Oracle® Identity Manager

Connector Guide for SAP User Management

Release 9.0.1

B31137-01

June 2006

ORACLE®

Oracle Identity Manager Connector Guide for SAP User Management, Release 9.0.1

B31137-01

Primary Author: Deepa Aswani

Contributing Authors: Lyju Vadassery, Don Gosselin

Contents

Preface

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

Note: This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for SAP 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 set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Connector Framework Guide*
- Connector guides for various third-party applications

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.1 connector documentation set, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The connector for SAP 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:

Supported Functionality

This section discusses the functions available with this connector.

Function	Type	Description
Create User	Provisioning	Creates a user in the target system
Update User	Provisioning	Updates the user in the target system
Delete User	Provisioning	Deletes a user from the target system
Lock User	Provisioning	Locks the user in the target system
UnLock User	Provisioning	Unlocks the user in the target system
Add User Role	Provisioning	Adds a role to the user in the target system
Add User Profile	Provisioning	Adds a profile to the user in the target system
Remove User Role	Provisioning	Removes the role of the user in the target system
Remove User Profile	Provisioning	Removes the profile from the user in the target system
List Roles of User	Provisioning	Lists the roles of the user in the target system

Function	Type	Description
List Profiles of User	Provisioning	Lists the profiles of the user in the target system
List All Roles	Provisioning	Lists all the roles present in the target system
List All Profiles	Provisioning	Lists all the Profiles present in the target system
Reconciliation Insert Received	Reconciliation	Inserts a user into Oracle Identity Manager if a user is created in the target system
Reconciliation Update Received	Reconciliation	Updates a user in the Oracle Identity Manager if a user is updated in the target system
Reconciliation Delete Received	Reconciliation	Deletes a user in the Oracle Identity Manager if a user is deleted in the target system

Reconciliation Module

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

- The default data elements of each reconciliation event record are Organization, Xellerate Type, and Role.
- The default labels for the data elements in each reconciliation event record are as follows:
  - `Event Linked` (for successful reconciliation)
  - `No Matched Found` (for failed reconciliation)
- The `TimeStamp` parameter present in the IT Resource is used for reconciliation. Its value is the date and time at which reconciliation was last run.
- The connector has a configurable option to specify the trusted/nontrusted reconciliation. The Task Scheduler has the `isTrusted` parameter, which you can use to specify whether you want to perform trusted or nontrusted 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`

User Reconciliation

This section discusses elements that are specific to user reconciliation with the SAP User Management connector.

Reconciled SAP R3 Resource Object Fields

The following fields are reconciled for SAP R3 resource objects:

- Extension
- Telephone
- Time Zone
- Lang Logon
- User Group
- Department
- Lang Comm
- Last Name
- First Name
- User Title
- Password
- User ID (Required Field)
- Start Menu
- User Type
- Alias
- Lock User
- Comm Type
- Code
- Building
- Floor
- Room No
- Function
- Decimal Notation
- Date Format
- Email
- Fax
- IT Resource Type
- User Profile
  - User Profile
- User Role

– User Role

For user reconciliation to work, the following fields should be available in the lookup definition. In addition, the lookup values should be reconciled before the User Recon reconciliation scheduled task is run.

- `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`

Reconciled Xellerate User Fields

The following Xellerate user fields are reconciled:

- UserId
- Password
- Organization
- FirstName
- LastName
- Xellerate
- Role
- Xellerate Type

Provisioning Module

The following fields must be specified for a provisioning task to work for SAP R3 resource objects:

- User ID
- Password
- First Name
- Last Name

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are compressed in the `SAP User Management Rev 3.1.0.zip` file, which is in the following directory on the installation media:

`Enterprise Applications\SAP Enterprise Applications\`

These files and directories are listed in the following table.

