

Oracle® Identity Manager

Connector Guide for SAP User Management

Release 9.1.0

E11212-02

July 2009

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	ix
Audience	ix
Documentation Accessibility	ix
Related Documents	x
Documentation Updates	x
Conventions	x
 What's New in Oracle Identity Manager Connector for SAP User Management? ..	xi
Software Updates	xi
Documentation-Specific Updates.....	xii
 1 About the Connector	
1.1 Certified Components	1-1
1.2 Certified Languages.....	1-2
1.3 Connector Architecture.....	1-3
1.4 Features of the Connector	1-4
1.4.1 SoD Validation of Entitlement Requests	1-4
1.4.2 Full and Incremental Reconciliation	1-4
1.4.3 Limited (Filtered) Reconciliation.....	1-5
1.4.4 Batched Reconciliation	1-5
1.4.5 SNC Communication Between the Target System and Oracle Identity Manager	1-5
1.5 Lookup Definitions Used During Connector Operations.....	1-5
1.6 Connector Objects Used During Reconciliation	1-8
1.6.1 User Attributes for Reconciliation.....	1-8
1.6.2 Reconciliation Rules	1-9
1.6.2.1 Reconciliation Rule for Target Resource Reconciliation.....	1-10
1.6.2.2 Viewing Reconciliation Rules in the Design Console	1-10
1.6.3 Reconciliation Action Rules	1-11
1.6.3.1 Reconciliation Action Rules for Target Resource Reconciliation	1-11
1.6.3.2 Viewing Reconciliation Action Rules in the Design Console	1-11
1.7 Connector Objects Used During Provisioning	1-12
1.7.1 User Provisioning Functions.....	1-12
1.7.2 User Attributes for Provisioning	1-13
1.8 Roadmap for Deploying and Using the Connector	1-14

2 Deploying the Connector

2.1	Preinstallation.....	2-1
2.1.1	Preinstallation on Oracle Identity Manager.....	2-1
2.1.1.1	Files and Directories on the Installation Media	2-1
2.1.1.2	Determining the Release Number of the Connector	2-2
2.1.2	Preinstallation on the Target System	2-3
2.1.2.1	Creating a Target System User Account for Connector Operations.....	2-3
2.1.2.2	Using External Code Files	2-4
2.2	Installation	2-6
2.3	Postinstallation.....	2-8
2.3.1	Configuring the Oracle Identity Manager Server	2-8
2.3.1.1	Enabling Request-Based Provisioning.....	2-9
2.3.1.2	Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server 2-13	
2.3.1.3	Configuring the SAP Change Password Function	2-15
2.3.1.4	Changing to the Required Input Locale	2-17
2.3.1.5	Clearing Content Related to Connector Resource Bundles from the Server Cache ... 2-17	
2.3.1.6	Enabling Logging	2-18
2.3.2	Configuring the Target System.....	2-20
2.3.2.1	Creating an Entry in the BAPIF4T Table.....	2-20
2.3.2.2	Importing the Request	2-21
2.3.2.2.1	Downloading the SAPCAR Utility	2-22
2.3.2.2.2	Extracting the Request Files	2-23
2.3.2.2.3	Performing the Request Import Operation.....	2-23
2.3.2.3	Configuring SAP Ports for Communication with Oracle Identity Manager	2-27
2.3.3	Configuring SoD.....	2-27
2.3.3.1	Configuring the SAP GRC to Act As the SoD Engine.....	2-28
2.3.3.2	Specifying Values for SoD-Related Entries in the Lookup.SAP.R3.Configuration Lookup Definition 2-28	
2.3.3.3	Specifying the System Name in the Lookup.SAP.R3.Systems Lookup Definition..... 2-29	
2.3.3.4	Specifying a Value for the TopologyName IT Resource Parameter	2-29
2.3.3.5	Disabling and Enabling SoD	2-29
2.3.4	Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System 2-32	
2.3.4.1	Prerequisites for Configuring the Connector to Use SNC.....	2-33
2.3.4.2	Installing the Security Package.....	2-33
2.3.4.3	Configuring SNC	2-34
2.3.5	Configuring the IT Resource	2-35

3 Using the Connector

3.1	Scheduled Task for Lookup Field Synchronization.....	3-1
3.2	Configuring Reconciliation.....	3-2
3.2.1	Full Reconciliation vs. Incremental Reconciliation.....	3-2
3.2.2	Limited Reconciliation vs. Regular Reconciliation	3-2
3.2.3	Batched Reconciliation	3-4

3.2.4	Reconciliation Scheduled Task	3-4
3.3	Configuring Scheduled Tasks	3-5
3.4	Provisioning Operations Performed in an SoD-Enabled Environment.....	3-7
3.4.1	Overview of the Provisioning Process in an SoD-Enabled Environment	3-7
3.4.2	Direct Provisioning in an SoD-Enabled Environment	3-7
3.4.3	Request-Based Provisioning in an SoD-Enabled Environment	3-16
4	Extending the Functionality of the Connector	
4.1	Modifying Field Lengths on the Process Form.....	4-1
4.2	Configuring the Connector for Multiple Trusted Source Reconciliation	4-1
5	Testing and Troubleshooting	
5.1	Testing Provisioning.....	5-1
5.2	Testing Partial Reconciliation.....	5-2
5.3	Testing Batched Reconciliation	5-3
6	Known Issues	

List of Figures

1-1	Architecture of the Connector	1-3
1-2	Reconciliation Rule	1-10
1-3	Reconciliation Action Rules.....	1-12
2-1	Dialog Box Displayed on Running the SAP JCo Test.....	2-6

List of Tables

1-1	Certified Components	1-2
1-2	Entries in the Lookup.SAP.R3.LookupMappings Lookup Definition	1-6
1-3	Other Lookup Definitions.....	1-7
1-4	User Attributes for Target Resource Reconciliation	1-9
1-5	Action Rules for Target Resource Reconciliation.....	1-11
1-6	User Provisioning Functions	1-12
1-7	User Attributes for Provisioning	1-13
2-1	Files and Directories On the Installation Media	2-1
2-2	Ports for SAP Services	2-27
3-1	Attributes of the SAP R3 LookupRecon Scheduled Task	3-2
3-2	Scheduled Tasks for Lookup Field Synchronization and Reconciliation	3-6

Preface

This guide provides information about Oracle Identity Manager Connector for SAP User Management.

Audience

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

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at <http://www.fcc.gov/cgb/consumerfacts/trs.html>, and a list of phone numbers is available at <http://www.fcc.gov/cgb/dro/trsphonebk.html>.

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/oim1014.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/oim1014.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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	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 Oracle Identity Manager Connector for SAP User Management?

This chapter provides an overview of the updates made to the software and documentation for release 9.1.0 of the SAP User Management connector.

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

- [Software Updates](#)
These include updates made to the connector software.
- [Documentation-Specific Updates](#)
These include major changes made to the connector documentation. These changes are not related to software updates.

Software Updates

The following sections discuss software updates:

- [Software Updates in Release 9.1.0](#)

Software Updates in Release 9.1.0

The following are software updates in release 9.1.0:

- [Support for SoD Validation of Entitlement Requests](#)
- [Linking of Entries in Lookup Definitions with Corresponding Target System Installations \(Support for Dependent Lookup Values\)](#)
- [Changes in Certified Components](#)
- [Change in the Reconciliation Rule](#)
- [Trusted Source Reconciliation Mode of the Connector Deprecated](#)

Support for SoD Validation of Entitlement Requests

From this release onward, the connector supports the Segregation of Duties (SoD) feature introduced in Oracle Identity Manager release 9.1.0.2. Requests for SAP role and profile entitlements can be validated with SAP GRC. Entitlements are provisioned into SAP ERP only if the request passes the SoD validation process. This preventive simulation approach helps identify and correct potentially conflicting assignment of entitlements to a user, before the requested entitlements are granted to users.

See [Section 1.4.1, "SoD Validation of Entitlement Requests"](#) for more information.

Linking of Entries in Lookup Definitions with Corresponding Target System Installations (Support for Dependent Lookup Values)

In earlier releases, if you had multiple installations of the target system, then entries in a lookup definition were not linked with the target system installation from which the entries were copied. During a provisioning operation, you could not select lookup field values that were specific to the target system installation on which the provisioning operation was to be performed.

From this release onward, entries in lookup definitions are linked to the target system installation from which they are copied. See [Section 1.5, "Lookup Definitions Used During Connector Operations"](#) for more information.

Support for the Multiple Trusted Source Reconciliation Feature of Oracle Identity Manager

The connector now supports the multiple trusted source reconciliation feature of Oracle Identity Manager. See *Oracle Identity Manager Design Console Guide* for detailed information about multiple trusted source reconciliation.

Changes in Certified Components

From this release onward:

- The required SAP JCo version is 3.0.
- The minimum certified release of Oracle Identity Manager is release 9.1.0.2.
- AIX is one of the certified operating systems for the host computer on which Oracle Identity Manager is installed.

See [Section 1.1, "Certified Components"](#) for the complete listing of certified components. See the following Oracle Technology Network page for information about certified components of Oracle Identity Manager:

http://www.oracle.com/technology/software/products/ias/files/idm_certification_101401.html

Note: The title of that section has been changed from "Certified Deployment Configurations" to "Certified Components."

Change in the Reconciliation Rule

The reconciliation rules for target resource reconciliation have been modified. See [Section 1.6.2, "Reconciliation Rules"](#) for more information.

Trusted Source Reconciliation Mode of the Connector Deprecated

From this release onward, the trusted source reconciliation mode of the connector has been deprecated. All features related to this mode of the connector will be removed in a future release.

Documentation-Specific Updates

Major changes have been made in the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of information provided by the guide.

See [Section 1.8, "Roadmap for Deploying and Using the Connector"](#) for detailed information about the organization of content in this guide.

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 ERP Applications as a managed (target) resource of Oracle Identity Manager.

In the account management (target resource) mode of the connector, data about users created or modified directly on SAP ERP can be reconciled into Oracle Identity Manager. This data is used to provision (assign) resources or update resources already assigned to OIM Users. In addition, you can use Oracle Identity Manager to provision or update resources assigned to OIM Users. These provisioning operations performed on Oracle Identity Manager translate into the creation of or updates to the corresponding target system accounts.

Note: At some places in this guide, SAP ERP is referred to as the **target system**.

This chapter contains the following sections:

- [Section 1.1, "Certified Components"](#)
- [Section 1.2, "Certified Languages"](#)
- [Section 1.3, "Connector Architecture"](#)
- [Section 1.4, "Features of the Connector"](#)
- [Section 1.5, "Lookup Definitions Used During Connector Operations"](#)
- [Section 1.6, "Connector Objects Used During Reconciliation"](#)
- [Section 1.7, "Connector Objects Used During Provisioning"](#)
- [Section 1.8, "Roadmap for Deploying and Using the Connector"](#)

1.1 Certified Components

[Table 1–1](#) lists the certified components for the connector.

Table 1–1 Certified Components

Component	Requirement
Oracle Identity Manager	<p>Oracle Identity Manager release 9.1.0.2 or later</p> <p>Note: This release of the connector leverages features, such as SoD validation of entitlement provisioning, introduced in Oracle Identity Manager release 9.1.0.2.</p>
Target systems	<p>The target system can be any one of the following:</p> <ul style="list-style-type: none"> ■ SAP R/3 4.6C (running on Basis 4.6C) ■ SAP R/3 4.7 (running on WAS 6.20) ■ mySAP ERP 2004 (ECC 5.0 running on WAS 6.40) ■ mySAP ERP 2005 (ECC 6.0 running on WAS 7.00)
SoD engine	<p>If you want to enable and use the Segregation of Duties (SoD) feature of Oracle Identity Manager with this target system, then install the version of SAP GRC that is supported by Oracle Identity Manager.</p> <p>See Section 1.4.1, "SoD Validation of Entitlement Requests" for more information about the SoD feature. See <i>Oracle Identity Manager Readme for Release 9.1.0.2</i> for information about the supported releases of SAP GRC.</p>
External code	<p>The following SAP custom code files:</p> <ul style="list-style-type: none"> ■ sapjco3.jar version 3.0 ■ For Microsoft Windows: sapjco3.dll version 3.0 <p>For AIX, Solaris, and Linux: libsapjco3.so version 3.0</p> <p>Note: You must verify that the Oracle Identity Manager and application server combination that you use supports JDK 1.5. This requirement is imposed by support for SAP JCo 3.0 from release 9.0.4.5 of the connector. SAP JCo 3.0 supports JDK 1.5 and later.</p> <p>See the following Oracle Technology Network Web site for information about certified components of Oracle Identity Manager:</p> <p>http://www.oracle.com/technology/software/products/ias/files/idm_certification_101401.html</p>

1.2 Certified Languages

The connector supports the following languages:

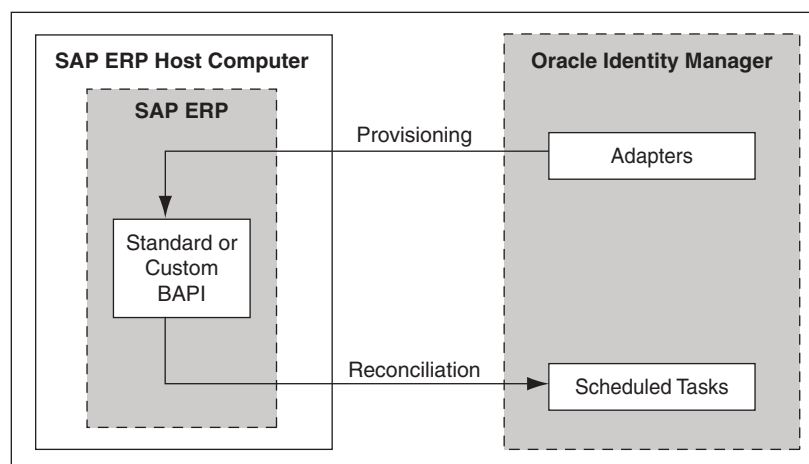
- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

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

1.3 Connector Architecture

Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of the Connector



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

Note: This is the standard provisioning process. See [Section 3.4, "Provisioning Operations Performed in an SoD-Enabled Environment"](#) for detailed information about how provisioning takes place in an SoD-enabled environment.

During reconciliation, the scheduled task establishes a connection with the target system and sends reconciliation criteria to the custom BAPIs.

Note: You deploy these custom BAPIs on the target system as part of the connector deployment procedure.

The custom BAPIs extracts 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 is compared with SAP ERP resources that are already provisioned to OIM Users. If a match is found, then the update made to the SAP ERP record from the target system is copied to the SAP ERP resource in Oracle Identity Manager. If no match is found between a record from the target system and an existing SAP ERP resource, then the user ID of the record is compared with the user ID of each OIM User. If a match is found, then data in the target system record is used to provision an SAP ERP resource to the OIM User.

1.4 Features of the Connector

The following are features of the connector:

- [Section 1.4.1, "SoD Validation of Entitlement Requests"](#)
- [Section 1.4.2, "Full and Incremental Reconciliation"](#)
- [Section 1.4.3, "Limited \(Filtered\) Reconciliation"](#)
- [Section 1.4.4, "Batched Reconciliation"](#)
- [Section 1.4.5, "SNC Communication Between the Target System and Oracle Identity Manager"](#)

1.4.1 SoD Validation of Entitlement Requests

Starting from this release, the connector supports the SoD feature introduced in Oracle Identity Manager release 9.1.0.2. The following are the focal points of this software update:

- The SoD Invocation Library (SIL) is bundled with Oracle Identity Manager release 9.1.0.2. The SIL acts as a pluggable integration interface with any SoD engine.
- The SAP User Management connector is preconfigured to work with SAP GRC as the SoD engine. To enable this, changes have been made in the approval and provisioning workflows of the connector.

Note: The default approval workflow and associated object form can be used as an example of how to configure the SoD validation capabilities of SAP GRC into the SAP connector. You can use this to develop your own approval workflows and object forms.

- The SoD engine processes role and profile entitlement requests that are sent through the connector. This preventive simulation approach helps identify and correct potentially conflicting assignment of entitlements to a user, before the requested entitlements are granted to users.

See Also:

Oracle Identity Manager Tools Reference for Release 9.1.0.2 for detailed information about the SoD feature

[Section 2.3.3, "Configuring SoD"](#) in this guide

1.4.2 Full and Incremental Reconciliation

In full reconciliation, all person records are fetched from the target system to Oracle Identity Manager. In incremental reconciliation, only person records that are added or modified after the last reconciliation run are fetched into Oracle Identity Manager.

A parameter of the IT resource is used as the time stamp at which a reconciliation run begins. If that parameter is set to 0, then full reconciliation is performed. If that parameter holds a non-zero value, then incremental reconciliation is performed.

As mentioned earlier in this chapter, you can switch from incremental to full reconciliation at any time.

1.4.3 Limited (Filtered) Reconciliation

To limit or filter the records that are fetched into Oracle Identity Manager during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled.

See [Section 3.2.2, "Limited Reconciliation vs. Regular Reconciliation"](#) for more information.

1.4.4 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 3.2.3, "Batched Reconciliation"](#) for more information.

1.4.5 SNC Communication Between the Target System and Oracle Identity Manager

You can configure SNC to secure communication between Oracle Identity Manager and the target system.

See [Section 2.3.4, "Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System"](#) 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 Date Format lookup field to select a date format from the list of supported date formats. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are 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.

Note: The target system allows you to use special characters in lookup fields. However, in Oracle Identity Manager, special characters are not supported in lookup definitions.

The `Lookup.SAP.R3.LookupMappings` lookup definition is used to map each lookup definition with the BAPI that is used to fetch values for the lookup definition from the target system.

The Code Key column of the `Lookup.SAP.R3.LookupMappings` lookup definition contains names of the lookup definitions that are synchronized with the target system. The Decode column contains the name and parameters of the corresponding BAPIs.

[Table 1–2](#) lists the entries in the `Lookup.SAP.R3.LookupMappings` lookup definition.

Table 1–2 Entries in the Lookup.SAP.R3.LookupMappings Lookup Definition

Code Key	Decode
Lookup.SAP.R3.CommType	BAPI_HELPVALUES_GET;GETDETAIL;ADDRESS;COMM_TYPE;COMM_TYPE;COMM_TEXT
Lookup.SAP.R3.DateFormat	BAPI_HELPVALUES_GET;GETDETAIL;DEFAULTS;DATFM;_LOW;_TEXT
Lookup.SAP.R3.DecimalNotation	BAPI_HELPVALUES_GET;GETDETAIL;DEFAULTS;DCPFM;_LOW;_TEXT
Lookup.SAP.R3.LangComm	BAPI_HELPVALUES_GET;GETDETAIL;ADDRESS;LANGU_P;SPRAS;SPTEXT
Lookup.SAP.R3.TimeZone	BAPI_HELPVALUES_GET;CHANGE;ADDRESS;TIME_ZONE;TZONE;DESCRIPT
Lookup.SAP.R3.UserGroups	BAPI_HELPVALUES_GET;GETDETAIL;GROUPS;USERGROUP;USERGROUP;TEXT
Lookup.SAP.R3.UserTitle	BAPI_HELPVALUES_GET;GETDETAIL;ADDRESS;TITLE_P;TITLE_MEDI;TITLE_MEDI;
Lookup.SAP.R3.Roles	BAPI_HELPVALUES_GET;GETDETAIL;ACTIVITYGROUPS;AGR_NAME;AGR_NAME;TEXT;AGR_COLL;AGR_SINGLE;SH
Lookup.SAP.R3.Profiles	BAPI_HELPVALUES_GET;GETDETAIL;PROFILES;BAPIPROF;PROFN;PTEXT

The following is the format of entries in the lookup definitions listed in the preceding table:

- Code Key value: *IT_RESOURCE_KEY~LOOKUP_FIELD_ID*

In this format:

- *IT_RESOURCE_KEY* is the numeric code assigned to each IT resource in Oracle Identity Manager.
- *LOOKUP_FIELD_ID* is the target system code assigned to each lookup field entry.

