cancel** on the warning box that is displayed.

• Message.Ver out of Transforms: SCC\_CONSTITUENT\_FULLSYNC.VERSION\_1

The following screenshot displays the Parameters tab:



Routing Definitions	Parameters	Connector Properties	Routing Properties	
	Routing Na	me CONSTITUENT_FUL	LSYNC_TO_FILE	
	Service Opera	tion SCC_CONSTITUEN	T_FULLSYNC	
Servio	e Operation Vers	sion INTERNAL		
	Sender N	ode CS900IMA		
	Receiver N	ode OIM_FILE_NODE		
Parameters				
		Type Outbound Reque	est	
	Extern	al Alias SCC_CONSTITU	ENT_FULLSYNC.VERS	ION_1
			Alias References	
Messa	age.Ver into Trans	sform 1 SCC_CONSTITU	ENT_FULLSYNC.INTER	RNAL Q
	Transform Pro	gram 1 HMTF_TR_OA		م
	Transform Pro	gram 2		Q
Messag	e.Ver out of Tran	sforms SCC_CONSTITU	ENT_FULLSYNC.VERS	ION_1Q
Save	Return			

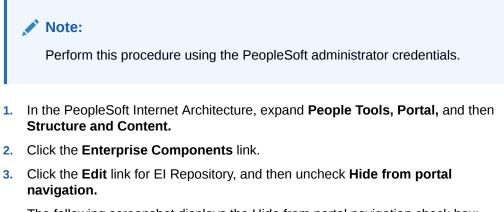
Routing Definitions | Parameters | Connector Properties | Routing Properties

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

### 2.2.2.1.2.5 Displaying the EI Repository Folder

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

To display the EI Repository folder:



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



Name:	EIP_CATALOG		Parent Folder:	Enterprise Components	
'Label:	El Repository		Copy object	Select New Parent Folder	
Long Description: (254 Characters)	Enterprise Integration Rep	oository			
Product: Sequence number: Object Owner ID Hide from portal	0000			Creation Date: thor: PSEO Add Folder	10/29/2
Folder Navigation	ation Disabled		Q		
Folder Attributes				✓ Translate	De

Save Notify
Folder Administration | Folder Security

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

2.2.2.1.2.6 Activating the SCC\_CONSTITUENT\_FULLSYNC Message

You must activate the SCC\_CONSTITUENT\_FULLSYNC message so that it can be processed.

To activate the SCC\_CONSTITUENT\_FULLSYNC message:

- 1. In the PeopleSoft Internet Architecture, expand Enterprise Components, El Repository, and then click Message Properties.
- 2. Search for and open the SCC\_CONSTITUENT\_FULLSYNC message.
- 3. Click Activate All.

The following screenshot displays the message to be activated:



#### **Message Properties**

the first few letters of a Messag	ges and their Subscriptions, nar je Name. Select which Message manually make changes or by j	es and Subscrip	tions you	
Message Name Begins With:	SCC_CONSTITUENT_FULLS	YNC	Search	
Message Subscription	Personalize   Find   View All   💌	📕 🛛 First	1 of 1 🚺 Last	Activate A
Message Name		Message Statu	<u>15</u>	
1 SCC_CONSTITUENT_I	FULLSYNC	Active	~	Inactivate

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

#### Note:

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

#### 2.2.2.1.2.7 Activating the Full Data Publish Rule

You must define and activate the Full Data Publish rule, because it acts as a catalyst for the full reconciliation process. This rule provides the full reconciliation process the desired information to initiate reconciliation.

To activate the full data publish rule:

- 1. In the PeopleSoft Internet Architecture, expand Enterprise Components, Integration Definitions, and then click Full Data Publish Rules.
- 2. Search for and open the SCC\_CONSTITUENT\_FULLSYNC message.
- 3. In the Publish Rule Definition region:
  - a. In the Publish Rule ID field, enter SCC\_CONSTITUENT\_FULLSYNC.
  - **b.** In the Description field, enter SCC\_CONSTITUENT\_FULLSYNC.
  - c. From the Status list, select Active.

The following screenshot displays the preceding steps:



Full Table Publish Rules	Record Mapping	Languages	3	
Message Name: SCC	C_CONSTITUENT_FULL	SYNC		
Description: Con	stituent Full Sync			
Publish Rule Definition	n		Find View All	First 💶 2 of 2 🚺 Last
*Publish Rule ID:	SCC_CONSTITUENT_	FULLSYNC		+ -
*Description:	SCC_CONSTITUENT_	FULLSYNC		
*Status:	Active 💌			
Chunking Rule ID:			Q	
Alternate Chunk Table:				
Message Options		Output Fo	rmat	
	essage Header essage Trailer	F	Aessage Tat File Tat File with Con	trol Record

4. Click Save.

# 2.2.2.2 Enabling Content-based Filtering for Full Reconciliation in SCC\_CONSTITUENT\_FULLSYNC Message

Content-based filtering uses PeopleSoft Campus Solutions Affiliations codes for publishing rules. Affiliation Codes represent the relationship(s) a person has with an institution. This section assumes that you have already configured the SCC\_CONSTITUENT\_FULLSYNC message by following the procedure described in Configuring the SCC\_CONSTITUENT\_FULLSYNC Service Operation.

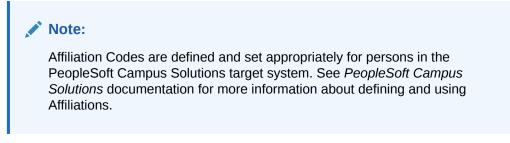
The following procedures are discussed in this section:

- Setting Affiliation Routing Rules
- Setting the Routing Transformation Parameters for the SCC\_CONSTITUENT\_FULLSYNC message
- Activating the Full Data Publish Rule with Content-based Filtering

#### 2.2.2.1 Setting Affiliation Routing Rules

Using content-based filtering for the SCC\_CONSTITUENT\_FULLSYNC message requires that you define valid Affiliation Codes that you wish to include in the data sent to Oracle Identity Manager. Selecting Affiliation Codes allows you to define the scope of persons which will be included in the generated XML files.





To set Affiliate Routing rules:

- 1. Open the Affiliation Routing component details by expanding Set Up SACR, Common Definitions, Affiliations, Affiliation Routing.
- 2. Select the node that represents your OIM File Node, as displayed in the following sample screenshot.

Asg	Node	OIM_FILE_N	NOD	E 💌	OIM File node for data publish	Find View All	
ffi	liations				Personalize Find View.	AII 🖓 📜 💡	irst 🚺 1-4 of 4 🔝 Last
	Institution	Affiliation Co	de	Description			
1	PSUNV C	ALUMN_TMP	ιQ	PSUNV Alumni			÷ =
2	PSUNV C	EMPLOYEE	Q	Sample manual emple	oyee code.		÷ E
3	PSUNV	RECTR_TMP	ιq	PSUNV Recruiter			÷ =
4	PSUNV C	STUDENT	Q	Student of PS UNV.			÷ E

- 3. In the **Institution** field, select the Institution Code(s).
- 4. In the Affiliation Code field, select the Affiliation Code(s) you wish to include.
- 5. If needed, click the plus (+) button to insert additional rows.
- 6. Click Save.

## 2.2.2.2 Setting the Routing Transformation Parameters for the SCC\_CONSTITUENT\_FULLSYNC message

You will transform the message being sent by enabling an additional transform program on the Affiliation Routing parameters.

To define the routing for SCC\_CONSTITUENT\_FULLSYNC service operation:

- 1. In the PeopleSoft Internet Architecture, expand PeopleTools, Integration Broker, Integration Setup, and then click Service Operations.
- 2. Search for and open the SCC\_CONSTITUENT\_FULLSYNC message.
- 3. On the Routing Definitions tab, click the routing name.
- 4. Click the **Parameters** tab and enter the following details in the fields:
  - Transform Program 1: SCC\_AFL\_FLTR



• Transform Program 2: HMTF\_TR\_OA

Click **Cancel** on the warning box that is displayed.

The following screenshot displays the routing transformation program settings on the Parameters tab:

Routing Definitions Parameters Co	nnector Properties Routing Properties
Routing Name	CONSTITUENT_FULLSYNC_TO_FILE
Service Operation	SCC_CONSTITUENT_FULLSYNC
Service Operation Version	INTERNAL
Sender Node	CS900IMA
Receiver Node	OIM_FILE_NODE
Parameters	
Ту	pe Outbound Request
External Ali	ias SCC_CONSTITUENT_FULLSYNC.VERSION_1
	Alias References
Message.Ver into Transform	n 1 SCC_CONSTITUENT_FULLSYNC.INTERNAL
Transform Program	n 1 SCC_AFL_FLTR
Transform Program	n 2 HMTF_TR_OA
Message.Ver out of Transform	
Save Return	

Routing Definitions | Parameters | Connector Properties | Routing Properties

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

#### 2.2.2.3 Activating the Full Data Publish Rule with Content-based Filtering

You must define and activate the Full Data Publish rule that uses the Affiliation Routing settings you defined. This rule provides the full reconciliation process the desired information to initiate reconciliation.

To activate the full data publish rule:

- 1. In the PeopleSoft Internet Architecture, expand Enterprise Components, Integration Definitions, and then click Full Data Publish Rules.
- 2. Search for and open the SCC\_CONSTITUENT\_FULLSYNC message.
- 3. In the Publish Rule Definition region:
  - a. In the Publish Rule ID field, enter AFFILIATION\_FILTER.
  - b. In the Description field, enter Only affiliations of interest.
  - c. From the Status list, select Active.
  - d. Verify in the Message Options box that Create Message Header and Create Message Trailer are selected.

The following screenshot displays the preceding steps:



Description: Co Publish Rule Definitio	nstituent Full Sync	Find   View All	First 🚺 1 of 2 🕨 Ls
*Publish Rule ID:	AFFILIATION_FILTER		
*Description:	Only affiliations of inte	rest	
*Status:	Active 🖌		
Chunking Rule ID:		٩	
Alternate Chunk			
Table: Message Options		Output Format	
Create M	essage Header essage Trailer	Message     Flat File     Flat File	trol Record

#### 4. Click the **Record Mapping** tab.

5. In the Record Source Mapping region, enter the following values:

Message Record Name	Source/Order by Record Name
ADDRESS_TYPE_V2	SCC_ADRTYP_AFLT
NAME_TYPE_VW2	SCC_NAMTYP_AFLT
PERSON_SA	SCC_PER_SA_AFLT
SCC_AFL_PERSON	SCC_PERAFL_AFLT
SCC_CM_PERSON_I	SCC_PERSON_AFLT
SCC_PER_ADDR_I	SCC_PERADR_AFLT
SCC_PER_NAME_I2	SCC_PERNAM_AFLT
SCC_PER_NID_I	SCC_PERNID_AFLT
SCC_PER_PDE_I	SCC_PERPDE_AFLT
SCC_PER_PHONE_I	SCC_PERPHN_AFLT

The following screenshot displays the preceding steps:



Description: Co	onstituent Full Sync		
Publish Rule Definiti	ion	Find View All	First 🚺 1 of 2 🕨 L
*Publish Rule ID:	AFFILIATION_FIL	TER	
*Description:	Only affiliations of	finterest	
Record Source	Mapping	Find   View 4 First 🚺 1-	11 of 11 🚺 Last
Message Rec ADDRESS_T		Source/Order by Record Name:	ŧ.
NAME_TYPE_	Q	SCC_NAMTYP_AFLT	+ <b>-</b>
PERSON_SA	٩	SCC_PER_SA_AFLT	÷-
SCC_AFL_PE	RSON	SCC_PERAFL_AFLT	<b>+</b> -
SCC_CM_PE	RSON_I Q	SCC_PERSON_AFLT Q	+-
SCC_PER_A		SCC_PERADR_AFLT	÷-
SCC PER E	MAILIQ	SCC_PEREML_AFLT	Ξ
SCC_PER_N		SCC_PERNAM_AFLT	Ξ
SCC_PER_N		SCC_PERNID_AFLT	ŧ
SCC_PER_P		SCC_PERPDE_AFLT	÷-
SCC_PER_P		SCC_PERPHN_AFLT	ŧ

6. Click Save.

### 2.2.2.3 Configuring the Target System for Incremental Reconciliation

Configuring the target system for incremental reconciliation involves configuring PeopleSoft Integration Broker and configuring the SCC\_CONSTITUENT\_SYNC messages.

A message is the physical container for the XML data that is sent from the target system. Message definitions provide the physical description of data that is sent from the target system. This data includes fields, field types, and field lengths. A queue is used to carry messages. It is a mechanism for structuring data into logical groups. A message can belong to only one queue.

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



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

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

#### Note:

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

- Configuring PeopleSoft Integration Broker
- Configuring the SCC\_CONSTITUENT\_SYNC Service Operation
- Preventing Transmission of Unwanted Fields During Incremental Reconciliation

#### 2.2.2.3.1 Configuring PeopleSoft Integration Broker

To configure PeopleSoft Integration Broker:

## Note:

- SectionConfiguring PeopleSoft Integration Broker Gateway describes the procedure to configure the PeopleSoft Integration Broker gateway.
- The PeopleSoft Campus, PeopleSoft Employee Reconciliation, and PeopleSoft User Management connectors have different IT resources. Therefore, you must configure separate HTTP nodes for messages of the Campus, Employee Reconciliation, and User Management connectors.

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

- A single listener is sufficient for all the connectors. However, you must remove any existing listeners and deploy the listener from the installation media of the PeopleSoft Campus connector. You can configure the nodes to point to the same listener with different IT resource names.
- 1. Create a remote node by performing the following steps:
  - a. In 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\_CS\_NODE, and then click **Add.**
  - c. On the Node Definition tab, enter a description for the node in the **Description** field. In addition, specify the SuperUserID in the **Default User ID** field. For example, PS.



- d. Make this node a remote node by deselecting the **Local Node** check box and selecting the **Active Node** check box.
- e. Ensure Node Type is PIA.
- f. On the **Connectors** tab, search for the following information by clicking the Lookup icon:

Gateway ID: LOCAL

Connector ID: HTTPTARGET

g. On the Properties page in the Connectors tab, enter the following information:
 Property ID: HEADER

Property Name: sendUncompressed

Required value: Y

Property ID: HTTP PROPERTY

Property Name: Method

Required value: POST

Property ID: HEADER

Property Name: Location

Required value: Enter the value of the IT Resource name as configured for PeopleSoft Campus

Sample value: PSFT Campus

Property ID: PRIMARYURL

Property Name: URL

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

```
http://ORACLE_IDENTITY_MANAGER_SERVER_IPADDRESS:PORT/
PeopleSoftOIMListener
```

The URL depends on the application server that you are using. For an environment on which SSL is not enabled, the URL must be in the following format:

For IBM WebSphere Application Server:

http://10.121.16.42:9080/PeopleSoftOIMListener

For Oracle WebLogic Server:

http://10.121.16.42:7001/PeopleSoftOIMListener

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

https://COMMON\_NAME:PORT/PeopleSoftOIMListener

For IBM WebSphere Application Server:

https://example088196:9443/PeopleSoftOIMListener

For Oracle WebLogic Server:



https://example088196:7002/PeopleSoftOIMListener

Note:

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

- h. Click **Save** to save the changes.
- i. Click the **Ping Node** button to check whether a connection is established with the specified IP address.

Note:

Ping also validates the target authentication, in this case, the IT resource name.

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



#### Note:

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

HttpTargetConnector:PSHttpFactory init or setCertificate failed

You might also encounter the following error when you ping the node:

Cannot establish HTTP connection

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

secureFileKeystorePath=<path to pskey>

secureFileKeystorePasswd=password

To find the integrationgateway.properties file, go to PeopleTools, Integration Broker, Configuration, Gateways, and then click Gateway Setup Properties.After logging in, click on the Advanced Properties Page link

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

- 1. Verify if secureFileKeystorePath in the integrationgateway.properties file is correct.
- 2. Verify if secureFileKeystorePasswd in the integrationgateway.properties file is correct.
- 3. Then, find the secureFileKeystorePasswd option and copy the password down to the Password Encryption box. Next, click Encrypt to get your encrypted version.
- 4. Finally, copy the encrypted version back up to the setting.
- 5. Save and exit.

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

For more information, see https://support.oracle.com/epmos/ faces/ui/km/DocumentDisplay.jspx?id=1270683.1

#### 2.2.2.3.2 Configuring the SCC\_CONSTITUENT\_SYNC Service Operation

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

To configure the SCC\_CONSTITUENT\_SYNC service operation perform the following procedures:



- Activating the PERSON\_BASIC\_SYNC Service Operation
- Activating the SCC\_PERSON\_SYNC Service Operation
- Activating the SCC\_CONSTITUENT\_SYNC Service Operation
- Activating the SSC\_CONSTITUENT\_SYNC Event
- Activating the PERSON\_BASIC\_SYNC Notification Handler
- Activating the SCC\_PERSON\_SYNC Notification Handler
- Verifying the Queue Status for the SCC\_CONSTITUENT\_SYNC Service Operation
- Setting Up the Security for Service Operations
- Defining the Routing for the SCC\_CONSTITUENT\_SYNC Service Operation
- Displaying the EI Repository Folder
- Activating the PERSON\_BASIC\_SYNC Message

#### 2.2.2.3.2.1 Activating the PERSON\_BASIC\_SYNC Service Operation

To activate the PERSON\_BASIC\_SYNC service operation:

- 1. In PeopleSoft Internet Architecture, expand PeopleTools, Integration Broker, Integration Setup, and then click Service Operations.
- 2. On the Find Service Operation tab, enter PERSON\_BASIC\_SYNC in the Service field, and then click Search.
- 3. Click the **PERSON\_BASIC\_SYNC** link.
- 4. In the Default Service Operation Version region, enter INTERNAL in the Version field and click Active.

The following screenshot displays the default version of the PERSON\_BASIC\_SYNC service operation:



General Handlers	Routings	
Service Operation: Operation Type: *Operation Description: Operation Comments: Owner ID:	PERSON_BASIC_SYNC Asynchronous - One Way Personal Data Sync HR Core Objects	User/Password Required *Req Verification: None  Service Operation Security
Operation Alias:	n Version	
Default Service Operation "Version: Version Description: Version Comments:	INTERNAL Personal Data Sync  Non-Repudiation Runtime Schema Validation	✓ Default     ✓ Active
Message Information		
Type: Message.Version: *Queue Name:	Request PERSON_BASIC_SYNC.INTERNAL PERSON_DATA	Q <u>View Message</u> Q <u>View Queue</u> Add New Queue
Non-Default Versions	Р	ersonalize   Find   🗗   🛗 🛛 First 🗹 1-4 of 4 🔟 Last -
Version	Description	Active
VERSION_1 VERSION_2	Personal Data Sync Personal Data Sync	
VERSION_3	Personal Data Sync	
VERSION_4	Personal Data Sync	
Save	Return to Service Add Version	

5. In the Non-Default Versions region, click the **VERSION\_4** link and click **Active.** 

The following screenshot displays the non-default version of the PERSON\_BASIC\_SYNC service operation:



Service Service Operation Version Operation Type Description Comments	PERSON_BASIC_SYNC PERSON_BASIC_SYNC VERSION_4 Asynchronous - One Way Personal Data Sync	R		
Message Information				
Туре	Request			
Message Version	PERSON_BASIC_SYNC.VERSION_4	Q	<u>View Message</u>	2
*Queue Name	PERSON_DATA	Q	View Queue	Add New Queue
Save				
Service Operation Versions   Service	Operation Versions			

6. Click the Handlers tab, as shown in the following screenshot.

Service Operation Version

Operation Ty Handlers	ype: Asynchronous - C		a heisa dha san an ta 🕅 t 👹	First 1-4	- * *	<b>N</b>		
Name	*Туре		I Eind   View All   🖓   🛗	*Status	of 4	Last		
SCC_HR_PERSON	On Notify	1	Application Class	Inactive	~	Details	+	1
SCC_NSI_PERSON_SYNC	On Notify		Application Class	Inactive	*	<b>Details</b>	+	
SCC_PERSON	On Notify		Application Class	Inactive	~	Details	+	1
SCC_SERVICE	On Notify		Application Class	Active	~	Details	+	

- 7. Confirm that the SCC\_SERVICE OnNotify Handler is Active. Click Details.
- 8. Confirm that the values are set as shown in the following screenshot and click **OK**.



Handler Details		
Handler Name: Handler Type: Description: Comments:	SCC_SERVICE OnNty Personal Data Sync	
Handler Owner: Application Class		
*Package Name: *Path: Class ID:	SCC_SERVICE Q HANDLERS Q OnNotifyManager Q	
Method:	OnNotify	

- 9. Click the Routing Definitions tab.
- **10.** Confirm that the **Local Routing SCC\_PERSON** is Active, as shown in the following screenshot:

Routing Definitions Paran	neters Routing Properties	
*Service Operation Version	SCC_PERSON PERSON_BASIC_SYNC INTERNAL SCC Person Sync routing	Active System Generated Graphical View
*Sender Node *Receiver Node		Unordered Segments
Operation Type Owner ID Save	Asynchronous - One Way Campus Community	

Routing Definitions | Parameters | Routing Properties

**11.** On the Parameters tab, confirm that the values are set as shown in the following screenshot:



Routing Definitions	Parameters	Routin	g Properties			
	Routing Nan	ne SC	C_PERSON			
	Service Operation	on PE	RSON_BASIC_	SYNC		
Servic	e Operation Versi	on INT	ERNAL			
	Sender No	de CS	900IMA			
	Receiver No	de CS	900IMA			
Parameters						
		Туре	Outbound Re	quest		
	Externa	l Alias	PERSON_BAS	SIC_SYNC.INTERNAL		
				Alias References		
Messa	ige.Ver into Transf	form 1				Q
	Transform Prog	ram 1			Q	
	Transform Prog	ram 2			Q	
	-					
Messag	e.Ver out of Trans	torms				Q
Save	Return					

Routing Definitions | Parameters | Routing Properties

- 12. Click Save.
- 13. Click Return.

#### 2.2.2.3.2.2 Activating the SCC\_PERSON\_SYNC Service Operation

To activate the SCC\_PERSON\_SYNC service operation:

- 1. In PeopleSoft Internet Architecture, expand PeopleTools, Integration Broker, Integration Setup, and then click Service Operations.
- 2. On the Find Service Operation tab, enter SCC\_PERSON\_SYNC in the Service field, and then click Search.
- 3. Click the SCC\_PERSON\_SYNC link.
- **4.** In the Default Service Operation Version region, enter v1 in the **Version** field and click **Active**.

The following screenshot displays the default version of the SCC\_PERSON\_SYNC service operation:

General Handlers f	Routings	
General Handlers I Service Operation: Operation Type: *Operation Description: Operation Comments: Owner ID:	SCC_PERSON_SYNC Asynchronous - One Way Person Extensions Data	User/Password Required *Reg Verification: None v Service Operation Security
Operation Alias:		
Default Service Operation	Version	
*Version: Version Description: Version Comments:	V1 Person Extensions Data	C Default C Active Routing Status Any-to-Local: Does not exist
		Local-to-Atom: Does not exist.
Introspection	Non-Repudiation Runtime Schema Validation	Routing Actions Upon Save  Generate Any-to-Local  Regenerate Local-to-Local  Warning: Regenerating sets all routing field values to their initial state.
Message Information		
Type: Message.Version: *Queue Name:	Request SCC_PERSON_SYNC.VERSION_1 PERSON_DATA	Q         View Message           Q         View Queue         Add New Queue
Save R	eturn to Service Add Version	

- 5. On the Handlers tab, confirm that the SCC\_SERVICE is Active. Click Details.
- 6. Confirm that the values are set as shown in the following screenshot and click **OK**.

