Oracle® Identity Manager

Connector Guide for SAP CUA

Release 9.0.2

B32170-01

September 2006

ORACLE®

Oracle Identity Manager Connector Guide for SAP CUA, Release 9.0.2

B32170-01

Primary Author: Deepa Aswani

Contributing Authors: Don Gosselin, Lyju Vadassery

Contents

Preface

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

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 SAP CUA Connector.

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 Table*s
- *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:

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

What's New in the Oracle Identity Manager Connector for SAP CUA?

This chapter provides an overview of the updates made to the connector and documentation for SAP CUA 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 1-4.
- The "Step 2: Copying the Connector Files and External Code" section on page 2-2 specifies 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 two new issues 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 1-5.

External Code Files Not Bundled in the Connector Pack

External code files are not bundled along with the connector file in the installation media directory. Instead, instructions to download and copy the external code files are given in the "Step 2: Copying the Connector Files and External Code" section on page 2-2.

Addition of Attributes in the User Reconciliation Scheduled Task

The following attributes have been added to the user reconciliation scheduled task:

- `IsTrusted`
- `FirstTimeReconRecords`

These attributes are described in the "User Reconciliation Scheduled Task" section on page 2-12.

New Items in the Known Issues List

The following items have been added in the Known Issues list in Chapter 4:

- The limitation arising out of the situation in which a user is created in SAP CUA and then locked has been added.
- The message to be ignored when a user is deleted from Oracle Identity Manager during reconciliation has been added.

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 "Lookup Data Reconciliation" section on page 1-2, the list of lookup fields that are reconciled has 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 download and copy the external code files have been reworded in the "Step 2: Copying the Connector Files and External Code" on page 2-2.
- Instructions to copy the connector JAR files and adapter 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 on page 2-2
  - Step 3: Configuring the Oracle Identity Manager Server on page 2-3

  - Step 7: Compiling Adapters on page 2-12

- Instructions to configure the target system have been reworded in the "Step 4: Configuring the Target System" on page 2-4.
- Instructions and pointers to information about configuring trusted source reconciliation have been moved to the "Configuring Trusted Source Reconciliation" section on page 2-10.
- Instructions in the "Step 8: Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System" section on page 2-14 have been reworded.
- Instructions to use Oracle Identity Manager for linking multiple installations of SAP CUA are given in the "Configuring the Connector for Multiple Installations of the Target System" section on page 2-16.
- The following changes have been made in the Known Issues list in Chapter 4:
  - The connector is compatible only with Oracle Identity Manager 8.5.3 or later. Therefore, an issue related to a bug in an earlier release of Oracle Identity Manager has been removed from the list.
  - The instruction to perform lookup reconciliation immediately after deploying the connector has been removed from the list. This item was redundant.
  - The issue pertaining to the implementation of the connection pool has been reworded.
- Appendix A provides information about attribute mappings between Oracle Identity Manager and SAP CUA.
- The "Supported Platforms" section has been removed.

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 CUA is used to integrate Oracle Identity Manager with SAP CUA.

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 functions that are available with this connector.

Function	Type	Description
Create User	Provisioning	Creates a user in SAP CUA
Delete User	Provisioning	Deletes a user from SAP CUA
Lock User	Provisioning	Locks a user in SAP CUA
Unlock User	Provisioning	Unlocks a user in SAP CUA
Reset User Password	Provisioning	Resets a user password in SAP CUA
Edit User	Provisioning	Modifies information about a user in SAP CUA
Add User To Activity Group (Role)	Provisioning	Adds a user to an activity group in SAP CUA
Remove User From Activity Group(Role)	Provisioning	Removes a user from an activity group in SAP CUA
Assign Profile to User	Provisioning	Adds a profile to a user in SAP CUA

Function	Type	Description
Remove Profile from User	Provisioning	Removes a profile from a user in SAP CUA
Create User	Reconciliation	Creates a user in Oracle Identity Manager
Delete User	Reconciliation	Deletes a user from Oracle Identity Manager
Lock User	Reconciliation	Locks a user in Oracle Identity Manager
Unlock User	Reconciliation	Unlocks a user in Oracle Identity Manager
Edit User	Reconciliation	Modifies information about a user in Oracle Identity Manager
Add User To Activity Group(Role)	Reconciliation	Assigns an activity group to a user in Oracle Identity Manager
Remove User From Activity Group(Role)	Reconciliation	Removes an activity group from a user in Oracle Identity Manager
Add Profile to User	Reconciliation	Assigns a profile to a user in Oracle Identity Manager
Remove Profile From User	Reconciliation	Removes a profile from a user in Oracle Identity Manager

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

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.

