

**Oracle® Identity Manager**

Connector Guide for SAP Employee Reconciliation

Release 9.0.2

**B32171-01**

September 2006

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

---

---

# Contents

<b>Preface</b> .....	v
Audience .....	v
Documentation Accessibility .....	v
Related Documents .....	vi
Documentation Updates .....	vii
Conventions .....	vii
<b>What's New in the Oracle Identity Manager Connector for SAP Employee Reconciliation?</b> .....	ix
Software Updates .....	ix
Documentation-Specific Updates.....	x
<b>1 About the Connector</b>	
<b>Supported Functionality</b> .....	1-1
<b>Multilanguage Support</b> .....	1-1
<b>Reconciliation Module</b> .....	1-2
Reconciled SAP Employee Reconciliation Fields .....	1-2
Reconciled Xellerate User Fields.....	1-2
<b>Files and Directories That Comprise the Connector</b> .....	1-3
<b>Determining the Release Number of the Connector</b> .....	1-4
<b>2 Deploying the Connector</b>	
<b>Step 1: Verifying Deployment Requirements</b> .....	2-1
<b>Step 2: Copying the Connector Files and External Code</b> .....	2-2
<b>Step 3: Configuring the Oracle Identity Manager Server</b> .....	2-3
Changing to the Required Input Locale.....	2-3
Clearing Content Related to Connector Resource Bundles from the Server Cache .....	2-4
<b>Step 4: Configuring the Target System</b> .....	2-4
Gathering Required Information .....	2-4
Creating an Entry in the BAPIF4T Table .....	2-5
Importing the Request.....	2-5
Downloading the SAPCAR Utility .....	2-6
Extracting the Request Files .....	2-6
Performing the Request Import Operation .....	2-7
<b>Step 5: Importing the Connector XML File</b> .....	2-7

Defining IT Resources .....	2-8
<b>Step 6: Configuring Reconciliation.....</b>	<b>2-9</b>
Configuring Trusted Source Reconciliation .....	2-9
Creating the Reconciliation Scheduled Tasks .....	2-10
Specifying Values for the Scheduled Task Attributes .....	2-11
<b>Step 7: Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System .....</b>	<b>2-12</b>
Prerequisites for Configuring the Connector to Use SNC .....	2-12
Installing the Security Package .....	2-13
Configuring SNC.....	2-13
<b>Configuring the Connector for Multiple Installations of the Target System .....</b>	<b>2-15</b>

### **3 Testing and Troubleshooting**

Running Test Cases .....	3-1
<b>Troubleshooting.....</b>	<b>3-2</b>
Connection Errors .....	3-2
Common SNC Errors.....	3-3

### **4 Known Issues**

#### **A Attribute Mappings Between Oracle Identity Manager and SAP Employee Reconciliation**

#### **Index**

---

---

# Preface

*Oracle Identity Manager Connector Guide for SAP Employee Reconciliation* provides information about integrating Oracle Identity Manager with SAP Employee Reconciliation.

---

---

**Note:** Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

---

---

## Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for SAP Employee Reconciliation.

## Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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.

## TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

## Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Connector Guide for BMC Remedy User Management*
- *Oracle Identity Manager Connector Guide for CA-ACF2 Advanced*
- *Oracle Identity Manager Connector Guide for CA-Top Secret Advanced*
- *Oracle Identity Manager Connector Guide for Database Application Tables*
- *Oracle Identity Manager Connector Guide for Database User Management*
- *Oracle Identity Manager Connector Guide for IBM RACF*
- *Oracle Identity Manager Connector Guide for IBM RACF Advanced*
- *Oracle Identity Manager Connector Guide for IBM Lotus Notes and Domino*
- *Oracle Identity Manager Connector Guide for Microsoft Active Directory*
- *Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide*
- *Oracle Identity Manager Connector Guide for Microsoft Exchange 2000 and 2003*
- *Oracle Identity Manager Connector Guide for Microsoft Exchange 5.5*
- *Oracle Identity Manager Connector Guide for Microsoft Windows 2000*
- *Oracle Identity Manager Connector Guide for Microsoft Windows NT 4.0*
- *Oracle Identity Manager Connector Guide for Novell eDirectory*
- *Oracle Identity Manager Connector Guide for Novell GroupWise*
- *Oracle Identity Manager Connector Guide for Oracle e-Business Employee Reconciliation*
- *Oracle Identity Manager Connector Guide for Oracle e-Business User Management*
- *Oracle Identity Manager Connector Guide for Oracle Internet Directory*
- *Oracle Identity Manager Connector Guide for PeopleSoft Employee Reconciliation*