File	Description
xml\SAPR3ResourceObject.xml	This XML file contains all the components of the SAP R3 connector. These components include the following objects for SAP R3: ■ IT Resource definition ■ SAP User form ■ Lookup definitions ■ Connectors ■ Resource object ■ Process definition ■ Reconciliation tasks ■ Task Scheduler
xml\SAPR3XLResourceObject.xml	This file is used only if the connector is configured as a trusted source. The SAPR3XLResourceObject.xml file contains only the Oracle Identity Manager resource objects and dependent values.
xml\SAPCRMResourceObject.xml	This file contains all the components of the SAP CRM connector. These components include the following objects for SAP CRM: ■ IT Resource definition ■ SAP User form ■ Lookup definitions ■ Connectors ■ Resource object ■ Process definition ■ Reconciliation tasks ■ Task Scheduler
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\SAPBIWResourceObject.xml	This file contains all the components of the SAP BIW connector. These components include the following objects for SAP BIW: ■ IT Resource definition ■ SAP User form ■ Lookup definitions ■ Connectors ■ Resource object ■ Reconciliation tasks ■ Task Scheduler
SAPBIWXLResourceObject.xml	This file is used only if the connector is configured as a trusted source. The SAPBIWXLResourceObject.xml file contains only the Oracle Identity Manager resource objects and dependent values.
lib\XLSAPAdapter.jar	This file contains all the classes and definitions required for provisioning, reconciliation, master maintenance, and troubleshooting.

File	Description
BAPI\xlsapcar.sar	This file contains information for configuring the SAP system for the connector to be able to access the APIs on the target system.
troubleshoot\log.properties troubleshoot\troubleshoot.properties	Property files where you can specify connection and task parameters.
troubleshoot\TroubleShootingUtility.class	The TroubleShootingUtility class file used to test the connector and debug any issues.
External 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	You can download these files from the SAP service Web site at https://websmp104.sap-ag.de/connectors This file is part of the Java connector *java_connector*.zip file. **Note:** A valid SAP license is required to download these files.
docs\B31137_01.pdf docs\html	Oracle Identity Manager Connector Guide for SAP User Management

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

2

Deploying the Connector

Deploying the connector involves the following steps:

- Step 1: Verifying Deployment Requirements
- Step 2: Copying the Connector Files and External Code
- Step 3: Configuring the Target System
- Step 4: Importing the Connector XML File
- Step 5: Configuring Reconciliation
- Step 6: Compiling Adapters
- Step 7: Changing the SAP Password Behavior
- Step 8: Configuring the Connector to Use SNC

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target system host platforms	SAP 4.6C, SAP 4.7, SAP BIW 3.1, SAP CRM 4.0, SEM BCS on BIW3.1
External code	SAP custom code (`sapjco.jar`, `librfc32.dll`, and `sapjcorfc.dll`)
Other systems	SAP JCO
SAP JCO	Version 2.0.10

Step 2: Copying the Connector Files and External Code

Create the `SAP`, `xml`, `lib`, and `docs`, and `xlsapcar` directories in the paths indicated, and then copy the files to the destinations specified in the following table:

File to Be Copied	Destination
xml\sapbiwresourceobject.xml xml\sapcrmresourceobject.xml xml\sapr3resourceobject.xml xml\SAPBIWXLResourceObject.xml xml\SAPCRMXLResourceObject.xml xml\SAPR3XLResourceObject.xml	*OIM_HOME*\Xellerate\SAP\xml
lib\SAPAdapter.jar	*OIM_HOME*\Xellerate\SAP\lib *OIM_HOME*\Xellerate\JavaTasks\
BAPI\xlsapcar.sar	C:\xlsapcar\
docs\B31137_01.pdf docs\html	*OIM_HOME*\Xellerate\SAP\docs

See Also: Files and Directories That Comprise the Connector

To copy the external code into the correct location:

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

   To do this:

   a. Open the following page in a Web browser:

      https://websmp104.sap-ag.de/connectors

   b. Open the SAP JAVA Connector page by selecting **Application Platform, Connectivity, Connectors, SAP Java Connector,** and **Tools & Services.**

   c. On the SAP JAVA Connector page, links for files that you can download are displayed on the right pane. Click the link for the SAP JCo release that you want to download.

   d. In the dialog box that is displayed, specify that you want to save the file with the following name and path:

      OIM_HOME\Xellerate\SAP\lib\SAP_JCO.zip

2. Extract the SAP_JCO.zip file in the C:\xlsapcar\ directory.
3. Check if the sapjco.jar, librfc32.dll, and sapjco.dll files are extracted in the directory.
4. Copy the *OIM_HOME*\Xellerate\SAP\lib\sapjco.jar file into the *OIM_HOME*\Xellerate\JavaTasks directory.
5. To set the path to the system variables:
   - On Microsoft Windows:
     - To enable access to the SAP DLLs at run time, add *OIM_HOME*\Xellerate\SAP\lib\ to the system PATH variable.
   - On Solaris:
     - To enable access to the SAP DLLs at run time, add *OIM_HOME*\Xellerate\SAP\lib\ to the system LD_LIBRARY_PATH variable.