#### Handler Details

Handler Name: Handler Type: Description: Comments:	SCC_SERVICE OnNty Constituent Information
Handler Owner:	
Application Class	
*Package Name:	SCC_SERVICE
*Path:	HANDLERS
Class ID:	OnNotifyManager
Method:	OnNotify 🗸
OK Cancel	



- 7. Click the **Routings** tab.
- 8. Select the SCC\_SERVICE routing definition and click Activate Selected Routings, as shown in the following screenshot:

Defau	andlers Routings Operation SCC_PERSON_ It Version v1 ting Name	SYNC	Add						
Routing Defin	nitions					Personalize   Find	View Al   🐼   🗮	First 🚺 1-2 of 2 🚺 (J	ast
Selected	Name	Version	Operation Type	Sender Node	Receiver Node	Direction	Status	Results	
	SCC_SERVICE	v1	Asynch	CS900IMA	CS900IMA	Local	Active		-
	SCC PERSON SYNC	v1	Asynch	CS900IMA	PSFT_CR	Outbound	Inactive		
Inactivate	e Selected Routings		Selected Routings						
	Ret	im to Service							
eneral ( Handi	ers   Routings								

If the SCC\_SERVICE routing is not available by default, you must add it manually and enter the following fields:

Service Operation: SCC\_PERSON\_SYNC

Sender Node, Receiver Node: Name of the default local active node. To determine the default local active node, perform the steps in the note in Defining the Routing for the SCC\_CONSTITUENT\_FULLSYNC Service Operation.

9. Click Save.

#### 2.2.2.3.2.3 Activating the SCC\_CONSTITUENT\_SYNC Service Operation

To activate the SCC\_CONSTITUENT\_SYNC service operation:

- 1. In PeopleSoft Internet Architecture, expand PeopleTools, Integration Broker, Integration Setup, and then click Service Operations.
- 2. On the Find Service Operation tab, enter SCC\_CONSTITUENT\_SYNC in the Service field, and then click Search.
- 3. Click the SCC\_CONSTITUENT\_SYNC link.
- 4. In the Default Service Operation Version region, click Active.

The following screenshot displays the default version of the SCC\_CONSTITUENT\_SYNC service operation:



General Handlers R	toutings			
Service Operation: Operation Type: *Operation Description: Operation Comments:	SCC_CONSTITUENT_SYNC Asynchronous - One Way Outbound Constituent Notificat	User/Password F *Req Verification: Service Operation Se	None	*
Owner ID:	Campus Community			
Operation Alias:				
Default Service Operation	Version			
*Version:	v1	🗹 Default	Active	
Version Description:	Outbound Constituent Notificat	Routing Status		
Version Comments:		Local-to-Local:	Does not exist Does not exist Does not exist.	
	Non-Repudiation	Routing Actions Upon	Save	
Introspection	Runtime Schema Validation	Generate Any-to-L		
Message Information				
Type:	Request			
Message.Version:	SCC_CONSTITUENT_DS.v1	Q View Message		
*Queue Name:	PERSON_DATA	Q <u>View Queue</u> Add	<u>1 New Queue</u>	
	eturn to Service Add Version			
General   Handlers   Routings				

5. Click Save.

#### 2.2.2.3.2.4 Activating the SSC\_CONSTITUENT\_SYNC Event

To activate SCC\_CONSTITUENT\_SYNC event:

- 1. In the PeopleSoft Internet Architecture, expand Set Up SACR, System Administration, Integrations, and Event Registry.
- 2. Search for and open the **SCC\_CONSTITUENT\_SYNC** message.
- 3. Click Active.
- **4.** In the Application Class region, confirm the values shown in the following screenshot:



Event Registry			
Service Operation: Description:	SCC_CONSTITUENT_SYNC Constituent Outbound Service	Active	
Long Description:			
Owner ID: Batch Replay Chunk Size:	Campus Community	<b>v</b>	
	Event Replay Support	Effective Dated Filtering	_
Application Class			
Package Name: Path:	SCC_CONSTITUENT_MGR	Q	
Application Class ID:	OutboundConstituentEvent	٩	
Save 🔍 Return to Search	TE Previous in List + Next in List		🛃 Add 🔬 Update/Display

#### 2.2.2.3.2.5 Activating the PERSON\_BASIC\_SYNC Notification Handler

To activate PERSON\_BASIC\_SYNC notification handler:

- 1. In the PeopleSoft Internet Architecture, expand Set Up SACR, System Administration, Integrations, and Notification Handler.
- 2. On the Find Service Operation tab, enter PERSON\_BASIC\_SYNC in the Service field and CM Handler in the Subscriber field. Click **Search.**
- 3. Click Active.

Notification Handlers

**4.** In the Application Class region, confirm the values shown in the following screenshot:

Service Operation: Subscriber:	PERSON_BASIC_SYNC CM Handler CM Handler	✓ Active Flag	
Description: Long Description:	Constituent Management Handler for	PERSON_BASIC_SYNC	
Application Class			
Package Name: Path: Application Class ID:	SCC_CONSTITUENT_MGR HANDLER ConstituentNotifyProcessor	<u>व</u> व	
Save Return to Searc	h Previous in List 4 Next in List		E Add Update/Display

#### 2.2.2.3.2.6 Activating the SCC\_PERSON\_SYNC Notification Handler

To activate SCC\_PERSON\_SYNC notification handler:

1. In the PeopleSoft Internet Architecture, expand Set Up SACR, System Administration, Integrations, and Notification Handler.



- 2. On the Find Service Operation tab, enter SCC\_PERSON\_SYNC in the Service field and CM Handler in the Subscriber field. Click **Search**.
- 3. Click Active.
- 4. In the Application Class region, confirm the values shown in the following screenshot:

Notification Han	dlers			
Service Operation:	SCC_PERSON_SYNC		Active Flag	
Subscriber:	CM Handler			
Description:	CM Handler			
Long Description:	Constituent Management Handler	for SCC_PERS	SON_SYNC	
Application Class			,	
Package Name:	SCC_CONSTITUENT_MGR	Q		
Path:	HANDLER		٩	
Application Class ID:	ConstituentNotifyProcessor	٩		
Save Return to Search	ch			E Add Update/Display

2.2.2.3.2.7 Verifying the Queue Status for the SCC\_CONSTITUENT\_SYNC Service Operation

To ensure that the status of the queue for the SCC\_CONSTITUENT\_SYNC service operation is Run:

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

Note:	
If the queu	e status is not Run:
a. From t	he Queue Status list, select <b>Run.</b>
b. Click S	ave.
	ON_BASIC_SYNC and SCC_PERSON_SYNC service also use this queue.

The queue status is shown in the following screenshot:



#### Queue Definitions

Queue Name PERSON_DAT/	A					
Description MaintainPerson	alData	] [	Archive	Unordered	1	
Comments HR Message Cl	hannel used by 🖉 🖉		Queue Status	Run		*
Message Object Employee and M			Owner ID	HR Core Ob	ects	~
Employee and t	von-Employee					
Operations Assigned to Queue		Define Partiti	oning Fields			
	1-10 of	Common Fie	lds	View Al	First 🚺 1-3 (	of 3 🔝 Last
Operations 90	Last	Include	Field		<u>Alias Name</u>	
Service Operation	Version		OPERATIONNAME			
CS ADM APPL DATA FULLSYNC	VERSION_1		PUBLISHER			
CS ADM PRSPCT DATA FULLSYNC	-		PUBPROC			
CS TEST SCORES FULLSYNC	VERSION_1		robritoo			
HCR ADD JOB	VERSION_1 VERSION_1					
HCR ADD JOB ACK HCR ADD PERSON	VERSION_1					
HCR ADD PERSON ACK	VERSION 1					
HCR CAN JOB	VERSION_1					
PERSON ACCOMP FULLSYNC	VERSION 1					
PERSON ACCOMP SYNC	VERSION_2					
	_	Add Field				
Save		Add Field				
Return to Search 🐨 Notify						🛃 Add 🔊 Update

4. Click Return to Search.

#### 2.2.2.3.2.8 Setting Up the Security for Service Operations

Perform this procedure for each of the following service operations:

- PERSON\_BASIC\_SYNC
- SCC\_PERSON\_SYNC
- SCC\_CONSTITUENT\_SYNC

To set up the security for the PERSON\_BASIC\_SYNC service operation:

- 1. In PeopleSoft Internet Architecture, expand PeopleTools, Integration Broker, Service Utilities, and then click Service Operation Permissions.
- 2. In the Operation field, enter PERSON\_BASIC\_SYNC and click Search.
- 3. In the Service Operations region, click the **Set Security** link, as shown in the following screenshot:



#### **Service Operation Permissions**

Service System Status Development

Level			
O Integration Group	Group Name		
Show All	Subgroups		
O Filter by	Subgroup		
🔿 No Subg	roups		
✓ Show Se	ervices tied to Group		
Service	Service		
Operation	Operation	PERSON_BASIC_SYNC	Q
	No Permissio	ns Exist	
Service Operations	Personalize   Find	View All   🖾   🛗 🛛 First	💶 1 of 1 💵 Last
<u>Service</u>	Service Operation	Permissions Set	
PERSON_BASIC_SYNC	PERSON_BASIC_SYNC		Set Security

 Attach the OIMCS permission list to the PERSON\_BASIC\_SYNC service operation. This list is created in Step 3 of the preinstallation procedure discussed in Creating a Permission List.

To attach the permission list:

#### Note:

This procedure describes how to grant access to the OIMCS permission list. The OIMCS permission list is used as an example. But, to implement this procedure you must use the permission list (attached through a role) to the user profile that has the privilege to modify personal data in the target system.

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

The **OIMCS** permission list appears.

c. From the Access list, select Full Access.

The following screenshot displays the permission list with Full Access:



Permission	Personalize   Find	First 📔	1-5 of 5 🖸 Last
Permission List		Access	
HCCPCSSA1000		Full Access	+ -
HCSPSERVICE		Full Access	✓ ± -
HCSPSERVICETL		Full Access	✓ + -
OHCSPRSSERVICE	l .	Full Access	✓ + -
OIMCS	Q	Full Access	<ul> <li>+</li> </ul>
UMCS	<u> </u>	Full Access	

- d. Click Save.
- e. Click Return to Search.
- 5. Repeat the Steps 1 to 4 for the SCC\_PERSON\_SYNC and SCC\_CONSTITUENT\_SYNC service operations.

2.2.2.3.2.9 Defining the Routing for the SCC\_CONSTITUENT\_SYNC Service Operation

To define the routing for the SCC\_CONSTITUENT\_SYNC service operation:

- **1.** On the Routing tab, enter SCC\_CONSTITUENT\_SYNC\_CS\_OIM as the routing name and then click **Add**.
- 2. On the Routing Definitions tab, enter the following:

Sender Node: PSFT\_CS



No	te:
Th no	e Sender Node is the default active local node. To locate the sender de:
a.	Click the Look up icon.
b.	Click <b>Default</b> to sort the results in descending order.
	The default active local node should meet the following criteria:
	Local Node: 1
	Default Local Node: Y
	Node Type: PIA
	Only one node can meet all the above conditions at a time.
c.	Select the node.
d.	Click Save.

Receiver Node: OIM\_CS\_NODE

The following screenshot displays the Sender and Receiver nodes:

Routing Definitions	Parameters	Connector Properties	Routing Properties	
* Service Ope V *Desc	ersion v1	S_TO_OIM DNSTITUENT_SYNC ntal constituent sync	Active System Graphical Vi	n Generated
	r Node CS900II r Node OIM_CS			
Ow	/ner ID	ronous - One Way	~	
Save	Retu	m		

Routing Definitions | Parameters | Connector Properties | Routing Properties

- 3. On the Parameters tab, verify that the following values are set as default:
  - a. In the External Alias field, enter SCC\_CONSTITUENT\_SYNC.v1.
  - b. In the Message.Ver into Transform 1 field, enter SCC\_CONSTITUENT\_DS.v1.
     The following screenshot displays the preceding steps:



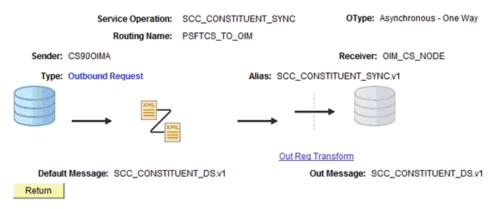
Routing Definitions	Parameters	Connector Properties	Routing Properties			
	Routing Name PSFTCS_TO_OIM					
	-	tion SCC_CONSTITUEN	T_SYNC			
Servic	e Operation Vers	_	-			
	Sender No	ode CS900IMA				
	Receiver No	ode OIM_CS_NODE				
Parameters						
		Type Outbound Reque	est			
	Extern	al Alias SCC_CONSTITU	ENT_SYNC.v1			
			Alias References			
Messa	ge.Ver into Trans	form 1 SCC_CONSTITU	ENT_DS.v1	Q		
	Transform Pro	gram 1		Q		
	Transform Pro	gram 2		Q		
		-				
Messag	e.ver out of Tran	sforms SCC_CONSTITU	ENT_DS.VI	Q		
Save	Return					

Routing Definitions | Parameters | Connector Properties | Routing Properties

- c. In the Message.Ver out of Transforms field, enter SCC\_CONSTITUENT\_DS.v1.
- d. Click Save.
- e. Click **Return** to go back to the Routings tab of the Service Operation, and verify whether your routing is active.

The following graphic displays the routing SCC\_CONSTITUENT\_SYNC\_CS\_OIM and its transformation:

#### Integration Broker Routing Graphic



2.2.2.3.2.10 Displaying the EI Repository Folder

To display the EI Repository folder:



Note:

- If you have performed this procedure as described in Displaying the El Repository Folder, then you can skip this section.
- Perform this procedure using the PeopleSoft administrator credentials.
- 1. In the PeopleSoft Internet Architecture, expand **People Tools, Portal,** and then **Structure and Content.**
- 2. Click the Enterprise Components link.
- 3. Click the Edit link for El Repository, and then uncheck Hide from portal navigation.

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

Folder Administratio	Folder Security			<u></u>	
Folder Admir	nistration				
Name:	EIP_CATALOG		Parent Folder:	Enterprise Components	
'Label:	EI Repository		Copy object	Select New Parent Folder	
Long Description: (254 Characters)	Enterprise Integration R	(epository			×
Product: Sequence number:	200 Valid	to date:	1900 🖲 🛛 Auti	Creation Date: Ior: PSEO	10/29/2001
Object Owner ID	0.000	Integration Repos	ISF navigation	Add Folder	
Folder Navigation					
☐ Is Folder Naviga Folder Navigation (			Q		
Folder Attributes					
Name:			F	₹ Translate	Delete
Label:					
Attribute value:					*
Add					

Save Notify
Folder Administration | Folder Security

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

#### 2.2.2.3.2.11 Activating the PERSON\_BASIC\_SYNC Message

To activate PERSON\_BASIC\_SYNC message:



	Note: To perform this step, your User Profile must have the EIR Administrator role consisting of <b>EOEI9000</b> and <b>EOCO9000</b> permission lists.				
1.	In the PeopleSoft Internet Architecture, expand Enterprise Components, El Repository, and then click Message Properties.				
2.	Search for and open the <b>PERSON_BASIC_SYNC</b> message.				
3.	Click Activate All.				
	The following screenshot displays the message to be activated:				
	<b>Message Properties</b> To activate or inactivate Messages and their Subscriptions, narrow your search by entering the first few letters of a Message Name. Select which Messages and Subscriptions you want to activate or inactivate by manually make changes or by pushing the Activate All or Inactivate All button, then Save.				
	Message Name Begins With: PERSON_BASIC_SYNC Search				
	Personalize   Find   View All   🖾   🛗 First 🗹 1 of 1 🔽 Last				
	Message Subscription ETT Activate All Activate All				
	1 PERSON_BASIC_SYNC Active V Inactivate All				
	Save				

4. Click Save.

2.2.2.3.3 Preventing Transmission of Unwanted Fields During Incremental Reconciliation

This section contains the following topics:

- About Preventing Transmission of Unwanted Fields During Incremental Reconciliation
- Removing Unwanted Fields at Message Level

2.2.2.3.3.1 About Preventing Transmission of Unwanted Fields During Incremental Reconciliation

By default, PeopleSoft messages contain fields that are not needed in Oracle Identity Manager. If there is a strong use case that these fields should not be published to Oracle Identity Manager, then do the following:

Locate if there are any local-to-local or local-to-third party PeopleSoft active routings for the service operations using the message under study.

• If none, then you can safely remove the unwanted fields at message level. See Removing Unwanted Fields at Message Level section for more information.



- If active routings exist, analyze the subscription or handler code of the routing to determine the fields they are utilizing and the ones not needed in Oracle Identity Manager. If so, remove the unwanted fields at message level. See Removing Unwanted Fields at Message Level section for more information.
- Lastly, if there are active routings that use these sensitive fields that you do not want to transmit to Oracle Identity Manager, then you need to write a transformation.

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

http://download.oracle.com/docs/cd/E13292\_01/pt849pbr0/eng/psbooks/ tibr/book.htm

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

http://download.oracle.com/docs/cd/E13292\_01/pt849pbr0/eng/psbooks/ tpcr/book.htm

#### 2.2.2.3.3.2 Removing Unwanted Fields at Message Level

To remove unwanted fields at the message level:

- 1. Expand PeopleTools, Integration Broker, Integration Setup, and then click Messages.
- 2. Search for and open the desired message, for example, SCC\_CONSTITUENT\_DS.v1 used for incremental reconciliation.
- **3.** Expand the message.



Message Definition	Schema		
⊥ Status:	Message cannot be cha	inged. Message	referenced in runtime tables.
Message	SCC_CONSTITUENT_D	S	Schema Exists: Yes
Version	v1		Part Message
			Exclude Description in Schema
Description:	Outbound Constituent Sy	nc Msg.	Single Level 0 Row
Owner ID	Campus Community	<b>N</b>	Include Namespace
	Outbound Constituent Sy	nc Message	Suppress Empty XML Tags
Comments	outbound constituent of	ne message	Message Type
			Rowset-based
			Nonrowset-based
Service Operation Refe	rences		Container
View Records Only	View Inclue	ded Fields Only	Add Record to Root
Left Right			
SCC_CONSTITUEN	-		
	ERSON I		
	<u>`</u>		
	DUNTRY		
Interview And American Amer	ATE		
~	AME TYPE I		
	DR TYPE I		
	<u>ER PDE I</u> ER NID I		
	ER PHONE I		
_	ER EMAIL I		
~	L PERSON		
Save	Save As		

4. Navigate to the field that you do not want to transmit to Oracle Identity Manager, for example, NAME\_ROYAL\_PREFIX.



✓ ✓ DT OF DEATH		
🖃 😂 <u>SCC NAME TYPE I</u>		
SCC UID		
🖉 🖌 <u>Emplid</u>		
🖉 🖌 NAME TYPE		
🖃 😂 <u>SCC PER NAME I</u>		
🖉 🖌 <u>EMPLID</u>		
🖉 🖌 NAME TYPE		
🖉 🖌 <u>EFFDT</u>		
EFF STATUS		
COUNTRY NM FORMAT		
🖉 🖌 NAME		
MAME_INITIALS		
NAME_PREFIX		
V V NAME SUFFIX		
MAME ROYAL PREFIX		
🖉 🗸 NAME ROYAL SUFFIX		
NAME_TITLE		
LAST NAME SRCH		
FIRST NAME SRCH		
🖉 🖌 LAST NAME		
V Y FIRST NAME		
V V MIDDLE NAME		
SECOND LAST NAME		
SECOND LAST SRCH		
VAME AC		
PREF FIRST NAME		
PARTNER LAST NAME		
PARTNER ROY PREFIX		
A LAST NAME PREF NLD		
VAME DISPLAY		
E SCC ADDR TYPE I		
E SCC PER PDE I		
E SCC PER NID I		

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



Message Field Properties		
Record:	NAMES	
Field Name:	NAME_ROYAL_PREFIX	
Alias Name:		
Include		
OK	Cancel	

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

# 2.2.2.4 Enabling Content-based Routing for Incremental Reconciliation in SCC CONSTITUENT SYNC Message

This section contains the following topics:

- About Content-based Routing with Affiliations
- Enabling Content-Based Routing With Affiliations

#### 2.2.2.4.1 About Content-based Routing with Affiliations

The assumption is that other routings and service operations are properly configured. When person data is added or updated, a PERSON\_BASIC\_SYNC message triggers an SCC\_CONSTITUENT\_SYNC message to publish. Before that message routes to any target nodes, it runs through the OnRoute Send handler to determine the list of nodes to which it will route. It starts with the list of current routings for that service operation and winnows it down. If the node is not found in the Affiliation Routing table, it will not route to that node. If it is found, then it checks to see if the Send Blank Affiliations option is enabled. If it is and there are no affiliation codes in the message (and in this case there are not), then it sends it on through. If it is not enabled (not checked), then it does not send it through. You will be leaving it unchecked.

When an affiliation is added, changed or deleted for a person, an SCC\_CONSTITUENT\_SYNC message is published. The OnRoute Send grabs this one and looks to see if any of the affiliations in the message are in the Affiliation Routing table. If they are, the message is sent on through. If they are not, then the message skips that node.

Next if the message is going on through, it gets to the routing transformation. The transformation program checks to see if the person data is blank in this message. If it is, then it fills it in with data from the database and sets the PSCAMA AUDIT\_ACTN to 'A' (add). Then it lets it go out to the target node.

#### 2.2.2.4.2 Enabling Content-Based Routing With Affiliations

To enable content-based routing with affiliations:

**1.** Set affiliation routings as follows:



- a. Navigate to Set Up SACR, Common Definitions, Affiliations, and Affiliation Routing.
- **b.** Add the Oracle Identity Manager target node.
- c. Add the affiliation codes for which you want to receive SCC\_CONSTITUENT\_SYNC messages.
- 2. Enable affiliation content-based routing as follows:
  - a. Navigate to PeopleTools, Integration Broker, Integration Setup, and Service Operations.
  - b. Select service operation SCC\_CONSTITUENT\_SYNC.
  - c. Select the Handlers tab.
  - d. Add a new row with the following details:

Handler name: ROUTERSENDHDLR.\*

**Type**: OnRoute

Implementation: Application Class

Status: Active

e. Click Details and enter the following information:

Description: Affiliations Filter

Comments: Affiliations Filter

Handler Owner: SCC

Package Name: SCC\_AFFILIATIONS

Path: HANDLER

Class ID: AffiliationOnRouteSend

Method: OnRouteSend

- f. Click OK and Save.
- g. Click the Routings tab.
- **h.** Click the link for the routing name that corresponds to the outbound routing from PeopleSoft Campus to the Oracle Identity Manager target node.
- i. Click the **Parameters** tab and add the following details:

Transform Program 1: SCC\_AFL\_RICH (this may clear defaults.)

The External Alias: SCC\_CONSTITUENT\_SYNC.v1

Message.Ver into Transform 1: SCC\_CONSTITUENT\_DS.v1

Message.Ver out of Transforms: SCC\_CONSTITUENT\_DS.v1

Transform Program: blank

j. Click Save, Return, and then Save.



