Oracle® Identity Manager

Connector Guide for SAP Employee Reconciliation

Release 9.0.4

E10442-10

April 2010

ORACLE®

Oracle Identity Manager Connector Guide for SAP Employee Reconciliation, Release 9.0.4

E10442-10

Primary Author: Alankrita Prakash

Contributing Authors: Devanshi Mohan, Lyju Vadassery

Contents

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with SAP Employee Reconciliation.

Audience

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

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

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

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

http://www.oracle.com/technology/documentation/oim.html

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

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

This chapter provides an overview of the updates made to the software and documentation for SAP Employee Reconciliation connector in release 9.0.4.8.

> **See Also:** The earlier release of this guide for information about updates that were new for that release

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 sections discuss software updates:

- Software Updates in Release 9.0.4.1
- Software Updates in Releases 9.0.4.2
- Software Updates in Releases 9.0.4.3
- Software Updates in Releases 9.0.4.4
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.6
- Software Updates in Release 9.0.4.7
- Software Updates in Release 9.0.4.8

Software Updates in Release 9.0.4.1

The following are software updates in release 9.0.4.1:

- Changes to the Connector Files on the Installation Media
- Support for Oracle Application Server

Changes to the Connector Files on the Installation Media

There are some changes in the directory structure of the testing utility files. These changes have been made in the "Files and Directories on the Installation Media" section.

Support for Oracle Application Server

In this release, the connector supports Oracle Application Server. Changes related to this software update have been made in the following sections:

- Installing the Security Package section on page 2-12
- Enabling Logging section on page 2-7

From Chapter 5, "Known Issues" on page 5-1, the following item has been removed:

The connector uses the JCO API that supports JDK 1.4 to communicate with SAP Employee Reconciliation. Oracle Identity Manager supports the Oracle Containers for J2EE (OC4J) release that works on JDK 1.5. Therefore, the connector does not support OC4J.

Software Updates in Releases 9.0.4.2

There are no software updates in releases 9.0.4.2.

Software Updates in Releases 9.0.4.3

The following are issues resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
7134299	The employee ID attribute of the target system is mapped to the User ID attribute of the OIM User. If you modified the User ID attribute of an OIM User, then subsequent updates made to the user on the target system were not reconciled.	This issue has been resolved. The `PERSONNEL_NUMBER` attribute has been added to the predefined set of OIM User attributes. The employee ID attribute of the target system is mapped to both the User ID and the `PERSONNEL_NUMBER` attribute. On Oracle Identity Manager, any change made to the User ID attribute is not propagated to the `PERSONNEL_NUMBER` attribute. During reconciliation, the `PERSONNEL_NUMBER` attribute is used to match records fetched from the target system. Therefore, updates made on the target system are successfully reconciled even after you change the value of the User ID attribute.

Software Updates in Releases 9.0.4.4

The following is a software update in release 9.0.4.4:

- Using the Connector Installer

Using the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See "Installing the Connector" on page 2-3 for details.

Software Updates in Release 9.0.4.5

The following are issues resolved in release 9.0.4.5:

Bug Number	Issue	Resolution
7418360	The `java.lang.OutOfMemoryError` exception was encountered if a provisioning operation involved a large number of users.	This issue has been resolved. The connector now supports SAP JCo 3.0. The issue is not encountered when you use SAP custom code files provided along with this version of the SAP JCo. **Note:** SAP JCo 3.0 replaces SAP JCo 2.0 and SAP JCo 2.1. It requires JVM version 1.5 or later, and it is incompatible with earlier versions of SAP JCo. See "Verifying Deployment Requirements" on page 2-1 for information about the required external files.

Software Updates in Release 9.0.4.6

There are no software updates in release 9.0.4.6.

Software Updates in Release 9.0.4.7

There are no software updates in release 9.0.4.7.

Software Updates in Release 9.0.4.8

There are no software updates in release 9.0.4.8.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.7
- Documentation-Specific Updates in Release 9.0.4.8

Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.7

The following documentation-specific updates have been made in releases 9.0.4.1 through 9.0.4.7:

- The connector cannot be used with an Oracle Identity Manager installation on OC4J. This point is mentioned in the "Known Issues" chapter. Instructions to enable logging on OC4J have been removed from the "Enabling Logging" section on page 2-7.
- The following changes have been made in the "Verifying Deployment Requirements" section on page 2-1:

  This section provides information about the permissions to be assigned to the target system user account that Oracle Identity Manager uses to connect to and communicate with the target system. This information has been modified.

  Information about the certified Oracle Identity Manager releases has been modified.

  The JDK requirement has been added.

Documentation-Specific Updates in Release 9.0.4.8

The following is a documentation-specific update that has been made in release 9.0.4.8:

- In the "Multilanguage Support" section, Arabic has been added to the list of languages that the connector supports.
- From this release onward:

The minimum certified release of Oracle Identity Manager is release 9.1.0.1.

The minimum certified release of JDK is release 1.4.2.

See "Verifying Deployment Requirements" section for the complete listing of certified components.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. This guide discusses the procedure to deploy the connector that is used to integrate Oracle Identity Manager with SAP Employee Reconciliation.

Note: Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

This chapter contains the following sections:

- Reconciliation Module
- Supported Functionality
- Multilanguage Support
- Files and Directories on the Installation Media
- Determining the Release Number of the Connector

Note: In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.

At some places in this guide, SAP Employee Reconciliation has been referred to as the *target system*.

1.1 Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. It is an automated process initiated by a scheduled task that you configure.

See Also: The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Concepts Guide* for conceptual information about reconciliation configurations

Based on the type of data reconciled from the target system, reconciliation can be divided into the following types:

- Reconciled SAP Employee Reconciliation Fields

1.1.1 Reconciled SAP Employee Reconciliation Fields

The following fields are reconciled:

- Title
- FirstName
- LastName
- City
- State
- Country
- District
- PostalCode
- TelephoneNumber
- Manager
- StartDate
- EndDate
- Department
- EmailAddress
- EmplUserId
- EmployeeId
- MiddleName
- SSN
- UserLocked
- UserLinked

1.1.2 Reconciled Xellerate User (OIM User) Fields

If trusted source reconciliation is implemented, then the following fields are reconciled:

- User ID
- FirstName
- LastName
- Middle Name
- Organization
- Email
- Employee Type
- User Type
- LinkedUserID
- UserFromHRMS

1.2 Supported Functionality

The following table lists the functions that are available with this connector.

