Oracle® Identity Manager

Connector Guide for SAP User Management

Release 9.0.4

E10173-01

May 2007

ORACLE®

Oracle Identity Manager Connector Guide for SAP User Management, Release 9.0.4

E10173-01

Copyright © 2006, 2007, Oracle. All rights reserved.

Primary Author: Deepa Aswani

Contributing Authors: Don Gosselin, Vijaykarthik Sathiyamurthy, Lyju Vadassery

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

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

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

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

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

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

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

Contents

Preface

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

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

Audience

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

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 library:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation 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 Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack Release 9.0.4 documentation library, 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 User Management?

This chapter provides an overview of the updates made to the software and documentation for the SAP User Management connector in release 9.0.4 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.3.1 release of this guide for information about updates that were new for the 9.0.3.1 release

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 updates made to this release of the connector software.

Change in the Version of the Supported sapjco File

The required version of the sapjco file for all supported platforms has been changed from 2.0.10 to 2.1.8. This change has been made in the "Step 1: Verifying Deployment Requirements" section on page 2-1.

Partial Reconciliation

The `CustomizedReconQuery` parameter has been added to the IT resource definition. You can use this parameter to customize the query that the reconciliation module uses to determine the records to be retrieved from the target system. The `CustomizedReconQuery` parameter is explained in the following sections:

- Defining IT Resources on page 2-11
- Partial Reconciliation on page 3-1
- Testing Partial Reconciliation on page 4-2

Enabling Logging

By following the instructions in the "Enabling Logging" section on page 2-4, you can configure the generation of log information that is specific to the target system.

Batched Reconciliation

In this release of the connector, user reconciliation scheduled task is added with attributes such as `StartRecord`, `BatchSize`, and `NumberofBatches`. By specifying values for these attributes, you can reconcile users in various batches. These attributes are discussed in the following sections:

- User Reconciliation Scheduled Task on page 3-6
- Batched Reconciliation on page 3-3
- Testing Batched Reconciliation on page 4-3

Documentation-Specific Updates

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

- Instructions in the "Determining the Release Number of the Connector" section on page 1-7 have been revised.
- In the "User Reconciliation Scheduled Task" section on page 3-6, descriptions of the `InfoTypeStatus` and `EmpStatus` attributes have been added.

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 User Management is used to integrate Oracle Identity Manager with SAP User Management.

> **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:

> **Note:** At some places in this guide, SAP User Management has been referred to as the *target system.*

Reconciliation Module

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

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

This section discusses the elements that are extracted from the target system by the reconciliation module for constructing reconciliation event records. The following are features of the reconciliation module:

- The default data elements of each reconciliation event record are Organization, User Type, and Employee Type.

- The default labels for the data elements in each reconciliation event record are as follows:
  - Event Linked (for successful reconciliation)
  - No Match Found (for failed reconciliation)

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

- Lookup Data Reconciliation
- User Reconciliation

Lookup Data Reconciliation

The following lookup fields are reconciled:

- Lookup.SAP.R3.Roles
- Lookup.SAP.R3.TimeZone
- Lookup.SAP.R3.LangComm
- Lookup.SAP.R3.UserTitle
- Lookup.SAP.R3.DecimalNotation
- Lookup.SAP.R3.DateFormat
- Lookup.SAP.R3.UserGroups
- Lookup.SAP.R3.CommType
- Lookup.SAP.R3.Profiles

The following lookup fields are *not* reconciled:

- Lookup.SAP.R3.UserType
- Lookup.SAP.R3.LockUser
- Lookup.SAP.R3.FieldNames
- Lookup.SAP.R3.FieldNamesX
- Lookup.SAP.R3.BAPIKeys
- Lookup.SAP.R3.BAPIXKeys

User Reconciliation

User reconciliation can be divided into the following:

- Reconciled SAP User Management Resource Object Fields
- Reconciled Xellerate User Fields

Reconciled SAP User Management 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
- User ID
- Start Menu
- Xellerate Type
- Alias
- Lock User
- Comm Type
- Code
- Building
- Floor
- Room No
- Function
- Decimal Notation
- Date Format
- Email
- Fax
- User Profile
- User Role

Reconciled Xellerate User Fields

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

- User ID
- FirstName
- LastName
- Organization
- Email
- Employee Type
- User Type

Provisioning Module

Provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. You use the Administrative and User Console to perform provisioning operations.