#### Note:

No matter what you name this handler, the system always automatically renames it to ROUTESENDHDLR. This means that you can only have one OnRoute Send handler for a given service operation.

## 2.2.3 Installation with Other PeopleSoft Connectors

If you want to use the PeopleSoft Campus connector along with the PeopleSoft Employee Reconciliation and PeopleSoft User Management connectors, then consider the following points:

 Installing the Campus connector after installing the Employee Reconciliation and PeopleSoft User Management connectors

When installing the Campus connector after the Employee Reconciliation or the User Management connector, you must remove the existing listener (PeopleSoftOIMListener) and deploy the new listener shipped with the Campus connector. This is required because the listener uses the PSFTCommon.jar file, which has been modified to include Campus specific classes.You must also ensure that the PSFTCommon.jar file has been updated in the Oracle Identity Manager database during the connector installation.

 Installing the Employee Reconciliation or User Management connector after installing the Campus connector

When the Employee Reconciliation or User Management connector is installed after the Campus connector, you must continue to use the existing listener shipped with the Campus connector.

During installation, the PSFTCommon.jar file in the Oracle Identity Manager database would be replaced with the PSFTCommon.jar file shipped with the Employee Reconciliation or User Management connector. To restore the PSFTCommon.jar file shipped with the Campus connector, run the UpdateJars utility shipped with Oracle Identity Manager. This file has some Campus connector specific additions.

## 2.3 Postinstallation

Postinstallation information is divided across the following sections:

- Configuring Oracle Identity Manager
- Configuring the Target System

### 2.3.1 Configuring Oracle Identity Manager

#### Note:

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



- Enabling Logging
- Setting Up the Lookup.PSFT.Campus.Configuration Lookup Definition
- Setting Up the Lookup.PSFT.Campus.ExclusionList Lookup Definition
- Configuring SSL
- Creating an Authorization Policy for Campus ID
- Displaying UDFs in Oracle Identity Manager 11.1.2 or Later
- Localizing Field Labels in UI Forms

### 2.3.1.1 Enabling Logging

This section contains the following topics:

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

#### 2.3.1.1.1 Log Levels and ODL Message Types

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

• SEVERE.intValue()+100

This level enables logging of information about fatal errors.

SEVERE

This level enables logging of information about errors that may allow Oracle Identity Manager to continue running.

WARNING

This level enables logging of information about potentially harmful situations.

INFO

This level enables logging of messages that highlight the progress of the application.

CONFIG

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

FINE, FINER, FINEST

These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These message types are mapped to ODL message type and level combinations as shown in Table 2-4.

Table 2-4	Log Levels and ODL	Message Type:Level Combinat	tions
-----------	--------------------	-----------------------------	-------

Java Level	ODL Message Type:Level	
SEVERE.intValue()+100	INCIDENT_ERROR:1	



Java Level	ODL Message Type:Level
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

Table 2-4 (Cont.) Log Levels and ODL Message Type:Level Combinations

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

DOMAIN\_HOME/config/fmwconfig/servers/OIM\_SERVER/logging.xml

Here, *DOMAIN\_HOME* and *OIM\_SEVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

#### 2.3.1.1.2 Enabling Logging on Oracle WebLogic Server

To enable logging on Oracle WebLogic Server:

- **1.** Edit the logging.xml file as follows:
  - a. Add the following blocks in the file:

```
<log_handler name='psft-cs-handler' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='[FILE_NAME]'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/></property name='encoding' value='UTF-8'/>
   </log_handler>
<logger name="ORACLE.IAM.CONNECTORS.PSFT" level="[LOG_LEVEL]"</pre>
useParentHandlers="false">
     <handler name="psft-cs-handler"/>
     <handler name="console-handler"/>
   </logger>
<logger name="ORACLE.IAM.CONNECTORS.PSFT.CAMPUS" level="[LOG_LEVEL]"</pre>
useParentHandlers="false">
<handler name="psft-cs-handler"/>
<handler name="console-handler"/>
</logger>
```

b. Replace all occurrences of [LOG\_LEVEL] with the ODL message type and level combination that you require. Table 2-4 lists the supported message type and level combinations.

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

## The following blocks show sample values for [LOG\_LEVEL] and [FILE\_NAME]:

```
<log_handler name='psft-cs-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
    <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers
\oim_server1\logs\oim_server1-diagnostic-1.log'/>
    <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
    <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>
<logger name="ORACLE.IAM.CONNECTORS.PSFT" level="NOTIFICATION:1"</pre>
useParentHandlers="false">
    <handler name="psft-cs-handler"/>
     <handler name="console-handler"/>
  </logger>
<logger name="ORACLE.IAM.CONNECTORS.PSFT.CAMPUS" level="NOTIFICATION:1"</pre>
useParentHandlers="false">
<handler name="psft-cs-handler"/>
<handler name="console-handler"/>
</logger>
```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

#### Note:

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

- 2. Save and close the file.
- 3. Set the following environment variable to redirect the server logs to a file:

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

export WLS\_REDIRECT\_LOG=FILENAME

Replace *FILENAME* with the actual name of the file to which you want to redirect the output.

4. Restart the application server.



### 2.3.1.2 Setting Up the Lookup.PSFT.Campus.Configuration Lookup Definition

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

For example, the mapping for the SCC\_CONSTITUENT\_SYNC message in this lookup definition is defined as follows:

Code Key: SCC\_CONSTITUENT\_SYNC

Decode: Lookup.PSFT.Message.SccConstituentSync.Configuration

You can configure the message names, such as SCC\_CONSTITUENT\_SYNC and SCC\_CONSTITUENT\_FULLSYNC defined in this lookup definition.

Consider a scenario in which the target system sends the SCC\_CONSTITUENT\_SYNC.VERSION\_3 message. You must change the Code Key value in this lookup definition to implement the message sent by the target system.

To modify or set the Code Key value:

- 1. On the Design Console, expand Administration and then double-click Lookup Definition.
- 2. Search for and open the Lookup.PSFT.Campus.Configuration lookup definition.
- 3. Click Add.
- 4. In the Code Key column, enter the name of the message you want to modify. In this scenario define the mapping as follows:

Code Key: SCC\_CONSTITUENT\_SYNC.VERSION\_3

Decode: Lookup.PSFT.Message.SccConstituentSync.Configuration

- 5. Repeat Steps 3 and 4 to modify the Code Key values for all the standard PeopleSoft messages you want to rename in this lookup definition.
- 6. Click the Save icon.

### 2.3.1.3 Setting Up the Lookup.PSFT.Campus.ExclusionList Lookup Definition

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

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



#### Note:

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

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

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

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

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

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

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

Code Key	Decode
User ID[PATTERN]	User001 User002 User088

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

Code Key	Decode
User ID[PATTERN]	00012*

6. Click the Save icon.

### 2.3.1.4 Configuring SSL

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

Configuring SSL on IBM WebSphere Application Server



Configuring SSL on Oracle WebLogic Server

#### 2.3.1.4.1 Configuring SSL on IBM WebSphere Application Server

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

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

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

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

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

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

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



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

# 2.3.1.4.1.2 Configuring SSL on IBM WebSphere Application Server with a CA Certificate

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

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

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

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

#### Note:

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



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

was\_profile\_root\config\cells\cell\_name\nodes\node\_name\key.p12

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

- **17.** To receive a signed certificate issued by a CA, perform the following tasks:
  - a. In the WebSphere Integrated Solutions Console, click Security, SSL certificate and key management, Related items, Key stores and certificates, NodeDefaultKeyStore, and then click Personal Certificates.
  - b. Click Receive a certificate from a certificate authority.
  - c. Enter the full path and name of the certificate file.
  - d. Select the default data type from the list.
  - e. Click Apply and then Save.

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

#### 2.3.1.4.2 Configuring SSL on Oracle WebLogic Server

You can configure SSL connectivity on Oracle WebLogic Server with either a selfsigned certificate or a CA certificate. Perform the procedure described in one of the following sections:



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

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

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

- Generating Keystore
- Configuring Oracle WebLogic Server

#### 2.3.1.4.2.1.1 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 the IP address of the computer on which you are configuring SSL.

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

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

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

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

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

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

#### For example:

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

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



keytool -import -alias ALIAS\_NAME -keystore NEW\_KEYSTORE\_ABSOLUTE\_PATH -file CERTIFICATE\_FILE\_ABSOLUTE\_PATH

#### For example:

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

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

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

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

#### 2.3.1.4.2.1.2 Configuring Oracle WebLogic Server

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

- Log in to the Oracle WebLogic Server console at http://localhost:7001/ console and perform the following:
  - a. Expand the servers node and select the **oim** server instance.
  - b. Select the General tab.
  - c. Select the SSL Listen Port Enabled option.
  - **d.** Ensure that a valid port is specified in the SSL Listen Port field. The default port is 7002.
  - e. Click Apply to save your changes.
- 2. Click the Keystore & SSL tab, and then click Change.
- 3. From the Keystores list, select **Custom identity And Java Standard Trust,** and then click **Continue.**
- 4. Configure the keystore properties. To do so:
  - a. In the Custom Identity Key Store File Name column, specify the full path of the keystore generated in Step 1 of Generating Keystore, for example, c:\temp\keys\keystore.jks. In the Custom Identity Key Store Type column, specify the type of keystore, for example, JKS. In the Custom Identity Key Store Pass Phrase and Confirm Custom Identity Key Store Pass Phrase columns, specify the keystore password.
  - b. Provide the Java standard trust keystore pass phrase and the Confirm Java standard trust keystore pass phrase. The default password is changeit, unless you change the password.
  - c. Click Continue.
- 5. Specify the private key alias, pass phrase and the confirm pass phrase as the keystore password. Click **Continue**.
- 6. Click Finish.
- 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 *.*>
```

ORACLE

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



2.3.1.4.2.2 Configuring SSL on Oracle WebLogic Server with a CA Certificate

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



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

- Generating Keystore
- Configuring Oracle WebLogic Server

#### 2.3.1.4.2.2.1 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 persons attempting to access a secure page in the application. This is illustrated in the following example:

```
keytool -genkey -keystore c:\temp\keys\keystore.jks -alias example088196
-keyalg RSA -storepass example1234 -keypass example1234
What is your first and last name?
[Unknown]: Must be the name or IP address of the computer
```



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

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

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

keytool -certreq -keystore ABSOLUTE\_KEYSTORE\_PATH -alias ALIAS\_NAME -keyalg
KEY\_ALGORITHM -file CERTIFICATE\_FILE\_ABSOLUTE\_PATH

For example:

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

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

- Get the certificate from a CA by using the certificate request generated in the previous step and store the certificate in a file.
- Export the keystore generated in Step 1 to a new certificate file, for example, myCert.cer, by running the following command:

keytool -export -keystore ABSOLUTE\_KEYSTORE\_PATH -alias alias-name specified in step 1 -file CERTIFICATE\_FILE\_ABSOLUTE\_PATH

#### For example:

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

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

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

#### For example:

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

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

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

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



#### 2.3.1.4.2.2.2 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, 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, for example, c:\temp\keys\rootkeystore.jks. In the Custom Trust Key Store Type column, specify the type of keystore, for example, JKS. In the Custom Trust Key Store Pass Phrase and Confirm Custom Trust Key Store Pass Phrase columns, specify the keystore password.
  - c. Provide the Java standard trust keystore password. The default password is changeit, unless you change the password.
  - d. Click Continue.
- 5. Specify the alias name and private key password. Click Continue.
- 6. Click Finish.
- 7. Restart Oracle WebLogic Server. If the server starts successfully with the SSL configuration, then lines similar to the following are recorded in the startup log:

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

#### Note:

7002 is the default SSL port for Oracle WebLogic Server.



### 2.3.1.5 Creating an Authorization Policy for Campus ID

### Note:

Perform this procedure only if you are using Oracle Identity Manager release prior to 11.1.2.

To create an authorization policy for Campus ID, refer to the instructions given in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*. The following instructions are specific to individual steps of the procedure described in Creating an Authorization Policy for User Management. For detailed information on the individual steps, see http://docs.oracle.com/cd/E21764\_01/doc.1111/e14316/ auth\_policy.htm#BGBHGHJI.

• When you reach Step 3, then:

In the Policy Name field, enter Campus ID Authorization Policy.

• When you reach Step 4, then:

In the Description field, enter Campus ID Authorization Policy.

• When you reach Step 7, then:

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

- Modify User Profile
- Search User
- View User Details

#### Click Edit Attributes.

On the Attribute Settings page, clear all the check boxes and select Campus ID.

• When you reach Step 14 c, then:

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

### 2.3.1.6 Displaying UDFs in Oracle Identity Manager 11.1.2 or Later

In Oracle Identity Manager release 11.1.2 or later, some user-defined attributes (UDFs), such as Campus ID, that are included in the connector are created only in the backend. If you want to display these attributes as form fields in the Oracle Identity Manager user interface (UI), then you must customize the associated pages on the UI to add the custom form fields. To do so:

- **1.** Log in to Oracle Identity System Administration.
- 2. Create and activate a sandbox.
- 3. From the Identity System Administration Console, in the Upgrade region, click Upgrade User Form.

All the UDFs are listed.

4. Click Upgrade now.



5. Publish the sandbox.

For detailed steps to be performed, see Configuring Custom Attributes in Oracle Fusion Middleware Administering Oracle Identity Manager.

### 2.3.1.7 Localizing Field Labels in UI Forms

### Note:

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

To localize field label that you add to in UI forms:

- 1. Log in to Oracle Enterprise Manager.
- 2. In the left pane, expand Application Deployments and then select oracle.iam.console.identity.sysadmin.ear.
- 3. In the right pane, from the Application Deployment list, select MDS Configuration.
- 4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
- 5. Extract the contents of the archive, and open one of the following files in a text editor:
  - For Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0) and later:

SAVED\_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle\_en.xlf

For releases prior to Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):

SAVED\_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf

- 6. Edit the BizEditorBundle.xlf file in the following manner:
  - a. Search for the following text:

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

**b.** Replace with the following text:

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

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

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

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



```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_AFFLN_CODE__c_description']}">
<source>Affiliation Code</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.PSFTCampus.entity.PSFTCam
pusEO.UD_AFFLN_CODE__c_LABEL">
<source>Affiliation Code</source>
<target/>
</trans-unit>
```

- d. Open the resource file from the connector package, for example PSFT-CS\_fr.properties and get the value of the attribute from the file, for example, global.udf.UD\_AFFLN\_CODE=Code d'affiliation.
- e. Replace the original code shown in Step 6.c with the following:

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_AFFLN_CODE__c_description']}">
<source>Affiliation Code</source>
<target>Code d'affiliation</target>
</trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.PSFTCampus.entity.PSFTCam
pusEO.UD_AFFLN_CODE__c_LABEL">
<source>Affiliation Code</source>
<target>Code d'affiliation</target>
</trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.PSFTCampus.entity.PSFTCam
pusEO.UD_AFFLN_CODE__c_LABEL">
<source>Affiliation Code</source>
<target>Code d'affiliation</target>
</trans-unit>
```

- f. Repeat Steps 6.a through 6.d for all attributes of the process form.
- **g.** Save the file as BizEditorBundle\_*LANG\_CODE*.xlf. In this file name, replace LANG\_CODE with the code of the language to which you are localizing.

Sample file name: BizEditorBundle\_fr.xlf.

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

### See Also:

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

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

### 2.3.2 Configuring the Target System

Postinstallation on the target system configuring SSL.

To configure SSL:

**1.** Copy the certificate to the computer on which PeopleSoft Campus is installed.



#### Note:

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

2. Run the following command:

PEOPLESOFT\_HOME/webserv/peoplesoft/bin/pskeymanager.cmd -import

- 3. When prompted, enter the current keystore password.
- 4. When prompted, enter the alias of the certificate to import.

#### Note:

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

If you are using IBM WebSphere Application Server, then enter  ${\tt root}$  as the alias.

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

#### Note:

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

6. When prompted for the following:

Trust this certificate? [no]: yes

Select yes and press Enter.

7. Restart the Web server of the target system.

# 2.4 Postcloning Steps

You can clone the PeopleSoft Campus connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

### See Also:

Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about cloning connectors and the steps mentioned in this section



After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

Lookup Definition

If the lookup definition contains the old lookup definition details, then you must modify it to provide the new cloned lookup definition names. If the Code Key and Decode values are referring the base connector attribute references, then replace these with new cloned attributes.

Scheduled Task

You must replace the base connector resource object name in the scheduled task with the cloned resource object name. If the scheduled task parameter has any data referring to the base connector artifacts or attributes, then these must be replaced with the new cloned connector artifacts or attributes.

Localization Properties

You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

For example, the process form attributes are referenced in the Japanese properties file, Campus\_ja.properties, as global.udf.UD\_CAMPUS\_ALIASNAME. During cloning, if you change the process form name from UD\_CAMPUS to UD\_CAMPUS1, then you must update the process form attributes to global.udf.UD\_CAMPUS1\_ALIASNAME.



# 3 Using the Connector

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

- Summary of Steps to Use the Connector
- Seeding Roles into Oracle Identity Manager
- Verifying the Affiliation Status Code
- Verifying the Entries in Attribute Mapping Lookup Definitions
- Performing Full Reconciliation
- Performing Incremental Reconciliation
- Limited Reconciliation
- Resending Messages That Are Not Received by the PeopleSoft Listener
- Configuring Scheduled Jobs

## 3.1 Summary of Steps to Use the Connector

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

### Note:

It is assumed that you have performed all the procedures described in the preceding chapter.

- 1. Generate a CSV file on the PeopleSoft Campus target system containing all the affiliation data.
- 2. Copy this file to a directory on the Oracle Identity Manager host computer.
- 3. Run the PeopleSoft Campus Role Creation scheduled job to seed the roles in Oracle Identity Manager corresponding to each unique affiliation.
- Generate XML files for the SCC\_CONSTITUENT\_FULLSYNC message for all persons. See Generating XML Files for more information.
- 5. Copy these XML files to a directory on the Oracle Identity Manager host computer.
- 6. Configure the PeopleSoft Campus Trusted Full Reconciliation scheduled task for the SCC\_CONSTITUENT\_FULLSYNC message. The XML files are read by this scheduled task to generate reconciliation events. See Configuring the Scheduled Task for Person Data Reconciliation for more information.
- Configure the PeopleSoft Campus Affiliation Effective Date Processor scheduled task. See Configuring the Scheduled Task for Processing Affiliation Effective Date for more information.



8. Configure the PeopleSoft Campus Role Creation scheduled task. This scheduled task reads the affiliation data from a CSV file and creates corresponding roles in Oracle Identity Manager. See Importing CSV File into Oracle Identity Manager to Create Roles for more information.

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

# 3.2 Seeding Roles into Oracle Identity Manager

You must seed roles into Oracle Identity Manager corresponding to each unique affiliation in PeopleSoft Campus. This is done so that when a particular affiliation (a resource in Oracle Identity Manager) is assigned to a user, then if the affiliation is active, the corresponding role is assigned to the user.

This section contains the following procedures:

- Generating CSV File
- Importing CSV File into Oracle Identity Manager to Create Roles

### 3.2.1 Generating CSV File

To generate CSV file for all existing roles in the target system:

- **1.** In PeopleSoft Internet Architecture, navigate to Reporting Tools, Query, and Query Manager.
- 2. Enter the query name as SCC\_AFFILIATION\_TYPE\_CODES and click **Search**, as shown in the following screenshot.

- 3. Click HTML under the Run to HTML column.
- In the new html page, click CSV Text File and save the CSV file, as shown in the following screenshot.



	Jownload ew All	l results in :	Excel Sprea	dSheet CSV T	ext File	XML Fil	<u>e</u> (7 kb)				First	₹ 1-7 o	f 7 🕞 Las
	Institution	Aff. Code	Eff Date	Sponsoring Dept	Status	Descr	Description	AppClass	Children	Root	Filter	Manual	Affiliation Ran
1	PSUNV	STUDENT	08/16/2012		A		Student of PS UNV.	SCC_AFFILIATIONS:IMPLEMENTATION:ManualStub	N	N		N	03000
2	GLAKE	LECTURER	09/04/2012		A		GLAKE LECTURER	SCC_AFFILIATIONS:IMPLEMENTATION:ManualStub	N	N		N	05000
3	PSUNV	PROSPECT	08/21/2012	ADMISSIONS	A		PROSPECT affiliation	SCC_AFFILIATIONS:IMPLEMENTATION:ManualStub	N	N		N	01000
4	PSUNV	EMPLOYEE	08/13/2012		A		Sample manual employee code.	SCC_AFFILIATIONS:IMPLEMENTATION:ManualStub	N	N		N	04000
5	PSUNV	RECTR_TMPL	01/01/1900	10000	A		PSUNV Recruiter	SCC_AFFILIATIONS:IMPLEMENTATION:Recruiter_template	N	Y		N	02000
6	GLAKE	STUDENT	09/03/2012		A		GLAKE Student	SCC_AFFILIATIONS:IMPLEMENTATION:ManualStub	N	N		N	
7	PSUNV	ALUMN_TMPL	02/20/2009	ADVANCEMNT	A	Alumni for PSUNV	PSUNV Alumni	SCC_AFFILIATIONS:IMPLEMENTATION:Alumni_template	N	Y		N	01000

You must copy this CSV file to a directory on the Oracle Identity Manager host computer.

### 3.2.2 Importing CSV File into Oracle Identity Manager to Create Roles

When you run the Connector Installer, the PeopleSoft Campus Role Creation scheduled task is automatically created in Oracle Identity Manager.

This scheduled task reads the affiliation data from a CSV file and creates corresponding roles in Oracle Identity Manager. You must enter the path of the CSV file generated in Generating CSV File as the value of the scheduled task attribute. The role names are in the following format:

#### PSFTCAMPUS~<INSTITUTION CODE>~<AFFILIATION CODE>

For example: PSFTCampus~PSUNV~STUDENT

Affiliation Ranks are stored as role description in the *AFFILIATION RANK:*<*RANK VALUE*> format. For example, Affiliation rank:0800.

Table 3-1 describes the attributes of this scheduled task.

#### Table 3-1 Attributes of the PeopleSoft Campus Role Creation Scheduled Task

Attribute	Description
File Path	Enter the path of the CSV file on the Oracle Identity Manager host computer.
	Sample value: /usr/data/sample.csv

### 3.3 Verifying the Affiliation Status Code

This section contains the following topics:

- About Affiliation Status
- Verifying the Affiliation Status Code on PeopleSoft Campus



### 3.3.1 About Affiliation Status

In PeopleSoft Campus, the Affiliations have a field called Affiliation Status. This connector reconciles the value of this field. You can also add your own status codes in PeopleSoft Campus. The status of the Affiliation Resource in Oracle Identity Manager (Enabled or Disabled) depends on the value of this field.

The following screenshot displays a sample Affiliation Status in PeopleSoft Campus:

Add/Update Affiliations												
24JFIRST 24jlast ID24J1												
Institution: Peop	leSoft University											
Relations to Institu	utions								Personalize	<u>Find</u>   🗖	First	1-2 of 2 🗈 Last
*Affiliation Code	Description	<u>*Start Date</u>		End Date		*Affiliation Status		<u>Descriptor</u>	Affiliation Ranking	<u>System</u> Maintained	<u>Hierarchy</u> <u>level</u>	View Details
ALUMN_TMPL	PSUNV Alumni	07/23/2012			,	Inactive		Completed	01000		1	View Details
	Student of PS UNV.		Ħ		Ħ		~	Applied 💉	03000			View Details
						Active Error						Add
						Inactive						
Save Retur	n to Search									Spell Chec	k E-Add	//////////////////////////////////////

### 3.3.2 Verifying the Affiliation Status Code on PeopleSoft Campus

To verify the Affiliation Status code on PeopleSoft Campus that corresponds to Enabled status in Oracle Identity Manager, perform the following procedure:

 Check the status code value that is passed in the SCC\_CONSTITUENT\_SYNC or SCC\_CONSTITUENT\_FULLSYNC message when the Affiliation is made Active in PeopleSoft Campus.