Function	Description
Create User	Creates a user in Oracle Identity Manager
Delete User	Deletes a user in Oracle Identity Manager
Disable User	Disables a user in Oracle Identity Manager
Enable User	Enables a user in Oracle Identity Manager
Update User	Updates a user in Oracle Identity Manager

See Also: Appendix A for information about attribute mappings between Oracle Identity Manager and SAP Employee Reconciliation

1.3 Multilanguage Support

This release of the connector supports the following languages:

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

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

1.4 Files and Directories on the Installation Media

The files and directories on the installation media are listed and described in Table 1–1.

Table 1–1 Files and Directories on the Installation Media

File in the Installation Media	Description
`configuration/SAPHRMS-CI.xml`	This XML file contains configuration information that is used during connector installation.
`BAPI/xlhsapcar.sar`	This file is extracted and the components are deployed on the SAP Employee Reconciliation server for the connector to work with SAP Employee Reconciliation.
`lib/xliSAPHR.jar`	This JAR file contains the class files that are required for reconciliation. During connector deployment, this file is copied into the following directory: *OIM_HOME*`/xellerate/ScheduleTask`
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. During connector deployment, this file is copied into the following directory: *OIM_HOME*`/xellerate/connectorResources` **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/troubleshoot/troubleShootingUtility.class`	This utility is used to test connector functionality.
`test/troubleshoot/global.properties`	This file is used to specify the parameters and settings required to connect to the target system by using the testing utility.
`test/troubleshoot/log.properties`	This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility.
`xml/SAPHRResourceObject.xml`	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ Custom process form ■ Process task and adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules ■ Reconciliation process ■ Lookup definitions
`xml/SAPHRXLResourceObject.xml`	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

Note: The files in the `test` directory are used only to run tests on the connector.

1.5 Determining the Release Number of the Connector

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

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

OIM_HOME/xellerate/ScheduleTask/xliSAPHR.jar

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

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

2

Deploying the Connector

Deploying the connector involves the following steps:

- Verifying Deployment Requirements
- Using External Code Files
- Installing the Connector
- Configuring the Oracle Identity Manager Server
- Configuring the Target System
- Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System

2.1 Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 9.1.0.1 or later **Note:** From release 9.0.4.5 onward, the connector supports SAP JCo 3.0, and SAP JCo 3.0 supports JDK 1.5 and later. Therefore, you must verify that the Oracle Identity Manager and application server combination that you use supports JDK 1.5. See the following Oracle Technology Network page for information about certified configurations of Oracle Identity Manager: `http://www.oracle.com/technology/software/products/ias/files/idm_certification_101401.html`
Target system	The target system can be any one of the following: ■ SAP R/3 4.6C (running on Basis 4.6C) ■ SAP R/3 4.7 (running on WAS 6.20) ■ mySAP ERP 2004 ECC 5.0 (running on WAS 6.40) ■ mySAP ERP 2005 ECC 6.0 (running on WAS 7.00) **Note:** From version 6.40 onward, SAP WAS is also known as "SAP NetWeaver."

Item	Requirement
External Code	The following SAP custom code files: `sapjco3.jar` version 3.0 **Additional file for Microsoft Windows:** `sapjco3.dll` version: 3.0 **Additional file for Solaris and Linux:** `libsapjco3.so` version: 3.0
Target system user account	Oracle Identity Manager uses this user account to connect to and communicate with the target system. For minimum authorization, create a user account and assign the `S_CUS_CMP` profile, `P_ALL` profile, and `SAP_BC_USER_ADMIN` role to it. The User type must be set to `Communication`. This is the default setting for user accounts. If you are not able to find the profiles or role for minimum authorization, then you need to create a user account and assign it to the `SAP_ALL` and `SAP_NEW` groups. These are used for full authorization. You provide the credentials of this user account while configuring the IT resource. The procedure is described later in this guide. If this target system user account is not assigned the specified rights, then the following error message may be displayed during connector operations: `SAP Connection JCO Exception: User TEST_USER has no RFC authorization for function group SYST`
JDK	JDK 1.4.2

2.2 Using External Code Files

Note: In a clustered environment, copy the JAR files and the contents of the `connectorResources` directory to the corresponding directories on each node of the cluster.

To download and copy the external code files to the required locations:

1. Download the SAP Java connector file from the SAP Web site as follows:
   a. Open the following page in a Web browser:
      `https://websmp104.sap-ag.de/connectors`
   b. Open the SAP JAVA Connector page by selecting **Application Platform, Connectivity, Connectors, SAP Java Connector,** and **Tools & Services.**
   c. On the SAP JAVA Connector page, links for files that you can download are displayed on the right pane. Click the link for the SAP JCO release that you want to download.
   d. In the dialog box that is displayed, specify the path of the directory in which you want to save the file.
2. Extract the contents of the file that you download.
3. Copy the `sapjco3.jar` file into the *`OIM_HOME`*`/Xellerate/ThirdParty` directory.
4. Copy the RFC files into the required directory, and then modify the appropriate environment variable so that it includes the path to this directory:

- On Microsoft Windows:

  Copy the `sapjco3.dll` file into the `winnt\system32` directory. Alternatively, you can copy these files into any directory and then add the path to the directory in the `PATH` environment variable.

- On Solaris and Linux:

  Copy the `libsapjco3.so` file into the `/usr/local/jco` directory, and then add the path to this directory in the `LD_LIBRARY_PATH` environment variable.

5. Restart the server for the changes in the environment variable to take effect.

2.3 Installing the Connector

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

Installing the connector involves the following procedures:

- Running the Connector Installer
- Configuring the IT Resource

2.3.1 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console*.
3. Click **Deployment Management**, and then click **Install Connector**.
4. From the Connector List list, select **SAP HRMS *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

   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 **SAP HRMS *RELEASE_NUMBER***.
5. Click **Load**.
6. 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 adapters

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 are 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.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

a. Ensuring that the prerequisites for using the connector are addressed

---

Note: At this stage, run the `PurgeCache` utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-6 for information about running the `PurgeCache` utility.

There are no prerequisites for some predefined connectors.