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Framework Guide* for conceptual information about provisioning

For this target system, the following fields are provisioned:

- User ID
- Password
- First Name
- Last Name

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 User Management
Update User	Provisioning	Updates a user in SAP User Management
Delete User	Provisioning	Deletes a user from SAP User Management
Lock User	Provisioning	Locks a user in SAP User Management
UnLock User	Provisioning	Unlocks a user in SAP User Management
Add User Role	Provisioning	Adds a role to a user in SAP User Management
Add User Profile	Provisioning	Adds a profile to a user in SAP User Management
Remove User Role	Provisioning	Removes the role of a user in SAP User Management
Remove User Profile	Provisioning	Removes the profile of a user in SAP User Management
List Roles of User	Provisioning	Lists the roles of a user in SAP User Management
List Profiles of User	Provisioning	Lists the profiles of a user in SAP User Management
List All Roles	Provisioning	Lists all the roles present in SAP User Management
List All Profiles	Provisioning	Lists all the profiles present in SAP User Management
Reconciliation Insert Received	Reconciliation	Creates a user in Oracle Identity Manager if a user is created in SAP User Management
Reconciliation Update Received	Reconciliation	Updates a user in Oracle Identity Manager if a user is updated in SAP User Management

Function	Type	Description
Reconciliation Delete Received	Reconciliation	Deletes a user from Oracle Identity Manager if a user is deleted from SAP User Management

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

Multilanguage Support

This release of the connector supports the following languages:

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

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

Files and Directories That Comprise the Connector

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

`Enterprise Applications/SAP Enterprise Applications/SAP User Management`

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`BAPI/xlsapcar.sar`	This file contains information for configuring the SAP system so that the connector is able to access the APIs on the target system.
`lib/SAPAdapter.jar`	This file contains all the classes and definitions required for provisioning, reconciliation, and troubleshooting.
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.

File in the Installation Media Directory	Description
test/troubleshoot/troubleShootingUtility.class	This utility is used to test connector functionality.
test/troubleshoot/global.properties	This file is used to specify the parameters and settings required to connect to the target system by using the testing utility.
test/troubleshoot/log.properties	This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility.
xml/SAPBIWResourceObject.xml	This file contains definitions for the following components of the SAP BIW connector: ■ IT resource definition ■ SAP User form ■ Lookup definitions ■ Connectors ■ Resource object ■ Reconciliation scheduled tasks
xml/SAPBIWXLResourceObject.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.
xml/SAPCRMResourceObject.xml	This file contains definitions for the following components of the SAP CRM connector: ■ IT resource definition ■ SAP User form ■ Lookup definitions ■ Connectors ■ Resource object ■ Process definition ■ Reconciliation scheduled tasks
xml/SAPCRMXLResourceObject.xml	This file is used only if the connector is configured as a trusted source. The SAPCRMXLResourceObject.xml file contains only the Oracle Identity Manager resource objects and dependent values.
xml/SAPR3ResourceObject.xml	This XML file contains definitions for the following components of the connector: ■ IT resource definition ■ SAP User form ■ Lookup definitions ■ Adapters ■ Resource object ■ Process definition ■ Reconciliation scheduled tasks
xml/SAPR3XLResourceObject.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.

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 Files" section on page 2-2 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

You can use any one of the following methods to determine the release number of the connector.

Before Deployment

To determine the release number of a connector:

1. Extract the contents of the `SAPAdapter.jar` file. This file is in the following directory on the installation media:

   `Enterprise Applications/SAP Enterprise Applications/SAP User Management/lib`

2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `SAPAdapter.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 `SAPAdapter.jar` file after deployment, you can use this method to determine the release number of the connector at any stage. After you deploy the connector, it is recommended that you use the "After Deployment" method, which is described in the following section.