In the following example, the Affiliation Status code is ACT. If this code has been customized in the target system, then the value may be different.



```
<?xml version="1.0" encoding="us-ascii"?>
<scc_constituent_fullsync>
FieldTypes>
白
   <MsgData>
申
     <Transaction>
Ē
      <Transaction>
       <SCC CM PERSON I class="R">
         <EMPLID IsChanged="Y">EXCLUDE2</EMPLID>
          <SCC_UID></SCC_UID>
          <BIRTHDATE IsChanged="Y">1961-03-29</BIRTHDATE>
          <BIRTHPLACE></BIRTHPLACE>
          <BIRTHCOUNTRY IsChanged="Y">USA</BIRTHCOUNTRY>
          <BIRTHSTATE></BIRTHSTATE>
          <DT_OF_DEATH></DT_OF_DEATH>
          <NAME TYPE VW2 class="R">
申
          <PSCAMA class="R">
申
          <ADDRESS_TYPE_V2 class="R">
          <PSCAMA class="R">
<SCC_PER_PDE_I class="R">
申
          <PSCAMA class="R">
          <SCC PER NID I class="R">
          <PSCAMA class="R">
Ŧ
中
          <PERSON_SA class="R">
          <PSCAMA class="R">
申
          <SCC AFL PERSON class="R">
          <PSCAMA class="R">
申
          <SCC_AFL_PERSON class="R">
Ė
           <EMPLID>EXCLUDE2</EMPLID>
            <INSTITUTION IsChanged="Y">PSAUS</INSTITUTION>
            <SCC_AFL_CODE_IsChanged="Y">EMPLOYEE</SCC_AFL_CODE>
            <START_DT_IsChanged="Y">2012-07-15</START_DT>
            <SCC_AFL_SPONS_DEPT_IsChanged="Y">ADVANCEMNT</SCC_AFL_SPONS_DEPT>
            <END DT />
            <LASTUPDOPRID IsChanged="Y">PS</LASTUPDOPRID>
            <LASTUPDDTTM IsChanged="Y">2012-07-24T04:33:07.000000-0700</LASTUPDDTTM>
            <SCC_AFL_PLCD_MTD_IsChanged="Y">M</SCC_AFL_PLCD_MTD>
            <SCC_AFL_RLCD_MTD />
            <SCC_AFL_STATUS IsChanged="Y">ACT</SCC_AFL_STATUS>
<SCC_AFL_STS_DESCR IsChanged="Y">Applied</SCC_AFL_STS_DESCR>
            <SCC_AFL_RANK IsChanged="Y">01000</SCC_AFL_RANK>
          </SCC_AFL_PERSON>
          <PSCAMA class="R">
Ŧ
        </SCC CM PERSON I>
        <PSCAMA class="R">
      </Transaction>
```

2. In the Oracle Identity Manager Design Console, open the PSFTStatusEvaluator adapter.

Adapter Fact	tory							
		Disable Adapter			🗩 Build			
Adapter Name	PSF	TStatusEvaluator	Compile S	itatus <mark>OK</mark>				
Adapter Type	Adapter Type Process Task			2012-09-07				
Description	PSF	T Status Evaluator						
Adapter Ta	sks	Execution Schedule	e Resourc	es Variable List	Usage Lookup Responses			
Add		Name	Type	Mapped As	Description 🔻			
	1	status	String	Resolve at runtime	Affiliation Status			
Delete	2	endDate	Date	Resolve at runtime	End Date			
	3	inEffPeriodFieldName	String	Resolve at runtime	Field name for "In Effective Period"			
4 processinstance L			Long	Resolve at runtime	Process Instance Key			
	5 startDate [		Date	Resolve at runtime	Start Date			
	6	statusEnabledVal	String	Literal	Status value that means affiliation status is active			



3. On the Variable List tab, double-click statusEnabledVal.

As shown in the following screenshot, ensure that the Literal Value field contains the same value as in the XML message, which is ACT.

-Adapter Fact	ory								
Adapter Name	_	Disable Adapter TStatusEvaluator	Compile S	itatus <mark>OK</mark>					
Adapter Type	Pro	cess Task	Last Edit	2012-09-07	Adapter Variable				
Description	PSF	F Status Evaluator			Final				
Adapter Ta	sks	Execution Schedul	e Resourc	es Variable Lis	Variable Name statusEnabledVal				
Add		Name	Туре	Mapped As	Type String 💌				
 Delete	1 2 3 4		String Date String Long	Resolve at runtime Resolve at runtime Resolve at runtime Resolve at runtime	Status value that means affiliation status is active				
	5	startDate statusEnabledVal	Date String	Resolve at runtime Literal	Map To Literal 💌				
					Qualifier String				
					Literal Value ACT				

If the status codes on the target system are changed, then you must update the code for the Active status in the Literal Value field of this adapter. Then, recompile the adapter.

# 3.4 Verifying the Entries in Attribute Mapping Lookup Definitions

#### Ensure that Decode entries of the

Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping lookup definition are based on the message structure shown in Message Structure.

If the message structure received from the target system is different from this message structure (if the node names in the XML files are different), then the Decode entries in the lookup definition need to be updated as per the modified message structure.

Similarly, if the message structure sent to PeopleSoft listener is different from the message structure shown in Message Structure, then change the Decode entries in the Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping lookup definition as per the modified message structure.

# 3.5 Performing Full Reconciliation

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

The following sections discuss the procedures involved in full reconciliation:

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



### 3.5.1 Generating XML Files

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

### Note:

Before performing the procedure to generate XML files, you must ensure that you have configured the SCC\_CONSTITUENT\_FULLSYNC messages. See Installation on the Target System for more information.

To generate XML files for full reconciliation, run the SCC\_CONSTITUENT\_FULLSYNC message as follows:

- 1. In PeopleSoft Internet Architecture, expand Enterprise Components, Integration Definitions, Initiate Processes, and then click Full Data Publish.
- 2. Click the Add a New Value tab.
- 3. In the Run Control ID field, enter a value and then click ADD.
- 4. In the Process Request region, provide the following values:

Request ID: Enter a request ID.

Description: Enter a description for the process request.

Process Frequency: Select Always.

Message Name: Select SCC\_CONSTITUENT\_FULLSYNC.

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

The Process Scheduler Request page appears.

- 7. From the Server Name list, select the appropriate server.
- 8. Select Full Table Data Publish process list, and click OK.
- 9. Click **Process Monitor** to verify the status of EOP\_PUBLISHT Application Engine. The **Run Status** is **Success** if the transaction is successfully completed.

On successful completion of the transaction, XML files for the SCC\_CONSTITUENT\_FULLSYNC message are generated at a location that you specified in the FilePath property while creating the OIM\_FILE\_NODE node for PeopleSoft Web Server. See Configuring the PeopleSoft Integration Broker section for more information.

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



#### Note:

After you have performed this procedure, remove the permission list created in Setting Up the Security for the SCC\_CONSTITUENT\_FULLSYNC Service Operation. This is for security purposes.

### 3.5.2 Importing XML Files into Oracle Identity Manager

This section contains the following topics:

- Configuring the Scheduled Task for Person Data Reconciliation
- Configuring the Scheduled Task for Processing Affiliation Effective Date

See Configuring Scheduled Jobs for instructions on running a scheduled task.

### 3.5.2.1 Configuring the Scheduled Task for Person Data Reconciliation

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

To perform a full reconciliation run, you must configure the scheduled task to reconcile all person data into Oracle Identity Manager depending on the values that you specified in the scheduled task attributes. Table 3-2 describes the attributes of this scheduled task.

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

Attribute	Description						
Archive Mode	Enter yes if you want XML files used during full reconciliation to be archived. After archival the file is deleted from the original location.						
	If no, the XML file is not archived.						
Archive Path	Enter the full path and name of the directory in which you want XML files used during full reconciliation to be archived.						
	You must enter a value for the Archive Path attribute only if you specify $yes$ as the value for the Archive Mode attribute.						
	Sample value: /usr/archive						
File Path	Enter the path of the directory on the Oracle Identity Manager host computer into which you copy the file containing XML data.						
	Sample value: /usr/data						
IT Resource Name	Enter the name of the IT resource that you create by performing the procedure described in Configuring the IT Resource.						
	Default value: PSFT Campus						

Table 3-2	Attributes of the PeopleSoft Campus Trusted Full Reconciliation Scheduled Task
-----------	--



Attribute	Description				
Message Name	Use this attribute to specify the name of the delivered message used for full reconciliation.				
	Sample value: SCC_CONSTITUENT_FULLSYNC				
	<b>Note:</b> This value must match the entry in the Lookup.PSFT.Campus.Configuration lookup definition, as it is used to determine the class name of the message handler.				
Task Name	This attribute holds the name of the scheduled task.				
	Value: PeopleSoft Campus Trusted Full Reconciliation				

Table 3-2 (Cont.) Attributes of the PeopleSoft Campus Trusted Full Reconciliation ScheduledTask

### 3.5.2.2 Configuring the Scheduled Task for Processing Affiliation Effective Date

When you run the Connector Installer, the PeopleSoft Campus Affiliation Effective Date Processor scheduled task is automatically created in Oracle Identity Manager.

This scheduled task searches for all the disabled affiliation resources and evaluates if the current date is between affiliation start date and end date. If it does and if the affiliation is active, then the task enables the resource. This triggers the affiliation-role assignment to the user. Table 3-3 describes the attributes of this scheduled task.

# Table 3-3Attributes of the PeopleSoft Campus Affiliation Effective Date Processor ScheduledTask

Attribute	Description						
End Date Field	Enter the affiliation end date.						
	Default value: UD_AFFLN_END_DATE						
Resource Object Name	Enter the name of the resource object.						
	Default value: Affiliation						
Start Date Field	Enter the affiliation start date.						
	Default value: UD_AFFLN_ST_DATE						
Status Field	Enter the status of the affiliation date.						
	Default value: UD_AFFLN_EFFDT_STATUS						
Task Name	This attribute holds the name of the scheduled task.						
	Value: PeopleSoft Campus Affiliation Effective Date Processor						

# 3.6 Performing Incremental Reconciliation

You do not require additional configuration for incremental reconciliation.

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

# 3.7 Limited Reconciliation

This section contains the following topics:



- About Limited Reconciliation
- Configuring Limited Reconciliation

## 3.7.1 About Limited Reconciliation

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

You configure segment filtering to specify the attributes whose values you want to fetch into Oracle Identity Manager. Similarly, you can configure limited reconciliation to specify the subset of target system records that must be fetched into Oracle Identity Manager.

You configure limited reconciliation by specifying a query condition as the value of the Custom Query attribute in the message-specific configuration lookup.

You must use the following format to specify a value for the Custom Query attribute:

 $RESOURCE\_OBJECT\_ATTRIBUTE\_NAME=VALUE$ 

For example, suppose you specify the following as the value of the Custom Query attribute:

Last Name=Doe

With this query condition, only records for persons whose last name is Doe are considered for reconciliation.

You can add multiple query conditions by using the ampersand (&) as the AND operator and the vertical bar (|) as the OR operator. For example, the following query condition is used to limit reconciliation to records of those persons whose first name is John and last name is Doe:

First Name=John & Last Name=Doe

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

First Name=John | User ID=219786

# 3.7.2 Configuring Limited Reconciliation

To configure limited reconciliation:

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

### See Also:

Lookup.PSFT.Campus.CustomQuery for a listing of the default contents of this lookup definition



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

- 2. Create the query condition. Apply the following guidelines when you create the query condition:
  - Use only the equal sign (=), the ampersand (&), and the vertical bar (|) in the query condition. Do not include any other special characters in the query condition. Any other character that is included is treated as part of the value that you specify.
  - Add a space before and after the ampersand and vertical bar used in the query condition. For example:

First Name=John & Last Name=Doe

This is to help the system distinguish between ampersands and vertical bars used in the query and the same characters included as part of attribute values specified in the query condition.

 You must not include unnecessary blank spaces between operators and values in the query condition.

A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

First Name=John & Last Name=Doe

First Name= John & Last Name= Doe

In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.

• Ensure that attribute names that you use in the query condition are in the same case (uppercase or lowercase) as the case of values in the Lookup.PSFT.Campus.CustomQuery lookup definitions. For example, the following query condition would fail:

fiRst Name = John

3. Configure the message-specific configuration lookup with the query condition as the value of the Custom Query attribute. For example, to specify the query condition for the SCC\_CONSTITUENT\_FULLSYNC message, search and open the Lookup.PSFT.Message.SccConstituentFullSync.Configuration lookup. Specify the query condition in the Decode column of the Custom Query attribute.

# 3.8 Resending Messages That Are Not Received by the PeopleSoft Listener

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



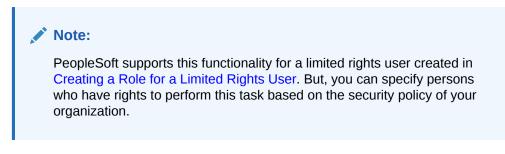
- Sending Messages Manually
- Resending Messages Manually in Error or TimeOut Status

### 3.8.1 Sending Messages Manually

If Oracle Identity Manager is not running when a message is published, then the message is added to a queue. You can check the status of the message in the queue in the **Message Instance** tab. This tab lists all the published messages in queue. When you check the details of a specific message, the status is listed as <code>Timeout</code> or <code>Error</code>.

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

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



### 3.8.2 Resending Messages Manually in Error or TimeOut Status

To manually resend messages in Error or TimeOut status:

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

PeopleTools	4						NewV	Vindow Custo	omize Page
D Security D Utilities D Workflow	/ Monitor Overview Ope	ration Instances $\gamma$	Publication Contra	acts 丫 Subscr	iption Contr	acts			_
<ul> <li>Portal</li> <li>Search Engine</li> <li>Personalization</li> </ul>	Publish Node		٩			Archiv	/ed		
D Process Scheduler	'Queue Level Oper Ins	t 💌 'Group By	Queue		*				
D Cube Manager D Application Engine	Time Period								
<ul> <li>D Query Access Services</li> <li>         Integration Broker         ▷ Configuration         ▷ Integration Setup     </li> </ul>	From Date: From Time:		Date: Time:	<u>(1</u>	Refres	sh			
D Service Utilities	Result			c	ustomize	Find   View.	AIL] 🗱	First 🖪 1 of 1	▶ Last
	Queue Name	Error New	Started Wo	king <u>Done</u>	Retry	Timeout	Edited	Canceled	Hold
Monitor v Monitoring	PERSON_DATA	1 1	0	0 1	0	0	0	0	0
– Asynchronous Services									
- Asynchronous									
Details - Synchronous									
Services									
<ul> <li>Synchronous Details</li> <li>Error Notification</li> </ul>	E Martin I								
Inchine Manifer Date	T Notify								



The number is in the form of a link, which when clicked displays the details of the message.

- 3. Click the link pertaining to the message to be resent, for example, the link under the Error or the TimeOut column.
- 4. Click the **Details** link of the message to be resent. A new window appears.
- 5. Click the **Error Messages** link to check the error description.
- 6. Click **Resubmit** after you have resolved the issue.

# 3.9 Configuring Scheduled Jobs

This section describes the procedure to configure scheduled jobs. It contains the following topics:

- Configurable Scheduled Tasks
- Configuring a Scheduled Task

### 3.9.1 Configurable Scheduled Tasks

The following scheduled tasks can be configured:

PeopleSoft Campus Role Creation

See Importing CSV File into Oracle Identity Manager to Create Roles for information about the attributes of this task.

PeopleSoft Campus Trusted Full Reconciliation

See Configuring the Scheduled Task for Person Data Reconciliation for information about the attributes of this task.

PeopleSoft Campus Affiliation Effective Date Processor

See Configuring the Scheduled Task for Processing Affiliation Effective Date for information about the attributes of this task.

### 3.9.2 Configuring a Scheduled Task

To configure a scheduled task:

- **1.** Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
  - For Oracle Identity Manager release 11.1.1:
    - a. Log in to the Administrative and User Console.
    - b. On the Welcome to Oracle Identity Manager Self Service page, click Advanced in the upper-right corner of the page.
  - For Oracle Identity Manager release 11.1.2.x:
    - a. Log in to Oracle Identity System Administration.
    - b. In the left pane, under System Management, click Scheduler.
- 2. Search for and open the scheduled job as follows:



- a. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
- **b.** In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
- c. In the search results table on the left pane, click the scheduled job in the Job Name column.
- 3. Modify the details of the scheduled task. To do so:
  - On the Job Details tab, you can modify the following parameters:

- **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

- **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

### Note:

See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule tasks.

In addition to modifying the job details, you can enable or disable a job.

- 4. Specify values for the attributes of the scheduled task. To do so:
  - On the Job Details tab, under the Parameters section, specify values for the attributes of the scheduled task.

### Note:

- Attribute values are predefined in the connector XML that is imported during the installation of the connector. Specify values only for the attributes to change.
- If you want to stop a scheduled task while it is running, the process is terminated only after the complete processing of the file that is being run. For instance, you want to reconcile data from five XML files. But, if you stop the scheduled task when it is reconciling data from the third file, then the reconciliation will stop only after processing the third file completely.
- 5. After specifying the attributes, click **Apply** to save the changes.

### Note:

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



# 4 Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

### Note:

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

- Adding New User Attributes for Reconciliation
- Adding New Affiliation Attributes for Reconciliation
- Adding Support for Primary Affiliations
- Modifying Field Lengths on the OIM User Form
- Configuring Validation of Data During Reconciliation
- Configuring Transformation of Data During Reconciliation
- Setting Up the Lookup.PSFT.Campus.CustomQuery Lookup Definition
- Configuring the Connector for Multiple Installations of the Target System

# 4.1 Adding New User Attributes for Reconciliation

You can modify the default field mappings between Oracle Identity Manager and the PeopleSoft Campus target system. For full reconciliation, see Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping lookup definition which holds the default attribute mappings. For incremental reconciliation, see Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping lookup definition which holds the default attribute mappings. If required, you can add user attributes to these predefined attribute mappings.

This section contains the following topics:

- Adding a New User Attribute for Reconciliation
- Creating a User-Defined Field

### 4.1.1 Adding a New User Attribute for Reconciliation

To add a new user attribute for reconciliation:



- **1.** In the Oracle Identity Manager Design Console, make the required changes as follows:
  - a. Create a new user-defined field. For the procedure to create a user-defined field, see "Creating a User-Defined Field".
  - b. Add a reconciliation field corresponding to the new attribute in the PeopleSoft Campus resource object. For example, you can add the National ID reconciliation field.
  - c. Modify the PeopleSoft Campus Person process definition to include the mapping between the newly added field and the corresponding reconciliation field. For the example described earlier, the mapping is as follows:

```
National ID = National ID
```

- d. On the Object Reconciliation tab, click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.
- 2. Add the new attribute in the message-specific attribute mapping lookup definition. For example, the Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping lookup definition for the SCC CONSTITUENT FULLSYNC message.

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

Code Key	Decode
AttributeName	NODE~PARENT NODE~NODE TYPE=Value~EFFECTIVE DATED NODE~PRIMARY

For example:

Code Key: National ID

Decode: NATIONAL\_ID~SCC\_PER\_NID\_I

In this example, National ID is the reconciliation field and its equivalent target system field is NATIONAL\_ID.

3. Add the new attribute in the Resource Object attribute reconciliation lookup definition. For example, the Lookup.PSFT.Campus.SccConstituentSync.Recon lookup for the SCC\_CONSTITUENT\_FULLSYNC message.

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

Code Key	Decode
RO Attribute	ATTRIBUTE FIELD~LOOKUP NAME

For example:

Code Key: National ID

Decode: National ID

In this example, RO Attribute refers to the resource object attribute name added in the preceding steps. The decode value is the code key value in the messagespecific attribute mapping lookup definition.

4. Add the new attribute in the Custom Query lookup definition. See Setting Up the Lookup.PSFT.Campus.CustomQuery Lookup Definition for more information.



### 4.1.2 Creating a User-Defined Field

(Optional) If you want to create a custom attribute on Oracle Identity Manager, then perform the following steps:

- 1. Log in to the Oracle Identity Management Administration Console.
- 2. Click Advanced.
- 3. On the Configuration tab, click User Configuration.
- 4. From the Actions menu, select User Attributes.
- 5. Click Create Attribute.
- 6. Enter details of the attribute (UDF) that you want to create. From the Category list, select **Custom Attributes**.
- 7. Set values for the attribute properties.
- 8. Review the data that you have entered, and then save the attribute.

If you are using Oracle Identity Manager release 11.1.2.x or later, see Configuring Custom Attributes in Oracle Fusion Middleware Administering Oracle Identity Manager.

# 4.2 Adding New Affiliation Attributes for Reconciliation

This section contains the following topics:

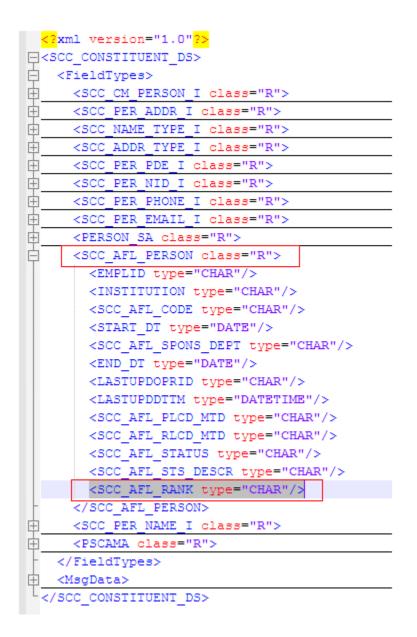
- About Affiliation Attributes
- Adding the New Field to the List of Reconciliation Fields
- Creating a New Version of the Process Form
- Adding a New Field on the Process Form
- Creating a Reconciliation Field Mapping for the New Field
- Creating an Entry for the Field in the Lookup Definition for Attribute Mapping
- · Creating an Entry for the Field in the Lookup Definition for Reconciliation
- Creating an Entry for the Field in the Configuration Lookup Definition
- Verifying the Affiliation Rank Attribute

### 4.2.1 About Affiliation Attributes

Standard reconciliation involves the reconciliation of predefined user and affiliation attributes. If required, you can add new affiliation attributes to the list of attributes that are reconciled.

The attribute that you want to reconcile should be part of the SCC\_CONSTITUENT\_SYNC or SCC\_CONSTITUENT\_FULLSYNC message. For example, consider the XML message shown in the following screenshot. For the Affiliation Rank attribute, the node name is SCC\_AFL\_RANK and the parent node name is SCC\_AFL\_PERSON. These two values will be added to the attribute mapping lookup definitions.





### 4.2.2 Adding the New Field to the List of Reconciliation Fields

To add the new field to the list of reconciliation fields in the resource object:

- 1. Log in to the Oracle Identity Manager Design Console.
- 2. Expand Resource Management.
- 3. Double-click Resource Objects.
- 4. Search for and open the PeopleSoft Campus resource object.
- 5. On the Object Reconciliation tab, click Add Field.
- 6. In the Add Reconciliation Field dialog box, enter the details of this field.