Sample value: 1~PRT

- Decode value: Description of the lookup field entry

Sample value: Printer

The SAP R3 Lookup Recon scheduled task is used to synchronize values of these lookup definitions with the target system. See [Section 3.1, "Scheduled Task for Lookup Field Synchronization"](#) for more information about this scheduled task.

While performing a provisioning operation on the Administrative and User Console, you select the IT resource for the target system on which you want to perform the operation. When you perform this action, the lookup definitions on the page are automatically populated with values corresponding to the IT resource (target system installation) that you select.

[Table 1–3](#) describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

Table 1–3 Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.SAP.LockUnlock	<p>This lookup definition is used to populate the Lock User list on the Admin and User Console. The following are the Code Key and Decode values in this lookup definition:</p> <ul style="list-style-type: none"> ■ Lock: Lock User ■ Unlock: Unlock User 	This lookup definition is preconfigured. You must not change the entries in this lookup definition.
Lookup.SAP.R3.BAPIKeys	<p>Code Key: Resource object attribute name</p> <p>Decode: Structure name in the corresponding BAPI</p> <p>This lookup definition is used during linking of an SAP HRMS account with an SAP ERP account, for all attributes other than the UserAlias attribute.</p>	This lookup definition is preconfigured. You must not change the entries in this lookup definition.
Lookup.SAP.R3.BAPIXKeys	<p>Code Key: Resource object attribute name</p> <p>Decode: Structure name in the corresponding BAPI</p> <p>This lookup definition is used during linking of an SAP HRMS account with an SAP ERP account, for only the UserAlias attribute.</p>	This lookup definition is preconfigured. You must not change the entries in this lookup definition.
Lookup.SAP.R3.Configuration	This lookup definition contains configuration values that are used during SoD validation.	This lookup definition is preconfigured. You can only set a value for the Risk Level entry. See Section 2.3.3.2, "Specifying Values for SoD-Related Entries in the Lookup.SAP.R3.Configuration Lookup Definition" for more information.
Lookup.SAP.R3.FieldNames	<p>Code Key: Resource object attribute name</p> <p>Decode: Attribute name in the corresponding BAPI</p> <p>This lookup definition is used during linking of an SAP HRMS account with an SAP ERP account, for all attributes other than the UserAlias attribute.</p>	This lookup definition is preconfigured. You must not change the entries in this lookup definition.
Lookup.SAP.R3.FieldNamesX	<p>Code Key: Resource object attribute name</p> <p>Decode: Attribute name in the corresponding BAPI</p> <p>This lookup definition is used during linking of an SAP HRMS account with an SAP ERP account, for only the UserAlias attribute.</p>	This lookup definition is preconfigured. You must not change the entries in this lookup definition.

Table 1–3 (Cont.) Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.SAP.R3.LookupMappings	Code Key: Names of lookup definitions to be synchronized with the target system Decode: Name of the corresponding BAPI and parameters to be passed to the BAPI	This lookup definition is preconfigured. You must not change the entries in this lookup definition.
Lookup.SAP.R3.Systems	Both Code Key and Decode columns contain the system name of the SAP ERP installation This lookup definition is used during SoD validation of entitlement requests.	You must enter the system name of the SAP ERP system in both Code Key and Decode columns. There can be only one entry in this lookup definition.
Lookup.SAP.R3.RoleChildformMappings	Code Key: Dummy role child form attribute name Decode: Corresponding actual role child form attribute name This lookup definition is used during SoD validation of entitlement requests.	This lookup definition is preconfigured. You must not change the entries in this lookup definition.
Lookup.SAP.R3.ProfileChildformMappings	Code Key: Dummy profile child form attribute name Decode: Corresponding actual profile child form attribute name This lookup definition is used during SoD validation of entitlement requests.	This lookup definition is preconfigured. You must not change the entries in this lookup definition.

1.6 Connector Objects Used During Reconciliation

The R3 Recon scheduled task is used to initiate a target resource reconciliation run. This scheduled task is discussed in [Section 3.2.4, "Reconciliation Scheduled Task"](#).

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

This section discusses the following topics:

- [Section 1.6.1, "User Attributes for Reconciliation"](#)
- [Section 1.6.2, "Reconciliation Rules"](#)
- [Section 1.6.3, "Reconciliation Action Rules"](#)

1.6.1 User Attributes for Reconciliation

[Table 1–4](#) lists the user attributes whose values are fetched during a target resource reconciliation run.

Table 1–4 User Attributes for Target Resource Reconciliation

Process Form Field	SAP ERP Attribute	Description
Alias	USERALIAS	User alias
Building	BUILDING_P	Building number
Code	INITS_SIG	Code
CommType	COMM_TYPE	Communication type
DateFormat	DATFM	Date format
DecimalNotation	DCPFM	Decimal notation
Department	DEPARTMENT	Department
Email	E_MAIL	E-mail address
Extension	TEL1_EXT	Extension for the telephone number
Fax	FAX_NUMBER	Fax number
FirstName	FIRSTNAME	First name
Floor	FLOOR_P	Floor number
Function	FUNCTION	Function
LangComm	LANGU_P	Communication language
LangLogon	LANGU	Logon language
LastName	LASTNAME	Last name
LockUser	Lock User	Status (either Locked or Unlocked) of the user
RoomNo	ROOM_NO_P	Room number
TimeZone	TZONE	Time zone
StartMenu	START_MENU	Default menu for the user
Telephone	TEL1_NUMBR	Telephone number
UserGroup	CLASS	Group to which the user is assigned
UserId	USERNAME	Login ID
UserProfile	BAPIPROF	Multivalued attribute for profiles
UserRole	AGR_NAME	Multivalued attribute for roles
UserTitle	TITLE_P	Title of the user
Xellerate Type	USTYP	Type of user

1.6.2 Reconciliation Rules

See Also: *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

The following sections provide information about the reconciliation rules for this connector:

- [Section 1.6.2.1, "Reconciliation Rule for Target Resource Reconciliation"](#)
- [Section 1.6.2.2, "Viewing Reconciliation Rules in the Design Console"](#)

1.6.2.1 Reconciliation Rule for Target Resource Reconciliation

The following is the process-matching rule:

Rule name: SAP R3 Recon Rule

Rule element: (SAP Linked User ID Equals UserId) or (User Login Equals UserId)

In the first element:

- SAP Linked User ID is the field in SAP HRMS that holds the User ID of the linked SAP ERP account.
- UserId is the User ID of the SAP ERP account in Oracle Identity Manager.

In the second element:

- User Login is the User ID field of the OIM User form.
- UserId is the User ID of the SAP ERP account.

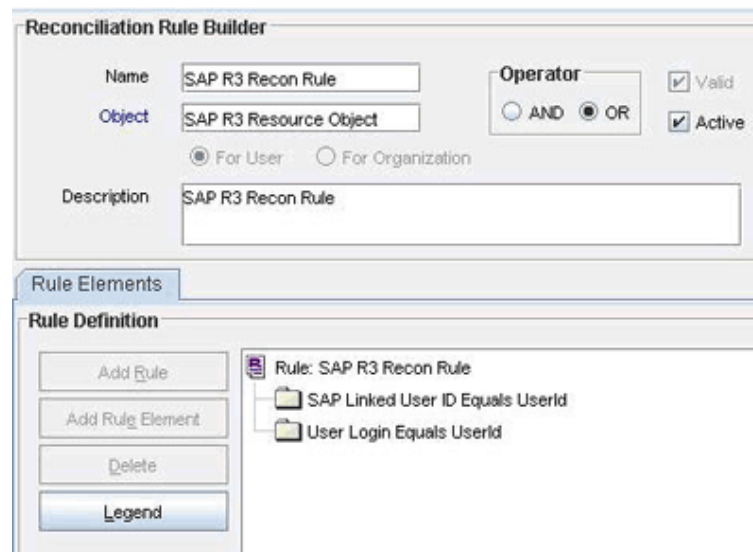
1.6.2.2 Viewing Reconciliation Rules in the Design Console

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**.
3. Double-click **Reconciliation Rules**.
4. Search for **SAP R3 Recon Rule**. [Figure 1–2](#) shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule



1.6.3 Reconciliation Action Rules

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.

The following sections provide information about the reconciliation rules for this connector:

- [Section 1.6.3.1, "Reconciliation Action Rules for Target Resource Reconciliation"](#)
- [Section 1.6.3.2, "Viewing Reconciliation Action Rules in the Design Console"](#)

1.6.3.1 Reconciliation Action Rules for Target Resource Reconciliation

[Table 1–5](#) lists the action rules for target resource reconciliation.

Table 1–5 Action Rules for Target Resource Reconciliation

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

1.6.3.2 Viewing Reconciliation Action Rules in the Design Console

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. If you want to view the reconciliation action rules for target resource reconciliation, then search for and open the **SAP UM Resource Object** 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 1–3](#) shows the reconciliation action rules for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules

Reconciliation Action Rules		Rule Condition	Action	User
1	One Entity Match Found	Establish Link		
2	One Process Match Found	Establish Link		

1.7 Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

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

This section discusses the following topics:

- [Section 1.7.1, "User Provisioning Functions"](#)
- [Section 1.7.2, "User Attributes for Provisioning"](#)

1.7.1 User Provisioning Functions

[Table 1–6](#) lists the supported user provisioning functions and the adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.

See Also: *Oracle Identity Manager Connector Concepts* for generic information about process tasks and adapters

Table 1–6 User Provisioning Functions

Function	Adapter
Create a user account	SAP R3 Create User
Delete a user account	SAP R3 Delete User
Lock a user account	SAP R3 Lock UnLock User
Unlock a user account	SAP R3 Lock UnLock User
Change password	SAP R3 Password Change
Edit a user account	SAP R3 Modify User
Change a user's alias	SAP R3 Modify UserX

Table 1–6 (Cont.) User Provisioning Functions

Function	Adapter
Add a user account to an activity group (role)	SAP R3 Add Role
Remove a user account from an activity group (role)	SAP R3 Remove Role
Assign a profile to a user account	SAP R3 Add Profile
Remove a profile from a user account	SAP R3 Remove Profile

1.7.2 User Attributes for Provisioning

[Table 1–7](#) lists the user attributes for which you can specify or modify values during provisioning operations.

Table 1–7 User Attributes for Provisioning

Process Form Field	SAP ERP Attribute	Description
Alias	USERALIAS	User alias
Building	BUILDING_P	Building number
Code	INITS_SIG	Code
CommType	COMM_TYPE	Communication type
DateFormat	DATFM	Date format
DecimalNotation	DCPFM	Decimal notation
Department	DEPARTMENT	Department
Email	E_MAIL	E-mail address Note: In SAP 4.7 or later, you can enter only English letters in the E-mail Address field.
Extension	TEL1_EXT	Extension for the telephone number
Fax	FAX_NUMBER	Fax number
FirstName	FIRSTNAME	First name
Floor	FLOOR_P	Floor number
Function	FUNCTION	Function
LangComm	LANGU_P	Communication language
LangLogon	LANGU	Logon language
LastName	LASTNAME	Last name
LockUser	BAPIPWD	Password
RoomNo	ROOM_NO_P	Room number
TimeZone	TZONE	Time zone
StartMenu	START_MENU	Default menu for the user
Telephone	TEL1_NUMBR	Telephone number
UserGroup	CLASS	Group to which the user is assigned
UserId	USERNAME	Login ID

Table 1–7 (Cont.) User Attributes for Provisioning

Process Form Field	SAP ERP Attribute	Description
Password	PASSWORD	Password Note: You must ensure that the password specified during a provisioning operation adheres to password policies set on the target system. Otherwise, you might encounter the following error: SAP.PASSWORD_CHANGE_ERROR
UserProfile	BAPIPROF	Multivalue attribute for profiles
UserRole	AGR_NAME	Multivalue attribute for roles
UserTitle	TITLE_P	Title of the user
Xellerate Type	USTYP	Type of user

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 the procedures to perform if you want to extend the functionality of the connector.
- [Chapter 5, "Testing and Troubleshooting"](#) describes procedures to test and troubleshoot the connector.
- [Chapter 6, "Known Issues"](#) lists known issues associated with this release of the connector.

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"](#)

Note: Some of the procedures described in this chapter must be performed on the target system. To perform these procedures, you must use an SAP administrator account to which the SAP_ALL and SAP_NEW profiles have been assigned.

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- [Section 2.1.1, "Preinstallation on Oracle Identity Manager"](#)
- [Section 2.1.2, "Preinstallation on the Target System"](#)

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- [Section 2.1.1.1, "Files and Directories on the Installation Media"](#)
- [Section 2.1.1.2, "Determining the Release Number of the Connector"](#)

2.1.1.1 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 Installation Media

File in the Installation Media Directory	Description
configuration/SAPUM-CL.xml	This XML file contains configuration information that is used during connector installation.
BAPI/xlsapcar.sar	This file contains information for configuring the SAP system so that the connector is able to access the APIs on the target system.
lib/SAPUserMgmt.jar	This JAR file contains the class files that are used in connector operations. During connector deployment, this file is copied into the following directory: <i>OIM_HOME/xellerate/JavaTasks</i>

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

File in the Installation Media Directory	Description
lib/SAPCommon.jar	This JAR file contains the class files that are common to all SAP connectors. During connector deployment, this file is copied into the following directory: <i>OIM_HOME</i> /xellerate/JavaTasks
lib/Common.jar	This JAR file contains the class files that are common to all connectors. During connector deployment, this file is copied into the following directory: <i>OIM_HOME</i> /xellerate/JavaTasks
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied into the following directory: <i>OIM_HOME</i> /xellerate/connectorResources Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
test/Troubleshoot/com/thortech/xl/integration/sap/test/troubleShootingUtility.class	This utility is used to test connector functionality.
test/config/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/config/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/SAP-UserMgmt-Main-ConnectorConfig.xml	This XML file contains definitions for the following components of the connector: <ul style="list-style-type: none"> ■ IT resource definition ■ SAP User form ■ Lookup definitions ■ Connectors ■ Resource object ■ Process definition ■ Reconciliation scheduled tasks
xml/SAP-UserMgmt-RequestApproval-ConnectorConfig.xml	This file contains information required to enable request-based provisioning. See Section 2.3.1.1, "Enabling Request-Based Provisioning" for instructions on importing this file.
xml/SAPUMTrusted.xml	This XML file is not used by the connector. It will be removed in a future release.

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

2.1.1.2 Determining the Release Number of the Connector

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 connector JAR file that is in the *OIM_HOME*/xellerate/JavaTasks directory.

2. Open the Manifest.mf file in a text editor. The Manifest.mf file is one of the files bundled inside the connector JAR file.

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

2.1.2 Preinstallation on the Target System

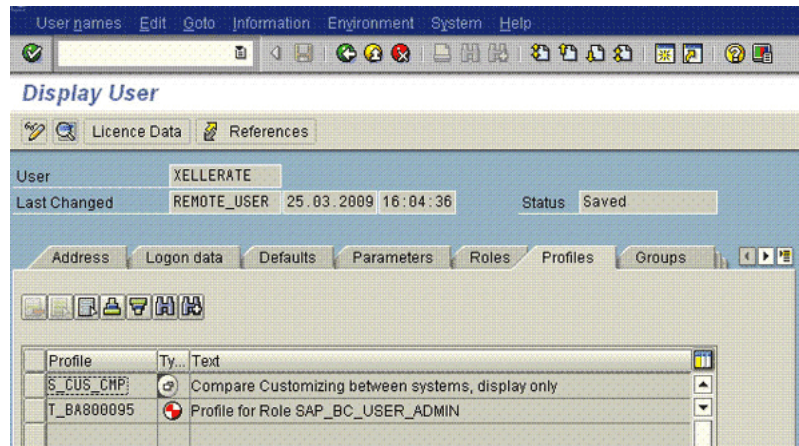
Preinstallation on the target system involves performing the following procedures:

2.1.2.1 Creating a Target System User Account for Connector Operations

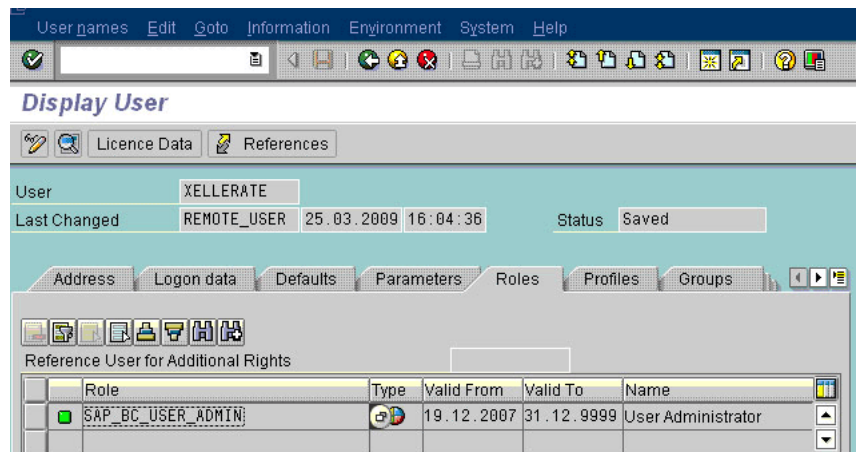
Note: You provide the credentials of this user account while configuring the IT resource. The procedure is described later in the guide.

The connector uses a target system account to connect to the target system during reconciliation. For minimum authorization, create a user account and assign the S_CUS_CMP profile and SAP_BC_USER_ADMIN role to it. The User type must be set to Communication. This is the default setting for user accounts.

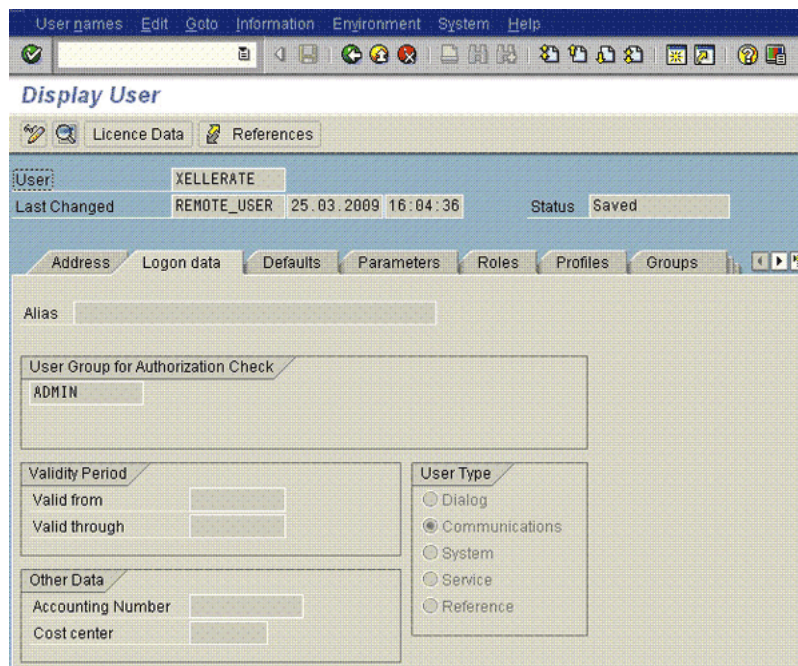
The S_CUS_CMP profile is displayed in the following screenshot:



The SAP_BC_USER_ADMIN role is displayed in the following screenshot:



The following screenshot shows the Communications user type selected:



If you are not able to find the profiles or role for minimum authorization, then create a user account and assign it to the SAP_ALL and SAP_NEW groups. These groups are used for full authorization.

