Oracle® Identity Manager

Connector Guide for PeopleSoft Campus

11.1.1
E36940-11
July 2020

Oracle Identity Manager Connector Guide for PeopleSoft Campus, 11.1.1

E36940-11

Primary Author: Gowri.G.R

Contributing Authors: Alankrita Prakash

Contents

3 Using the Connector

4 Extending the Functionality of the Connector

List of Figures

List of Tables

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 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

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

http://docs.oracle.com/cd/E52734_01/index.html

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

http://docs.oracle.com/cd/E22999_01/index.htm

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:

1.1 Certified Components

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

Table 1-1 Certified Components

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

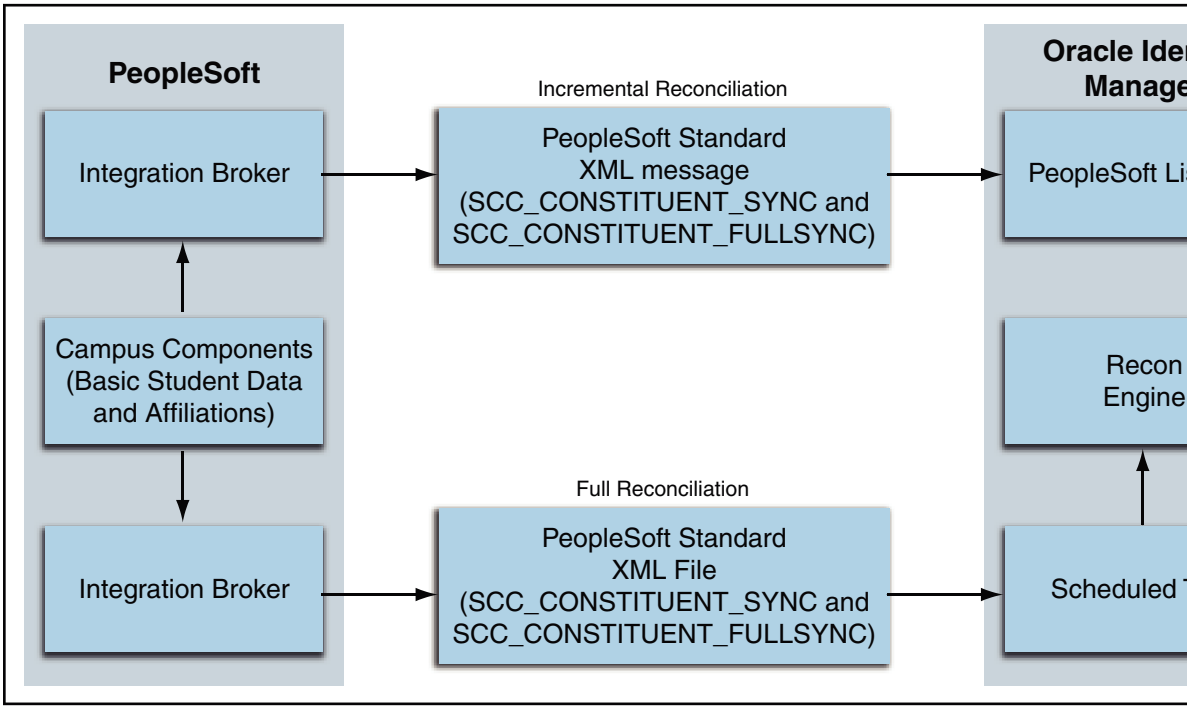
Table 1-1 (Cont.) Certified Components

Item	Requirement
Target systems	The target system can be any one of the following: • PeopleSoft Campus Solutions Maintenance Pack 9.0 Bundle 27 with PeopleTools 8.50 • PeopleSoft Campus Solutions Maintenance Pack 9.0 with PeopleTools 8.51 • PeopleSoft Campus Solutions Maintenance Pack 9.0 with PeopleTools 8.52 • PeopleSoft Campus Solutions Maintenance Pack 9.0 with PeopleTools 8.53 • PeopleSoft Campus Solutions Maintenance Pack 9.2 with PeopleTools 8.54 • PeopleSoft Campus Solutions Maintenance Pack 9.2 with PeopleTools 8.55 • PeopleSoft Campus Solutions Maintenance Pack 9.2 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: • Tuxedo and Jolt (the application server) • PeopleSoft Internet Architecture • PeopleSoft Application Designer (2-tier mode) The following standard PeopleSoft messages are available: • SCC_CONSITTUENT_SYNC • SCC_CONSTITUENT_FULLSYNC

1.2 Connector Architecture

Figure 1-1 shows the architecture of the connector.

Figure 1-1 Architecture of the Connector

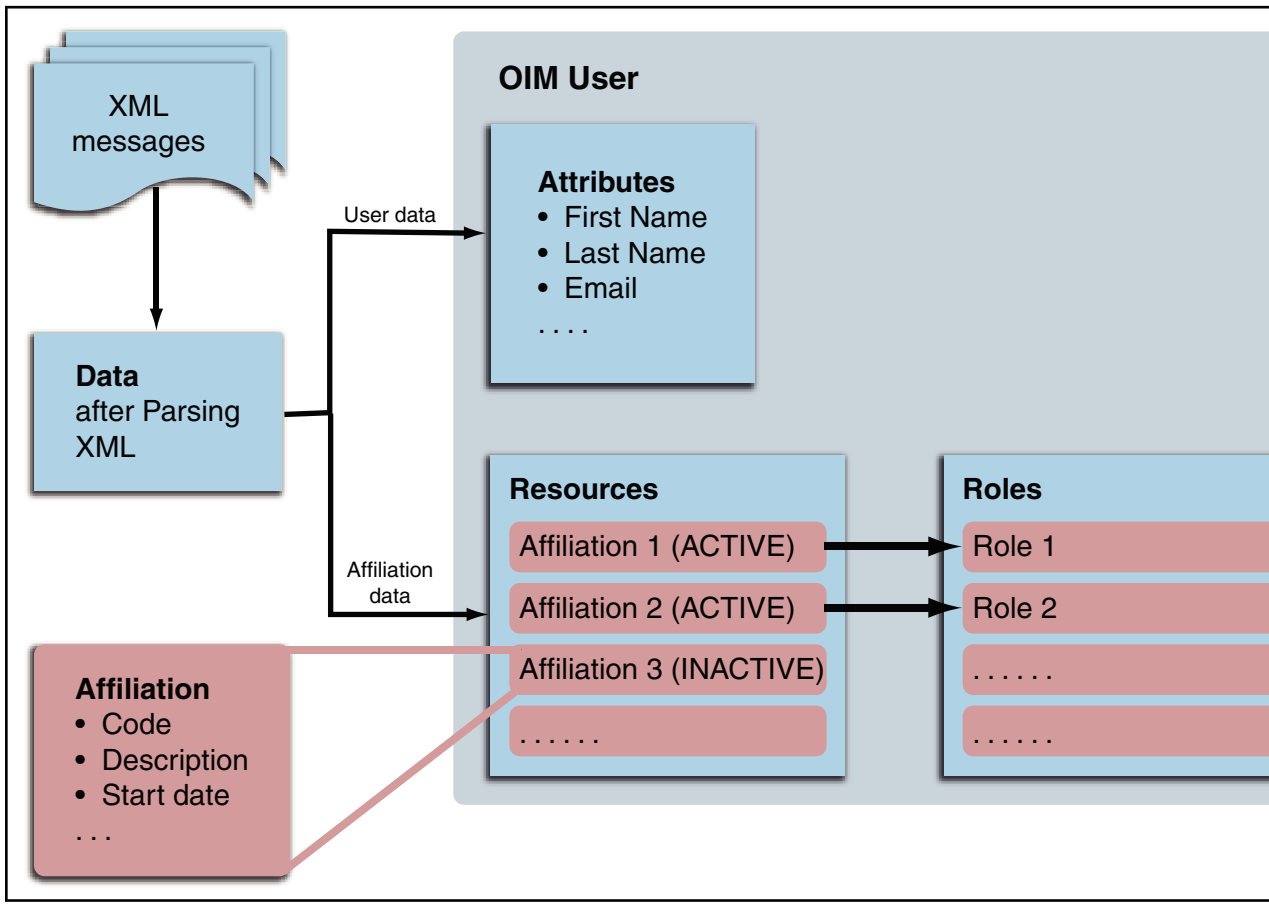


The target system is configured as a trusted source of identity data for Oracle Identity Manager. In other words, identity data that is created and updated on the target system is fetched into Oracle Identity Manager and used to create and update OIM Users.

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

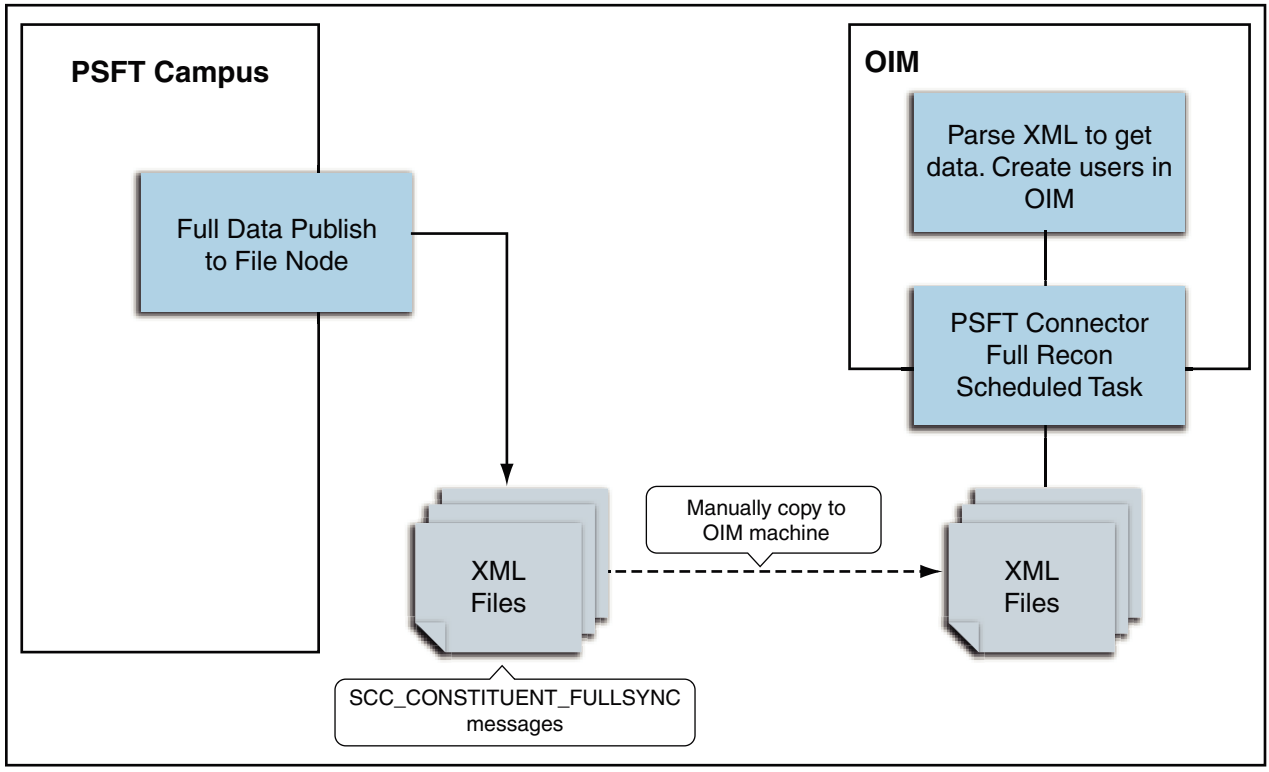
1.3.1 Full Reconciliation

> **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.

Figure 1-3 Full Reconciliation



Full reconciliation involves the following steps:

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

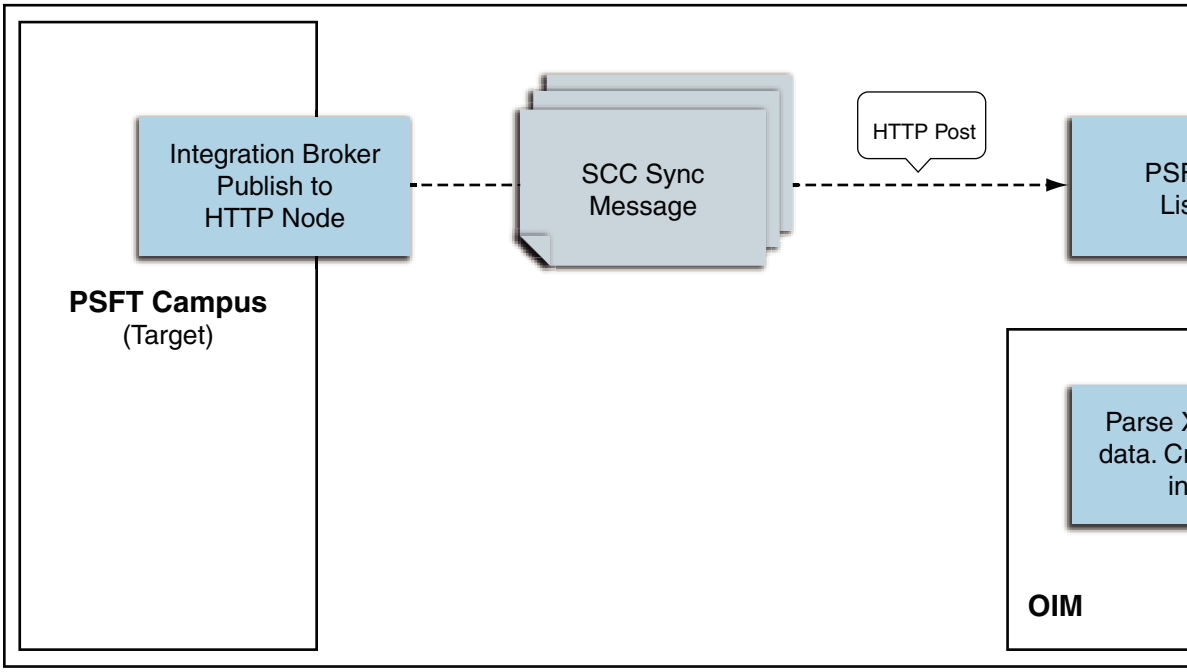
1. The PeopleSoft Integration Broker populates the XML files for the SCC_CONSTITUENT_FULLSYNC messages with all the person data, such as biographical information and student information.
2. Copy these XML files to a directory on the Oracle Identity Manager host computer.
3. Configure the PeopleSoft Campus 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.
2. 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

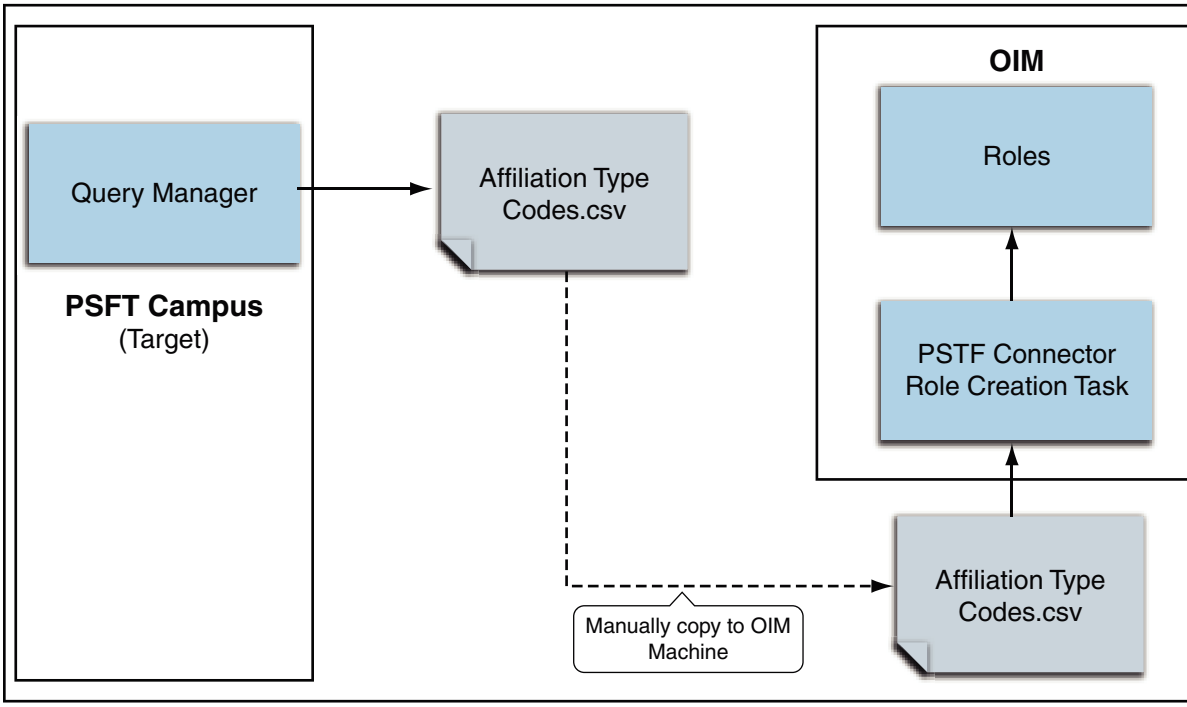
The connector provides all the features required for setting up PeopleSoft Campus as a trusted (authoritative) source of identity data for Oracle Identity Manager. Oracle Identity Manager uses this message for incremental reconciliation. In other words, the connector does not support provisioning operations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

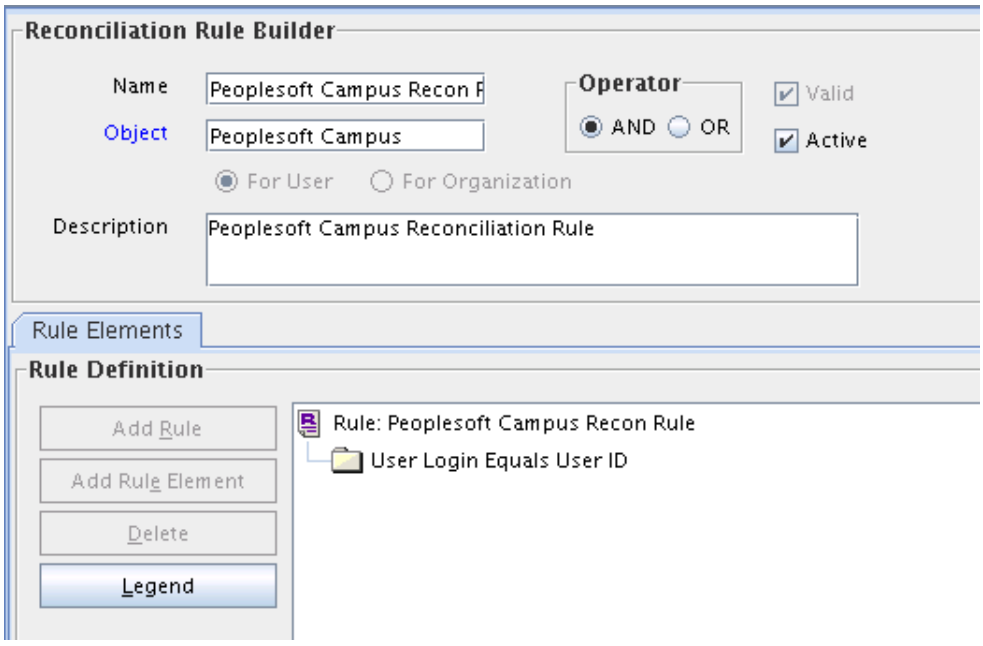
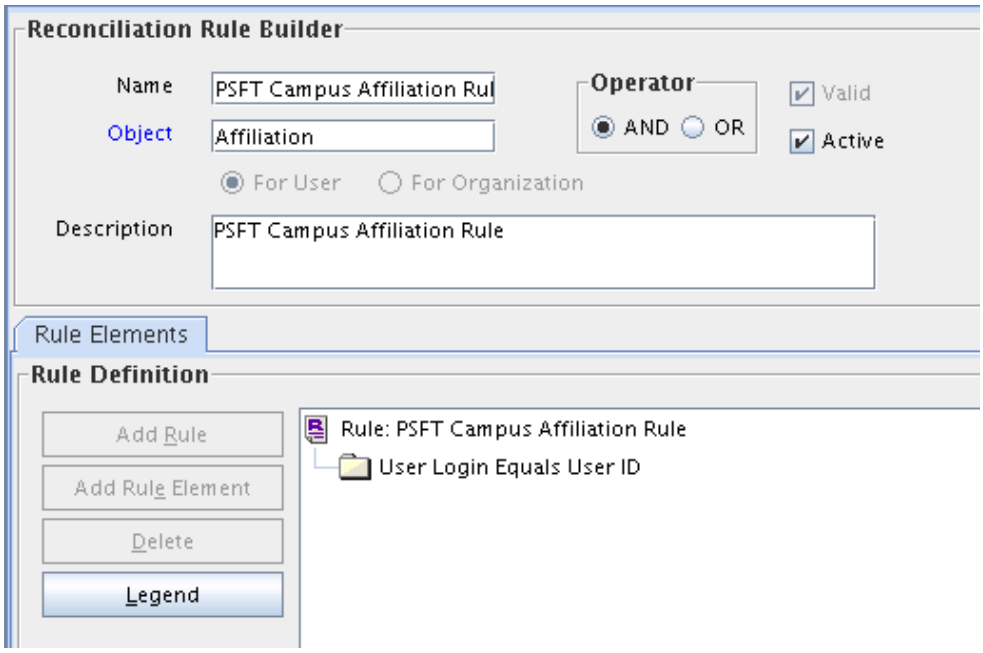


Figure 1-7 Affiliation Reconciliation Rule



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

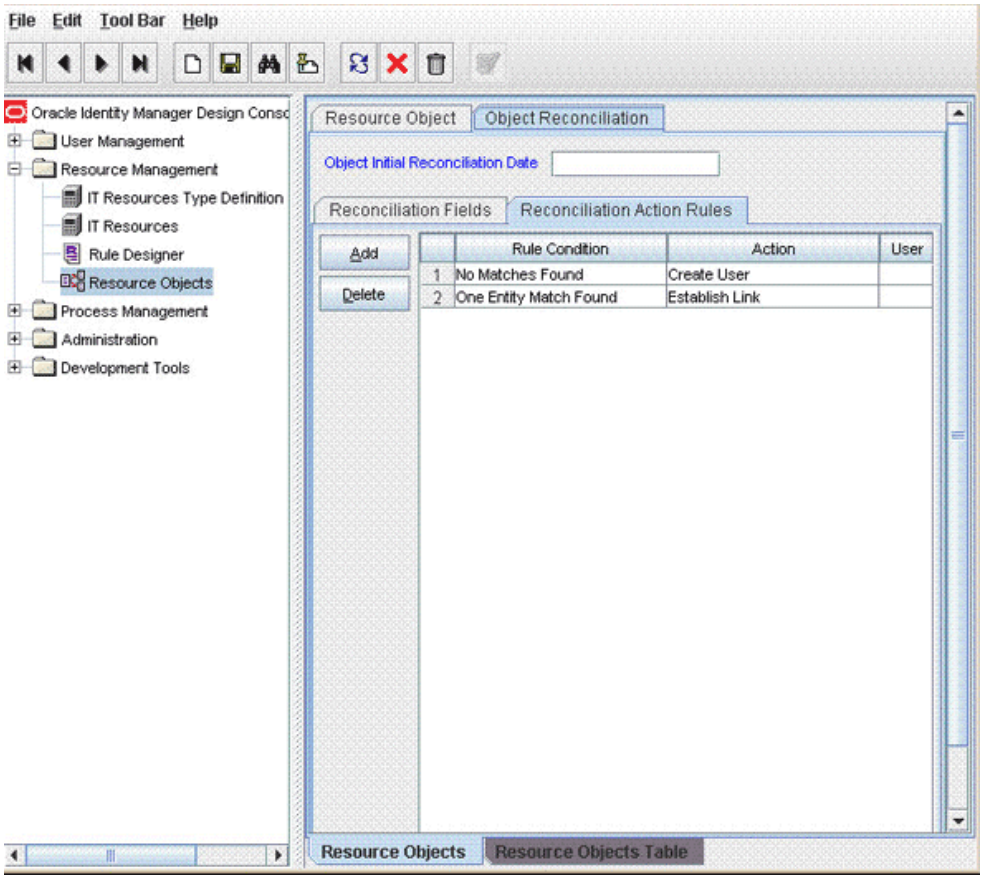
1.5.2.2 Viewing the Reconciliation Action Rules in the Design Console

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.
5. Click the **Object Reconciliation** tab and then the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1-8 shows these reconciliation action rules.

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.ExclusionList	Name of the Resource Exclusion lookup for PeopleSoft Campus See Lookup.PSFT.Campus.ExclusionList 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_FULLSYNC	Lookup.PSFT.Message.SccConstituentFullSync.Configuration	Name of the lookup definition for SCC_CONSTITUENT_FULLSYNC message See Lookup.PSFT.Message.SccConstituentFullSync.Configuration for more information about this lookup definition.
SCC_CONSTITUENT_SYNC.v1	Lookup.PSFT.Message.SccConstituentSync.Configuration	Name of the lookup definition for SCC_CONSTITUENT_SYNC message See Lookup.PSFT.Message.SccConstituentSync.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 *not* 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.SccConstituentFullSync.AttributeMapping	Name of the lookup definition that maps Oracle Identity Manager attributes with the attributes in the SCC_CONSTITUENT_FULLSYNC message XML See Lookup.PSFT.Campus.SccConstituentFullSync.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.CustomQuery	This entry holds the name of the lookup definition that maps resource object fields with OIM User form fields. This lookup definition is used during application of the custom query. See Limited Reconciliation for more information.
Data Node Name	Transaction	Name of the node in the XML files to 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 **Note:** 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.common.handler.impl.PSFTCampusSyncReconMessageHandlerImpl	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.common.parser.impl.CampusMessageParser	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.SccConstituentSync.Recon	Name of the lookup definition that maps Oracle Identity Manager attributes with the Resource Object attributes See Lookup.PSFT.Campus.SccConstituentSync.Recon for more information about this lookup definition.
Resource Object	PeopleSoft Campus	Name of the resource object
Transformation Lookup Definition	Lookup.PSFT.Campus.SccConstituentSync.Transformation	Name of the transformation lookup definition See Configuring Transformation of Data During Reconciliation for more information about adding entries in this lookup definition. **Note:** The default value for transformation lookups for both SCC_CONSTITUENT_SYNC and SCC_CONSTITUENT_FULLSYNC 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_FULLSYNC 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.SccConstituentSync.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_FULLSYNC 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~RESOURCE=Affiliations
Affiliation End Date	END_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations
Affiliation Start Date	START_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations

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=Affiliations
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.