For example, enter Affiliation Rank in the Field Name field and select Number from the Field Type list.



7. Click the save icon.

Figure 4-1 is a sample screenshot of the newly added affiliation field.

Figure 4-1	Adding a New Affiliation Field for Reconciliation
------------	---

Resource Object Object Reconciliation
Object Initial Reconciliation Date
Reconciliation Fields Reconciliation Action Rules
Reconciliation Fields
Add Field       Reconciliation Fields for Object: Affiliation         Delete Field       Affiliation Rank [Number]         Image: Strain St

### 4.2.3 Creating a New Version of the Process Form

To create a new version of the process form:

- **1.** Expand **Development Tools**.
- 2. Double-click Form Designer.
- 3. Search for and open the UD\_AFFLN process form.
- 4. Click Create New Version.

On the Create a new version dialog box, enter a new version in the Label field, and then click the save icon.

### 4.2.4 Adding a New Field on the Process Form

To add the new field on the process form:

1. Click Add.

A field is added to the list. Enter the details of the field.

For example, if you are adding the Affiliation Rank field, enter UD\_AFFLN\_RANK in the **Name** field and then enter the rest of the details of this field.

- 2. Click Save.
- 3. To activate the newly created form, click Make Version Active.

Figure 4-2 is a sample screenshot of the new version of process form.



Form Desig	ner										
Table Infor	matio	on									
Table Name UD_AFFLN				Form Type							
Description PSFT Campus Affiliations				Process							
		Preview Form									
-Version In	form	ation									
Latest Vers	ion 🖪		Active Versio	1 1 2							
				1.2							
- Operatio	ns —					1					
Current Ve	ers	12		Curr	te New Version						
		1.2		Crea	te new version						
				Make	Version Active						
Additional	Colum	ins Child Table(s) Obje	ect Permission	is Pr	operties 🛛 Admir	nistrators	Usag	le Pre	-Po	opula	
Add		Name	Variant Ty	Len	Field Label	Field Type	D	Order			
	1	UD_AFFLN_EFFDT_STATUS	boolean	1	In Effective Period	CheckBox	1	9			
<u>D</u> elete	2	UD_AFFLN_ST_DATE	Date		Affiliation Start Da	DateFieldDlg		4			
	3	UD_AFFLN_CODE	String	50	Affiliation Code	TextField		1			
	4	UD_AFFLN_USER_ID	String	50	User ID	TextField		6			
	5	UD_AFFLN_END_DATE	Date		Affiliation End Dat	DateFieldDIg		5			
	б	UD_AFFLN_STATUS	String	30	Affiliation Status	TextField		2			
	7	UD_AFFLN_SERVER	long		Server	ITResourceLo		7			
	8	UD_AFFLN_INST	String	50	Institution	TextField		10			
	9	UD_AFFLN_DESC	String	100	Affiliation Descrip	TextField		3			
	10	UD_AFFLN_RANK	long		Affiliation Rank	TextField		11			

Figure 4-2 Adding a New Version of Process Form

### 4.2.5 Creating a Reconciliation Field Mapping for the New Field

To create a reconciliation field mapping for the new field on the process form:

- 1. Expand Process Management.
- 2. Double-click Process Definition.
- 3. From the Process Definition table, select and open the Affiliation resource object.
- 4. Click Reconciliation Field Mappings and then click Add Field Map.
- In the Field Name field, select the value for the field that you want to add.
   For example, select Affiliation Rank.
- 6. In the Field Type field, select the type of the field that is prepopulated.
- 7. Double-click the Process Data Field field.

A list of process data columns is displayed. From the list, select the process data column corresponding to the process data field.

For example, select Affiliation Rank [Number] = UD\_AFFLN\_RANK.

8. Click the save icon.

Figure 4-3 is a sample screenshot of the affiliation field mappings.



Process Definition				
Name Affiliatio	on Process	Map Descriptive Field	<u>R</u> ender Workflow	
Type Provisio	ning	🖌 Default Process 🛛 🗌 A	Auto Pre-populate	
Object Name Affiliatio	on	Auto Save Form		
Form Assignment—				
Table Name UD_AFF	LN			
Tasks Reconciliati	on Field Mappings Ad	ministrators		
Reconciliation Field Mappings				
Add Field Map	dd Field Map 🛛 📳 Reconciliation Field Mappings for process: Affiliation Process			
Add Table Map	Affiliation Rank [Number] = UD_AFFLN_RANK			
	User ID [String] = UD_AFFLN_USER_ID, <key></key>			
<u>D</u> elete Map	Affiliation Code [String] = UD_AFFLN_CODE, <key></key>			
	— Institution [String] = UD_AFFLN_INST, <key></key>			
	— ITResource Name [IT Resource] = UD_AFFLN_SERVER, <key></key>			
	Affiliation Status [String] = UD_AFFLN_STATUS			
	Affiliation Description [String] = UD_AFFLN_DESC			
	- Affiliation Start Date [Date] = UD_AFFLN_ST_DATE			
	Affiliation End Date [Date] = UD_AFFLN_END_DATE			

Figure 4-3 Adding a Affiliation Field Mapping

# 4.2.6 Creating an Entry for the Field in the Lookup Definition for Attribute Mapping

Create an entry for the field in the lookup definition for attribute mapping as follows:

- **1.** Expand **Administration**.
- 2. Double-click Lookup Definition.
- Search for and open the Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping lookup definition.

For full reconciliation, you must also add this entry in the **Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping** lookup definition.

4. Click Add and enter the Code Key and Decode values for the field.

The Code Key value must be the form field name. The Decode value must be the attribute node name and the parent name of the field in the XML message shown at the beginning of this section. For the format of the Decode value, see Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping.

For example, enter Affiliation Rank in the Code Key field and then enter SCC\_AFL\_RANK~SCC\_AFL\_PERSON~NONE~NONE~RESOURCE=Affiliations in the Decode field.

5. Click the save icon.

Figure 4-4 is a sample screenshot of the new entry added to the attribute mapping lookup definition.



ookup De	finiti	on		
Cod	fe	2SFT.Campus.SccConstituentSync.AttributeMapping		
Field	4			
There	•			
(	🖲 Lo	okup Type 🛛 🔾 Field Type		
		_		
Requir	ed			
Grou	Jp	PSFT Campus		
antina Car	an a mara			
ookup Coo	ae inf	ormation		
Add		Code Key	Decode 🐺	
	1	CAMPUS_ID~PERSON_SA		
Delete	2	Start Date EFFDT~SCC_PER_NAME_I~None~EFFDT		
	3	Email	EMAIL_ADDR~SCC_PER_EMAIL_I	
	4	User ID	EMPLID~SCC_CM_PERSON_I~None~None~PRIMARY	
	5	Affiliation End Date	END_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations	
	б	First Name	FIRST_NAME~SCC_PER_NAME_I~NAME_TYPE=PRI~EFFDT	
	7	Institution	INSTITUTION~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations	
	8	Last Name	LAST_NAME~SCC_PER_NAME_I~NAME_TYPE=PRI~EFFDT	
	9	Home Phone	PHONE~SCC_PER_PHONE_I	
	10	Affiliation Code	SCC_AFL_CODE~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations	
	11	Affiliation Rank	SCC_AFL_RANK~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations	
	12	Affiliation Status	SCC_AFL_STATUS~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations	
	13	Affiliation Description	scription SCC_AFL_STS_DESCR~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations	
	14	Affiliation Start Date START_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations		

Figure 4-4 Adding an Entry to Attribute Mapping Lookup

# 4.2.7 Creating an Entry for the Field in the Lookup Definition for Reconciliation

Create an entry for the field in the lookup definition for reconciliation as follows:

- 1. Expand Administration.
- 2. Double-click Lookup Definition.
- 3. Search for and open the Lookup.PSFT.Campus.SccConstituentSync.Recon lookup definition.
- 4. Click Add and enter the Code Key and Decode values for the field.

The Code Key value must be the form field name. For the format of the Decode value, see Lookup.PSFT.Campus.SccConstituentSync.Recon.

For example, enter Affiliation Rank in the Code Key field and then enter Affiliation Rank~NONE~Resource in the Decode field.

5. Click the save icon.

Figure 4-5 is a sample screenshot of the new entry added to the reconciliation lookup definition.

Lookup Definition				
Lookup De				
Cod	de Lookup.PSFT.Campus.SccConstituentSync.Recon			
	-	cookaptron r. campus. seccons	and encounter of the second	
Field				
(	Lo	okup Type i 🔾 Field Type		
Requir	ed			
Grou	tb	PSFT Campus		
Lookup Cod	to lef	ormation		
LUOKup COU	ie ini	ormation		
Add		Code Key	Decode 🔻	
	1	Affiliation Code	Affiliation Code~None~Resource	
<u>D</u> elete	2	Affiliation Description	Affiliation Description~None~None~Resource	
	3	Affiliation End Date Affiliation End Date~None~Resource		
	4	Affiliation Rank	Affiliation Rank~None~None~Resource	
	5	Affiliations	Affiliations	
	б	Affiliation Start Date	Affiliation Start Date~None~Resource	
	7	Affiliation Status	Affiliation Status~None~Resource	
	8	Campus ID	Campus ID	
	9	Email	Email	
	10	First Name	First Name	
	11	Home Phone	Home Phone	
	12	Institution	Institution~None~Resource	
	13	13 Last Name Last Name		
	14	National ID	National ID	
	15	Effective Start Date	Start Date	
	16	User ID	User ID	
	17	User Type	User Type	

Figure 4-5 Adding an Entry to Reconciliation Lookup

# 4.2.8 Creating an Entry for the Field in the Configuration Lookup Definition

Create an entry for the field in the configuration lookup definition as follows:

- **1.** Expand **Administration**.
- 2. Double-click Lookup Definition.
- 3. Search for and open the Lookup.PSFT.Message.SccConstituentSync.Configuration lookup definition.

For full reconciliation, you must also add this entry in the **Lookup.PSFT.Message.SccConstituentFullSync.Configuration** lookup definition.

4. For the Code Key with value Affiliations, append the new affiliation field name, Affiliation Rank, in the Decode field.

For example, enter Affiliation Code~Affiliation Status~Affiliation Description~Affiliation Start Date~Affiliation End Date~Institution~Affiliation Rank in the **Decode** field.

5. Click the save icon.

Figure 4-6 is a sample screenshot of the new entry added to the configuration lookup definition.



Lookup Def	initi	on			
Code	de Jp. PSFT. Message. SccConstituentSync. Configuration				
Field					
Field	I.				
	) Los	okup Type 🛛 Field Type			
	LOC	skup type Upretu type			
Require	d				
Grou	n li	PSFT Campus			
0100	r [	rari campus			
Lookup Cod	e Infi	ormation			
		Code Key	Decode 🔻		
<u>A</u> dd	1		Affiliation		
Delete		Affiliation Resource Object	Affiliation Affiliation Code~Affiliation Status~Affiliation Description~Affiliation Start Date~Affiliation End Date~Institution ~Affiliation Rank		
	-		Affiliation Code-Affiliation Status-Affiliation Description-Affiliation start Date-Affiliation End Date-Institution Affiliation Kank		
		Employee Status	Enabled		
		User Type	End-User		
			Enter a Value		
	7	Custom Query Lookup Definiti	Lookup.PSFT.Campus.CustomQuery		
	8	Attribute Mapping Lookup	Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping		
	9	Recon Lookup Definition	Lookup.PSFT.Campus.SccConstituentSync.Recon		
	10	Transformation Lookup Defini	Lookup.PSFT.Campus.SccConstituentSync.Transformation		
		Validation Lookup Definition	Lookup.PSFT.Campus.SccConstituentSync.Validation		
		Use Validation	No		
		Use Transformation	No		
		Message Handler Class	oracle.iam.connectors.psft.common.handler.impl.PSFTCampusSyncReconMessageHandlerImpl		
		Message Parser	oracle.iam.connectors.psft.common.parser.impl.CampusMessageParser		
		Resource Object	Peoplesoft Campus		
		Data Node Name Organization	ransaction (ellerate Users		
	18	organization			

Figure 4-6 Adding an Entry to Configuration Lookup

#### 4.2.9 Verifying the Affiliation Rank Attribute

- 1. On the Resource Objects form, for the Affiliation resource object, click Create Reconciliation Profile.
- 2. Perform reconciliation to verify the Affiliation Rank attribute.

You should be able to see Affiliation Rank in the connector logs. Ensure that they appear in the reconciliation events.

## 4.3 Adding Support for Primary Affiliations

Affiliations in PeopleSoft Campus are defined as the relationship between an individual and an institution. However, there is no concept of Primary Affiliations in PeopleSoft Campus. There is no cross-institution or cross-campus attribute that would inherently define a "primary" affiliation for an individual who is affiliated with multiple institutions in a multi-institution PeopleSoft Campus Solutions deployment.

In some cases, Affiliations are deployed in a manner that would benefit from an ability to identify a primary affiliation. Ranks for affiliations can be used to reflect hierarchy amongst the different affiliations.

For example, consider an institution called BIG University with BIGUNV as the Institution Code. The following table shows a sample list of Affiliation Codes and their ranks:

Affiliation Code	Affiliation Description	Ranking
EMPFULL	Employee Full Time	9999
STDNTFULL	Student Full Time	8888
STDNTPART	Student Part Time	7777

Roles are created in Oracle Identity Manager that correspond to each unique PeopleSoft Campus Affiliations. The Ranks of the affiliations are stored in the role descriptions in Oracle Identity Manager.



Oracle Identity Manager users would have an active role for each active affiliation. For implementing primary affiliations, the connector can be extended to add a task that reads the role names (the affiliation and the institution codes) and the role descriptions (the affiliation ranks). Then, the affiliation with the highest rank can be picked as the primary affiliation.

For the previous example, the following table indicates sample role names and descriptions in Oracle Identity Manager:

Role Name	Role Description
PSFTCampus~BIGUNV~EMPFULL	Affiliation rank :9999
PSFTCampus~BIGUNV~STDNTFULL	Affiliation rank :8888
PSFTCampus~BIGUNV~STDNTPART	Affiliation rank :7777

The following screenshot shows another example of roles and ranks for supporting primary affiliations:

🔓 first28a last28a				
	ources Proxies Direct F	Requests		
Display Name	Role Name	Description		
ALL USERS	ALL USERS	Default role for all users		
PSFTCampus~PSUNV~ALUMN_TMPL	PSFTCampus~PSUNV~ALUMN_TMPL	Affiliation rank :"01000"		
PSFTCampus~PSUNV~EMPLOYEE	PSFTCampus~PSUNV~EMPLOYEE	Affiliation rank :"04000"		
PSFTCampus~PSUNV~STUDENT	PSFTCampus~PSUNV~STUDENT	Affiliation rank : "03000"		

#### 4.4 Modifying Field Lengths on the OIM User Form

You might want to modify the lengths of the fields (attributes) on the OIM User form. For example, if you use the Japanese locale, then you might want to increase the lengths of OIM User form fields to accommodate multibyte data from the target system.

If you want to modify the length of a field on the OIM User form, then:

- **1.** Log in to the Design Console.
- 2. Expand Administration, and double-click User Defined Field Definition.
- 3. Search for and open the Users form.
- 4. Modify the length of the required field.
- 5. Click the Save icon.

## 4.5 Configuring Validation of Data During Reconciliation

You can configure validation of reconciled single-valued data according to your requirements. For example, you can validate data fetched from the First Name



attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the user form so that the number sign (#) is not sent to Oracle Identity Manager during reconciliation operations.

For data that fails the validation check, the following message is displayed or recorded in the log file:

Value returned for field FIELD\_NAME is false.

To configure validation of data, perform the following steps:

- Implementing the Validation Logic in a Java Class
- Uploading the JAR File to Oracle Identity Manager
- Updating the Message-Specific Configuration Lookup Definition
- Redeploying the PeopleSoftOIMListener.ear File on the Application Server

#### 4.5.1 Implementing the Validation Logic in a Java Class

To implement the validation logic in a Java class:

1. Write the code that implements the required validation logic in a Java class.

See Also:

The Javadocs shipped with the connector for more information about this interface

You must create a class with the following signature:

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

In this signature code:

- arg0 contains User form field values
- arg1 contains Affiliation resource field values
- arg2 is the field on which validation needs to be done

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

```
* the code must return true or false.
             * In this sample code, the value "false" is returned if the field
             * contains the number sign (#). Otherwise, the value "true" is
             * returned.
             * /
           log = Logger.getLogger("PSFT.VALIDATION");
           boolean valid = true;
            String sFirstName = (String) hmUserDetails.get(field);
            if(sFirstName != null){
                for(int i=0;i<sFirstName.length();i++){</pre>
                    if (sFirstName.charAt(i) == '#'){
                        log.warning("Validation failed for " + field);
                        return false;
                }
            }
            //If validation of affiliation data is not required, comment the
   next line.
           valid = validateAffiliationData(hmAffiliationDetails, field);
            return valid;
        }
        private boolean validateAffiliationData(HashMap hmAffiliationDetails,
                String field) {
           log.fine("Checking for affiliation data");
           boolean valid = true;
           ArrayList<HashMap> affList =
                (ArrayList<HashMap>) hmAffiliationDetails.get("Affiliations");
            if(affList !=null && affList.size() > 0){
                HashMap affMap = affList.get(0);
                String fieldVal = (String)affMap.get(field);
                log.fine("Field value is " + fieldVal);
                //TODO Validation can now be applied on fieldVal.
                //Set 'valid' to true or false depending on validation outcome.
            }
           return valid;
        }
   Create a JAR file to hold the Java class.
2.
```

#### 4.5.2 Uploading the JAR File to Oracle Identity Manager

Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Implementing the Validation Logic in a Java Class to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

#### Note:

Before you use this utility, verify that the WL\_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.



For Microsoft Windows:

OIM\_HOME/server/bin/UploadJars.bat

For UNIX:

OIM\_HOME/server/bin/UploadJars.sh

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

#### 4.5.3 Updating the Message-Specific Configuration Lookup Definition

If you created the Java class for validating a process form field for reconciliation, then:

- 1. Log in to the Design Console.
- 2. Search for and open the message-specific configuration lookup definition.

For example, locate the

Lookup.PSFT.Message.SccConstituentSync.Configuration lookup definition for the SCC\_CONSTITUENT\_SYNC message. See Lookup.PSFT.Message.SccConstituentSync.Configuration for information about this lookup definition. Check for the parameter Validation Lookup Definition in this lookup definition. The Decode value specifies the name of the validation lookup. In this example, the Decode value is Lookup.PSFT.Campus.SccConstituentSync.Validation.

- 3. Search for and open the Lookup.PSFT.Campus.SccConstituentSync.Validation lookup definition.
- 4. In the Code Key column, enter First Name. In the Decode column, enter com.validate.MyValidation.

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

- 5. Save the changes to the lookup definition.
- 6. Search for and open the message-specific configuration lookup definition, in this example, the Lookup.PSFT.Message.SccConstituentSync.Configuration lookup definition.
- 7. Set the value of the Use Validation entry to yes.
- 8. Save the changes to the lookup definition.

# 4.5.4 Redeploying the PeopleSoftOIMListener.ear File on the Application Server

To redeploy the PeopleSoftOIMListener.ear file on the application server:

- 1. Remove the PeopleSoftOIMListener.ear file from the application server.
- 2. Copy the validation JAR file created in Step 2 to the following directory:

CONN\_HOME/listener/deployable-archive/PeoplSoftOIMListener.ear/ PeoplSoftOIMListener.war/WEB-INF/lib



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

ant redeploy

See Deploying the PeopleSoft Listener for information about the deployment tool.

# 4.6 Configuring Transformation of Data During Reconciliation

You can configure the transformation of reconciled single-valued data according to your requirements. For example, you can use the First Name value to prefix 'Mr.' to the First Name field in Oracle Identity Manager.

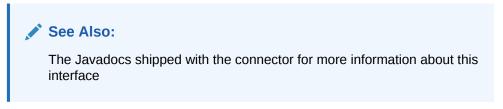
To configure the transformation of data, perform the following steps:

- Implementing the Transformation Logic in a Java Class
- Uploading the JAR File to Oracle Identity Manager
- Updating the Message-Specific Configuration Lookup Definition
- Redeploying the PeopleSoftOIMListener.ear File on the Application Server

#### 4.6.1 Implementing the Transformation Logic in a Java Class

To implement the transformation logic in a Java class:

1. Write code that implements the required transformation logic in a Java class.



The following sample transformation class modifies a value for the First Name attribute by prefixing a 'Mr.' in the First Name value received from the target system. It also shows how the affiliation data can be transformed by prefixing 'Description:' to the Affiliation Description field received from the target system.

```
package com.transform;
import java.util.ArrayList;
public class MyTransform {
   Logger log;
   /**Abstract method for transforming the attributes
   * @param hmUserDetails HashMap<String,Object> containing parent data
details
   * @param hmAffiliationDetails ArrayList of HashMap<String,Object>
containing affiliation details
   * @param sField Field name to transform
   * @return
   */
```



```
public Object transform(HashMap hmUserDetails, HashMap
            hmAffiliationDetails,String sField) {
        /*
        You must write code to transform the attributes.
        User attribute values can be fetched by
        using hmUserDetails.get("Field Name").
        Return the transformed attribute.
        To fetch affiliation resource data values, loop through the
        ArrayList fetched by hmAffiliationDetails("<aff. Resource name>")
        User data would be passed as null when passing affiliation resource
data.
        Return the transformed hashmap.
        */
        log = Logger.getLogger("PSFT.TRANSFORMATION");
        if(hmUserDetails == null){
            //User data is null when affiliation data is passed.
            /*If transformation of affiliations is not required,
            * these can be commented/removed.
            */
            log.fine("Transforming affiliation data");
            return transformAffiliations(hmAffiliationDetails,sField);
        }
        //Only User data is passed
        log.fine("Transforming User data");
        log.fine("Field to transform = " + sField);
        String sName= (String)hmUserDetails.get(sField);
        if(sName == null){
            return null;
        //Sample transformation for first name: Prefix 'Mr.'
        sName = "Mr. "+sName;
        return sName;
    }
    private Object transformAffiliations(HashMap hmEntitlementDetails,
String sField) {
        ArrayList<HashMap> affList = (ArrayList<HashMap>)
hmEntitlementDetails.get("Affiliations");
        ArrayList<HashMap> transformedList = new ArrayList<HashMap>();
        if(affList == null || affList.size() < 1){</pre>
            log.warning("Affiliation list is empty. Returning original map");
            return hmEntitlementDetails;
        }
        for (HashMap hashMap : affList) {
            String sName= (String)hashMap.get(sField);
            if(sName == null){
                transformedList.add(hashMap);
                continue;
            //Sample transformation.
            //Affiliation description field is passed
            //It is prefixed with 'Description:'
```

```
sName = "Description: " + sName;
hashMap.put(sField, sName);
transformedList.add(hashMap);
}
return new HashMap().put("Affiliations",transformedList);
}
}
```

2. Create a JAR file to hold the Java class.

#### 4.6.2 Uploading the JAR File to Oracle Identity Manager

Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Implementing the Transformation Logic in a Java Class to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:



Before you use this utility, verify that the WL\_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

For Microsoft Windows:

OIM\_HOME/server/bin/UploadJars.bat

For UNIX:

OIM\_HOME/server/bin/UploadJars.sh

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

#### 4.6.3 Updating the Message-Specific Configuration Lookup Definition

If you created the Java class for validating a process form field for reconciliation, then:

- **1.** Log in to the Design Console.
- Search for and open the message-specific configuration lookup definition, in this example, the Lookup.PSFT.Message.SccConstituentSync.Configuration lookup definition for the SCC\_CONSTITUENT\_SYNC message.

