Oracle® Identity Manager

Connector Guide for SAP Enterprise Portal

Release 9.0.4

E11211-07

September 2013

ORACLE®

Oracle Identity Manager Connector Guide for SAP Enterprise Portal, Release 9.0.4

E11211-07

Primary Author: Alankrita Prakash

Contributing Authors: Debapriya Datta, Gowri G.R, Prakash Hulikere, Gauhar Khan, Devanshi Mohan

Contents

3 Using the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with SAP Enterprise Portal.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

http://www.oracle.com/technology/documentation/oim.html

Documentation Updates

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

http://www.oracle.com/technology/documentation/oim.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 Enterprise Portal?

This chapter provides an overview of the updates made to the software and documentation for the SAP Enterprise Portal connector in release 9.0.4.12.

Note: Release 9.0.4.12 of the connector comes after release 9.0.4.3. Release numbers from 9.0.4.4 through 9.0.4.11 have not been used.

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

- Software Updates

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

  These include major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

See Also: *Oracle Identity Manager Release Notes*

Software Updates

The following sections discuss software updates:

- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.1

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning
- Support for New Target System Version

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See Section 3.6.2, "Request-Based Provisioning" for more information.

Support for New Target System Version

From this release onward, SAP Enterprise Portal 7.01 with SP3 has been added to the list of supported target systems.

See Section 1.1, "Certified Components" for the full list of supported target systems.

Software Updates in Release 9.0.4.3

The following is a software update in release 9.0.4.3:

Resolved Issues

The following are issues that have been resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
7496046	During incremental reconciliation, all the users created on a given day were fetched into Oracle Identity Manager.	This issue has been resolved. Now, during incremental reconciliation, only user records that are added or modified after the time stamp are fetched into Oracle Identity Manager.
8682180	The status of the Delete User task was Rejected when the connector was configured for identity reconciliation (trusted source) mode. In addition, the status of the user remained at provisioned even after the corresponding OIM User was deleted.	This issue has been resolved. After the Delete User operation, the status of the user changes to Revoked and Delete User task changes to Completed.

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- Support for a New Version of the Target System
- Support for Batched Reconciliation
- No Requirement for External Code Files
- Other Software Updates

Support for a New Version of the Target System

This release of the connector supports SAP Enterprise Portal 7.0 SP15. Versions of the target system supported by earlier releases of the connector are desupported from this release onward.

See "Verifying Deployment Requirements" on page 2-1 for more information.

Support for Batched Reconciliation

Batched reconciliation is supported from this release onward. The BatchSize attribute has been introduced in the SAPEP UserRecon scheduled task. The FirstTimeReconRecords attribute has been removed from the scheduled task.

See "User Reconciliation Scheduled Task" on page 3-5 for more information.

No Requirement for External Code Files

Earlier releases of the connector required you to copy files from the following directory during the deployment procedure:

SAPEP_HOME/EP6J/j2ee/j2ee_00/cluster/server/

This requirement has been removed.

Other Software Updates

The following are some minor updates made in this release:

- The CustomizedReconQuery parameter has been moved from the IT resource to the SAPEP UserRecon scheduled task. In addition, the TrustedResourceObject attribute has been added to this scheduled task. See "User Reconciliation Scheduled Task" on page 3-5 for more information.
- In "Configuring Provisioning" on page 3-6, the SAP EP Email Modify adapter has been added to the list of adapters to be compiled when you deploy the connector.
- In "Testing Partial Reconciliation" on page 5-2, the list of examples for testing partial reconciliation has been modified.
- From the "Known Issues" chapter, the following point has been removed:

  "The configuration details of the SAP Enterprise Portal database are in plaintext in the sapum.properties file, the location of which is available in the IT resource definition. This poses a security threat."

Software Updates in Release 9.0.4.1

The SAPEPConnector.jar file has been split into two files, SAPEPConnector.jar and SAPEPRecon.jar. Corresponding changes have been made in the following sections:

- Files and Directories That Comprise the Connector on page 1-9
- Determining the Release Number of the Connector on page 1-10
- Copying the Connector Files and External Code Files on page 2-6

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 9.0.4.12
- Documentation-Specific Updates in Release 9.0.4.3
- Documentation-Specific Updates in Release 9.0.4.2
- Documentation-Specific Updates in Release 9.0.4.1

Documentation-Specific Updates in Release 9.0.4.12

The following documentation-specific update has been made in revision "7" of release 9.0.4.12:

Information regarding the com.sap.pdk.JavaDeveloper role has been added to Section 2.3.3, "Creating a Target System User Account for Connector Operations."

The following documentation-specific updates have been made in revision "6" of release 9.0.4.12:

- In the "Certified Components" section, changes have been made to the "Infrastructure requirements" row.
- Information in the "Using the Apache Axis JAR Files" section has been modified. In addition, the following sections have been added:
  - Setting the Classpath on Oracle WebLogic Server Running on Microsoft Windows
  - Setting the Classpath on Oracle WebLogic Server Running on Linux

Documentation-Specific Updates in Release 9.0.4.3

The following are documentation-specific updates in release 9.0.4.3:

- In "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2" on page 3-6, the status that Oracle Identity Manager assigns to a task after completing the maximum number of retries has been changed from `FAILED` to `ERROR`.
- In the "Multilanguage Support" on page 1-4, Arabic has been added to the list of languages that the connector supports.
- In the "Testing Partial Reconciliation" section, a minor change in the example for the CustomizedReconQuery parameter has been made.
- In the "Defining IT Resources" section, the SOAPAdminUserID and SOAPAdminPassword parameters have been added. There parameters have been supported from release 9.0.4.2. Similarly, the SAPUMLocation parameter has been deleted. This parameter has been deleted from release 9.0.4.2.
- The "Configuring SSL to Secure Communication Between Oracle Identity Manager and the Target System" section has been added.
- The following item has been removed from the "Known Issues" chapter:

  The connector does not support Secure Network Communication (SNC) or Secure Sockets Layer (SSL).
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target systems" row.

Documentation-Specific Updates in Release 9.0.4.2

The following are documentation-specific updates in release 9.0.4.2:

- In "Reconciled Xellerate User Fields" on page 1-7, the list of fields has been modified.
- In "Deploying Web Services on the Target System" on page 2-23, the procedure has been modified.
- In "Limited Reconciliation" on page 3-3, the row for the UserID to uniqueName field mapping has been removed. Some other changes have been made in the names of attributes for groups and roles.

Documentation-Specific Updates in Release 9.0.4.1

There are no documentation-specific updates in release 9.0.4.1.

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 external, identity-aware applications. This guide discusses the connector that enables you to use SAP Enterprise Portal either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

Note: It is recommended that you do not configure the target system as both an authoritative (trusted) source and a managed (target) resource.

This chapter contains the following sections:

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

At some places in this guide, SAP Enterprise Portal has been referred to as the **target system.**

- Section 1.8, "Roadmap for Deploying and Using the Connector"

1.1 Certified Components

Table 1–1 lists the certified components for this connector.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager release 9.0.1 through 9.0.3.2 ■ Oracle Identity Manager release 9.1.0.1 or later **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* release 1 (11.1.1) **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1).
Target systems	The target system can be one of the following: ■ SAP Enterprise Portal 7.0 This target system is also known as SAP NetWeaver 7.0. ■ SAP Enterprise Portal 7.01 with SP3 **Note:** The SAP Enterprise Portal connector is an application developed using the UME APIs. It is published as a Web Service. The application follows SAP Enterprise Portal best practices and provides the library and deployment descriptor as part of a PAR file deployment. As mentioned in the SAP documentation, the security settings are defined in the portalapp.xml file. The connector requires that the safety level be set to `high_security`. There must be no SAP Enterprise Portal configuration overriding this setting. If you have deployed additional login modules, servlet filters, or other security extensions that override the security setting, then the connector will not work correctly.
Infrastructure requirements	■ SAP Enterprise Portal running on SAP Web Application Server (WAS) ■ SAP User Management Engine (UME) 7.0 APIs must be available on the SAP Enterprise Portal ■ Apache Axis Web Services Framework 1.3
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.2, use JDK 1.4 or later in the 1.4 series. ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or later in the 1.5 series. ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 or later in the 1.6 series.

