Oracle® Identity Manager

Connector Guide for SAP Employee Reconciliation

Release 9.0.1

B31135-01

June 2006

ORACLE®

Oracle Identity Manager Connector Guide for SAP Employee Reconciliation, Release 9.0.1

B31135-01

Primary Author: Deepa Aswani

Contributing Authors: Lyju Vadassery, Don Gosselin

Contents

Preface

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

Note: This is a transitional release following Oracle's acquisition of Thor Technologies. 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 Framework Guide*
- Connector guides for various third-party applications

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.1 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:

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.

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. 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

The following table lists the reconciliation functions supported by the SAP Employee Reconciliation connector.

Function	Description
Create User	Create a user in Oracle Identity Manager
Delete User	Delete a user in Oracle Identity Manager
Disable User	Disable a user in Oracle Identity Manager
Enable User	Enable a user in Oracle Identity Manager
Update User	Update a user in Oracle Identity Manager

Reconciliation Module

This section describes the elements that the reconciliation module extracts from the target system to construct a reconciliation event record.

User Reconciliation

This section discusses the user reconciliation functionality of the SAP Employee Reconciliation connector.

Reconciled SAP User Fields

The following fields are reconciled with the SAP Employee Reconciliation connector:

- 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

The following 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 SAP Employee Reconciliation connector are compressed in the `SAP Employee Reconciliation Rev 3.1.0.zip` file, which is in the following directory on the installation media:

`Enterprise Applications\SAP Enterprise Applications\`

These files and directories are listed in the following table.

Files	Description
`xml\SAPHRResourceObject.xml`	These XML files contain all the components of the connector. These components include the following: ■ Resource asset 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`	Use the `SAPHRXLResourceObject.xml` file to configure the connector as a trusted source. The SAPEPXLResourceObject.xml file contains only the Oracle Identity Manager resource objects and dependent values.
`lib\xliSAPHR.jar` `lib\sapjco.jar`	These JAR file contains the `class` files that are required for reconciliation between the Oracle Identity Manager system and the SAP HRMS system.
`BAPI\xlsapcar.sar`	This file is extracted and the components are deployed on the target system for the connector to work with the target SAP Employee Reconciliation system.
`troubleshoot\troubleShoot.properties` `troubleshoot\log.properties`	The files contain parameters and settings to connect to the target system using the troubleshooting utility, and information to create a log file to log related events.
`troubleshoot\TroubleShootingUtility.class`	This utility is used to test the connector and for troubleshooting.
`docs\B31135_01.pdf` `docs\html`	The SAP Employee Reconciliation connector documentation.

See Also: Step 2: Copying the Connector Files and External Code

2

Deploying the Connector

Deploying the connector involves the following steps:

- Step 1: Verifying Deployment Requirements
- Step 2: Copying the Connector Files and the External Code
- Step 3: Configuring the Target System
- Step 4: Importing the Connector XML File
- Step 5: Configuring Reconciliation
- Step 6: Configuring the Connector to Use SNC

Note: This connector does not have any resource adapter dependencies.

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 host platform	SAP R3 4.7
External Code	`sapjco.jar`, `librfccm.so`, `libsapjcorfc.so`, `librfccm.dll`, and `libsapjcorfc.dll`
Sap JCO	Version 2.0.10

Step 2: Copying the Connector Files and the External Code

Copy the following connector files to the destinations indicated in the following table:

Files	Destination
`xml\SAPHRResourceObject.xml` `xml\SAPHRXLResourceObject.xml`	`OIM_HOME\xellerate\XLIntegrations\saphrms\xml\`
`lib\xliSAPHR.jar` `lib\sapjco.jar`	`OIM_HOME\Xellerate\JavaTasks\`
`BAPI\xlsapcar.sar`	`C:\xlsapcar\`
`troubleshoot\*.*`	`C:\connector_test_directory`

Files	Destination
docs\B31135_01.pdf docs\html	*OIM_HOME*\Xellerate\saphrms\docs\

To copy the external code into the correct location:

1. Download the SAP Java connectors file from the SAP Web site.

   To do this:

   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 that you want to save the file with the following name and path:

      OIM_HOME\Xellerate\SAP\lib\SAP_JCO.zip

2. Extract the SAP_JCO.zip file in the directory in which you downloaded it.
3. Copy the sapjco.jar file into the *OIM_HOME*\Xellerate\JavaTasks directory.
4. On Solaris and Linux, copy the librfccm.so and libsapjcorfc.so files to the /usr/local/jco directory, and set the path to LD_LIBRARY_PATH.