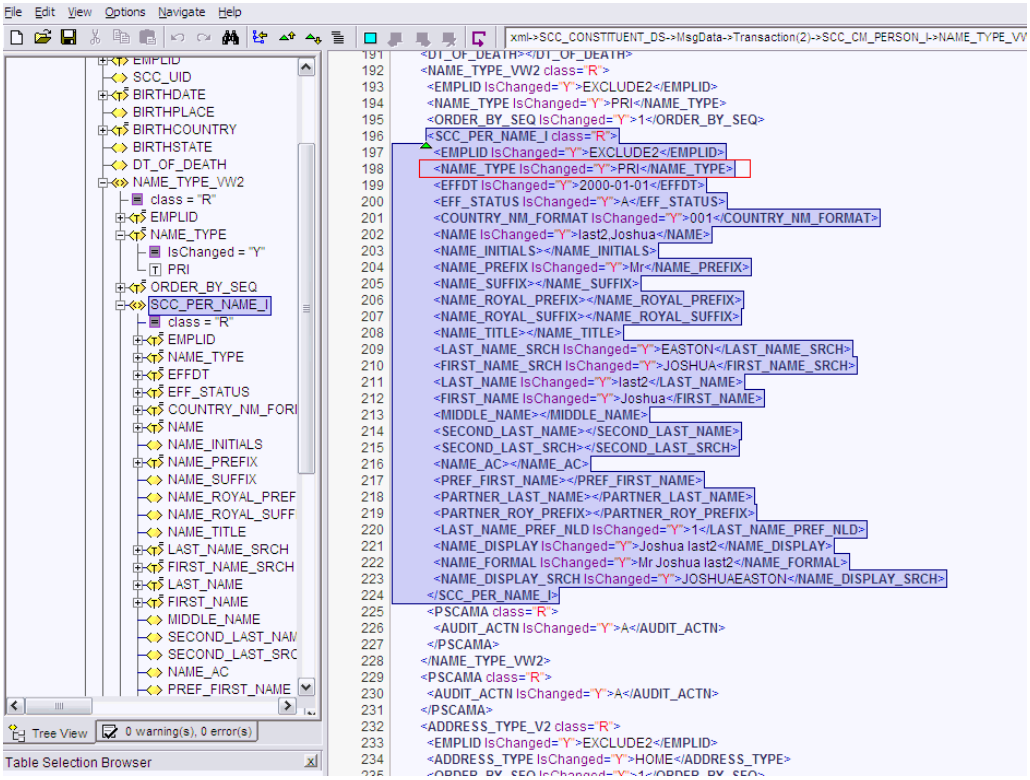
For example, in the SCC_CONSTITUENT_SYNC message, the rowset NAME_TYPE_VW lists the names assigned to a person. The names assigned could be primary, secondary, or nickname, depending on how it is configured in PeopleSoft.

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:

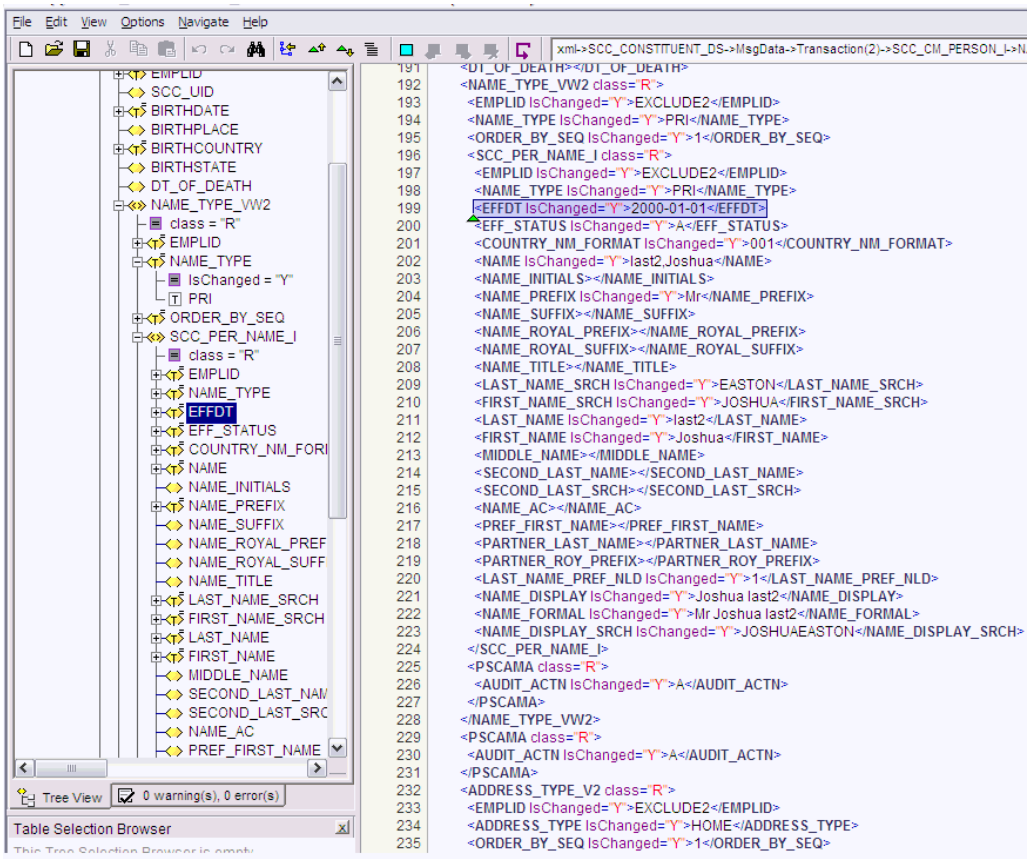


`EFFECTIVE DATED NODE`: Effective-dated node for the `NODE`, if any.

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

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

The EFFDT node is shown in the following screenshot:

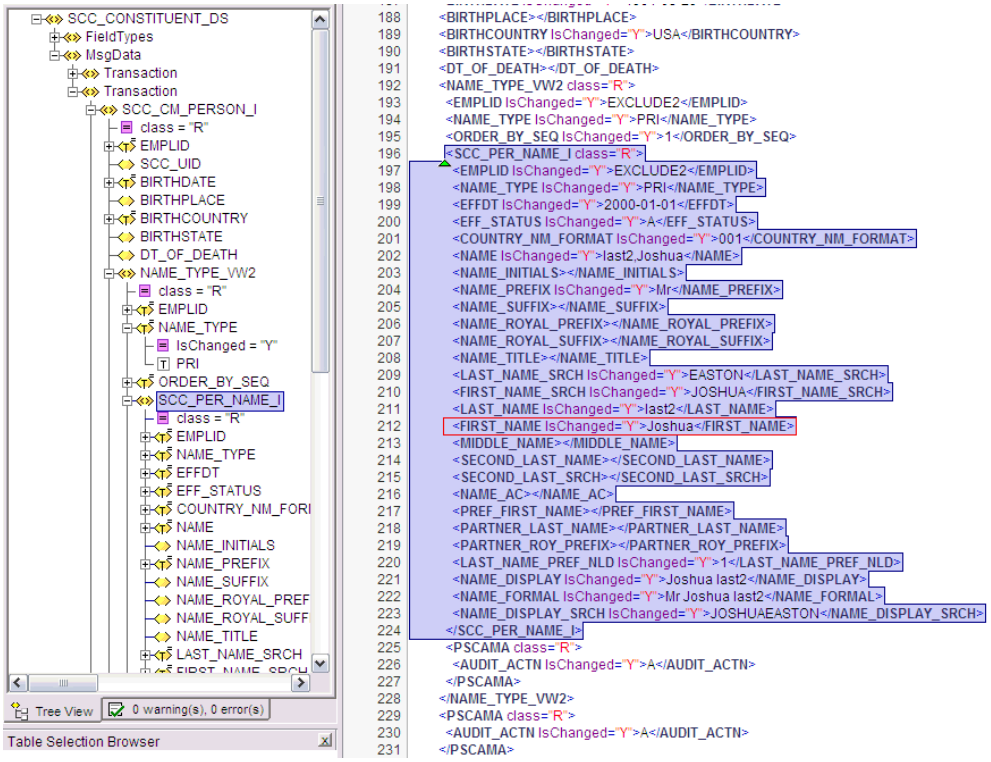


`Primary or RESOURCE=Resource Name:` Specifies if the node is a mandatory field or a resource field. For example, in case of a resource field, RESOURCE=Affiliations specifies that it is a field in the Affiliations resource object.

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.SccConstituentSync.AttributeMapping	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.CustomQuery	This entry holds the name of the lookup definition that maps resource object fields with OIM User form fields. This lookup definition is used during application of the custom query. See Limited Reconciliation for more information.
Data Node Name	Transaction	Name of the node in the XML files to run a transaction
Employee Status	Enabled	Default status of an employee during the creation of an OIM User **Note:** You can change the status to Disabled, if you want the status to be Inactive when the OIM User is created.
Message Handler Class	oracle.iam.connectors.psft.common.handler.impl.PSFTCampusSyncReconMessageHandlerImpl	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.common.parser.impl.CampusMessageParser	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.SccConstituentSync.Recon	Name of the lookup definition that maps Oracle Identity Manager attribute with Resource Object attribute See Lookup.PSFT.Campus.SccConstituentSync.Recon for more information about this lookup definition.
Resource Object	PeopleSoft Campus	Name of the resource object

Code Key	Decode	Description
Transformation Lookup Definition	Lookup.PSFT.Campus.SccConstituentSync.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_FULLSYNC messages is the same. You can use different lookups by 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_SYNC message.
Use Transformation	No	Enter yes to implement transformation while reconciling records. Otherwise, enter no.
Use Validation	No	Enter yes to implement validation while reconciling records. Otherwise, enter no.
Validation Lookup Definition	Lookup.PSFT.Campus.SccConstituentSync.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_FULLSYNC messages is the same. You can use different lookups by 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=Affiliations
Affiliation Description	SCC_AFL_STS_DESCR~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations
Affiliation End Date	END_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations
Affiliation Start Date	START_DT~SCC_AFL_PERSON~None~None~RESOURCE=Affiliations

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=Affiliations
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~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~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.

Table 2-1 Files and Directories on the Installation Media

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

Table 2-1 (Cont.) 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

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.

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

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

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

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

6. On the People Tools tab, select the **Application Designer Access** check box and click the **Definition Permissions** link. The Definition Permissions page is displayed.
7. On this page, grant full access to the following object types by selecting **Full Access** from the Access list:
   - App Engine Program
   - Message
   - Component
   - Project
   - Application Package
8. Click **OK.**
9. Click the **Tools Permissions** link. The Tools Permissions page is displayed. On this page, grant full access to the SQL Editor tool by selecting **Full Access** from the Access list.
10. Click **OK.** The application returns to the People Tools tab.
11. On the Process tab, click the **Process Group Permissions** link. The Process Group Permission page is displayed.
12. In the Process Group lookup, click the search icon. From the list, select **TLSALL.**
13. On the Process Group Permission page, click the plus sign (+) to add another row for **Process Group.**
14. In the Process Group lookup, click the search icon. From the list, select **STALL.** The application returns to the Process Group Permission page.
15. Click **OK.**
16. On the Web Libraries tab, click the search icon for the Web Library Name field and perform the following:

a. In the Web Library Name lookup, enter `WEBLIB_PORTAL` and then click **Lookup.** From the list, select **WEBLIB_PORTAL.** The application returns to the Web Libraries tab. Click the **Edit** link.

b. On the WebLib Permissions page, click **Full Access(All).**

c. Click **OK** and then click **Save.**

d. Click the plus sign (+) to add a row for the **Web Library Name** field and repeat Steps a through c for the WEBLIB_PT_NAV library.

e. Click **Save** to save all the settings specified for the permission list.

2.1.3.1.2 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-11.1.1.5.0/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`

l. 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` **Note:** You must not change the value of this parameter. However, if you create a copy of all the connector objects, then you can specify the unique name of the copy of this lookup definition as the value of the Configuration Lookup Name parameter in the copy of the IT resource.