After Deployment

To determine the release number of a connector that has already been deployed:

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

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 systems	The target system can be any one of the following: ■ SAP User Management Basis 4.6 ■ WAS 6.20 ■ mySAP2004(CP9.0.3.1) ■ mySAP2005(CP9.0.3.1)

External code	The following SAP custom code files:
	`sapjco.jar` version 2.1.8
	For Microsoft Windows:
	`sapjcorfc.dll`
	`librfc32.dll`
	
	Version: 2.1.8
	For Solaris and Linux:
	`libsapjcorfc.so`
	`librfccm.so`
	
	Version: 2.1.8

Item	Requirement
Target system user account	Create a user account, and assign it to the SAP_ALL and SAP_NEW groups. You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-11. If this target system user account is not assigned the specified rights, then the following error message may be displayed during connector operations: SAP Connection JCO Exception: User TEST_USER has no RFC authorization for function group SYST

Step 2: Copying the Connector Files and External Code Files

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 directory on the installation media:

Enterprise Applications/SAP Enterprise Applications/SAP User Management

Refer to the "Files and Directories That Comprise the Connector" section on page 1-5 for more information about these files.

File in the Installation Media Directory	Destination Directory
BAPI/xlsapcar.sar	This file can be copied to any location on the target system. For example: C:/xlsapcar/ Refer to the "Extracting the Request Files" section on page 2-9 for more information.
lib/SAPAdapter.jar	*OIM_home*/xellerate/SAP/lib *OIM_home*/xellerate/JavaTasks
Files in the resources directory	*OIM_home*/xellerate/connectorResources
Files in the test directory	*OIM_home*/xellerate/SAP/test
Files in the xml directory	*OIM_home*/xellerate/SAP/xml

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.

Note: Ensure that you are using version 2.1.8 of the sapjco.jar file.

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

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

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

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

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

Changing to the Required Input Locale

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

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

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Step 2: Copying the Connector Files and External Code Files" section on page 2-2, you copy files from the `resources` directory on the installation media into the *`OIM_home`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

   Note: You must perform Step 1 before you perform Step 2. If you run the command described in Step 2 as follows, then an exception is thrown:

   `OIM_home``/xellerate/bin/`*`batch_file_name`*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

   `OIM_home``/xellerate/config/xlConfig.xml`

Enabling Logging

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- INFO

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

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

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

- FATAL

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

- OFF

  This level disables logging for all events.

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

- **BEA WebLogic**

  To enable logging:

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

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

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

     For example:

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

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

  WebLogic_home/user_projects/domains/*domain_name*/*server_name*/*server_name*.log

- **IBM WebSphere**

  To enable logging:

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

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

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

     For example:

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

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

WebSphere_home/AppServer/logs/*server_name*/startServer.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBoss_home*/server/default/conf/log4j.xml file, locate or add the following lines:

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

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

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

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

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

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

  JBoss_home/server/default/log/server.log

- **OC4J**

  To enable logging:

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

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

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

     For example:

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

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

  OC4J_home/opmn/logs/default_group~home~default_group~1.log

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

Gathering Required Information

The following information is required to configure the target system:

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

- Login details of an admin user having the permissions required to import requests
- Client number of the server on which the request is to be imported
- System number
- Server IP address
- Server name
- User ID of the account to be used for connecting to the SAP application server
- Password of the account to be used for connecting to the SAP application server

Creating an Entry in the BAPIF4T Table

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

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

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

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

Importing the Request

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

Object Type	Object Name
Package	ZBAPI

Object Type	Object Name
Function Group	ZXLGROUP
	ZXLHELPVALUES
	ZXLPROFILE
	ZXLROLE
	ZXLUSER
Message class	ZXLBAPI
Program	ZF4HLP_DATA_DEFINITIONS
	ZMS01CTCO
	ZMS01CTCO1
	ZMS01CTP2
	ZXLGROUP
	ZXLHELPVALUES
	ZXLPROFILE
	ZXLROLE
	ZXLUSER
Business object types	ZXLGROUP
	ZXLHELP
	ZXLPROFILE
	ZXLROLE
	ZXLUSER
Table	ZXLBAPIMODE
	ZXLBAPIMODM
	ZXLSTRING

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

Importing the request into SAP involves the following steps:

- Downloading the SAPCAR Utility
- Extracting the Request Files
- Performing the Request Import Operation

Downloading the SAPCAR Utility

The two files, Data file and Cofile, that constitute the request are compressed in the `xlsapcar.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:/xlsapcar`

Extracting the Request Files

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

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

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

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

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

   `K900863.I47` (Cofile)

   `R900863.I47` (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 (`K900863.I47`) and Data file (`R900863.I47`), the transport request number is `900863`.