- *Oracle Identity Manager Connector Guide for PeopleSoft User Management*
- *Oracle Identity Manager Connector Guide for Siebel Enterprise Applications*
- *Oracle Identity Manager Connector Guide for RSA Authentication Manager*
- *Oracle Identity Manager Connector Guide for RSA ClearTrust*
- *Oracle Identity Manager Connector Guide for SAP CUA*
- *Oracle Identity Manager Connector Guide for SAP Employee Reconciliation*
- *Oracle Identity Manager Connector Guide for SAP Enterprise Portal*
- *Oracle Identity Manager Connector Guide for SAP User Management*
- *Oracle Identity Manager Connector Guide for Sun Java System Directory*
- *Oracle Identity Manager Connector Guide for UNIX SSH*
- *Oracle Identity Manager Connector Guide for UNIX Telnet*

## Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.2 connector documentation set, visit Oracle Technology Network at

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

## Conventions

The following text conventions are used in this document:

<b>Convention</b>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	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 SAP Employee Reconciliation?

This chapter provides an overview of the updates made to the connector and documentation for SAP Employee Reconciliation in release 9.0.2 of the Oracle Identity Manager connector pack.

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

- [Software Updates](#)

These include updates made to the connector software.

- [Documentation-Specific Updates](#)

These include major changes made to the connector documentation. These changes are not related to software updates.

**See Also:** *Oracle Identity Manager Release Notes*

## Software Updates

This section discusses the following software updates implemented in this release of the connector.

### **Incorporation of Multilanguage Support**

In addition to English, this release of the connector supports the French and Japanese languages. The following are documentation updates pertaining to the incorporation of this feature:

- The installation media directory includes resource bundle files for the languages supported by the connector. These resource bundle files are described in the "[Files and Directories That Comprise the Connector](#)" section on page 1-3.
- The "[Step 2: Copying the Connector Files and External Code](#)" section on page 2-2 provides the destination directory into which you must copy the resource bundle files during the deployment procedure.
- The "[Step 3: Configuring the Oracle Identity Manager Server](#)" section on page 2-3 describes the procedure to change to the required input locale and to clear content related to connector resource bundles from the server cache.

- A new IT resource parameter has been added to carry language code information to the target system. This parameter is described in the ["Defining IT Resources"](#) section on page 2-8.
- Changes have been made in the procedure described in the ["Running Test Cases"](#) section on page 3-1 to accommodate the multilanguage support feature.
- [Chapter 4, "Known Issues"](#) discusses a new issue related to the use of non-English locales.

### **Determining the Release Number of the Connector**

Instructions to determine the release number of the connector are given in the ["Determining the Release Number of the Connector"](#) section on page 1-4.

### **External Code Files are Not Bundled in the Connector Installation Media Directory**

The `sapjco.jar` file is not bundled with the rest of the connector files on the installation media directory. Instead, instructions to download this file are provided in the ["Step 2: Copying the Connector Files and External Code"](#) on page 2-2.