Table 2-3 (Cont.) IT Resource Parameters

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`

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
   ```

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

2.2.2.1.1.2 Configuring PeopleSoft Integration Broker

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

To configure PeopleSoft Integration Broker:

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

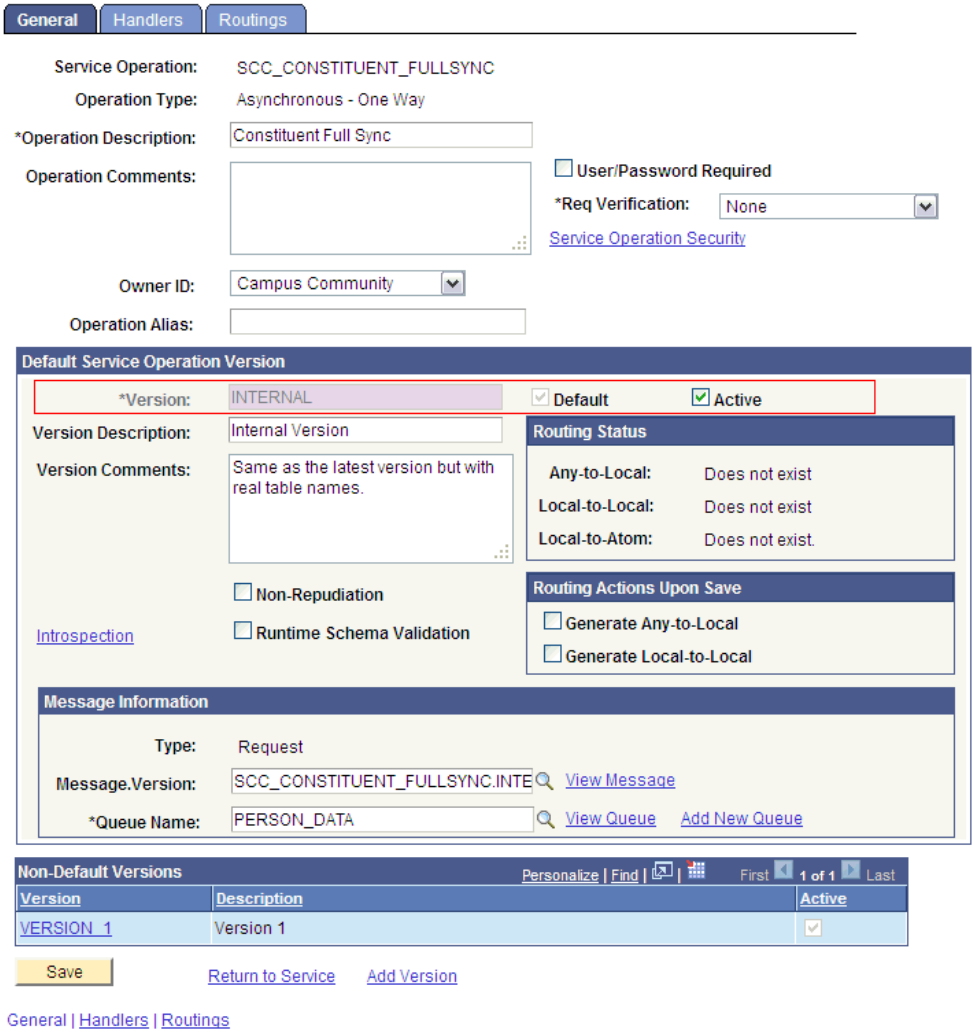
The service operation is a mechanism to trigger, receive, transform, and route messages that provide information about updates in PeopleSoft or an external application. You must activate the service operation to successfully transfer or receive messages.

To activate the SCC_CONSTITUENT_FULLSYNC service operation:

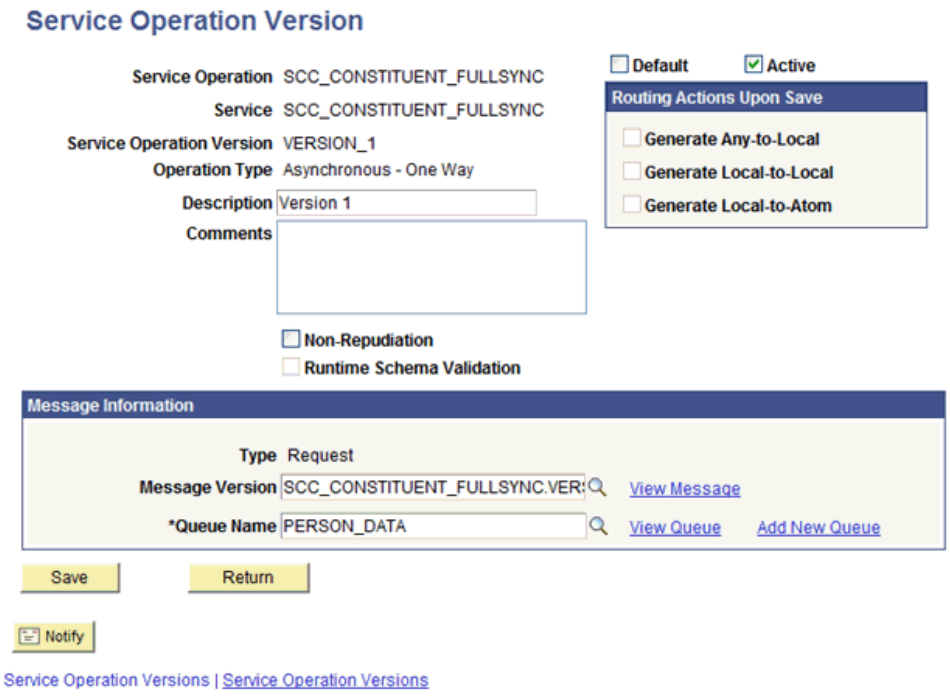
1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
2. On the Find Service Operation tab, enter `SCC_CONSTITUENT_FULLSYNC` in the **Service** field, and then click **Search.**
3. Click the **SCC_CONSTITUENT_FULLSYNC**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



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.



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

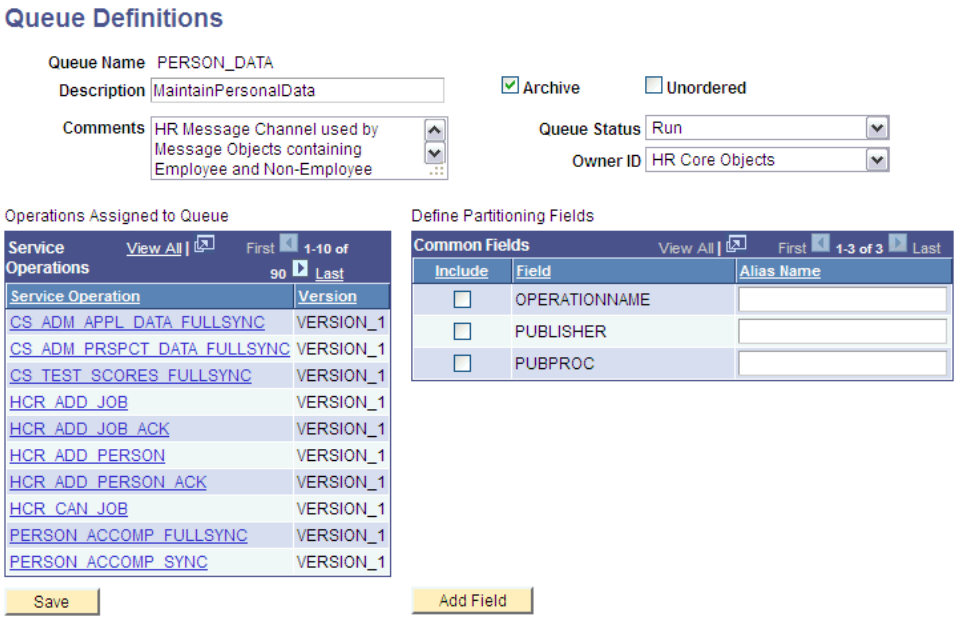
All messages in PeopleSoft are sent through a queue. This is done to ensure that the messages are delivered in a correct sequence. Therefore, you must ensure that the queue is in the Run status.

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.

> **Note:**
>
> If the queue status is not Run:
>
> a. From the Queue Status list, select **Run.**
>
> b. Click **Save.**

The queue status is highlighted in the following screenshot:



4. Click **Return to Search.**

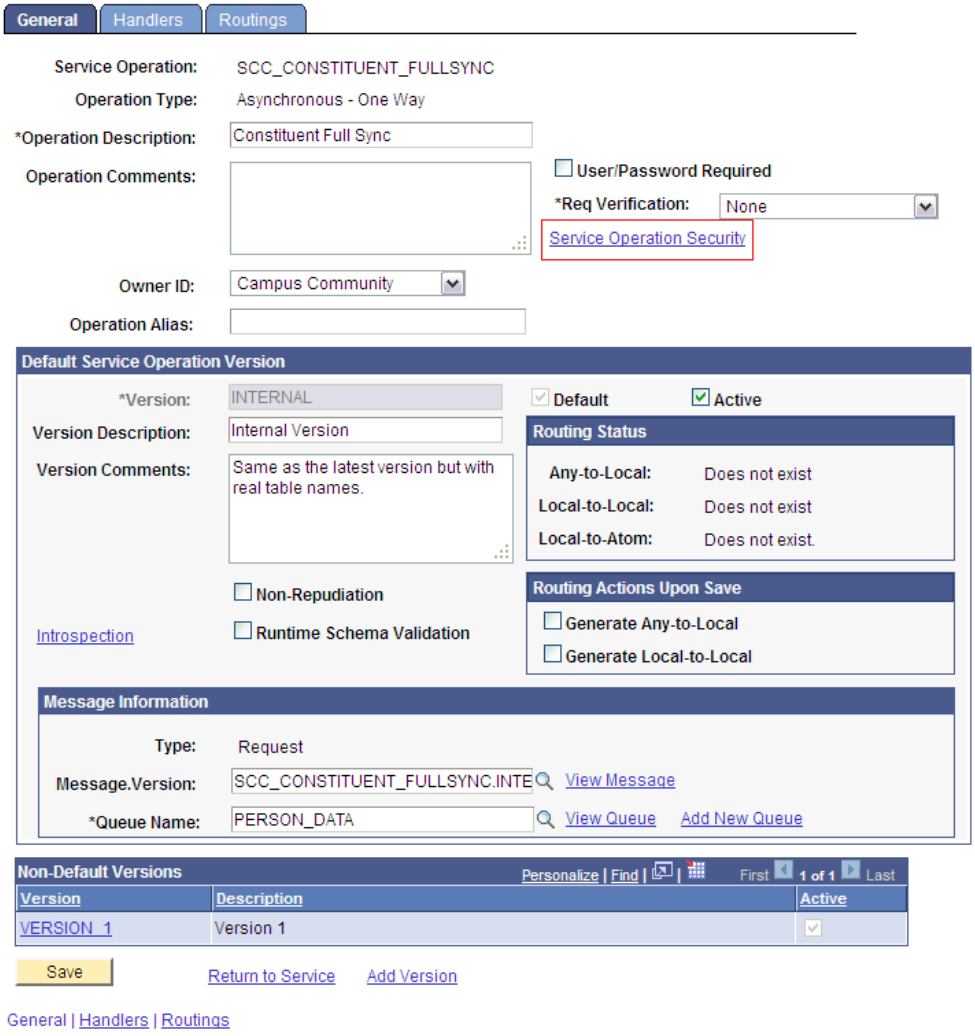
2.2.2.1.2.3 Setting Up the Security for the SCC_CONSTITUENT_FULLSYNC Service Operation

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:



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:

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:

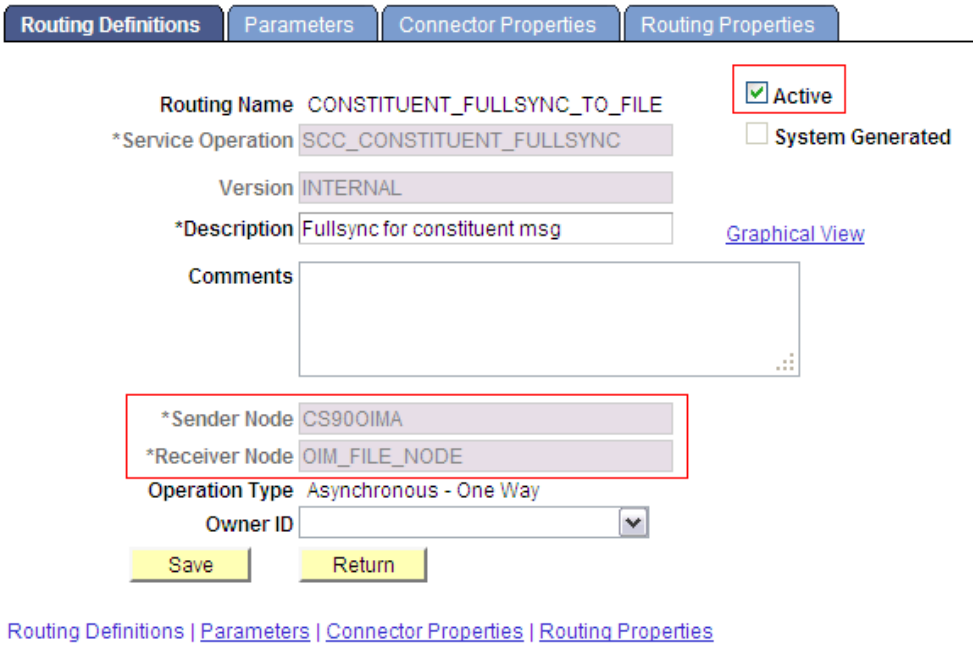
1. On the Routing tab, enter `SCC_CONSTITUENT_FULLSYNC_CS_FILE` as the routing name and then click **Add.**
2. On the Routing Definitions tab, enter the following:

   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:



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:

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

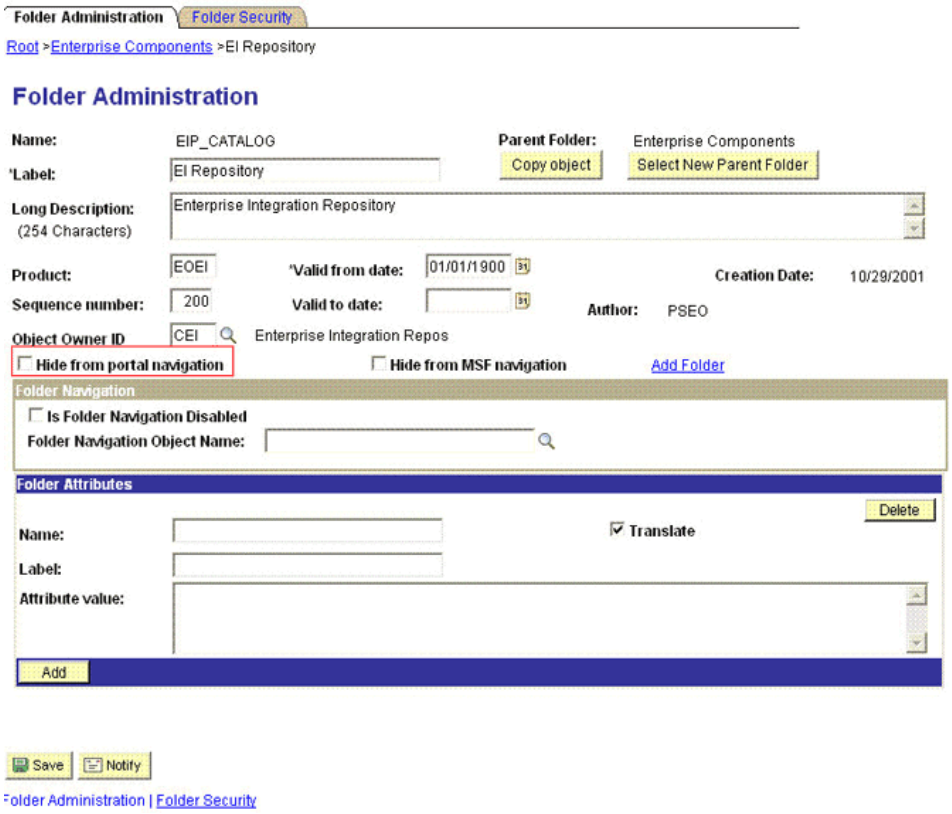
EI Repository is a hidden folder in PeopleSoft. Therefore, you must display this folder.

To display the EI Repository folder:

> **Note:**
>
> Perform this procedure using the PeopleSoft administrator credentials.

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

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



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

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, EI 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:

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:

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

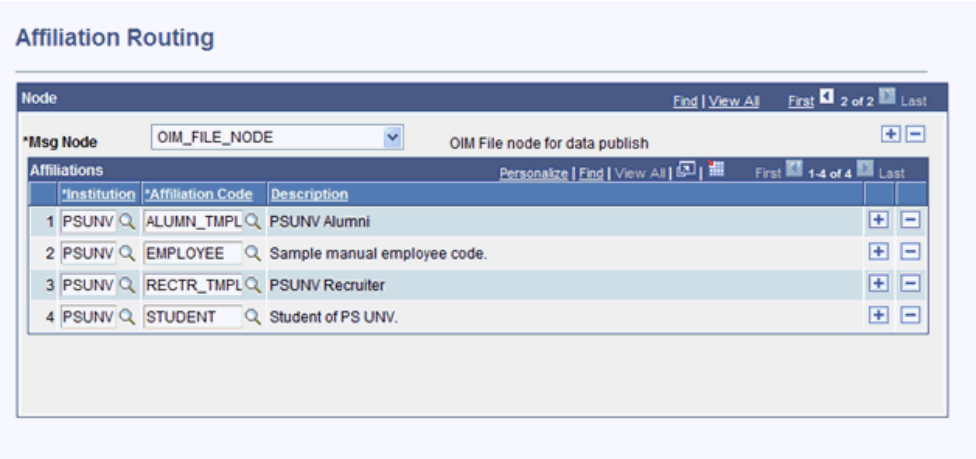
2.2.2.2.1 Setting Affiliation Routing Rules

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.

> **Note:**
>
> Affiliation Codes are defined and set appropriately for persons in the PeopleSoft Campus Solutions target system. See *PeopleSoft Campus Solutions* documentation for more information about defining and using Affiliations.

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.



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.**

2.2.2.2.2 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:

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

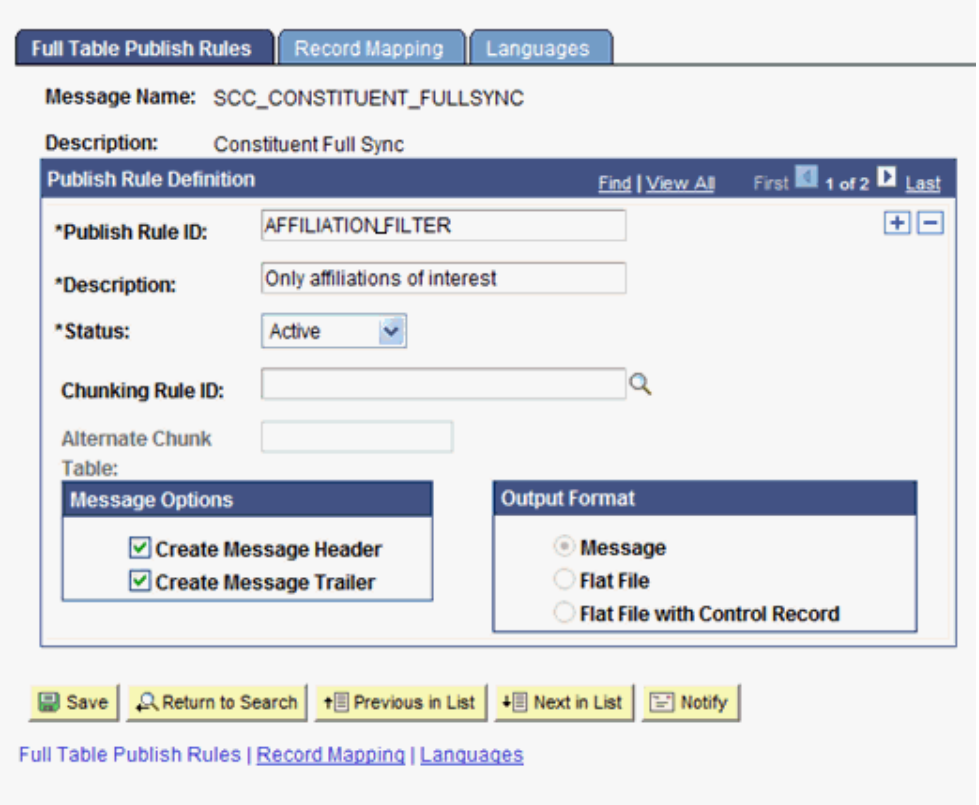
2.2.2.2.3 Activating the Full Data Publish Rule with Content-based Filtering

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.

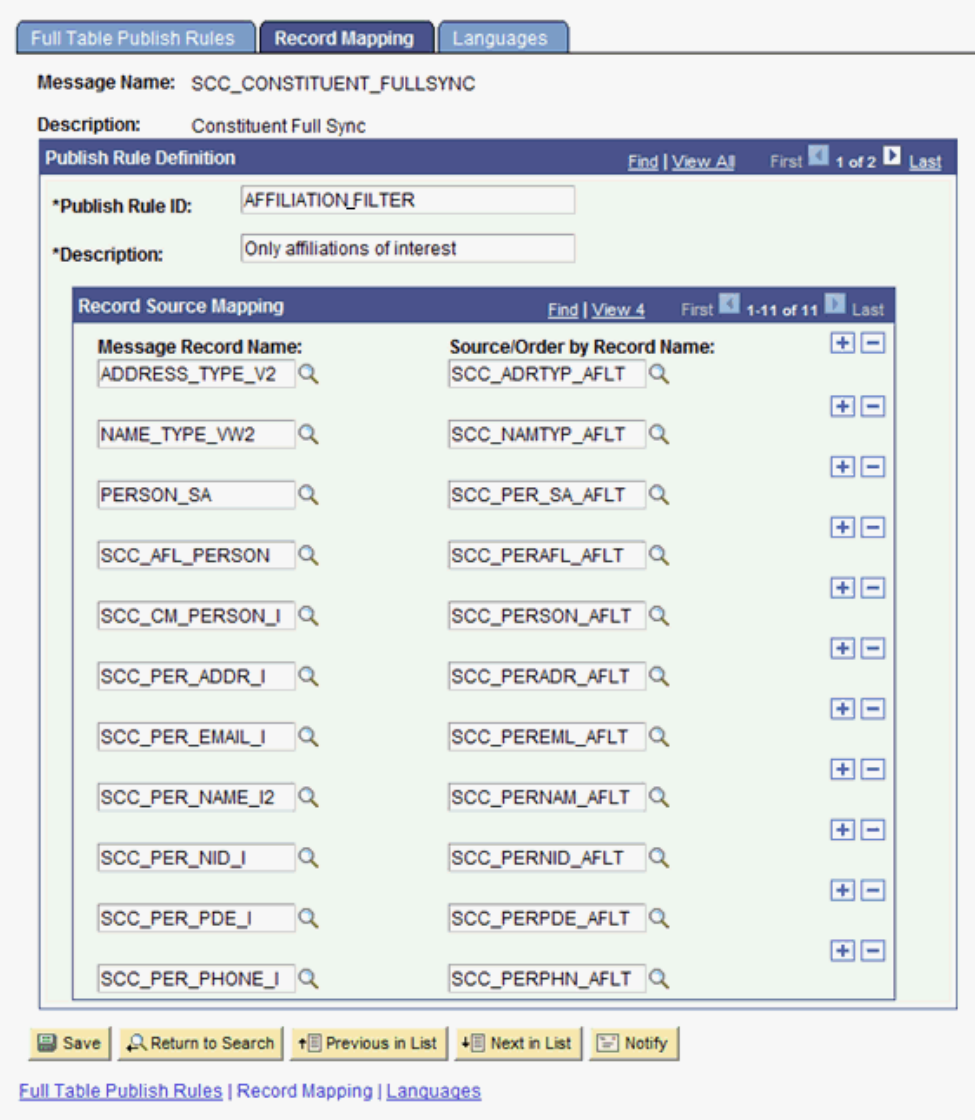
   The following screenshot displays the preceding steps:



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:



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:

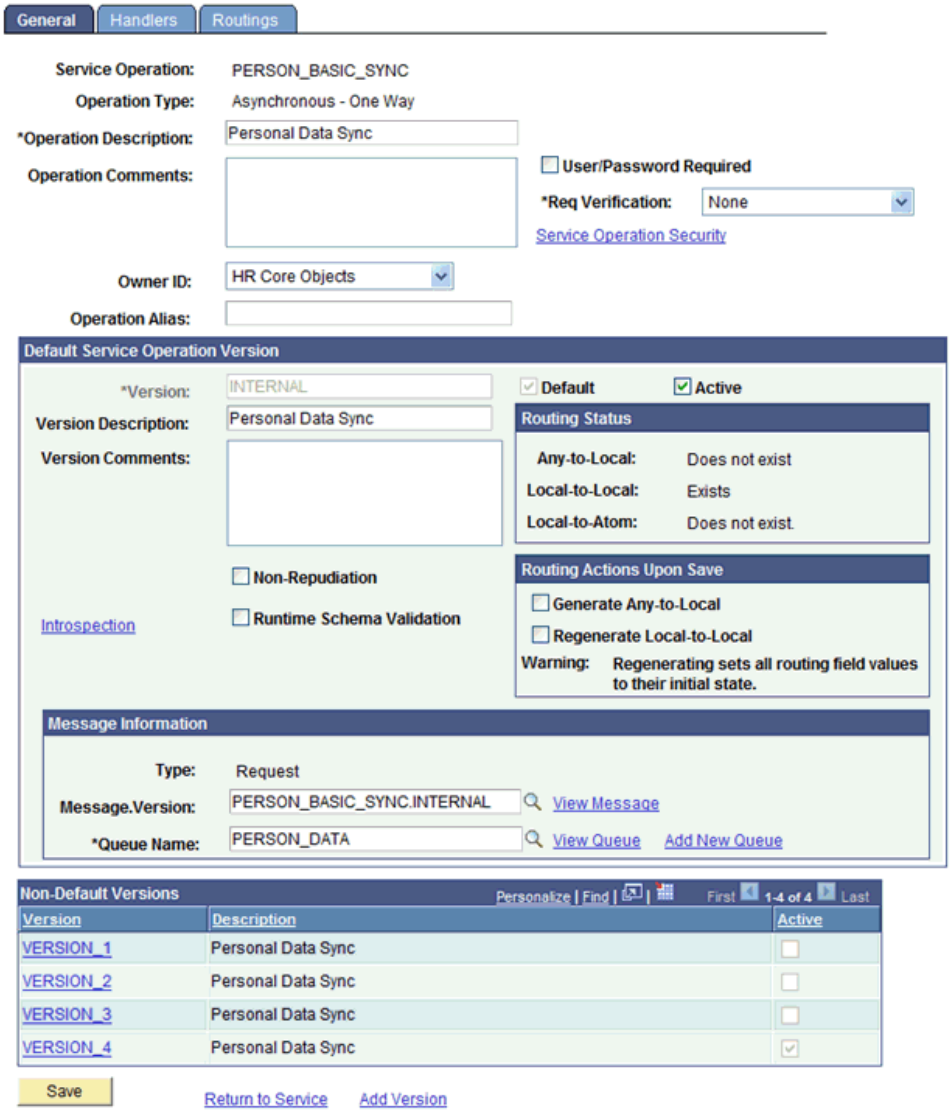
- Activating the PERSON_BASIC_SYNC Service Operation
- Activating the SCC_PERSON_SYNC Service Operation
- Activating the SCC_CONSTITUENT_SYNC Service Operation
- Activating the SSC_CONSTITUENT_SYNC Event
- Activating the PERSON_BASIC_SYNC Notification Handler
- Activating the SCC_PERSON_SYNC Notification 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:

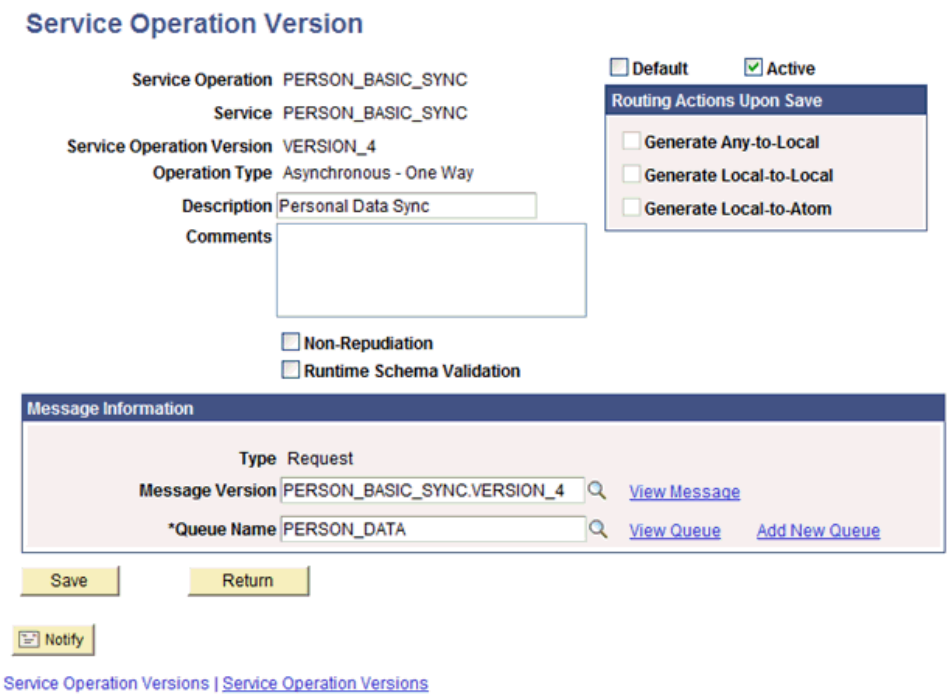
1. In PeopleSoft Internet Architecture, expand **PeopleTools, Integration Broker, Integration Setup,** and then click **Service Operations.**
2. On the Find Service Operation tab, enter `PERSON_BASIC_SYNC` in the **Service** field, and then click **Search.**
3. Click the **PERSON_BASIC_SYNC** link.
4. 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:

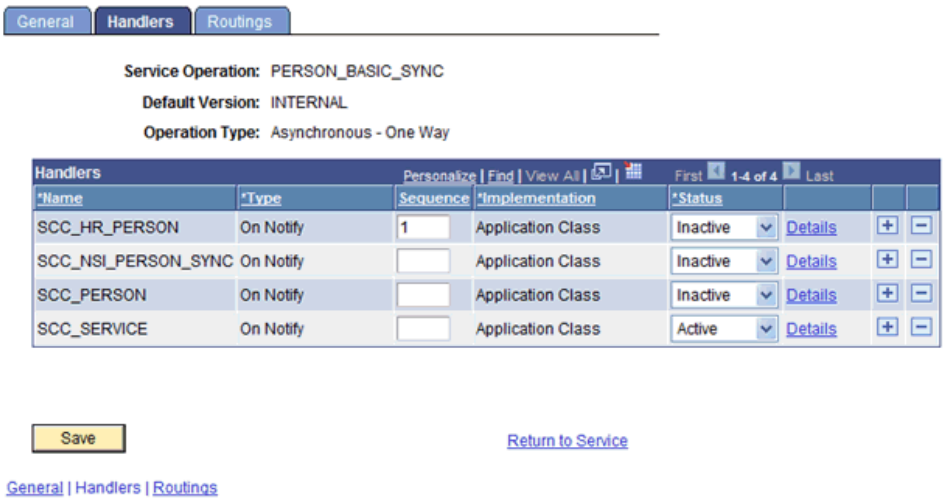


5. In the Non-Default Versions region, click the **VERSION_4** link and click **Active.**

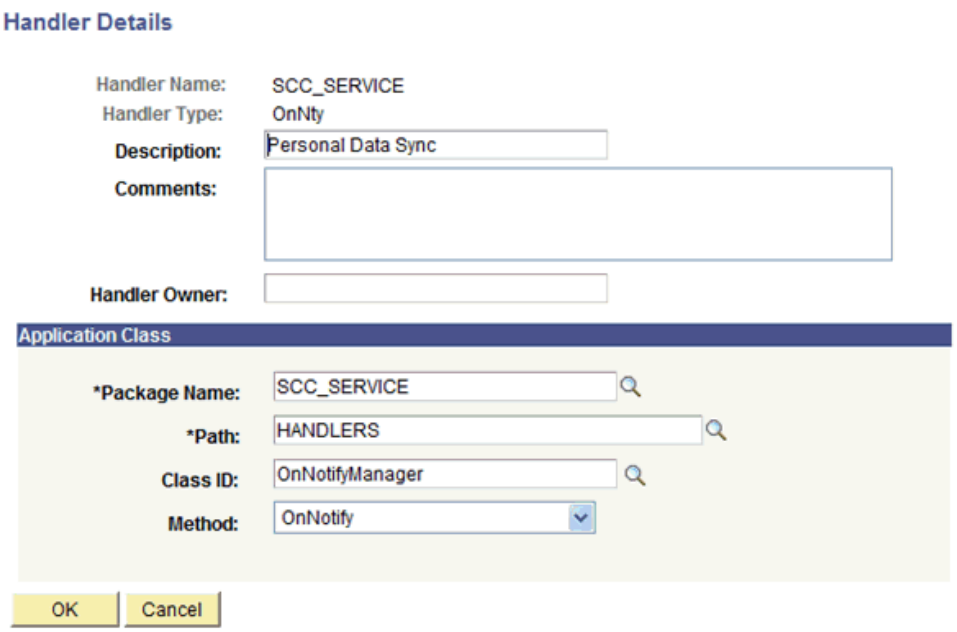
   The following screenshot displays the non-default version of the PERSON_BASIC_SYNC service operation:



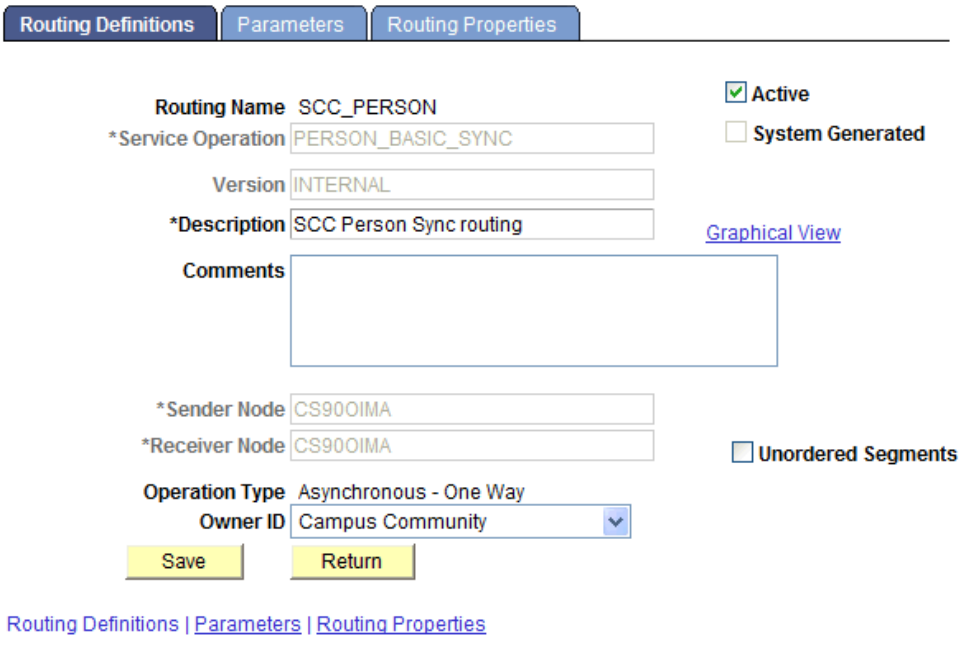
6. Click the **Handlers** tab, as shown in the following screenshot.



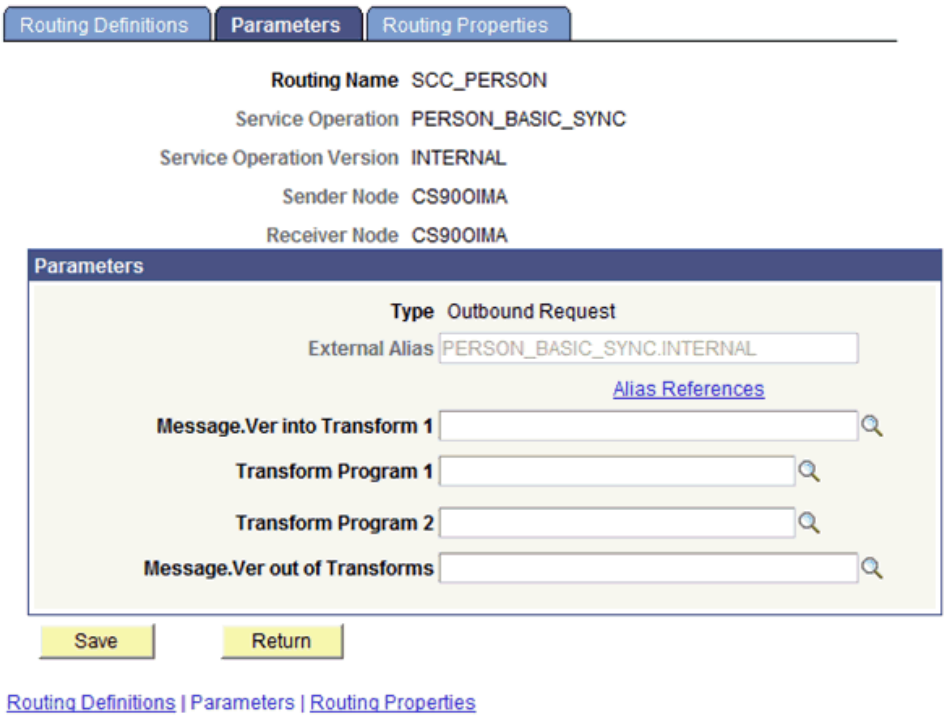
7. Confirm that the **SCC_SERVICE OnNotify Handler** is Active. Click **Details.**
8. Confirm that the values are set as shown in the following screenshot and click **OK.**



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



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



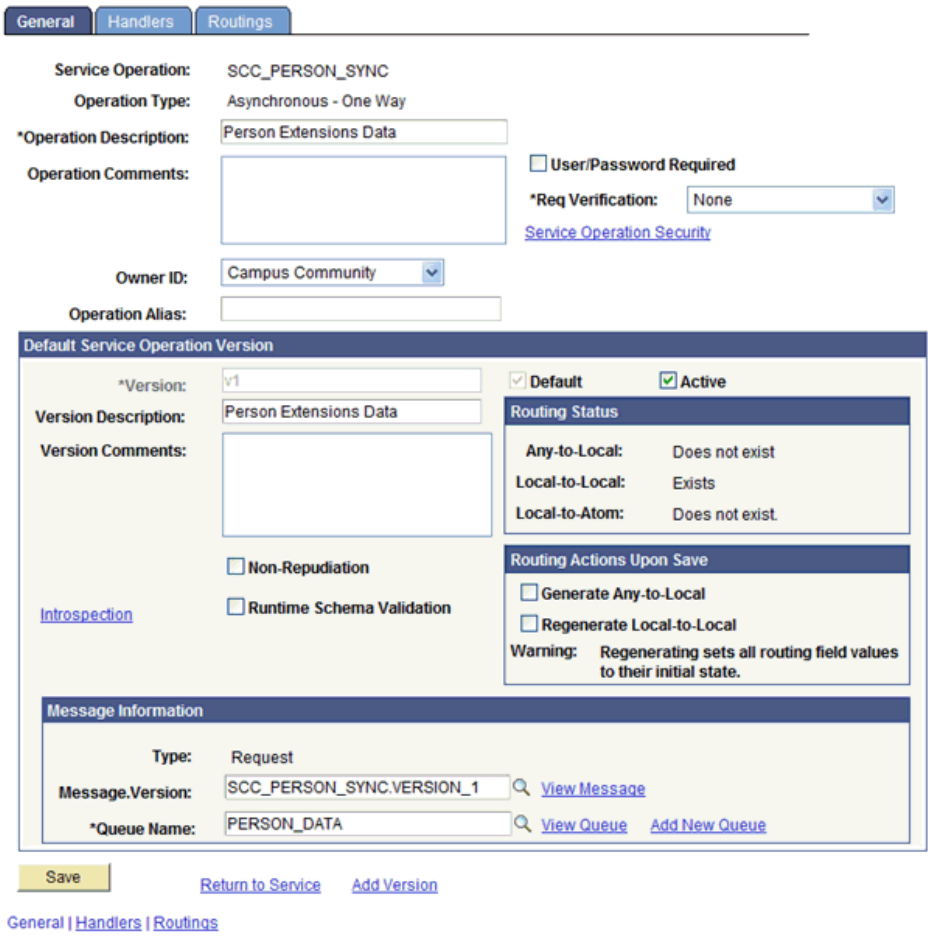
12. Click **Save.**
13. Click **Return.**

2.2.2.3.2.2 Activating the SCC_PERSON_SYNC Service Operation

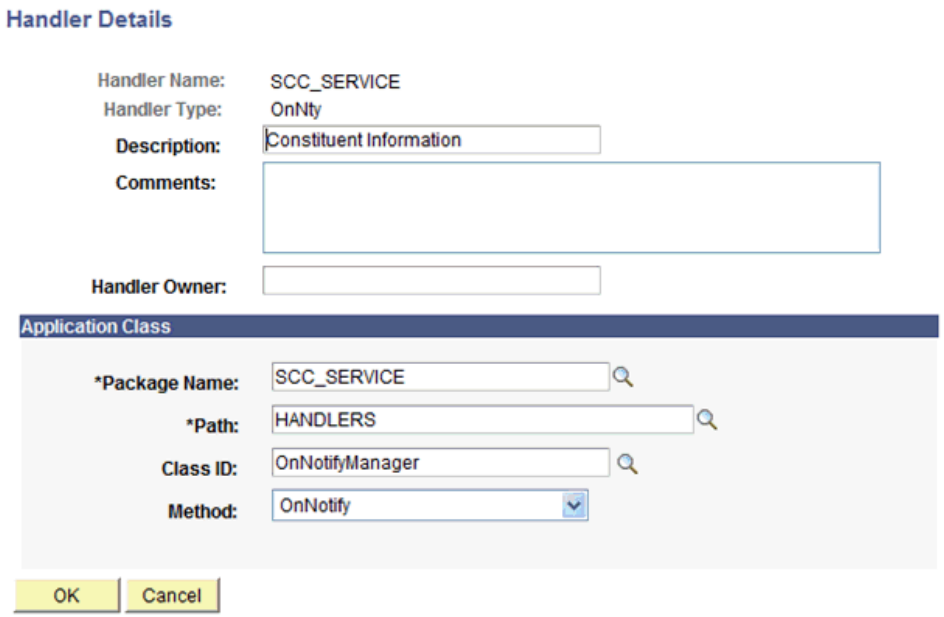
To activate the SCC_PERSON_SYNC service operation:

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**.

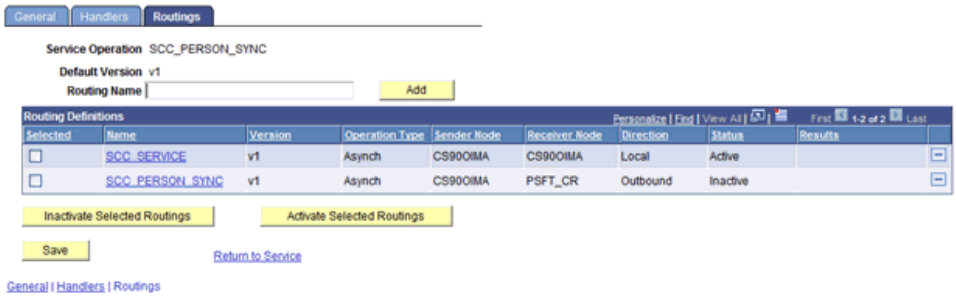