1.2 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)

- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

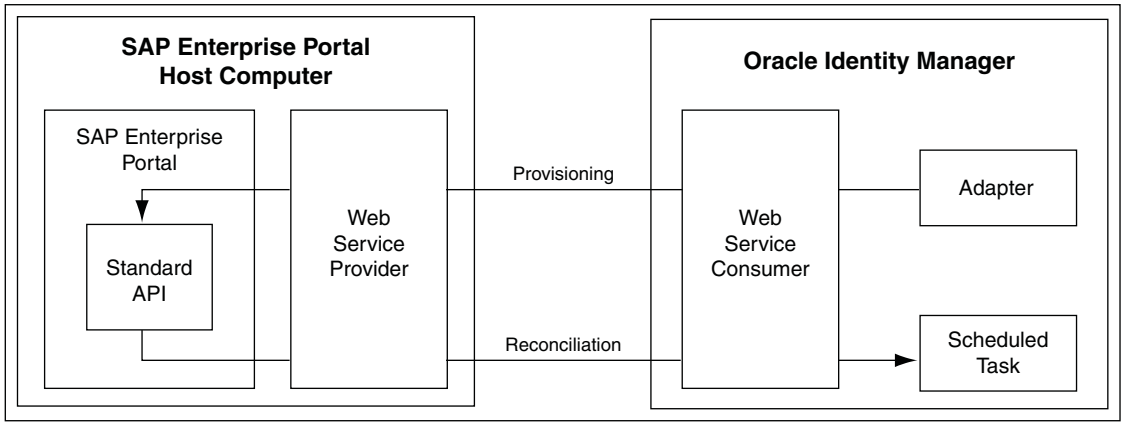
See Also: For information about supported special characters

- On Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*, see *Oracle Identity Manager Globalization Guide*.
- On Oracle Identity Manager release 11.1.1, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

1.3 Connector Architecture

The architecture of the connector is the blueprint for the functionality of the connector. Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of the Connector



The connector can be configured to run in one of the following modes:

Note: In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

- Identity reconciliation

  In the identity reconciliation mode, SAP Enterprise Portal is used as the trusted source and users are directly created and modified on it.

  During reconciliation, a scheduled task establishes a connection with the target system and sends reconciliation criteria to the APIs. The APIs extract user records that match the reconciliation criteria and hand them over to the scheduled task, which brings the records to Oracle Identity Manager.

  Each record fetched from the target system is compared with existing OIM Users. If a match is found, then the update made to the record on the target system is applied to the OIM User record. If no match is found, then the target system record is used to create an OIM User.

- Account Management

  In the account management mode, SAP Enterprise Portal is used as a target resource. The connector enables the target resource reconciliation and provisioning operations. Through provisioning operations performed on Oracle Identity Manager, user accounts are created and updated on the target system for OIM Users. During reconciliation from the target resource, the SAP Enterprise Portal connector fetches into Oracle Identity Manager data about user accounts that are created or modified on the target system. This data is used to add or modify resources allocated to OIM Users.

  During provisioning operations, adapters carry provisioning data submitted through the process form to the target system. APIs on the target system accept provisioning data from the adapters, carry out the required operation on the target system, and return the response from the target system to the adapters. The adapters return the response to Oracle Identity Manager.

  During reconciliation, a scheduled task establishes a connection with the target system and sends reconciliation criteria to the APIs. The APIs extract user records that match the reconciliation criteria and hand them over to the scheduled task, which brings the records to Oracle Identity Manager. The next step depends on the mode of connector configuration.

1.4 Features of the connector

The following are features of the connector:

- Section 1.4.1, "Support for Both Target Resource and Trusted Source Reconciliation"
- Section 1.4.2, "Support for Both Full and Incremental Reconciliation"
- Section 1.4.3, "Support for Limited Reconciliation"
- Section 1.4.4, "Support for Batched Reconciliation"

1.4.1 Support for Both Target Resource and Trusted Source Reconciliation

You can use the connector to configure SAP Enterprise Portal as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.3, "Configuring Reconciliation" for more information.

1.4.2 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, change-based or incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time.

See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for more information.

1.4.3 Support for Limited Reconciliation

You can set a reconciliation filter as the value of the CustomizedReconQuery attribute of the scheduled tasks. This filter specifies the subset of newly added and modified target system records that must be reconciled.

See Section 3.3.2, "Limited Reconciliation" for more information.

1.4.4 Support for Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See Section 3.3.3, "Batched Reconciliation" for more information.

1.5 Lookup Definitions Used During Connector Operations

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Country lookup field to select a group name for the user's initial login group. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are automatically created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

The following lookup definitions are populated with values fetched from the target system by the SAPEP LookupRecon scheduled task:

- Lookup.SAP.EP.Country
- Lookup.SAP.EP.Groups
- Lookup.SAP.EP.Language
- Lookup.SAP.EP.Roles
- Lookup.SAP.EP.TimeZone

Section 3.2, "Scheduled Task for Lookup Field Synchronization" provides information about this scheduled task.

1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning

The following sections provide information about connector objects used during target resource reconciliation and provisioning:

See Also: The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about reconciliation

- Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.2, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.3, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.4, "Provisioning Functions"

1.6.1 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–2 provides information about user attribute mappings for target resource reconciliation and provisioning.

Table 1–2 User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Attribute	Description
Street	street	Street name
City	city	City
State	state	State
Zip	zip	Zip
Country	country	Country
TimeZone	timezone	Time zone
Department	department	Department
ValidFrom	validFrom	Date from which the account on the target system is valid
ValidTo	validTo	Date up to which the account on the target system is valid
Locked	locked	Status of the account on the target system
UserID	userId	User ID
Password	password	Password
FirstName	firstname	First name
LastName	lastname	Last name
EmailID	email	E-mail address
Language	locale	Language
telephone	telephone	Telephone number
Fax	fax	Fax number
Mobile	mobile	Mobile phone number
Group	Group	Group name
Role	Role	Role name

1.6.2 Reconciliation Rule for Target Resource Reconciliation

The following is the process-matching rule:

Rule name: SAP EP Recon Rule

Rule element: User Login Equals User ID

In this rule:

- User Login is one of the following:
  - For Oracle Identity Manager releases 9.0.1 through 9.0.3.2:

    User ID attribute on the Xellerate User form
  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.1:

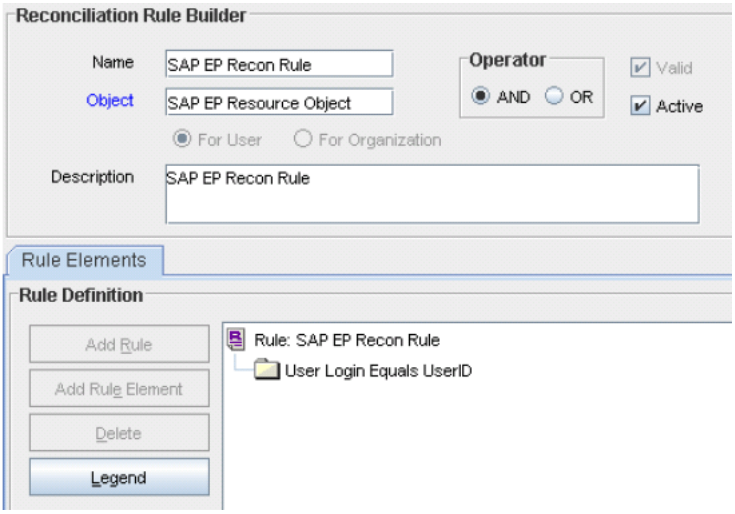
    User ID attribute on the OIM User form
- User ID is the User ID field of the account on SAP Enterprise Portal.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

> **Note:** Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Reconciliation Rules**.
3. Search for **SAP EP Recon Rule**. Figure 1–2 shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



1.6.3 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–3 lists the action rules for target resource reconciliation.