### **Changes in the Known Issues List**

The following items have been removed from the Known Issues list in [Chapter 4](#):

- The issue about correctly specifying the `Recon Key` parameter value
- The issue about mentioning the name of the resource object in the scheduled task definition

## **Documentation-Specific Updates**

The following documentation-specific updates have been made in this release of the guide:

- In the ["Supported Functionality"](#) section on page 1-1, the descriptions of some of the functions have been reworded.
- In the ["Step 1: Verifying Deployment Requirements"](#) section on page 2-1, the "External code" requirement has been broken down into requirements for Microsoft Windows and UNIX systems.
- Instructions to configure SAP Employee Reconciliation have been reworded in the ["Step 1: Verifying Deployment Requirements"](#) section on page 2-1.
- Instructions to copy the connector JAR files to all the nodes of a clustered environment have been added in the following sections:
  - [Step 2: Copying the Connector Files and External Code](#) section on page 2-2
  - [Step 3: Configuring the Oracle Identity Manager Server](#) on page 2-3
- Instructions and pointers to information about configuring trusted source reconciliation have been moved to the ["Configuring Trusted Source Reconciliation"](#) section on page 2-9.
- Changes in the attributes listed in the ["Specifying Values for the Scheduled Task Attributes"](#) section on page 2-11:

The `Server` parameter has been removed.

The following parameters have been added:

- `ReconKey`

- SAPUserResourceObject
- SAPResourceObjectUserId
- FirstTimeReconRecords
- InfoType
- EmpStatus
- InfoTypeStatus
- RecordLimit
- Instructions in the "[Step 7: Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System](#)" section on page 2-12 have been reworded.
- Instructions to use Oracle Identity Manager for linking multiple installations of SAP Employee Reconciliation are given in the "[Configuring the Connector for Multiple Installations of the Target System](#)" section on page 2-15.
- [Appendix A](#) provides information about attribute mappings between Oracle Identity Manager and SAP Employee Reconciliation.
- The "Supported Platforms" section has been removed.



---

---

## 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. The connector for SAP Employee Reconciliation 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:

- [Supported Functionality](#)
- [Multilanguage Support](#)
- [Reconciliation Module](#)
- [Files and Directories That Comprise the Connector](#)
- [Determining the Release Number of the Connector](#)

### Supported Functionality

The following table lists the reconciliation functions supported by the 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

### Multilanguage Support

In addition to English, this release of the connector supports the following languages:

- French
- Japanese

## Reconciliation Module

This section discusses the elements that the reconciliation module extracts from the target system to construct reconciliation event records.

### Reconciled SAP Employee Reconciliation Fields

The following fields are reconciled:

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

### Reconciled Xellerate User Fields

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

- UserID
- Password
- Organization
- FirstName

- LastName
- Xellerate
- Role
- EmailAddress
- EmployeeId
- UserLinked
- MiddleName

## Files and Directories That Comprise the Connector

The files and directories that comprise the connector are compressed in the following ZIP file on the installation media:

Enterprise Applications\SAP Enterprise Applications\SAP Employee Reconciliation  
Rev 3.2.0.zip

These files and directories are listed in the following table.

File in the Installation Media	Description
xml\SAPHRResourceObject.xml	This XML file contains definitions for the following components of the connector: <ul style="list-style-type: none"> <li>■ IT resource type</li> <li>■ Custom process form</li> <li>■ Process task and adapters (along with their mappings)</li> <li>■ Resource object</li> <li>■ Provisioning process</li> <li>■ Pre-populate rules</li> <li>■ Reconciliation process</li> <li>■ Lookup definitions</li> </ul>
xml\SAPHRXLResourceObject.xml	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.
lib\xliSAPHR.jar	This JAR file contains the class files that are required for reconciliation.
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.
Files in the resources directory	Each of these files contains locale-specific information that is used by the connector.
troubleshoot\TroubleShootingUtility.class	This utility is used to test connector functionality.
troubleshoot\global.properties	This file is used to specify the parameters and settings required to connect to the target system by using the troubleshooting utility.
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 troubleshooting utility.
docs\B32171_01.pdf	This guide, which provides instructions to deploy the connector.

---

---

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

---

---

The "[Step 2: Copying the Connector Files and External Code](#)" section on page 2-2 provides instructions to copy these files into the required directories.