Step 3: Configuring the Target System

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

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

Manual Entry in SAP

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

Table Maintenance for BAPIF4T

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

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

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

Transport System Method

This section discusses the transport system method.

SAP Transport Request

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

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

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

1. Log on to the SAP Web site at

   https://service.sap.com/swdc

2. Select a digital certificate.
3. Enter your SAP user name and password to connect to the SAP service marketplace.
4. Click **Downloads**, **SAP Support Packages**, **Entry by Application Group**, and **Additional Components.**
5. Select **SAPCAR, SAPCAR 6.20,** and the operating system. This displays the download object.
6. Select the **Object** check box, and then click **Add to Download Basket.**

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

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

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

      This command extracts the `K900208.I46` (Cofile) and `R900208.I46` (Data file) files into this directory.
4. The SAP Basis administrator must copy these files to the SAP server in their respective locations, and then import these requests in SAP like other transport requests.
5. Check the log file to determine whether or not the transport was successful by clicking on the request number in transaction code STMS. Check the error codes in the log file. If the return code is 4, then the import ended with warnings. This usually happens if the object is overwritten or already exists in SAP system. If the return code is 8 and greater then it means that there are errors in the imports. To view error details, click on the detail log. This log is useful for analyzing any issues related to transport.

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

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

Step 4: Importing the Connector XML File

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the xml file.

- If the Target system is R3 locate SAPR3ResourceObject.xml file
- If the Target system is BIW locate SAPBIWResourceObject.xml file
- If the Target system is CRM locate SAPCRMResourceObject.xml file

which is in the *OIM_HOME*\Xellerate\SAP\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 OIM_HOME IT resource is displayed.
8. Specify values for the parameters of the SAP R3 IT resource. Refer to the table in the Defining IT Resources section for information about the values to be specified.
9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the SAP IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

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

11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. You must remove these nodes. To do this, right-click each such node and then select **Remove.**
12. Click **Import**. The connector file is imported into Oracle Identity Manager.
13. If you plan to use the connector in trusted source reconciliation mode, then perform the same procedure to import the SAPR3XLResourceObject.xml file. This file is in the *OIM_HOME*\Xellerate\sap\xml directory.

    Caution: Only one connector can be configured as a trusted source. If you import the SAPR3XLResourceObject.xml, SAPBIWXLResourceObject.xml, or SAPCRMXLResourceObject.xml file while you have another trusted source configured, then both connector reconciliations would stop working.

After importing the connector XML file, proceed to Step 6: Compiling Adapters.

Defining IT Resources

You need to specify values for the SAP R3 IT resource parameters listed in the following table.

Parameter	Sample Value	Description and Sample Values
SAPClient	800	SAP client ID
SAPHost	172.20.70.204	SAP host IP address
SAPLanguage	EN	SAP language

Parameter	Sample Value	Description and Sample Values
SAPUser	xellerate	SAP user of the target SAP system
SAPPassword	changethis	Password of SAP user
SAPsnc_lib	c:\\usr\\sap\\sapcrypto.dll	Path where the crypto library is placed. This is required only if Secure Network Communication (SNC) is enabled.
SAPsnc_mode	0	If SNC is enabled on the SAP server, then set this field to 1. Otherwise, set it to 0.
SAPsnc_myname	p:CN=TST,OU=SAP, O=ORA,c=IN	SNC system name This is required only if SNC is enabled.
SAPsnc_partnername	p:CN=I47,OU=SAP, O=ORA, c=IN	Domain name of the SAP server This is required only if SNC is enabled.
SAPsnc_qop	3	This parameter controls the protection level (quality of protection, QOP) at which data is transferred. The default value is 3. Valid values are: ■ 1: Secure authentication only ■ 2: Data integrity protection ■ 3: Data privacy protection ■ 8: Use value from the parameter ■ 9: Use maximum value available This is required only if SNC is enabled.
SAPSystemNo	00	SAP system number
SAPType	R3	Type of SAP system.For example, R3, BIW, CRM. This is optional.
TimeStamp	Nov 16, 2004 at 11:35:00 IST	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.