Table 1–3 Action Rules for Target Resource Reconciliation

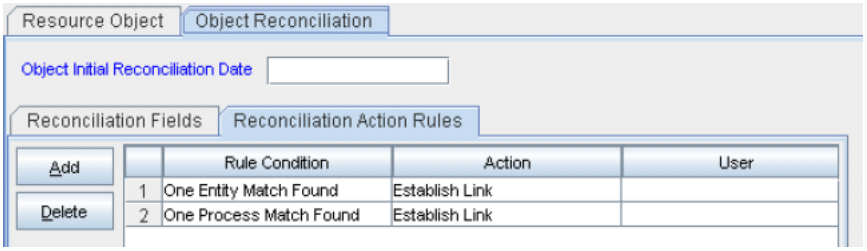
Rule Condition	Action
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. Search for and open the **SAP EP Resource Object** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rule for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules for Target Resource Reconciliation



1.6.4 Provisioning Functions

Table 1–4 lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

Table 1–4 Provisioning Functions

Function	Adapter
Create User	SAPEPCREATEUSER
Update User	SAPEPMODIFYUSER
Delete User	SAPEPDELETEUSER
Reset Password	SAPEPPASSWORDCHANGE
Lock User	SAPEPLOCKUNLOCKUSER
UnLock User	SAPEPLOCKUNLOCKUSER
Add Role	SAPEPADDROLE
Add Group	SAPEPADDGROUP
Remove Role	SAPEPREMOVEROLE
Remove Group	SAPEPREMOVEGROUP

1.7 Connector Objects Used During Trusted Source Reconciliation

The following sections provide information about connector objects used during trusted source reconciliation:

- Section 1.7.1, "User Attributes for Trusted Source Reconciliation"
- Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"
- Section 1.7.3, "Reconciliation Action Rules for Trusted Source Reconciliation"

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–5 lists user attributes for trusted source reconciliation.

Table 1–5 User Attributes for Trusted Source Reconciliation

OIM User Form Field	Target System Attribute	Description
User ID	UserLogin	User ID
First Name	First Name	First name
Last Name	Last Name	Last name
EmailID	E-mail address	E-mail address
User Type	User Type	User type
Organization	Organization	Organization

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

The following is the process matching rule:

Rule name: Trusted Source recon Rule

Rule element: User Login Equals User ID

In this rule element:

- User Login is one of the following:
  - For Oracle Identity Manager releases 9.0.1 through 9.0.3.2:

    User ID attribute on the Xellerate User form
  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.1:

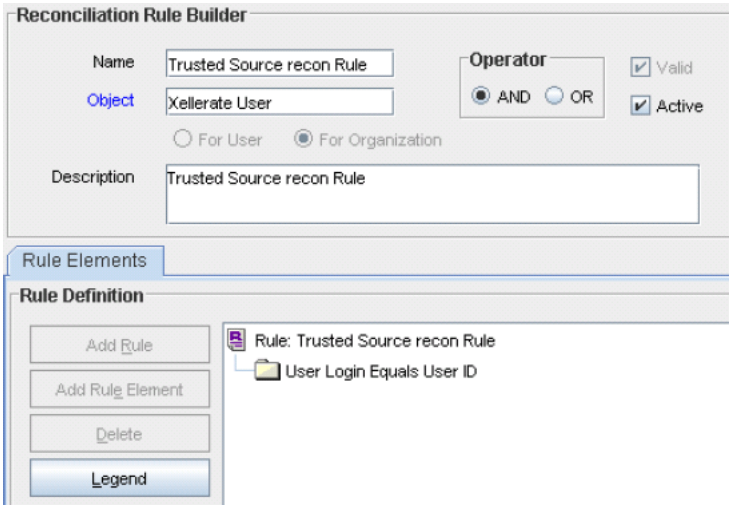
    User ID attribute on the OIM User form
- User ID is the user ID of the SAP Enterprise Portal account.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

> **Note:** Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Reconciliation Rules**.
3. Search for **Trusted Source Recon Rule**. Figure 1–5 shows the reconciliation rule for trusted source reconciliation.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–6 lists the action rules for target resource reconciliation.

Table 1–6 Action Rules for Target Source Reconciliation

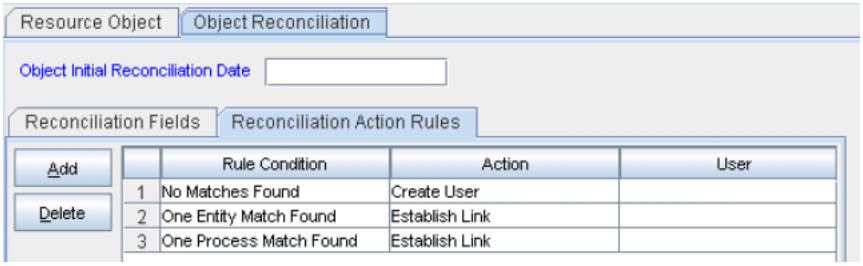
Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Xellerate User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–5 shows the reconciliation action rules for trusted source reconciliation.

Figure 1–5 Reconciliation Action Rules for Trusted Source Reconciliation



1.8 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures to perform if you want to extend the functionality of the connector.
- Chapter 5, "Testing and Troubleshooting" describes the procedure that you must perform to test the connector. In addition, this chapter provides instructions for identifying and resolving some commonly encountered errors.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.

2

Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"

2.1 Preinstallation

This section is divided into the following topics:

- Section 2.1.1, "Files and Directories on the Installation Media"
- Section 2.1.2, "Determining the Release Number of the Connector"
- Section 2.1.3, "Using the Apache Axis JAR Files"
- Section 2.1.4, "Determining the URL of the Web Service Running on the Target System"

2.1.1 Files and Directories on the Installation Media

Table 2–1 describes the files and directories on the installation media.

Table 2–1 Files and Directories On the Connector Installation Media

File in the Installation Media Directory	Description
configuration/SAPEP-CI.xml	This XML file contains configuration information that is used during connector installation.
DataSet/ModifyResourceSAP EP Resource Object.xml DataSet/ProvisionResourceSAP EP Resource Object.xml	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
lib/SAPEPConnector.jar	This JAR file contains the class files that are used to implement provisioning. During connector deployment, this file is copied to the following location: ■ For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database

Table 2–1 (Cont.) Files and Directories On the Connector Installation Media

File in the Installation Media Directory	Description
lib/SAPEPRecon.jar	This JAR file contains the class files that are used to implement reconciliation. During connector deployment, this file is copied to the following location: ■ For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
par/ConnectorService.par	This file is used to call Web services on the SAP Enterprise Portal system.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied to the following location: ■ For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
test/Troubleshoot/TroubleShootUtility.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/SAPEPResourceObject.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Process form ■ Lookup definitions ■ Adapters ■ Resource object ■ Process definition ■ Scheduled tasks
xml/SAPEPXLResourceObject.xml	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

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

2.1.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.1, then skip this section.

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME/xellerate/JavaTasks/SAPEPRecon.jar

2. Open the manifest.mf file in a text editor. The manifest.mf file is one of the files bundled inside the SAPEPRecon.jar file.

   In the manifest.mf file, the release number of the connector is displayed as the value of the Version property.

2.1.3 Using the Apache Axis JAR Files

Note: In an Oracle Identity Manager cluster, perform this step on each node of the cluster.

The Apache Axis JAR files are required for SOAP communication with the Web service running on the SAP Enterprise Portal server. The version of Axis used is axis-1_3. You can download the JAR files from the Apache Web site and copy in into the ThirdParty directory or the Oracle Identity Manager database as follows:

1. Log on to the Apache Web site at

   `http://ws.apache.org/axis/`

2. Download the zip file corresponding to the Axis 1.3 version, and then extract its contents to obtain the following JAR files:

   For JBoss Application Server

   axis-1.3.jar

   commons-discovery-0.2.jar

   For Oracle WebLogic Server

   axis-1.3.jar

   commons-discovery-0.2.jar

   commons-logging.jar

   wsdl4j-1.5.1.jar

   For IBM WebSphere Application Server

   axis-1.3.jar

3. Copy the JAR files into one of the following directories:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

  OIM_HOME/xellerate/ThirdParty

- For Oracle Identity Manager release 11.1.1:

  OIM_HOME/server/ThirdParty

If Oracle Identity Manager is running on Oracle WebLogic Server, then add the directory in which the JAR files are present to the classpath environment variable. Perform the procedures described in one of the following sections:

- Section 2.1.3.1, "Setting the Classpath on Oracle WebLogic Server Running on Microsoft Windows"
- Section 2.1.3.2, "Setting the Classpath on Oracle WebLogic Server Running on Linux"

2.1.3.1 Setting the Classpath on Oracle WebLogic Server Running on Microsoft Windows

To add the directory containing the JAR files to the classpath in the WebLogic Application Server on Windows:

1. In the WebLogic server installation directory, navigate to the domain name directory.
2. Open the startWebLogic.cmd file in a text editor.
3. Edit the following command:

   ```
   CLASSPATH=%JAVA_HOME%\jre\lib\rt.jar;
   ```

   Add the Apache Axis JAR files corresponding to the Oracle WebLogic Server in the ThirdParty directory to the classpath as shown below:

   ```
   set CLASSPATH=%JAVA_HOME%\jre\lib\rt.jar;JAR_FILES;
   ```

   In this command, replace *JAR_FILES* with a semicolon-separated list of the full path and name of the Apache Axis JAR files present in the ThirdParty directory.