If this target system user account is not assigned the specified rights, then the following error message may be displayed during connector operations:

SAP Connection JCO Exception: User TEST_USER has no RFC authorization for function group SYST

2.1.2.2 Using External Code Files

Note:

To download files from the SAP Web site, you must have access to the SAP service marketplace with Software Download authorization.

In a clustered environment, copy the JAR files and the contents of the connectorResources directory to the corresponding directories on each node of the cluster.

To download and copy the external code files to the required locations:

1. Download the SAP Java connector file from the SAP Web site as follows:
 - a. Open the following page in a Web browser:
<https://websmp104.sap-ag.de/connectors>
 - b. Open the SAP JAVA Connector page by selecting **Application Platform, Connectivity, Connectors, SAP Java Connector, and Tools & Services**.
 - c. On the SAP JAVA Connector page, links for files that you can download are displayed on the right pane. Click the link for the SAP JCo release that you want to download.

- d. In the dialog box that is displayed, specify the path of the directory in which you want to save the file.
2. Extract the contents of the file that you download.
3. Copy the sapjco3.jar file into the *OIM_HOME/Xellerate/ThirdParty* directory.

Note: Ensure that you are using version 3.0 of the sapjco3.jar file.

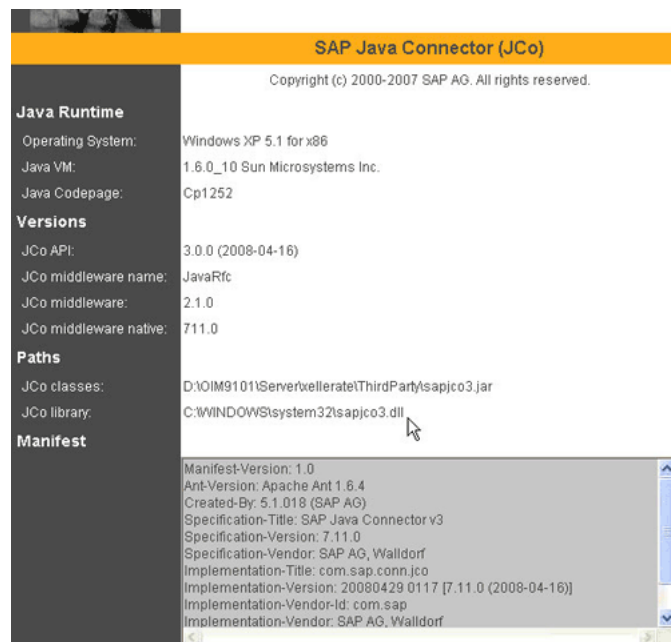
4. Copy the RFC files into the required directory on the Oracle Identity Manager host computer, and then modify the appropriate environment variable so that it includes the path to this directory:
 - On Microsoft Windows:
Copy the sapjco3.dll file into the winnt\system32 directory. Alternatively, you can copy these files into any directory and then add the path to the directory in the PATH environment variable.
 - On Solaris and Linux:
Copy the sapjco3.so file into the /usr/local/jco directory, and then add the path to this directory in the LD_LIBRARY_PATH environment variable.
5. Restart the server for the changes in the environment variable to take effect.

Note: You can either restart the server now or after the connector is installed.

6. To check if SAP JCo is correctly installed, in a command window, run one of the following commands:

```
java -jar JCO_DIRECTORY/sapjco3.jar
java -classpath JCO_DIRECTORY/sapjco3.jar com.sap.conn.jco.rt.About
```

Figure 2–1 shows the dialog box that is displayed. The JCo classes and JCo library paths must be displayed in this dialog box.

Figure 2–1 Dialog Box Displayed on Running the SAP JCo Test

7. Ensure that the msvc80.dll and msvcp80.dll files are in the c:\WINDOWS\system32 directory. If required, both files can be downloaded from various sources on the Internet.

2.2 Installation

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.

Direct provisioning is automatically enabled after you run the Connector Installer. If required, you can enable request-based provisioning in the connector. Direct provisioning is automatically disabled when you enable request-based provisioning. See [Section 2.3.1.1, "Enabling Request-Based Provisioning"](#) if you want to use the request-based provisioning feature for this target system.

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:
OIM_HOME/xellerate/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 *Oracle Identity Manager Administrative and User Console*.
3. Click **Deployment Management**, and then click **Install Connector**.
4. From the Connector List list, select **SAP UM 9.1.0.0**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

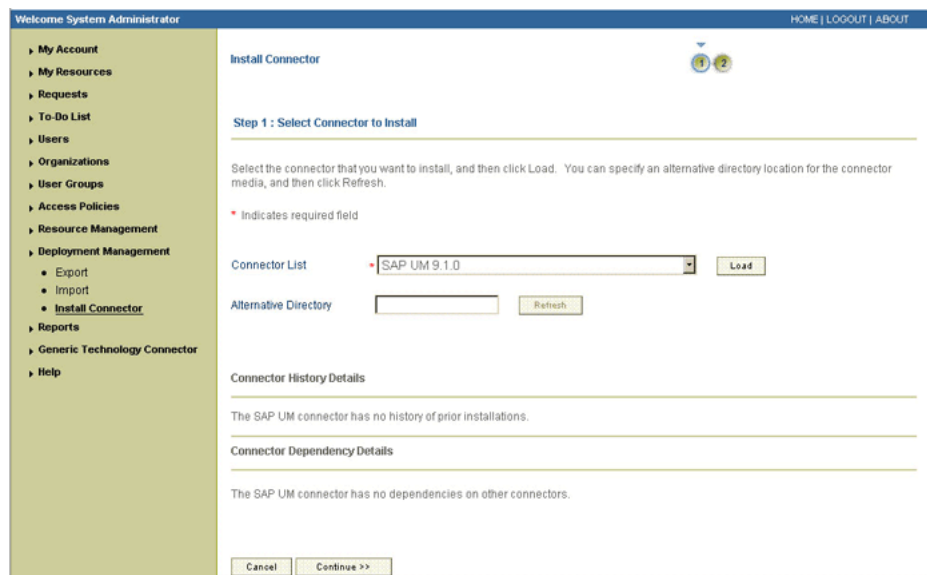
OIM_HOME/xellerate/ConnectorDefaultDirectory

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 UM 9.1.0.0**.

5. Click **Load**.

The following screenshot shows this Administrative and User Console page:



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 XML files (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 3.

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 2.3.1.5, "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

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. Restart Oracle Identity Manager.

Note: 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 clustered environment, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. Then, restart each node. See [Section 2.1.1.1, "Files and Directories on the Installation Media"](#) for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- [Section 2.3.1, "Configuring the Oracle Identity Manager Server"](#)
- [Section 2.3.2, "Configuring the Target System"](#)
- [Section 2.3.3, "Configuring SoD"](#)
- [Section 2.3.4, "Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System"](#)
- [Section 2.3.5, "Configuring the IT Resource"](#)

2.3.1 Configuring the Oracle Identity Manager Server

Configuring Oracle Identity Manager involves performing the following procedures:

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

- [Section 2.3.1.1, "Enabling Request-Based Provisioning"](#)

- [Section 2.3.1.2, "Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server"](#)
- [Section 2.3.1.3, "Configuring the SAP Change Password Function"](#)
- [Section 2.3.1.4, "Changing to the Required Input Locale"](#)
- [Section 2.3.1.5, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#)
- [Section 2.3.1.6, "Enabling Logging"](#)

2.3.1.1 Enabling 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 cannot 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: Do not configure the connector for request-based provisioning if you also want to use the connector for direct provisioning. See [Section 2.3.1.1, "Enabling Request-Based Provisioning"](#) for information about that procedure.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.
- Direct provisioning cannot be used if you enable request-based provisioning.

Prerequisites

You must run Oracle Identity Manager in INFO mode when you import the XML file for request-based provisioning. If Oracle Identity Manager is running in DEBUG mode when you import the XML file, then the import operation does not work correctly.

Before you perform this procedure, set your browser to use JRE version 1.6.0_07. If you try to import the XML file with your browser set to any other JRE version, then the browser stops responding.

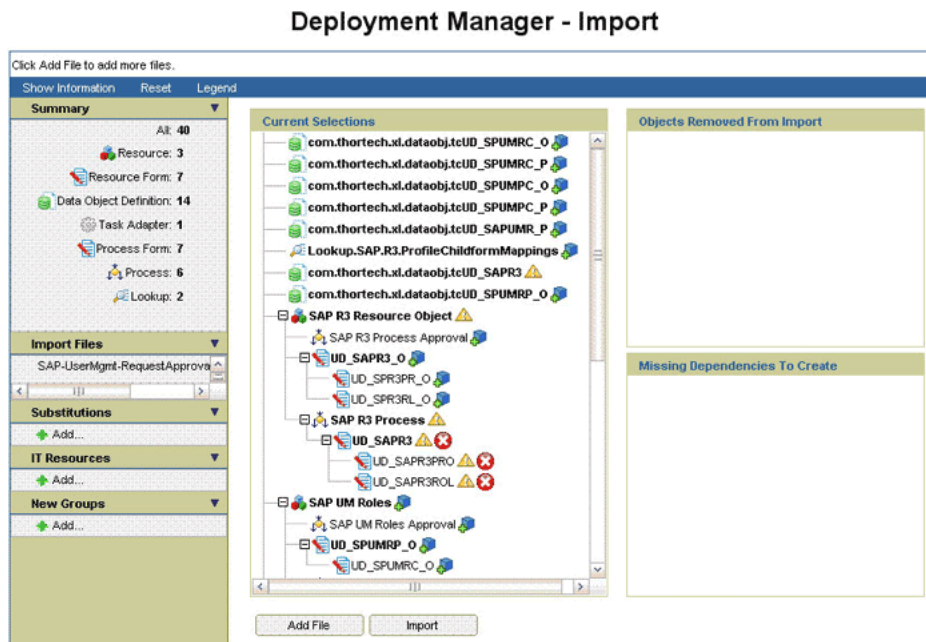
To enable request-based provisioning:

Note: Before you perform this procedure, set your browser to use JRE version 1.6.0_07. If you try to import the XML file with your browser set to any other JRE version, then the browser stops responding.

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 SAP-UserMgmt-RequestApproval-ConnectorConfig.xml file, which is in the xml directory on the installation media. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.

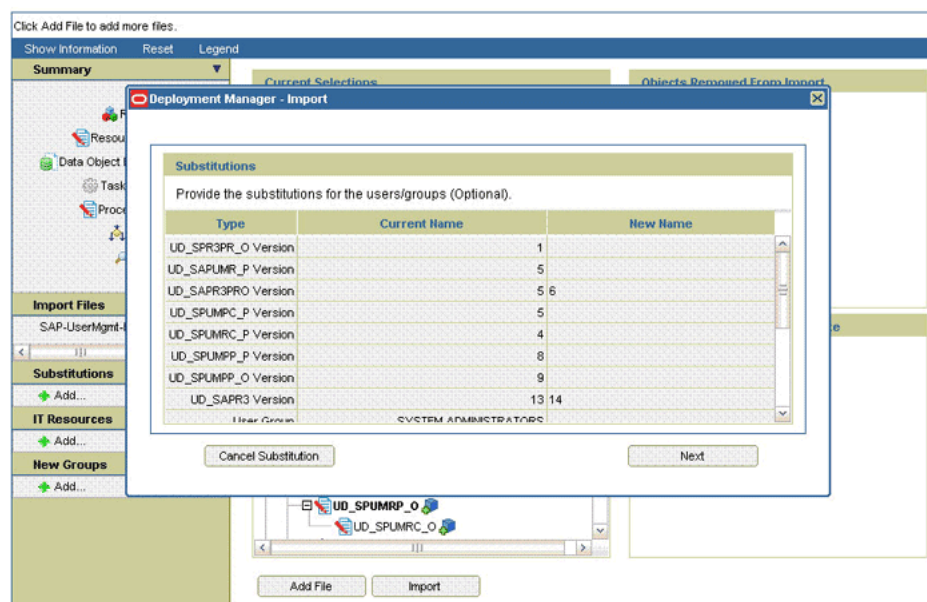
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.

At this stage, the Deployment Manager Import page shows an error because the process form version for request-based provisioning is the same as the process form version for direct provisioning. To work around this issue:



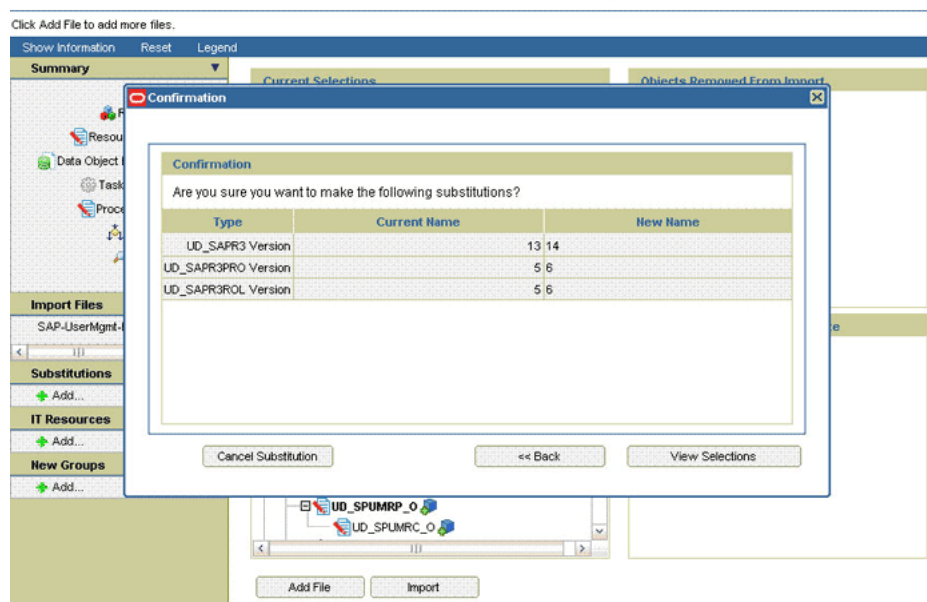
8. Note down the names of the forms that show errors, that is, the red cross sign against their names.
9. On the left pane, click **Add** under Substitutions.
The Add link is shown in the following screenshot:
10. In the pop-up window that is displayed, enter new version names for process forms that had name conflicts.

Deployment Manager - Import



11. Click **Next**. The forms for which you enter new form versions are displayed.

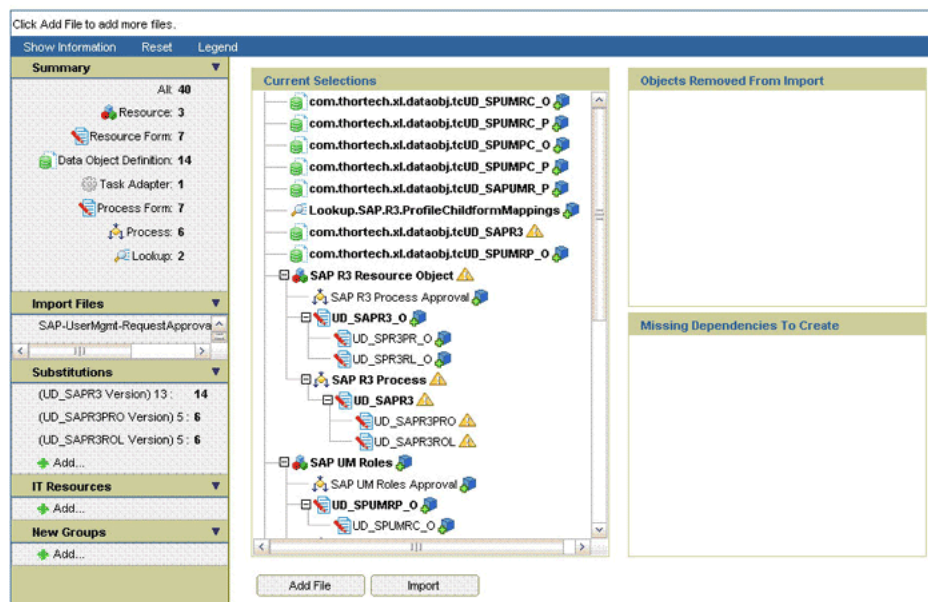
Deployment Manager - Import



12. Click **View Selections**.

At this stage, the Deployment Manager Import page should not show an error. See the following screenshot:

Deployment Manager - Import



13. Click **Import**.

In the message that is displayed, click **Import** to confirm that you want to import the XML file and then click **OK**.

To suppress the Standard Approval process definition:

Note: The Standard Approval process is common to all resource objects. If you enable request-based provisioning, then you must suppress this process definition.

1. On the Design Console, expand **Process Management** and double-click **Process Definition**.
2. Search for and open the **Standard Approval** process definition.
3. On the Tasks tab, double-click the **Approve** task.
4. On the Integration tab of the Editing Task dialog box, click **Add**.
5. In the Handler Selection dialog box:
 - Select **System**.
 - Select the **tcCompleteTask** handler.
 - Click the Save icon, and then close the dialog box.
6. In the Editing Task dialog box, click the Save icon and close the dialog box.
7. Click the Save icon to save changes made to the process definition.

2.3.1.2 Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server

Note: Perform the procedure described in this section only if your Oracle Identity Manager installation is running on Microsoft SQL Server.

In this connector, the child forms of a resource implement the dependent lookup feature of Oracle Identity Manager. By default, the queries for synchronization of lookup field's values from the target system are based on Oracle Database SQL. If your Oracle Identity Manager installation is running on Microsoft SQL Server, then you must modify the lookup queries for synchronization of lookup definitions as follows:

1. On the Design Console, expand **Development Tools** and double-click **Form Designer**.
2. From this point onward, the procedure depends on the type of form that you are modifying:

- **For child forms:**

The following are the child forms shipped with this connector:

- UD_SAPR3RO
- UD_SAPR3PRO
- UD_SPUMRC_O
- UD_SPUMPC_O
- UD_SPUMPC_P
- UD_SPUMRC_P
- UD_SPR3RL_O
- UD_SPR3PR_O

Perform the following procedure for the child forms:

- a. Search for and open the parent form of the child form.
- b. On the Additional Columns tab for the Parent form, search for the row containing the `ITResourceLookupField` field type and note down the value in the Name column for the row.
- c. Search for and open the child form.
- d. Click **Create New Version**.
- e. Enter a version for the form, click the Save icon, and then close the dialog box.
- f. On the Properties tab, double-click **Lookup Query** in the list of components.
- g. From the Edit Property dialog box, copy the contents of the Property Value field for the Lookup Query property name into a text file. The contents of the Property Value field are the SQL query for Oracle Database.