The following types of reconciliation are covered in this section:

- Lookup Data Reconciliation
- User Reconciliation

Lookup Data Reconciliation

The following fields of SAP CUA are reconciled:

- Lookup.SAP.CUA.Roles
- Lookup.SAP.CUA.TimeZone
- Lookup.SAP.CUA.LangComm
- Lookup.SAP.CUA.UserTitle
- Lookup.SAP.CUA.DecimalNotation
- Lookup.SAP.CUA.DateFormat
- Lookup.SAP.CUA.UserGroups
- Lookup.SAP.CUA.CommType

- Lookup.SAP.CUA.Profiles

The following lookup fields are not reconciled:

- Lookup.SAP.CUA.UserType
- Lookup.SAP.CUA.LockUser
- Lookup.SAP.CUA.RoleProfileOption

User Reconciliation

This section discusses elements that are specific to user reconciliation between SAP CUA and Oracle Identity Manager.

Reconciled SAP CUA Resource Object Fields

The following fields are reconciled:

- Extension
- Telephone
- Time Zone
- Lang Logon
- User Group
- Department
- Lang Comm
- Last Name
- First Name
- User Title
- Password
- User ID
- Start Menu
- User Type
- Alias
- Lock User
- Communication Type
- Code
- Building
- Floor
- Room No
- Function
- Decimal Notation
- Date Format
- Email Address
- Fax Number

- IT Resource Type
- User Profile
  - User Profile
  - System Name
- User Role
  - User Role
  - System Name

Reconciled Xellerate User Fields

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

- UserID
- Password
- Organization
- FirstName
- LastName
- Xellerate
- Role

Provisioning Module

The following fields are provisioned:

- User ID
- Password
- Last Name
- User Group

The following fields are mandatory for the Create User provisioning function to work:

- User Role or Profile
- Role or Profile Option

Files and Directories That Comprise the Connector

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

```
Enterprise Applications\SAP Enterprise Applications\SAP CUA Rev 3.2.0.zip
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
xml\SAPCUAResourceObject.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ Custom process form ■ Process task and adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules ■ Reconciliation process ■ Lookup definitions
xml\SAPCUAXLResourceObject.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\xliSAPCUA.jar	This JAR file contains the class files that are required for provisioning and reconciliation.
BAPI\xlsapcuacar.sar	This file is extracted and the components are deployed on the SAP CUA server for the connector to work with SAP CUA.
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.
doc\B32170_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 `xliSAPCUA.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 `xliSAPCUA.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 `xliSAPCUA.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.

2

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: Compiling Adapters
- Step 8: 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 CUA, 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 master systems	The target master system can be any one of the following: ■ SAP R3 4.7 ■ SAP R3 4.6c
Target child systems	The target child system can be any one of the following: ■ SAP R3 4.7 ■ SAP R3 4.6c ■ SAP CRM

Item	Requirement

External code	The following SAP custom code files:
	`sapjco.jar`
	
	For Microsoft Windows:
	`sapjcorfc.dll`
	`librfc32.dll`
	
	Version: 2.0.10
	For Solaris and Linux:
	`libsapjcorfc.so`
	`librfccm.so`
	
	Version: 2.0.10

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

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 CUA Rev 3.2.0.zip`

Refer to the "Files and Directories That Comprise the Connector" section on page 1-4 for more information about these files.

File in the Installation Media	Destination
Files in the `xml` directory	*`OIM_home`*`\xellerate\sapcua\xml`
`lib\xliSAPCUA.jar`	*`OIM_home`*`\xellerate\JavaTasks`
Files in the `resources` directory	*`OIM_home`*`\xellerate\connectorResources`
`BAPI\xlsapcuacar.sar`	This file can be copied to any location on the target system. For example: `C:\xlsapcuacar\` Refer to the "Extracting the Request Files" section on page 2-6 for more information.
Files in the `Troubleshoot` directory	*`OIM_home`*`\xellerate\sapcua\troubleshoot`
`doc\B32170_01.pdf`	*`OIM_home`*`\xellerate\docs\sapcua`

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.

- 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 certain custom objects in the SAP system. These objects are listed in Appendix B.

The `xlsapcuacar.sar` file contains the definitions for these objects. When you import the request represented by the contents of the `xlsapcuacar.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 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 `xlsapcuacar.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:\xlsapcuacar`

Extracting the Request Files

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

1. Copy the `xlsapcuacar.sar` file into the directory in which you download the SAPCAR utility.

   The `xlsapcuacar.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 `xlsapcuacar.sar` file.
3. Enter the following command to extract the Data file and Cofile components of the request:

   ```
   sapcar -xvf xlsapcuacar.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 (`K900208.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 ZXLC 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 `SAPCUAResourceObject.xml` file, which is in the *`OIM_home`*`\Xellerate\sapcua\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 CUA IT Resource` IT resource is displayed.
8. Specify values for the parameters of the `SAP CUA IT Resource` IT resource. Refer to 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 R3 IT Resource` 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 CUA IT resource parameters listed in the following table.