See Lookup.PSFT.Message.SccConstituentSync.Configuration for information about this lookup definition. Check for the parameter Transformation Lookup Definition in this lookup definition. The Decode value specifies the name of the transformation lookup. In this example, the Decode value is Lookup.PSFT.Campus.SccConstituentSync.Transformation.

- 3. Search for and open the Lookup.PSFT.Campus.SccConstituentSync.Transformation lookup definition.
- 4. In the Code Key column, enter First Name. In the Decode column, enter com.transform.MyTransform.



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

- 5. Save the changes to the lookup definition.
- Search for and open the message-specific configuration lookup definition, in this example, the Lookup.PSFT.Message.SccConstituentSync.Configuration lookup definition.
- 7. Set the value of the Use Transformation entry to yes.
- 8. Save the changes to the lookup definition.

# 4.6.4 Redeploying the PeopleSoftOIMListener.ear File on the Application Server

To redeploy the PeopleSoftOIMListener.ear file on the application server:

- 1. Remove the PeopleSoftOIMListener.ear file from the application server.
- Copy the transformation JAR file created in Step 2 to the following directory: *CONN HOME*/listener/deployable-archive/PeoplSoftOIMListener.ear/

PeoplSoftOIMListener.war/WEB-INF/lib

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

ant redeploy

See Deploying the PeopleSoft Listener for information about the deployment tool.

# 4.7 Setting Up the Lookup.PSFT.Campus.CustomQuery Lookup Definition

You configure limited reconciliation by specifying a query condition as the value of the Custom Query attribute in the message-specific configuration lookup. See Lookup.PSFT.Campus.CustomQuery for more information about this lookup definition.

You must ensure that the OIM User attribute to use in the query exists in the Lookup.PSFT.Campus.CustomQuery lookup definition. You must add a row in this lookup definition whenever you add a UDF in the user form.

To add a new UDF to this lookup definition:

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



Note:

The Code Key value represents the resource object field name and the Decode value specifies the column name of the USR table.

4. In the Code Key and Decode columns, enter the values for the UDF.

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

Code Key	Decode
RO Attribute Name	Column name of the USR table

If you have added a UDF Empl ID with column name as USR\_UDF\_EMPLOYEE\_ID, then define the following entry in this lookup definition:

Code Key: Empl ID

Decode: USR\_UDF\_EMPLOYEE\_ID

5. Click the Save icon.

# 4.8 Configuring the Connector for Multiple Installations of the Target System

This section contains the following topics:

- About Configuring the Connector for Multiple Installations of the Target System
- Creating Copies of the Connector Objects

# 4.8.1 About Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

The London and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you can create copies of connector objects, such as the IT resource and resource object.

The decision to create a copy of a connector object is based on a requirement. For example, an IT resource can hold connection information for one target system installation. Therefore, it is mandatory to create a copy of the IT resource for each target system installation.

With some other connector objects, you do not need to create copies at all. For example, a single attribute-mapping lookup definition can be used for all installations of the target system.



#### Note:

A single listener is sufficient for multiple installations of the target system. You can configure the nodes to point to the same listener with different IT resource names.

All connector objects are linked. For example, a scheduled task holds the name of the IT resource. Similarly, the IT resource holds the name of the common configuration lookup definition, which is Lookup.PSFT.Campus.Configuration. If you create a copy of an object, then you must specify the name of the copy in other connector object. Table 4-1 lists association between connector objects whose copies can be created and the other objects that reference these objects. When you create a copy of an object, use this information to change the associations of that object with other objects.

Connector Object	Name	Referenced By	Description
IT Resource	PSFT Campus	<ul> <li>Scheduled Task: PeopleSoft Campus Trusted Reconciliation</li> <li>Resource Object: PeopleSoft Campus</li> </ul>	You need to create a copy of IT Resource with a different name.
Resource Object	PeopleSoft Campus	Message-specific configuration lookup definitions: Lookup.PSFT.M essage.SccCons tituentSync.Conf iguration Lookup. PSFT.Message. SccConstituentF ullSync.Configur ation	It is optional to create a copy of a resource object. If you are reconciling the same set of attributes from the other target system, then you need not create a new resource object. <b>Note:</b> Create copies of this resource object only if there are differences in attributes between the two installations of the target system.
Common Configuration Lookup Definition	Lookup.PSFT.Ca mpus.Configurati on	Message-specific configuration lookup definitions: Lookup.PSFT.M essage.SccCons tituentSync.Conf iguration Lookup. PSFT.Message. SccConstituentF ullSync.Configur ation	It is optional to create a copy of the common configuration lookup definition. <b>Note:</b> Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.

#### Table 4-1 Connector Objects and Their Associations



Connector Object	Name	Referenced By	Description
Message-specific Configuration Lookup Definition	Lookup definitions: Lookup.PSF T.Message.S ccConstituen tSync.Config uration Lookup. PSFT.Messa ge.SccConsti tuentFullSyn c.Configurati on	<ul> <li>Attribute mapping lookup definitions:</li> <li>Lookup.PSFT.C ampus.SccCons tituentSync.Attri buteMapping</li> <li>Lookup.PSFT.C ampus.SccCons tituentFullSync.A ttributeMapping</li> </ul>	It is optional to create a copy of the message-specific lookup definitions. <b>Note:</b> Create copies of this lookup definition only if there ar differences in attributes betwee the two installations of the target system.
Attribute Mapping Lookup Definition	Lookup definitions: Lookup.PSF T.Campus.S ccConstituen tSync.Attribu teMapping Lookup.PSF T.Campus.S ccConstituen tFullSync.Att ributeMappin g	NA	This lookup definition holds the information of the attributes reconciled from the XML message file from the target system. <b>Note:</b> Create copies of this lookup definition only if there ar differences in attributes betwee the two installations of the target system.
Recon Map Lookup Definition	Lookup.PSFT.Ca mpus.SccConstit uentSync.Recon	NA	This lookup definition maps the resource object field with the data reconciled from the message. <b>Note:</b> Create copies of this lookup definition only if there ar differences in attributes betwee the two installations of the target system.

#### 4.8.2 Creating Copies of the Connector Objects

To create copies of the connector objects:

#### Note:

See Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the steps in this procedure.

- 1. Create a copy of the IT resource. See Configuring the IT Resource for information about this IT resource.
- 2. Create a copy of the PeopleSoft Campus resource object.



- 3. Create copy of the SCC\_CONSTITUENT\_FULLSYNC and SCC\_CONSTITUENT\_SYNC message-specific configuration lookup.
- 4. Create a copy of the Lookup.PSFT.Campus.Configuration lookup definition. Add the new lookup to the Configuration Lookup parameter of the new IT resource created in Step 1. See Lookup.PSFT.Campus.Configuration for information about this lookup definition.
- Create a copy of the message-specific attribute mapping and reconciliation lookup definition, for example, the Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping and the Lookup.PSFT.Campus.SccConstituentSync.Recon for SCC\_CONSTITUENT\_SYNC message. Similarly, the Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping for SCC\_CONSTITUENT\_FULLSYNC message.
- 6. Create a copy of the PeopleSoft Campus Trusted Reconciliation scheduled task. See Configuring the Scheduled Task for Person Data Reconciliation for information about this scheduled task.

To reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the ITResource scheduled task attribute.



## 5 Testing and Troubleshooting

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

#### Note:

Using the testing utility, you can test connectivity and perform sanity tests on basic connector operations. The testing utility does not support functions such as validation, transformation, resource exclusion, multiple-version support, and remote connector server.

## 5.1 Testing Reconciliation

The testing utility enables you to test the functionality of the connector. The testing utility takes as input the XML file or message generated by the target system. It can be used for testing full and incremental reconciliation.

The testing utility is located in the test directory on the installation media. See Files and Directories on the Installation Media for more information.

To run the testing utility for reconciliation:

1. Open and edit the test/config/reconConfig.properties file as follows:

i) Enter the PeopleSoftOIMListener servlet URL as the value of ListenerURL in following syntax:

http://HOSTNAME:PORT/PeopleSoftOIMListener

For example:

ListenerURL=http://10.1.6.83:8080/PeopleSoftOIMListener

ii) Enter the absolute XML message file path as the value of XMLFilePath as shown in the following example:

XMLFilePath=c:/xmlmessages/scc\_constituent\_sync.xml

#### Note:

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

iii) Enter a value for the MessageType. For a ping message, specify Ping, None, or otherwise as shown in the following example:



MessageType=None

iv) Enter a value for **ITResourceName.** This value must match the active IT resource in Oracle Identity Manager.

For example:

ITResourceName=PSFT Campus

v) Enter the name of the message for which you run the testing utility.

For example:

MessageName=SCC\_CONSTITUENT\_SYNC

2. Open a command window, and navigate to the scripts directory.

You must run the testing utility from the OIM\_HOME/ server/ConnectorDefaultDirectory/CONN\_HOME/test/scripts directory, where CONN\_HOME is the connector directory.

For example:

OIM\_HOME/server/ConnectorDefaultDirectory/PSFT\_CS-11.1.1.5.0/test/scripts

3. Run the following script:

For Microsoft Windows:

InvokeListener.bat

For UNIX:

InvokeListener.sh

Verify that a reconciliation event is created in Oracle Identity Manager and that the event contains the data specified in the message-specific XML file.

#### 5.2 Troubleshooting

The following table lists solutions to some commonly encountered issues associated with this connector:

Problem Description	Solution	
When you try to run an operation, you get an error similar to the following errors: oracle.iam.connectors.psft.commo n.parser.impl.CampusMessageParse r: processMessage: No data found in XML	Ensure that Decode entries of the Lookup.PSFT.Campus.SccConstituentFullSync.Attri buteMapping lookup definition are based on the message structure shown in Message Structure. If the message structure changes (if the node names in the XML file are different), then the Decode entries in the lookup definition need to be	
MissingRequiredAttributeExceptio	updated as per the modified message structure.	
n: [Last Name]	<b>Note:</b> If this problem is encountered during incremental reconciliation, then change the Decode entries in the Lookup.PSFT.Campus.SccConstituentSync.Attribut eMapping lookup definition.	
When you try to run a reconciliation operation, sometimes two CREATE user events will be created for a single entity.	Ensure that the reconciliation batchSize parameter is set to 0 in the reconciliation profile of the Resource Object.	



# A Determining the Root Audit Action Details

An XML message that is published by PeopleSoft contains a Transaction node. In case of full reconciliation, the XML files for SCC\_CONSTITUENT\_FULLSYNC messages have multiple transaction nodes. However, in case of incremental reconciliation, the XML messages SCC\_CONSTITUENT\_SYNC have only one transaction node.

This appendix contains the following topics:

- The PSCAMA Subnode
- Root Audit Action

#### A.1 The PSCAMA Subnode

Every transaction node has a PeopleSoft Common Application Messaging Attributes (PSCAMA) subnode.

The following screenshot shows the PSCAMA node:



🗅 😅 🖬 🐇 🖻 💼 🗠 🖂 🛤 😫 🗠 🛶	, 1		<b>4</b> . <b>4</b> .	<b>G</b> xml	->SCC_CONSTITUENT_FU	LLSYNC->MsgData-	>Transaction(1)->PSCAMA
G SCC_CONSTITUENT_FULLSYNC		442	<scc< td=""><td>_AFL_PER</td><td>SON class="R"&gt;</td><td></td><td></td></scc<>	_AFL_PER	SON class="R">		
± ↔ FieldTypes		443	<emi< td=""><td>PLID IsCha</td><td>inged="Y"&gt;ADCRM100</td><td>1</td><td></td></emi<>	PLID IsCha	inged="Y">ADCRM100	1	
		444			sChanged="Y">PSUN\		
ide → Transaction		445			DE IsChanged="Y">STI		L_CODE>
two SCC_CM_PERSON_I		446			Changed="Y">2002-08-	27	
		447			ONS_DEPT/>		
Lass = "R"		448		)_DT/>			200
		449			ID IsChanged="Y">SAI		
		450 451					.000000-0700
BASE_LANGUAGE_CD		451		C_AFL_PLC	CD_MTD IsChanged="\ CD_MTD/>	-WIS/SUC_AFL_P	CCD_MID>
		452			ATUS IsChanged="Y">/		
MSG_SEQ_FLG		454			S_DESCR IsChanged="		
		455			NK IsChanged="Y">300		
		456		_AFL_PER		ALC_ALC_NAM	N*
		457		AMA class			
+ (*) Transaction		458			sChanged="Y">A <td>DIT ACTN&gt;</td> <td></td>	DIT ACTN>	
Transaction		459	<td></td> <td>bonangoa i rintor</td> <td></td> <td></td>		bonangoa i rintor		
		460		CM PERS	ON I>		
⊕-≪> Transaction		461		MA class=			
🕂 🖘 Transaction		462			>ENG <td>D&gt;</td> <td></td>	D>	
🕂 🖘 Transaction		463			Changed="Y">A <td></td> <td></td>		
🕂 🖘 Transaction		464	<bas< td=""><td>E_LANGUA</td><td>GE_CD&gt;ENG<td>ANGUAGE_CD&gt;</td><td></td></td></bas<>	E_LANGUA	GE_CD>ENG <td>ANGUAGE_CD&gt;</td> <td></td>	ANGUAGE_CD>	
🕀 🚸 Transaction		465	<msg< td=""><td>_SEQ_FLG</td><td>i/&gt;</td><td></td><td></td></msg<>	_SEQ_FLG	i/>		
🕂 🖘 Transaction		466	<pro< td=""><td>CESS_INST</td><td>TANCE IsChanged="Y":</td><td>976<td>IN STANCE&gt;</td></td></pro<>	CESS_INST	TANCE IsChanged="Y":	976 <td>IN STANCE&gt;</td>	IN STANCE>
🕀 🚸 Transaction		467	<pub< td=""><td>LISH_RULE</td><td>E_ID IsChanged="Y"&gt;AI</td><td>FILIATION FILTER</td><td>R</td></pub<>	LISH_RULE	E_ID IsChanged="Y">AI	FILIATION FILTER	R
🕁 🐟 Transaction		468	<msg< td=""><td>NODENAM</td><td>E IsChanged="Y"&gt; <td>SGNODENAME&gt;</td><td></td></td></msg<>	NODENAM	E IsChanged="Y"> <td>SGNODENAME&gt;</td> <td></td>	SGNODENAME>	
🗄 🐟 Transaction		469					
🕁 🐟 Transaction		470	470				
🗄 🐟 Transaction		471 <transaction></transaction>					
🕁 🚸 Transaction		472			DN_I class="R">		
+ A Transaction		473			nged="Y">ADCRM1003		
+ A Transaction		474	<scc< td=""><td></td><td></td><td></td><td></td></scc<>				
+ A Transaction		475 476			hanged="Y">1986-03-	06	
+	<		<rir i<="" td=""><td>HPI ACE/&gt;</td><td></td><td></td><td></td></rir>	HPI ACE/>			
			Har Daar				
	1-11	ee Selec	tion Brow	ser			
						PSCAMA	ł
<	1	Attribute	es:				
Tree View 🔽 0 warning(s), 0 error(s)		name	value				
Table Selection Browser	×  1	🔳 da	ss R				
- This Tree Selection Browser is empty		Subtage					
		Tag na	me/Text		T Text	IsChanged	
	1	<t> LA</t>	NGUAGE_	CD	ENG		
	2	<r>   &lt;</r>	DIT_ACT	4	A	Y	
	3	<	SE_LANG	UAGE_CD	ENG		
	4	4 🔶 MSG_SEQ_FLG					
	5			NSTANCE	976	Y	
	6	117	BLISH_R		AFFILIATION FILTER	-	
	7	M17	GNODEN			Y	
	Ľ		SHODEN				

PSCAMA is an XML tag that contains fields common to all messages. The PSCAMA tag is repeated for each row in each level of the Transaction section of the message. PSCAMA provides the following information about the message data:

- Language in which the data is written
- Type of transaction the row represents, such as add or update

When receiving a message, PeopleCode inspects the PSCAMA node for this information and responds accordingly.

#### A.2 Root Audit Action

The AUDIT\_ACTN subnode of PSCAMA, known as Root Audit Action, filters the data records in an XML message. It indicates the action taken against a person, such as Add or Change in Oracle Identity Manager.

If the biographical information is changed for a person on the target system, then the Root Audit Action value is C. If a person is added, then the Root Audit Action is either A or empty.

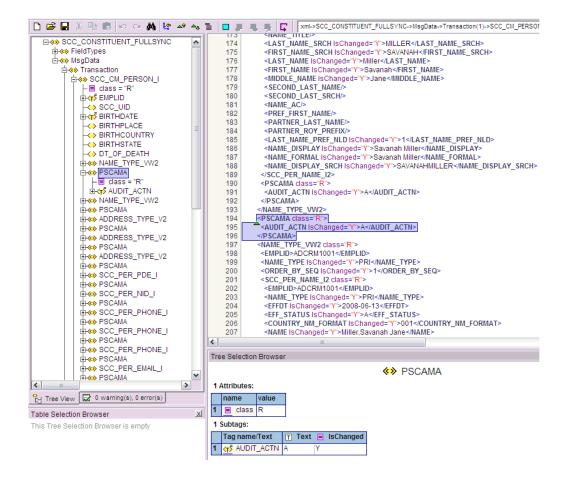
The Add Root Audit Action is shown in the following screenshot:



🗋 🗃 🖬 🐇 🖿 💼 📖 🗠 🚧 🔽 🔺 🗛		
SCC CONSTITUENT FULLSYNC	442	<scc_afl_person class="R"></scc_afl_person>
+w FieldTypes	443	<emplid ischanged="Y">ADCRM1001</emplid>
⊟-«» MsgData	444	<institution ischanged="Y">PSUNV</institution>
⊢ (→ moge ata	445	<scc_afl_code lschanged="Y">STUDENT</scc_afl_code>
SCC_CM_PERSON_I	446	<start_dt ischanged="Y">2002-08-27</start_dt>
E-w PSCAMA	447	<scc_afl_spons_dept></scc_afl_spons_dept>
	448	<end_dt></end_dt>
-	449	<lastupdoprid ischanged="Y">SAMPLE</lastupdoprid>
EANGUAGE_CD	450	<lastupddttm ischanged="Y">2009-08-02T23:34:16.000000-0700</lastupddttm>
⊕≺ <del>T</del> ≶AUDIT_ACTN	451	<scc_afl_plcd_mtd ischanged="Y">M</scc_afl_plcd_mtd>
	452	<scc_afl_rlcd_mtd></scc_afl_rlcd_mtd>
MSG_SEQ_FLG	453	<scc_afl_status lschanged="Y">ACT</scc_afl_status>
Instance Instance	454	<scc_afl_sts_descr lschanged="Y">Applied</scc_afl_sts_descr>
ti+	455	<scc_afl_rank ischanged="Y">300</scc_afl_rank>
±<⁵ MSGNODENAME	456	
🕁 🐟 Transaction	457	<pscama class="R"></pscama>
🕁 🐟 Transaction	458	<audit_actn ischanged="Y">A</audit_actn>
	459	
Transaction	460	
+ «» Transaction	461	<pscama class="R"></pscama>
+-«» Transaction	462	<language_cd>ENG</language_cd> AUDIT_ACTN IsChanged="Y">A
Transaction	463	<pre>SAUDIT_ACTNISCHanged= Y &gt;AA</pre> SBASE_LANGUAGE_CD>ENG
Transaction	464	
+- (*) Transaction	465	<msg_seq_flg></msg_seq_flg> <process_instance lschanged="Y">976</process_instance>
+-«» Transaction	400	<pre><process_instance r"="" schanged="1~\$76&lt;/pre&gt;Process_instance/ &lt;pre&gt;&lt;pre&gt;end&lt;/pre&gt;&lt;pre&gt;center&lt;/pre&gt;&lt;pre&gt;&lt;pre&gt;center&lt;/pre&gt;&lt;pre&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;+-«» Transaction&lt;/td&gt;&lt;td&gt;467&lt;/td&gt;&lt;td&gt;&lt;pre&gt;&lt;pre&gt;&lt;pre&gt;&lt;pre&gt;&lt;pre&gt;&lt;pre&gt;&lt;pre&gt;&lt;pre&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Transaction&lt;/td&gt;&lt;td&gt;469&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;+&lt;/td&gt;&lt;td&gt;409&lt;/td&gt;&lt;td&gt;&lt;/Transaction&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;471&lt;/td&gt;&lt;td&gt;&lt;Transaction&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;⊕≪» Transaction&lt;/td&gt;&lt;td&gt;472&lt;/td&gt;&lt;td&gt;&lt;SCC_CM_PERSON_I class="></process_instance></pre>
	473	<emplid ischanged="Y">ADCRM1003</emplid>
+ (*) Transaction	474	<scc_uid></scc_uid>
+ «» Transaction	475	<birthdate ischanged="Y">1986-03-06</birthdate>
🕂 🚸 Transaction	476	<pre><birthpi ace=""></birthpi></pre>
🕂 🖘 Transaction	<	
	Tree Dele	ction Browser
	Thee Sele	
		AUDIT_ACTN
<	1 Attribu	tes:
Tree View 🔽 0 warning(s), 0 error(s)	name	value
		Changed Y
This Tree Selection Browser is empty	1 Text se	ecuon:
	A	
	_	

The nonzero level PSCAMA node and its Root Audit Action are shown in the following screenshot:





# Setting Up SSL on Oracle WebLogic Server

This section describes how to configure SSL on Oracle WebLogic Server for PeopleTools 8.50, PeopleTools 8.51, PeopleTools 8.52 and PeopleTools 8.53 versions.

To set up SSL on Oracle WebLogic Server, perform the following steps:

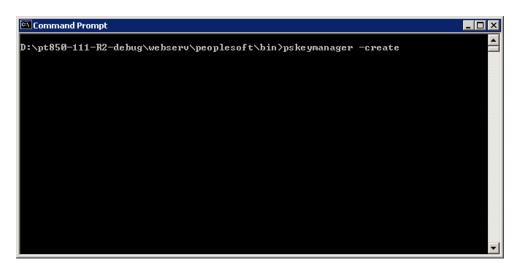
- Generating Signed Public Encryption Key and CSR
- Submitting CSRs to CAs for Signing
- Downloading the Root Certificate
- Importing a Server-Side Public Key into a Keystore
- Generating and Importing Public Keys
- Configuring Oracle WebLogic Server to Use the Keystore
- Adding the Root Certificate
- Configuring the PeopleSoft Certificates

## B.1 Generating Signed Public Encryption Key and CSR

To generate signed public encryption key and certificate signing request (CSR):

- **1.** Start PSKeyManager by navigating to the appropriate directory on the MS-DOS command prompt.
- 2. Enter the following at the command line:

pskeymanager -create



The PSKeyManager opens.



3. Enter the following at the command line:

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

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

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

Press Enter.