   The following is a sample command:

   ```
   set
   CLASSPATH=%JAVA_HOME%\jre\lib\rt.jar;%XLHOME%\ThirdParty\axis.3.jar;%XLHOME%\Th
   irdParty\commons-logging.jar;%XLHOME%\ThirdParty\commons-discovery-0.2.jar;%XLH
   OME%\ThirdParty\wsdl4j-1.5.1.jar;
   ```

   Here, replace %XLHOME% with the path to the directory in which Oracle Identity Manager is installed. In other words, the complete path to the *OIM_HOME* directory.

4. Save and close the file.

2.1.3.2 Setting the Classpath on Oracle WebLogic Server Running on Linux

To add the directory containing the JAR files to the classpath in the WebLogic Application Server on Linux:

1. In the WebLogic server installation directory, navigate to the domain name directory.
2. Open the startWebLogic.sh file in a text editor.
3. Edit the following command:

```
CLASSPATH=%JAVA_HOME%\jre\lib\rt.jar;
```

Add the Apache Axis JAR files corresponding to the Oracle WebLogic Server in the ThirdParty directory to the classpath as shown below:

```
set CLASSPATH=%JAVA_HOME%\jre\lib\rt.jar :JAR_FILES;
```

In this command, replace *JAR_FILES* with a colon-separated list of the full path and name of the Apache Axis JAR files present in the ThirdParty directory.

The following is a sample command:

```
set CLASSPATH=%JAVA_HOME%/jre/lib/rt.jar :${ XLHOME
}/ThirdParty/axis.3.jar;%XLHOME%/ThirdParty/commons-logging.jar: ${
XLHOME}/ThirdParty/commons-discovery-0.2.jar; ${
XLHOME}/ThirdParty/wsdl4j-1.5.1.jar;
```

Here, replace %XLHOME% with the path to the directory in which Oracle Identity Manager is installed. In other words, the complete path to the *OIM_HOME* directory.

4. Save and close the file.

2.1.4 Determining the URL of the Web Service Running on the Target System

The WSDLLocation parameter of the IT resource holds the URL of the Web service that is running on SAP Enterprise Portal. While configuring the IT resource, you provide this URL as the value of the WSDLLocation parameter.

To determine the URL of the Web service:

1. Log in to SAP EP as an administrator.
2. Click the **System Administration** tab.
3. Click the **Support** tab.
4. Select **Portal Runtime** in the Top Level Areas region.

   The Portal Support Desk: Portal Runtime page is displayed.
5. On this page, click **SOAP Admin** in the Test and Configuration Tools region.

   The SOAP Administration page is displayed.
6. On this page, select **Web Services.**

   All the Web Services are displayed.
7. Click **com.sap.portal.prt.soap.ConnectorService.**

   All the WSDL files are displayed.
8. Click the **Present** link next to RPC Literal.

   An XML file is opened.
9. In the XML file, search for the tag that starts with the following text:

   ```
   <soap:address location=
   ```

   This tag holds the WSDL URL of the Web service. For example:

   ```
   <soap:address
   location="http://mlbpsap02:50000/irj/servlet/prt/soap/com.sap.portal.prt.soap.C
   onnectorService?style=rpc_lit" />
   ```

2.2 Installation

The procedure to install the connector depends on the release of Oracle Identity Manager that you are using:

- Section 2.2.1, "Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2"
- Section 2.2.2, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"

2.2.1 Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2

Installing the connector on Oracle Identity Manager release 9.0.1 through 9.0.3.2 involves performing the following procedures:

- Section 2.2.1.1, "Copying the Connector Files and External Code Files"
- Section 2.2.1.2, "Importing the Connector XML File"
- Section 2.2.1.3, "Compiling Adapters"

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

See the Section 2.1.1, "Files and Directories on the Installation Media" for more information about these files.

Table 2–2 Connector Files to Be Copied

Connector File	Destination Directory
Files in the lib directory	*OIM_HOME*/Xellerate/SAP_EP/lib *OIM_HOME*/Xellerate/SAP_EP/JavaTasks
lib/SAPEPRecon.jar	*OIM_HOME*/Xellerate/ScheduleTask
par/ConnectorService.par	See Section 2.3.2, "Deploying Web Services on the Target System" for more information.
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources
Files in the test directory	*OIM_HOME*/Xellerate/SAP_EP/test
Files in the xml directory	*OIM_HOME*/Xellerate/SAP_EP/xml

2.2.1.2 Importing the Connector XML File

As mentioned in Section 2.1.1, "Files and Directories on the Installation Media," 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 opening files is displayed.
4. Locate and open the SAPEPResourceObject.xml file, which is in the *OIM_HOME*/Xellerate/xml directory. Details of this XML file are shown on the File Preview page.

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

5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the SAP EP IT Resource IT resource is displayed.
8. Specify values for the parameters of the SAP EP IT Resource IT resource. See Section 2.2.2.2, "Configuring the IT Resource" for information about the values to be specified.
9. If you want to configure the connector for another instance of the target system, then:
   a. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the SAP EP IT Resource IT resource type is displayed.
   b. To define an IT resource for the next instance of the target system, first assign a name to the new IT resource on this page. Then, see Section 2.2.2.2, "Configuring the IT Resource" for information about the values to be specified for the parameters of the new IT resource.

   Repeat Steps a and b for the remaining instances of the target system.

   See Also: *Oracle Identity Manager Tools Reference Guide*

10. Click **Skip** after you define IT resources for all the instances of the target system. The Confirmation page is displayed.

    See Also: If you want to define another IT resource, then see *Oracle Identity Manager Administrative and User Console 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.

2.2.1.3 Compiling Adapters

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

- SAP EP Remove Role

- SAP EP Remove Group
- SAP EP Password Change
- SAP EP Modify User Date
- SAP EP Modify User
- SAP EP Delete User
- SAP EP Create User
- SAP EP Add Role
- SAP EP Add Group
- SAP EP Lock UnLock User
- PrePopulate SAP EP Form
- SAP EP Email Modify

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. In an Oracle Identity Manager cluster, 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.

2.2.2 Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1

Note: In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

Installing the connector on Oracle Identity Manager release 9.1.0.*x* or release 11.1.1 involves performing the following procedures:

- Section 2.2.2.1, "Running the Connector Installer"
- Section 2.2.2.2, "Configuring the IT Resource"

2.2.2.1 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:

   Note: In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME/xellerate/ConnectorDefaultDirectory

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Oracle Identity Manager Administrative and User Console Guide

   - For Oracle Identity Manager release 11.1.1:

     Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Click **Deployment Management**, and then click **Install Connector**.

   - For Oracle Identity Manager release 11.1.1:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.

4. From the Connector List list, select **SAP Enterprise Portal *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

If you have copied the installation files into a different directory, then:

a. In the **Alternative Directory** field, enter the full path and name of that directory.

b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

c. From the Connector List list, select **SAP Enterprise Portal *RELEASE_NUMBER***.

5. Click **Load**.

6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager).

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

   Note: At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.1.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.

   There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

   Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks that are created when you installed the connector

Note: In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

8. Copy the files in the config directory on the installation media to the *OIM_HOME*/xellerate/XLIntegrations/LotusNotes/config directory.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Table 2–1 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.2.2.2 Configuring the IT Resource

You must specify values for the parameters of the SAP EP IT Resource IT resource as follows:

1. Log in to the Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `SAP EP IT Resource` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2–3 describes each parameter.