Parameter	Description	Default/Sample Value
SAPChangePasswordSystem	Flag that accepts the value X or ' ' If the value is X, then the password is changed only in the master system. If the value is ' ', then the password is changed in both master and child systems. This parameter is used by the Reset Password function.	X **Note:** If you want to enter X, then enter it in uppercase.
SAPClient	SAP client ID	800
SAPHost	SAP host IP address	172.20.70.204
SAPLanguage	SAP language The value can be any one of the following: ▪ EN (for English) ▪ JA (for Japanese) ▪ FR (for French)	EN
SAPMasterSystem	SAP CUA master system	CUA47
SAPPassword	Password of the SAP user	changethis
SAPsnc_lib	Path where the crypto library is placed This is required only if Secure Network Communication (SNC) is enabled.	c:\\usr\\sap\\sapcrypto.dll
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
SAPsnc_myname	SNC system name This is required only if SNC is enabled.	p:CN=TST,OU=SAP, O=ORA,c=IN
SAPsnc_partnername	Domain name of the SAP server This is required only if SNC is enabled.	p:CN=I47,OU=SAP, O=ORA, c=IN

Parameter	Description	Default/Sample Value
SAPsnc_qop	Protection level (quality of protection, QOP) at which data is transferred The default value is 3. Valid values are: ■ 1: Secure authentication only ■ 2: Data integrity protection ■ 3: Data privacy protection ■ 8: Use value from the parameter ■ 9: Use maximum value available This is required only if SNC is enabled.	3
SAPSystemNo	SAP system number	00
SAPType	Type of SAP system	CUA
SAPUser	SAP user	Xellerate
TimeStamp	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.	The following are sample timestamp values: English: Jun 01, 2006 at 10:00:00 GMT+05:30 French: juin. 01, 2006 at 10:00:00 GMT+05:30 Japanese: 6 01, 2006 at 10:00:00 GMT+05:30

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 `SAPCUAXLResourceObject.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 `SAPCUAXLResourceObject.xml` file, which is in the *`OIM_home`*`\Xellerate\sapcua\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**.

Then, set the value of the `IsTrusted` reconciliation scheduled task attribute to `true` while performing the procedure described in the following section.

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 tasks are displayed on two different tabs.
5. For the first scheduled task, 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.

11. Repeat Steps 5 through 10 to create the second scheduled task.

After you create both scheduled tasks, proceed to the "Step 7: Compiling Adapters" section on page 2-12.

Specifying Values for the Scheduled Task Attributes

This section provides information about the values to be specified for the following scheduled tasks:

- Lookup Fields Reconciliation Scheduled Task
- User Reconciliation Scheduled Task

Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the lookup fields 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	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 the connection to the target system	`SAP CUA`
`ResourceObject`	Name of the resource object into which users need to be reconciled	`SAP CUA Resource Object`
`Server`	Name of the server This is an optional parameter.	`CUA`

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

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.