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 ZBAPI package in the ABAP objects.

Step 5: Importing the Connector XML File

As mentioned in the "Files and Directories That Comprise the Connector" section on page 1-5, the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

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 XML file.
   - If the target system is SAP R3, then open the `SAPR3ResourceObject.xml` file.
   - If the target system is BIW, then open the `SAPBIWResourceObject.xml` file.
   - If the target system is SAP CRM, then open the `SAPCRMResourceObject.xml` file.

   These files are in the *`OIM_home`*`/Xellerate/SAP/xml` directory. Details of the XML file that you select 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 R3 IT Resource` IT resource is displayed.
8. Specify values for the parameters of the `SAP R3 IT Resource` IT resource. Refer to the table in the "Defining IT Resources" section on page 2-11 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. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file,

you must remove these entities 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 the SAP Change Password Function" section on page 2-12.

Defining IT Resources

You must specify values for the `SAP R3` IT resource parameters listed in the following table.

Parameter	Description	Sample Value
`SAPClient`	SAP client ID	`800`
`SAPHost`	SAP host IP address	`172.20.70.204`
`SAPLanguage`	SAP language	`EN`
`SAPUser`	SAP user of the target SAP system	`xellerate`
`SAPPassword`	Password of 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/sapcryp to.dll`
`SAPsnc_mode`	If SNC is enabled on the SAP server, then set this field to 1. Otherwise, set it to 0. **Note:** It is recommended that you enable SNC to secure communication with the target system.	`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`
`SAPsnc_qop`	Specifies the protection level (quality of protection, QOP) at which data is transferred The default value is 3. The value can be any one of the following: ■ 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 For example, `R3`, `BIW`, and `CRM`. This is optional.	`R3`

Parameter	Description	Sample Value
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
CustomizedReconQuery	Query condition on which reconciliation must be based If you specify a query condition for this parameter, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then do not specify a value for this parameter. The query can be composed with the AND (&) and OR (|) logical operators. For more information about this parameter, refer to the "Partial Reconciliation" section on page 3-1.	firstname=John

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

Step 6: Configuring the SAP Change Password Function

You can configure the Change Password function to modify password behavior in scenarios such as when a user profile on the target system gets locked or expires. For such scenarios, you can configure the system so that the administrator is not able to reset the password for a locked or expired user profile. This helps prevent discrepancies between data in Oracle Identity Manager and the target system.

To configure the Change Password function:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Process Management** folder.
3. Open the **Process Definition** form.
4. Select the SAP R3 Process process definition.
5. Double-click the **Password Updated** task.
6. On the Integration tab, specify values for the following parameters:
   - validityChange: This is a flag that can be assigned the value true or false.
     - true: If the user's validity period has expired, then it is extended to the date specified in the validityDate parameter.
     - false: If the user's validity period has expired, then it is not extended and the user's password cannot be changed.

- lockChange: This is a flag that can be assigned the value true or false.
  - true: If the user is locked (not by the administrator), then the user is unlocked before the password is changed. If the user is locked by the administrator, then the password cannot be changed.
  - false: If the user is locked, then the password cannot be changed.
- validityDate: This is the date up to which the user's validity must be extended. The date must be in the following format:

  ```
  Dec 28, 2005 at 11:25:00 GMT+05:30
  ```

  If this field is empty, then the user will be valid for an indefinite period.
- userGroupCheck: This is a string literal with the following format:

  ```
  user_group_to_check, flag(1|0),
  user_group_to_be_updated_after_reset_password
  ```

  This parameter can be an empty string if there are no groups to check when the password is reset.