## Determining the Release Number of the Connector

You can determine the release number of the connector at any of the following stages:

### Before Deployment

To determine the release number of the connector before you deploy it:

1. Extract the contents of the `xliSAPHR.jar` file. This file is in the `lib` directory inside the installation media directory.
2. Open the `manifest.mf` file in a text editor, which 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.

---

---

**Note:** If you maintain a copy of the `xliSAPHR.jar` file after deployment, you can use this method to determine the release number of the connector at any stage. However, after you deploy the connector, it is recommended that you use the [After Deployment](#) method.

---

---

### During Deployment

To determine the release number of the connector while deploying the connector, refer to Step 4 of the procedure described in the "[Step 5: Importing the Connector XML File](#)" section on page 2-7.

### After Deployment

To determine the release number of the connector after deploying the connector:

**See Also:** *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. In the Form Designer, open the process form. The release number of the connector is the value of the `Version` field.

---



---

## Deploying the Connector

Deploying the connector involves the following steps:

- [Step 1: Verifying Deployment Requirements](#)
- [Step 2: Copying the Connector Files and External Code](#)
- [Step 3: Configuring the Oracle Identity Manager Server](#)
- [Step 4: Configuring the Target System](#)
- [Step 5: Importing the Connector XML File](#)
- [Step 6: Configuring Reconciliation](#)
- [Step 7: Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System](#)

If you want to configure the connector for multiple installations of SAP Employee Reconciliation, then perform the following procedure:

- [Configuring the Connector for Multiple Installations of the Target System](#)

### Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target system	SAP R3 4.7
External Code	<p>The following SAP custom code files:</p> <p>sapjco.jar</p> <p><b>For Microsoft Windows:</b></p> <p>sapjcorfc.dll librfc32.dll</p> <p>Version: 2.0.10</p> <p><b>For Solaris and Linux:</b></p> <p>libsapjcorfc.so librfccm.so</p> <p>Version: 2.0.10</p>

Item	Requirement
Target system user account	<p>Create a user account, and assign it to the SAP_ALL group.</p> <p>You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-8.</p>

## Step 2: Copying the Connector Files and External Code

The connector files to be copied and the directories to which you must copy them are given in the following table.

**Note:** The directory paths given in the first column of this table correspond to the location of the connector files in the following ZIP file on the installation media:

Enterprise Applications\SAP Enterprise Applications\SAP Employee Reconciliation Rev 3.2.0.zip

Refer to the "Files and Directories That Comprise the Connector" section on page 1-3 for more information about these files.

File in the Installation Media	Destination
Files in the xml directory	<i>OIM_home</i> \xellerate\XLIntegrations\saphrms\xml
Files in the lib directory	<i>OIM_home</i> \xellerate\JavaTasks
BAPI\xlhsapcar.sar	<p>This file can be copied to any location on the target system. For example:</p> <p>C:\xlhsapcar\</p> <p>Refer to the "Extracting the Request Files" section on page 2-6 for more information.</p>
Files in the resources directory	<i>OIM_home</i> \xellerate\connectorResources
Files in the troubleshoot directory	<i>OIM_home</i> \xellerate\XLIntegrations\saphrms\tro ubleshoot
docs\B32171_01.pdf	<i>OIM_home</i> \xellerate\docs\saphrms

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 `sapjco.jar` file into the `OIM_home\Xellerate\JavaTasks` 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 `librfccm.dll` and `libsapjcorfc.dll` files 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 `librfccm.so` and `libsapjcorfc.so` files 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.

---

**Note:** While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the `connectorResources` directory and the JAR files to the corresponding directories on each node of the cluster.

---

## Step 3: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves 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](#)

### Changing to the Required Input Locale

Changing to the required input locale involves installing the required fonts and setting the required input locale.