Attribute	Description	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 the connection to SAP CUA	`SAP CUA`
`ResourceObject`	Name of the resource object into which users need to be reconciled	`SAP CUA Resource Object`
`Server`	Name of the server This is an optional parameter.	`CUA`
`IsTrusted`	Configuration for a trusted or nontrusted target If it is set to `true`, then the target is a trusted source. If it is set to `false`, then the target is a nontrusted target, or target resource. The default value is `false`.	`false`
`FirstTimeRecon Records`	Number of records to be fetched during first-time reconciliation, if the reconciliation scheduled task times out Initially, Oracle Identity Manager tries to fetch all the records. If the process times out, then Oracle Identity Manager tries to fetch the number of records specified by this parameter. If the task times out even before this number of records are fetched, then Oracle Identity Manager tries to fetch records by recursively dividing this number by two, until all records are fetched from the target system.	5000

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

Step 7: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- PrePopulate SAP Form
- SAP CUA Delete User
- SAP CUA Modify User
- SAP CUA Add Role
- SAP CUA Password Change
- SAP CUA Create User
- SAP CUA Lock UnLock User
- SAP CUA Remove Role
- SAP CUA Add Profile
- SAP CUA Remove Profile
- SAP CUA Modify UserX

You must compile these adapters before you can use them to provision accounts on the target system.

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you import into the current database, select **Compile All**.

   To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select **Compile Selected**.

   Note: Click **Compile Previously Failed** to recompile only those adapters that were not compiled successfully. Such adapters do not have an `OK` compilation status.

3. Click **Start.** Oracle Identity Manager compiles all the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *`OIM_home`*`\xellerate\Adapter` directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes. Then, restart each node.

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

   Note: To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms.

Step 8: 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

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 2-15

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 CUA IT resource object:

   - SAPsnc_lib
   - SAPsnc_mode
   - SAPsnc_myname
   - SAPsnc_partnername
   - 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 CUA. 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 CUA 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 CUA` 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 process definition.

   The Form Designer form is in the Development Tools folder. The following process forms are created when you import the connector XML file:

   - `UD_SAPCUA` (main form)
   - `UD_SAPCUARL` (child form for multivalue attributes)
   - `UD_SAPCUAPR` (child form for multivalue attributes)

   You can use these process forms as templates 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 CUA 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`
   - `IsTrusted`

   Set the `IsTrusted` attribute to `true` for the SAP CUA installation that you want to designate as a trusted source. You can designate either a single or multiple installations of SAP CUA as the trusted source. For the remaining SAP CUA installations, set this attribute to `false`.

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 CUA installation to which you want to provision the user.

3

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:

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

   This file is in the *`OIM_home`*`\Xellerate\sapcua\troubleshoot` directory. The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
SAP CUA connection parameters	Connection parameters required to connect to the target system Refer to the "Defining IT Resources" section on page 2-8 for information about the values that you must provide.
User information	Field information required to create, modify, and delete a user profile
Reconciliation information	The From Date timestamp The To Date is set to the current date and time by default.

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

   ```
   OIM_home\xellerate\ext\log4j-1.2.8.jar
   OIM_home\Xellerate\JavaTasks\xliSAPCUA.jar
   OIM_home\xellerate\lib\xlUtils.jar
   OIM_home\Xellerate\JavaTasks\sapjco.jar
   OIM_home\xellerate\lib\xlLogger.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. Perform the following tests:

- Enter the following command to create a user:

```
java
-DTproperties=OIM_home\Xellerate\sapcua\troubleshoot\troubleshoot.propertie
s
-Dlog4j.configuration=file:\OIM_home\Xellerate\sapcua\troubleshoot\log.prop
erties TroubleShootingUtility C
```

- Enter the following command to modify a user:

```
java
-DTproperties=OIM_home\Xellerate\sapcua\troubleshoot\troubleshoot.propertie
s
-Dlog4j.configuration=file:\OIM_home\Xellerate\sapcua\troubleshoot\log.prop
erties TroubleShootingUtility M
```

- Enter the following command to delete a user:

```
java
-DTproperties=OIM_home\Xellerate\sapcua\troubleshoot\troubleshoot.propertie
s
-Dlog4j.configuration=file:\OIM_home\Xellerate\sapcua\troubleshoot\log.prop
erties TroubleShootingUtility D
```

- Enter the following command to test reconciliation:

```
java
-DTproperties=OIM_home\Xellerate\sapcua\troubleshoot\troubleShoot.properties
-Dlog4j.configuration=file:\OIM_home\Xellerate\sapcua\troubleshoot\log.properties TroubleShootingUtility R
```

Troubleshooting

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

Connection Errors

The following table provides solutions to common connection errors.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to SAP CUA. **Returned Error Message:** SAP connection exception **Returned Error Code:** `INVALID_CONNECTION_ERROR`	■ Ensure that SAP CUA is running. ■ Ensure that Oracle Identity Manager is running (that is, the database is running). ■ Ensure that all the adapters have been compiled. ■ Examine the Oracle Identity Manager record (from the IT Resources form). Ensure that the IP address, admin ID, and admin password are correct.
Target not available **Returned Error Message:** Target Server not available **Returned Error Code:** `TARGET_UNAVAILABLE_ERROR`	■ Ensure that SAP CUA is running ■ Ensure that the specified SAP connection values are correct.
Authentication error **Returned Error Message:** Authentication error **Returned Error Code:** `AUTHENTICATION_ERROR`	Ensure that the specified SAP connection user ID and password are correct.

Common SNC Errors

The following table provides a solution to an SNC error.

Problem Description	Solution

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

Create User Errors

The following table provides solutions to common Create User errors.

Problem Description	Solution
Oracle Identity Manager cannot create a user. **Returned Error Message:** Require information missing **Returned Error Code:** `INSUFFICIENT_INFORMATION_PROVIDED`	Ensure that the following information is specified: ■ User ID ■ User first name ■ User last name ■ User password ■ User group ■ Profile option ■ Role or profile
Oracle Identity Manager cannot create a user. **Returned Error Message:** User already exists **Returned Error Code:** `USER_ALREADY_EXIST`	User with the assigned ID already exists in SAP. Assign a new ID to this user, and try again.
Oracle Identity Manager cannot create a user. **Returned Error Message:** User creation failed **Returned Error Code:** `USER_CREATION_FAILED`	User may not have been created because of one of the following errors: ■ The Change Password operation failed. ■ Role/profile assignment failed.

Delete User Errors

The following table provides solutions to common Delete User errors.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** Require information missing **Returned Error Code:** INSUFFICIENT_INFORMATION_PROVIDED	Ensure that the user ID has been correctly specified.
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist in target **Returned Error Code:** USER_DOESNOT_EXIST	The specified user does not exist in SAP CUA.

Modify User Errors

The following table provides solutions to common Modify User errors.

Problem Description	Solution
Oracle Identity Manager cannot update new information about a user. **Returned Error Message:** Error while updating user info **Returned Error Code:** USER_MODIFICATION_FAILED	Generic error. Refer to the log file for more details.
Oracle Identity Manager cannot update a user. **Returned Error Message:** User does not exist in target **Returned Error Code:** USER_DOESNOT_EXIST	The specified user does not exist in SAP CUA.

Child Data Errors

The following table provides solutions to common Child Data errors.

Problem Description	Solution
Oracle Identity Manager cannot add a user to a profile. **Returned Error Message:** Profile does not exist **Returned Error Code:** PROFILE_NOT_MEMBER_OF_TARGET_SYSTEM	The specified profile does not exist in SAP CUA. Check the profile name.

Problem Description	Solution
Oracle Identity Manager cannot assign a role to a user. **Returned Error Message:** Role does not exist **Returned Error Code:** ROLE_NOT_MEMBER_OF_TARGET_SYSTEM	The specified role for the user in Oracle Identity Manager does not exist in SAP CUA. Check the role name.
The operation failed because a duplicate value was being added to a profile or role. **Returned Error Message:** Duplicate value **Returned Error Code:** ROLE_ALREADY_EXISTS PROFILE_ALREADY_EXISTS	The user has already been added to the specified profile or role.