   The following screenshot displays the default version of the SCC_PERSON_SYNC service operation:



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.**



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



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.

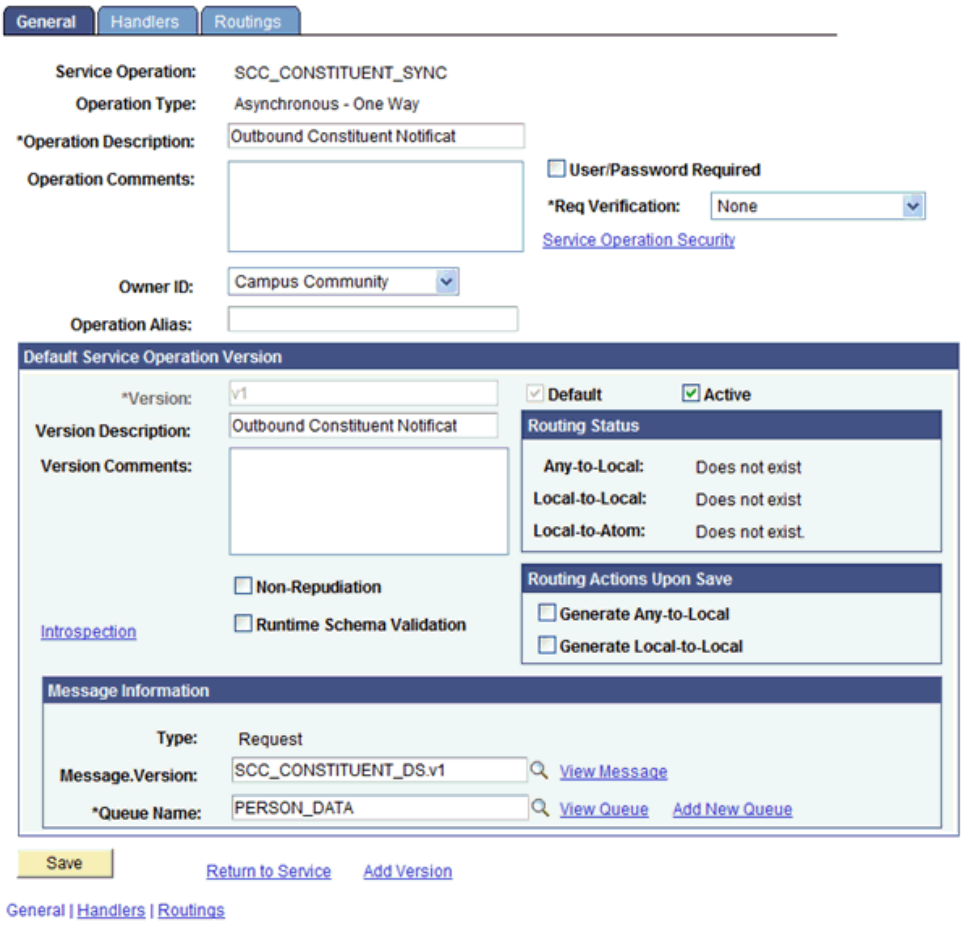
9. Click **Save.**

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:

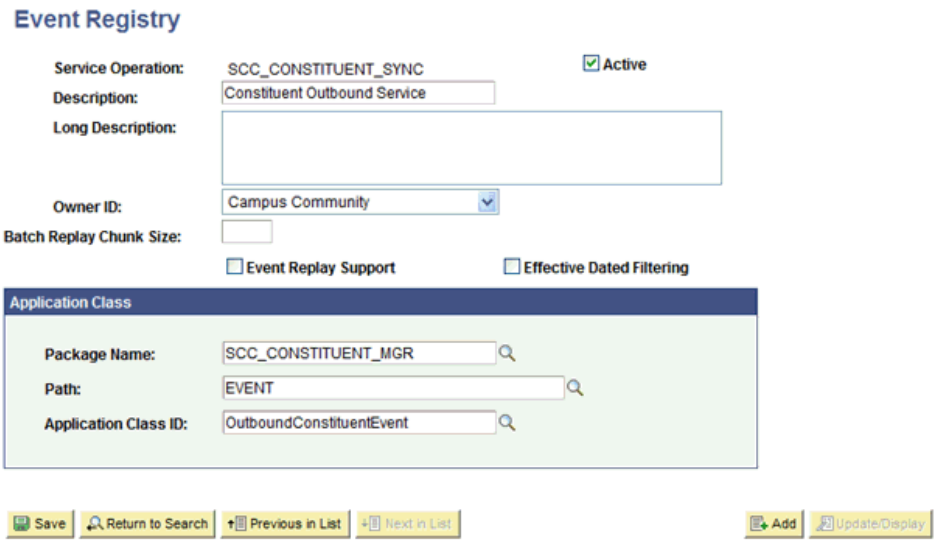


5. Click **Save.**

2.2.2.3.2.4 Activating the SSC_CONSTITUENT_SYNC Event

To activate SCC_CONSTITUENT_SYNC event:

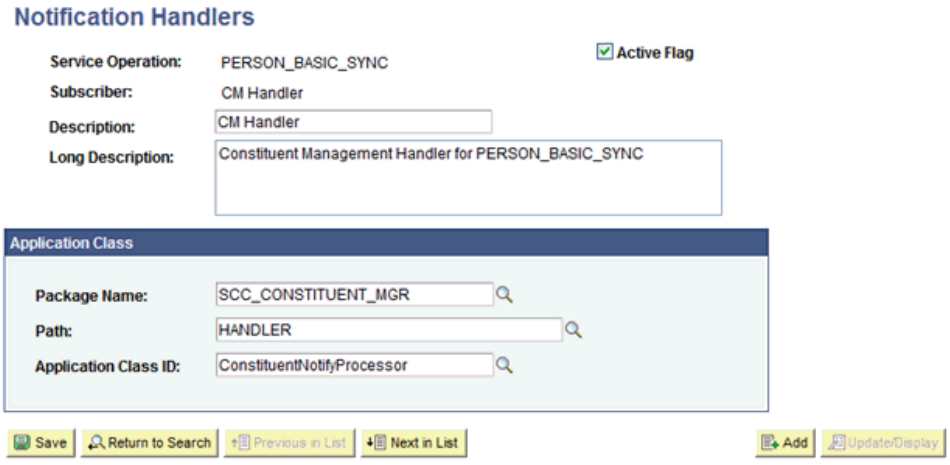
1. In the PeopleSoft Internet Architecture, expand **Set Up SACR, System Administration, Integrations,** and **Event Registry.**
2. Search for and open the **SCC_CONSTITUENT_SYNC** message.
3. Click **Active.**
4. In the Application Class region, confirm the values shown in the following screenshot:



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

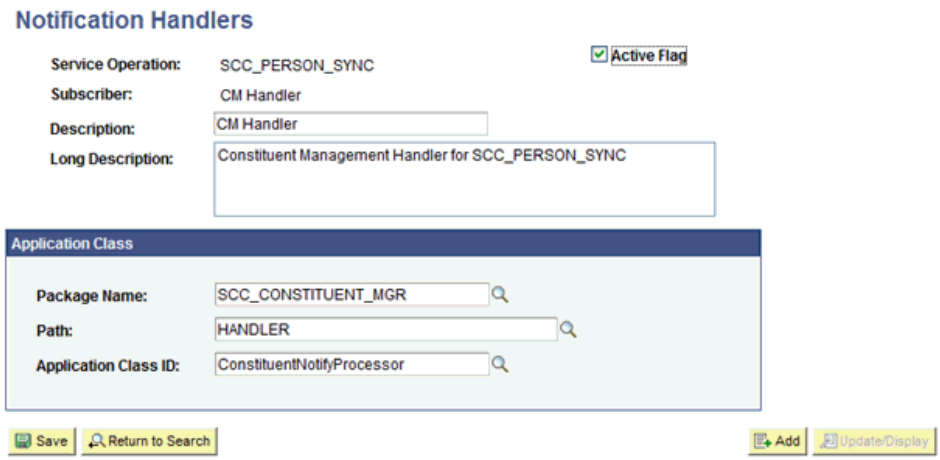


2.2.2.3.2.6 Activating the SCC_PERSON_SYNC Notification Handler

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:



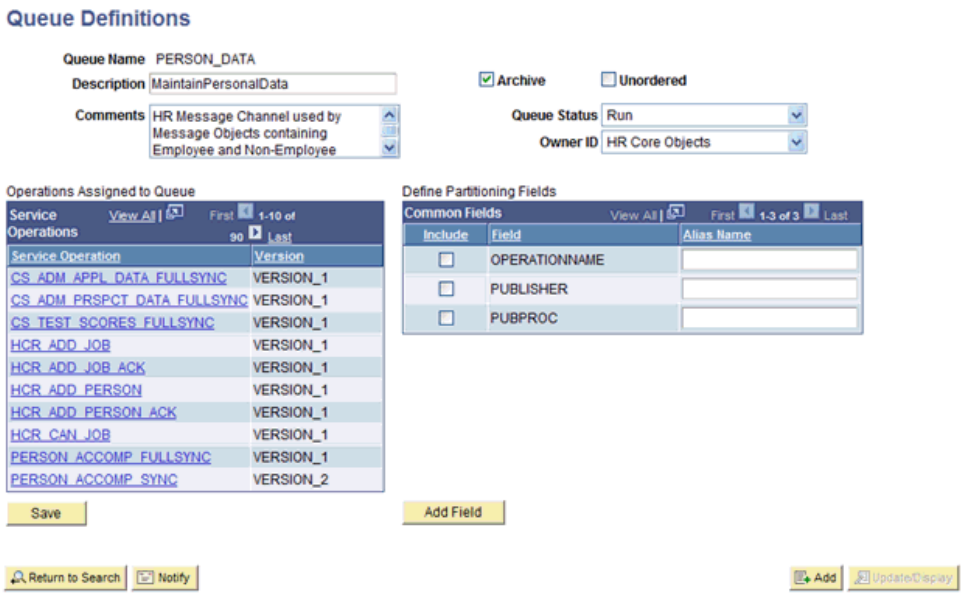
2.2.2.3.2.7 Verifying the Queue Status for the SCC_CONSTITUENT_SYNC Service Operation

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 queue status is not Run:
>
> a. From the Queue Status list, select **Run.**
>
> b. Click **Save.**
>
> The PERSON_BASIC_SYNC and SCC_PERSON_SYNC service operations also use this queue.

The queue status is shown in the following screenshot:



4. Click **Return to Search.**

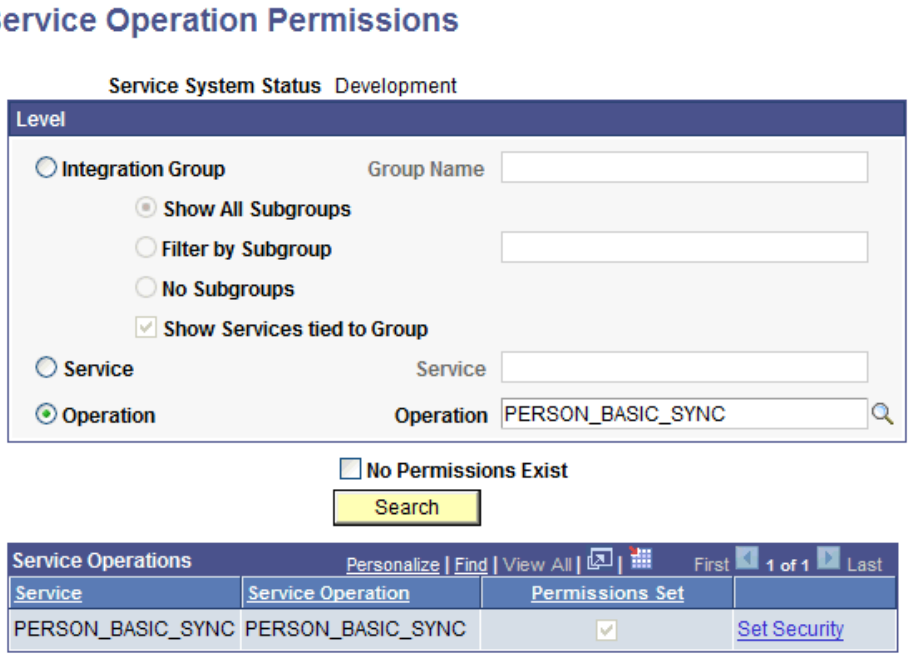
2.2.2.3.2.8 Setting Up the Security for Service Operations

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:



4. 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.

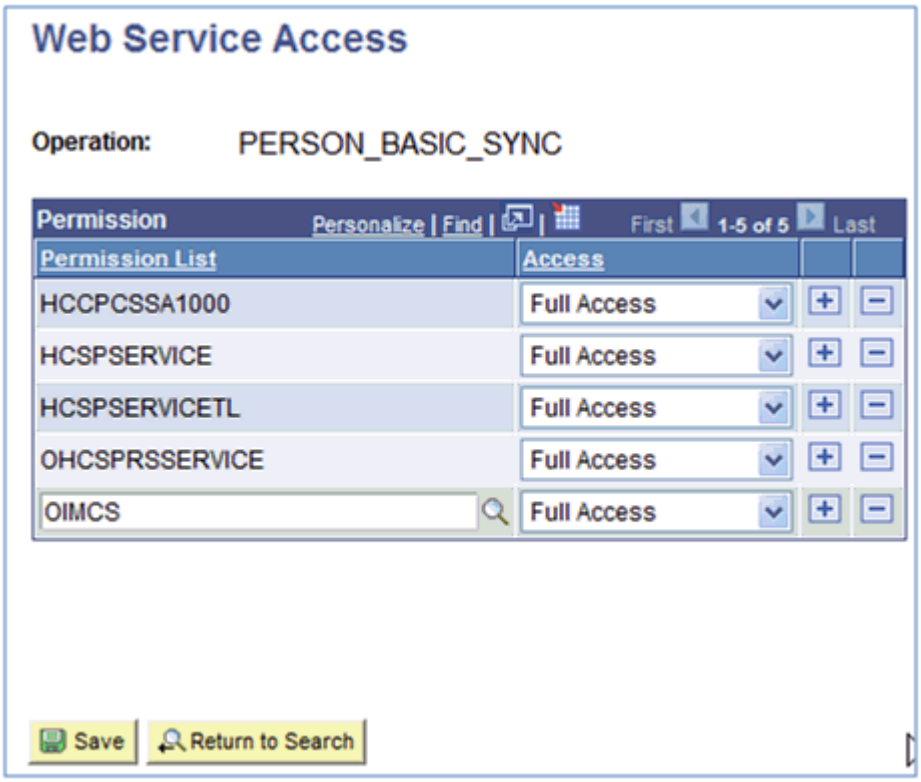
   a. Click the plus sign (+) to add a row for the Permission List field.

   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:



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:

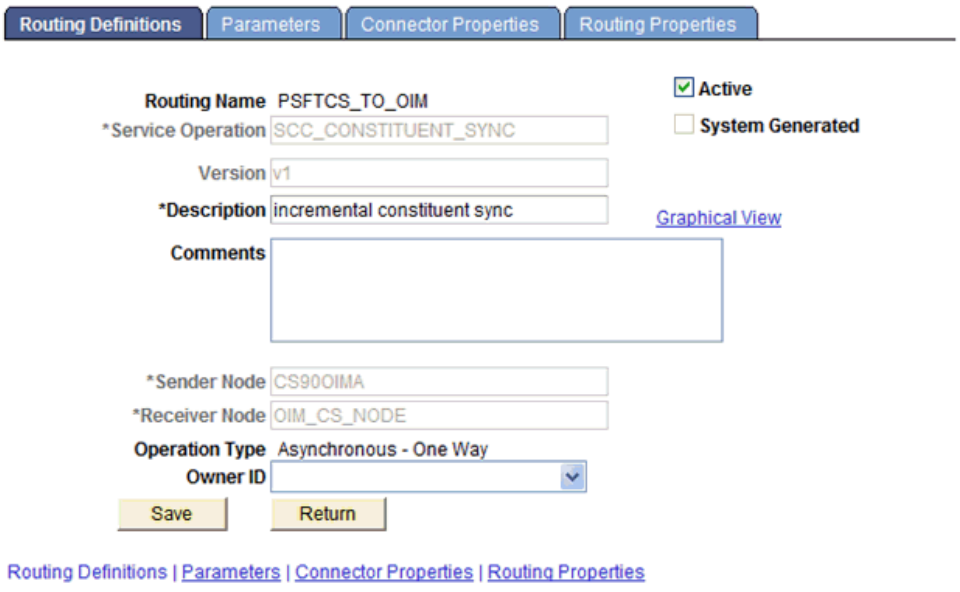
1. On the Routing tab, enter `SCC_CONSTITUENT_SYNC_CS_OIM` as the routing name and then click **Add.**
2. On the Routing Definitions tab, enter the following:

   Sender Node: `PSFT_CS`

> **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.**

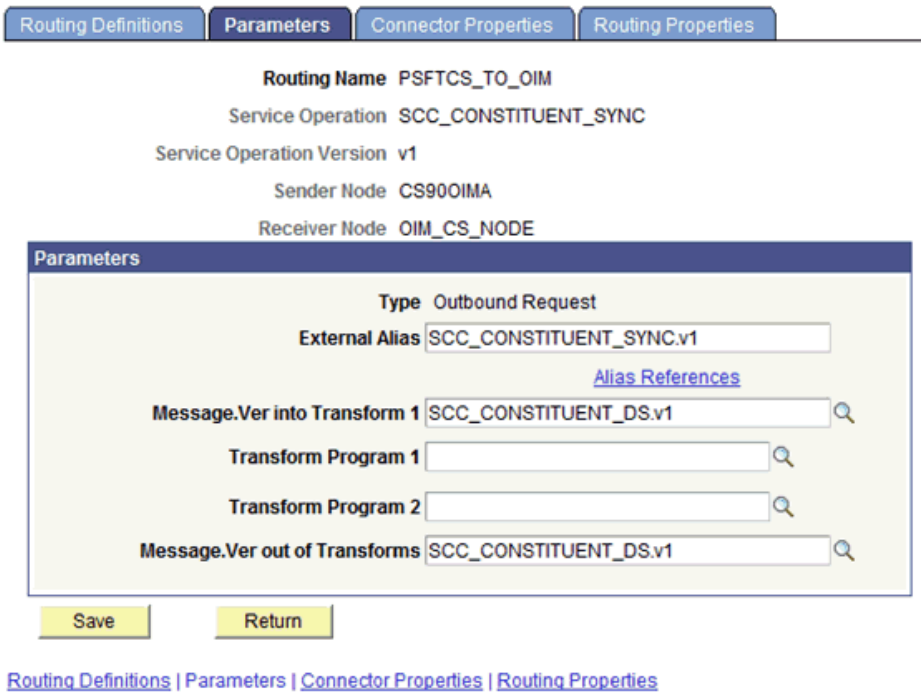
Receiver Node: `OIM_CS_NODE`

The following screenshot displays the Sender and Receiver nodes:



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:

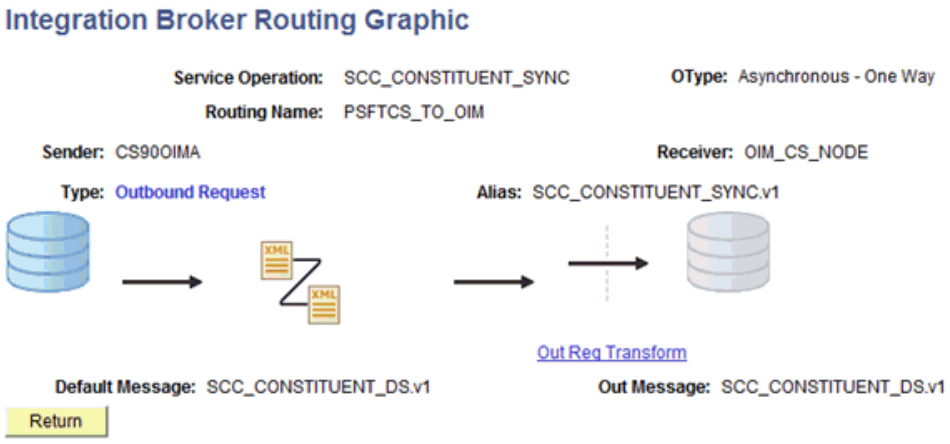


c. In the Message.Ver out of Transforms field, enter `SCC_CONSTITUENT_DS.v1`.

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:



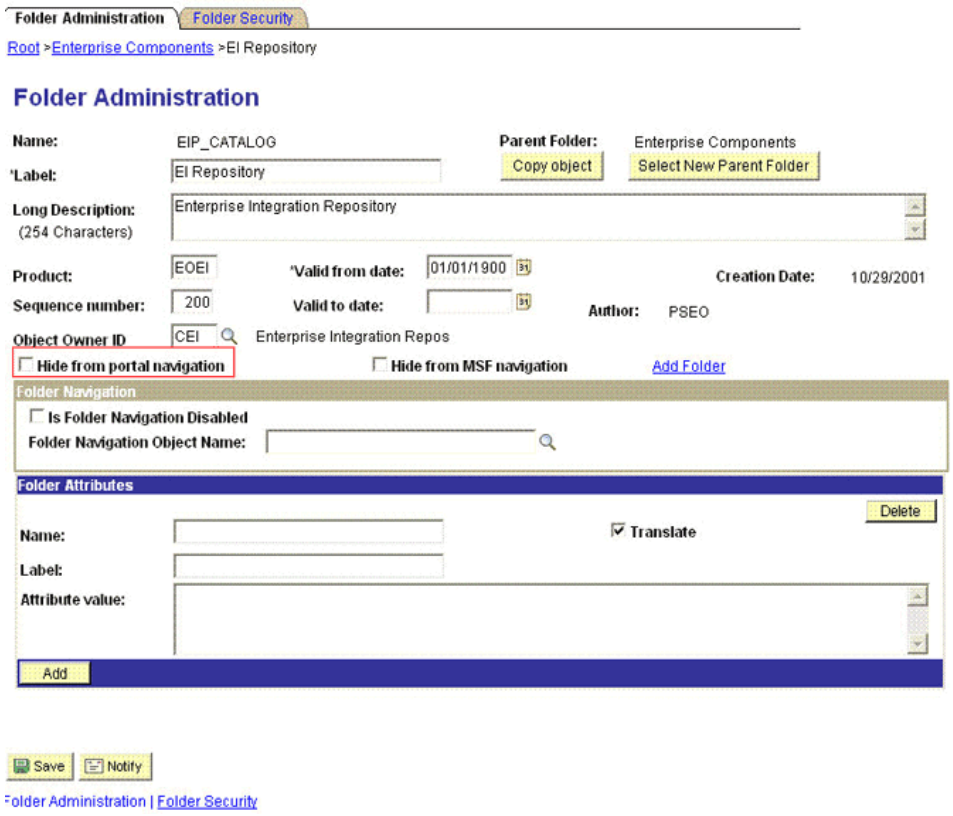
2.2.2.3.2.10 Displaying the EI Repository Folder

To display the EI Repository folder:

> **Note:**
>
> - If you have performed this procedure as described in Displaying the EI Repository Folder, then you can skip this section.
> - Perform this procedure using the PeopleSoft administrator credentials.

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

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



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

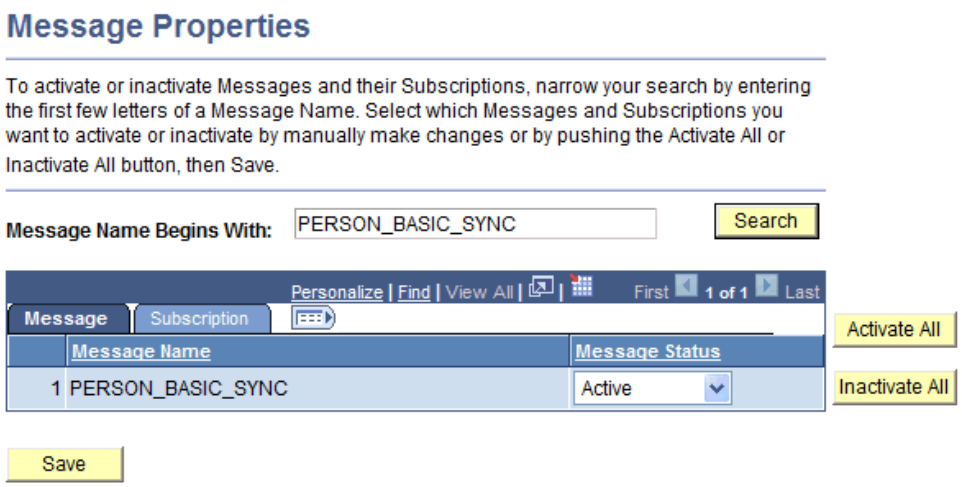
2.2.2.3.2.11 Activating the PERSON_BASIC_SYNC Message

To activate PERSON_BASIC_SYNC message:

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

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

   The following screenshot displays the message to be activated:



4. Click **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`

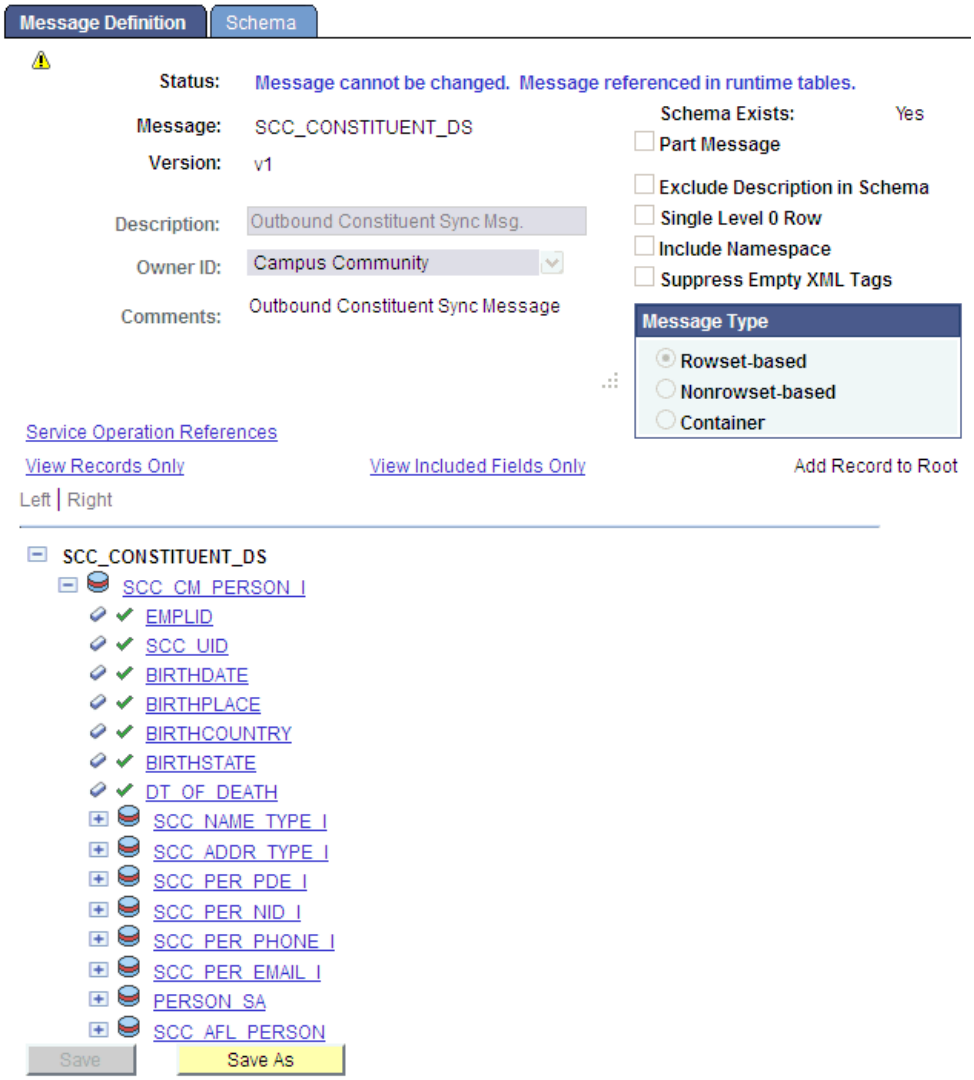
  In addition, refer to Chapter 43 of PeopleCode API Reference PeopleBook on Oracle Technology Network at the following location

  `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

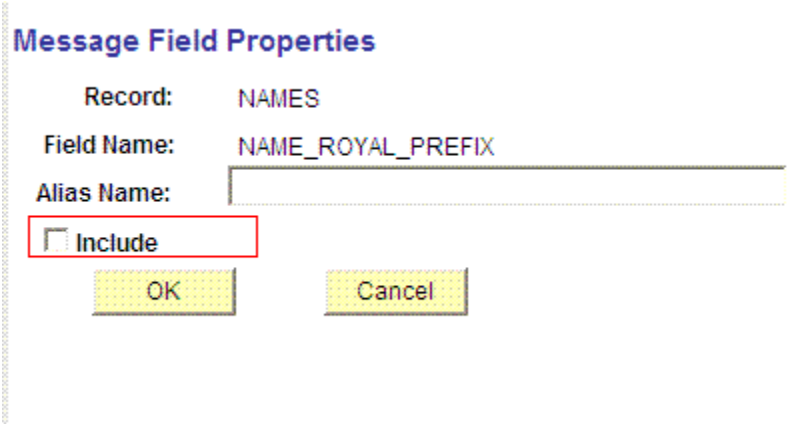
To remove unwanted fields at the message level:

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.



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

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



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.

2.3.1.1 Enabling Logging

This section contains the following topics:

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 Combinations

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

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

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

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'/>
   </log_handler>

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

<logger name="ORACLE.IAM.CONNECTORS.PSFT.CAMPUS" level="[LOG_LEVEL]"
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"
useParentHandlers="false">
     <handler name="psft-cs-handler"/>
     <handler name="console-handler"/>
   </logger>

<logger name="ORACLE.IAM.CONNECTORS.PSFT.CAMPUS" level="NOTIFICATION:1"
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 self-signed certificate or a CA certificate. Perform the procedure described in one of the following sections:

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

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

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

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

- 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:

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

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

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

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

2.3.1.4.2.2 Configuring SSL on Oracle WebLogic Server with a CA Certificate

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

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

- 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]:  US
Is <CN=Name or IP address of the computer, OU=example, O=example, L=New
York, ST=New York, C=US> correct?
  [no]:  yes
```