Table 2–3 IT Resource Parameters

Parameter	Description
TimeStamp	For the first reconciliation run, the time stamp 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 time stamp values: ■ English: `Jun 01, 2006 at 10:00:00 GMT+05:30` ■ French: `juil. 01, 2006 at 10:00:00 GMT+05:30` ■ Japanese: `6 01, 2006 at 10:00:00 GMT+05:30` See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for information about using this parameter to switch from incremental to full reconciliation.
WSDLLocation	This parameter holds the location of the WSDL URL, where the Web service is running on SAP Enterprise Portal. See Section 2.1.4, "Determining the URL of the Web Service Running on the Target System" for more information.
SOAPAdminUserID	Enter the user ID of the user account that the connector will use to login to the target system for reconciliation and provisioning operations. See Section 2.3.3, "Creating a Target System User Account for Connector Operations" for more information. Sample value: `admin`
SOAPAdminPassword	Enter the password of the user account that the connector will use to login to the target system for reconciliation and provisioning operations.

8. To save the values, click **Update**.

2.3 Postinstallation

The following sections discuss postinstallation procedures:

- Section 2.3.1, "Configuring the Oracle Identity Manager Server"
- Section 2.3.2, "Deploying Web Services on the Target System"
- Section 2.3.3, "Creating a Target System User Account for Connector Operations"
- Section 2.3.4, "Configuring SSL to Secure Communication Between Oracle Identity Manager and the Target System"

2.3.1 Configuring the Oracle Identity Manager Server

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

- Section 2.3.1.1, "Configuring Trusted Source Reconciliation"
- Section 2.3.1.2, "Changing to the Required Input Locale"
- Section 2.3.1.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.1.4, "Enabling Logging"
- Section 2.3.1.5, "Configuring the SAP Change Password Function"
- Section 2.3.1.6, "Enabling Request-Based Provisioning"

2.3.1.1 Configuring Trusted Source Reconciliation

Note: This section describes an optional procedure. Perform the procedure only if you want to configure the connector for 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 during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a target resource, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, SAPEPXLResourceObject.xml, by using the Deployment Manager. This section describes the procedure to import the XML file.
2. Set the IsTrustedSource 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. If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
   a. Click the Deployment Management link on the left navigation bar.
   b. Click the Import link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.
4. Locate and open the SAPEPXLResourceObject.xml file, which is in the xml directory on the installation media.
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 IsTrustedSource reconciliation scheduled task attribute to `True`. This procedure is described in Section 3.4, "Configuring Scheduled Tasks."

2.3.1.2 Changing to the Required Input Locale

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster.

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.

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*, and the Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to 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, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/bin directory.

   Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

   For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*:

   OIM_HOME/xellerate/bin/*SCRIPT_FILE_NAME*

   For Oracle Identity Manager release 11.1.1:

   OIM_HOME/server/bin/*SCRIPT_FILE_NAME*

2. Enter one of the following commands:

Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *`CATEGORY_NAME`* on Microsoft Windows or `PurgeCache.sh` *`CATEGORY_NAME`* on UNIX. The *`CATEGORY_NAME`* argument represents the name of the content category that must be purged.

For example, the following commands purge Metadata entries from the server cache:

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

- For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*:

  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. This exception is different from the one mentioned in Step 1.

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

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

  When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

  `t3://`*`OIM_HOST_NAME`*`:`*`OIM_PORT_NUMBER`*

  In this format:

  – Replace *`OIM_HOST_NAME`* with the host name or IP address of the Oracle Identity Manager host computer.

  – Replace *`OIM_PORT_NUMBER`* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.3.1.4 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform the procedure described in one of the following sections:

- Section 2.3.1.4.1, "Enabling Logging on Oracle Identity Manager Releases 9.0.1 through 9.0.3.2 and 9.1.0.x"
- Section 2.3.1.4.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.3.1.4.1 Enabling Logging on Oracle Identity Manager Releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster.

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 messages that highlight the progress of the application at a 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 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:

- **IBM WebSphere Application Server**

  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.SAPEPCONNECTOR=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.SAPEPCONNECTOR=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.SAPEPCONNECTOR">
        <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.SAPEPCONNECTOR">
        <priority value="INFO"/>
     </category>
     ```

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

  JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

  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.SAPEPCONNECTOR=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.SAPEPCONNECTOR=INFO
     ```

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

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

- **Oracle WebLogic Server**

  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.SAPEPCONNECTOR=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.SAPEPCONNECTOR=INFO
```

After you enable logging, log information is displayed on the server console.

2.3.1.4.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

Oracle Identity Manager release 11.1.1 uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. 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:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

  This level enables logging of messages that highlight the progress of the application.

- CONFIG

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

- FINE, FINER, FINEST

  These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in Table 2–4.

Table 2–4 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

```
<log_handler name='sapep-handler' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='[FILE_NAME]'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="XL_INTG.SAPEPCONNECTOR" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="sapep-handler"/>
     <handler name="console-handler"/>
   </logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–4 lists the supported message type and level combinations.

   Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

   The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]**:

```
<log_handler name='sapep-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="XL_INTG.SAPEPCONNECTOR" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="sapep-handler"/>
     <handler name="console-handler"/>
   </logger>
```

   With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the `NOTIFICATION:1` level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

   Replace ***FILENAME*** with the location and name of the file to which you want to redirect the output.
4. Restart the application server.

2.3.1.5 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 EP Process** process definition.
5. Double-click the **Password Updated** task.
6. On the Integration tab, specify values for the following parameters:
   - ValidityChange: You can specify either `True` or `False`.
     - `True`: If the user's validity period has expired, then it is extended to the date specified in the `ValidTo` parameter.
     - `False`: If the user's validity period has expired, then it does not extend the validity and the user's password cannot be changed.
   - `lockChange`: You can specify either `True` or `False`.
     - `True`: If the user is locked but not by the administrator, then the user is unlocked before the change of password. 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.
   - `ValidTo`: Date to which the user's validity must be extended. The date format must be as follows:

     ```
     Apr 1 10 11:18:29 AM
     ```

     If this field is left empty, then the value is set to `1970-01-01`, which is the default date.

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

2.3.1.6 Enabling Request-Based Provisioning

Note: The feature described in this section is supported only on Oracle Identity Manager release 11.1.1. Perform the procedure described in this section only if you want to enable request-based provisioning.

In request-based provisioning, an end user creates a request for a resource or entitlement by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource or entitlement on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

Note: Direct provisioning cannot be used if you enable request-based provisioning.

Enabling request-based provisioning involves performing the following procedures:

- Section 2.3.1.6.1, "Copying Predefined Request Datasets"
- Section 2.3.1.6.2, "Importing Request Datasets into the MDS"
- Section 2.3.1.6.3, "Enabling the Auto Save Form Feature"
- Section 2.3.1.6.4, "Running the PurgeCache Utility"

2.3.1.6.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following is the list of predefined request datasets in the DataSet directory on the installation media:

- ModifyResourceSAP EP Resource Object.xml
- ProvisionResourceSAP EP Resource Object.xml

Copy the files from the DataSets directory on the installation media to the *OIM_HOME*/DataSet/file directory.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about modifying request datasets.

2.3.1.6.2 Importing Request Datasets into the MDS

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into the MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.
2. In a command window, change to the *OIM_HOME*/server/bin directory.
3. Run one of the following commands:
   - On Microsoft Windows

     `weblogicImportMetadata.bat`

   - On UNIX

     `weblogicImportMetadata.sh`

4. When prompted, enter values for the following:
   - `Please enter your username [weblogic]`

     Enter the user name used to log in to Oracle WebLogic Server.

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

     Enter the password used to log in to Oracle WebLogic Server.

   - `Please enter your server URL [t3://localhost:7001]`

     Enter the URL of the application server in the following format:

     `t3://`*`HOST_NAME_IP_ADDRESS`*`:`*`PORT`*

     In this format, replace:

     – *`HOST_NAME_IP_ADDRESS`* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

     – *`PORT`* with the port on which Oracle Identity Manager is listening.

   The request dataset is imported into the MDS.

2.3.1.6.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**
3. Search for and open the **LOTUSRO** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.3.1.6.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.1.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to enable request-based provisioning ends with this step.