4

Known Issues

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

- To ensure that provisioning is completed successfully, you must specify either the role or profile in the field provided in the process form and then specify whether it is a role or profile. This is to activate the user on the SAP CUA master system.
- The connector can reconcile elements present in the SAP CUA master system only.
- The connection pool cannot be implemented because the current release of Oracle Identity Manager does not support it.
- Creation of a user on the SAP system involves running the Create User and Change Password functions in sequence. This event makes three RFC calls to the SAP system. The Create User RFC and Change Password RFC functions commit the transaction explicitly at the end of the call. This commit is enforced by the SAP architecture. This architecture constraint of SAP makes transactional maintenance between Create User and Change Password infeasible.
- When a user is created, the password specified is not allocated to the user. Later, the SAP system requires the user to specify the password again, which is assigned to the user at this stage. To prevent the occurrence of this event, when a user is created, the user is assigned a dummy password and after user creation the Change Password function is run automatically. The password changes from the dummy password to the one entered by the user in the SAP User form in Oracle Identity Manager. This process is not visible to the user.
- When a user is created, the password is set only for the SAP CUA Master system, not the SAP CUA Child system.
- Password validation is not done in Oracle Identity Manager because the password rule is configurable on the SAP system.
- Suppose a user is created in SAP CUA and then locked. When this user is reconciled for the first time, the user may not get locked because linking in Oracle Identity Manager takes place in an asynchronous manner. This user is successfully locked during the next reconciliation run.
- Suppose a user is deleted from SAP CUA. During reconciliation, the user is deleted from Oracle Identity Manager. However, the Delete User function is also run and a message saying that the user does not exist on the target system is displayed. This message can be ignored.
- 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.

- In SAP 4.7 or later, you cannot enter non-English letters in the E-mail Address field.

A

Attribute Mappings Between Oracle Identity Manager and SAP CUA

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

Oracle Identity Manager Attribute	SAP CUA Attribute	Description
UserId	USERNAME	Login ID
Password	BAPIPWD	Password
UserTitle	TITLE_P	Title
LastName	LASTNAME	Last name
FirstName	FIRSTNAME	First name
Function	FUNCTION	Function
Department	DEPARTMENT	Department
RoomNo	ROOM_NO_P	Room number
Floor	FLOOR_P	Floor number
Building	BUILDING_P	Building number
Code	INITS_SIG	Code
LangComm	LANGU_P	Communication language
Telephone	TEL1_NUMBR	Telephone number
Extension	TEL1_EXT	Extension for the telephone number
Fax	FAX_NUMBER	Fax number
Email	E_MAIL	E-mail address
CommType	COMM_TYPE	Communication type
Alias	USERALIAS	User alias
UserGroup	CLASS	Group to which the user is assigned
UserType	USTYP	Type of user
StartMenu	START_MENU	Default menu displayed when the user logs in
LangLogon	LANGU	Logon language
DecimalNotation	DCPFM	Decimal notation
TimeZone	TZONE	Time zone

Oracle Identity Manager Attribute	SAP CUA Attribute	Description
DateFormat	DATFM	Date format
UserRole	AGR_NAME	Multivalue attribute for roles
UserProfile	PROFILE .	Multivalue attribute for profiles
SystemName	SUBSYSTEM	System name where this role/profile exists

B

Custom Objects Created in the SAP System

The following table categorizes the custom objects that are created in the SAP system when you import the request.

Object Type	Object Name
Package	ZXLC
Function Group	ZXLCGRP
	ZXLCHLPVALUES
	ZXLCPRF
	ZXLCRL
	ZXLCUSR
Message Class	ZXLCBAPI
Program	ZLCF4HLP_DATA_DEFINITIONS
	ZLCMS01CTCO
	ZLCMS01CTCO1
	ZLCMS01CTP2
	ZXLCGRP
	ZXLCHLPVALUES
	ZXLCPRF
	ZXLCRL
	ZXLCUSR
Search Help	ZXLC_ROLE
	ZXLC_SYS
Business Object Types	ZXLCGRP
	ZXLCHLP
	ZXLCPRF
	ZXLCRL
	ZXLCUSR
Table	ZXLCBAPIMODE
	ZXLCBAPIMODM
	ZXLCGROUPS
	ZXLCPRF
	ZXLCROLE
	ZXLCSYSNAME

Index

O

P

R

S

T

U

X