---

b. Configuring the IT resource for the connector

Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

c. Configuring the scheduled tasks that are created when you installed the connector

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

8. Copy the files from the test directory on the installation media to the following directory:

OIM_HOME`/xellerate/XLIntegrations/saphrms/test`

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

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the `connectorResources` directory into the corresponding directories on each node of the cluster. See "Files and Directories on the Installation Media" on page 1-3 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.3.2 Configuring the IT Resource

You must specify values for the parameters of the `SAP HRMS` IT resource as follows:

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

Parameter	Description	Sample Value
`SAPClient`	SAP client ID	`800`
`SAPHost`	Server address of the target system	`172.20.30.267`
`SAPLanguage`	Language of communication	The default is English (`EN`).
`SAPPassword`	Password to connect to the target system	NA
`SAPSystemNo`	SAP system number	`00`
`SAPType`	SAP system name	`R/3`
`SAPUser`	SAP user ID	`xellerate`
`SAPsnc_mode`	Specifies whether or not SNC is to be used to secure communication between Oracle Identity Manager and the target system The value is 1 if SNC is enabled. Otherwise, it is 0. Other SNC values are required only if this parameter is set to 1. **Note:** It is recommended that you enable SNC to secure communication with the target system.	`0`
`snc_lib`	Location of the SNC library file	`c://usr//sap//sapcrypto.dll`
`snc_myname`	Name of the SNC system	`p:CN=TST, OU=SAP, O=ORA, C=IN`
`snc_partnername`	Name of the partner system, the system on which SAP is installed	`p:CN=I47, OU=SAP, O=ORA, C=IN`
`snc_qop`	This parameter controls the protection level (quality of protection, QOP) at which data is transferred. The default value is 3. Valid values are: ■ `1`: Secure authentication only ■ `2`: Data integrity protection ■ `3`: Data privacy protection ■ `8`: Use value from the parameter ■ `9`: Use maximum value available This is required only if SNC is enabled.	3

Parameter	Description	Sample Value
TimeStamp	For the first trusted source reconciliation run, the time-stamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of reconciliation was completed is stored in this parameter.	The following are sample timestamp values: English: Jun 01, 2006 at 10:00:00 GMT+05:30 French: juin. 01, 2006 at 10:00:00 GMT+05:30 Japanese: 6 01, 2006 at 10:00:00 GMT+05:30
CustomizedReconQuery	Query condition on which reconciliation must be based If you specify a query condition for this parameter, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then do not specify a value for this parameter. The query can be composed with the AND (&) and OR (|) logical operators. For more information about this parameter, refer to the "Partial Reconciliation" section on page 3-1.	firstname=John&lastname=Doe

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

2.4 Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves performing the following procedures:

Note: In a clustered environment, you must perform this step on each node of the cluster. Then, restart each node.

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

2.4.1 Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

You may require the assistance of the system administrator to change to the required input locale.

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

The Connector Installer copies resource bundles into the *OIM_home*/xellerate/connectorResources directory. Whenever you add a new resource bundle in the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

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

   OIM_home/xellerate/bin/*batch_file_name*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

     Note: You can ignore the exception that is thrown when you perform Step 2.

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

   OIM_home/xellerate/config/xlConfig.xml

2.4.3 Enabling Logging

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

- ALL

  This level enables logging for all events.

- DEBUG

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

- INFO

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

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

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

- FATAL

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

- `OFF`

  This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **Oracle WebLogic**

  To enable logging:

  1. Add the following lines in the *OIM_home*`/xellerate/config/log.properties` file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SAPHRMS=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.SAPHRMS=INFO
     ```

  After you enable logging, log information is displayed on the server console.

- **IBM WebSphere**

  To enable logging:

  1. Add the following lines in the *OIM_home*`/xellerate/config/log.properties` file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SAPHRMS=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.SAPHRMS=INFO
     ```

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

  WEBSPHERE_HOME`/AppServer/logs/`*SERVER_NAME*`/SystemOut.log`

- **JBoss Application Server**

  To enable logging:

  1. In the *JBoss_home*`/server/default/conf/log4j.xml` file, add the following lines if they are not already present in the file:

     ```
     <category name="XELLERATE">
        <priority value="log_level"/>
     </category>

     <category name="XL_INTG.SAPHRMS">
        <priority value="log_level"/>
     </category>
     ```

  2. In the second XML code line of each set, replace *log_level* with the log level that you want to set. For example:

```
<category name="XELLERATE">
   <priority value="INFO"/>
</category>

<category name="XL_INTG.SAPHRMS">
   <priority value="INFO"/>
</category>
```

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

JBoss_home/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SAPHRMS=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.SAPHRMS=INFO
     ```

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

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

2.5 Configuring the Target System

This section describes the procedures involved in configuring the target system. You may need the assistance of the SAP Basis administrator to perform some of these procedures.

Configuring the target system involves the following tasks:

- Gathering Required Information
- Creating an Entry in the BAPIF4T Table
- Importing the Request

2.5.1 Gathering Required Information

The following information is required to configure the target system:

Note: During SAP installation, a system number and client number are assigned to the server on which the installation is carried out. These items are mentioned in the following list.

- Login details of an admin user having the permissions required to import requests
- Client number of the server on which the request is to be imported
- System number
- Server IP address

- Server name
- User ID of the account to be used for connecting to the SAP application server
- Password of the account to be used for connecting to the SAP application server

2.5.2 Creating an Entry in the BAPIF4T Table

The User Group field is one of the fields that hold user data in SAP. F4 values are values of a field that you can view and select from a list. You must create an entry in the BAPIF4T table to be able to view F4 values of the User Group field. To create this entry in the BAPIF4T table:

1. Run the SM30 transaction on the SAP system.
2. Enter `BAPIF4T` as the table name, and then click **Maintain**. Ignore any warnings or messages that may be displayed.
3. Click **New Entries**.
4. Enter `XUCLASS` as the data element and `ZXL_PARTNER_BAPI_F4_AUTHORITY` as the function name.

   Note: If an entry already exists for the `XUCLASS` data element, then do not change its value.

5. Save the entry that you create, and then exit.

2.5.3 Importing the Request

You must import the request to create the following custom objects in the SAP system.