   On Microsoft Windows, copy the librfccm.dll and libsapjcorfc.dll files to the winnt\system32 directory.

See Also: Files and Directories That Comprise the Connector

Step 3: Configuring the Target System

This section provides instructions for configuring the target system. You need the following information to configure the target system to deploy the SAP connector:

- Login ID (administration user) having the full authorizations to import the request.
- Client Number on which connector to be deployed
- System number
- System IP address
- Server name
- Login ID of the application server
- Password for the application server login

Manual Entry in SAP

This section discusses tasks that need to be performed manually in the SAP system.

Table Maintenance for BAPIF4T

The following entry is required on the SAP system for viewing F4 values of User Groups. F4 values are applicable values of a field that you can view as a drop-down list and select from. User Group is one of the fields available in the login data of user. To view the valid User Groups for a user, follow these instructions:

1. Run transaction code `SM30` on the SAP system.
2. Enter `BAPIF4T` as the table name and click **Maintain**. Ignore any warnings or messages.
3. Click **New Entries**.
4. On the following screen, enter `XUCLASS` as the **Data element** and `ZXL_PARTNER_BAPI_F4_AUTHORITY` as the **Function name**.
5. Save and exit.

> **Note:** If an entry already exists for the `XUCLASS` Data element, then do not change this value.

Transport System Method

This section discusses the transport system method.

SAP Transport Request

The SAP deployment is done by SAP transport request (PACK) with the help of the SAP Basis consultant (administrator).

The connector files are compressed using the SAPCAR utility. The two files, `Data` and `Cofile`, of the SAP connector transport request are compressed into a single file named `xlsapcar.sar`.

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. Select a digital certificate.
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. This displays the download object.
6. Select the **Object** check box, and then click **Add to Download Basket.**

To install the SAPCAR utility and extract the SAP connector files:

1. On the local computer, create the `C:\xlsapcar\` directory.
2. Copy the `sapcar.exe` and `xlsapcar.sar` files on the local computer in the `C:\xlsapcar\` directory from the connector installation media.
3. Run the `sapcar` utility to extract the `xlsapcar.sar` file. To do this:
   a. Click **Start,** and then run the `cmd` command.
   b. In the command window, open the `c:\xlsapcar` directory.

c. Use the `dir` command to verify that the two downloaded files, `sapcar.exe` and `xlsapcar.sar`, are in the directory.

d. Enter the following command to extract the `xlsapcar` file:

```
sapcar -xvf xlsapcar.sar
```

This command extracts the `K900208.I46` (Cofile) and `R900208.I46` (Data file) files into this directory.

4. The SAP Basis administrator must copy these files to the SAP server in their respective locations, and then import these requests in SAP like other transport requests.

5. Check the log file to determine whether or not the transport was successful by clicking on the request number in transaction code STMS. Check the error codes in the log file. If the return code is 4, then the import ended with warnings. This usually happens if the object is overwritten or already exists in SAP system. If the return code is 8 or greater, then it means that there are errors in the imports. To view error details, click on the detail log. This log is useful for analyzing any issues related to transport.

   Alternatively, you can confirm the transport of objects by using SAP transaction code SE80 and checking Package ZXLH in the ABAP objects.

After the successful import of the transport request, the SAP system is ready for use.

Step 4: 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.
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 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 EP` 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. You must remove these nodes. To do this, right-click each such node and then select **Remove.**

12. Click **Import**. The connector file is imported into Oracle Identity Manager.
13. If you plan to use the connector in trusted source reconciliation mode, then perform the same procedure to import the `SAPHRXLResourceObject.xml` file. This file is in the *`OIM_HOME`*`\xellerate\XLIntegrations\saphrms\xml\` directory.

Caution: Only one connector can be configured as a trusted source. If you import the `SAPHRResourceObject.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

After importing the connector XML file, proceed to Step 5: Configuring Reconciliation.