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

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

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

For example:

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

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

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

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

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

For example:

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

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

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

For example:

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

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

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

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

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 11*g* 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 11*g* 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>
<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 `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:

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.
4. 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.
7. 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.

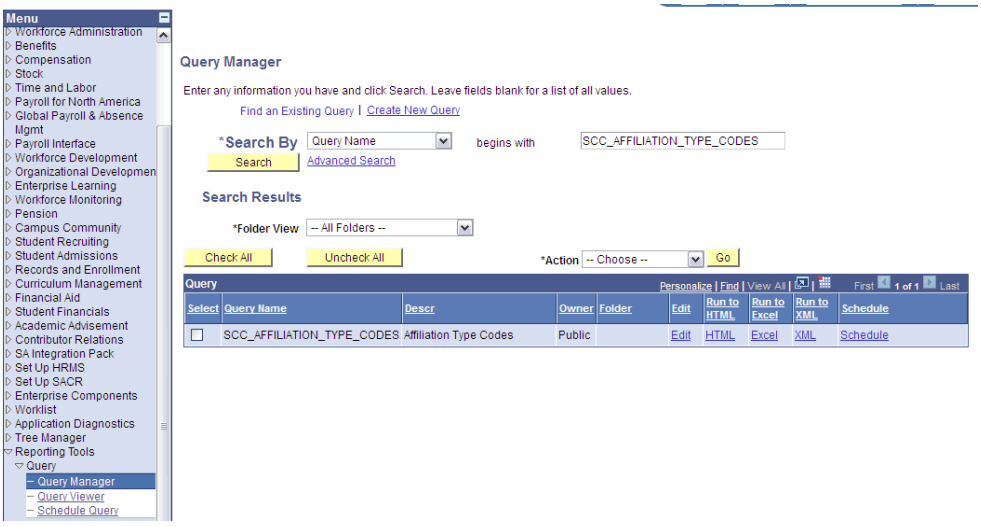
This section contains the following procedures:

- 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.
4. In the new html page, click **CSV Text File** and save the CSV file, as shown in the following screenshot.

SCC_AFFILIATION_TYPE_CODES- Affiliation Type Codes

Download results in : Excel SpreadSheet | CSV Text File | XML File (7 kb)

View All First 1-7 of 7 Last

	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

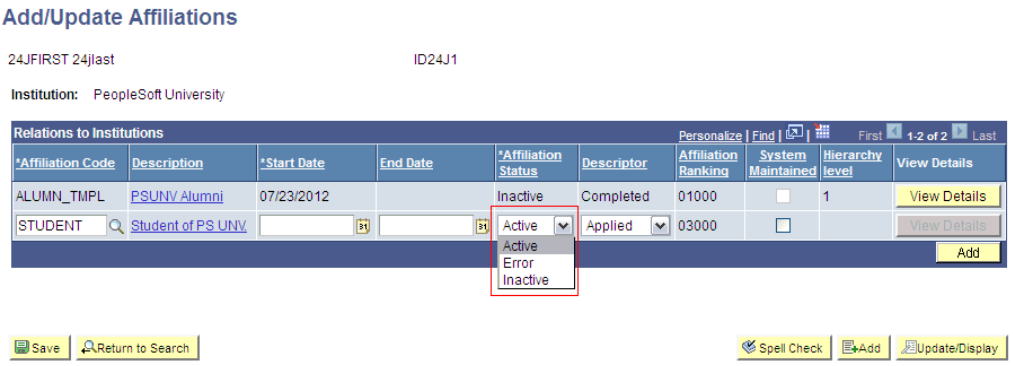
This section contains the following topics:

- 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:



3.3.2 Verifying the Affiliation Status Code on PeopleSoft Campus

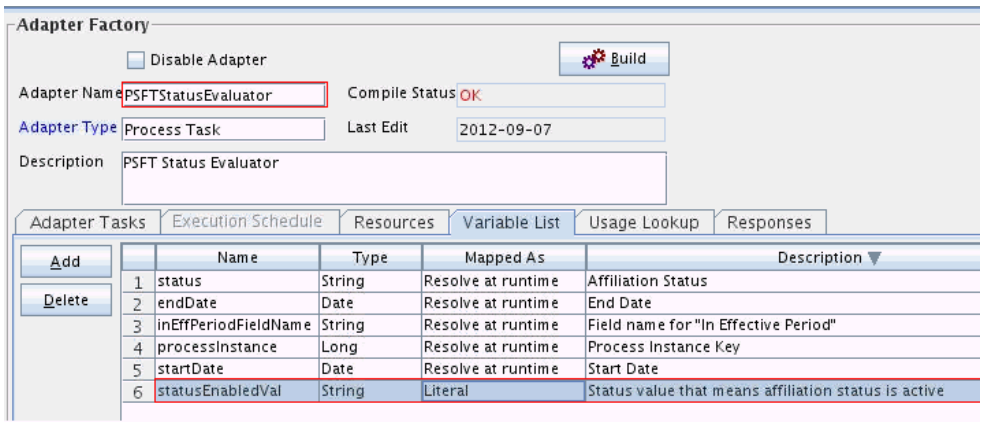
To verify the Affiliation Status code on PeopleSoft Campus that corresponds to Enabled status in Oracle Identity Manager, perform the following procedure:

1. 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.

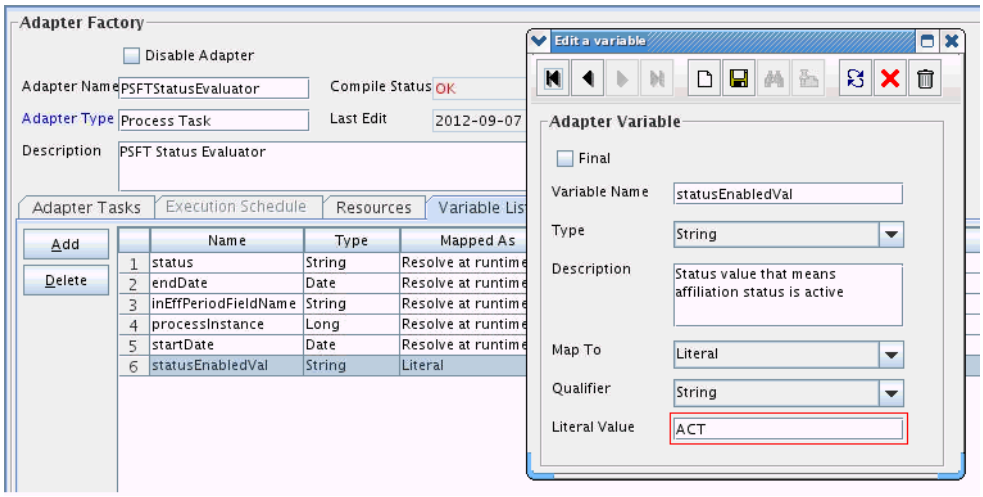
```
<?xml version="1.0" encoding="us-ascii"?>
<SCC_CONSTITUENT_FULLSYNC>
  <FieldTypes>
  <MsgData>
    <Transaction>
    <Transaction>
      <SCC_CM_PERSON_I class="R">
        <EMPLID IsChanged="Y">EXCLUDE2</EMPLID>
        <SCC_UID></SCC_UID>
        <BIRTHDATE IsChanged="Y">1961-03-29</BIRTHDATE>
        <BIRTHPLACE></BIRTHPLACE>
        <BIRTHCOUNTRY IsChanged="Y">USA</BIRTHCOUNTRY>
        <BIRTHSTATE></BIRTHSTATE>
        <DT_OF_DEATH></DT_OF_DEATH>
        <NAME_TYPE_VW2 class="R">
        <PSCAMA class="R">
        <ADDRESS_TYPE_V2 class="R">
        <PSCAMA class="R">
        <SCC_PER_PDE_I class="R">
        <PSCAMA class="R">
        <SCC_PER_NID_I class="R">
        <PSCAMA class="R">
        <PERSON_SA class="R">
        <PSCAMA class="R">
        <SCC_AFL_PERSON class="R">
        <PSCAMA class="R">
        <SCC_AFL_PERSON class="R">
          <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">
      </SCC_CM_PERSON_I>
      <PSCAMA class="R">
    </Transaction>
```

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



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.



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.

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

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

Table 3-2 (Cont.) 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` **Note:** 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`

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 3-3 Attributes of the PeopleSoft Campus Affiliation Effective Date Processor Scheduled Task

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:

1. 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 `Timeout` or `Error`.

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

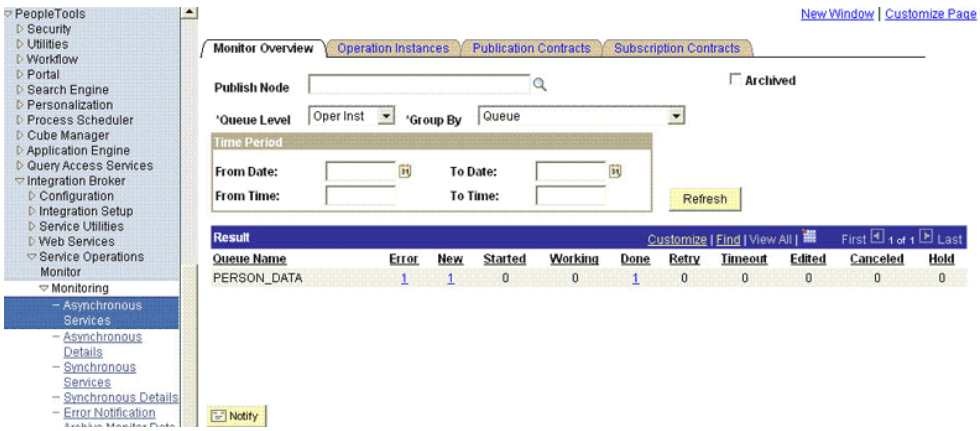
If the status of the message is `New` or `Started` and it does not change to `Timeout` or `Done`, then you must restart the PeopleSoft application server after you restart Oracle Identity Manager.

> **Note:**
>
> PeopleSoft supports this functionality for a limited rights user created in Creating a Role for a Limited Rights User. But, you can specify persons who have rights to perform this task based on the security policy of your organization.

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.



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 message-specific 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:

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.

```
<?xml version="1.0"?>
<SCC_CONSTITUENT_DS>
  <FieldTypes>
    <SCC_CM_PERSON_I class="R">
    <SCC_PER_ADDR_I class="R">
    <SCC_NAME_TYPE_I class="R">
    <SCC_ADDR_TYPE_I class="R">
    <SCC_PER_PDE_I class="R">
    <SCC_PER_NID_I class="R">
    <SCC_PER_PHONE_I class="R">
    <SCC_PER_EMAIL_I class="R">
    <PERSON_SA class="R">
    <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>
    <SCC_PER_NAME_I class="R">
    <PSCAMA class="R">
  </FieldTypes>
  <MsgData>
</SCC_CONSTITUENT_DS>
```

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:

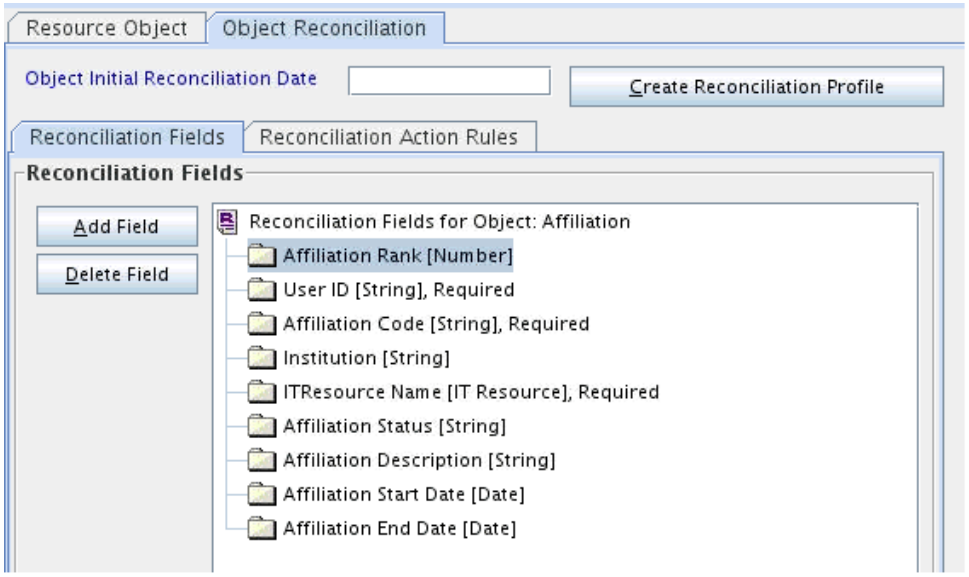
1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management.**
3. Double-click **Resource Objects.**
4. Search for and open the **PeopleSoft Campus** resource object.
5. On the Object Reconciliation tab, click **Add Field.**
6. In the Add Reconciliation Field dialog box, 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



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:

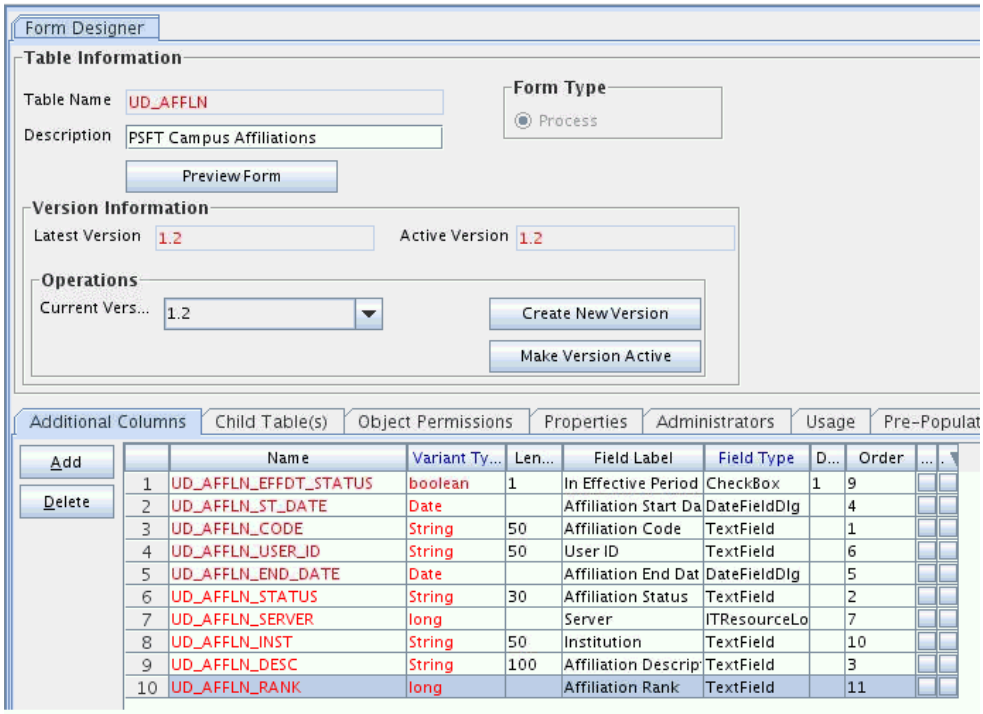
1. Click **Add**.

   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.

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.**
5. In the Field Name field, select the value for the field that you want to add.

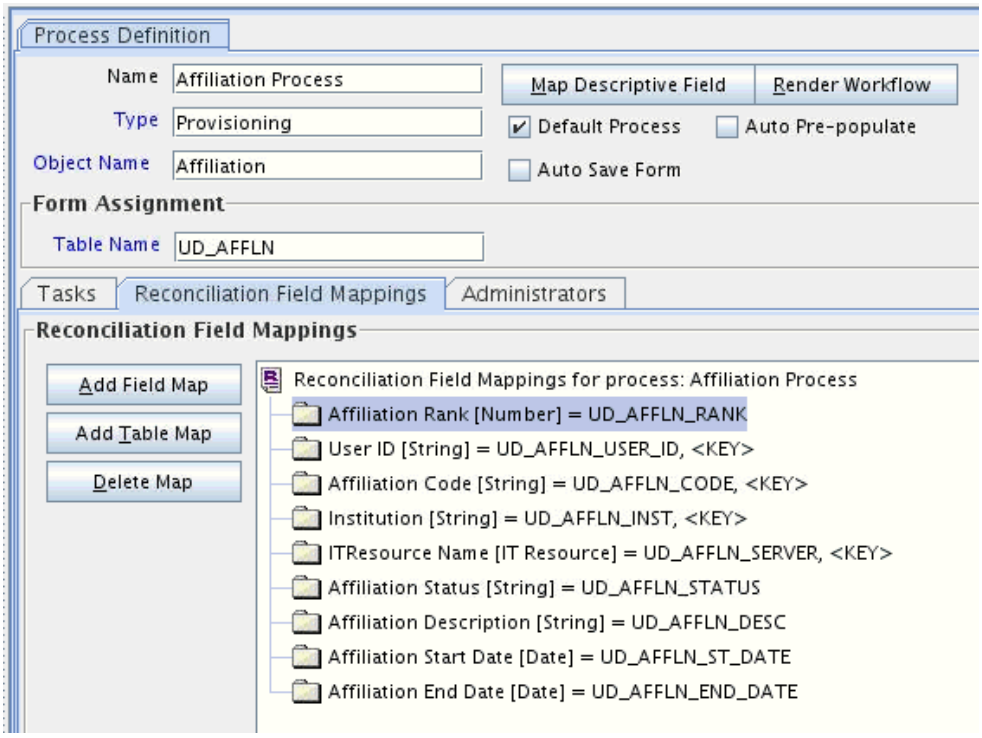
   For example, select `Affiliation Rank.`
6. In the **Field Type** field, select the type of the field that is prepopulated.
7. Double-click the **Process Data Field** field.

   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.

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.**
3. Search for and open the **Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping** lookup definition.