🖾 PeopleSoft PSkeymanager.	
PeopleSoft PSKeyManager: A wrapper to Sun's keytool for managing keys and certificates.	
Default passwords are 'password' Enter current keystore password [press ENTER to quit]:password	
Warning: Your keystore password is set to the default password of 'password'. This is too obvious and should NEVER be used in a production environment. You can change you keystore password via the -changekeystorepassword option.	
Generate new keys.	
All certificates and keys require an alias that they will be referenced by. To use local machine name press ENTER, to exit enter 'QUIT'.	
Specify an alias for this certificate [PLE-DC23641-B]?pt850gw	
Specify a common name for this certificate. For server certificates specify the host name as requested by clients. For client certificates specify the name is the name of the client.	
What is the common name for this certificate [pt850gw]?	-

Enter the appropriate information at the following command prompts:

Organization unit

Organization

City or Locality

State or Province

Country code

Number of days the certificate should be valid (Default is 90.)

Key size to use (Default is 1024.)

Key algorithm (Default is RSA.)

Signing algorithm (Default is MD5withRSA or SHA1withDSA.)

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



🖼 PeopleSoft PSkeymanager.	_ 🗆 ×
Generate new keys.	-
All certificates and keys require an alias that they will be referenced by. To use local machine name press ENTER, to exit enter 'QUIT'.	
Specify an alias for this certificate [PLE-DC23641-B]?pt850gw	
Specify a common name for this certificate. For server certificates specify the host name as requested by clients. For client certificates specify the name is the name of the client.	
What is the common name for this certificate [pt850gw]?ple-dc23641-b.people	soft.
com What is the name of your organizational unit?PeopleTools	
What is the name of your organization?Oracle What is the name of your City or Locality?Pleasanton	
What is the name of your State or Province?CA	
What is the two-letter country code for this unit?US	
How many days should this certificate request be valid for [90]?	
What key size would you like to use [1024]? What key algorithm would you like to use (RSA or DSA) [RSA]?	
What signing algorithm would you like to use (MD5withRSA or SHA1withDSA) [M	D5wit
hRSA J?	
Enter a private key password (press ENTER to use keystore password) ?passwo	rd 🔽

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

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

The following example shows a sample CSR:

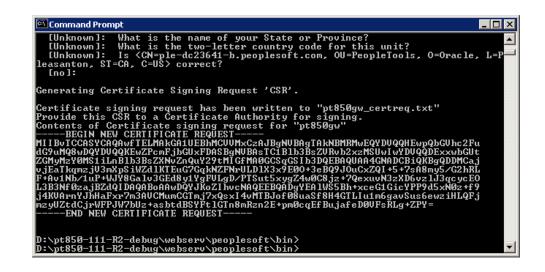
----BEGIN NEW CERTIFICATE REQUEST----

MIIBtDCCAR0CAQAwdDELMAkGA1UEBhMCVVMxEDAOBgNVBAgTB0FyaXpvbmExEDAOBgNVBAcTB1Bob 2VuaXgxFDASBgNVBAoTC1B1b3BsZVRvb2xzMRMwEQYDVQQLEwpZW9wbGVzb2Z0MRYwFAYDVQQDEw1 NREFXU09OMDUxNTAzMIGfMA0GCSqGS1b3DQEBAQUAA4GNADCBiQKBgQC431CZWxrsyxven5QethAd sLIEEPhhh17TjA0r8pxpO+ukD8LI7T1TntPOMU535qMGfk/

jYtG0QbvpwHDYePyNMtVou6wAs2yr1B+wJSp6Zm42m8PPihfMUXYLG9RiIqcmp2FzdIUi4M07J8ob 8rf0W+Ni1bGW2dmXZ0jGvBmNHQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAKx/

ugTt0soNVmiH0YcI8FyW8b81FWGIR0f1Cr2MeDi0Q2pty24dKKLUqIhogTZdFAN0ed6Ktc82/5xBo H1gv7YeqyPBJvAxW6ekMsg0EzLq90U3ESezZorYFdrQTzqsEXUp1A+cZdfo0eKwZTFmjNAsh1kis+ H0LoQQwyjgaxYI=

-----END NEW CERTIFICATE REQUEST-----



The CSR is a text file, and is written to the *<PSFT\_HOME*>\webserv\peoplesoft directory. The file name is *<*host\_name>\_certreq.txt.



## B.2 Submitting CSRs to CAs for Signing

To submit CSRs to CAs for signing:

#### Note:

The set of pages are different depending on what CA you plan on using.

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

Microsoft Certificate Services PeopleTools TEST root CA Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

2. Click advanced certificate request.

Microsoft Certificate Services PeopleTools TEST root CA	<u>Home</u>
Request a Certificate	
Select the certificate type: <u>Web Browser Certificate</u> <u>E-Mail Protection Certificate</u>	
Or, submit an <u>advanced certificate request</u> .	

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



Microsoft	Certificate	Services.	Peo	pleTools	s TEST	root C	A
inite obtaile	Commonio.	CONNECC.	1 00	proroon		1001 0	~ ``

#### Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

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

The Submit a Certificate Request or Renewal page appears.

4. Paste the content of the CSR in the **Saved Request** list box.

Microsoft Certificate Services -- PeopleTools TEST root CA

<u>Home</u>

<u>Home</u>

#### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:		
	coCzePJpz2FrdNsJDB+7WVnM4NpXSm4LNarVX1v3	•
	ATNrjFOCF8UgW/s7EgBDLeYeOghr4GhZb5+OqL7B	
certificate request	RaCDyB3ctT/mtwIDAQABoAAwDQYJKoZIhvcNAQEE	
(CMC or	yILeQWoL2cOtfFUB3YGvTWk/B07yxtivTiUL7kC7	
PKCS #10 or	vAsawubYd9FpP7mN0RwFVnRCDLDRLak/kPeh5rhG	
PKCS #7):	END NEW CERTIFICATE REQUEST	Ŧ
	Browse for a file to insert.	

#### Additional Attributes:

	<b>A</b>	
Attributes:	-	

The CA may send the signed public key (root) certificate to you by e-mail or require you to download it from a specified web page.

5. Download and save the signed public key on your local drive.

Microsoft Certificate Services Peo	pleTools TEST root CA	<u>Hom</u> e
Certificate Issued		
The certificate you requested wa	is issued to you.	
© DER encoded or <u> Download certificate</u> <u> Download certificate</u>	● Base 64 encoded chain	



## B.3 Downloading the Root Certificate

To download the root certificate:

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

 Microsoft Certificate Services -- PeopleTools TEST root CA
 Home

 Welcome
 Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

 You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

 For more information about Certificate Services, see Certificate Services Documentation.

 Select a task:

 Request a certificate

 View the status of a pending certificate request

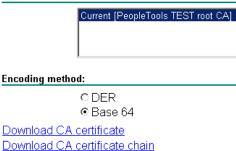
 Download a CA certificate, certificate chain, or CRL

2. From the CA certificate list, select the certificate.

 Microsoft Certificate Services
 PeopleTools TEST root CA
 Home

 Download a CA Certificate, Certificate Chain, or CRL
 To trust certificates issued from this certification authority, install this CA certificate chain.

 To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.
 CA certificate:



3. Download and save the root certificate on your local drive.

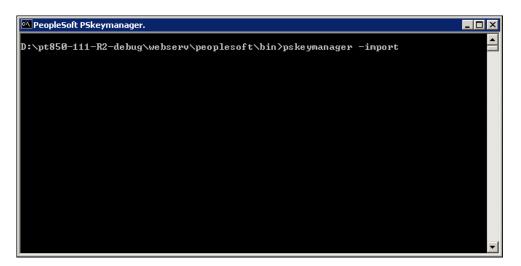
## B.4 Importing a Server-Side Public Key into a Keystore

To import a server-side public key into a keystore.



- 1. Open PSKeyManager.
- 2. Navigate to the required directory on the MS-DOS command prompt.
- 3. Enter the following at the command line:

pskeymanager -import



- 4. At the Enter current keystore password command prompt, enter the password and press Enter.
- 5. At the Specify an alias for this certificate <host\_name>? command prompt, enter the certificate alias and press Enter.
- 6. At the Enter the name of the certification file to import command prompt, enter the path and name of the certificate to import.



7. At the Trust this certificate command prompt, enter Yes and press Enter.



🖾 Command I	Prompt _	
	'password'. This is too obvious and should NEVER be used in a production environment. You can change you keystore password via the -changekeystorepassword option.	
	icates and keys require an alias that they will be referenced by. R to use local machine name, to exit enter 'QUIT'.	
Specify an	alias for this certificate [PLE-DC23641-B]?PeopleTools	
RootCA.cer Owner: CN= pment, O=P Issuer: CN opment, O= Serial num Valid from Certificat S Trust this	name of the certificate file to import [press ENTER to quit]:D:\cer PeopleTools TEST root CA, DC=peoplesoft, DC=com, OU=PeopleTools Dev PeopleSoft Inc, L=Pleasanton, ST=CA, C=US =PeopleTools TEST root CA, DC=peoplesoft, DC=com, OU=PeopleTools De PeopleSoft Inc, L=Pleasanton, ST=CA, C=US bher: 3056c40e07cb9991450c34f5e4af8160 :: Thu Nov 20 09:31:30 PST 2003 until: Mon Nov 20 09:36:28 PST 2023 :e fingerprints: ID5: BE:91:16:2D:10:CC:FA:78:5E:4B:C0:CD:55:97:86:FB HA1: 05:58:F8:FF:43:EA:74:48:9A:44:24:4A:9E:5C:72:19:93:51:91:9C : certificate? [no]: yes e was added to keystore	elo
D:\pt84705	a-debug\webserv\peoplesoft2>	

## **B.5 Generating and Importing Public Keys**

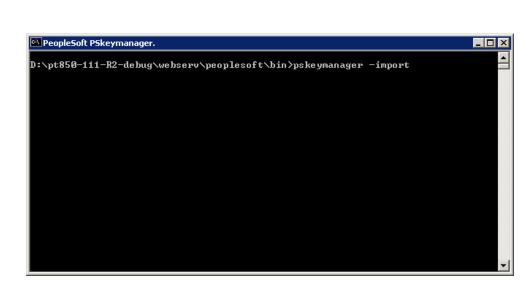
To generate and import public keys:

pskeymanager -import

1. Place the public key from your CA in the keystore. The location of the keystore is as follows:

<PSFT\_HOME>\webserv\peoplesoft\keystore

 Install the certificate for server authentication SSL on Oracle WebLogic Server using the following command:

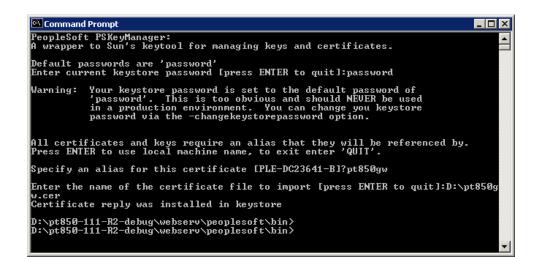


- 3. At the Enter current keystore password command prompt, enter the password and press Enter.
- 4. At the Specify an alias for this certificate <host\_name>? command prompt, enter the certificate alias and press Enter.
- 5. At the Enter the name of the certification file to import command prompt, enter the path and name of the certificate to import.



🖼 PeopleSoft PSkeymanager.	
PeopleSoft PSKeyManager: A wrapper to Sun's keytool for managing keys and certificates.	<b></b>
Default passwords are 'password' Enter current keystore password [press ENTER to quit]:password	
Warning: Your keystore password is set to the default password of 'password'. This is too obvious and should NEVER be used in a production environment. You can change you keystore password via the -changekeystorepassword option.	
All certificates and keys require an alias that they will be referenced by. Press ENTER to use local machine name, to exit enter 'QUIT'.	
Specify an alias for this certificate [PLE-DC23641-B]?pt850gw	
Enter the name of the certificate file to import [press ENTER to quit]:D:\p $w.cer_{-}$	t850g
	<b>~</b>

Certificate is successfully installed in the keystore.



# B.6 Configuring Oracle WebLogic Server to Use the Keystore

Configuring the Oracle WebLogic Server to use the keystore:

1. Log in to Oracle WebLogic Administration Console.



(bea	WEBLOGIC SE ADMINISTRATION (	
	Log in to wor	k with the WebLogic Server domain
	Username:	system
	Password:	******
		Log In

2. Expand **PeopleSoft, Environment, Servers, PIA** to setup the SSL configuration for the PIA server.

Change Center	Welcome, system Connected to: people
View changes and restarts	Home > Summary of Environment > Summary of Servers > PIA
No pending changes exist. Click the Release Configuration button to allow others to edit the	Settings for PIA
domain.	Configuration Protocols Logging Debug Monitoring Control Deployments Services Securi
Lock & Edit	General Cluster Services Keystores SSL Federation Services Deployment Migra
Release Configuration	Save
Domain Structure	Keystores ensure the secure storage and management of private keys and trusted certificate aut
peoplesoft ®-Environment Deployments ®-Services	keystore configurations. These settings help you to manage the security of message transmission
-Security Realms  -Interoperability  -Diagnostics	Keystores: Demo Identity and Demo Trust Vhich could identity and Demo Trust
E Diagi lostica	Identity
How do I	Demo Identity Keystore: D:/beawls92/WEBLOG~1/server\lib\DemoIdentity.jks The path
Configure identity and trust Configure keystores	Demo Identity Keystore jks The type Type: blank, it c
Set up SSL	Demo Identity Keystore *******************************
System Status	Passphrase: then the l

- 3. Click the **Keystores** tab.
- 4. From the Keystores list, select Custom Identity and Custom Trust.
- 5. In the **Identity** region, complete the following fields:
  - In the Custom Identity Keystore field, enter keystore/pskey.
  - In the Custom Identity Keystore Type field, enter JKS.
  - In the Custom Identity Keystore Passphrase field, enter password.
  - In the Confirm Custom Identity Keystore Passphrase field, enter password again.



Release Configuration	General Cluster Services K	eystores   SSL   Federation Services	s Deployment Migration Tuning Overload
	Save		
Domain Structure			
ecoplesoft E-Environment Servers Clusters		rage and management of private keys a settings help you to manage the security	nd trusted certificate authorities (CAs). This page le of message transmissions.
Virtual Hosts Migratable Targets Machines Work Managers	Keystores:	Custom Identity and Custom Trust	Which configuration rules should be used trust keystores? More Info
-Startup & Shutdown Classes -Deployments	- Identity		
Services     Security Realms     F-Interoperability	Custom Identity Keystore:	keystore/pskey	The path and file name of the identity key
B-Diagnostics	Custom Identity Keystore Type:	JKS	The type of the keystore. Generally, this is
iow do I	Custom Identity Keystore Passphrase:	*************	The encrypted custom identity keystore's the keystore will be opened without a pas
# Configure identity and trust # Configure keystores # Set up SSL	Confirm Custom Identity Keystore Passphrase:	*****	Re-enter the custom identity keystore pas
System Status	— Trust —		
Health of Running Servers	Custom Trust Keystore:	keystore/pskey	The path and file name of the custom tru:
Failed (0)	Custom Trust Keystore	[1.02]	The type of the keystore. Generally, this k

6. On the SSL tab, ensure that the parameter **Two Way Client Cert Behavior** is set to **Client Certs Requested and Enforced.** 

Failed (0)			<b>_</b>
Critical (0)	49 Hostname Verification:	BEA Hostname Verifier	Specifies wł weblogic.se
Overloaded (0)			acting as a (
Warn (0)	🚳 Custom Hostname Verifier:		The name o weblogic.sei
	Export Key Lifespan:	500	Indicates the exportable k before gene Server to be generating a
	Two Way Client Cert Behavior:	Client Certs Requested and Enforced	The form of
	<section-header> Cert Authenticator:</section-header>		The name o weblogic.sei this release security only Authenticati
	SSLRejection Logging Er	abled	Indicates wł when SSL o
	Inbound Certificate Validation:	Builtin SSL Validation Only	Indicates the Info
4	Outhound Cortificato		Indicates the

7. Click the Activate Changes button.



<b>WEBLOGIC SERV</b>		
Change Center	Welcome, system	Connected to: peoplesoft
View changes and restarts	Home > Summary of Environment > Summary	of Servers > PIA
Pending changes exist. They must be activated to take effect. Activate Changes	Messages Settings updated successfully.	
Undo All Changes	Settings for PIA	
Domain Structure  peoplesoft  E-Environment Deployments Services Services E-Interoperability Diagnostics	General Cluster Services k Save	Debug         Monitoring         Control         Deployments         Services         Security           (eystores         SSL         Federation         Services         Deployment         Migration           fine various         Secure         Sockets Layer         (SSL) settings for this server instance         Secure
How do I	Identity and Trust Locations:	Keystores Indicates where SS key) as well as the
Set up SSL     Verify host name verification is     enabled     Configure a custom host name	— Identity Private Key Location:	from Custom Identity Keystore The keystore attrib Info

## B.7 Adding the Root Certificate

To add root certificate:

1. Expand Security, Security Objects, and then click Digital Certificates.

				THEFT	Yvorklist MultiChannel Console		306	
atu 2	-	Digital C	ertificates		New Window	<u>Customize F</u>	<u>Page</u>	h
- Single Signon - Signon PeopleCode		Digital Certific	ates		Customize   Find   🛗 First	1.19 of 19	D ,	ast
- Security PeopleCode		TYPE	<u>'Alias</u>	<u>'Issuer Alias</u>	Valid to			
Options		Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail	+	-
D Query Security D Encryption		Root CA 💌	PeopleTools Test Root CA	PeopleTools Test Root CA		Add Root	+	-
- Common Queries		Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail	+	
- Mass Change Operator		Root CA	KeyWitness Root	KeyWitness Root		Detail	+	
Security Utilities		Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	Detail	+	
Workflow		Root CA	Thawte Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	Detail	+	
Portal		Root CA	Thawte Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	Detail	+	
Search Engine Personalization		Root CA	Thawte Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	Detail	+	-
Process Scheduler		Root CA	Thawte Server	Thawte Server	12/31/20 3:59:59PM	Detail	+	
Cube Manager		Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	Detail	+	
Application Engine Query Access Services		Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	Detail	+	E
Integration Broker		Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	Detail	+	
REN Server Configuration Setup Manager		Root CA	Verisign Class 2 - 02	Verisign Class 2 - G2	05/18/18 4:59:59PM	Detail	+	
Setup Manager MultiChannel Framework		Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	Detail	+	_
			-	-			_	_

2. Click Add Root.

## **B.8 Configuring the PeopleSoft Certificates**

To configure the PeopleSoft certificates:



Note:

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

- 1. Expand Security, Security Objects, and then click Digital Certificates.
- 2. Add a local node type certificate.
- 3. Set Alias to the default local node.

ORACLE			не	me   Worklist   MultiChannel Co	nsole Add to Favori	tes Is	-
u 2 🗖					and I management		
	-			New W	indow Customize I	Page	3
- User Profile Types - Tables to Skip							
- Security Links	Digita	l Certificates					
- Digital Certificates	Digita	Certificates					
<ul> <li>Single Signon</li> <li>Signon PeopleCode</li> </ul>	Digital Ce	rtificales		Customize   Find	First 🛃 1.20 of 20	🗈 La	st
- Security PeopleCode	IVDE	<u>"Alias</u>	<u>'Issuer Alias</u>	Valid to			
Options	Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail	+	=
Query Security Encryption	Local No	Id CE_LOCAL	PeopleTools Test Root CA	Q.	Request	÷.	-
Common Queries	Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail	+	-
Mass Change Operator	Root CA	KeyWitness Root	KeyWitness Root		Detail	+	-
Security Milities	Root CA	PeopleTools Test Root CA	PeopleTools Test Root CA	11/20/23 9:36:28AM	Detail	+	-
forkflow	Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	Detail	+	-
ortal	Root CA	Thawte Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	Detail	+	
earch Engine ersonalization	Root CA	Thawle Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	Detail	<b>H</b>	
rocess Scheduler	Root CA	Thawte Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	Detail	+	-
ube Manager pplication Engine	Root CA	Thawle Server	Thawte Server	12/31/20 3:59:59PM	Detail	+	-
uery Access Services	Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	Detail	+	-
itegration Broker	Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	Detail	<b>H</b>	-
EN Server Configuration etup Manager	Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	Detail	+	-
ultiChannel Framework	Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	05/18/18 4:59:59PM	Detail	<b>+</b>	=
rchive Data	Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	Detail	+	-
ata Archive Manager ranslations	Root CA	Verisign Class 3 - G3	Verisign Class 3 - 03	05/18/18 4:59:59PM	Detail	E I	
							1

- 4. Click Request.
- 5. Send this certificate request to the CA to get a new certificate.

ORACLE	
	Home Worklast MadiChennel Console Addito Fevorites Sign out
Menu 2 🗖	
	🔺 New Window   Customice Page   🔍 🛋
- User Profile Types	CONVENTION CONVENTION CONVENTION
- Tables to Skip	Request New Certificate
- Security Links	
- Digital Certificates	Subject Information
- Single Signon	Common Name: GE_LOCAL
- Signon PeopleCode	Carling Rome, ac_coore
<ul> <li>Security PeopleCode Options</li> </ul>	Org Unit: PeopleTools
D Query Security	
D Encryption	Organization: Oracle
- Common Queries	
- Mass Change Operator	Locality: Pleasanton
Security	a state Residence for
D Utilities	State/Province: CA Country: US
Viorkflow	Key Pair Information
D Portal	
D Search Engine D Personalization	Algorithm: SHA1 with RSA encryption
D Process Scheduler	
D Cube Manager	*Key Size: 1024 bits
Application Engine	
D Query Access Services	Additional Certificate Attributes
Integration Broker	Email Address:
D REN Server Configuration	Lindi Pase das
Setup Manager	Challenge Pswd:
D MultiChannel Framework D Archive Data	
Data Archive Manager	OK Cancel Refresh
D Translations	
D EDI Manager	

6. Click OK.



Menu 2       Image: Customize Pi         > Security Opicstic       Image: Customize Pi         - Licar Profile Types       - Licar Profile Types         - Tables to Sking       - Customize Pi         - Binon PeopleCode       - Security Links         - Sinon PeopleCode       - Security Picture         - Binon PeopleCode       - Security Picture         - Dide Standon       - Dide Control Council Code         - Security PeopleCode       - Security Picture         - Common Queries       - Social Control Council Processing         - Missic Change Operator       - Security Picture         - Workflow       - Portal         - Workflow       Portal         - Portal Description       - Standard Provide Code         - Workflow       - Portal         - Portal Description       - Standard Provide Code         - Workflow       - Portal         - Portal Description       - Standard Provide Code         - Process Scheduler       - Cuber Manager         - Refresh       - Nume Control Code Refresh         - Refresh       - Refresh

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

				Hon	e Worklist MultiChannel Conso	le Add to Favor	tes	200
nu 2 Security Objects					Now Mine	tow Customize	Page	13
- User Profile Types	-					Net Subannee	1.040	1 No
<ul> <li>Tables to Skip</li> <li>Security Links</li> </ul>		Distant of						
- Digital Certificates		Digital C	Certificates					
- Single Signon		Digital Certifi	cates		Customize   Find	First 🛃 1.20 of 20	D.	act
- Signon PeopleCode - Security PeopleCode		Type	'Alias	'Issuer Alias	Valid to			
Options		Local Node	QE_LOCAL	PeopleTools Test Root CA		Import	+	Ξ
D Query Security		Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail	+	-
Encryption – Common Queries		Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail	+	-
- Mass Change Operator		Root CA	KeyWitness Root	KeyWitness Root		Detail	+	-
Security		Root CA	PeopleTools Test Root CA	PeopleTools Test Root CA	11/20/23 9:36:28AM	Detail	+	Ξ
Utilities Workflow		Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	Detail	+	-
Portal		Root CA	Thawle Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	Detail	+	-
Search Engine		Root CA	Thawte Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	Detail	+	
Personalization Process Scheduler		Root CA	Thawle Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	Detail	+	Ξ
Cube Manager		Root CA	Thawte Server	Thawte Server	12/31/20 3:59:59PM	Detail	+	-
Application Engine Query Access Services		Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	Detail	+	Ξ
Integration Broker		Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	Detail	+	-
REN Server Configuration		Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	Detail	+	-
Setup Manager MultiChannel Framework		Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	05/18/18 4:59:59PM	Detail	+	=
Archive Data	-	Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	Detail	+	Ξ
Data Archive Manager		Root CA					+	

8. Click Import.

The Import Certificate page appears.