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

Step 5: Configuring Reconciliation

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

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager should attempt to complete the task before assigning the ERROR status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.

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

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

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

After you create both scheduled tasks, proceed to the Step 6: Compiling Adapters section.

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	Sample Value	Description
`Password`	`Dummy`	Default password taken while creating the Xellerate User
`Organization`	`Xellerate Users`	Default organization assigned to a new user
`Role`	`Consultant`	Default role assigned to a new user
`Xellerate Type`	`End-User Administrator`	Default type assigned to a new user
`ITResource`	`SAP R3 IT Resource`	Name of the IT Resource for setting up a connection with the SAP system

Attribute	Sample Value	Description
ResourceObject	SAP R3 Resource Object	Resource object name into which users need to be reconciled
Server	R3	SAP Server Type (R3, BIW, CRM)

After you specify values for these task attributes, go 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 Name	Sample Value	Description
Password	Dummy	Default password taken while creating the Xellerate User
Organization	Xellerate Users	Default organization assigned to a new user
Role	Consultant	Default role assigned to a new user
Xellerate Type	End-User Administrator	Default type assigned to a new user
ITResource	SAP R3 IT Resource	Name of the IT Resource for setting up a connection to SAP
ResourceObject	SAP R3 Resource Object	Resource object name into which users need to be reconciled
IsTrusted	False	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.
FirstTimeReconRecords	5000	Number of records to be fetched during first-time reconciliation, if reconciliation scheduled task times out. Initially, OIM tries to fetch all records. If process times out, then it tries to fetch the number of records specified by this parameter. If the task times out with this number also, OIM tries to fetch records by recursively dividing this number by 2 in event of time out, until all records have been fetched from the target system.
Server	R3	SAP Server Type (R3, BIW, CRM)

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

See Also: Reconciliation Module

Step 6: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when the connector XML file is deployed. You must compile these adapters before you can use them to provision accounts on the target system.

- 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

Note: To compile multiple adapters simultaneously, use the Adapter Manager form. To compile one adapter at a time, use the Adapter Factory form.

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 the **Compile All** option.

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

   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 adapters that you specify.

   See Also: *Oracle Identity Manager Design Console Guide* for instructions on how to use these 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.

Step 7: Changing the SAP Password Behavior

This connector has the following configuration parameters that affect the behavior of the Change Password functionality:

- `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. The password is changed after this date.
  - `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 will be unlocked before the password is changed. If 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`: 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 change password is to be done and if the user has that group, then the value of the flag is `1`. If change password is *not* to be done and if the user has 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 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 casing on the SAP system.

Step 8: Configuring the Connector to Use SNC

To connect to a SAP system application server, the Java Application Server uses the Java Connector (.jco file) and RFC (.dll files). You can use Secure Network Communication (SNC) to secure such connections.

Prerequisites to Configuring the Connector to Use SNC

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

- The external security product must be installed on the server. To install the security package on the Java Application Server:

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

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

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

     This package contains the following files:

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

     – A corresponding license ticket file

     – The configuration tool, `sapgenpse.exe`

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

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

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

  5. Copy the ticket file to the `sec` directory. This is also the directory in which the Personal Security Environment (PSE) and credentials of the Java Application Server will be generated.

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

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

- You should be familiar with the SNC infrastructure. You must know which PSE the application server uses for SNC. You must also know whether you are using the same PSE for both communication partners or individual ones.
- SNC must be activated on the SAP application server.

Configuring the Connector to Use SNC

To configure the connector to use SNC:

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

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

2. Create credentials for the Java Application Server.

   The Java Application Server must have active credentials at run time to be able to access its PSE. Therefore, use the configuration tool's command-line `seclogin` to open the PSE.

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

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

   For the user specified with the `-o` option, the credentials file, `cred_v2`, is created in the `SECUDIR` directory.

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

   a. Export the OIM system certificate in the file by entering the following command:

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

   b. Import the certificate file into the SAP application server. Obtain the certificate of the SAP application server, which will need to be generated by the SAP system administrator.