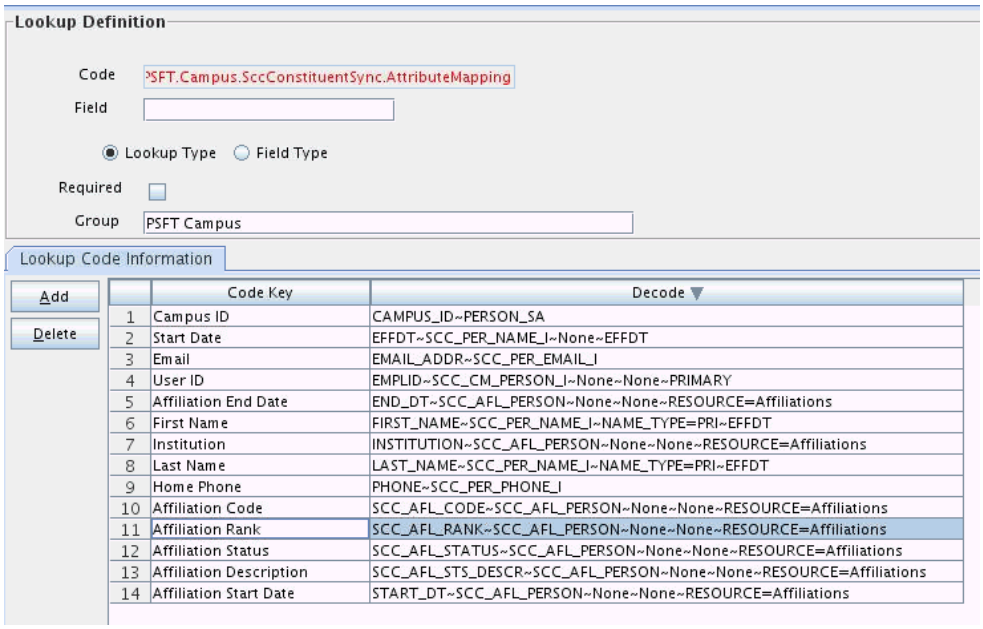
   For full reconciliation, you must also add this entry in the **Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping** lookup definition.
4. Click **Add** and enter the Code Key and Decode values for the field.

   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.

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:

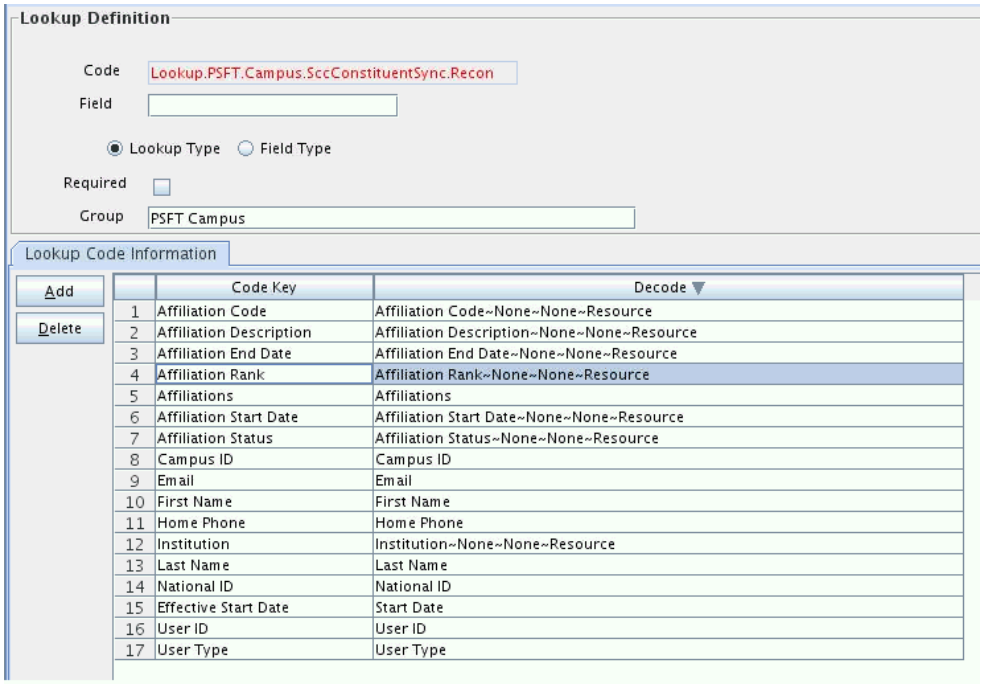
1. Expand **Administration**.
2. Double-click **Lookup Definition.**
3. Search for and open the **Lookup.PSFT.Campus.SccConstituentSync.Recon** lookup definition.
4. Click **Add** and enter the Code Key and Decode values for the field.

   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~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.

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:

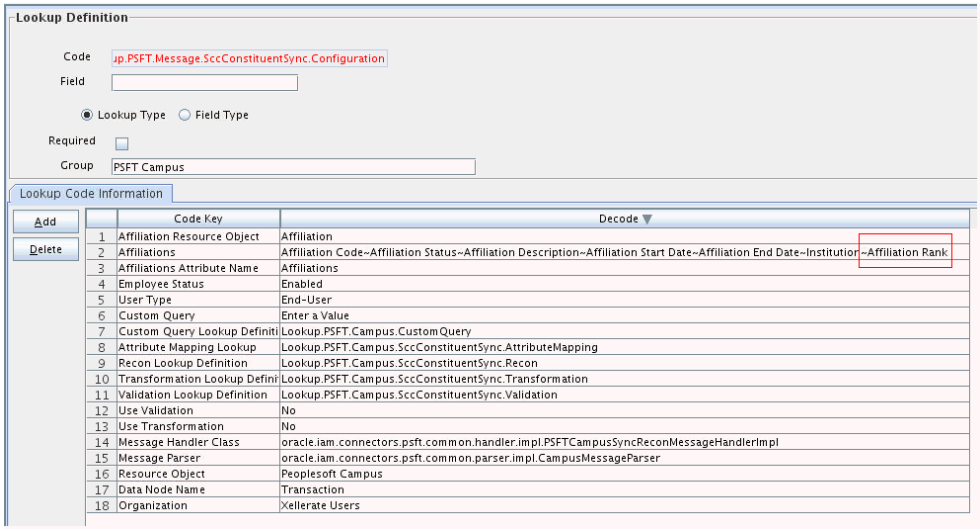
1. Expand **Administration**.
2. Double-click **Lookup Definition.**
3. Search for and open the **Lookup.PSFT.Message.SccConstituentSync.Configuration** lookup definition.

   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.

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

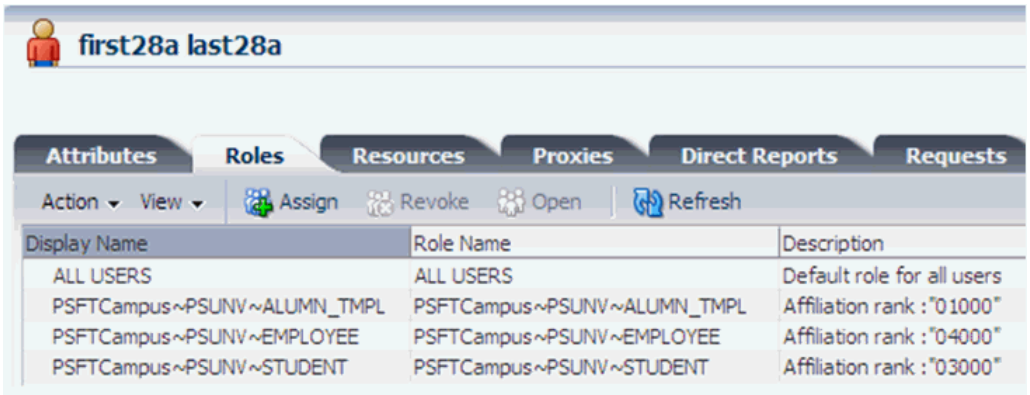
Roles are created in Oracle Identity Manager that correspond to each unique PeopleSoft Campus Affiliations. The Ranks of the affiliations are stored in the role descriptions in Oracle Identity Manager.

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:



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 (#):

```
package com.validate;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.logging.Logger;
public class MyValidation {

    Logger log;
    public boolean validate(HashMap hmUserDetails,
            HashMap hmAffiliationDetails, String field) {
        /*
         * You must write code to validate attributes. Parent
         * data values can be fetched by using hmUserDetails.get(field)
         * For child data values, loop through the
         * ArrayList fetched by hmAffiliationDetails.get("Affiliations")
         * Depending on the outcome of the validation operation,
```

```
             * the code must return true or false.
             *
             * In this sample code, the value "false" is returned if the field
             * contains the number sign (#). Otherwise, the value "true" is
             * returned.
             */
            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++){
                    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;
        }
    }
```

2. Create a JAR file to hold the Java class.

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.

> **See Also:**
>
> The Javadocs shipped with the connector for more information about this interface

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){
            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:

> **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.

4.6.3 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.
2. 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.
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 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.
2. 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.

Table 4-1 Connector Objects and Their Associations

Connector Object	Name	Referenced By	Description
IT Resource	PSFT Campus	• Scheduled Task: PeopleSoft Campus Trusted Reconciliation • Resource Object: PeopleSoft Campus	You need to create a copy of IT Resource with a different name.
Resource Object	PeopleSoft Campus	Message-specific configuration lookup definitions: • Lookup.PSFT.Message.SccConstituentSync.Configuration • Lookup.PSFT.Message.SccConstituentFullSync.Configuration	It is optional to create a copy of a resource object. If you are reconciling the same set of attributes from the other target system, then you need not create a new resource object. **Note:** Create copies of this resource object only if there are differences in attributes between the two installations of the target system.
Common Configuration Lookup Definition	Lookup.PSFT.Campus.Configuration	Message-specific configuration lookup definitions: • Lookup.PSFT.Message.SccConstituentSync.Configuration • Lookup.PSFT.Message.SccConstituentFullSync.Configuration	It is optional to create a copy of the common configuration lookup definition. **Note:** Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.

Table 4-1 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Description
Message-specific Configuration Lookup Definition	Lookup definitions: • Lookup.PSFT.Message.SccConstituentSync.Configuration • Lookup.PSFT.Message.SccConstituentFullSync.Configuration	Attribute mapping lookup definitions: • Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping • Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping	It is optional to create a copy of the message-specific lookup definitions. **Note:** Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.
Attribute Mapping Lookup Definition	Lookup definitions: • Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping • Lookup.PSFT.Campus.SccConstituentFullSync.AttributeMapping	NA	This lookup definition holds the information of the attributes reconciled from the XML message file from the target system. **Note:** Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.
Recon Map Lookup Definition	Lookup.PSFT.Campus.SccConstituentSync.Recon	NA	This lookup definition maps the resource object field with the data reconciled from the message. **Note:** Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.

4.8.2 Creating Copies of the Connector Objects

To create copies of the connector objects:

> **Note:**
>
> See Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the steps in this procedure.

1. Create a copy of the IT resource. See Configuring the IT Resource for information about this IT resource.
2. Create a copy of the PeopleSoft 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.
5. 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.common.parser.impl.CampusMessageParser: processMessage: No data found in XML`
`MissingRequiredAttributeException: [Last Name]`
	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 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 modified message structure.
	Note: If this problem is encountered during incremental reconciliation, then change the Decode entries in the Lookup.PSFT.Campus.SccConstituentSync.AttributeMapping 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

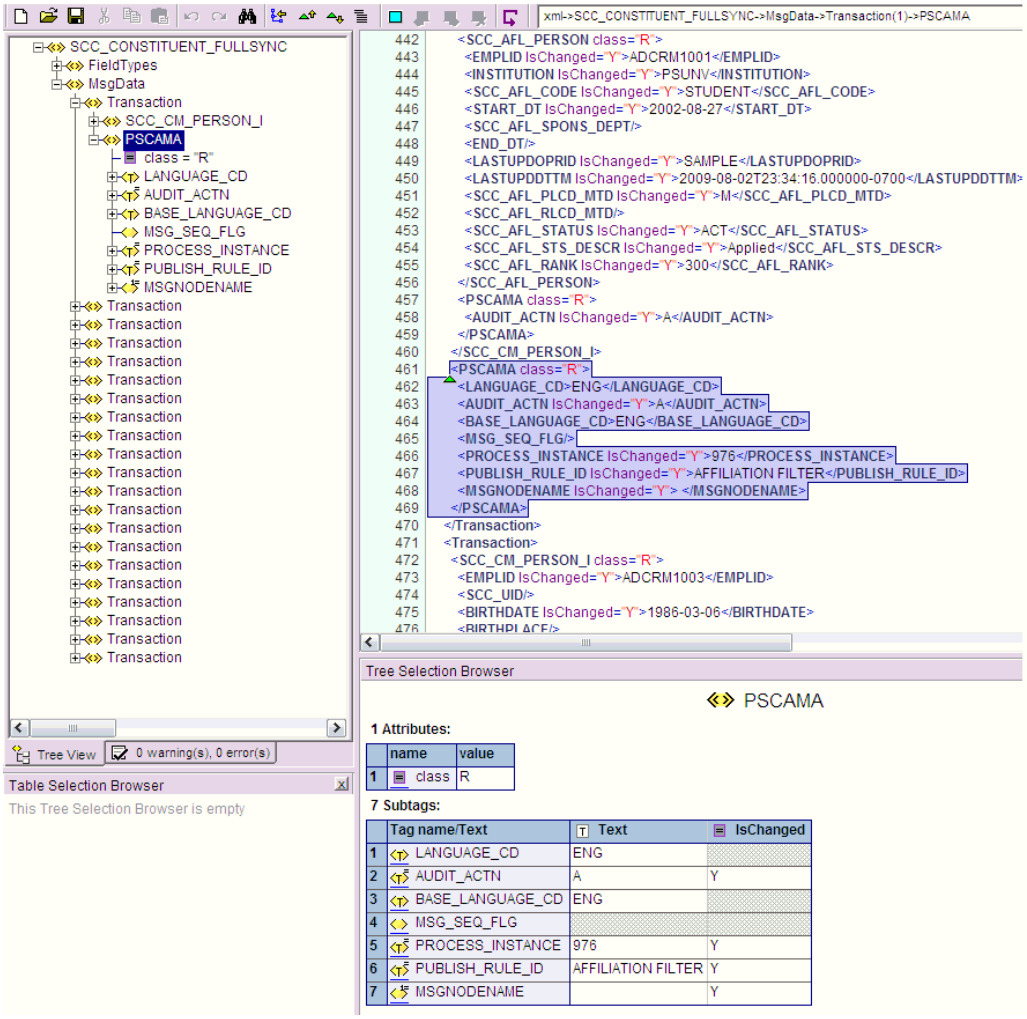
An XML message that is published by PeopleSoft contains a Transaction node. In case of full reconciliation, the XML files for SCC_CONSTITUENT_FULLSYNC messages have multiple transaction nodes. However, in case of incremental reconciliation, the XML messages SCC_CONSTITUENT_SYNC have only one transaction node.

This appendix contains the following topics:

A.1 The PSCAMA Subnode

Every transaction node has a PeopleSoft Common Application Messaging Attributes (PSCAMA) subnode.

The following screenshot shows the PSCAMA node:



PSCAMA is an XML tag that contains fields common to all messages. The PSCAMA tag is repeated for each row in each level of the Transaction section of the message. PSCAMA provides the following information about the message data:

- Language in which the data is written
- Type of transaction the row represents, such as add or update

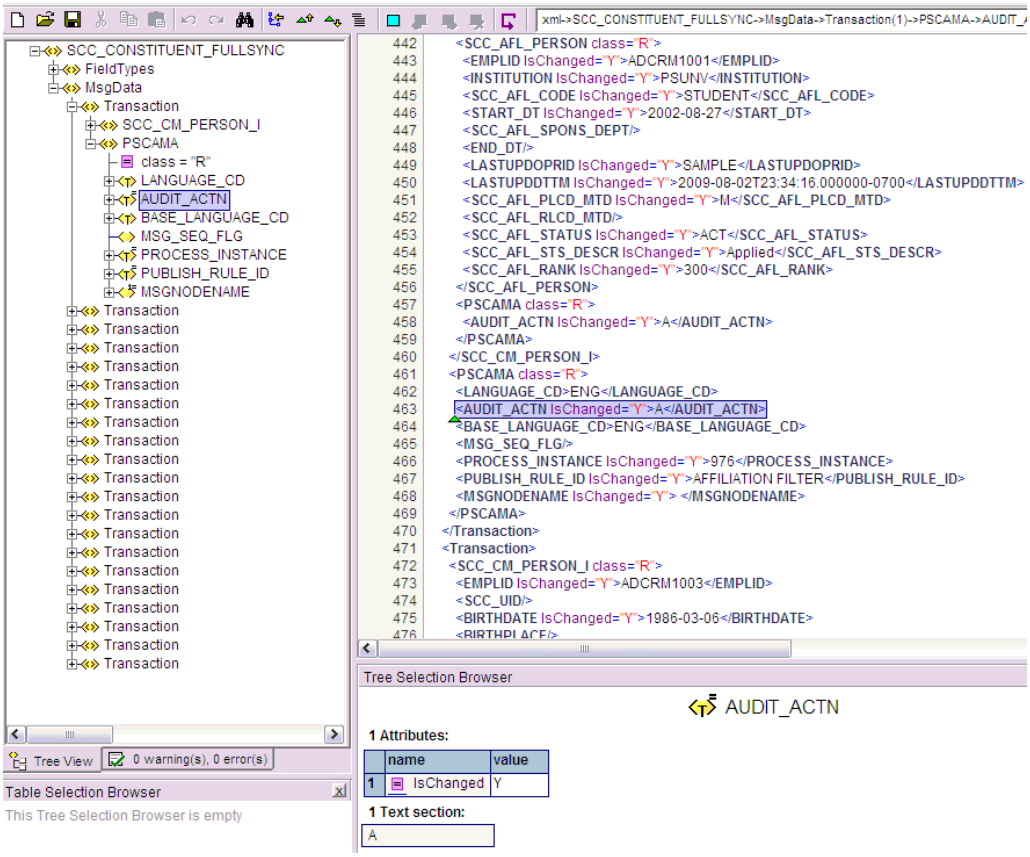
When receiving a message, PeopleCode inspects the PSCAMA node for this information and responds accordingly.

A.2 Root Audit Action

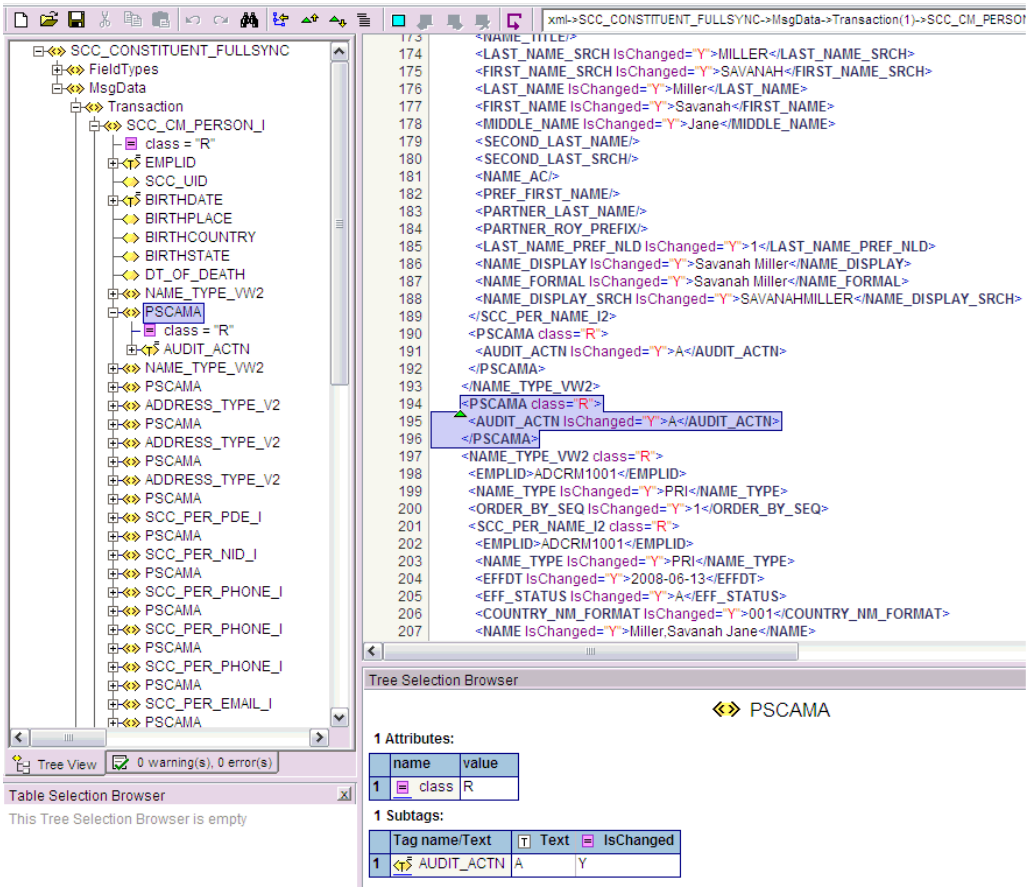
The AUDIT_ACTN subnode of PSCAMA, known as Root Audit Action, filters the data records in an XML message. It indicates the action taken against a person, such as Add or Change in Oracle Identity Manager.

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:



The nonzero level PSCAMA node and its Root Audit Action are shown in the following screenshot:


xml->SCC_CONSTITUENT_FULLSYNC->MsgData->Transaction(1)->SCC_CM_PERSON
SCC_CONSTITUENT_FULLSYNC
FieldTypes
MsgData
Transaction
SCC_CM_PERSON_I
class = "R"
EMPLID
SCC_UID
BIRTHDATE
BIRTHPLACE
BIRTHCOUNTRY
BIRTHSTATE
DT_OF_DEATH
NAME_TYPE_VW2
PSCAMA
class = "R"
AUDIT_ACTN
Tree View
0 warning(s), 0 error(s)
Table Selection Browser
This Tree Selection Browser is empty
<LAST_NAME_SRCH IsChanged="Y">MILLER</LAST_NAME_SRCH>
<FIRST_NAME_SRCH IsChanged="Y">SAVANAH</FIRST_NAME_SRCH>
<LAST_NAME IsChanged="Y">Miller</LAST_NAME>
<FIRST_NAME IsChanged="Y">Savanah</FIRST_NAME>
<MIDDLE_NAME IsChanged="Y">Jane</MIDDLE_NAME>
<SECOND_LAST_NAME/>
<SECOND_LAST_SRCH/>
<NAME_AC/>
<PREF_FIRST_NAME/>
<PARTNER_LAST_NAME/>
<PARTNER_ROY_PREFIX/>
<LAST_NAME_PREF_NLD IsChanged="Y">1</LAST_NAME_PREF_NLD>
<NAME_DISPLAY IsChanged="Y">Savanah Miller</NAME_DISPLAY>
<NAME_FORMAL IsChanged="Y">Savanah Miller</NAME_FORMAL>
<NAME_DISPLAY_SRCH IsChanged="Y">SAVANAHMILLER</NAME_DISPLAY_SRCH>
</SCC_PER_NAME_I2>
<PSCAMA class="R">
<AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
</PSCAMA>
</NAME_TYPE_VW2>
<PSCAMA class="R">
<AUDIT_ACTN IsChanged="Y">A</AUDIT_ACTN>
</PSCAMA>
<NAME_TYPE_VW2 class="R">
<EMPLID>ADCRM1001</EMPLID>
<NAME_TYPE IsChanged="Y">PRI</NAME_TYPE>
<ORDER_BY_SEQ IsChanged="Y">1</ORDER_BY_SEQ>
<SCC_PER_NAME_I2 class="R">
<EMPLID>ADCRM1001</EMPLID>
<NAME_TYPE IsChanged="Y">PRI</NAME_TYPE>
<EFFDT IsChanged="Y">2008-06-13</EFFDT>
<EFF_STATUS IsChanged="Y">A</EFF_STATUS>
<COUNTRY_NM_FORMAT IsChanged="Y">001</COUNTRY_NM_FORMAT>
<NAME IsChanged="Y">Miller,Savanah Jane</NAME>
Tree Selection Browser
PSCAMA
1 Attributes:
name
value
class
R
1 Subtags:
Tag name/Text
Text
IsChanged
AUDIT_ACTN
A
Y

B

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:

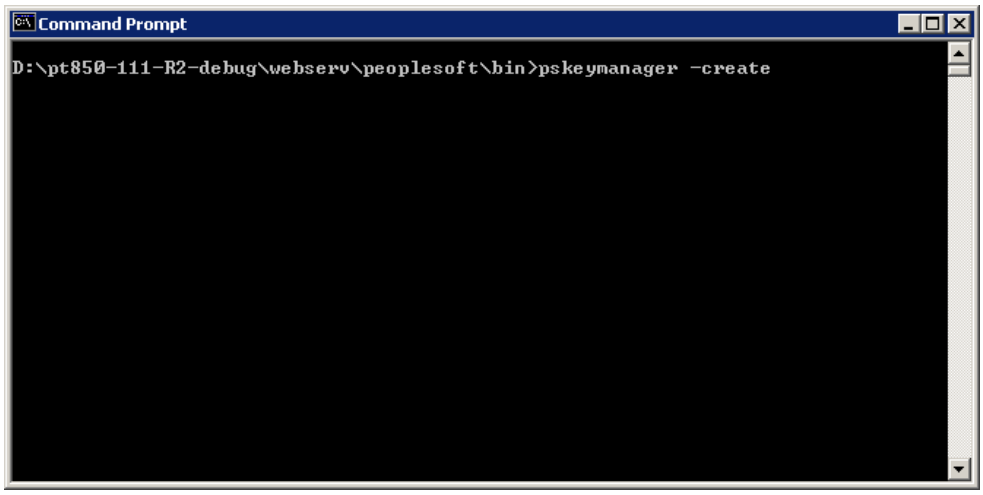
- Generating Signed Public Encryption Key and CSR
- Submitting CSRs to CAs for Signing
- Downloading the Root Certificate
- Importing a Server-Side Public Key into a Keystore
- Generating and Importing Public Keys
- Configuring Oracle WebLogic Server to Use the Keystore
- Adding the Root Certificate
- 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.