2.3.2 Deploying Web Services on the Target System

To be able to use Web services with the SAP Enterprise Portal connector, you must deploy the ConnectorService.par file as follows:

1. Log in to SAP Enterprise Portal as the administrator.
2. Click the **System Administration** tab, the **Support** secondary tab, select **Portal Runtime** and then select **Administration Console**.
3. In the Archive Uploader region, browse to the ConnectorService.par file, and then click **Upload.** After the file is uploaded, an INFO message is displayed.
4. From the list in the Archive Deployment Checker region, select **ConnectorService,** and then click **Refresh**.

2.3.3 Creating a Target System User Account for Connector Operations

Create a target system user account, and assign the super_admin_role and com.sap.pdk.JavaDeveloper roles to it. If the com.sap.pdk.JavaDeveloper role is not available, then obtain the PDK for Java from SAP to get that role required for the installation to work.

The SAPUMLocation parameter of the IT resource holds information about this user account. See Section 2.2.2.2, "Configuring the IT Resource" for information about this parameter.

If the specified roles are not assigned to this user account, then Oracle Identity Manager cannot connect to the target system.

2.3.4 Configuring SSL to Secure Communication Between Oracle Identity Manager and the Target System

This section discusses the following topics:

- Section 2.3.4.1, "Configuring the Target System for SSL"
- Section 2.3.4.2, "Configuring Oracle Identity Manager for SSL"

2.3.4.1 Configuring the Target System for SSL

For instructions on configuring the target system for SSL, visit the SAP Web site at

`http://help.sap.com/erp2005_ehp_04/helpdata/DE/a6/98f73dbc570302e10000000a114084/frameset.htm`

2.3.4.2 Configuring Oracle Identity Manager for SSL

Configuring Oracle Identity Manager for SSL involves importing the certificate that was created on the target system. To import the certificate:

1. Copy the certificate of the target system into the *JAVA_HOME*/lib/security directory of the Oracle Identity Manager host computer.
2. In a terminal window, change to the *JAVA_HOME*/bin directory, and then run the following command:

   ```
   keytool -import -alias ALIAS -file CERT_FILE_NAME -trustcacerts -keystore
   MY_CACERTS -storepass PASSWORD
   ```

   In this command:

   - *ALIAS* is the alias for the certificate.

- *CERT_FILE_NAME* is the complete name and path of the certificate.
- *MY_CACERTS* is the full path and name of the certificate store.
- *PASSWORD* is the keystore password.

The following is a sample command:

```
keytool -import -alias sapep_trusted_cert -file
JAVA_HOME/lib/security/globalsv.crt -trustcacerts -keystore
JAVA_HOME/lib/security/cacerts -storepass changeit
```

3

Using the Connector

This chapter is divided into the following sections:

3.1 Performing First-Time Reconciliation

First-time reconciliation involves synchronizing lookup definitions in Oracle Identity Manager with the lookup fields of the target system, and performing full reconciliation. In full reconciliation, all existing user records from the target system are brought into Oracle Identity Manager.

Note: In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

See Section 3.4, "Configuring Scheduled Tasks" for information about the procedure to configure scheduled tasks.

- If you are using the target system as a target resource, then:

  1. Configure and run the SAPEP LookupRecon scheduled task to synchronize the lookup definitions. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" information about the attributes of this scheduled task.
  2. Configure and run the SAPEP UserRecon scheduled task to reconcile user records from the target system. See Section 3.3.4, "User Reconciliation Scheduled Task" for information about the attributes of this scheduled task.

Reconciled user records are converted into SAP Enterprise Portal resources assigned to OIM Users.

- If you are using the target system as a trusted source, then configure and run the SAPEP UserRecon scheduled task to reconcile user records from the target system. See Section 3.3.4, "User Reconciliation Scheduled Task" for information about the attributes of this scheduled task.

  Reconciled user records are converted into OIM Users.

After first-time reconciliation, depending on the mode in which you configure the connector, the TimeStamp parameter of the IT resource is automatically set to the time stamp at which the reconciliation run began. Table 2–3 describes this parameter.

From the next reconciliation run onward, only target system user records that are added or modified after the time stamp stored in the IT resource are considered for incremental reconciliation. These records are brought to Oracle Identity Manager when you configure and run the user reconciliation scheduled task.

3.2 Scheduled Task for Lookup Field Synchronization

The SAPEP LookupRecon scheduled task is used for lookup field synchronization. You must specify values for the attributes of this scheduled tasks. Table 3–1 describes the attributes of these scheduled tasks. Section 3.4, "Configuring Scheduled Tasks" describes the procedure to configure scheduled tasks.

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.

Table 3–1 Attributes of the SAPEP LookupRecon Scheduled Task

Attribute	Description	Sample Value
ITResource	This attribute holds the name of the IT resource.	`SAP EP IT Resource`

3.3 Configuring Reconciliation

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

- Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation"
- Section 3.3.2, "Limited Reconciliation"
- Section 3.3.3, "Batched Reconciliation"
- Section 3.3.4, "User Reconciliation Scheduled Task"

3.3.1 Full Reconciliation vs. Incremental Reconciliation

The TimeStamp parameter of the IT resource store the time stamp at which a reconciliation run begins. During the next reconciliation run, the scheduled task fetches only target system records that are added or modified after the time stamp stored in the TimeStamp parameter. This is incremental reconciliation.

If you delete the value of the TimeStamp parameter, then full reconciliation is performed when the scheduled task is run. In full reconciliation, all existing target system records are fetched into Oracle Identity Manager.

You can perform a full reconciliation run to fetch all existing target system records into Oracle Identity Manager. To perform a full reconciliation run:

1. Delete the value of the TimeStamp IT resource parameter. See Section 2.2.2.2, "Configuring the IT Resource" for information about setting values for parameters of the IT resource.
2. Set the BatchSize attribute of the SAPEP UserRecon scheduled task to a non-zero value. See Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2" for information about configuring scheduled tasks.

After a full reconciliation run, the time stamp at which the reconciliation run ends is stored in the time stamp parameter of the IT resource. From the next reconciliation run onward, only target system records added or modified after the last reconciliation run are fetched to Oracle Identity Manager. In other words, incremental reconciliation is automatically activated from the next run onward.

3.3.2 Limited 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 attribute of the scheduled task. Section 3.3.4, "User Reconciliation Scheduled Task" describes the attributes of the scheduled task.

The following table lists the SAP Enterprise Portal attributes that you can use to build the query condition. You specify this query condition as the value of the CustomizedReconQuery attribute.

SAP Enterprise Portal Attribute	Oracle Identity Manager Attribute
firstname	FirstName
lastname	LastName
department	Department
email	EmailID
telephone	Telephone
mobile	Mobile
fax	Fax
streetaddress	Street
city	City

SAP Enterprise Portal Attribute	Oracle Identity Manager Attribute
zip	Zip
country	Country
state	State
locale	Language
timezone	TimeZone
Group	Group
Role	Role

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|email=test@example.com`

  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's e-mail address is `test@example.com`.

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

You must apply the following guidelines while specifying a value for the CustomizedReconQuery attribute:

- For the SAP Enterprise Portal 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 (|).

- To specify multiple roles and groups in the query, roles and groups must be provided with the comma separator.

You specify a value for the CustomizedReconQuery attribute while performing the procedure described in Section 3.4, "Configuring Scheduled Tasks."

3.3.3 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 these problems.

To configure batched reconciliation, you must specify an integer value for the BatchSize attribute of the user reconciliation scheduled task (SAPEP UserRecon).

Suppose you specify the 20 as the value of the BatchSize attribute. Suppose that 314 user records were created or modified after the last reconciliation run. These 314 records would be reconciled in batches of 20 records each.

You specify values for the BatchSize attribute by following the instructions described in Section 3.4, "Configuring Scheduled Tasks."

3.3.4 User Reconciliation Scheduled Task

You must specify values for the following attributes of the SAPEP UserRecon 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.