Object Type	Object Name
Package	ZXLH
Function Group	ZXLHRCON
Message Class	ZXLHBAPI
Business Object Types	ZXLHEMP
Table	ZBPEMPLOYEES
	ZXLHBAPIMODE
	ZXLHEMPLOYEE
	ZXLHINFO
	ZXLHRECON
	ZXLHSTRING
Program	ZXLHEMP

The `xlhsapcar.sar` file contains the definitions for these objects. When you import the request represented by the contents of the `xlhsapcar.sar` file, these objects are automatically created in SAP. This procedure does not result in any change in the existing configuration of SAP.

Importing the request into SAP involves the following steps:

- Downloading the SAPCAR Utility

- Extracting the Request Files
- Performing the Request Import Operation

2.5.3.1 Downloading the SAPCAR Utility

The two files, Data file and Cofile, that constitute the request are compressed in the `xlhsapcar.sar` file. You can use the SAPCAR utility to extract these files.

To download the SAPCAR utility from the SAP Help Web site:

1. Log on to the SAP Web site at

   `https://service.sap.com/swdc`
2. Click OK to confirm that the certificate displayed is the certificate assigned for your SAP installation.
3. Enter your SAP user name and password to connect to the SAP service marketplace.
4. Click **Downloads**, **SAP Support Packages**, **Entry by Application Group**, and **Additional Components.**
5. Select **SAPCAR, SAPCAR 6.20,** and the operating system. The download object is displayed.
6. Select the **Object** check box, and then click **Add to Download Basket.**
7. Specify the directory in which you want to download the SAPCAR utility. For example: `C:/xlhsapcar`

2.5.3.2 Extracting the Request Files

To extract the Data file and Cofile components of the request:

1. Copy the `xlhsapcar.sar` file into the directory in which you downloaded the SAPCAR utility.

   The `xlhsapcar.sar` file is in the `BAPI` directory inside the installation media directory.
2. In a command window, change to the directory in which you store the SAPCAR utility and the `xlhsapcar.sar` file.
3. Enter the following command to extract the Data file and Cofile components of the request:

   ```
   sapcar -xvf xlhsapcar.sar
   ```

   The format of the extracted files is similar to the following:

   `K900874.I47` (Cofile)

   `R900874.I47` (Data file)

2.5.3.3 Performing the Request Import Operation

To perform the request import operation:

> **Note:** You would need the SAP Basis administrator's assistance to perform the following steps.

1. Copy the Data file and Cofile to the required locations on the SAP server.

2. Import the request into SAP.
3. Check the log file to determine whether or not the import was successful.

   To display the log file:

   a. Run the STMS transaction.

      The list of transport requests is displayed.

   b. Select the transport request number corresponding to the request that you import.

      The transport request number is the same as the numeric part of the Cofile or Data file names. In Step 3 of the preceding procedure, for the sample Cofile (`K900874.I47`) and Data file (`R900874.I47`), the transport request number is `900874`.

   c. Click the log file icon.

      If the return code displayed in the log file is 4, then it indicates that the import ended with warnings. This may happen if the object is overwritten or already exists in the SAP system. If the return code is 8 or a higher number, then there were errors during the import.
4. Confirm the import of the request by running the SE80 transaction and checking the ZXLH package in the ABAP objects.

2.6 Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System

Oracle Identity Manager uses a Java application server. To connect to the SAP system application server, this Java application server uses the Java connector (`sapjco.jar`) and RFC (`librfc32` and `sapjcorfc` files). If required, you can use Secure Network Communication (SNC) to secure such connections.

Note: The Java application server used by Oracle Identity Manager can be IBM WebSphere, Oracle WebLogic, or JBoss Application Server.

This section discusses the following topics:

- Prerequisites for Configuring the Connector to Use SNC
- Installing the Security Package
- Configuring SNC

2.6.1 Prerequisites for Configuring the Connector to Use SNC

The following are prerequisites for configuring the connector to use SNC:

- SNC must be activated on the SAP application server.
- You must be familiar with the SNC infrastructure. You must know which Personal Security Environment (PSE) the application server uses for SNC.

2.6.2 Installing the Security Package

To install the security package on the Java application server used by Oracle Identity Manager:

1. Extract the contents of the SAP Cryptographic Library installation package.

   The SAP Cryptographic Library installation package is available for authorized customers on the SAP Service Marketplace Web site at

   `http://service.sap.com/download`

   This package contains the following files:

   - SAP Cryptographic Library (`sapcrypto.dll` for Microsoft Windows or `libsapcrypto.ext` for UNIX)
   - A corresponding license ticket (`ticket`)
   - The configuration tool, `sapgenpse.exe`

2. Copy the library and the `sapgenpse.exe` file into a local directory. For example: `C:/usr/sap`

3. Check the file permissions. Ensure that the user under which the Java application server runs is able to run the library functions in the directory into which you copy the library and the `sapgenpse.exe` file.

4. Create the `sec` directory inside the directory into which you copy the library and the `sapgenpse.exe` file.

   Note: You can use any names for the directories that you create. However, creating the `C:\usr\sap\sec` (or `/usr/sap/sec`) directory is an SAP recommendation.

5. Copy the ticket file into the `sec` directory. This is also the directory in which the Personal Security Environment (PSE) and credentials of the Java application server are generated.

   See Also: The "Configuring SNC" section on page 2-14

6. Set the `SECUDIR` environment variable for the Java application server user to the `sec` directory.

   Note: From this point onward, the term *SECUDIR directory* is used to refer to the directory whose path is defined in `SECUDIR` environment variable.

   For Oracle Application Server:

   a. Remove the `SECUDIR` entry from the Windows environment variables, if it has been set.

   b. Edit the *`ORACLE_HOME`*`\opmn\config\opmn.xml` file as follows:

      Change the following:

      ```
      <ias-instance id="home.BMPHKTF120" name="home.BMPHKTF120">
        <environment>
          <variable id="TMP" value="C:\DOCUME~1\login user\LOCALS~1\Temp"/>
        </environment>
      ```

      To:

      ```
      <ias-instance id="home.BMPHKTF120" name="home.BMPHKTF120">
      ```

```
<environment>
  <variable id="TMP" value="C:\DOCUME~1\login user\LOCALS~1\Temp"/>
  <variable id="SECUDIR" value="D:\snc\usr\sec"/>
</environment>
```

Note: Oracle Application Server automatically creates the temporary folder based on the operating system of the computer on which it is installed.

c. Restart Oracle Application Server.