The following is a sample Oracle Database query for child forms role:

```
select lkv_encoded,lkv_decoded from lkv lkv,lku lku where
```

```
lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.R3.Roles'
and substr(lkv_encoded, 1, length(concat('$Form
data.UD_SAPR3_RESOURCE_TYPE$', '~')))=concat('$Form
data.UD_SAPR3_RESOURCE_TYPE$', '~')
```

- h. On the Additional Columns tab, search for the lookup containing the User Role field label. Note down the value in the Name column.
- i. Note down the value of the lku_type_string_key column from the Oracle Database query. In the sample Oracle Database query, the value of the lku_type_string_key column is Lookup.SAP.R3.Roles.
- j. Delete the contents of the Property Value field.
- k. Copy the following query into the Property Value field:

```
select lkv_encoded,lkv_decoded from lkv lkv,lku lku where
lkv.lku_key=lku.lku_key and lku_type_string_key=
'LOOKUP_DEFINITION_NAME' and CHARINDEX('IT_RESOURCE_COLUMN_NAME' + '~'
, lkv_encoded)>0
```

In this query:

Replace *LOOKUP_DEFINITION_NAME* with the lookup definition name that you copy in Step i.

Replace *IT_RESOURCE_COLUMN_NAME* with the name of the value that you note down in Step h.

- l. In the Edit Property dialog box, click the Save icon and then close the dialog box.
- m. Click the Save icon to save changes to the process form.
- n. From the **Current Version** list, select the version that you modified.
- o. Click **Make Version Active**.
- p. Click the Save icon.
- **For parent forms:**
Perform the following procedure for the UD_SAPR3 and UD_SAPR3_O forms:
 - a. Search for and open the form.
 - b. Click **Create New Version**.
 - c. Enter a version for the form, click the Save icon, and then close the dialog box.
 - d. On the Additional Columns subtab of the Properties tab, search for the row containing the ITResourceLookupField field type.
 - e. Note down the value in the Name column for the row containing the ITResourceLookupField field type.
 - f. On the Child Tables subtab of the Properties tab, double-click **Lookup Query** in the list of components.
 - g. From the Edit Property dialog box, copy the contents of the Property Value field for the Lookup Query property name into a text file. The contents of the Property Value field are the SQL query for Oracle Database.

The following is a sample Oracle Database query for parent forms:


```
select lkv_encoded, lkv_decoded from lkv lkv, lku lku where
lkv.lku_key=lku.lku_key and
lku_type_string_key='Lookup.SAP.R3.LangComm' and
substr(lkv_encoded,1,length(concat((select svr_key from svr where
svr_name='$Form data.UD_SAPR3_RESOURCE_TYPE$'),'~')))=concat((select
svr_key from svr where svr_name='$Form
data.UD_SAPR3_RESOURCE_TYPE$'),'~')
```

- h. Note down the value of the lku_type_string_key column from the Oracle Database query. In the sample Oracle Database query, the value of the lku_type_string_key column is Lookup.SAP.R3.LangComm.
- i. Delete the contents of the Property Value field.
- j. Copy the following query into the Property Value field:

```
select lkv_encoded, lkv_decoded from lkv lkv, lku lku where
lkv.lku_key=lku.lku_key and
lku_type_string_key='LOOKUP_DEFINITION_NAME' and CHARINDEX( (select
CONVERT(varchar, svr_key) from svr where svr_name='$Form
data.IT_RESOURCE_COLUMN_NAME$') + '~' , lkv_encoded)>0
```

In this query:

Replace *LOOKUP_DEFINITION_NAME* with the lookup definition name that you copy in Step h.

Replace *IT_RESOURCE_COLUMN_NAME* with the name of the value that you note down in Step e.

- k. In the Edit Property dialog box, click the Save icon and then close the dialog box.
- l. Click the Save icon to save changes to the process form.
- m. From the **Current Version** list, select the version that you modified.
- n. Click **Make Version Active**.
- o. Click the Save icon.

2.3.1.3 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 UM Process process definition.
5. Double-click the **Password Updated** task.
6. On the Integration tab, specify values for the following parameters:

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

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

If this field is empty, then the user will be valid for an indefinite period.

- **userGroupCheck:** This is a string literal with the following format:

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

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

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

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

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

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

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

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

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

```
TERMINATED,0,;
```

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

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

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

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

```
TERMINATED, 0, ;
```

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

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

2.3.1.4 Changing to the Required Input Locale

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

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

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

During the connector deployment procedure, files are copied from the resources directory on the installation media into the `OIM_HOME/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

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

```
OIM_HOME/xellerate/bin/batch_file_name
```

2. Enter one of the following commands:

- On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

- On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

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

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

OIM_HOME/xellerate/config/xlConfig.xml

2.3.1.6 Enabling Logging

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

- **ALL**
This level enables logging for all events.
- **DEBUG**
This level enables logging of information about fine-grained events that are useful for debugging.
- **INFO**
This level enables logging of 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:

- **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.SAPUSERMANAGEMENT=log_level
```

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

For example:

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

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

- **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.SAPUSERMANAGEMENT=log_level
```

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

For example:

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

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

`WEBSPHERE_HOME/AppServer/logs/SERVER_NAME/SystemOut.log`

■ JBoss Application Server

To enable logging:

1. In the `JBOSS_HOME/server/default/conf/jboss-log4j.xml` file, locate or add the following lines if they are not already present in the file:

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

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

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

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

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

After you enable logging, 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.SAPUSERMANAGEMENT=log_level
```

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

For example:

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

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

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

2.3.2 Configuring the Target System

This section describes the procedures involved in configuring the target system. You may need the assistance of the SAP Basis administrator to perform some of these procedures.

Configuring the target system involves the following tasks:

- [Section 2.3.2.1, "Creating an Entry in the BAPIF4T Table"](#)
- [Section 2.3.2.2, "Importing the Request"](#)
- [Section 2.3.2.3, "Configuring SAP Ports for Communication with Oracle Identity Manager"](#)

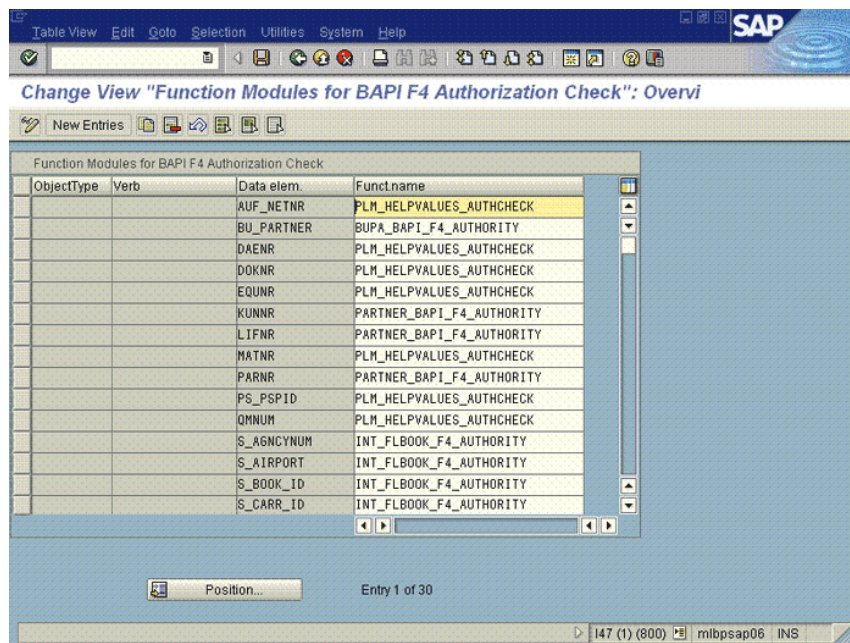
2.3.2.1 Creating an Entry in the BAPIF4T Table

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

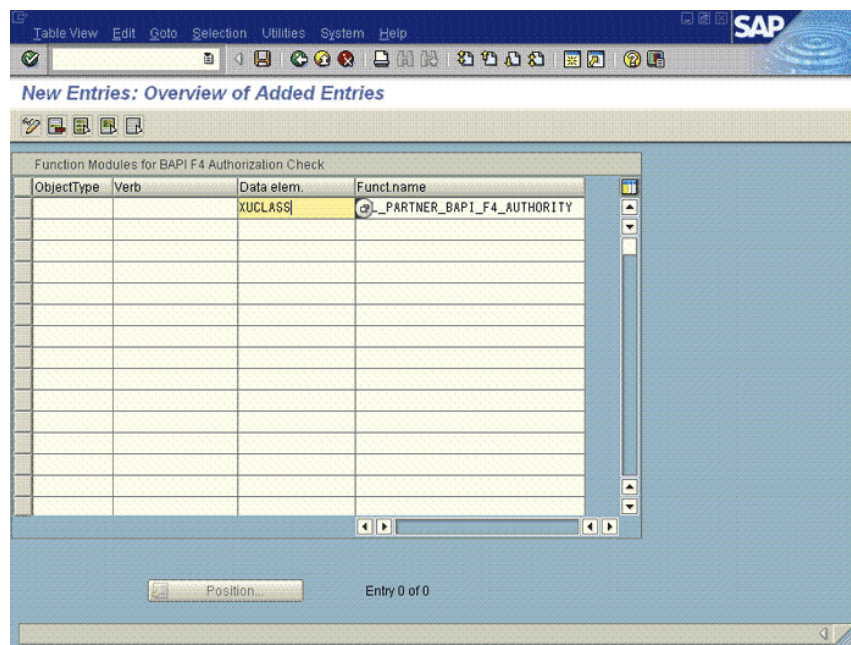
1. Run the SM30 transaction on the SAP system.

Note: SM30 is a *mandatory transaction* required to maintain tables in the SAP system.

2. Enter BAPIF4T as the table name, and then click **Maintain**. Ignore any warnings or messages that may be displayed.



3. Click **New Entries**.
4. Enter XUCLASS as the data element and ZXCL_PARTNER_BAPI_F4_AUTHORITY as the function name.



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

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

2.3.2.2 Importing the Request

Custom BAPIs are used during lookup field synchronization, reconciliation, and provisioning. You must import the request that contains the components of these BAPIs. When you import the request, the following custom objects are created on the SAP system:

Object Type	Object Name
Package	ZBAPI
Function Group	ZXLGROUP ZXLHELPVALUES ZXLPROFILE ZXLROLE ZXLUSER
Message class	ZXLBAPI

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

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

Importing the request into SAP involves the following steps:

- [Section 2.3.2.2.1, "Downloading the SAPCAR Utility"](#)
- [Section 2.3.2.2.2, "Extracting the Request Files"](#)
- [Section 2.3.2.2.3, "Performing the Request Import Operation"](#)

2.3.2.2.1 Downloading the SAPCAR Utility

Note: To download files from the SAP Web site, you must have access to the SAP service marketplace with Software Download authorization.

Every SAR file contains two files, Datafile and Cofile. These files contain the requests that are transported to the SAP system. These files constitute the xlsapcar.sar. You can use the SAPCAR utility to extract these files.

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

1. Log on to the SAP Web site at
<https://service.sap.com/swdc>
2. Click **OK** to confirm that the certificate displayed is the certificate assigned for your SAP installation.
3. Enter your SAP user name and password to connect to the SAP service marketplace.

4. Click **Downloads, SAP Support Packages, Entry by Application Group, and Additional Components**.
5. Select **SAPCAR, SAPCAR 7.0**, and the operating system. The download object is displayed.
6. Select the **Object** check box, and then click **Add to Download Basket**.
7. Specify the directory in which you want to download the SAPCAR utility. For example: C:/xlsapcar

2.3.2.2.2 Extracting the Request Files To extract the Datafile and Cofile components of the request:

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

The xlsapcar.sar file is in the BAPI directory inside the installation media directory.

2. In a command window, change to the directory in which you stored the SAPCAR utility and the xlsapcar.sar file.
3. Enter the following command to extract the Datafile and Cofile components of the request:

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

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

R999999..I47 (data)

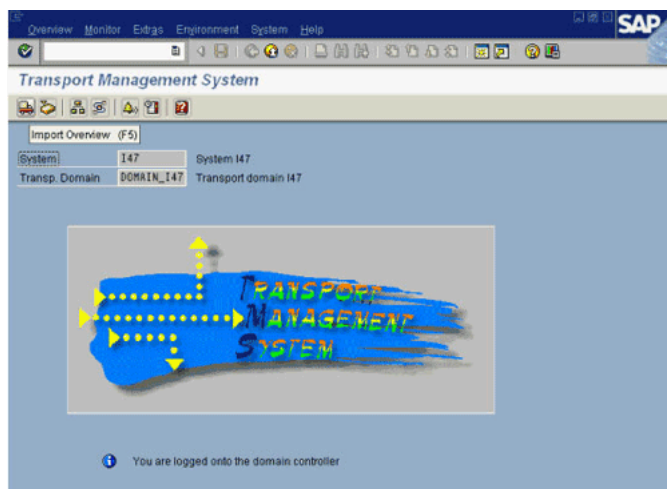
K999999.I47 (cofile)

The list of extracted files is displayed in the command window.

2.3.2.2.3 Performing the Request Import Operation To perform the request import operation:

Note: You would need the SAP Basis administrator's assistance to perform the following steps.

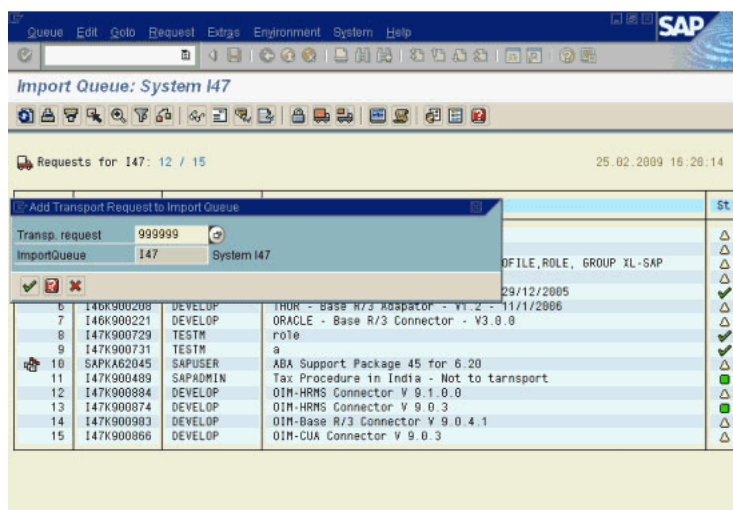
1. Copy the data and cofile into the *SAP_HOME*/trans/data and *SAP_HOME*/trans/cofiles directories, respectively.
2. Log in to SAP, and run transaction STMS.
3. To display the list of import queues, click the truck-shaped icon.



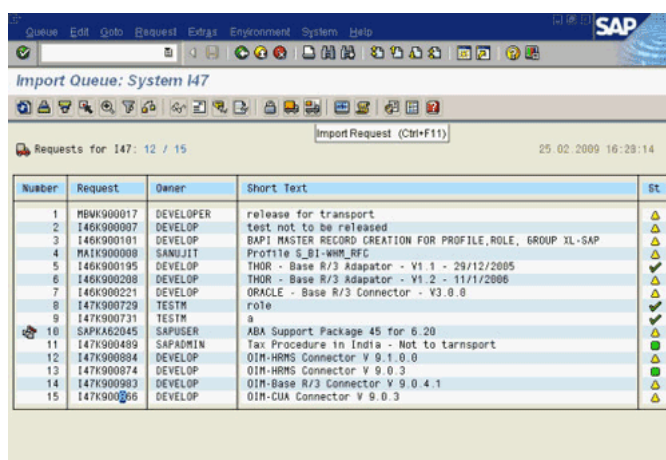
4. Double-click the appropriate queue.
Details of the queue are displayed.

Queue	Description	Requests	Status
I47	System I47	12	
ZVT	Virtual System	174	
		186	

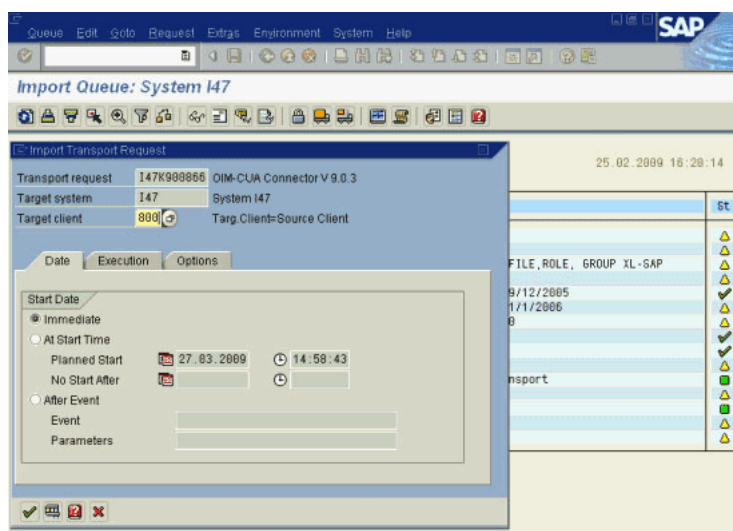
5. From the Extras menu, select **Other** requests and then select **Add**.
6. In the Transp. request field of the Add Transport Request to Import Queue dialog box, enter the transport request number and then press **Enter**.



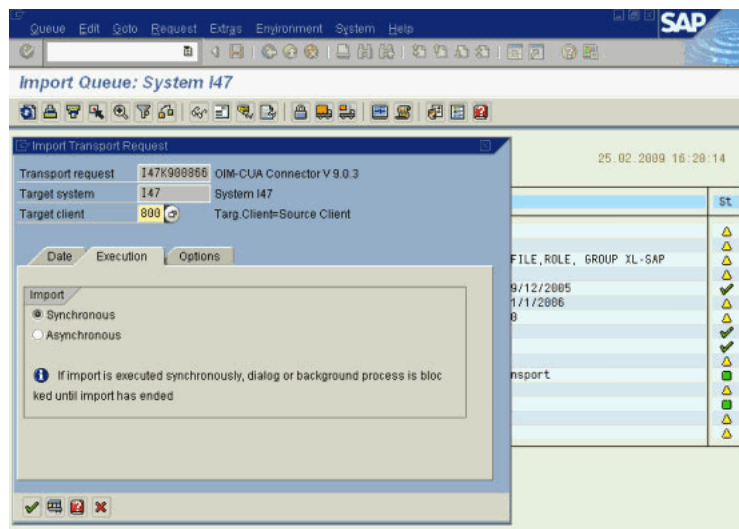
- When the request is added to the queue, select the request in the queue and then click the Import Request (half-truck-shaped) icon.



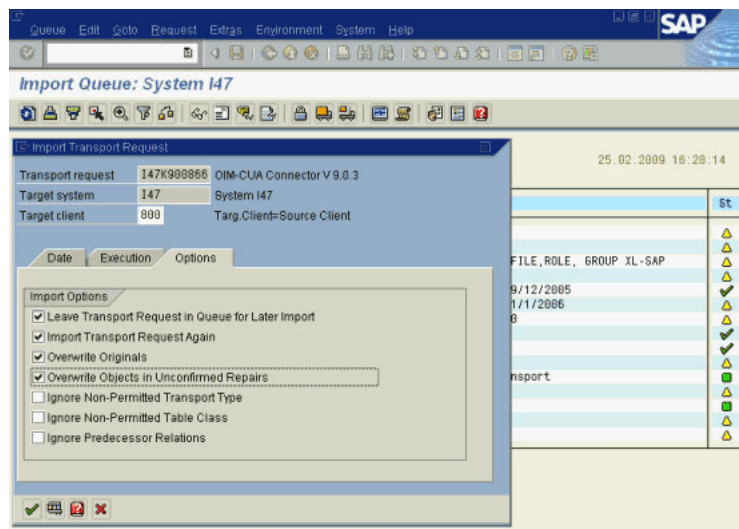
- On the Date tab of the Import Transport Request dialog box, enter the number of the client into which you are importing the request and then select **Immediate**.



9. On the Execution tab, select **Synchronous**.



10. On the Options tab, select import options according to your requirement.



Note: It is recommended that you select the first four options displayed on the tab.

11. Press **Enter**.

The request is imported to the specified system.

12. Check the log file to determine whether or not the import was successful.

To display the log file:

- a. Run transaction STMS.

Note: The STMS *needed transaction* is used to transport requests to the SAP system. SAR files that contain customized BAPI code are imported using the STMS transaction.

- b. Click Import overview, and double-click the appropriate transport queue on the next page.

The list of transport requests is displayed.

- c. Select the transport request number corresponding to the request that you import.

The transport request number is the same as the numeric part of the Cofile or Datafile names. In Step 3 of the preceding procedure, for the sample Cofile (K900863.I47) and Datafile (R900863.I47), the transport request number is 900863.

- d. Click the log file icon.

If the return code displayed in the log file is 4, then it indicates that the import ended with warnings. This may happen if the object is overwritten or already exists in the SAP system. If the return code is 8 or a higher number, then there were errors during the import.

13. Confirm the import of the request by running the SE80 transaction, and checking the ZBAPI package in the ABAP objects.

2.3.2.3 Configuring SAP Ports for Communication with Oracle Identity Manager

To enable communication between the target system and Oracle Identity Manager, you must ensure that ports listed in [Table 2-2](#).

Table 2-2 Ports for SAP Services

Service	Port Number Format	Default Port
Dispatcher	32SYSTEM_NUMBER	3200
Gateway (for non-SNC communication)	33SYSTEM_NUMBER	3300
Gateway (for SNC communication)	48SYSTEM_NUMBER	4800
Message server	36SYSTEM_NUMBER	3600

To check if these ports are open, you can, for example, try to establish a Telnet connection from Oracle Identity Manager to these ports.

2.3.3 Configuring SoD

See Also: [Section 3.4.3, "Request-Based Provisioning in an SoD-Enabled Environment"](#)

This section discusses the following procedures:

- [Section 2.3.3.1, "Configuring the SAP GRC to Act As the SoD Engine"](#)
- [Section 2.3.3.2, "Specifying Values for SoD-Related Entries in the Lookup.SAP.R3.Configuration Lookup Definition"](#)
- [Section 2.3.3.3, "Specifying the System Name in the Lookup.SAP.R3.Systems Lookup Definition"](#)
- [Section 2.3.3.4, "Specifying a Value for the TopologyName IT Resource Parameter"](#)
- [Section 2.3.3.5, "Disabling and Enabling SoD"](#)

Note: The ALL USERS group has INSERT, UPDATE, and DELETE permissions on the UD_SAPR3, UD_SAPR3ROL, UD_SAPR3PRO process forms. This is required to enable the following process:

During SoD validation of an entitlement request, data first moves from a dummy object form to a dummy process form. From there data is sent to the SoD engine for validation. If the request clears the SoD validation, then data is moved from the dummy process form to the actual process form. Because the data is moved to the actual process forms through APIs, the ALL USERS group must have INSERT, UPDATE, and DELETE permissions on the three process forms.

2.3.3.1 Configuring the SAP GRC to Act As the SoD Engine

See the "Configuring SAP GRC" section in the "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in *Oracle Identity Manager Tools Reference for Release 9.1.0.2* for information about this procedure.

2.3.3.2 Specifying Values for SoD-Related Entries in the Lookup.SAP.R3.Configuration Lookup Definition

You must specify values for the following entries in the Lookup.SAP.R3.Configuration lookup definition:

- **GRC Version**

Enter the version of SAP GRC that you are using. Depending on the version of SAP GRC that you are using, the value can be either 5.2 or 5.3.

- **Risk Level**

In SAP GRC, each business risk is assigned a criticality level. You can control the risk analysis data returned by SAP GRC by specifying a risk level.

When you specify a risk level, SAP GRC will only check for violations that are at that level or higher levels.

You can specify one of the following risk levels:

- The number 3 stands for Critical. If you specify 3 as the risk level, then only risk violations that are assigned the Critical level will be returned by SAP GRC during the SoD validation process.
- The number 2 stands for High. If you specify 2 as the risk level, then risk violations at both the Critical and High levels will be returned by SAP GRC during the SoD validation process.
- The number 1 stands for Low. If you specify 1 as the risk level, then risk violations at the Critical, High, and Low levels will be returned by SAP GRC during the SoD validation process.
- The number 0 stands for All. If you specify 0 as the risk level, then SAP GRC returns risk violations at all the levels during the SoD validation process.

To specify values for the Risk Level and GRC Version entries in the Lookup.SAP.R3.Configuration lookup definition:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAP.R3.Configuration** lookup definition.

3. Click **Add**.
4. In the Decode column for the Risk Level Code Key, specify 0, 1, 2, or 3 as the value.
5. In the Decode column for the GRC Version Code Key, enter 5.2 or 5.3 as the value depending on the version of SAP GRC that you are using.
6. Click the Save icon.

2.3.3.3 Specifying the System Name in the Lookup.SAP.R3.Systems Lookup Definition

Enter the system name of the SAP ERP installation in the Lookup.SAP.R3.Systems lookup definition as follows:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAP.R3.Systems** lookup definition.
3. Click **Add**.
4. In the Code Key and Decode columns, enter the system name of the SAP ERP installation. You must enter the same value in both columns.
5. Click the Save icon.

2.3.3.4 Specifying a Value for the TopologyName IT Resource Parameter

The TopologyName IT resource parameter holds the name of the combination of the following elements that you want to use for SoD validation of entitlement provisioning operations:

- Oracle Identity Manager installation
- SAP GRC installation
- SAP ERP installation

The value that you specify for the TopologyName parameter must be the same as the value of the topologyName element in the SILConfig.xml file.

See the "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in *Oracle Identity Manager Tools Reference for Release 9.1.0.2* for information about this element.

See [Section 2.3.5, "Configuring the IT Resource"](#) for information about specifying values for parameters of the IT resource.

2.3.3.5 Disabling and Enabling SoD

This section describes the procedures to disable and enable SoD.

To disable SoD:

Note: The SoD feature is disabled by default. Perform the following procedure only if the SoD feature is currently enabled and you want to disable it.

1. Log in to the Design Console.
2. Set the XL.SoDCheckRequired system property to FALSE as follows:
 - a. Expand **Administration**, and double-click **System Configuration**.

- b. Search for and open the `XL.SoDCheckRequired` system property.
- c. Set the value of the system property to `FALSE`.

Note: You need not change the values of the `XL.SIL.Home.Dir` and `Triggers Synchronous SoD checks offline` system properties.

- d. Click the Save icon.
3. Disable the `Holder` and `SODChecker` process tasks as follows:
- a. Expand **Process Management**, and double-click **Process Definition**.
 - b. Search for and open the `SAP R3 Process` process definition.
 - c. On the **Tasks** tab, double-click the **Holder** task.
 - d. On the **Integration** tab of the **Editing Task** dialog box, click **Add**.
 - e. In the **Handler Selection** dialog box:
 - Select **System**.
 - Select the **tcCompleteTask** handler.
 - Click the Save icon, and then close the dialog box.
 - f. In the **Editing Task** dialog box, click the Save icon and close the dialog box.
 - g. On the **Tasks** tab, double-click **SODChecker**.
 - h. On the **Integration** tab of the **Editing Task** dialog box, click **Remove** and then click the save icon.
 - i. Click **Add**.
 - j. In the **Handler Selection** dialog box:
 - Select **System**.
 - Select the **tcCompleteTask** handler.
 - Click the Save icon, and then close the dialog box.
 - k. Click the Save icon in the **Editing Task** dialog box, and then close the dialog box.
 - l. Click the Save icon to save the changes made to the process definition.
4. If you are going to perform the procedure described in [Section 2.3.1.1, "Enabling Request-Based Provisioning"](#), then in the `SAP UM Roles Approval`, `SAP UM Profiles Approval`, and `SAP R3 Process Approval` process definitions, the human approval tasks must be made unconditional as follows:
- On the **Design Console**.
 - Expand **Process Management**, and then double-click **Process Definition**.
 - Search for and open the approval-type process definition for the connector that you are using.
 - On the **Task** tab, search for the **Approval** task.
 - Make this task unconditional by deselecting the **Conditional** check box. See the following screenshot:

- Save the changes to the process definition.

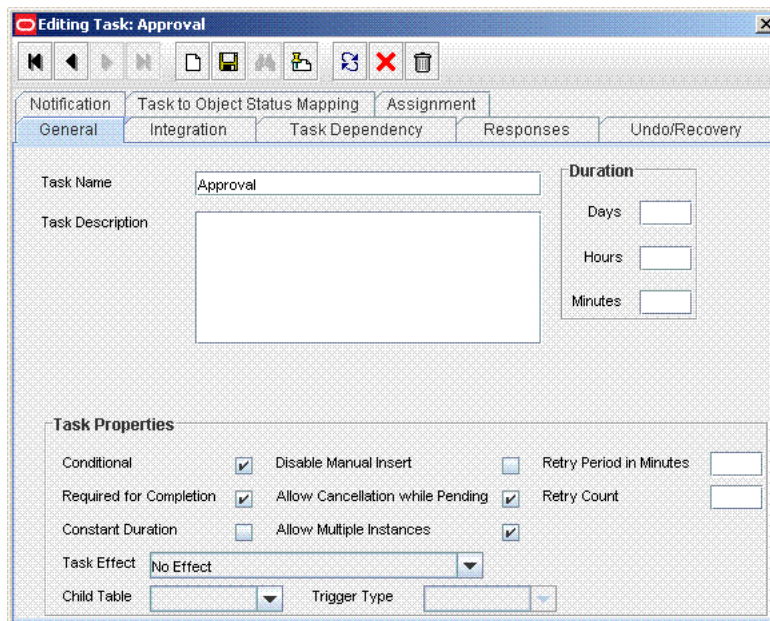
5. Restart Oracle Identity Manager.

To enable SoD:

Note: If you are enabling SoD for the first time, then see *Oracle Identity Manager Readme for Release 9.1.0.2* for detailed information.

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **System Configuration**.
3. Set the XL.SoDCheckRequired system property to TRUE as follows:
 - a. Search for and open the XL.SoDCheckRequired system property.
 - b. Set the value of the system property to TRUE.
 - c. Click the Save icon.
4. Search for and open the XL.SIL.Home.Dir system property.
5. Verify that the value of this system property is set to the full path and name of the *SIL_HOME* directory.
6. Enable the Holder and SODChecker process tasks as follows:
 - a. Expand **Process Management** and double-click **Process Definition**.
 - b. Search for and open the SAP R3 Process process definition.
 - c. On the Tasks tab, double-click the **Holder** task.
 - d. On the Integration tab of the Editing Task dialog box, click **Remove** to remove the tcCompleteTask handler
 - e. Click the Save icon, and then close the dialog box.
 - f. On the Tasks tab, double-click **SODChecker**.
 - g. On the Integration tab of the Editing Task dialog box, click **Add**.

- h. In the Handler Selection dialog box:
 Select **System**.
 Select the **InitiateSODCheck** handler.
 Click the Save icon, and then close the dialog box.
 - i. Click the Save icon in the Editing Task dialog box, and then close the dialog box.
 - j. Click the Save icon to save the changes made to the process definition.
7. If you are going to perform the procedure described in [Section 2.3.1.1, "Enabling Request-Based Provisioning"](#), then in the SAP UM Roles Approval, SAP UM Profiles Approval, and SAP R3 Process process definitions, the human approval tasks must be made conditional as follows:
- On the Design Console.
 - Expand Process Management, and then double-click Process Definition.
 - Search for and open the approval-type process definition for the connector that you are using.
 - On the Task tab, search for Manager Approval task.
 - Make this task conditional by selecting the Conditional check box. See the following screenshot:



- Save the changes to the process definition.
8. Restart Oracle Identity Manager.

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

Oracle Identity Manager uses a Java application server. To connect to the SAP system application server, this Java application server uses the SAP Java connector (JCo). If required, you can use Secure Network Communication (SNC) to secure such connections.

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

This section discusses the following topics:

- [Section 2.3.4.1, "Prerequisites for Configuring the Connector to Use SNC"](#)
- [Section 2.3.4.2, "Installing the Security Package"](#)
- [Section 2.3.4.3, "Configuring SNC"](#)

2.3.4.1 Prerequisites for Configuring the Connector to Use SNC

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

- SNC must be activated on the SAP application server.
- You must be familiar with the SNC infrastructure. You must know which Personal Security Environment (PSE) the application server uses for SNC.

2.3.4.2 Installing the Security Package

To install the security package on the Java application server used by Oracle Identity Manager:

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

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

<http://service.sap.com/download>

This package contains the following files:

- SAP Cryptographic Library (sapcrypto.dll for Microsoft Windows or libsapcrypto.ext for UNIX)
 - A corresponding license ticket (ticket)
 - The configuration tool, sapgenpse.exe
2. Copy the library and the sapgenpse.exe file into a local directory. For example: C:/usr/sap
 3. Check the file permissions. Ensure that the user under which the Java application server runs is able to run the library functions in the directory into which you copy the library and the sapgenpse.exe file.
 4. Create the sec directory inside the directory into which you copy the library and the sapgenpse.exe file.

Note: You can use any names for the directories that you create. However, creating the C:\usr\sap\sec (or /usr/sap/sec) directory is SAP recommendation.

5. Copy the ticket file into the sec directory. This is also the directory in which the Personal Security Environment (PSE) and credentials of the Java application server are generated.

See Also: [Section 2.3.4.3, "Configuring SNC"](#)

6. Set the SECUDIR environment variable for the Java application server user to the sec directory.

Note: From this point onward, the term *SECUDIR directory* is used to refer to the directory whose path is defined in SECUDIR environment variable.

For Oracle Application Server:

- a. Remove the SECUDIR entry from the Windows environment variables, if it has been set.
- b. Edit the `ORACLE_HOME\opmn\config\opmn.xml` file as follows:

Change the following:

```
<ias-instance id="home.BMPHKTF120" name="home.BMPHKTF120">
  <environment>
    <variable id="TMP" value="C:\DOCUME~1\login user\LOCALS~1\Temp"/>
  </environment>
```

To:

```
<ias-instance id="home.BMPHKTF120" name="home.BMPHKTF120">
  <environment>
    <variable id="TMP" value="C:\DOCUME~1\login user\LOCALS~1\Temp"/>
    <variable id="SECUDIR" value="D:\snc\usr\sec"/>
  </environment>
```

Note: Oracle Application Server automatically creates the temporary folder based on the operating system of the computer on which it is installed.

- c. Restart Oracle Application Server.
7. Set the SNC_LIB environment variable for the user of the Java application server to the cryptographic library directory, which is the parent directory of the sec directory.

2.3.4.3 Configuring SNC

To configure SNC:

1. Either create a PSE or copy the SNC PSE of the SAP application server to the SECUDIR directory. To create the SNC PSE for the Java application server, use the `sapgenpse.exe` command-line tool as follows:
 - a. To determine the location of the SECUDIR directory, run the `sapgenpse` command without specifying any command options. The program displays information such as the library version and the location of the SECUDIR directory.
 - b. Enter a command similar to the following to create the PSE:

```
sapgenpse get_pse -p PSE_Name -x PIN Distinguished_Name
```

The following is a sample distinguished name:

```
CN=SAPJ2EE, O=MyCompany, C=US
```

The `sapgenpse` command creates a PSE in the SECUDIR directory.

2. Create credentials for the Java application server.

The Java application server must have active credentials at run time to be able to access its PSE. To check whether or not this condition is met, enter the following command in the parent directory of the SECUDIR directory:

```
seclogin
```

Then, enter the following command to open the PSE of the server and create the `credentials.sapgenpse` file:

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

The `user_ID` that you specify must have administrator rights. `PSE_NAME` is the name of the PSE file.

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

3. Exchange the public key certificates of the two servers as follows:

Note: If you are using individual PSEs for each certificate of the SAP server, then you must perform this procedure once for each SAP server certificate. This means that the number of times you must perform this procedure is equal to the number of PSEs.

a. Export the Oracle Identity Manager certificate by entering the following command:

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

b. Import the Oracle Identity Manager certificate into the SAP application server. You may require the SAP administrator's assistance to perform this step.

c. Export the certificate of the SAP application server. You may require the SAP administrator's assistance to perform this step.

d. Import the SAP application server certificate into Oracle Identity Manager by entering the following command:

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

4. Configure the following parameters in the SAP R3 IT Resource IT resource object:

- SAPsnc_lib
- SAPsnc_mode
- SAPsnc_myname
- SAPsnc_partername
- SAPsnc_qop

2.3.5 Configuring the IT Resource

The SAP UM IT Resource IT resource is automatically created when you run the Connector Installer. You must specify values for the parameters of the IT resource.

Note: The ALL USERS group has INSERT, UPDATE, and DELETE permissions on the default IT resource. This is to ensure that end users can select the IT resource during request-based provisioning. If you create another IT resource, then you must assign INSERT, UPDATE, and DELETE permissions for the ALL USERS group on the IT resource.

To specify values for the parameters of the IT resource:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter SAP UM 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. The following table describes each parameter:

Parameter	Description	Sample Value
Configuration Lookup	Name of the lookup definition containing configuration information	Lookup.SAP.R3.Configuration
CustomizedReconQuery	<p>Query condition on which reconciliation must be based</p> <p>If you specify a query condition as the value of this parameter, then target system records are searched based on the query condition.</p> <p>If you want to reconcile all the target system records, then do not specify a value for this parameter.</p> <p>For more information about this parameter, see Section 3.2.2, "Limited Reconciliation vs. Regular Reconciliation".</p>	firstname=Test&lastname=UMuser
SAPClient	SAP client ID	800
SAPHost	SAP host IP address	172.20.70.204
SAPLanguage	SAP language	EN
SAPUser	<p>User ID of the target system user account that you create for connector operations</p> <p>See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for more information.</p>	oimuser
SAPPassword	<p>Password of the target system user account that you create for connector operations</p> <p>See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for more information.</p>	passw0rd1
SAPSystemNo	System number of the SAP ERP installation	00

Parameter	Description	Sample Value
SAPsnc_lib	Path where the crypto library is placed This is required only if Secure Network Communication (SNC) is enabled.	c:/usr//sap/sapcrypto.dll
SAPsnc_mode	If SNC is enabled on the SAP server, then set this field to 1. Otherwise, set it to 0. Note: It is recommended that you enable SNC to secure communication with the target system.	0
SAPsnc_myname	SNC system name Specify a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Manager.	p:CN=TST,OU=SAP, O=ORA,c=IN
SAPsnc_partnername	Domain name of the SAP server Specify a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Manager.	p:CN=I47,OU=SAP, O=ORA,c=IN
SAPsnc_qop	Specifies the protection level (quality of protection, QOP) at which data is transferred The default value is 3. The value can be any one of the following numbers: <ul style="list-style-type: none"> 1: Secure authentication only 2: Data integrity protection 3: Data privacy protection 8: Use value from the parameter 9: Use maximum value available Specify a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Manager.	3
SAPType	Type of SAP system Note: The default value is R3. Do not change this value.	R3
TimeStamp	For the first reconciliation run, the timestamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of target resource reconciliation was completed is stored in this parameter.	The following are sample timestamp values: English: Jun 01, 2006 at 10:00:00 GMT+05:30 French: juin. 01, 2006 at 10:00:00 GMT+05:30 Japanese: 6 01, 2006 at 10:00:00 GMT+05:30
TopologyName	Value of the Topology Name element in the SIL configuration file See <i>Oracle Identity Manager Tools Reference</i> for more information.	oim1-grc1-sap1
TimeoutRetryCount	Enter the number of times the connector method that is trying to add a role or profile to a user must be retried.	0
TimeoutCount	Enter the delay in milliseconds that the connector method that is trying to add a role or profile to a user must wait after a timeout is encountered.	0

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

Using the Connector

After you deploy the connector, you must first reconcile all existing user data from the target system into Oracle Identity Manager. To achieve this:

1. Configure and run the scheduled task for lookup field synchronization.
2. Run the scheduled task for user reconciliation. Because you are running this scheduled task for the first time, full reconciliation is performed. In other words, all existing user data is fetched from the target system into Oracle Identity Manager.

After you perform these two steps, the integration between Oracle Identity Manager and the target system is ready for provisioning operations and reconciliation runs.

This chapter is divided into the following sections:

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

- [Section 3.1, "Scheduled Task for Lookup Field Synchronization"](#)
- [Section 3.2, "Configuring Reconciliation"](#)
- [Section 3.3, "Configuring Scheduled Tasks"](#)
- [Section 3.4, "Provisioning Operations Performed in an SoD-Enabled Environment"](#)

3.1 Scheduled Task for Lookup Field Synchronization

The SAP R3 LookupRecon scheduled task is used for lookup field synchronization.

Note: The procedure to configure this scheduled task is described later in the guide.

[Table 3-1](#) describes the attributes of this scheduled task. The procedure to configure scheduled tasks is described later in the guide.

Table 3–1 Attributes of the SAP R3 LookupRecon Scheduled Task

Attribute	Description
IT Resource	<p>Enter the name of the IT resource for setting up the connection to the target system.</p> <p>The IT resource name that you specify must be the same as the name that you set while performing the procedure described in the "Configuring the IT Resource" section.</p>
Lookup Mapping	<p>This attribute holds the name of the lookup definition that stores mappings between names of lookup definitions to be synchronized and the corresponding BAPI details.</p> <p>Value: <code>Lookup.SAP.R3.LookupMappings</code></p> <p>Note: You must not change the default value of this attribute. See Table 1–2 for information about this lookup definition.</p>

3.2 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:

- [Limited Reconciliation vs. Regular Reconciliation](#)
- [Batched Reconciliation](#)
- [Reconciliation Scheduled Task](#)

3.2.1 Full Reconciliation vs. Incremental Reconciliation

The TimeStamp IT resource parameter stores the time stamp at which a reconciliation run begins. During a reconciliation run, the scheduled task fetches only target system records that are added or modified after the time stamp stored in the parameter for target resource reconciliation. This is incremental reconciliation. If you set the parameter to 0, then full reconciliation is performed. In full reconciliation, all existing target system records are fetched into Oracle Identity Manager for reconciliation.

As mentioned earlier in this chapter, you can switch from incremental to full reconciliation at any time.

3.2.2 Limited Reconciliation vs. Regular 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 Task Scheduler parameter while configuring the IT resource.

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

Oracle Identity Manager Attribute	SAP User Management Attribute
User ID	userid

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

The following are sample query conditions:

- `firstname=John&lastname=Doe`

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

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

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

- The user's first name is John or last name is Doe.
- The user belongs to the `contractors` user group.

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

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

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

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

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

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

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

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

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

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

You specify a value for the `CustomizedReconQuery` parameter while configuring the IT resource.

3.2.3 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 such problems.

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

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

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

You specify values for these attributes by following the instructions described in the ["Configuring Scheduled Tasks"](#) section.

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

3.2.4 Reconciliation Scheduled Task

You must specify values for the following attributes of the R3 Recon scheduled task.

Note:

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

Attribute	Description	Sample Value
OIMServerTimeZone	Time zone of the Oracle Identity Manager host computer	GMT
Exclude changes by SAPUser	Enter yes if you want to exclude changes made by the SAPUser directly on the target system. Otherwise, enter no.	no
Organization	Default organization assigned to a new user	Xellerate Users
Role	Default role assigned to a new user	Consultant
Xellerate Type	Default type assigned to a new user	End-User Administrator
ITResource	Name of the IT resource for setting up a connection to the SAP User Management server	SAP R3 IT Resource
ResourceObject	Name of the target system resource object into which users need to be reconciled	SAP R3 Resource Object
IsTrusted	Do not modify the value of this parameter. It will be removed in a future release.	false
Server	SAP server type The value is R3 . Note: Do not change the default value.	R3
StartRecord	Start record for batched reconciliation This attribute is also discussed in the " Batched Reconciliation " section on page 3-4.	1
BatchSize	Number of records that must be there in a batch This attribute is also discussed in the " Batched Reconciliation " section on page 3-4.	3
NumberOfBatches	Number of batches that must be reconciled This attribute is also discussed in the " Batched Reconciliation " section on page 3-4.	Default value: All Available (for reconciling all users) Sample value: 50

3.3 Configuring Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

[Table 3–2](#) lists the scheduled tasks that you must configure.

Table 3–2 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
SAP R3 LookupRecon	This scheduled task is used for lookup field synchronization.
R3 Recon	This scheduled task is used for user data reconciliation.

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage Scheduled Task**.
4. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.
5. In the search results table, click the edit icon in the Edit column for the scheduled task.
6. On the Edit Scheduled Task Details page, you can modify the following details of the scheduled task by clicking **Edit**:
 - **Status:** Specify whether or not 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.
7. After modifying the values for the scheduled task details listed in the previous step, click **Continue**.
8. Specify values for the attributes of the scheduled task. To do so, select each attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for the 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.
-

The attributes of the scheduled task that you select for modification are displayed on this page.

9. Click **Save Changes** to commit all the changes to the database.

Note: If you want to stop a scheduled task while it is running, then use the Stop Execution feature of the Design Console. See the "The Task Scheduler Form" section in *Oracle Identity Manager Design Console Guide* for information about this feature.

3.4 Provisioning Operations Performed in an SoD-Enabled Environment

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a SAP ERP account for the user. The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning of accounts
- Request-based provisioning of entitlements
- 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 3.4.1, "Overview of the Provisioning Process in an SoD-Enabled Environment"](#)
- [Section 3.4.2, "Direct Provisioning in an SoD-Enabled Environment"](#)
- [Section 3.4.3, "Request-Based Provisioning in an SoD-Enabled Environment"](#)

3.4.1 Overview of the Provisioning Process in an SoD-Enabled Environment

The following is the sequence of steps that take places during a provisioning operation performed in an SoD-enabled environment:

1. The provisioning operation triggers the appropriate adapter.
2. The user runs the scheduled task (either ResubmitUninitiatedProvisioningSODCheck or Resubmit Uninitiated Approval SOD Checks).
3. The scheduled task passes the entitlement data to the Web service of SAP GRC.
4. After SAP GRC runs the SoD validation process on the entitlement data, the response from the process is returned to Oracle Identity Manager.
5. The status of the process task that received the response depends on the response itself. If the entitlement data clears the SoD validation process, then the adapter carries provisioning data to the corresponding BAPI on the target system and the status of the process task changes to Completed. This translates into the entitlement being granted to the user. If the SoD validation process returns the failure response, then status of the process task changes to Canceled.

3.4.2 Direct Provisioning in an SoD-Enabled Environment

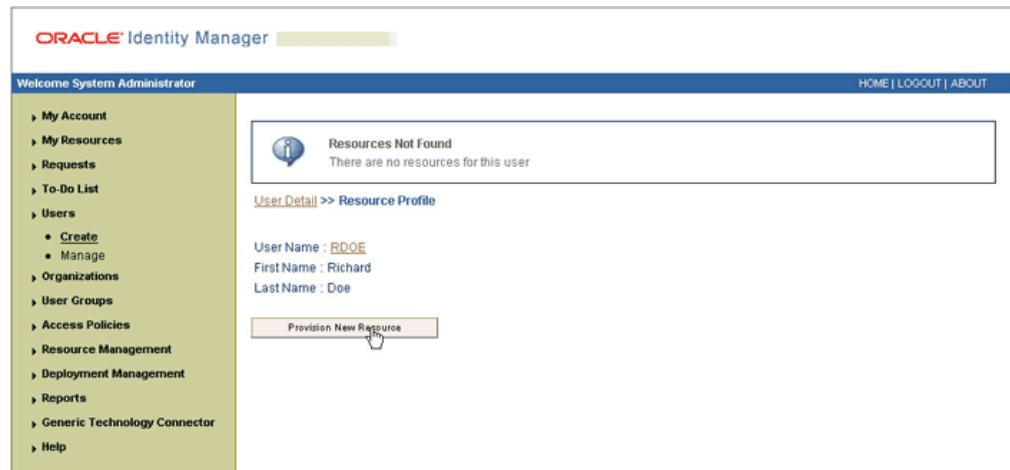
To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.

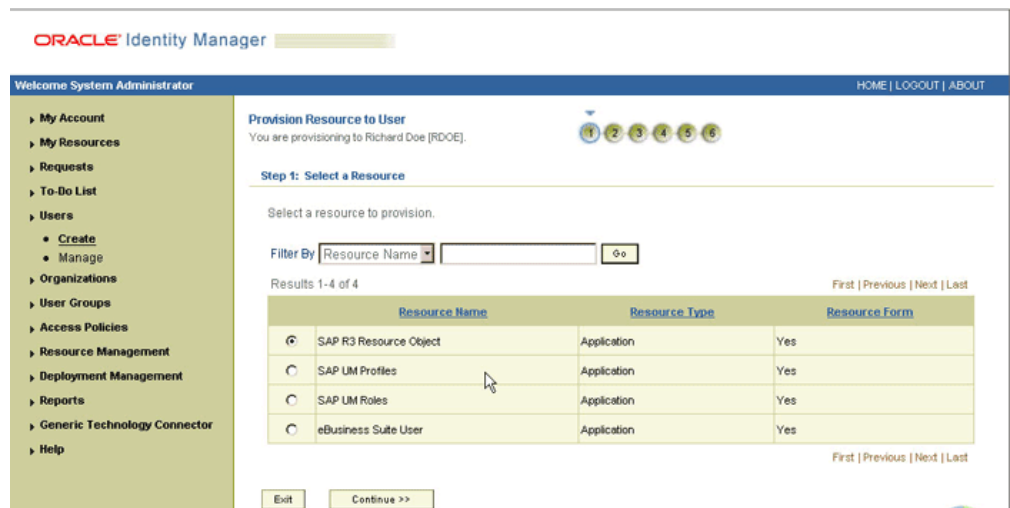
- From the Users menu, select **Manage** if you want to provision a target system account to an existing OIM User.
- If you select Create, on the Create User page, enter values for the OIM User fields and then click **Create User**. The following screenshot shows the Create User page.

- If you select Manage, then search for the OIM User and select the link for the user from the list of users displayed in the search results.
- On the User Detail page, select **Resource Profile** from the list at the top of the page. The following screenshot shows the User Detail page.

- On the Resource Profile page, click **Provision New Resource**. The following screenshot shows the Resource Profile page.



7. On the Step 1: Select a Resource page, select **SAP R3 Resource Object** from the list and then click **Continue**. The following screenshot shows the Step 1: Select a Resource page.



8. On the Step 2: Verify Resource Selection page, click **Continue**. The following screenshot shows the Step 2: Verify Resource Selection page.



9. On the Step 5: Provide Process Data page for process data, enter the details of the account that you want to create on the target system and then click **Continue**. The following screenshot shows the user details added.

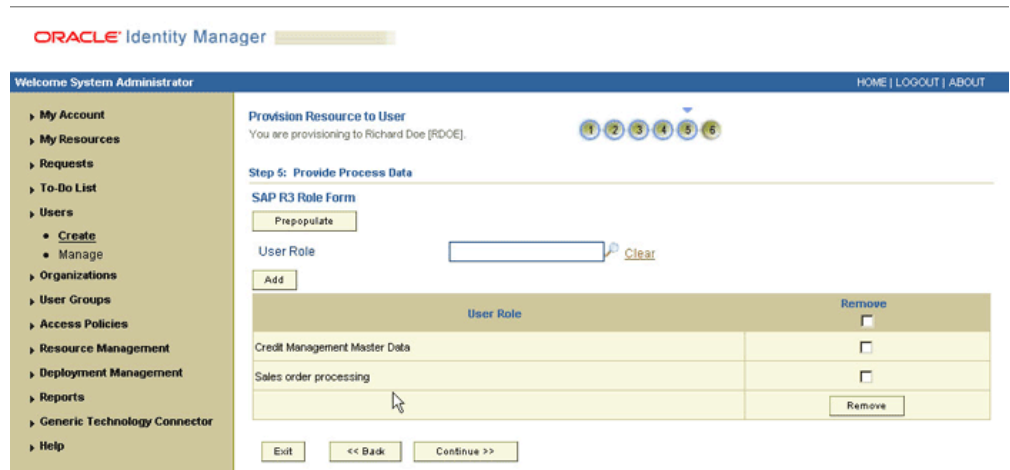
The screenshot shows the Oracle Identity Manager interface. The left sidebar contains navigation links: My Account, My Resources, Requests, To-Do List, Users (with sub-links Create and Manage), Organizations, User Groups, Access Policies, Resource Management, Deployment Management, Reports, Generic Technology Connector, and Help. The main content area is titled 'Provision Resource to User' and 'Step 5: Provide Process Data'. It shows a progress bar with steps 1 through 5, where step 5 is active. The user being provisioned is Richard Doe [RDOE]. The 'SAP R3' section has a 'Prepopulate' button. A list of fields with their values is shown:

Field	Value	Required	Action
User Id	RDOE	*	
Password	*****		
IT Resource Type	SAP R3 IT Resource	*	Clear
First Name	Richard		Clear
Last Name	Doe	*	
User Group			Clear
Department			Clear
Lang Comm			Clear
Lang Logon			Clear
Time Zone			Clear
Telephone			

10. On the Step 5: Provide Process Data page for profile data, search for and select profiles for the user on the target system and then click **Continue**. The following screenshot shows this page.

The screenshot shows the same Oracle Identity Manager interface as the previous screenshot, but at the 'SAP R3 Profile Form' section. It includes a 'Prepopulate' button, a 'User Profile' search field with a 'Clear' button, an 'Add' button, and navigation buttons: 'Exit', '<< Back', and 'Continue >>'.

11. On the Step 5: Provide Process Data page for role data, search for and select roles for the user on the target system and then click **Continue**. The following screenshot shows this page.



ORACLE Identity Manager

Welcome System Administrator

HOME | LOGOUT | ABOUT

My Account
My Resources
Requests
To-Do List
Users
 • Create
 • Manage
Organizations
User Groups
Access Policies
Resource Management
Deployment Management
Reports
Generic Technology Connector
Help

Provision Resource to User
You are provisioning to Richard Doe [RDOE].

Step 5: Provide Process Data

SAP R3 Role Form

Prepopulate

User Role Clear

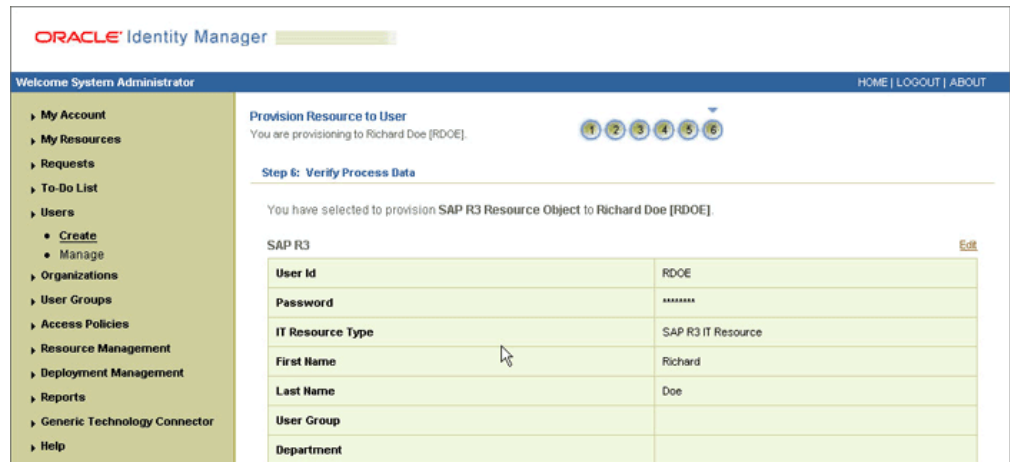
Add

User Role	Remove
Credit Management Master Data	<input type="checkbox"/>
Sales order processing	<input type="checkbox"/>

Remove

Exit << Back Continue >>

12. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**. The following screenshot shows Step 6: Verify Process Data page.



ORACLE Identity Manager

Welcome System Administrator

HOME | LOGOUT | ABOUT

My Account
My Resources
Requests
To-Do List
Users
 • Create
 • Manage
Organizations
User Groups
Access Policies
Resource Management
Deployment Management
Reports
Generic Technology Connector
Help

Provision Resource to User
You are provisioning to Richard Doe [RDOE].

Step 6: Verify Process Data

You have selected to provision SAP R3 Resource Object to Richard Doe [RDOE].

SAP R3 Edit

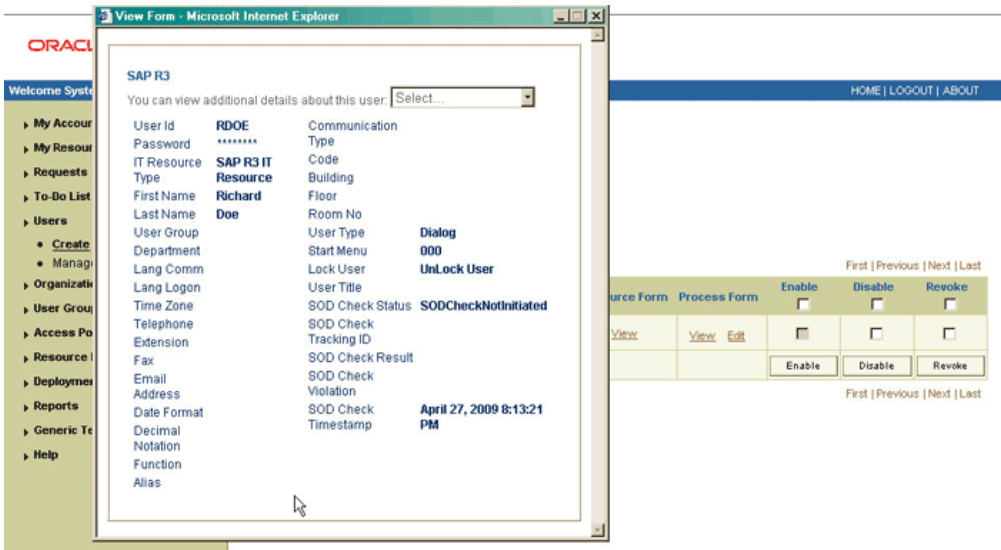
User Id	RDOE
Password	*****
IT Resource Type	SAP R3 IT Resource
First Name	Richard
Last Name	Doe
User Group	
Department	

13. The "Provisioning has been initiated" message is displayed. Click **Back to User Resource Profile**. The Resource Profile page shows that the resource has been provisioned to the user.

The following screenshot shows this page:



14. If you click the View link in the Process Form column, then the process form is displayed. The following screenshot shows this page:



In this screenshot, the SOD Check Status field shows SODCheckNotInitiated. The value in this field can be SoDCheckNotInitiated, SoDCheckResultPending, or SoDCheckCompleted.

15. If you click the resource, then the Resource Provisioning Details page is displayed. The following screenshot shows this page:

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

[User Detail](#) >> [Resource Profile](#) >> [Resource Provisioning Details](#)

The following are the provisioning tasks for the resource. You can also enable, disable, or revoke this resource from the user.

SAP R3 Resource Object provisioning details for **Richard Doe[RDOE]**

Results 1-6 of 6 First | Previous | Next | Last

Task Name	Task Status	Date Assigned	Assigned To	Retry
System Validation	Completed	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Create User	Completed	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Holder	Pending	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
SODChecker	Pending	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Add User Role	Waiting	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Add User Role	Waiting	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>

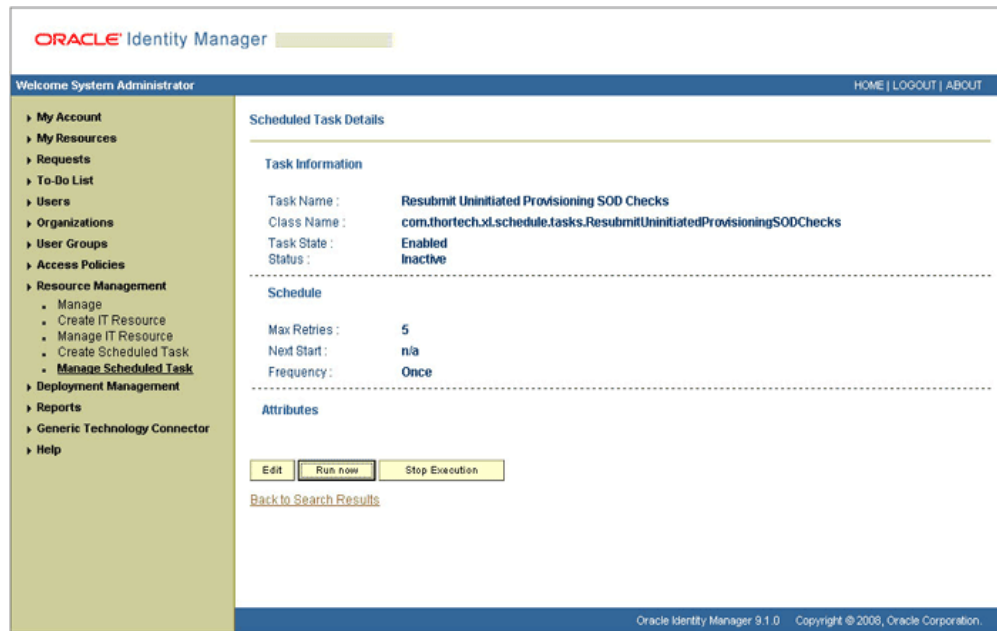
First | Previous | Next | Last