Table 3–2 Attributes of the SAPEP UserRecon Scheduled Task

Attribute	Description	Sample Value
Organization	Default organization assigned to a new user	`OIM Users`
Xellerate Type	Default type assigned to a new user	`End-User Administrator`
Role	Default employee type assigned to a new user	`Consultant`
ITResource	Name of the IT resource for setting up a connection with SAP	`SAP EP IT Resource`
ResourceObject	Name of the resource object that is used for user reconciliation	`SAP EP Resource Object`
IsTrustedSource	Configuration for trusted source / target resource If it is set to `True`, then it is a trusted source. If it is set to `False`, then the target is a target resource. By default, the value is `false`.	`False`

Table 3–2 (Cont.) Attributes of the SAPEP UserRecon Scheduled Task

Attribute	Description	Sample Value
BatchSize	Specifies the number of records that must be included in each batch fetched from the target system You use this attribute to implement the batched reconciliation feature.	`1000`
XLDeleteUsersAllowed	Flag that specifies whether or not users are to be deleted in Oracle Identity Manager during user reconciliation	`False`
CustomizedReconQuery	Query condition on which reconciliation must be based If you specify a query condition for this attribute, then the search for target system records is 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 include the AND (&) and OR (|) logical operators.	`firstname=John`
TrustedResourceObject	Name of the trusted resource object	`Xellerate User`

3.4 Configuring Scheduled Tasks

Table 3–3 lists the scheduled tasks that form part of the connector.

Table 3–3 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
SAPEP LookupRecon	This scheduled task is used for lookup field synchronization.
SAPEP UserRecon	This scheduled task is used for user reconciliation.

To configure these scheduled tasks, perform the procedure described in one of the following sections depending on the Oracle Identity Manager release that you are using:

- Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2"
- Section 3.4.2, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x and 11.1.1"

3.4.1 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2

To configure a scheduled task on Oracle Identity Manager release 9.0.1 through 9.0.3.2:

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. 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. See Section 3.3.4, "User Reconciliation Scheduled Task" 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.

Stopping Reconciliation

If you want to stop a scheduled task while it is running, open the scheduled task in the Design Console and then select the **Stop Execution** check box.

3.4.2 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x and 11.1.1

To configure a scheduled task on Oracle Identity Manager release 9.1.0.*x* and 11.1.1:

1. Log in to the Administrative and User Console.
2. Perform one of the following steps:
   a. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**
   b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.
     b. In the search results table, click the edit icon in the Edit column for the scheduled task.
     c. On the Scheduled Task Details page where the details of the scheduled task that you selected is displayed, click **Edit**.
   - If you are using Oracle Identity Manager release 11.1.1, then:

a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

c. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. Modify the details of the scheduled task. To do so:

a. If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

– **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

– **Max Retries:** Enter an integer value in this 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. The default value is 1.

– **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

– **Frequency:** Specify the frequency at which you want the task to run.

b. If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, you can modify the following parameters:

– **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

– **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

Note: See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task. To do so:

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 is left empty, then reconciliation is not performed.
- Attributes of the scheduled task are discussed in Section 3.3.4, "User Reconciliation Scheduled Task."

- If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the **Attribute** list, specify a value in the field provided, and then click **Update**.
- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

6. After specifying the attributes, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

     Note: The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

   - If you are using Oracle Identity Manager release 11.1.1, then click **Apply** to save the changes.

     Note: The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

Stopping Reconciliation

If you want to stop a scheduled task while it is running, open the scheduled task in the Design Console and then select the **Stop Execution** check box.

3.5 Guidelines on Performing Provisioning Operations

Apply the following guidelines while performing provisioning operations:

- While performing the Create User provisioning operation, you must also assign a role to the user. If you do not assign a role to the user, then the user would not be able to view any Portal content after logging in to SAP Enterprise Portal.

3.6 Performing Provisioning Operations

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.7, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

The following are types of provisioning operations:

- Direct provisioning

- Request-based provisioning
- Provisioning triggered by policy changes

See Also: *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- Section 3.6.1, "Direct Provisioning"
- Section 3.6.2, "Request-Based Provisioning"

3.6.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. From the Users menu, select **Create**.
     b. On the Create User page, enter values for the OIM User fields and then click **Create User**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
     b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM User, then:
   - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. From the Users menu, select **Manage**.
     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.
     b. On the Resource Profile page, click **Provision New Resource**.

- If you are using Oracle Identity Manager release 11.1.1, then:
  a. On the user details page, click the **Resources** tab.
  b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

5. On the Step 1: Select a Resource page, select **Auth Manager User** from the list and then click **Continue**.
6. On the Step 2: Verify Resource Selection page, click **Continue**.
7. On the Step 5: Provide Process Data for Auth Manager User Details page, enter the details of the account that you want to create on the target system and then click **Continue**.
8. On the Step 5: Provide Process Data for Auth Manager User page, search for and select a group for the user on the target system and then click **Continue**.
9. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
10. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
    - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
    - If you are using Oracle Identity Manager release 11.1.1, then:
      a. Close the window displaying the "Provisioning has been initiated" message.
      b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.6.2 Request-Based Provisioning

Note: The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

Note: The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- Section 3.6.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.6.2.2, "Approver's Role in Request-Based Provisioning"

3.6.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

> **See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **Auth Manager User**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.6.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.

2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

3.7 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

Note: It is assumed that you have performed the procedure described in Section 2.3.1.6, "Enabling Request-Based Provisioning.".

On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **Auth Manager User** process definition.
   c. Deselect the **Auto Save Form** check box.
   d. Click the Save icon.
   e. Repeat this procedure to deselect the Auto Save Form check box for the Auth Manager Token process definition.
3. If the Self Request Allowed feature is enabled, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **Auth Manager User** resource object.
   c. Deselect the **Self Request Allowed** check box.
   d. Click the Save icon.
   e. Repeat this procedure to deselect the Self Request Allowed check box for the Auth Manager Token process definition.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **Auth Manager User** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the Save icon.

e. Repeat this procedure to select the Auto Save Form check box for the Auth Manager Token process definition.

3. If you want to enable end users to raise requests for themselves, then:

   a. Expand **Resource Management**, and then double-click **Resource Objects**.

   b. Search for and open the **Auth Manager User** resource object.

   c. Select the **Self Request Allowed** check box.

   d. Click the Save icon.

   e. Repeat this procedure to select the Self Request Allowed check box for the Auth Manager Token process definition.

4

Extending the Functionality of the Connector

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

4.1 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 Enterprise Portal.

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

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

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

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 EP 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 EP 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_SAPEP (parent form)
- UD_SAPEPROL (child form for multivalued attributes)
- UD_SAPEPGP (child form for multivalued attributes)

You can use these process forms as templates for creating the remaining process forms.

4. Create and configure one process definition for each resource object.

   The Process Definition form is in the Process Management folder. The SAP EP 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. See Section 3.3, "Configuring Reconciliation" for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:

   - ITResource
   - ResourceObject
   - IsTrustedSource

   Set the `IsTrustedSource` attribute to `True` for the SAP Enterprise Portal 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 Enterprise Portal installation to which you want to provision the user.

5

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:

- Section 5.1, "Running Test Cases"
- Section 5.2, "Troubleshooting"

5.1 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_EP/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 Enterprise Portal connection Parameters	Connection parameters required to connect to the target system See Section 2.2.2.2, "Configuring the IT Resource" for information about the values that you must provide.
Create User Parameters	Field information required to create a user profile
Modify User Parameters	This covers multiple sections of parameters that are used to modify user profile information.
Delete User Parameters	Field information required to delete a user profile
Reconciliation information	The From Date time stamp The To Date is set to the current date and time by default.

2. Add all the JAR files mentioned in the "Copying the Connector Files and External Code Files" section on page 2-6 to the CLASSPATH environment variable. In addition, you need to add the JAR files in the following directories to the CLASSPATH environment variable:

   Sample commands for setting the CLASSPATH environment variable is given in the global.properties file.

   OIM_HOME/xellerate/lib

OIM_HOME/xellerate/ext

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/sapep/test/Troubleshoot

   b. Enter the following command:

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

      The troubleshoot.properties file 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_EP/test/Troubleshoot/troubleShoot.prop
     erties
     -Dlog4j.configuration=file:/OIM_HOME/Xellerate/SAP_EP/test/Troubleshoot/log
     .properties troubleshoot.TroubleShootUtility C
     ```

   - Enter the following command to modify a user:

     ```
     java
     -DTproperties=OIM_HOME/Xellerate/SAP_EP/test/Troubleshoot/troubleShoot.prop
     erties
     -Dlog4j.configuration=file:/OIM_HOME/Xellerate/SAP_EP/test/Troubleshoot/log
     .properties troubleshoot.TroubleShootUtility M
     ```

   - Enter the following command to delete a user:

     ```
     java
     -DTproperties=OIM_HOME/Xellerate/SAP_EP/test/Troubleshoot/troubleShoot.prop
     erties
     -Dlog4j.configuration=file:/OIM_HOME/Xellerate/SAP_EP/test/Troubleshoot/log
     .properties troubleshoot.TroubleShootUtility D
     ```

   - Enter the following command to test reconciliation:

     ```
     java
     -DTproperties=OIM_HOME/Xellerate/SAP_EP/test/Troubleshoot/troubleShoot.prop
     erties
     -Dlog4j.configuration=file:/OIM_HOME/Xellerate/SAP_EP/test/Troubleshoot/log
     .properties troubleshoot.TroubleShootUtility R
     ```

5.1.1 Testing Partial Reconciliation

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

- Simple query with user attributes

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

The users with first name `John` are reconciled.