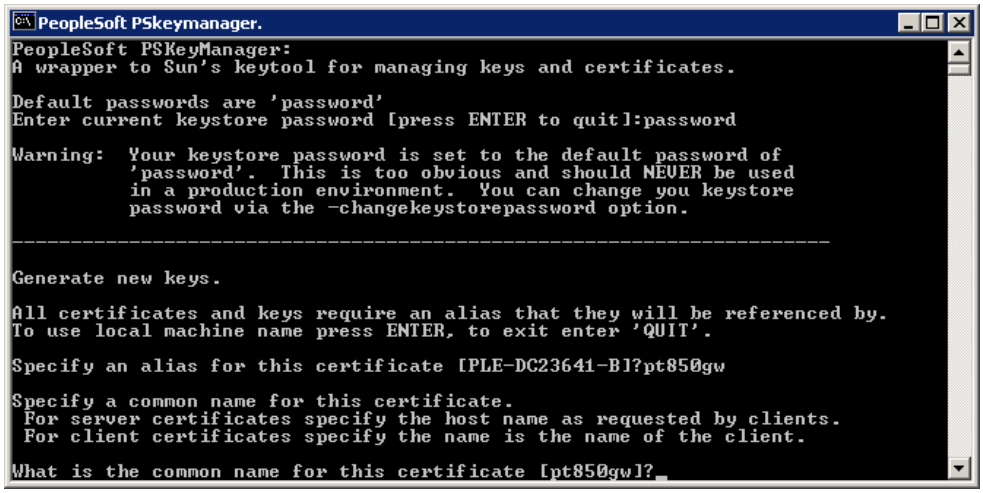
3. Enter the following at the command line:

   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.**



   Enter the appropriate information at the following command prompts:

   Organization unit

   Organization

   City or Locality

   State or Province

   Country code

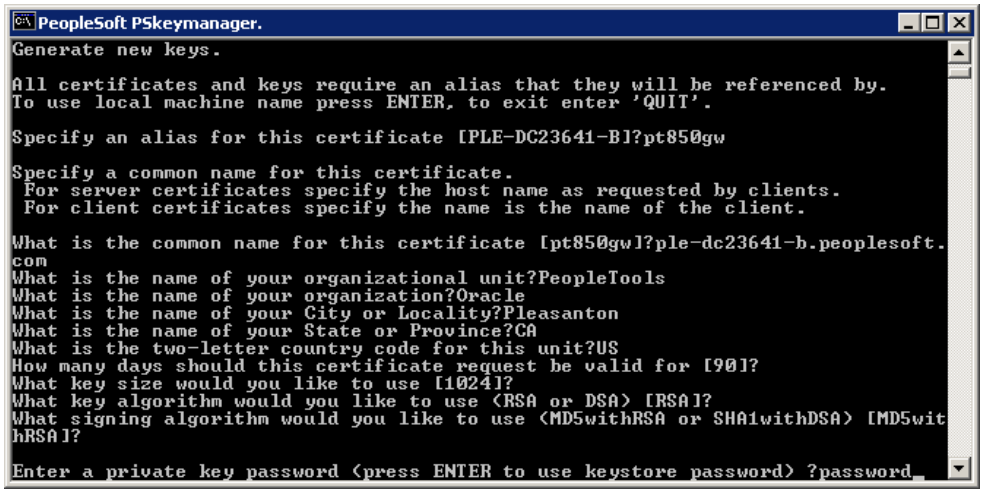
   Number of days the certificate should be valid (Default is 90.)