To set the required input locale:

---

**Note:** Depending on the operating system used, you may need to perform this procedure differently.

---

1. Open Control Panel.
2. Double-click **Regional Options**.

3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

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

Whenever you add a new resource bundle file in the `OIM_home\xellerate\connectorResources` directory or make a change in an existing resource bundle file, 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.
2. Enter one of the following commands:

---

---

**Note:** You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:

```
OIM_home\xellerate\bin\batch_file_name
```

---

---

- On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

- On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

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
```

---

---

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

---

---

## Step 4: 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](#)

### 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 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

## 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.

## 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
Program	ZXLHEMP
Business Object Types	ZXLHEMP
Table	ZXLHBAPIMODE
	ZXLHEMPLYEE
	ZXLHINFO
	ZXLHRECON

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](#)

### Downloading the SAPCAR Utility

The two files, Data file and Cofile, that constitute the request are compressed in the `xlhsapcar.sar`. 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`

### 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 download 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:

```
K900208.I46 (Cofile)
```

```
R900208.I46 (Data file)
```

## 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 (R900208.I46) and Data file (R900208.I46), the transport request number is 900208.

- 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.

## Step 5: Importing the Connector XML File

To import the connector XML file into Oracle Identity Manager:

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 locating files is displayed.
4. Locate and open the `SAPHRResourceObject.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.

---



---

**Note:** The connector version is also displayed on this page.

---



---

5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next**. The Provide IT Resource Instance Data page for the SAP HRMS IT resource is displayed.

8. Specify values for the parameters of the SAP HRMS IT resource. Refer to the table in the ["Defining IT Resources"](#) section on page 2-8 for information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the SAP HRMS IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

**See Also:** If you want to define another IT resource, then refer to *Oracle Identity Manager Tools Reference Guide* for instructions.

11. Click **View Selections**.

The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. Remove these nodes by right-clicking each node and then selecting **Remove**.

12. Click **Import**. The connector XML file is imported into Oracle Identity Manager.

After you import the connector XML file, proceed to the ["Step 6: Configuring Reconciliation"](#) section on page 2-9.

## Defining IT Resources

You must specify values for the SAP HRMS IT resource parameters listed in the following table.

Parameter	Description	Sample Value
SAPClient	Port number to connect to the target system	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	R3
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.	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_partnertype	Name of the partner system, the system on which SAP is installed	p:CN=I47, OU=SAP, O=ORA, C=IN

Parameter	Description	Sample Value
snc_qop	<p>This parameter controls the protection level (quality of protection, QOP) at which data is transferred. The default value is 3. Valid values are:</p> <ul style="list-style-type: none"> <li>▪ 1: Secure authentication only</li> <li>▪ 2: Data integrity protection</li> <li>▪ 3: Data privacy protection</li> <li>▪ 8: Use value from the parameter</li> <li>▪ 9: Use maximum value available</li> </ul> <p>This is required only if SNC is enabled.</p>	3
TimeStamp	<p>For the first reconciliation run, the timestamp 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.</p>	<p>The following are sample timestamp values:</p> <p>English: Jun 01, 2006 at 10:00:00 GMT+05:30</p> <p>French: juin. 01, 2006 at 10:00:00 GMT+05:30</p> <p>Japanese: 6 01, 2006 at 10:00:00 GMT+05:30</p>

After you specify values for these IT resource parameters, proceed to Step 9 of the procedure to import connector XML files.

## Step 6: Configuring Reconciliation

Configuring reconciliation involves the following steps:

- [Configuring Trusted Source Reconciliation](#)
- [Creating the Reconciliation Scheduled Tasks](#)

### Configuring Trusted Source Reconciliation

---

**Note:** Perform this step of the procedure only if you want to configure trusted source reconciliation. Only one connector can be configured for trusted source reconciliation. If you import the `SAPHRXLResourceObject.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

---

To configure trusted source reconciliation, you must first import the XML file for trusted source reconciliation as follows:

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 locating 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**.

## Creating the Reconciliation Scheduled Tasks

To create the scheduled tasks for lookup fields and user reconciliations:

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 2-11 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 the scheduled task, proceed to the "[Step 7: Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System](#)" section on page 2-12.

## Specifying Values for the Scheduled Task Attributes

You must specify values for the following attributes of the 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.

---

Attribute	Description	Default/Sample Value
Password	Default password, used while creating the Xellerate User	Dummy
Organization	Default organization assigned to a new user	Xellerate Users
Role	Default role 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
ReconKey	Configurable reconciliation key The value can be any one of the following: <ul style="list-style-type: none"> <li>■ SSN</li> <li>■ EMAIL</li> <li>■ EMPLOYEE</li> <li>■ USER</li> </ul>	SSN
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.	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
FirstTimeReconRecords	Size of batches in which the user detail records are to be fetched for the first reconciliation run  For example, if the value is 5000, then for a total of 1 million users, reconciliation is carried out 200 times.	5000

Attribute	Description	Default/Sample Value
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.	1
InfoTypeStatus	Infotypes currently used by SAP BAPI to store the status of employees  The value can be a comma-separated list of infotypes.	0001
RecordLimit	Used if a timeout occurs during regular reconciliation  If a timeout occurs, then user records are fetched in batches with a maximum size corresponding to the value of this parameter. For example, suppose the value of this parameter is 10000. If timeout occurs during reconciliation of 1 million user records, then the reconciliation engine tries to retrieve all the records in batches of 10000. This means that 100 reconciliation runs are performed to retrieve all 1 million records.	10000

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

## Step 7: 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 (`librfccm` and `libsapjcorfc` 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, BEA 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](#)

### 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.

## 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 2-13

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.

---

---

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

## 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:

```
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\_partername
- SAPsnc\_qop

**See Also:** The "[Defining IT Resources](#)" section on page 2-8

## 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. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

---



---

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

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 "[Step 6: Configuring Reconciliation](#)" section on page 2-9 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.

---



---

## 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](#)

### Running Test Cases

You can use the troubleshooting 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 troubleshooting utility for testing reconciliation:

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

This file is in the

`OIM_home\xellerate\XLIntegrations\saphrms\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  Refer to the " <a href="#">Defining IT Resources</a> " section on page 2-8 for information about the values that you must provide.
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\JavaTasks\xliSAPHR.jar
OIM_home\xellerate\lib\xlLogger.jar
OIM_home\xellerate\lib\xlUtils.jar
OIM_home\xellerate\JavaTasks\sapjco.jar
```

3. In the `log.properties` file in the same directory:

- a. Set the path of the directory in which you want to create the log files as the value of the following parameter:

```
log4j.appender.logfile.File=log_file_path
```

Here, *log\_file\_path* is the path of the directory in which you want to create the log file.

- b. Specify any one of the following log levels:

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

For example, if the log level for DEBUG is to be enabled, then you must add the following entry file:

```
log4j.rootLogger=DEBUG,stdout,logfile
```

4. 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\sapcua\troubleshoot
```

- b. Enter the following command:

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

The `troubleshoot.properties` 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.

5. Enter the following command to test reconciliation:

```
java
-DTproperties=OIM_home\xellerate\XLIntegrations\saphrms\troubleshoot\troubleshoot.properties
-Dlog4j.configuration=file:\OIM_home\xellerate\XLIntegrations\saphrms\troubleshoot\log.properties com.thortech.xl.troubleshooting.src.troubleshootingUtility R
```

## Troubleshooting

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

- [Connection Errors](#)
- [Common SNC Errors](#)

### Connection Errors

The following table provides solutions to common connection errors.

Problem Description	Solution
<p>Oracle Identity Manager cannot establish a connection to SAP Employee Reconciliation.</p> <p><b>Returned Error Message:</b> SAP Connection exception</p> <p><b>Returned Error Code:</b> INVALID_CONNECTION_ERROR</p>	<ul style="list-style-type: none"> <li>■ Ensure that SAP Employee Reconciliation is running.</li> <li>■ Ensure that Oracle Identity Manager is running (that is, the database is running).</li> <li>■ Ensure that all the adapters have been compiled.</li> <li>■ Examine the Oracle Identity Manager record (from the IT Resources form). Ensure that the IP address, admin ID, and admin password are correct.</li> </ul>
<p>Authentication error</p> <p><b>Returned Error Message:</b> Authentication error</p> <p><b>Returned Error Code:</b> AUTHENTICATION_ERROR</p>	<p>Ensure that the specified SAP connection user ID and password are correct.</p>

## Common SNC Errors

The following table provides a solution to an SNC error.