Distance       Weekligt       Multi-Value       Additional Control Control       Son and <ul> <li></li></ul>	Me	nu 2  Security Objects User Profile Types Tables to Skip Becurity Links	-	_
> Security Objects       Import Certificate         - Lidar Profile Tyrings       Import Certificate         - Lidar Profile Tyrings       Import Certificate         - Distance Certificate       Import Certificate         - Distance Certificate       Import Certificate         - Distance Certificate       Import Certificate         - Bindle Standn       - Bindle Standn         - Distand Ministary Pay (Standney Standney Standn	Me	Security Objects     User Profile Types     Tables to Skip     Security Links		New Window   Customize Page   🚇
> Security Objects       Import Certificate         - Lidar Profile Tyrings       Import Certificate         - Lidar Profile Tyrings       Import Certificate         - Distance Certificate       Import Certificate         - Distance Certificate       Import Certificate         - Distance Certificate       Import Certificate         - Bindle Standn       - Bindle Standn         - Distand Ministary Pay (Standney Standney Standn	me	Security Objects     User Profile Types     Tables to Skip     Security Links		New Window   Customize Page   🦷
- User Prefile Trynes     - Lifer Prefile Trynes     - Lifer Sking     - Diatal Certificates     - Diatal Certificate		- User Profile Types - Tables to Skip - Security Links		New Vendow   Customize Page   38
- Tables to Skin         - Distance for the certificate         - Distance for the certificate         - Distance for the certificate for OE_LOCAL, paste the PEM formatted certificate data here.         - Single Standor         - Single Standor         - Bingle Standor		- Tables to Skip - Security Links	Import Certificate	
Security Links     Distal Certificate     Distal Certificate     Distal Certificate     Distal Certificate     Distal Certificate     Distal Certificate     To import the certificate for OE_LOCAL, paste the PEM formatted certificate data here.     Teleport the certificate for OE_LOCAL, paste the PEM formatted certificate data here.     Security     Distal Standon     Distal Content		- Security Links	Import Certificate	
Distal Certificates     Distal     D				
Single Signon     Dianon PeopleCode     Dianon PeopleCode     Security PeopleCode     Dianon PeopleCode				
Signand RespireCode     Sugnative Respi			To import the certificate for QE_LOCAL, paste the PEM formatted certificate data here.	
Security PeopleScole         201932/CTC/h0d1H46U;94x005607040x198x2049x00280220LmNe950522/URPM9b3ta           Obtions         L18b33s2/VRb2z01FWc2047040x195x2048x00x9220LmNe950522b0U8499b3ta           D Clarger Security         Encryption           - Common Outgines         V049x05070040x195x20148x02048x20040x20140x050x050x050x050x050x050x050x0148           - Mass Changer Operator Broundty         Encryption           - Utilities         Common Outgines           - Mass Changer Operator Broundty         Common Outgines           - Willies         Vertified Security           - Utilities         Vertified Security           - Utilities         Vertified Security           - Willines         Vertified Security           - Willines         Vertified Security           - Workdow         Partial           - Personalization         Certified Security           - Process Scheduler         OK           - Occel         Retexth				
Options         L1Bib 3B 32/Rxb2zgTir/WEVTVCU/MIH/Mb30IMI8DQ85(cmy0502pb0U8Ly9cH80           0 Query Security         Discreption           0 Encryption         Encryption           0 Common Queries         Generative Security           Mass Change Operator         Generative Security           0 WorkSow         Chowa Anitowy B002/Supervised B002/Su				
Duary Security     Dishrict2(LaB):59:20%20(2):99(CNII:nPF pi):Ab0/02(UV/cOV/CVV/CVV/CVV/CVV)       Disnryston     Common Quaries       - Common Quaries     Common Quaries       - Minss: Change Operator Brouth     Common Quaries       - Minss: Change Operator Brouth     Common Quaries       - Withese     Common Quaries       - Minss: Change Operator Brouth     Common Quaries       - Withese     Common Quaries       - Minss: Change Operator Brouth     Common Quaries       - Withese     Common Quaries       - Workdow     Common Quaries       - Portal     Personitization       - Process Scheduler     OK       - Okanger     OK				
• Encrypton         - Common Queries           • Common Queries         - Common Queries           • Mass Change Operator         - Common Queries           • Mass Change Operator         - Common Queries           • Miss Change Operator         - Common Queries           • Workdow         - Common Queries           • Workdow         - Common Queries           • Workdow         - Common Queries           • Portail         - Common Periodic Operator           • Process Scheduler         - Miss Changer           • Cubit Manager         - OK           • Cubit Manager         OK				
Dommon Quartes     Hass Charge Demake     Hass Charge Demakee     Hass Charge Demakeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee				
- Missis Change Operator Becurity         Leftis 38 ± 20 M 2010 V/39 VFI Bio 38 ± 20 M 20 04 ± 10 ± 20 ±				
Binculty         Condwardiantian           Binculty         Condwardiantian           D Utilities         Condwardiantian           Visities         VertNiceRebandedsetter           Visities         VertNiceRebandedsetter           Portal         Portal           Pensionalization         Page 2015 PWTNdby/Bin/2018/Bin				
Dutting         Description           0 Utilities         VEXTVC-Bit/290IENBL_mNydDANBykqhki09V0BAQUFAA0BgCcl/hh8B0lq718a2b8I           0 Yoorsflow         VEXTVC-Bit/290IENBL_mNydDANBykqhki09W0BAQUFAA0BgCcl/hh8B0lq718a2b8I           0 Yoorsflow         TaincUHB8C/267hCUFW0BRHUdghABH2RPV04+tmUdul1a2(++hxCa4ki2K7VhV           0 Portal         Pp1.82rgs2rllL 671+effKUdghABH2RPV04+tmUdul1a2(++hxCa4ki2K7VhV           0 Personalization         Pincess Scheduler           0 Cube Manager         OK         Cancel				
> Workflow         VEVTVC5bp290IINBLmtkydDANBpichio5%03BAOUFAAOBg02Ch0ABg02Th62088           > Pontal         TutuUt98c2dmVLdfW38bRTUdfy38bB7B2R9V4 + tnut0a11 a2(++knCa4k02K7VIV)           > Personalization         Pp1.82xp22dLC7L+dT%UD68gu#4b06wyTe/SXAB30k+i6WpLCeTX200MMenUCh9           > Process Scheduler         Cq4W315fULJF601EPWTM0P8gu=           > Cube Manager         OK         Cancel				
Portal     TriarUHBBC2004T0/MVN06Hhr/UgMA8hb2HBY04FHr/Jan2HeY04Fh			VEVTVCByb290IENBLmNydDANBgkqhkiG9w0BAQUFAA0BgQCJhb6BQIq7I6a2b8I	
Search Engine     Personalization     Process Scheduler     OK     Cancel     Refresh				
Personalization     Process Scheduler     OK Cancel Refresh				
Process Scheduler     OK Cancel Refresh				
D Cube Manager OK Cancel Refresh			END CERTIFICATE	
			au and a start	
			OK Cancer Nelleen	
D Query Access Services				
D Integration Broker				
D REN Sever Configuration				
D Setu Manager				
P belug manager D MultiChannel Framework				
D Archive Data				
Distance Data				
Distance wantiger				
		EDI Manager	u	

#### 9. Click OK.

ORACLE			Hom	e Worklist MutiChannel Co	nsole Add to Fam	artes   Sigr
<ul> <li>User Profile Types</li> <li>Tables to Skip</li> <li>Security Links</li> <li>Digital Certificates</li> </ul>	-) Digital C	ertificates		New Y	ândow   <u>Customiz</u>	e Page   🐰
- Single Signon	Digital Certifi	cates		Customize   Find	First 🛃 1.20 of 2	a 🗈 Lasti
- Signon PeopleCode - Security PeopleCode	IVDE	'Alias	'Issuer Alias	Valid to		
Options	Local Node	QE_LOCAL	PeopleTools Test Root CA	07/27/08 10:49:25AM	Detail	+ -
Query Security	Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail	+ -
<ul> <li>Encryption</li> <li>Common Queries</li> </ul>	Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail	+ =
Mass Change Operator	Root CA	KeyWitness Root	KeyWitness Root		Detail	+ =
Security	Root CA	PeopleTools Test Root CA	PeopleTools Test Root CA	11/20/23 9:36:28AM	Detail	+ =
tilities (orkflow)	Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	Detail	+ -
ortal	Root CA	Thawte Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	Detail	+ =
earch Engine ersonalization	Root CA	Thawte Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	Detail	+ -
rocess Scheduler	Root CA	Thawte Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	Detail	+ =
ube Manager	Root CA	Thawte Server	Thawte Server	12/31/20 3:59:59PM	Detail	+ -
pplication Engine Juery Access Services	Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	Detail	+ -
itegration Broker	Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	Detail	+ =
EN Server Configuration	Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	Detail	+ =
etup Manager IultiChannel Framework	Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	05/18/18 4:59:59PM	Detail	
rchive Data	Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	Detail	+ =
lata Archive Manager	Root CA	Verisign Class 3 - G3	Verisign Class 3 - G3	05/18/18 4:59:59PM	Detail	+ =

**10.** Click Load Gateway Connectors.



ORACLE'			Home   Wischligt   MultiChannel Console	Add to Fevorites Sign
Menu 2  Prefestonization Performization Cube Manager Cube Manager Cube Manager Cube Manager Cuber Access Services Integration Broker Configuration Quadwars Configuration Quadwars Service Configuration Quadwars Diffegration Setup Diffegration Di	Gateways GatewayD: LOCAL ⊽ Local Gate	eway 🗌 Load Balancer		w   Customize Page   🚆
	URL: https://pie-dc2 Gatewar/Setup Properties Load Gatewary Connectors Connectors	23641-b.peoplesoft.com/PSIGW/Peo Return to Quick Conflouration		st 🖪 1-10 of 10 🕨 Last.
Monitor D File Utilities	Connector ID	Description	Connector Class Name	
REN Server Configuration	1 AS2TARGET		AS2TargetConnector	Properties 🛨 🖃
Setup Manager	2 FILEOUTPUT		SimpleFileTargetConnector	Properties + -
	2 ETOTADOET	1	ETPTarentConnector	Proposition (A) (A)
Archive Data	3 FTPTARGET		FTPTargetConnector	Properties + -
> Archive Data > Data Archive Manager > Translations	3 FTPTARGET 4 GETMAILTARGET		FTPTargetConnector GetMailTargetConnector	Properties + -
Archive Data Data Archive Manager Translations EDI Manager				
Archive Data Data Archive Manager Translations EDI Manager Mass Changes	4 GETMAILTARGET 5 HTTPTARGET		GetMailTargetConnector HttpTargetConnector	Properties + -
Archive Data     Data Archive Manager     Translations     EDI Manager     Mass Changes     Performance Monitor	4 GETMAILTARGET 5 HTTPTARGET 6 JIMSTARGET		GetMailTargetConnector HttpTargetConnector JIMSTargetConnector	Properties + - Properties + - Properties + -
Archive Data     Data Archive Manager     Data Archive Manager     Translations     EDI Manager     Mass Changes     Performance Monitor     Web Profile Change My Password	4 GETMAILTARGET 5 HTTPTARGET		GetMailTargetConnector HttpTargetConnector	Properties + - Properties + -
<ul> <li>MultiChannel Framework</li> <li>Archive Data</li> <li>Data Archive Manager</li> <li>Translations</li> <li>EDI Manager</li> <li>BEDI Manager</li> <li>Mass Changes</li> <li>Performance Monitor</li> <li>Web Profite</li> <li>Chance Mv Password</li> <li>Mv Password</li> <li>Mv Statem Profile</li> </ul>	4 GETMAILTARGET 5 HTTPTARGET 6 JIMSTARGET		GetMailTargetConnector HttpTargetConnector JIMSTargetConnector	Properties + - Properties + - Properties + -

The following message appear:

Loading Process was successful. Number of connectors loaded:0. Number of Properties loaded:0. (158,42)

Click OK.

**11.** Click **Ping Node** to ping your local node.

		Home   ytheritest   Multichennel Console   Austite Ferror	tes   Sian out	
Personalization     Process Scheduler     D Cube Manager	New Window   Customize Page   🕮			
D Application Engine D Query Access Services	Gateways			
Configuration Stroker     Configuration     Quick	Gateway ID: LOCAL			
	URL: https://pie-dc23 of Properties loaded:0. (156,4)	sful. Number of connectors loaded:0, Number 2)		
	Gateway Setue Properties	OK		
	Connectors Customize   First 🕘 4-10 of 10 🖻 Last			
Monitor D File Utilities	Connector ID Description	Connector Class Name		
D REN Server Configuration	1 AS2TARGET	AS2TargetConnector Properties	<b>E</b>	
Setup Manager D MultiChannel Framework	2 FILEOUTPUT	SimpleFileTargetConnector Properties		
D Archive Data	3 FTPTARGET	FTPTargetConnector Properties		
Data Archive Manager D Translations	4 GETMAILTARGET	GetMailTargetConnector Properties		
D EDI Manager	5 HTTPTARGET	HttpTargetConnector Properties		
D Mass Changes D Performance Monitor	8 JMSTARGET			
Veb Profile	7 LDAPTARGET			
<ul> <li>Change My Password</li> <li>My Personalizations</li> </ul>				
- My System Profile	8 PSFT81TARGET			
- My Dictionary	9 PSFTTARGET	PeopleSoftTargetConnector Properties	<b>H</b>	



# C Message Structure

All full data publish XML files contain the following message structure at the beginning of the files:

<?xml version="1.0"?> <SCC\_CONSTITUENT\_FULLSYNC> <FieldTypes> <SCC\_CM\_PERSON\_I class="R"> <EMPLID type="CHAR" /> <SCC\_UID type="CHAR" /> <BIRTHDATE type="DATE" /> <BIRTHPLACE type="CHAR" /> <BIRTHCOUNTRY type="CHAR" /> <BIRTHSTATE type="CHAR" /> <DT\_OF\_DEATH type="DATE" /> </SCC\_CM\_PERSON\_I> <SCC\_PER\_ADDR\_I class="R"> <EMPLID type="CHAR" /> <ADDRESS\_TYPE type="CHAR" /> <EFFDT type="DATE" /> <EFF\_STATUS type="CHAR" /> <COUNTRY type="CHAR" /> <ADDRESS1 type="CHAR" /> <ADDRESS2 type="CHAR" /> <ADDRESS3 type="CHAR" /> <ADDRESS4 type="CHAR" /> <CITY type="CHAR" /> <NUM1 type="CHAR" /> <NUM2 type="CHAR" /> <HOUSE\_TYPE type="CHAR" /> <ADDR\_FIELD1 type="CHAR" /> <ADDR\_FIELD2 type="CHAR" /> <ADDR\_FIELD3 type="CHAR" /> <COUNTY type="CHAR" /> <STATE type="CHAR" /> <POSTAL type="CHAR" /> <GEO\_CODE type="CHAR" /> <IN\_CITY\_LIMIT type="CHAR" /> <ADDRESS1\_AC type="CHAR" /> <ADDRESS2\_AC type="CHAR" /> <ADDRESS3\_AC type="CHAR" /> <CITY\_AC type="CHAR" /> <REG\_REGION type="CHAR" /> </SCC\_PER\_ADDR\_I> <SCC\_PER\_NAME\_I2 class="R"> <EMPLID type="CHAR" /> <NAME\_TYPE type="CHAR" /> <EFFDT type="DATE" /> <EFF\_STATUS type="CHAR" /> <COUNTRY\_NM\_FORMAT type="CHAR" /> <NAME type="CHAR" /> <NAME\_INITIALS type="CHAR" /> <NAME\_PREFIX type="CHAR" />

<NAME\_SUFFIX type="CHAR" /> <NAME\_ROYAL\_PREFIX type="CHAR" /> <NAME\_ROYAL\_SUFFIX type="CHAR" /> <NAME\_TITLE type="CHAR" /> <LAST\_NAME\_SRCH type="CHAR" /> <FIRST\_NAME\_SRCH type="CHAR" /> <LAST\_NAME type="CHAR" /> <FIRST\_NAME type="CHAR" /> <MIDDLE\_NAME type="CHAR" /> <SECOND\_LAST\_NAME type="CHAR" /> <SECOND\_LAST\_SRCH type="CHAR" /> <NAME\_AC type="CHAR" /> <PREF\_FIRST\_NAME type="CHAR" /> <PARTNER\_LAST\_NAME type="CHAR" /> <PARTNER\_ROY\_PREFIX type="CHAR" /> <LAST\_NAME\_PREF\_NLD type="CHAR" /> <NAME\_DISPLAY type="CHAR" /> <NAME\_FORMAL type="CHAR" /> <NAME\_DISPLAY\_SRCH type="CHAR" /> </SCC\_PER\_NAME\_I2> <NAME\_TYPE\_VW2 class="R"> <EMPLID type="CHAR" /> <NAME\_TYPE type="CHAR" /> <ORDER\_BY\_SEQ type="NUMBER" /> </NAME\_TYPE\_VW2> <ADDRESS\_TYPE\_V2 class="R"> <EMPLID type="CHAR" /> <ADDRESS\_TYPE type="CHAR" /> <ORDER\_BY\_SEQ type="NUMBER" /> </ADDRESS\_TYPE\_V2> <SCC\_PER\_PDE\_I class="R"> <EMPLID type="CHAR" /> <EFFDT type="DATE" /> <MAR\_STATUS type="CHAR" /> <MAR\_STATUS\_DT type="DATE" /> <SEX type="CHAR" /> <highest\_educ\_LVL type="CHAR" /> <FT\_STUDENT type="CHAR" /> <LANG\_CD type="CHAR" /> <ALTER\_EMPLID type="CHAR" /> </SCC\_PER\_PDE\_I> <SCC\_PER\_NID\_I class="R"> <EMPLID type="CHAR" /> <COUNTRY type="CHAR" /> <NATIONAL\_ID\_TYPE type="CHAR" /> <NATIONAL\_ID type="CHAR" /> <SSN\_KEY\_FRA type="CHAR" /> <PRIMARY\_NID type="CHAR" /> <TAX\_REF\_ID\_SGP type="CHAR" /> </SCC\_PER\_NID\_I> <SCC\_PER\_PHONE\_I class="R"> <EMPLID type="CHAR" /> <PHONE\_TYPE type="CHAR" /> <COUNTRY\_CODE type="CHAR" /> <PHONE type="CHAR" /> <EXTENSION type="CHAR" /> <PREF\_PHONE\_FLAG type="CHAR" /> </SCC\_PER\_PHONE\_I> <SCC\_PER\_EMAIL\_I class="R"> <EMPLID type="CHAR" /> <E\_ADDR\_TYPE type="CHAR" />



```
<EMAIL_ADDR type="CHAR" />
      <PREF_EMAIL_FLAG type="CHAR" />
    </SCC_PER_EMAIL_I>
    <PERSON_SA class="R">
      <EMPLID type="CHAR" />
      <VA_BENEFIT type="CHAR" />
      <CAMPUS_ID type="CHAR" />
      <DEATH_CERTIF_NBR type="CHAR" />
      <FERPA type="CHAR" />
      <PLACE_OF_DEATH type="CHAR" />
    </PERSON_SA>
    <SCC_AFL_PERSON class="R">
      <EMPLID type="CHAR" />
     <INSTITUTION type="CHAR" />
     <SCC_AFL_CODE type="CHAR" />
     <START_DT type="DATE" />
      <SCC_AFL_SPONS_DEPT type="CHAR" />
      <END_DT type="DATE" />
     <LASTUPDOPRID type="CHAR" />
     <LASTUPDDTTM type="DATETIME" />
      <SCC_AFL_PLCD_MTD type="CHAR" />
      <SCC_AFL_RLCD_MTD type="CHAR" />
      <SCC_AFL_STATUS type="CHAR" />
     <SCC_AFL_STS_DESCR type="CHAR" />
     <SCC_AFL_RANK type="CHAR" />
    </SCC_AFL_PERSON>
    <PSCAMA class="R">
      <LANGUAGE_CD type="CHAR" />
      <AUDIT_ACTN type="CHAR" />
      <BASE_LANGUAGE_CD type="CHAR" />
      <MSG_SEQ_FLG type="CHAR" />
      <PROCESS_INSTANCE type="NUMBER" />
      <PUBLISH_RULE_ID type="CHAR" />
      <MSGNODENAME type="CHAR" />
   </PSCAMA>
  </FieldTypes>
</SCC_CONSTITUENT_FULLSYNC>
```



## D Authorization Policy

You can define and manage authorization policies in the Authorization Policies section of the Oracle Identity Administration. This section is available to users who have the Manage Authorization Policies privilege.

The following are the structural components of an authorization policy:

- Identifying details: Each authorization policy must have a name and description.
- Oracle Identity Manager feature: Each authorization policy is defined for a specific feature in Oracle Identity Manager. Features are well-defined components in Oracle Identity Manager such as user management and role management. The authorization requirements of multiple features cannot be covered by a single authorization policy.
- **Assignee**: This is the role or roles that a policy grants privileges to. You can grant privileges to one or more roles for each policy. All members of the role (direct or indirect through inheritance) are granted the privileges by the authorization policy. For the user management feature, a rule based on the manager relationship is supported. Here, all the users that are in the management chain of the user being acted on are the assignees of the authorization policy.

#### Note:

For information about inheritance of role membership, see Managing Roles in *Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager.* 

Assignee can include additional conditions that must be fulfilled by the assignee. This is a way of making the authorization policy context aware. For example, for the user management feature, a condition can state that for the assignee to have the privileges, the assignee must be a member of the same organization listed in the data security.

• **Privileges**: These are the privileges that the assignees are granted. The list of privileges is defined by the feature for which this policy is being defined. For example, the user management feature defines privileges such as Search for Users, View User Detail, and Modify User Profile. For a complete list of privileges for the user management feature.

Some privileges also support fine-grained attribute-level controls that define which specific entity attributes of the feature are further granted to the assignee. For instance, for the View User Detail privilege, the policy can further define which of the attributes on the user entity can be viewed by the assignee at run time. Not all privileges support attribute-level details. For example, the Delete User privilege does not require or support any attribute-level details.

• **Data security**: These are the entities managed by the feature over which a privilege is granted to the assignee. This section is optional based on whether

or not the feature for which the authorization policy is being defined supports data security. The data security is expressed in the form of an entity selection criteria or a search criteria that is used to determine the entities over which the privilege is granted. The data security can also be a list of specific entities. The data security capabilities depend on the feature. For instance, the criteria can specify that the assignee is granted privileges over the users belonging to a list of organizations. This criteria can provide additional security settings that apply to the data security. For example, in the user management feature, an instruction can be that the organization condition applies down the hierarchy so that users in the specified organization and all child organizations are in scope for this data security policy.