Defining IT Resources

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

Parameter	Description
`SAPClient`	Port number to connect to the target system. For example: `800`
`SAPHost`	Server address of the target system. For example: `172.20.30.267`
`SAPLanguage`	Language of communication. The default is English (`EN`).
`SAPPassword`	Password to connect to the target system
`SAPSystemNo`	SAP system number (for example, `00`)
`SAPType`	SAP system name (`R3`, for example)
`SAPUser`	SAP User (for example, `xellerate`)
`TimeStamp`	The value is empty for the first reconciliation run. After the first run, the time at which the last reconciliation was completed is stored in this parameter. For example: `Oct 27, 2005 at 16:14:00 GMT+05:30`
`SAPsnc_mode`	This value shows if SNC is enabled or not(`0` or `1`). Other SNC values are required only if this is set to `1`.
`snc_lib`	The location of the SNC library file. For example: `c:\\usr\\sap\\sapcrypto.dll`.
`snc_myname`	This is the SNC system name. For example `p:CN=TST, OU=SAP, O=ORA, C=IN`
`snc_partnername`	This is partner system name. For example. `p:CN=I47, OU=SAP, O=ORA, C=IN`

Parameter	Description
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.

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

Step 5: Configuring Reconciliation

Configuring reconciliation involves creating scheduled tasks for lookup fields and user reconciliations. To create these scheduled tasks:

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 tasks are displayed on two different tabs.
5. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager should attempt to complete the task before assigning the ERROR status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.
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 appropriate table in the Specifying Values for the Scheduled Task Attributessection 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.
11. Repeat Steps 5 through 10 to create the second scheduled task.

After you create both scheduled tasks, proceed to the Step 6: Configuring the Connector to Use SNC section.

Specifying Values for the Scheduled Task Attributes

This section provides information about the values to be specified for the user reconciliation scheduled task:

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.

Parameter Name	Sample Value	Comments
Password	Dummy	Default password, taken while creating the Xellerate User
Organization	Xellerate Users	Default organization assigned to a new user
Role	Consultant	Default role assigned to a new user
Xellerate Type	End-user administrator	Default type assigned to a new user
ITResource	SAP CUA IT resource name	Name of the IT Resource for setting up the connection to SAP CUA
ResourceObject	SAP CUA resource object name	Name of the resource object into which users need to be reconciled
Server	CUA	Optional

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

See Also: Reconciliation Module

Step 6: Configuring the Connector to Use SNC

To connect to an SAP system application server, the Java Application Server uses the Java Connector and RFC. If you want to secure these connections, you can use Secure Network Communication (SNC).

Prerequisites to Configuring the Connector to Use SNC

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

- The external security product must be installed on the server.
- You should be familiar with the SNC infrastructure. You must know which Personal Security Environment (PSE) the application server uses for SNC. You must also know whether you are using the same PSE for both communication partners or individual ones.
- SNC must be activated on the SAP application server.

Installing the Security Package

To install the security package on the Java Application Server:

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

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

   http://service.sap.com/download

   This package contains the following files:

   – SAP Cryptographic Library (`sapcrypto.dll` for Microsoft Windows NT or `libsapcrypto.ext` for UNIX)

   – A corresponding license ticket (ticket)

   – he configuration tool, `sapgenpse.exe`

2. Copy the library and the `sapgenpse.exe` configuration tool to a local directory. For example, the `C:\`*`install_dir`*`\SAPCryptolib` directory.

3. Check the file permissions. The user under which the Java Application Server runs must be able to run the library functions in the `SAPCryptolib`.

4. Create the `sec` directory in the `SAPCryptolib` directory.

5. Copy the ticket file to the `sec` directory. This is also the directory in which the PSE and credentials of the Java Application Server are to be stored.

6. Set the `SECUDIR` environment variable for the user of the Java Application Server user to the `sec` directory.

7. Set the `SNC_LIB` environment variable for the user of the Java Application Server to the cryptographic library. In this case, the directory is `C:\`*`install_dir`*`\SAPCryptolib`.

Configuring the Connector to Use SNC

To configure the connector to use SNC:

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

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

   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 of the Java Application Server.

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. Therefore, use the command-line `seclogin` of the configuration tool to "open" the PSE.

Enter the following command to open the server's PSE and create the `credentials.sapgenpse` file:

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

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

3. If you are using individual PSEs, then exchange the public-key certificates of the two servers as follows:

   a. Export your own certificate in the file by entering the following command:

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

   b. Import the certificate file into the SAP application server. Obtain the certificate of the SAP application server.

   c. Import the certificate of the SAP application server by entering the following command:

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

4. Set the SNC parameters in the IT Resource.

   You must configure the following parameters in the IT Resource object:

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

3

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected. Tests that you can run on the connector can be divided into the following high-level categories:

- **Reconciliation Testing:** In this type of test, you reconcile Oracle Identity Manager with either a trusted source or a target resource. In other words, the trusted source or target resource is the starting point of the connector, and Oracle Identity Manager is the end point.
- **Linking Testing:** For this test, Oracle Identity Manager links an SAP HRMS employee and SAP User by updating the target resource. In other words, Oracle Identity Manager is the starting point of the connector, and the target resource is the end point.