- Query consisting of '&' or '|' logical operator

  Note:

  - The query condition cannot contain both '&' and '|' operators. You must use only one of these operators in any particular query.
  - A query condition containing both the '|' operator and the `TimeStamp` attribute is not supported.

  Value assigned to the `CustomizedReconQuery` parameter: `firstname=John&lastname=Doe&email=John@example.com`

  The users with first name `John`, the users with last name `Doe`, and the users with e-mail address `John@example.com` are reconciled.

- Query consisting of logical operators and lookup code

  Value assigned to the `CustomizedReconQuery` parameter: `firstname=John&lastname=Doe&email=John@example.com&country=US`

  The users with first name `John` and last name `Doe`, and the users with e-mail address `John@example.com`, who are located in the United States, are reconciled.

- Query consisting of roles only

  Value assigned to the `CustomizedReconQuery` parameter: `Role=pcd:portal_content/mycompany/RL_DEMO`

  Note: You cannot specify more than one role name in the query condition.

  The users who belong to the `pcd:portal_content/mycompany/RL_DEMO` role are reconciled.

- Query consisting of groups only

  Value assigned to the `CustomizedReconQuery` parameter: `Groups=group01`

  Note: You cannot specify more than one group name in the query condition.

  The users who belong to the `group01` group are reconciled.

- Query consisting of the LIKE (*) operator

  Value assigned to the `CustomizedReconQuery` parameter:

  – `firstname=*ohn`

    The users having the `ohn` string in their first name are reconciled.

  – `firstname=Joh*`

    The users having the `Joh` string in their first name are reconciled.

Note: The LIKE operator (*) can be the prefix or suffix. It cannot be used in the middle of the attribute value.

If you want to use the locale or timezone attributes in the query condition, then provide the Code key value of the `Lookup.SAP.EP.Language` or `Lookup.SAP.EP.TimeZone` lookup definition, respectively.

For example, value assigned to the `CustomizedReconQuery` parameter:

```
locale=ar_iq

timezone=Africa/Abidjan
```

5.2 Troubleshooting

The following sections list solutions to some commonly encountered issues associated with this connector:

- Section 5.2.1, "Connection Errors"
- Section 5.2.2, "Create User Errors"
- Section 5.2.3, "Delete User Errors"
- Section 5.2.4, "Modify User Errors"
- Section 5.2.5, "Child Data Errors"

5.2.1 Connection Errors

The following table lists solutions to some commonly encountered connection errors.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to SAP Enterprise Portal. **Returned Error Message:** SAP Connection exception **Returned Error Code:** `INVALID_CONNECTION_ERROR`	■ Ensure that SAP Enterprise Portal is running and that the `sapum.properties` file has been correctly configured. ■ Ensure that Oracle Identity Manager is running (that is, the database is running). ■ Ensure that all the adapters have been compiled. ■ Examine the Oracle Identity Manager record (from the IT Resources form). Ensure that the IP address, admin ID, and admin password are correct.
Target not available **Returned Error Message:** Target Server not available Connection error - unable to create SAP Enterprise Portal Connection. **Returned Error Code:** `TARGET_UNAVAILABLE_ERROR`	■ Ensure that SAP Enterprise Portal is running. ■ Ensure that the specified SAP Enterprise Portal connection values are correct.

Problem Description	Solution
Authentication error **Returned Error Message:** Authentication error **Returned Error Code:** AUTHENTICATION_ERROR	Ensure that the specified SAP Enterprise Portal connection user ID and password are correct.

5.2.2 Create User Errors

The following table lists solutions to some commonly encountered Create User errors.

Problem Description	Solution
Oracle Identity Manager cannot create a user **Returned Error Message:** Required information missing **Returned Error Code:** SAPEP.INSUFFICIENT_INFORMATION	Ensure that the following information has been provided: ■ User ID ■ User first name ■ User last name ■ User password ■ User e-mail address
Oracle Identity Manager cannot create a user **Returned Error Message:** User already exists in SAP EP **Returned Error Code:** USER_ALREADY_EXIST	User with the assigned ID already exists in SAP Enterprise Portal. Assign a new ID to this user, and try again.
Oracle Identity Manager cannot create a user **Returned Error Message:** Could not create user **Returned Error Code:** USER_CREATION_FAILED	User could not be created because of any one of the following reasons: ■ The Change Password function failed. ■ Values for mandatory fields have not been specified.

5.2.3 Delete User Errors

The following table lists solutions to some commonly encountered Delete User errors.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** Require information missing **Returned Error Code:** SAPEP.INSUFFICIENT_INFORMATION	Ensure that the required information has been provided. In this case, the required information is the user ID.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist **Returned Error Code:** `USER_DOESNOT_EXIST`	The specified user does not exist in SAP Enterprise Portal.

5.2.4 Modify User Errors

The following table lists solutions to some commonly encountered Modify User errors.

Problem Description	Solution
Oracle Identity Manager cannot update new information about the user. **Returned Error Message:** Could not modify user **Returned Error Code:** `USER_MODIFICATION_FAILED`	Generic error. Review the log for more details.
Oracle Identity Manager cannot update a user. **Returned Error Message:** User does not exist **Returned Error Code:** `USER_DOESNOT_EXIST`	The specified user does not exist in SAP Enterprise Portal. Check the user ID.

5.2.5 Child Data Errors

The following table lists solutions to some commonly encountered Child Data errors.

Problem Description	Solution
Oracle Identity Manager cannot add a user to a group. **Returned Error Message:** Group does not exist **Returned Error Code:** `GROUP_DOESNOT_EXIST`	The specified group does not exist in SAP Enterprise Portal. Check the name of the group.
Oracle Identity Manager cannot add a role to a user **Returned Error Message:** Role does not exist **Returned Error Code:** `SAPEP.ROLE_DOESNOT_EXIST`	The specified role for the user in Oracle Identity Manager does not exist in SAP Enterprise Portal. Check the role name.

Problem Description	Solution

Trying to add a duplicate value to a group or role.
Returned Error Message:
Role has already been assigned to user
Selected group is already assigned to user
Returned Error Code:
`ROLE_ALREADY_EXISTS`
`GROUP_ALREADY_EXISTS`
	The user has already been added to the particular profile or role.

6

Known Issues

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

- The connector uses the UME APIs that communicate directly with the data sources on the target systems instead of going through the SAP system. These data sources could be SAP Base, the Database, or LDAP.
- For certain functionality, such as Portal Role lookups, a SAP Enterprise Portal plug-in must be installed on the SAP Enterprise Portal server. Therefore, there is a dependency on the availability of the SAP Enterprise Portal server.
- After the connector is deployed, the first task that can be performed is lookup reconciliation. If the size of the lookup field that is being reconciled is more than 100, then an exception may be thrown. To resolve this issue, you must change the size of the column in the LKV table by running the following commands on the database:
  - `ALTER TABLE LKV MODIFY (LKV_ENCODED VARCHAR2(300 BYTE));`
  - `ALTER TABLE LKV MODIFY (LKV_DECODED VARCHAR2(300 BYTE));`
- Suppose a user is created in SAP Enterprise Portal and then locked. If this user is reconciled for the first time, then the user might not get locked because linking in Oracle Identity Manager takes place in an asynchronous manner. If the same user is reconciled for the second time, then the user gets locked.
- During lookup fields reconciliation, the Role field is reconciled in English. This is because SAP Enterprise Portal does not allow you to specify the role ID in non-English languages, although a non-English language can be used for the role name.

Index