7. Set the `SNC_LIB` and PATH environment variables for the user of the Java application server to the cryptographic library directory, which is the parent directory of the `sec` directory.

2.6.3 Configuring SNC

To configure SNC:

1. Either create a PSE or copy the SNC PSE of the SAP application server to the `SECUDIR` directory. To create the SNC PSE for the Java application server, use the `sapgenpse.exe` command-line tool as follows:

   a. To determine the location of the `SECUDIR` directory, run the `sapgenpse` command without specifying any command options. The program displays information such as the library version and the location of the `SECUDIR` directory.

   b. Enter a command similar to the following to create the PSE:

   ```
   sapgenpse get_pse -p PSE_Name -x PIN Distinguished_Name
   ```

   The following is a sample distinguished name:

   ```
   CN=SAPJ2EE, O=MyCompany, C=US
   ```

   The `sapgenpse` command creates a PSE in the `SECUDIR` directory.

2. Create credentials for the Java application server.

   The Java application server must have active credentials at run time to be able to access its PSE. To check whether or not this condition is met, enter the following command in the parent directory of the `SECUDIR` directory:

   ```
   Sapgenpse seclogin
   ```

   Then, enter the following command to open the PSE of the server and create the `credentials.sapgenpse` file:

   ```
   seclogin -p PSE_Name -x PIN -O [NT_Domain\]user_ID
   ```

   The *`user_ID`* that you specify must have administrator rights. *`PSE_NAME`* is the name of the PSE file.

   The credentials file, `cred_v2`, for the user specified with the `-O` option is created in the `SECUDIR` directory.

3. Exchange the public key certificates of the two servers as follows:

Note: If you are using individual PSEs for each certificate of the SAP server, then you must perform this procedure once for each SAP server certificate. This means that the number of times you must perform this procedure is equal to the number of PSEs.

a. Export the Oracle Identity Manager certificate by entering the following command:

```
sapgenpse export_own_cert -o filename.crt -p PSE_Name -x PIN
```

b. Import the Oracle Identity Manager certificate into the SAP application server. You may require the SAP administrator's assistance to perform this step.

c. Export the certificate of the SAP application server. You may require the SAP administrator's assistance to perform this step.

d. Import the SAP application server certificate into Oracle Identity Manager by entering the following command:

```
sapgenpse maintain_pk -a serverCertificatefile.crt -p PSE_Name -x PIN
```

4. Configure the following parameters in the `SAP HRMS` IT resource object:

- `SAPsnc_lib`
- `SAPsnc_mode`
- `SAPsnc_myname`
- `SAPsnc_partnername`
- `SAPsnc_qop`

See Also: Information about parameters of the IT resource given earlier in this chapter

3

Configuring the Connector

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

> **Note:** These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- Configuring Reconciliation
- Configuring the Connector for Multiple Installations of the Target System

3.1 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Partial Reconciliation
- Batched Reconciliation
- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks

3.1.1 Partial Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

For this connector, you create a filter by specifying values for the `CustomizedReconQuery` IT resource parameter while configuring the IT resource. The procedure is described in earlier in this guide.

The following table lists the SAP Employee Reconciliation attributes, and the corresponding Oracle Identity Manager attributes, that you can use to build the query condition. You specify this query condition as the value of the `CustomizedReconQuery` parameter.

Oracle Identity Manager Attribute	SAP Employee Reconciliation Attribute
User ID	userid
First Name	firstname
Last Name	lastname
City	city
State	state
Country	country
District	district
Postalcode	postalcode
Department	department
EmployeeID	employeeID
SSN	ssn
StartDate	startdate
EndDate	enddate

The following are sample query conditions:

- `firstname=John&lastname=Doe`

  With this query condition, records of users whose first name is John and last name is Doe are reconciled.

- `firstname=John&lastname=Doe|district=AcmeCounty`

  With this query condition, records of users who meet either of the following conditions are reconciled:

  – The user's first name is `John` or last name is `Doe`.

  – The user belongs to the `AcmeCounty` district.

If you do not specify values for the `CustomizedReconQuery` parameter, then all the records in the target system are compared with existing Oracle Identity Manager records during reconciliation.

The following are guidelines to be followed while specifying a value for the `CustomizedReconQuery` parameter:

- For the SAP Employee Reconciliation attributes, you must use the same case (uppercase or lowercase) as given in the table shown earlier in this section. This is because the attribute names are case-sensitive.
- 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:

  ```
  firstname=John&lastname=Doe
  ```

  ```
  firstname= John&lastname= 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.

- You must not include special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

Note: An exception is thrown if you include special characters other than the equal sign (=), ampersand (&), and vertical bar (|).

You specify a value for the `CustomizedReconQuery` parameter while configuring the IT resource. The procedure is described later in this guide.

3.1.2 Batched Reconciliation

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

You can configure batched reconciliation to avoid such problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- `StartRecord`: Use this attribute to specify the record number from which batched reconciliation must begin.
- `BatchSize`: Use this attribute to specify the number of records that must be included in each batch.
- `NumberOfBatches`: Use this attribute to specify the total number of batches that must be reconciled. If you do not want to use batched reconciliation, specify `All Available` as the value of this attribute.

Note: If you specify `All Available` as the value of this attribute, then the values of the `StartRecord` and `BatchSize` attributes are ignored.

You specify values for these attributes by following the instructions described in the "Specifying Values for the Scheduled Task Attributes" section on page 3-5.

After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then refer to the log file for information about the batch at which reconciliation has failed.

3.1.3 Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.

- Updates made to each account on the target system are propagated to the corresponding resource.

Note: Skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, `SAPHRXLResourceObject.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.
2. Set the `IsTrustedRecon` scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which is described later in this guide.

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the `SAPHRXLResourceObject.xml` file, which is in the *`OIM_home`*`/xellerate/XLIntegrations/saphrms/xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

After you import the XML file for trusted source reconciliation, you must set the value of the `IsTrustedRecon` reconciliation scheduled task attribute to `True`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-4.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you deploy the connector, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure the scheduled task:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler**.
4. Click **Find**. The details of the predefined scheduled task are displayed.
5. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.

7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 3-5 for information about the values to be specified.

   See Also: *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes
10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.

After you create both scheduled tasks, proceed to the "Configuring the Connector for Multiple Installations of the Target System" section on page 3-7

3.1.4.1 Specifying Values for the Scheduled Task Attributes

You must specify values for the following attributes of the `HR Reconciliation` user reconciliation scheduled task.

Note:

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

Attribute	Description	Default/Sample Value
`Organization`	Default organization assigned to a new user	`Xellerate Users`
`Role`	Default type assigned to a new user	`Consultant`
`Xellerate Type`	Default type assigned to a new user	`End-user administrator`
`ITResource`	Name of the IT resource for setting up a connection with the target system	`SAP HRMS`
`ResourceObject`	Name of the resource object into which users need to be reconciled	`SAP HRMS Resource Object`

Attribute	Description	Default/Sample Value
SAPUserResourceObject	The SAP resource object used to provision Oracle Identity Manager users to the SAP system This is required to get a SAP user ID. **See Also:** Appendix B, "Linking of User Accounts in SAP Employee Reconciliation and SAP User Management"	SAP R3 Resource Object
SAPResourceObjectUserId	Name of the user attribute field for linking an SAP User Management user with an SAP Employee Reconciliation user By using this parameter, you can use the SAP Employee Reconciliation connector to reconcile users created in SAP User Management. Set the value of the parameter to UD_SAPR3_USERID. This is the name of the field that uniquely identifies users created in SAP User Management.	UD_SAPR3_USERID
InfoType	Defines the type of employee data that SAP BAPI forwards to Oracle Identity Manager The value is a comma-separated list of infotypes.	0000,0001
EmpStatus	This value is used and returned by the SAP BAPI as the Active status of the Employee. This depends on the InfoTypeStatus field. If InfoTypeStatus=0001, then EmpStatus=1. If InfoTypeStatus=0000, then EmpStatus=3.	3
InfoTypeStatus	Infotype currently used by SAP BAPI to store the status of employees	0000
StartRecord	The start record for the batching process This attribute is also discussed in the "Batched Reconciliation" section on page 3-3.	1
BatchSize	The number of records that must be there in a batch This attribute is also discussed in the "Batched Reconciliation" section on page 3-3.	3
NumberOfBatches	The number of batches that must be reconciled This attribute is also discussed in the "Batched Reconciliation" section on page 3-3.	Default value: All Available (for reconciling all the users) Sample value: 50
IsTrustedRecon	Specifies whether reconciliation is to be performed in trusted source or target resource (nontrusted source) mode	Specify True if you want to enable trusted source reconciliation. Specify False if you want to enable trusted source (nontrusted source) reconciliation.

After you specify values for these task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

Stopping Reconciliation

Suppose the User Reconciliation Scheduled Task for the connector is running and user records are being reconciled. If you want to stop the reconciliation process:

1. Perform Steps 1 through 4 of the procedure to configure reconciliation scheduled tasks.
2. Select the **Stop Execution** check box in the task scheduler.
3. Click **Save**.

3.2 Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of SAP Employee Reconciliation.

You may want to configure the connector for multiple installations of SAP Employee Reconciliation. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Acme Multinational Inc. have their own installations of SAP Employee Reconciliation. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of SAP Employee Reconciliation.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of SAP Employee Reconciliation.

To configure the connector for multiple installations of the target system:

See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

1. Create and configure one resource object for each target system installation.

   The Resource Objects form is in the Resource Management folder. The `SAP HRMS Resource Object` resource object is created when you import the connector XML file. You can use this resource object as the template for creating the remaining resource objects.

2. Create and configure one IT resource for each resource object.

   The IT Resources form is in the Resource Management folder. The `SAP HRMS` IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

3. Design one process form for each resource object.

   The Form Designer form is in the Development Tools folder. The `UD_SAPHR` process form is created when you import the connector XML file. You can use this process form as a template for creating the remaining process forms.

4. Create and configure one process definition for each resource object.

   The Process Definition form is in the Process Management folder. The `SAP HR Process` process definition is created when you import the connector XML file. You can use this process definition as the template for creating the remaining process definitions.

   While creating process definitions for each target system installation, the following steps that you must perform are specific to the creation of each process definition:

- From the **Object Name** lookup field, select the resource object that you create in Step 1.
- From the **Table Name** lookup field, select the process form that you create in Step 3.
- While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list.

5. Configure reconciliation for each target system installation. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:
   - `ITResource`
   - `ResourceObject`
6. If required, modify the fields to be reconciled for the Xellerate User resource object.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the SAP Employee Reconciliation installation to which you want to provision the user.

4

Testing and Troubleshooting

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

- Running Test Cases
- Troubleshooting

4.1 Running Test Cases

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

To use the testing utility for testing reconciliation:

1. Specify the required values in the `global.properties` file.

   This file is in the *OIM_home*`/xellerate/XLIntegrations/saphrms/test/troubleshoot` directory. The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
SAP HRMS Server Parameters	Parameters required to connect to SAP Employee Reconciliation For information about the values that you must provide, refer to the description of the IT resource parameters. This is covered earlier in this guide.
Reconciliation Parameters	Date from which modified data is to be reconciled The To Date value is taken as the current date and time.

2. Add the following to the `CLASSPATH` environment variable:

   OIM_home`/xellerate/ext/log4j-1.2.8.jar`
   OIM_home`/Xellerate/ScheduleTask/xliSAPHR.jar`
   OIM_home`/xellerate/lib/xlLogger.jar`
   OIM_home`/xellerate/lib/xlUtils.jar`
   OIM_home`/Xellerate/ThirdParty/sapjco.jar`

3. Create an ASCII-format copy of the `global.properties` file as follows:

   Note: You must perform this procedure every time you make a change in the contents of the `global.properties` file.

   a. In a command window, change to the following directory:

OIM_home/Xellerate/XLIntegrations/saphrms/test/troubleshoot

b. Enter the following command:

```
native2ascii global.properties troubleshoot.properties
```

The `troubleshoot.properties` file is created when you run the `native2ascii` command. The contents of this file are an ASCII-format copy of the contents of the `global.properties` file.

4. Enter the following command to test reconciliation:

```
java
-DTproperties=OIM_home/xellerate/XLIntegrations/saphrms/test/troubleshoot/troub
leshoot.properties
-Dlog4j.configuration=file:/OIM_home/xellerate/XLIntegrations/saphrms/test/trou
bleshoot/log.properties troubleShootingUtility R
```

4.1.1 Testing Partial Reconciliation

To test query-based reconciliation, you can specify the following types of query conditions as values for the `CustomizedReconQuery` parameter:

- Simple queries with user attributes

  Value assigned to the `CustomizedReconQuery` parameter: `firstname=John`

  The users with first name John are reconciled.

- Queries with '&' and '|' logical operators
  - Value assigend to the CustomizedReconQuery parameter: `employeeid=E001|firstname=John`

    The users with employee id `E001` and users with first name `John` are reconciled.
  - Value assigned to the `CustomizedReconQuery` parameter: `firstname=John&lastname=Doe`

    Only the users with first name `John` and last name `Doe` are reconciled.
- Queries with time stamps
  - Value assigned to the `CustomizedReconQuery` parameter: None

    Value of the `TimeStamp` parameter: `Nov 3, 2006 at 10:00:00 GMT+05:30`

    The users that matches the time stamp value are reconciled.
  - Value assigned to the `CustomizedReconQuery` parameter: `firstname=John`

    Value of the `TimeStamp` parameter: `Nov 3, 2006 at 10:00:00 GMT+05:30`

    The users with first name `John` and who matches the time stamp value are reconciled.

4.1.2 Testing Batched Reconciliation

You can test reconciliation based on batching and data paging of user records by specifying values for the following user reconciliation scheduled task attributes:

- If you set the value of `StartRecord` to `1`, `BatchSize` to `0`, and `NumberOfBatches` to `All Available`, then all the users are reconciled.
- If you set the value of `StartRecord` to `1`, `BatchSize` to `5`, and `NumberOfBatches` to `50`, then all the users starting from record 1 are reconciled in 50 batches, with 5 records in each batch.
- If you set the value of `StartRecord` to `200`, `BatchSize` to `5`, and `NumberOfBatches` to `50`, then all the users starting from record 200 are reconciled in 50 batches, with 5 records in each batch.

The results of batching are displayed in the logger file, which is located in the following path:

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

In this file, you can view the batch numbers, the user ids of the users that are reconciled, and whether the reconciliation is successful or not.

4.2 Troubleshooting

The following sections provide solutions to some commonly encountered problems associated with the connector:

- Connection Errors
- Common SNC Errors

4.2.1 Connection Errors

The following table provides solutions to common connection errors.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to SAP Employee Reconciliation. **Returned Error Message:** Connection error encountered **Returned Error Code:** `INVALID_CONNECTION_ERROR`	▪ Ensure that SAP Employee Reconciliation is running. ▪ Ensure that Oracle Identity Manager is running (that is, the database is running). ▪ Ensure that all the adapters have been compiled. ▪ Examine the Oracle Identity Manager record (from the IT Resources form). Ensure that the IP address, admin ID, and admin password are correct.
Authentication error **Returned Error Message:** Invalid or incorrect password **Returned Error Code:** `AUTHENTICATION_ERROR`	Ensure that the specified SAP connection user ID and password are correct.

4.2.2 Common SNC Errors

The following table provides a solution to an SNC error.

Problem Descriptions	Solution

Trying to connect to SAP through SNC.
Returned Error Message:
SAP Connection JCO Exception
Returned Error Code:
SNC required for this connection
	Ensure that values for the following IT resource parameters are correctly specified as shown in the following example:
	`SAPsnc_mode: 1`
	`SAPsnc_myname: p:CN=win2003, OU=SAP, O=ORA, C=IN`
	`SAPsnc_qop: 3`
	`SAPsnc_partnername: p:CN=I47, OU=SAP, O=ORA, C=IN`
	`SAPsnc_lib: C://usr//sap//sapcrypto.dll`

5

Known Issues

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

- **Bug 7255041**

  During SAP Employee Reconciliation configuration, you must decide which infotypes and which fields in infotypes need to be recorded. The connector tracks the following infotypes: 0000, 0001, 0002, 0006, and 0105. These infotypes must be recorded at the time of SAP HRMS configuration.

- **Bug 7255024**

  Suppose an employee account is created in SAP Employee Reconciliation and then reconciled to Oracle Identity Manager. Next, you provision a user on SAP User Management through Oracle Identity Manager. You then link the user account on SAP User Management with the SAP Employee Reconciliation employee account. During the next reconciliation run, the link between the employee account and the user account is reflected in Oracle Identity Manager.

  However, if you do not reconcile the SAP Employee Reconciliation employee account to Oracle Identity Manager before you link the employee account and the user account on SAP, then the link will not be reflected in Oracle Identity Manager during the next reconciliation run.

- **Bug 8213548**

  The connector does not reconcile event dates because it does not differentiate between hire, terminate, and transfer events contained in the infotype 0000.

A

Attribute Mappings Between Oracle Identity Manager and SAP Employee Reconciliation

The following table discusses attribute mappings between Oracle Identity Manager and SAP Employee Reconciliation.

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

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

Oracle Identity Manager Attribute	SAP Employee Reconciliation Attribute	Description
UserId	PERNR	Personnel number
FirstName	VORNA	First name
LastName	NACHN	Last name
City	ORT01	City
State	STATE	State
Country	LAND1	Country
District	ORT02	District
PostalCode	PSTLZ	Postal code for the district
TelephoneNumber	TELNR	Telephone number
Manager	MSTBR	Manager
StartDate	BEGDA	Joining date
EndDate	ENDDA	Retirement date
Department	ORGEH	Department
EmplUserId	USRID	Linked user ID for the SAP HRMS employee

Oracle Identity Manager Attribute	SAP Employee Reconciliation Attribute	Description
EmailId	USRID_LONG	E-mail address
EmployeeId	PERNR	Personnel number
MiddleName	MIDNM	Middle name
UserTitle	ANRLT	Title
SSN	PERID	Social security number
EmpStatus	STAT2	Status

B

Linking of User Accounts in SAP Employee Reconciliation and SAP User Management

SAP provides a feature that enables you to link employee records in SAP Employee Reconciliation with user records in SAP User Management. This appendix discusses the use cases arising out of the interaction of Oracle Identity Manager with the SAP system in the context of this link between SAP Employee Reconciliation and SAP User Management.