This page shows the details of the process tasks that were run. The Holder and SODChecker tasks are in the Pending state. These tasks will change state after the status of the SoD check is returned from the SoD engine. The Add User Role tasks correspond to the two roles selected for assignment to this user.

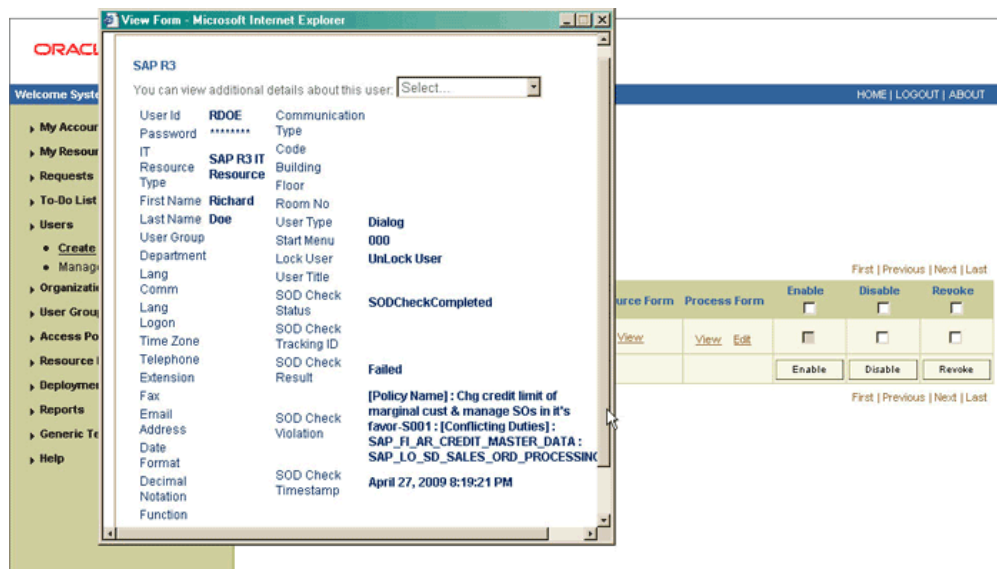
- The SODCheckNotInitiated status in the SOD Check Status field indicates that SoD validation has not started. To start SoD validation, you must run the ResubmitUninitiatedProvisioningSODChecks scheduled task.

Note: SoD validation by SAP GRC is synchronous. The validation process returns a result as soon as it is completed. However, if the requested entitlement throws a large number of violations in policies defined on SAP GRC, then the process might take a long time to complete. If that happens, then Oracle Identity Manager might time out. The ResubmitUninitiatedProvisioningSODChecks scheduled task has been introduced to circumvent this issue.

The following screenshot shows the ResubmitUninitiatedProvisioningSODChecks scheduled task in the Design Console:



17. After the ResubmitUninitiatedProvisioningSODChecks scheduled task is run, the results of the SoD validation process are brought to Oracle Identity Manager. If you click the View link in the Process Form column, then the process form is displayed. The following screenshot shows this page:



In this screenshot, the SOD Check Status field shows SoDCheckCompleted. Because a violation by the SoD engine in this particular example, the SoD Check Violation field shows the details of the violation.

In addition, the Resource Provisioning Details page shows the status of the SODChecker and Holder tasks as Completed.

The following screenshot shows this page:

ORACLE Identity Manager

Welcome System Administrator

HOME | LOGOUT | ABOUT

User Detail >> Resource Profile >> Resource Provisioning Details

The following are the provisioning tasks for the resource. You can also enable, disable, or revoke this resource from the user.

SAP R3 Resource Object provisioning details for Richard Doe[RDOE]

Results 1-6 of 6

Task Name	Task Status	Date Assigned	Assigned To	Retry
System Validation	Completed	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Create User	Completed	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
SODChecker	Completed	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Holder	Canceled	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Add User Role	Canceled	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Add User Role	Canceled	April 27, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>

Enable Disable Revoke Add Task

In this screenshot, the status of the Add User Role tasks is Canceled because the request failed the SoD validation process.

18. As the administrator assigning a resource to a user, you can either end the process when a violation is detected or modify the assignment data and then resend it. To modify the assignment data, first click the **Edit** link in the Process Form column on the Resource Profile page.
19. In the Edit Form window that is displayed, you can modify the role and profile data that you had selected earlier.

Note: To modify a set of entitlements In the Edit Form window, you must first remove all entitlements and then add the ones that you want to use.

In the following screenshot, one of the roles selected earlier is marked for removal:

ORACLE Identity Manager

Welcome System Administrator

HOME | LOGOUT | ABOUT

SAP R3 Role Form

User Role [Clear](#)

[Add](#)

Results 1-2 of 2

User Role	Update	Remove
Credit Management Master Data	<input type="checkbox"/>	<input type="checkbox"/>
Sales order processing	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Update Remove

First | Previous | Next | Last

20. Rerun the ResubmitUninitiatedProvisioningSODChecks scheduled task to initiate the SoD validation process.

- [illegible]

In addition, the Resource Provisioning Details page shows the status of the SODChecker and Holder tasks as Completed.

ORACLE Identity Manager

Welcome System Administrator

- > My Account
- > My Resources
- > Requests
- > To-Do List
- > Users
 - > Create
 - > Manage
- > Organizations
- > User Groups
- > Access Policies
- > Resource Management
- > Deployment Management
- > Reports
- > Generic Technology Connector
- > Help

[User Detail](#) >> [Resource Profile](#) >> [Resource Provisioning Details](#)

The following are the provisioning tasks for the resource. You can also enable, disable, or revoke this resource from the user.

SAP R3 Resource Object provisioning details for Richard Doe[RDOE]

Results 1-6 of 6

Task Name	Task Status	Date Assigned	Assigned To	Retry
System Validation	Completed	Apr 27, 2009	System Administrator [XELSYSADM]	
Create User	Completed	Apr 27, 2009	System Administrator [XELSYSADM]	
SOQChecker	Completed	Apr 27, 2009	System Administrator [XELSYSADM]	
Holder	Canceled	Apr 27, 2009	System Administrator [XELSYSADM]	
Add User Role	Canceled	Apr 27, 2009	System Administrator [XELSYSADM]	
Add User Role	Canceled	Apr 27, 2009	System Administrator [XELSYSADM]	

[First](#) | [Previous](#) | [Next](#) | [Last](#)

3.4.3 Request-Based Provisioning in an SoD-Enabled Environment

See Also: [Section 2.3.3, "Configuring SoD"](#)

The request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The request-based provisioning process described in this section covers steps to be performed by both entities.

In the example used in this section, the end user creates a request for two roles on the target system. The request clears the SoD validation process and is approved by the approver.

End-User's Role in Request-Based Provisioning

The following are types of request-based provisioning:

Request-based provisioning of accounts: OIM Users are created but not provisioned target system resources when they are created. Instead, the users themselves raise requests for provisioning accounts.

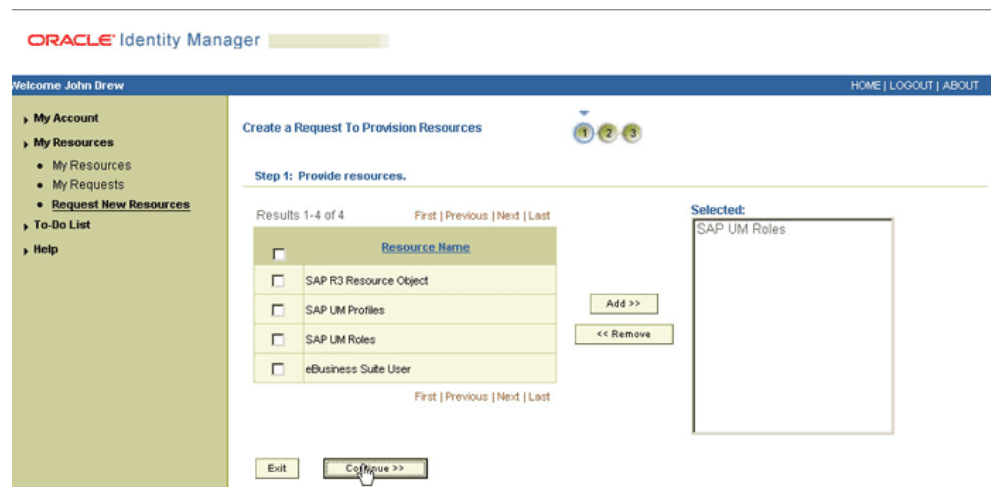
Request-based provisioning of entitlements: OIM Users who have been provisioned target system resources (either through direct or request-based provisioning) raise requests for provisioning entitlements.

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

Note: The procedure is almost the same for request-based provisioning of both accounts and entitlements. Differences have been called out in the following sequence of steps.

1. Log in to the Administrative and User Console.
2. Expand My Resources, and then click Request New Resources.
3. On the Step 1: Provide resources page, use the Add button to select one of the following:
 - SAP R3 Resource Object, if you want to create a request for a target system account
 - SAP UM Roles or SAP UM Profiles, if you want to create a request for an entitlement on the target system

The following screenshot shows the SAP UM Roles entitlement selected:



4. On the Step 2: Provide resource data page, click Continue.

The following screenshot shows this page:

The screenshot shows the Oracle Identity Manager interface. The left sidebar contains a navigation menu with 'My Account', 'My Resources' (expanded), 'My Requests', 'Request New Resources', 'To-Do List', and 'Help'. The main content area is titled 'Create a Request To Provision Resources' and shows 'Step 2: Provide resource data.' with a progress indicator (1, 2, 3). Below the title, it states: 'The subsequent screens will guide you through providing data about SAP UM Roles for the following users: :'. A list of users is shown: 'John Drew [JDREW]'. At the bottom, there are three buttons: 'Exit', '<< Back', and 'Continue >>'. A mouse cursor is pointing at the 'Continue >>' button.

5. On the second Step 2: Provide resource data page, select the IT resource corresponding to the target system installation on which you want the selected entitlement.

The following screenshot shows this page:

The screenshot shows the Oracle Identity Manager interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Create a Request To Provision Resources' and shows 'Step 2: Provide resource data.' with a progress indicator (1, 2, 3). Below the title, it states: 'Provide the following SAP UM Roles >> UD_SPUMRP_O details for John Drew [JDREW]:'. A red asterisk indicates a required field. The form has several input fields: 'Server' (with a dropdown menu showing 'SAP R3 IT Resource' and a 'Clear' button), 'SOD Check Status' (with a dropdown menu showing 'SODCheckNotInitiated'), 'SOD Check Tracking ID', 'SOD Check Result', 'SOD Check Violation', and 'SOD Check Timestamp'. At the bottom, there are three buttons: 'Exit', '<< Back', and 'Continue >>'.

6. On the third Step 2: Provide resource data page, select the entitlements that you want to request.

The following screenshot shows two roles selected on this page:

ORACLE Identity Manager

Welcome John Drew

My Account
My Resources
My Resources
My Requests
Request New Resources
To-Do List
Help

Create a Request To Provision Resources

Step 2: Provide resource data.

Provide the following SAP UM Roles >> UD_SPUMRC_O detail for John Drew [JDREW] and click the Add button to create a new entry.

User Role [Clear](#)

The following are the existing SAP UM Roles >> UD_SPUMRC_O entries for John Drew [JDREW]. You can select specific entries to remove.

User Role	Remove
Credit Management Master Data	<input type="checkbox"/>
Sales order processing	<input type="checkbox"/>

7. On the Step 3: Verify information page, review the information that you have provided and then submit the request.

The following screenshot shows this page:

ORACLE Identity Manager

Welcome John Drew

HOME | LOGOUT | ABOUT

Create a Request To Provision Resources

Step 3: Verify information.

Users Selected

User ID	First Name	Last Name
JDREW	John	Drew

Resources Selected [Change](#)

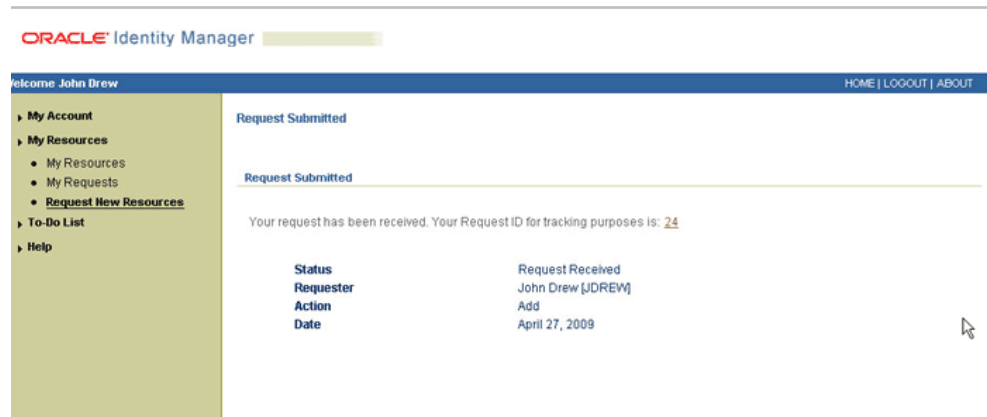
Resource Name	Details
SAP UM Roles	Edit

Comments

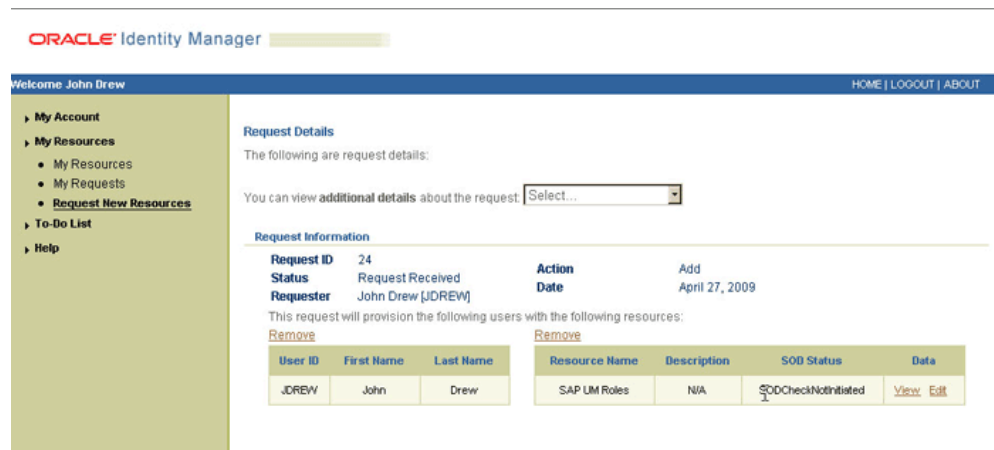
No comments have been added to this request. [Click here to add a comment.](#)

8. If you click Submit Now, then the Request Submitted page shows the request ID.

The following screenshot shows this page:



9. If you click the request ID, then the Request Details page is displayed. The following screenshot shows this page:



The SOD Status field shows SODCheckNotInitiated. The value in this field can be SoDCheckNotInitiated, SoDCheckResultPending, or SoDCheckCompleted.

10. To view details of the approval, select Approval Tasks from the list at the top of the page. The Approval Tasks page is displayed. The following screenshot shows this page:

The screenshot shows the Oracle Identity Manager interface. The left sidebar contains navigation links: My Account, My Resources (My Resources, My Requests, Request New Resources), To-Do List, and Help. The main content area is titled 'Request Details >> Approval Tasks'. It states: 'This is a list of all approvals (processed and pending) related to this request.' Below this, the 'Request ID' is 24. The 'Request Approval Tasks' section contains a table:

Task	Status	Assigned To	Action
Approve	Completed	System Administrator [XELSYSADM]	Approve Deny Reassign

The 'Resource Approval Tasks' section contains a table for 'SAP UIM Roles':

Task	Status	Assigned To	Action
SODChecker	Pending	System Administrator [XELSYSADM]	Approve Deny Reassign

On this page, the status of the SODChecker task is Pending.

11. To initiate SoD validation of pending entitlement requests, an administrator must run the Resubmit Uninitiated Approval SOD Checks scheduled task. The following screenshots shows this scheduled task in the Design Console:

The screenshot shows the 'Scheduled Task Details' page in Oracle Identity Manager. The left sidebar contains navigation links: My Account, My Resources, Requests, To-Do List, Users, Organizations, User Groups, Access Policies, Resource Management (Manage, Create IT Resource, Manage IT Resource, Create Scheduled Task, Manage Scheduled Task), Deployment Management, Reports, Generic Technology Connector, Attestation, and Help. The main content area is titled 'Scheduled Task Details' and contains the following information:

Task Information

Task Name : Resubmit Uninitiated Approval SOD Checks
 Class Name : com.thortech.xl.schedule.tasks.ResubmitUninitiatedApprovalSODChecks
 Task State : Enabled
 Status : Inactive

Schedule

Max Retries : 5
 Next Start : n/a
 Frequency : Once

Attributes

Buttons: Edit, Run now, Stop Execution

[Back to Search Results](#)

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

12. After the Resubmit Uninitiated Approval SOD Checks scheduled task is run, on the Approvals Task page, the status of the SODChecker task is Completed and the Approval task status is Pending. This page also shows details of the administrator who must now approve the request.

The following screenshot shows the Approvals Task page after the request passes the SoD validation process.

ORACLE Identity Manager

Welcome John Drew [HOME](#) | [LOGOUT](#) | [ABOUT](#)

My Account
My Resources
My Requests
Request New Resources
To-Do List
Help

[Request Details >> Approval Tasks](#)
Approval Tasks
This is a list of all approvals (processed and pending) related to this request.

Request ID [24](#)

Request Approval Tasks

Task	Status	Assigned To	Action
Approve	Completed	System Administrator [XELSYSADM]	<input type="checkbox"/>
			Approve Deny Reassign

Resource Approval Tasks

SAP UM Roles

Task	Status	Assigned To	Action
SODChecker	Completed	System Administrator [XELSYSADM]	<input type="checkbox"/>
Approval	Pending	System Administrator [XELSYSADM]	<input type="checkbox"/>
			Approve Deny Reassign

Approver's Role in Request-Based Provisioning

This section discusses the role of the approver in a request-based provisioning operation.

The approver to whom the request is assigned can use the Pending Approvals feature to view details of the request.

ORACLE Identity Manager

Welcome System Administrator [HOME](#) | [LOGOUT](#) | [ABOUT](#)

My Account
My Resources
Requests
To-Do List
Pending Approvals
Open Tasks
Users
Organizations
User Groups
Access Policies
Resource Management
Deployment Management
Reports
Generic Technology Connector
Help

Request Details
The following are request details:

You can view additional details about the request: [Select...](#)

Request Information

Request ID	24	Action	Add
Status	Approved	Date	April 27, 2009
Requester	John Drew [JDREW]		

This request will provision the following users with the following resources:

User ID	First Name	Last Name	Resource Name	Description	SOD Status	Data
JDREW	John	Drew	SAP UM Roles	N/A	SODCheckCompleted	View Edit

Pending Resource Approval Tasks

[Request More Information](#)

Task	Assigned To	Status	Resource Name	Approve/Deny
Approval	System Administrator [XELSYSADM]	Pending	SAP UM Roles	<input type="checkbox"/>
				Approve Deny Reassign

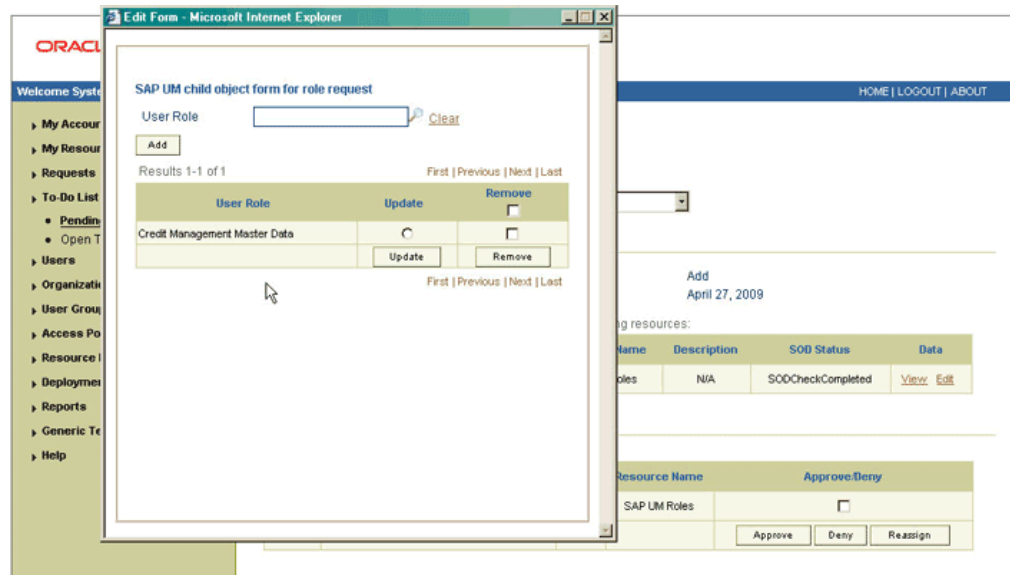
In addition, the approver can click the View link to view details of the SoD validation process.

The approver can decide whether to approve or deny the request, regardless of whether the SoD engine accepted or rejected the request. The approver can also modify entitlements in the request.

The following are steps that the approver can perform:

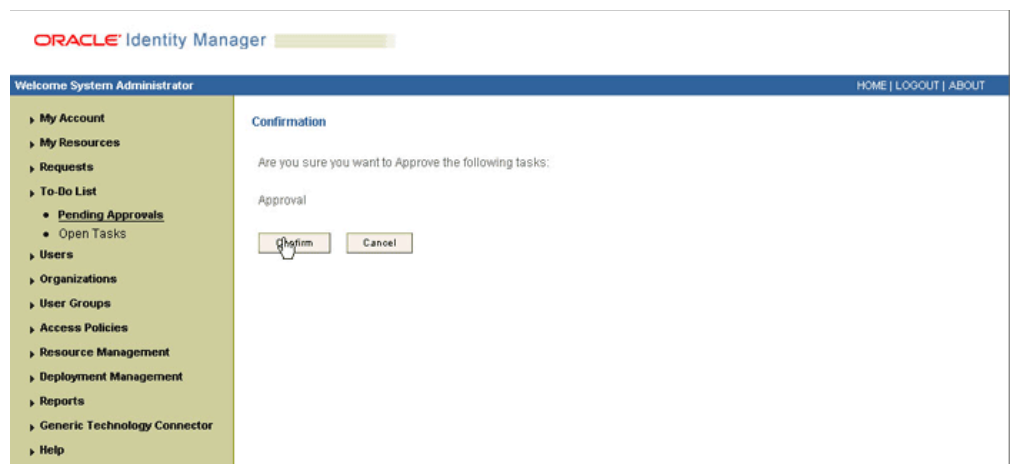
1. As the approver, to edit and approve a request, click the Edit link.
2. In the Edit Form window, select the entitlement request data that you want to modify from the list at the top of the window and then make the required change.

In the following screenshot, one of the roles that the requester had included in the request has been removed:



3. Close the Edit Form window, select the check box for the task that you want to approve, and then click Approve.
4. On the Confirmation page, click Confirm.

The following screenshot shows this page:



5. On the Request Details page, the SOD Status column shows SODCheckCompleted.

If you search for and open the requester's profile, the entitlements granted to the user are shown in the Provisioned state. This is shown in the following screenshot:

ORACLE Identity Manager

Welcome System Administrator

HOME | LOGOUT | ABOUT

My Account

My Resources

Requests

To-Do List

Users

Create

Manage

Organizations

User Groups

Access Policies

Resource Management

Deployment Management

Reports

Generic Technology Connector

Help

User Detail >> Resource Profile

User Name : [JOREW](#)
First Name : John
Last Name : Drew

Results 1-2 of 2

First | Previous | Next | Last

Resource Name	Status	Description	Request ID	Resource Form	Process Form	Enable	Disable	Revoke
SAP UM Roles	Provisioned	132		View	View Edit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SAP R3 Resource Object	Provisioned	129		View	View Edit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
						Enable	Disable	Revoke

First | Previous | Next | Last

Provision New Resource

Extending the Functionality of the Connector

This chapter discusses the following optional procedure:

- See [Section 4.1, "Modifying Field Lengths on the Process Form"](#) if you want to modify lengths of fields on the process form.
- The [Section 4.2, "Configuring the Connector for Multiple Trusted Source Reconciliation"](#) describes the procedure for using the target system as one of the trusted sources of identity data in your organization.

4.1 Modifying Field Lengths on the Process Form

You might want to modify the lengths of fields (attributes) on the process form. For example, if you use the Japanese locale, then you might want to increase the lengths of process form fields to accommodate multibyte data from the target system.

Note: On mySAP ERP 2005 (ECC 6.0 running on WAS 7.0), the default length of the password field is 40 characters. The default length of the password field on the process form is 8 characters. If you are using mySAP ERP 2005, then you must increase the length of the password field on the process form.

If you want to modify the length of a field on the process form, then:

1. Log in to the Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_SAPR3** process form.
4. Click **Create New Version**.
5. Enter a label for the new version, click the Save icon, and then close the dialog box.
6. From the **Current Version** list, select the version that you create.
7. Modify the length of the required field.
8. Click the Save icon.
9. Click **Make Version Active**.

4.2 Configuring the Connector for Multiple Trusted Source Reconciliation

The following are examples of scenarios in which there is more than one trusted source for user data in an organization:

- One of the target systems is a trusted source for data about employees. The second target system is a trusted source for data about contractors. The third target system is a trusted source for data about interns.
- One target system holds the data of some of the identity fields that constitute an OIM User. Two other systems hold data for the remaining identity fields. In other words, to create an OIM User, data from all three systems would need to be reconciled.

If the operating environment of your organization is similar to that described in either one of these scenarios, then this connector enables you to use the target system as one of the trusted sources of user data in your organization.

See *Oracle Identity Manager Design Console Guide* for detailed information about multiple trusted source reconciliation.

Testing and Troubleshooting

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

- [Section 5.1, "Testing Provisioning"](#)
- [Section 5.2, "Testing Partial Reconciliation"](#)
- [Section 5.3, "Testing Batched Reconciliation"](#)

5.1 Testing Provisioning

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

To use the testing utility:

1. Copy the contents of the test directory from the installation media to the *OIM_HOME/xellerate/SAP/test* directory.
2. Specify the required values in the *global.properties* file.

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

Section	Information
SAP User Management connection parameters	Connection parameters required to connect to the target system These parameters are the same as the parameters of the IT resource.
User information	Field information required to create, modify, and delete a user profile
Reconciliation information	The From Date timestamp The To Date is set to the current date and time by default.

3. Add the following to the CLASSPATH environment variable:

OIM_HOME/xellerate/ext/log4j-1.2.8.jar

OIM_HOME/Xellerate/JavaTasks/SAPUserMgmt.jar

OIM_HOME/Xellerate/ScheduleTask/SAPCommon.jar

OIM_HOME/xellerate/lib/xlLogger.jar

OIM_HOME/xellerate/lib/xlUtils.jar

OIM_HOME/xellerate/lib/xlAPI.jar

OIM_HOME/xellerate/ThirdParty/sapjco.jar

OIM_HOME/xellerate/ThirdParty/sapidoc3.jar

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

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

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

OIM_HOME/Xellerate/sap/test/config

- 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.

5. Perform the following tests:

- Enter the following command to create a user:

```
java
-DTproperties=OIM_HOME/Xellerate/SAP/test/config/troubleshoot.properties
-Dlog4j.configuration=file:/OIM_HOME/Xellerate/SAP/test/config/log.properties
TroubleShootingUtility C
```

- Enter the following command to modify a user:

```
java
-DTproperties=OIM_HOME/Xellerate/SAP/test/config/troubleshoot.properties
-Dlog4j.configuration=file:/OIM_HOME/Xellerate/SAP/test/config/log.properties
TroubleShootingUtility M
```

- Delete a user as follows:

```
java
-DTproperties=OIM_HOME/Xellerate/SAP/test/config/troubleshoot.properties
-Dlog4j.configuration=file:/OIM_HOME/Xellerate/SAP/test/config/log.properties
TroubleShootingUtility D
```

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

```
java
-DTproperties=OIM_HOME/Xellerate/SAP/test/config/troubleshoot.properties
-Dlog4j.configuration=file:/OIM_HOME/Xellerate/SAP/test/config/log.properties
TroubleShootingUtility R
```

5.2 Testing Partial Reconciliation

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

- Simple queries with user attributes

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

The users with first name John are reconciled.

- Queries with '&' and '|' logical operators
 - Value assigned to the CustomizedReconQuery parameter:
`firstname=John&lastname=Doe`
The users with first name John and last name Doe are reconciled.
 - Value assigned to the CustomizedReconQuery parameter:
`firstname=John&userrole=ASAP_AUTORENUMGEBUNG`
Only the users with first name John and who belong to the ASAP_AUTORENUMGEBUNG role are reconciled.

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

- Queries with time stamps
 - Value assigned to the CustomizedReconQuery parameter: `None`
Value of the TimeStamp parameter: `Nov 3, 2006 at 10:00:00 GMT+05:30`
The users that matches the time stamp value are reconciled.
 - Value assigned to the CustomizedReconQuery parameter: `firstname=John`
Value of the TimeStamp parameter: `Nov 3, 2006 at 10:00:00 GMT+05:30`
The users with first name John and who matches the time stamp value are reconciled.

5.3 Testing Batched Reconciliation

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

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

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

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

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

Known Issues

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

- **Bug 7255088**

Suppose a user is created in SAP ERP and then locked. When this user is reconciled for the first time, the user may not get locked because linking in Oracle Identity Manager takes place in an asynchronous manner. This user is successfully locked during the next reconciliation run.

- **Bug 7255110**

Suppose a user is deleted from SAP ERP. During reconciliation, the user is deleted from Oracle Identity Manager. However, the Delete User function is also run and a message saying that the user does not exist on the target system is displayed. This message can be ignored.

- **Bug 7516300**

On SAP ERP, you can create a lookup field entry with only the description (Decode) value and without a code (Code Key) value. After lookup field synchronization, the Code Key and Decode columns both contain the description (Decode) value.

- **Bug 7689555**

An empty (NULL) Code Key value is not fetched during lookup field synchronization.

- **Bug 7207232**

Some Asian languages use multibyte character sets. If the character limit for fields on the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this point:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

See [Section 4.1, "Modifying Field Lengths on the Process Form"](#) for information about working around this issue.

- **Bug 8470245**

The connector-cloning feature is not supported in this release of the connector.

- **Bug 8504052**

The Test Connectivity option does not work for the IT resource that you create to hold information about the SoD engine.

Index

A

additional files, 1-2
Administrative and User Console, 2-9
approver role, request-based provisioning, 3-22
architecture, 1-3
attributes
 user reconciliation scheduled task, 3-4

B

BAPIF4T table, 2-20
batched reconciliation, 1-5, 3-4

C

certified components, 1-1
certified languages, 1-2
changing input locale, 2-8, 2-17
clearing server cache, 2-17
components, certified, 1-1
configuring
 change password functionality, 2-15
 Oracle Identity Manager server, 2-8
 target system, 2-20
configuring connector, 3-1
configuring, SoD, 2-27
connector architecture, 1-3
connector features, 1-4
connector files and directories
 description, 2-1
connector functionality, extending, 4-1
Connector Installer, 2-6
connector release number, determining, 2-2
connector testing, 5-1
connector, configuring, 3-1

D

defining
 IT resources, 2-35
determining release number of connector, 2-2
disabling SoD, 2-29

E

enabling

 SoD, 2-31
enabling logging, 2-18
end-user's role, request-based provisioning, 3-17
extending connector functionality, 4-1
external code files, 1-2, 2-4

F

features of connector, 1-4
files
 additional, 1-2
 external code, 1-2
 See also XML files
files and directories of the connector
 See connector files and directories
filtered reconciliation
 See limited reconciliation, 1-5
full reconciliation, 1-4, 3-2

G

globalization features, 1-2

I

incremental reconciliation, 1-4, 3-2
input locale, changing, 2-8, 2-17
installation, 2-6
 preinstallation, 2-1
installing connector, 2-1, 2-6, 2-8
issues, 6-1
IT resources
 defining, 2-35
 parameters, 2-35
 SAP R3 IT Resource, 2-36

L

limitations, 6-1
limited reconciliation, 1-5, 3-2
logging enabling, 2-18
lookup field synchronization, 1-5, 1-6, 3-1
lookup fields, 1-5, 1-6, 3-1

M

- modifying
 - field mappings
 - field mappings, 4-1
- multilanguage support, 1-2
- multiple trusted source reconciliation, 4-1

O

- Oracle Identity Manager Administrative and User Console, 2-9
- Oracle Identity Manager server, configuring, 2-8

P

- parameters of IT resources, 2-35
- provisioning, 2-9
 - direct provisioning, 3-7
 - fields, 1-12
 - identity fields, 1-13
 - module, 1-12
 - provisioning triggered by policy changes, 3-7
 - request-based, 3-7
 - user provisioning, 1-12
 - user provisioning functions, 1-12
- provisioning operations in SoD-enabled environments, 3-7

R

- reconciliation
 - batched, 1-5, 3-4
 - full, 1-4, 3-2
 - incremental, 1-4, 3-2
 - limited, 1-5, 3-2
 - regular, 3-2
- reconciliation action rules, 1-11
- reconciliation rules, 1-9
- reconciliation, user attributes, 1-8
- regular reconciliation, 3-2
- release number of connector, determining, 2-2
- request import operation, 2-23
- request-based provisioning, 2-9, 3-16, 3-17, 3-22

S

- SAP GRC, 1-2, 1-4, 2-28, 3-7, 3-13
- SAP GRC, configuring, 2-28
- SAPCAR utility, 2-22
- scheduled tasks
 - defining, 3-5
 - user reconciliation, 3-4
- server cache, clearing, 2-17
- SNC
 - configuring, 2-32
 - configuring, parameters, 2-34
 - prerequisites, 2-33
 - security package, installing, 2-33
- SoD, 2-27
- SoD engine, 2-28

- SoD validation of entitlement requests, 1-4
- SoD, disabling, 2-29
- SoD, enabling, 2-31
- SoD-enabled environment, 3-7, 3-16
 - direct provisioning, 3-7
 - provisioning process, overview, 3-7
 - request-based provisioning, 3-16
- stages of connector deployment
 - installation, 2-6
 - preinstallation, 2-1, 2-8
- supported
 - releases of Oracle Identity Manager, 1-2
 - target systems, 1-2

T

- target resource reconciliation, 1-1, 1-8, 1-10, 1-11
 - reconciliation action rules, 1-11
- target system user account, 2-3
- target systems
 - configuration, 2-20
 - supported, 1-2
- test cases, 5-1
- testing
 - batched reconciliation, 5-3
 - partial reconciliation, 5-2
 - provisioning, 5-1
- testing the connector, 5-1
- testing utility, 2-2, 5-1
- transport request
 - creating, 2-21
 - importing, 2-21
- troubleshooting
 - associated files, 2-2

U

- user reconciliation scheduled task, 3-4