  If the password is to be changed and if the user belongs to that group, then the value of the flag is 1. If the password is *not* to be changed and if the user belongs to that group, then the value of the flag is 0.

  To check multiple users, add the record for each user to this string. Use the semicolon (;) as the delimiter. For example:

  ```
  user_group_to_check, flag(1|0),
  user_group_to_be_updated_after_reset_password;
  user_group_to_check, flag(1|0),
  user_group_to_be_updated_after_reset_password
  ```

  For example, if there is a user group named Inactive that is to be checked when a password is changed and if the user is assigned to this group, then the user must be moved to the Active group after the password change.

  Given the preceding scenario, the setting of the userGroupCheck parameter is as follows:

  ```
  INACTIVE,1,ACTIVE;
  ```

  If there is a group named Terminated that is to be checked when a password is changed and if the user is assigned to this group, then the password change must not be permitted. Given this scenario, the setting of the userGroupCheck parameter is as follows:

  ```
  TERMINATED,0,;
  ```

  The userGroupCheck configuration parameter has only two types of user group records:

  - User group for which password change is to be done along with user group update:

    ```
    INACTIVE,1,ACTIVE;
    ```

  - User group for which password change is not to be done:

    ```
    TERMINATED,0,;
    ```

If the user is assigned to a group that is not in the `userGroupCheck` parameter, then the password is changed. Password change would be permitted for all user groups that are not mentioned in the configuration parameter value.

Note: The values specified are case-sensitive and must match the case in the SAP system.

Step 7: Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System

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

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

This section discusses the following topics:

Prerequisites for Configuring the Connector to Use SNC

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 R3 IT Resource` IT resource object:

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

   See Also: The "Defining IT Resources" section on page 2-11

3

Configuring the Connector

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

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

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

Configuring Reconciliation

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

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

Partial Reconciliation

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

For this connector, you create a filter by specifying values for the `CustomizedReconQuery` IT resource parameter while performing the procedure described in the "Defining IT Resources" section on page 2-11.

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

Oracle Identity Manager Attribute	SAP User Management Attribute
User ID	userid
First Name	`firstname`
Last Name	`lastname`
Language	`langcomm`
User Type	`usertype`
Department	`department`
Functions	`function`
Country	`country`
User Group	`usergroup`
User Profile	`userprofile`
User Role	`userrole`

The following are sample query conditions:

- `firstname=John&lastname=Doe`

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

- `firstname=John&lastname=Doe|usergroup=contractors`

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

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

  – The user belongs to the `contractors` user group.

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

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

- For the target system attributes, you must use the same case (uppercase or lowercase) as given in the table shown earlier in this section. This is because the attribute names are case-sensitive.
- You must not include unnecessary blank spaces between operators and values in the query condition.

  A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

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

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

  In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.

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

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

- The query condition must be an expression without any braces.
- Searching users based on multiple value roles and groups are not supported. Only one value for roles and profiles can be queried at a time. For example, if the query condition is `Usergroup=a,b,c`, then the query generates an error.
- Searching users based on more than three user attributes are not supported. For example, if the query condition is `userid=JOHN&firstname=John&lastname=Doe&country=US`, then the query generates an error.

You specify a value for the `CustomizedReconQuery` parameter while performing the procedure described in the "Defining IT Resources" section on page 2-11.

Batched Reconciliation

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

You can configure batched reconciliation to avoid such problems.

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

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

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

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

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

Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

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

Configuring trusted source reconciliation involves the following steps:

1. Depending on the target system that you use, import the XML file for trusted source reconciliation, `SAPR3XLResourceObject.xml`, `SAPBIWXLResourceObject.xml`, or `SAPCRMXLResourceObject.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.
2. Set the `IsTrusted` scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which is described later in this guide.

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Depending on the target system that you use, locate and open the `SAPR3XLResourceObject.xml`, `SAPBIWXLResourceObject.xml`, or `SAPCRMXLResourceObject.xml` file. These files are in the *`OIM_home`*`/Xellerate/sap/xml` directory. Details of the XML file that you select are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

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

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Step 5: Importing the Connector XML File" section on page 2-10, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure the scheduled task:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled 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 3-5 for information about the values to be specified.