   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.**

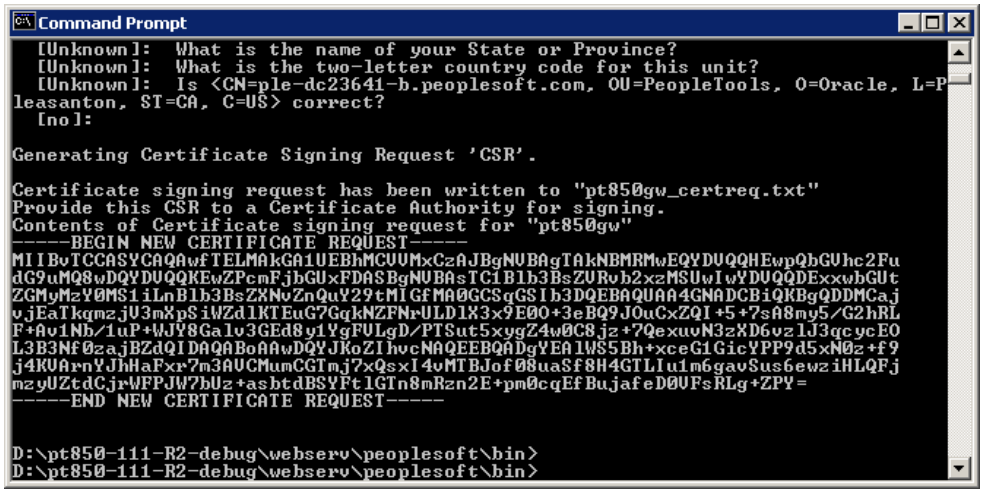


5. Verify that the values you entered are correct, and press **Enter.**

   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
2VuaXgxFDASBgNVBAoTC1Blb3BsZVRvb2xzMRMwEQYDVQQLEwpZW9wbGVzb2Z0MRYwFAYDVQQDEw1
NREFXU09OMDUxNTAzMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC43lCZWxrsyxven5QethAd
sLIEEPhhhl7TjA0r8pxpO+ukD8LI7TlTntPOMU535qMGfk/
jYtG0QbvpwHDYePyNMtVou6wAs2yr1B+wJSp6Zm42m8PPihfMUXYLG9RiIqcmp2FzdIUi4M07J8ob
8rf0W+Ni1bGW2dmXZ0jGvBmNHQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAKx/
ugTt0soNVmiH0YcI8FyW8b81FWGIR0f1Cr2MeDiOQ2pty24dKKLUqIhogTZdFAN0ed6Ktc82/5xBo
H1gv7YeqyPBJvAxW6ekMsgOEzLq9OU3ESezZorYFdrQTzqsEXUp1A+cZdfo0eKwZTFmjNAsh1kis+
HOLoQQwyjgaxYI=
-----END NEW CERTIFICATE REQUEST-----
```



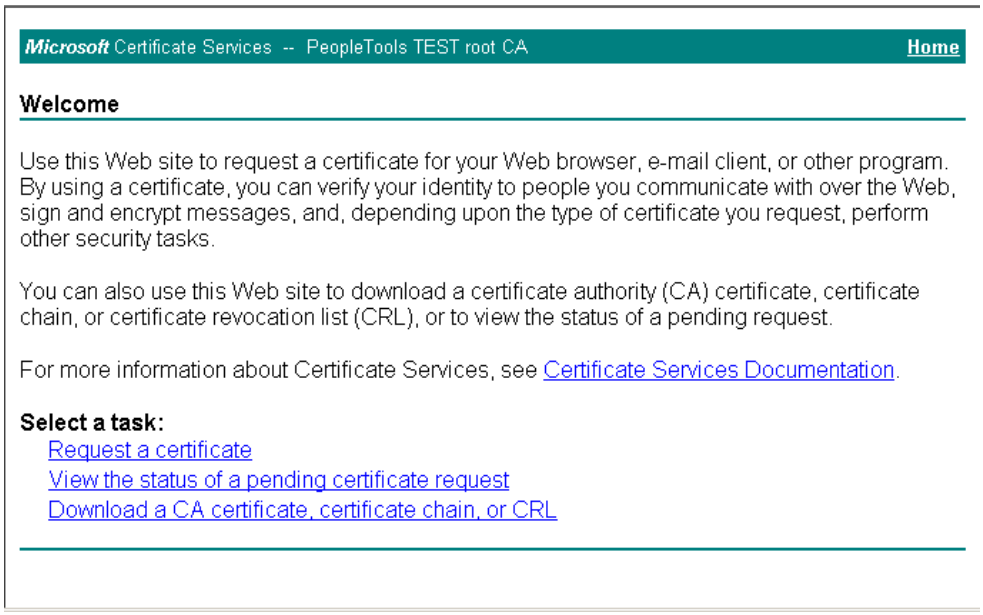
The CSR is a text file, and is written to the <*PSFT_HOME*>\webserv\peoplesoft directory. The file name is <host_name>_certreq.txt.

B.2 Submitting CSRs to CAs for Signing

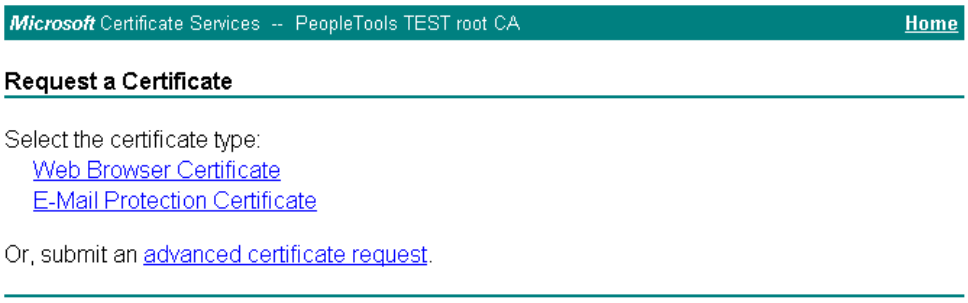
To submit CSRs to CAs for signing:

> **Note:**
>
> The set of pages are different depending on what CA you plan on using.

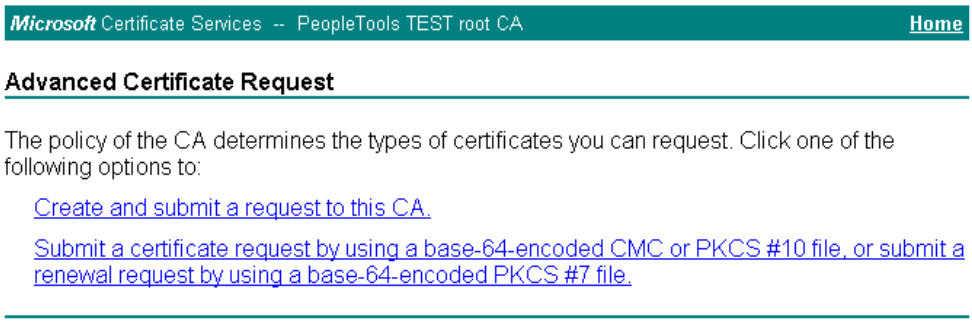
1. Click **Download a CA certificate, certificate chain, or CRL**.



2. Click **advanced certificate request.**

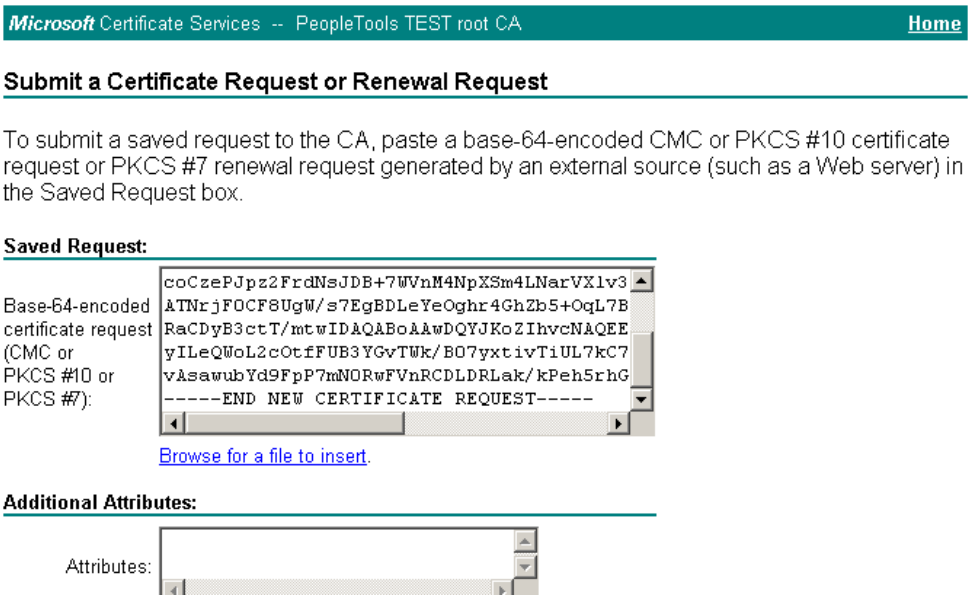


3. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.**



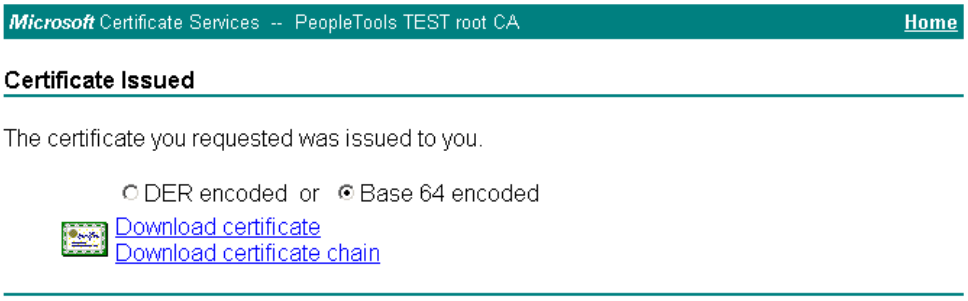
The Submit a Certificate Request or Renewal page appears.

4. Paste the content of the CSR in the **Saved Request** list box.



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.

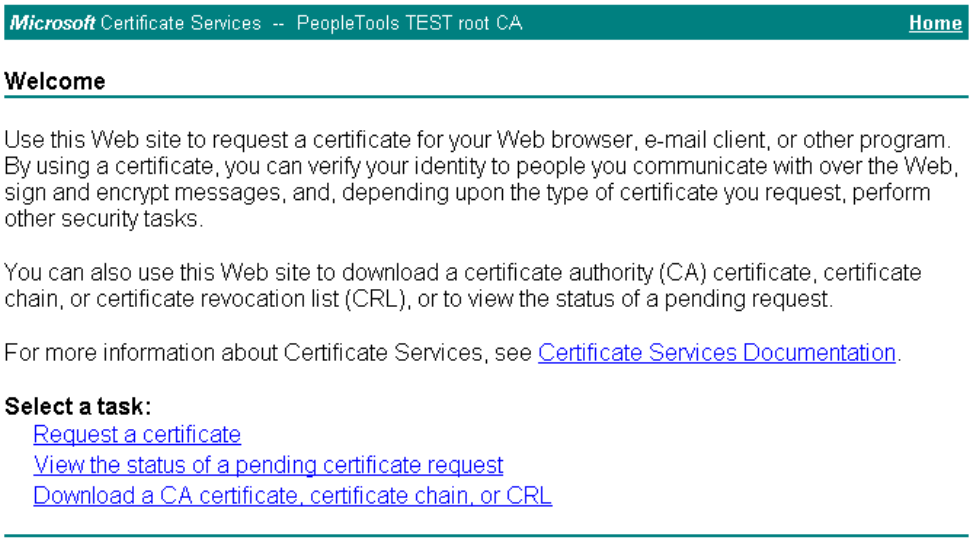
5. Download and save the signed public key on your local drive.



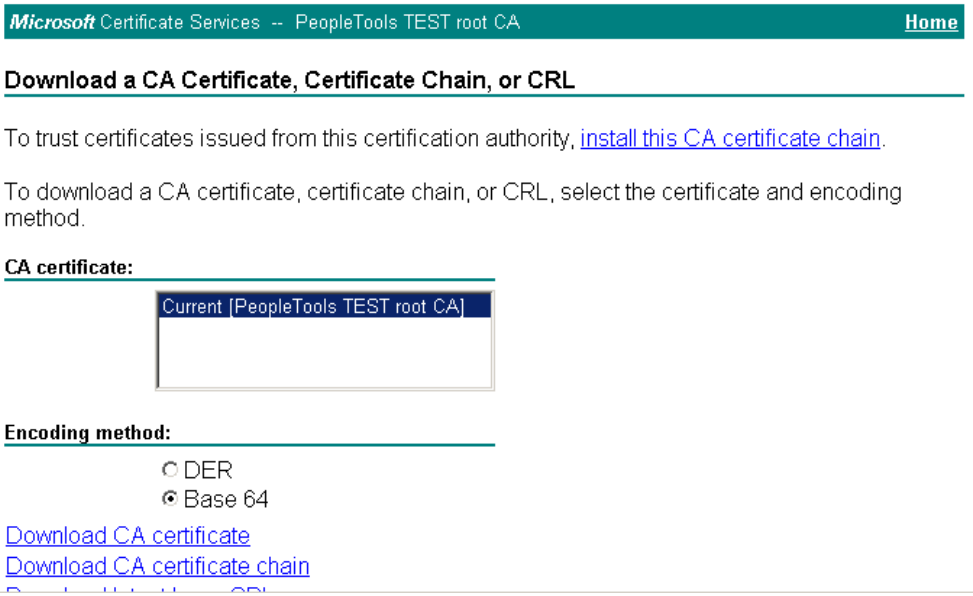
B.3 Downloading the Root Certificate

To download the root certificate:

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



2. From the **CA certificate** list, select the certificate.



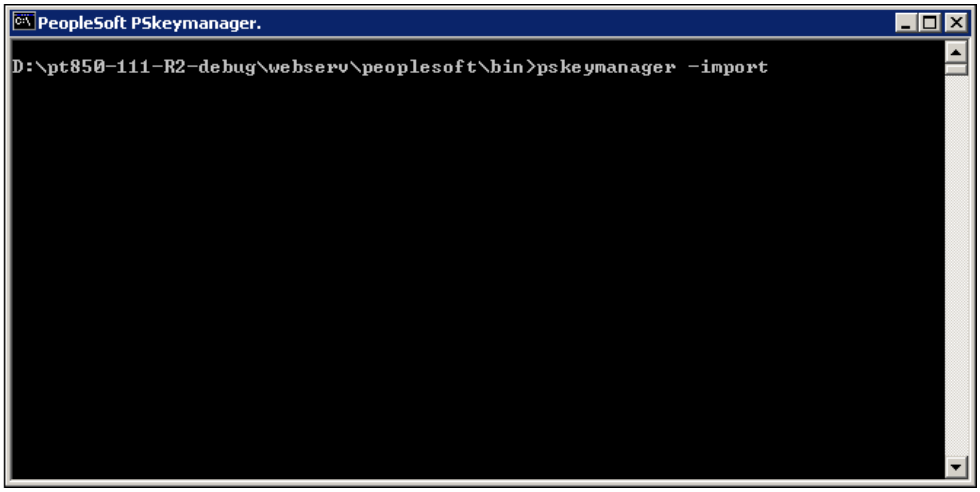
3. Download and save the root certificate on your local drive.

B.4 Importing a Server-Side Public Key into a Keystore

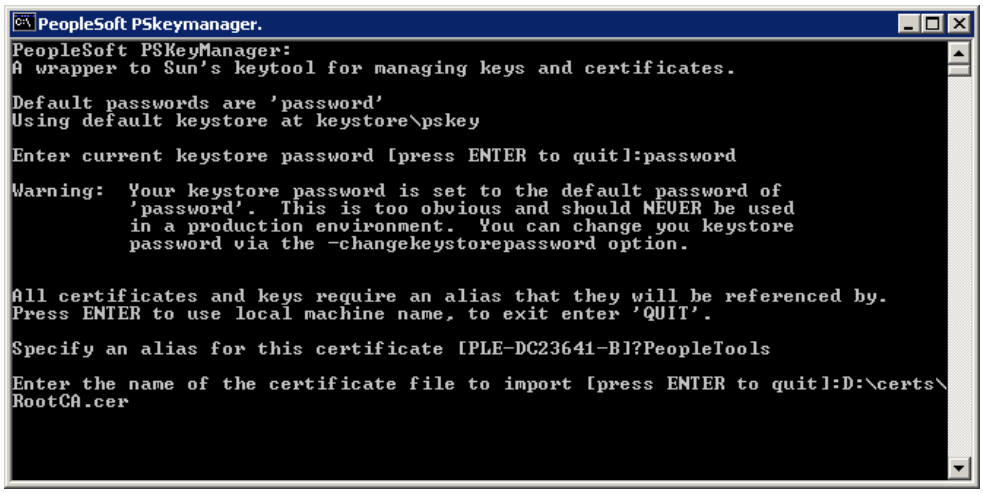
To import a server-side public key into a keystore.

1. Open PSKeyManager.
2. Navigate to the required directory on the MS-DOS command prompt.
3. Enter the following at the command line:

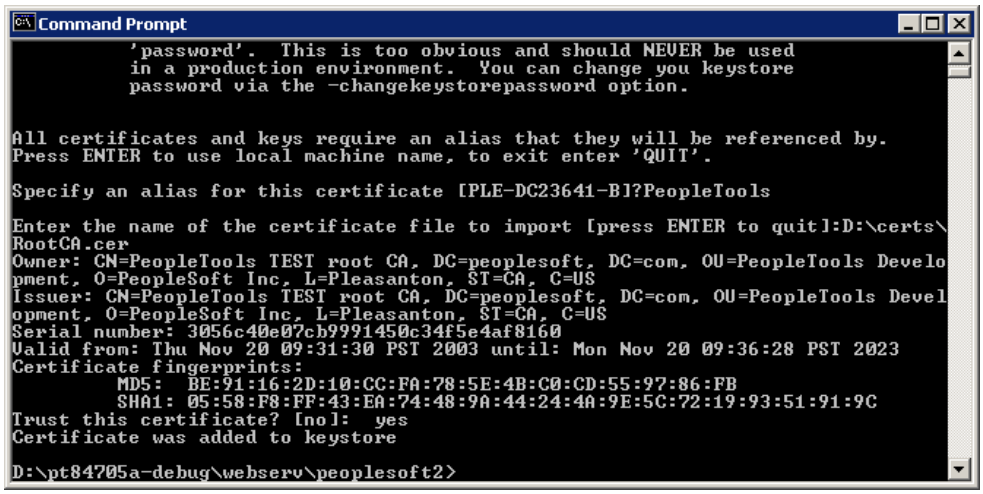
   ```
   pskeymanager -import
   ```



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.**



B.5 Generating and Importing Public Keys

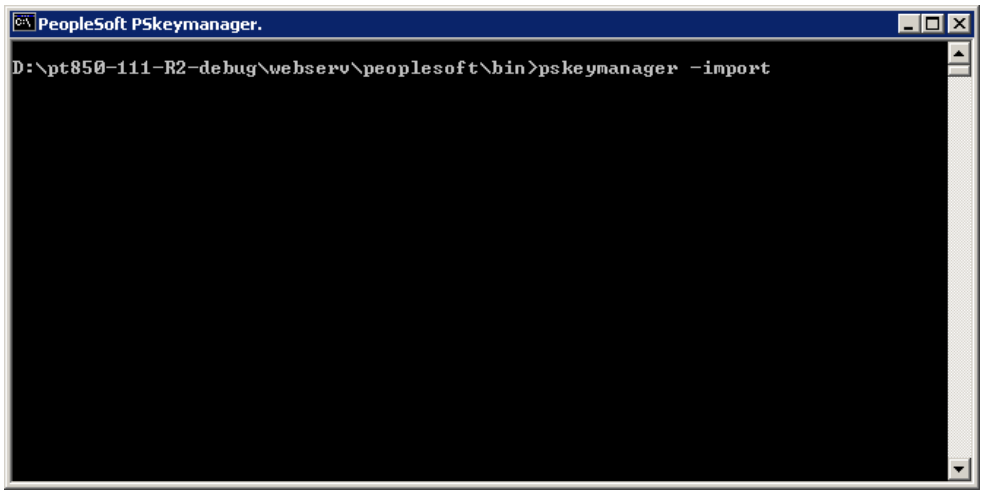
To generate and import public keys:

1. Place the public key from your CA in the keystore. The location of the keystore is as follows:

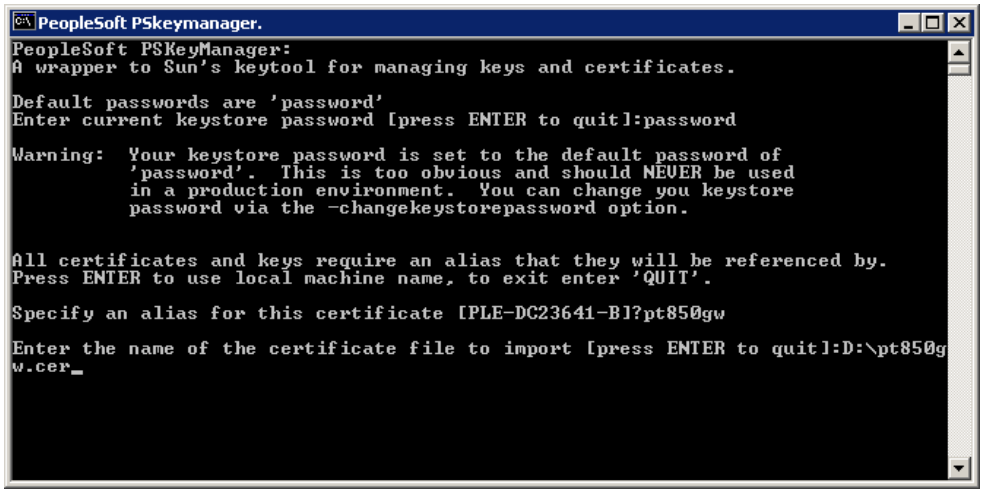
   <*PSFT_HOME*>\webserv\peoplesoft\keystore

2. Install the certificate for server authentication SSL on Oracle WebLogic Server using the following command:

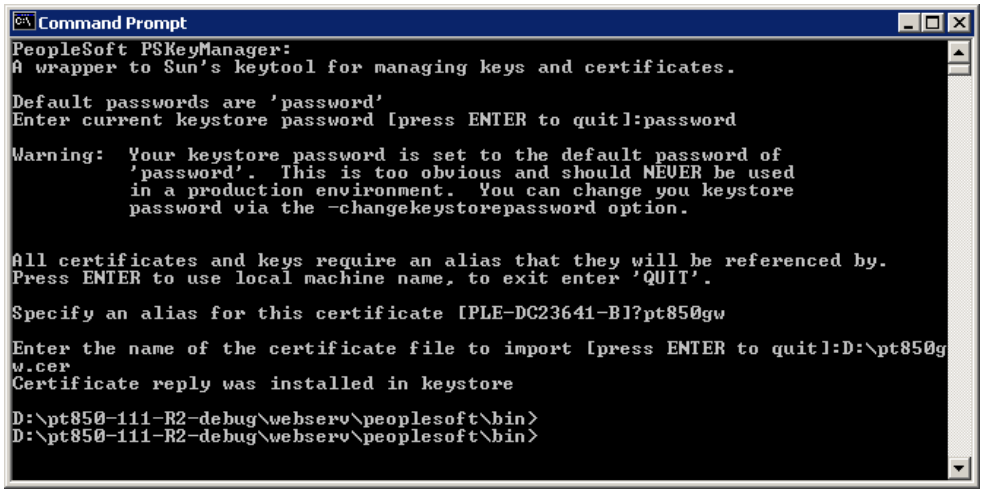
   ```
   pskeymanager -import
   ```



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.



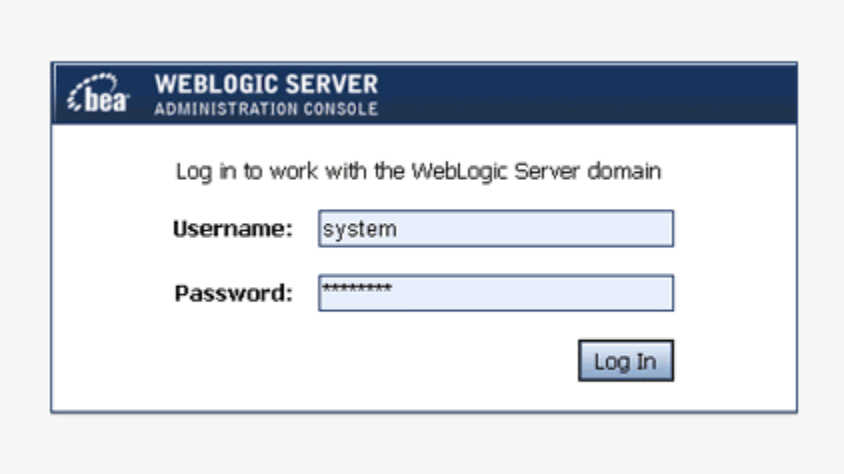
Certificate is successfully installed in the keystore.



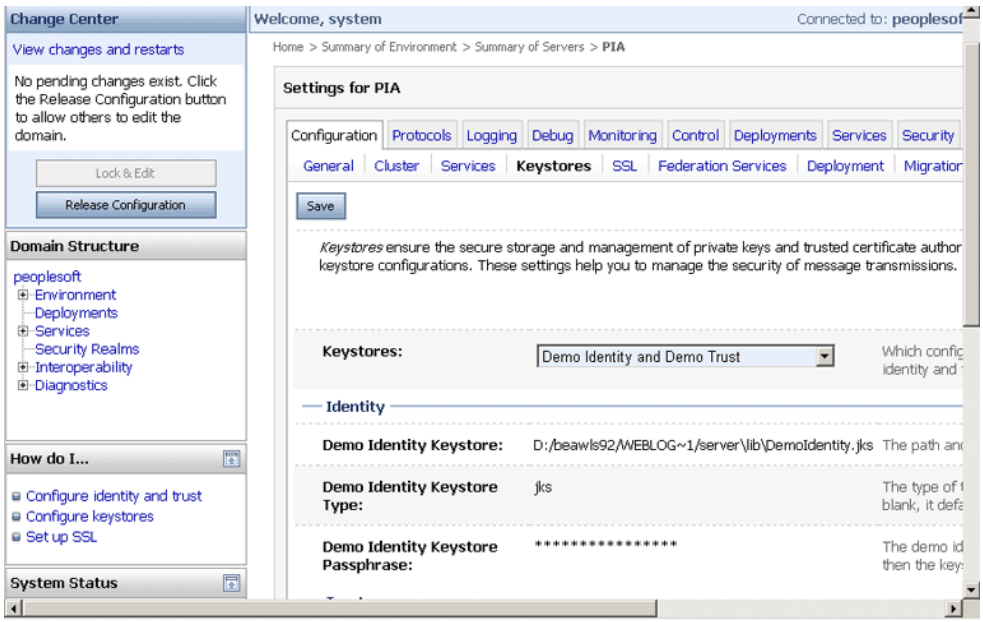
B.6 Configuring Oracle WebLogic Server to Use the Keystore

Configuring the Oracle WebLogic Server to use the keystore:

1. Log in to Oracle WebLogic Administration Console.



2. Expand **PeopleSoft, Environment, Servers, PIA** to setup the SSL configuration for the PIA server.



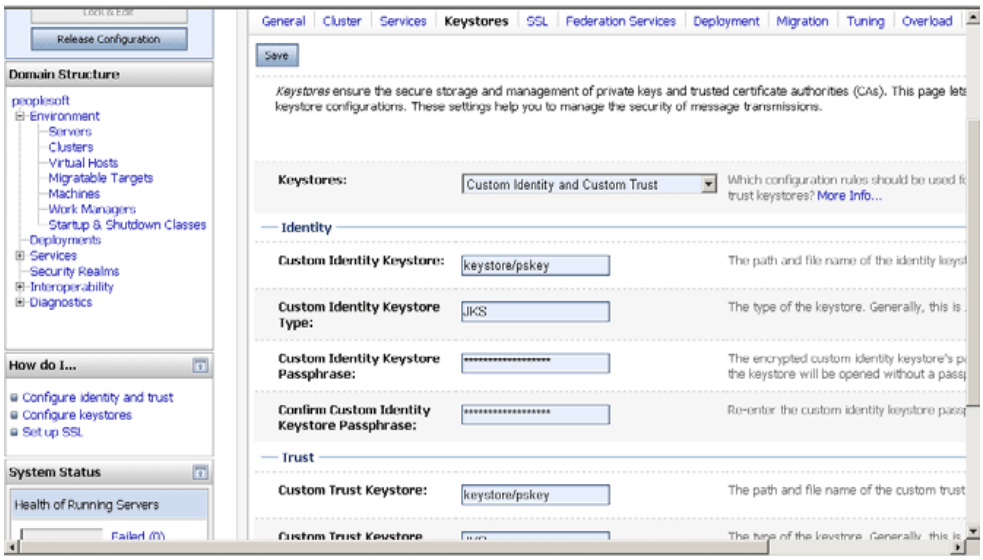
3. Click the **Keystores** tab.
4. From the **Keystores** list, select **Custom Identity and Custom Trust.**
5. In the **Identity** region, complete the following fields:

   - In the Custom Identity Keystore field, enter `keystore/pskey`.

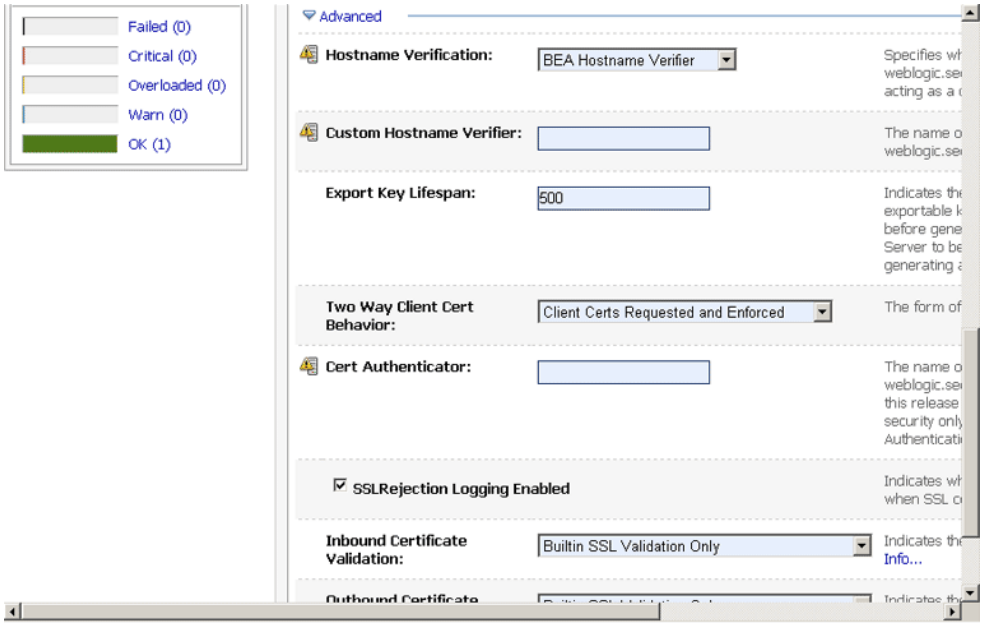
   - In the Custom Identity Keystore Type field, enter `JKS`.

   - In the Custom Identity Keystore Passphrase field, enter `password`.

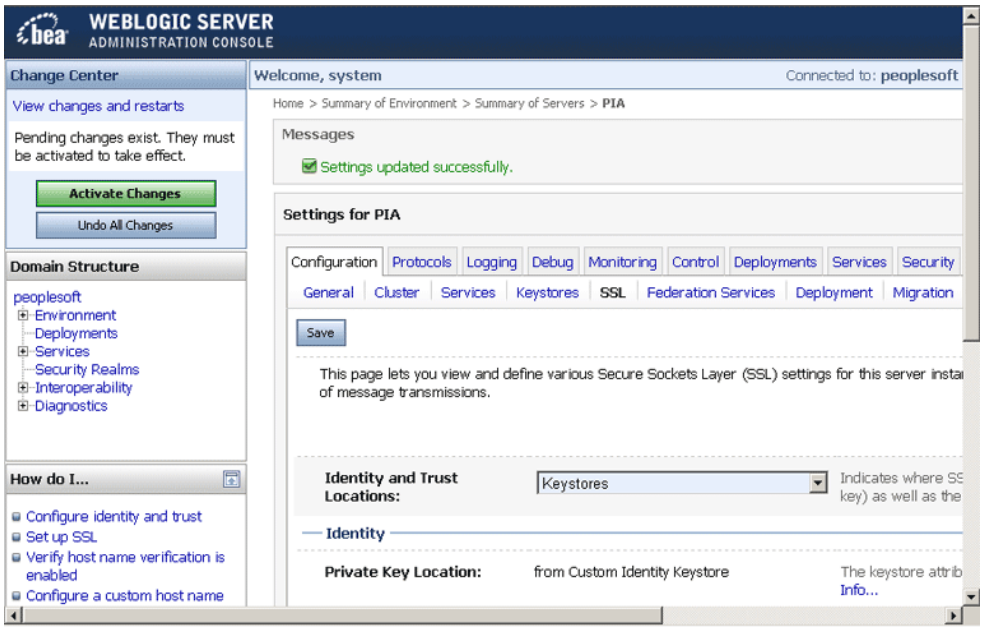
   - In the Confirm Custom Identity Keystore Passphrase field, enter `password` again.



6. On the SSL tab, ensure that the parameter **Two Way Client Cert Behavior** is set to **Client Certs Requested and Enforced.**



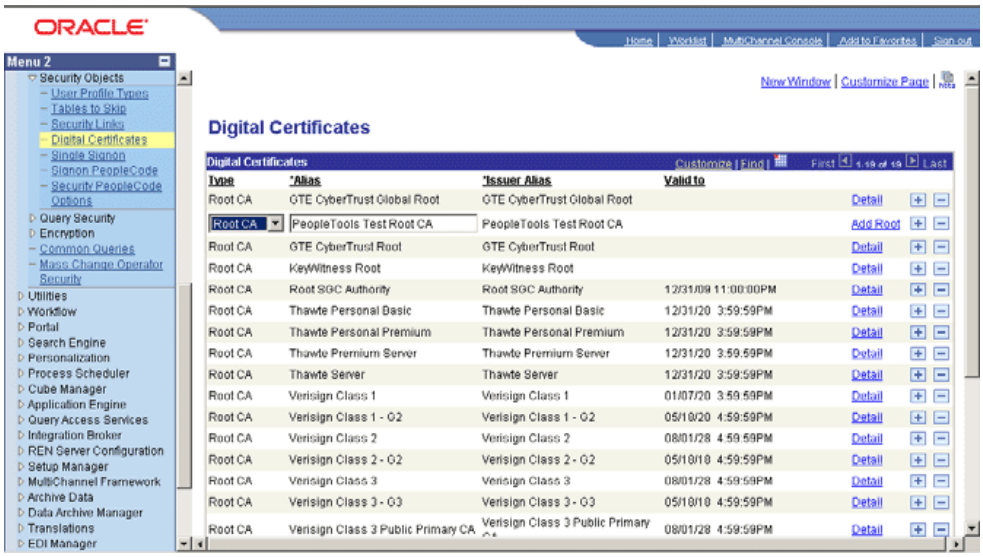
7. Click the **Activate Changes** button.



B.7 Adding the Root Certificate

To add root certificate:

1. Expand **Security, Security Objects,** and then click **Digital Certificates.**



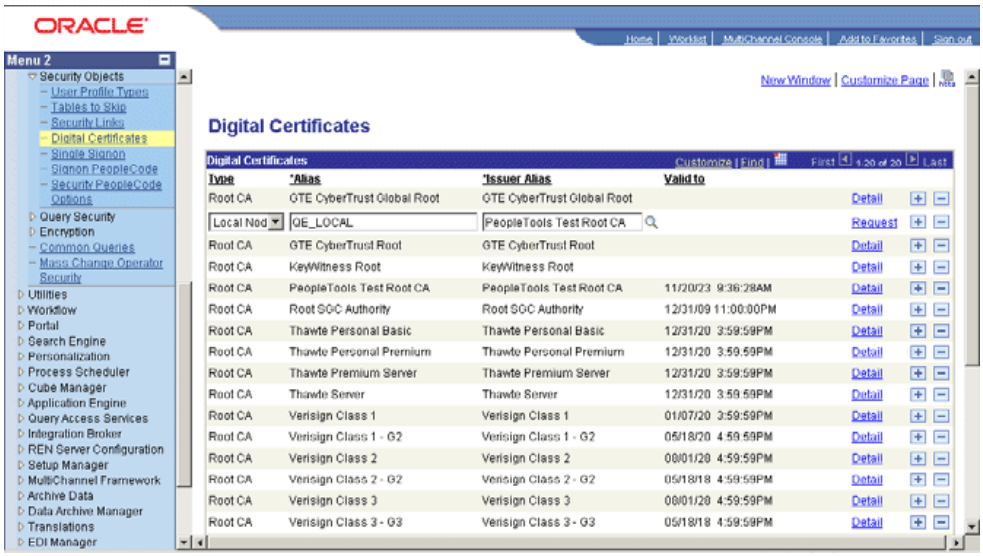
2. Click **Add Root.**

B.8 Configuring the PeopleSoft Certificates

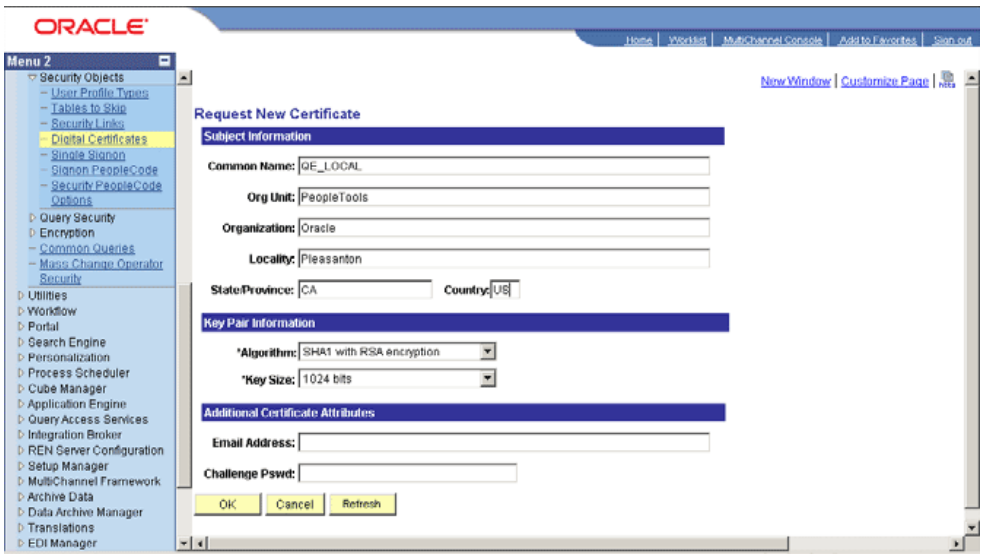
To configure the PeopleSoft certificates:

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

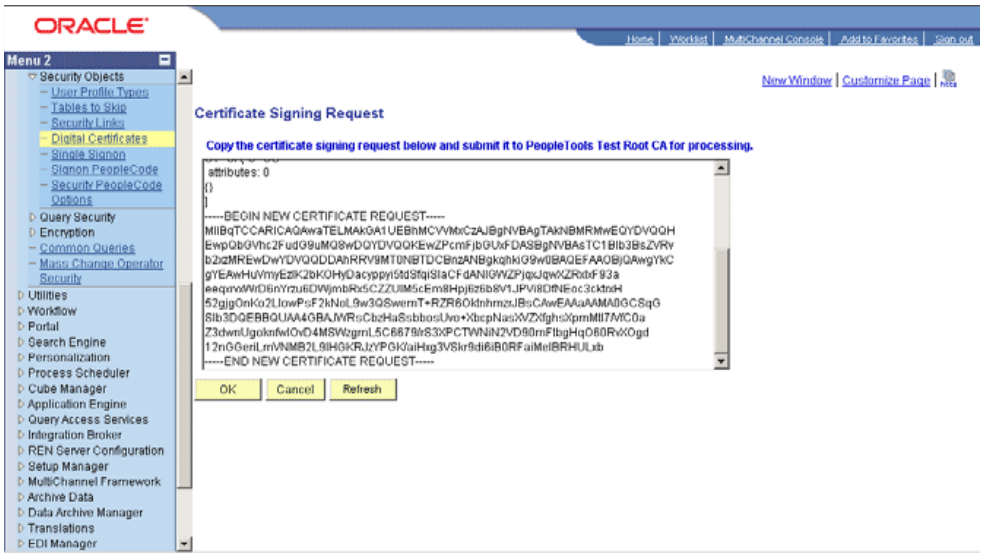
1. Expand **Security, Security Objects,** and then click **Digital Certificates.**
2. Add a local node type certificate.
3. Set **Alias** to the default local node.



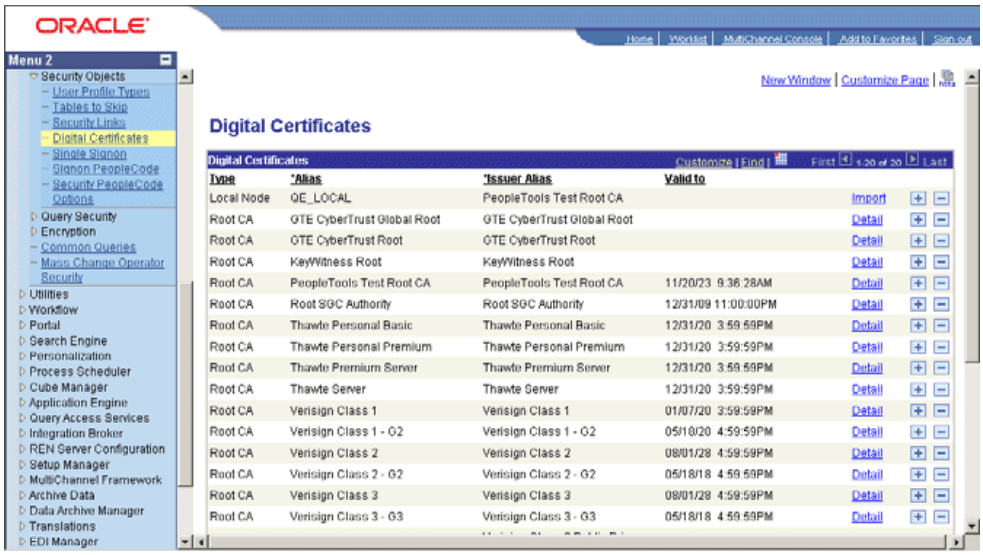
4. Click **Request.**
5. Send this certificate request to the CA to get a new certificate.



6. Click **OK.**

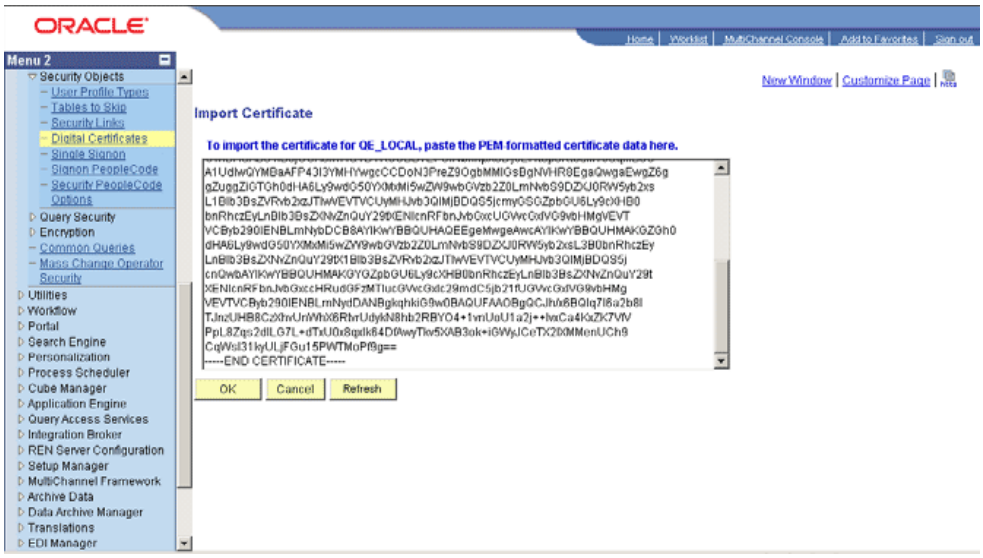


7. Ensure that the local node appears on the Digital Certificates list.

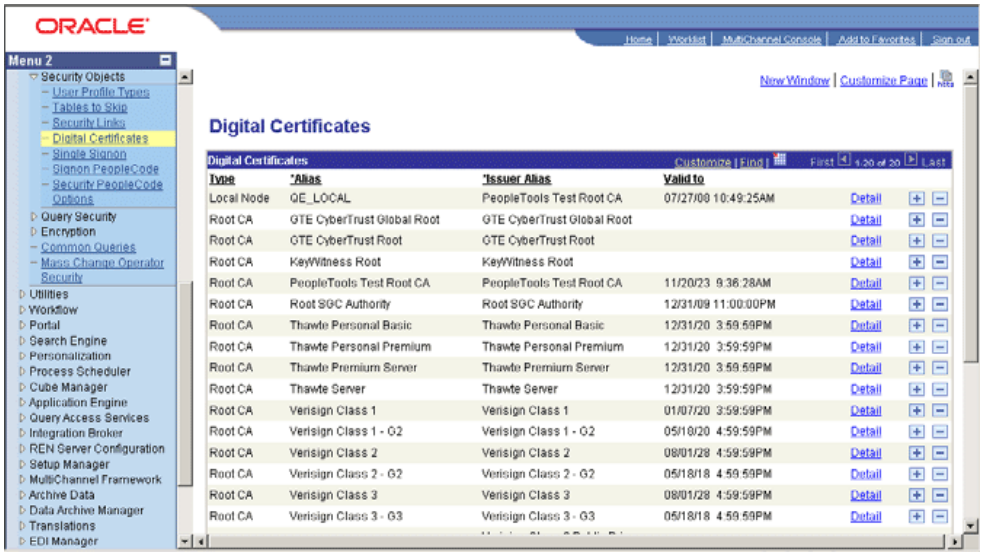


8. Click **Import.**

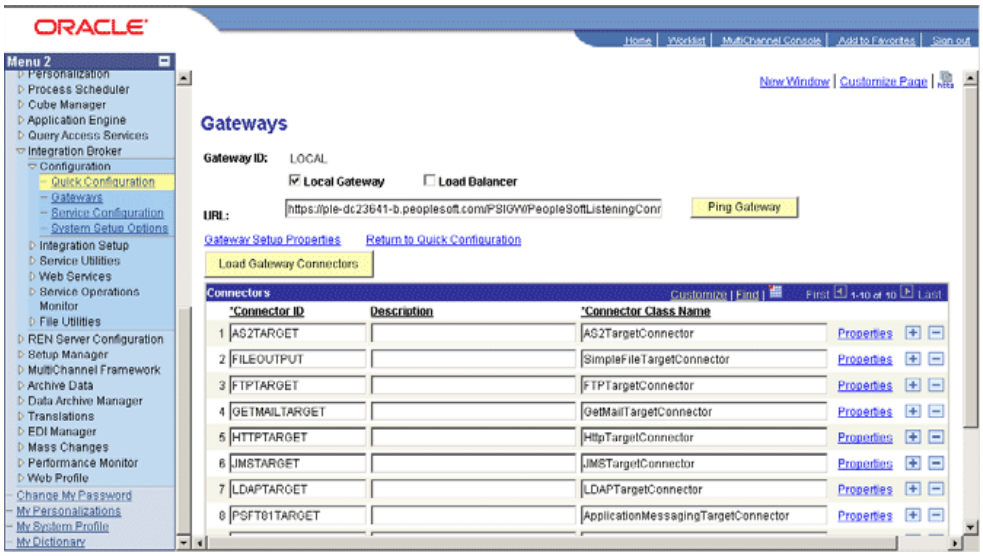
   The Import Certificate page appears.



9. Click **OK.**



10. Click **Load Gateway Connectors.**

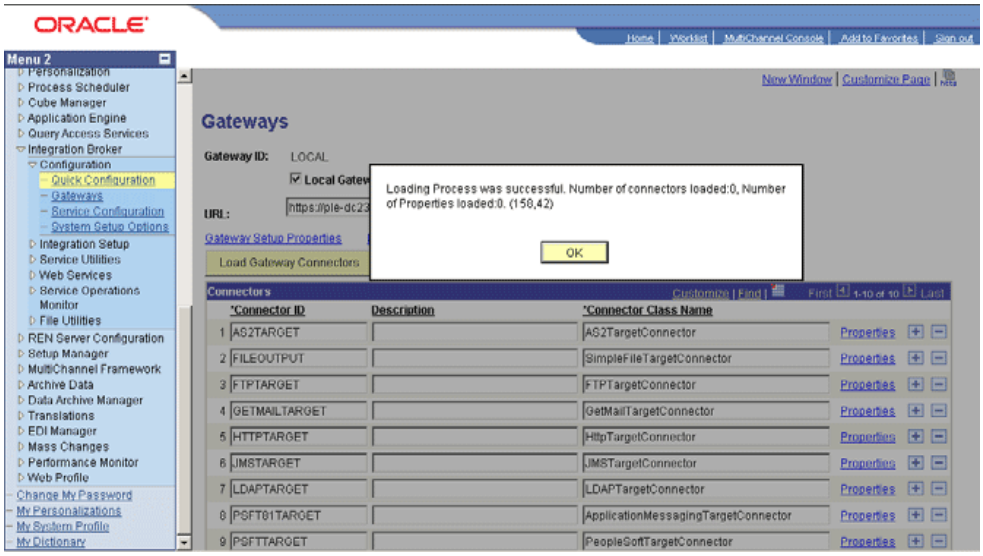


The following message appear:

```
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.



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.