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

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

4. Set the SNC parameters in the connector IT Resource object.

   You must configure the following parameters in the IT Resource:

   - `SAPsnc_lib`

- SAPsnc_mode
- SAPsnc_myname
- SAPsnc_partnername
- SAPsnc_qop

3

Testing the Connector

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

- **Provisioning testing:** This type of test involves using Oracle Identity Manager to provision or de-provision one of its users or organizations with a target resource. In other words, Oracle Identity Manager is the starting point of the connector and the target resource is the end point.
- **Reconciliation testing:** This type of test involves using Oracle Identity Manager to reconcile with either a trusted source or a target resource. In other words, the trusted source or target resource is the starting point of the connector, and Oracle Identity Manager is the end point.

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

This chapter contains the following sections:

Running Test Cases

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

The `SAP User Management_`*`versionno`*`\troubleshoot` directory contains the `troubleShoot.properties` file. The troubleshooting utility uses this file to connect to the SAP server. This file contains the following information:

- **SAP connection parameters**: Server-related information.
- **User information**: Field information required to create, modify, update, and delete a user profile.
- **Reconciliation information**: The "From date" timestamp information is passed from this file. The "To date" is set to the current time.
- **CLASSPATH information**: List of files to be included in the CLASSPATH.

This file also contains commands to test the connector functionality. You need to make the place the contents of the troubleshoot directory in the installation media in a test directory, for example: `C:\test\troubleshoot`.

Next, set the following SAP server connection parameters in the `troubleshooting.properties` file:

```
sapClient=800
sapUser=xellerate
sapPassword=project
sapLanguage=EN
sapSystem=00
sapIP=172.20.70.206
sapType=R3
SAPsnc_mode=0
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
```

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

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

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

Creating a User

To test the connector for the creation of a user, specify the following information for a new user object in the `troubleshooting.properties` file.

```
userId=R37003
password=IKK123
dummyPassword=OERFYE
lockStatus=UnLock
userGroup=SUPER
lastName=kiran
firstName=inguva
userTitle=Mr.
langComm=E
department=IT
langLogIn=N
timeZone=AUSVIC
telephone=12345678
extension=1234
Fax=12345678
email=sapuser@sap.com
dateFormat=1
decimalNotation=X
function=Function
roomNo=06
floor=1st
building=LBP
code=1
commType=FAX
alias
startMenu=000
userType
```

```
dummyPwd=INITIAL
validityDate=
validityChange=
lockChange=
pUserGroup=
```

On the command line, use the following command to create a user:

```
java -DTproperties=connector_test_directory\troubleshoot\troubleShoot.properties
-Dlog4j.configuration=file:\connector_test_directory\troubleshoot\log.properties
TroubleShootingUtility C
```

Deleting a User

Delete an SAP R3 user as follows:

```
java -DTproperties=connector_test_directory\troubleshoot\troubleShoot.properties
-Dlog4j.configuration=file:\connector_test_directory\troubleshoot\log.properties
TroubleShootingUtility D
```

Modifying a User

Specify the following parameters in the `troubleshooting.properties` file to modify a user:

```
changeUserId=cuakk21
fieldName=
fieldValue=jane
bapiKey=ADDRESS
bapiKeyX=ADDRESSX
```

Use the following command to modify a user:

```
java -DTproperties=connector_test_directory\troubleshoot\troubleShoot.properties
-Dlog4j.configuration=file:\connector_test_directory\troubleshoot\log.properties
TroubleShootingUtility M
```

Testing Reconciliation

To test reconciliation, specify a timestamp for the From Date of the reconciliation run as shown:

```
fromDate=Apr 10, 2006 at 10:00:00 GMT+05:30
```

To test reconciliation from the timestamp specified to the current time, run the following command:

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

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. **Returned Error Messages** `SAP.CONNECTION_ERROR`	■ Ensure that the SAP server is up and running. ■ Ensure that the IP Address of the SAP server is correct. ■ Check that information in the IT Resource, such as the user name and password, are correct. ■ Restart SAP server if nothing works.

4

Known Issues

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

- The connection pool implementation is not feasible because of current Oracle Identity Manager architecture support.
- Creation of a user on the SAP system involves running the Create User and Change Password use cases 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 transaction 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 eliminate 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 event 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 end user.

Index

Symbols

A

B

C

D

E

F

I

J

L

O

P

R

S

T

U

V

X