   See Also: *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes
10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.
11. Repeat Steps 5 through 10 to create the second scheduled task.

After you create both scheduled tasks, proceed to the "Configuring Provisioning" section on page 3-7.

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 `R3LookUpRecon` 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.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Attribute	Description	Sample Value
`ITResource`	Name of the IT resource for setting up a connection to the SAP User Management server	`SAP R3 IT Resource`
`Server`	SAP server type The value can be `R3`, `BIW`, or `CRM`.	`R3`

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 `R3 Recon` user reconciliation scheduled task.

Note:

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

Attribute	Description	Sample Value
`Organization`	Default organization assigned to a new user	`Xellerate Users`
`Role`	Default role assigned to a new user	`Consultant`
`Xellerate Type`	Default type assigned to a new user	`End-User Administrator`
`ITResource`	Name of the IT resource for setting up a connection to the SAP User Management server	`SAP R3 IT Resource`
`ResourceObject`	Name of the resource object into which users must be reconciled You must ensure that the value of this attribute is the same as the decode value of the `ResourceObjectName` code key in the `Lookup.SAP.R3.FieldNames` lookup definition. **See Also:** *Oracle Identity Manager Design Console Guide* for information about modifying lookup definitions	`SAP R3 Resource Object`
`IsTrusted`	Configuration for a trusted or nontrusted target If it is set to `True`, then the target is a trusted target. If it is set to `False`, then the target is a nontrusted target. The default value is `False`.	`False`
`Server`	SAP server type The value can be `R3`, `BIW`, or `CRM`.	`R3`
`StartRecord`	Start record for the batching process This attribute is also discussed in the "Batched Reconciliation" section on page 3-3.	`1`
`BatchSize`	Number of records that must be there in a batch This attribute is also discussed in the "Batched Reconciliation" section on page 3-3.	`3`
`NumberOfBatches`	Number of batches that must be reconciled This attribute is also discussed in the "Batched Reconciliation" section on page 3-3.	Default value: `All Available` (for reconciling all users) Sample value: `50`

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

Stopping Reconciliation

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

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

Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. Refer to the "Supported Functionality" section on page 1-4 for a listing of the provisioning functions that are available with this connector.

Note: You must perform the procedure described in this section if you want to use the provisioning features of the connector.

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

See Also: The "Supported Functionality" section on page 1-4 for a listing of the provisioning functions that are available with this connector

- `SAP R3 Create User`
- `SAP R3 Modify User`
- `SAP R3 Modify UserX`
- `SAP R3 Password Change`
- `SAP R3 Lock UnLock User`
- `SAP R3 Delete User`
- `SAP R3 Add Role`
- `SAP R3 Delete Role`
- `SAP R3 Add Profile`
- `SAP R3 Remove Profile`
- `PrePopulate SAP Form`
- `PrepopulateR3UserId`

You must compile these adapters before they can be used in provisioning operations.

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 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.

If you want to compile one adapter at a time, then use the Adapter Factory form.

See Also: *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms

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.

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 User Management.

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

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

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

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

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

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

   The Resource Objects form is in the Resource Management folder. The `SAP R3 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 R3 IT Resource` 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_SAPR3` (SAP R3)
   - `UD_SAPR3ROL` (SAP R3 role form)
   - `UD_SAPR3PRO` (SAP R3 profile form)

   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 R3 Process` process definition is created when you import the connector XML file. You can use this process definition as the template for creating the remaining process definitions.

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

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

5. Configure reconciliation for each target system installation. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:

   - `ITResource`
   - `ResourceObject`
   - `IsTrusted`

   Set the `IsTrusted` attribute to `True` for the SAP User Management installation that you want to designate as a trusted source.

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 User Management installation to which you want to provision the user.