Note: In earlier releases of this guide, the connector was referred to as the *integration.*

This chapter contains the following sections:

Running Test Cases

You can use the troubleshooting utility to connect to the SAP server and to perform basic operations aimed at identifying the cause of problems. You can also use it to run test cases to test the connector functionality.

The `SAP Employee Reconciliation_versionno\troubleshoot` directory contains the `troubleShoot.properties` file. The troubleshooting utility uses this file to connect to the SAP system. This file contains the following information:

- **SAP connection parameters**: SAP server-related information.
- **User information**: User parameters specified to create, modify, delete, and update user information for provisioning.
- **Reconciliation information**: The `From date` timestamp information is passed from this file. The `To date` is set to the current time.

This file also contains commands to test user reconciliation and provisioning. You need to place these files in a test folder to run the test case indicated here.

To test the connector, specify the following information in the `troubleshooting.properties` file:

```
sapClient=800
sapUser=xellerate
sapPassword=project
sapLanguage=EN
sapSystem=00
sapIP=172.20.70.204
sapType=R3
FirstTimeReconRecords=10000
snc_mode=0
snc_myname=p:CN=win2003, OU=SAP, O=ORA, C=IN
snc_qop=3
snc_partnername=p:CN=I47, OU=SAP, O=ORA, C=IN
snc_lib=C:\\usr\\sap\\sapcrypto.dll
```

In the `log.properties` file in the same directory, set the path for the log files in the following parameter:

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

Note: Ensure that all the JAR files associated with this connector are included in the `CLASSPATH`.

Testing Reconciliation

Run the following command to test reconciliation:

```
java -DTproperties=TEST_FOLDER_PATH\troubleshooting\troubleShoot.properties
-Dlog4j.configuration=file:/TEST_FOLDER_PATH/troubleshooting/log.properties
com.thortech.xl.troubleshooting.src.troubleShootingUtility R
```

Troubleshooting

The following table lists some commonly encountered issues associated with this resource adapter. For each issue, a suggested resolution is provided.

Connection Errors

The following table provides solutions to common connection errors.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to SAP HRMS. **Returned Error Message:** SAP Connection exception **Returned Error Code:** `INVALID_CONNECTION_ERROR`	■ Ensure that the SAP HRMS server is up and running. ■ Verify that Oracle Identity Manager is running (that is, the database is running). ■ Verify that all the adapters have been compiled. ■ Examine the Oracle Identity Manager record (from the IT Resources form). Verify that the IP address, admin ID, and admin password are correct.

Problem Description	Solution
Authentication error **Returned Error Message:** Authentication error **Returned Error Code:** AUTHENTICATION_ERROR	Verify that the given SAP connection user ID and password are correct.

Common SNC Errors

The following table provides a solution to an SNC error.

Problem Descriptions	Solution
Trying to connect to SAP through the SNC. **Returned Error Message:** SAP Connection JCO Exception **Returned Error Code:** SNC required for this connection	Ensure that all the required information is given. The required information includes the following: 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

4

Known Issues

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

- During HR configuration, you need to 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.
- To ensure correct reconciliation, the `Recon Key` parameter should be correctly entered in the Task Scheduler, based on which reconciliation takes place. Based on the Recon Key:
  - SSN: The SSN in the process form must be the same as the SSN in the Oracle Identity Manager form.
  - EMAIL: The e-mail address in the process form must be the same as the e-mail address in the Oracle Identity Manager form.
  - EMPLOYEE: The employee ID in the process form must be the same as the employee ID in the Oracle Identity Manager form.
  - USER: The employee ID in the process form must be the same as the user login in the Oracle Identity Manager form.
- The resource object used for provisioning Oracle Identity Manager users with the SAP system must be mentioned in the Task Scheduler (with the SAP R3 resource object or the SAP CUA resource object).
- The first time an employee is reconciled, a new Xellerate User is created. After the newly created Xellerate User is provisioned, the employee record should be modified, so that in the next reconciliation, this employee record gets reconciled and the employee is linked to the user provisioned in the SAP system. If the employee record is not modified, then the employee does not get linked to the SAP user in the next reconciliation.

Index

O

P

R

S

T

U

V

X