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



---

---

## Known Issues

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

- 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.
- 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.

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

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



## Attribute Mappings Between Oracle Identity Manager and SAP Employee Reconciliation

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

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
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



---

---

# Index

## A

---

additional files, 2-1  
Administrative and User Console, 2-7, 2-9  
attributes  
    user reconciliation scheduled task, 2-11  
attributes mappings, A-1

## B

---

BAPI folder, 1-3, 2-2  
BAPIF4T table, 2-5

## C

---

changing input locale, 2-3  
clearing server cache, 2-4  
common errors, 3-3  
common SNC errors, 3-3  
configuring  
    connector for multiple installations of the target system, 2-15  
    Oracle Identity Manager server, 2-3  
    reconciliation, 2-9  
    target system, 2-4  
Connection errors, 3-2  
connector files and directories  
    copying, 2-2  
    description, 1-3  
    destination directories, 2-2  
    installation media file, 1-3, 2-2  
connector release number, determining, 1-4  
connector testing, 3-1  
connector XML files  
    *See* XML files  
creating scheduled tasks, 2-9, 2-10

## D

---

defining  
    IT resources, 2-8  
    scheduled tasks, 2-9, 2-10  
deployment requirements, 2-1  
Design Console, 1-4, 2-10  
determining release number of connector, 1-4

## E

---

errors, 3-2  
    Connection, 3-2  
    SNC, 3-3  
external code files, 2-1

## F

---

files  
    additional, 2-1  
    external code, 2-1  
    *See also* XML files  
files and directories of the connector  
    *See* connector files and directories  
functionality supported, 1-1  
functions available, 1-1

## G

---

globalization features, 1-1

## I

---

importing connector XML files, 2-7  
input locale, changing, 2-3  
issues, 4-1  
IT resources  
    defining, 2-8  
    parameters, 2-8  
    SAP HRMS, 2-7

## L

---

limitations, 4-1

## M

---

mapping between attributes of target system and Oracle Identity Manager, A-1  
multilanguage support, 1-1

## O

---

Oracle Identity Manager Administrative and User Console, 2-7, 2-9  
Oracle Identity Manager Design Console, 1-4, 2-10

Oracle Identity Manager server, configuring, 2-3

## **P**

---

parameters  
  of IT resources, 2-8  
problems, 3-2  
process tasks, 1-1  
provisioning functions, 1-1

## **R**

---

reconciliation  
  configuring, 2-9  
  functions, 1-1  
  module, 1-2  
  trusted source, 2-9  
  trusted source mode, 1-3  
release number of connector, determining, 1-4  
requirements for deploying, 2-1

## **S**

---

SAPCAR utility, 2-6  
SAR files  
  BAPI, 1-3, 2-2  
scheduled tasks  
  attributes, 2-11  
  defining, 2-9, 2-10  
  user reconciliation, 2-11  
server cache, clearing, 2-4  
SNC  
  configuring, 2-12  
  configuring, parameters, 2-13  
  errors, 3-3  
  prerequisites, 2-12  
  security package, installing, 2-13  
supported  
  functionality, 1-1  
  languages, 1-1  
  releases of Oracle Identity Manager, 2-1  
  target systems, 2-1

## **T**

---

target system, multiple installations, 2-15  
target systems  
  configuration, 2-4  
target systems supported, 2-1  
test cases, 3-1  
testing the connector, 3-1  
transport request  
  creating, 2-5  
  importing, 2-5  
troubleshooting, 3-2  
  associated files, 1-3, 2-2  
troubleshooting utility, 1-3, 2-2, 3-1  
trusted source reconciliation, 1-3, 2-9

## **U**

---

user attribute mappings, A-1  
user reconciliation scheduled task, 2-11

## **X**

---

XML files  
  description, 1-3  
  for trusted source reconciliation, 1-3  
  importing, 2-7