4

Testing and Troubleshooting

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

- Running Test Cases
- Troubleshooting

Running Test Cases

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

To use the testing utility:

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

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

Section	Information
SAP User Management connection parameters	Connection parameters required to connect to the target system Refer to the "Defining IT Resources" section on page 2-11 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/SAPAdapter.jar
   OIM_home/xellerate/lib/xlLogger.jar
   OIM_home/xellerate/lib/xlUtils.jar
   OIM_home/xellerate/lib/xlAPI.jar
   OIM_home/xellerate/JavaTasks/sapjco.jar
   ```

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

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

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

```
OIM_home/Xellerate/sapcua/test/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.

4. Perform the following tests:

- Enter the following command to create a user:

```
java
-DTproperties=OIM_home/Xellerate/SAP/test/troubleshoot/troubleshoot.propert
ies
-Dlog4j.configuration=file:/OIM_home/Xellerate/SAP/test/troubleshoot/log.pr
operties TroubleShootingUtility C
```

- Enter the following command to modify a user:

```
java
-DTproperties=OIM_home/Xellerate/SAP/test/troubleshoot/troubleshoot.propert
ies
-Dlog4j.configuration=file:/OIM_home/Xellerate/SAP/test/troubleshoot/log.pr
operties TroubleShootingUtility M
```

- Delete a user as follows:

```
java
-DTproperties=OIM_home/Xellerate/SAP/test/troubleshoot/troubleshoot.propert
ies
-Dlog4j.configuration=file:/OIM_home/Xellerate/SAP/test/troubleshoot/log.pr
operties TroubleShootingUtility D
```

- Enter the following command to test reconciliation from the timestamp specified to the current time:

```
java
-DTproperties=OIM_home/Xellerate/SAP/test/troubleshoot/troubleshoot.propert
ies
-Dlog4j.configuration=file:/OIM_home/Xellerate/SAP/test/troubleshoot/log.pr
operties TroubleShootingUtility R
```

Testing Partial Reconciliation

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

- Simple queries with user attributes

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

  The users with first name `John` are reconciled.

- Queries with '&' and '|' logical operators
  - Value assigned to the `CustomizedReconQuery` parameter: `firstname=John&lastname=Doe`

    The users with first name `John` and last name `Doe` are reconciled.
  - Value assigned to the `CustomizedReconQuery` parameter: `firstname=John&userrole=ASAP_AUTORENUMGEBUNG`

    Only the users with first name `John` and who belong to the `ASAP_AUTORENUMGEBUNG` role are reconciled.

    Note: The code key for user role is used to get the exact value of each role or profile.

- Queries with time stamps
  - Value assigned to the `CustomizedReconQuery` parameter: None

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

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

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

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

Testing Batched Reconciliation

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

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

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

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

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

Troubleshooting

The following table lists solutions to a commonly encountered problem associated with this connector.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to SAP User Management. **Returned Error Messages** Connection error encountered **Returned Error Code** CONNECTION_ERROR	■ Ensure that SAP User Management is running. ■ Ensure that the connection parameters for the SAP User Management server have been correctly specified. ■ Check that information in the IT resource, such as the user name and password, are correct. ■ If required, restart SAP User Management.

5

Known Issues

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

- The connection pool implementation is not feasible because the Oracle Identity Manager architecture does not support it.
- Creation of a user on the SAP system involves running the Create User and Change Password functions in a sequence. This sequence 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. The commit is enforced by the SAP architecture. This architecture constraint of SAP makes it infeasible to conduct transactions such as Create User and Change Password.
- 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 new user is created, the user is assigned a dummy password and after user creation the Change Password function is called 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 transparent to the user.
- 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 language 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.
- The connector uses the JCO API that supports JDK 1.4 to communicate with SAP User Management. Oracle Identity Manager supports the Oracle Containers for J2EE (OC4J) release that works on JDK 1.5. Therefore, the connector does not support OC4J.

A

Attribute Mappings Between Oracle Identity Manager and SAP User Management

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

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

Oracle Identity Manager Attribute	SAP User Management Attribute	Description
StartMenu	START_MENU	Default menu for the user
UserProfile	BAPIPROF	Multivalue attribute for profiles
UserRole	AGR_NAME	Multivalue attribute for roles

Index

O

P

R

S

T

U

X