Note:

The information provided in this appendix is based on the scenario in which SAP Employee Reconciliation is configured as the trusted source for reconciliation and SAP User Management is configured as a target resource.

For the sake of simplicity, the following acronyms have been used in this appendix:

- SAP Employee Reconciliation is referred to as `SAP HR`.
- SAP User Management is referred to as `SAP UM`.

The link between SAP HR and SAP UM is implemented by the Infotype 105 field, which is one of the fields of the SAP HR record. This infotype stores the user ID assigned to the user in SAP UM. The following example illustrates how this infotype implements the link between SAP HR and SAP UM records:

Suppose you create an account for user `John Doe` in SAP HR and assign the employee ID `jdoe`. You also create an account for this user in SAP UM and assign the user ID `jdoe2`. When you create a link between SAP HR and SAP UM for `John Doe`, the Infotype 105 field of the SAP HR record stores the SAP UM user ID, `jdoe2`, of the user. The value of the Infotype 105 field enables the SAP system to link employee account `jdoe` with user account `jdoe2`.

Oracle Identity Manager uses the USR_UDF_LINKED_USER_ID field to track the relationship between an employee account on SAP HR and a user account on SAP UM. In other words, the function of the USR_UDF_LINKED_USER_ID field in Oracle Identity Manager is the same as the function of the Infotype 105 field in SAP.

The events that occur during a provisioning or reconciliation operation depend on whether or not the Infotype 105 field is used to link records in SAP HR and SAP UM and on the order in which reconciliation and provisioning are carried out. The following sections discuss use cases arising from these conditions:

B.1 Use Case 1: SAP HR and SAP UM Records Are Linked

This use case discusses the events that occur when SAP HR and SAP UM records are linked. The following example describes these events.

The following are the initial conditions:

1. You have created an employee account for user `John Doe` in SAP HR. The employee ID is `jdoe`.
2. You have also created a user account for user `John Doe` in SAP UM. The user ID is `jdoe2`.
3. You have linked the employee record to the user record in the SAP system. This means that the Infotype 105 field of the SAP HR record stores the user ID, `jdoe2`.
4. There is no account for user `John Doe` in Oracle Identity Manager.

The following events are the outcome of these initial conditions:

1. During trusted source reconciliation with SAP HR, the SAP HR record for user `John Doe` is created in Oracle Identity Manager. The USR_UDF_LINKED_USER_ID field of Oracle Identity Manager is used to store the contents of the Infotype 105 field. In this case, the value stored is `jdoe2`, which is the user ID of the SAP UM record for user `John Doe`.
2. The next event that occurs depends on whether you perform provisioning or reconciliation with SAP UM, after trusted source reconciliation with SAP HR:
   - You use Oracle Identity Manager to perform a provisioning operation for `John Doe` on SAP UM.

     Oracle Identity Manager uses the value (`jdoe2`) of the USR_UDF_LINKED_USER_ID field to establish a match with the corresponding SAP UM record. The resource object for user ID `jdoe2` is created in Oracle Identity Manager and updated in SAP UM.
   - You use Oracle Identity Manager to perform a reconciliation operation for John Doe on SAP UM.

     The SAP UM user ID is `jdoe2`. The same value is stored in the USR_UDF_LINKED_USER_ID field. By comparing the SAP UM user ID with the USR_UDF_LINKED_USER_ID field value, the reconciliation engine establishes a match between the user record in Oracle Identity Manager and the SAP UM record.

Note: If there is a link between SAP HR and SAP UM records, then the reconciliation rule that compares the USR_UDF_LINKED_USER_ID field value with the SAP UM user ID takes precedence over the reconciliation rule that compares the Oracle Identity Manager user ID with the SAP UM user ID.

B.2 Use Case 2: No Link Exists Between SAP HR and SAP UM Records

This use case discusses the events that occur when there is no link between SAP HR and SAP UM records. The following example describes these events.

The following are the initial conditions:

1. You have created an employee account for user `John Doe` in SAP HR. The employee ID is `jdoe`.
2. You have also created a user account for user John Doe in SAP UM. The user ID is `jdoe2`.
3. You have not linked the employee record to the user record in the SAP system. This means that the Infotype 105 field of the SAP HR record in empty.
4. There is no account for user `John Doe` in Oracle Identity Manager.

The following events are the outcome of these initial conditions:

1. During trusted source reconciliation with SAP HR, the SAP HR record for user `John Doe` is created in Oracle Identity Manager. The USR_UDF_LINKED_USER_ID field of Oracle Identity Manager is used to store the contents of the Infotype 105 field. In this case, nothing is stored in the USR_UDF_LINKED_USER_ID field because the Infotype 105 field is empty.
2. The next event that occurs depends on whether you perform provisioning or reconciliation with SAP UM, after trusted source reconciliation with SAP HR:
   - You use Oracle Identity Manager to perform a provisioning operation for `John Doe` on SAP UM.

     Oracle Identity Manager cannot determine that the `jdoe2` account in SAP UM and the `jdoe` account in Oracle Identity Manager represent the same user. Therefore, a new account is created in SAP UM with the user ID `jdoe`.

     If you had assigned the same user ID (for example, `jdoe`) to the employee account in SAP HR and the user account in SAP UM, then the provisioning operation would fail because the User Already Exists error is encountered.
   - You use Oracle Identity Manager to perform a reconciliation operation for John Doe on SAP UM.

     There is no link between the SAP HR and SAP UM accounts, and the SAP UM record has not been created on Oracle Identity Manager. Therefore, target resource reconciliation with SAP UM cannot take place.

Note: As mentioned in the preceding section, the reconciliation rule that compares the USR_UDF_LINKED_USER_ID field value with the SAP UM user ID takes precedence over the reconciliation rule that compares the Oracle Identity Manager user ID with the SAP UM user ID.

In a scenario in which there is no link between SAP HR and SAP UM, you can create a custom reconciliation rule that would override all other reconciliation rules. For example, you can create a reconciliation rule that maps e-mail addresses in OIM User accounts to SAP UM user IDs.

Refer to *Oracle Identity Manager Design Console Guide* for information about creating reconciliation rule

---

Index

P

R

S

T

U

X