Oracle® Identity Manager

Connector Guide for SAP User Management

Release 9.1.2

E11212-06

December 2009

Oracle Identity Manager Connector Guide for SAP User Management, Release 9.1.2

E11212-06

Copyright © 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

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

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

5 Known Issues

A Standard BAPIs Used During Connector Operations

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager Connector with SAP R/3 and SAP CUA.

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in Oracle Identity Manager Connector for SAP User Management?

This chapter provides an overview of the updates made to the software and documentation for release 9.1.2 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 9.1.1
- Software Updates in Release 9.1.2

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 1.4.3, "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.

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 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.

Software Updates in Release 9.1.1

The following are software updates in release 9.1.1:

- Support for Both SAP R/3 and SAP CUA
- Change in Oracle Identity Manager Release Requirement
- Use of Standard BAPIs
- Enhanced Set of Default Attribute Mappings
- New Provisioning Functions
- Configuring Password Changes for Newly Created Accounts

- Support for Mapping Standard and Custom Attributes for Reconciliation and Provisioning
- Support for Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations
- Support for Configuring Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts
- Support for Specifying a SAP JCo Trace Level
- Support for Specifying the Use of a Logon Group on the Target System for Connector Operations
- Support for Enabling and Disabling Accounts
- Support for Connection Pooling
- Testing Utility Deprecated

Support for Both SAP R/3 and SAP CUA

From this release onward, this connector replaces release 9.1.0 of both the SAP User Management and SAP CUA connectors.

See Section 1.4.1, "Support for Both SAP R/3 and SAP CUA" for more information.

Change in Oracle Identity Manager Release Requirement

The connector has been certified on Oracle Identity Manager release 9.1.0.2 BP02 and later. This change is mentioned in Section 1.1, "Certified Components".

Use of Standard BAPIs

In earlier releases, custom BAPIs were provided for reconciliation and provisioning with the target system. You deployed these BAPIs on the target system as part of the connector deployment procedure. From this release onward, only standard BAPIs are used during reconciliation and provisioning.

Enhanced Set of Default Attribute Mappings

The default set of attribute mappings for reconciliation and provisioning has been enhanced. See the following sections for a full listing of the attribute mappings:

- Section 1.6.1, "User Attributes for Reconciliation"
- Section 1.7.2, "User Attributes for Provisioning"

New Provisioning Functions

In Section 1.7.1, "User Provisioning Functions", the following provisioning functions have been added:

- Enable a user account
- Disable a user account
- Link a user account
- Update the start date or end date of a role
- Update a custom attribute added on the target system

Configuring Password Changes for Newly Created Accounts

When you log in to SAP by using a newly created account, you are prompted to change your password at first logon. This behavior can be configured for target system accounts created through Oracle Identity Manager. In addition, the connector can be configured so that it is not mandatory to specify passwords for new accounts.

See Section 1.4.12, "Configuring Password Changes for Newly Created Accounts" for more information.

Support for Mapping Standard and Custom Attributes for Reconciliation and Provisioning

From this release onward, you can create mappings for attributes that are not included in the list of default attribute mappings. These attributes can be part of the standard set of attributes provided by the target system or custom attributes that you add on the target system.

See Chapter 4, "Extending the Functionality of the Connector" for more information.

Support for Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations

From this release onward, you can specify a list of accounts that must be excluded from all reconciliation and provisioning operations.

See Section 2.3.7, "Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition" for more information.

Support for Configuring Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts

From this release onward, you can configure the manner in which an SAP R/3 or SAP CUA account is linked with an SAP HRMS account. When enabled, the linking process is automatically triggered during the Create User provisioning operation. If a matching SAP HRMS account cannot be found the first time, then you can manually trigger the linking process after the SAP HRMS account is created.

See Section 1.4.9, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts" for more information.

Support for Specifying a SAP JCo Trace Level

The connector uses the SAP JCo for reconciliation and provisioning operations. The JCo trace level is a numeric specification of the level of trace data that must be logged when the SAP JCo is used. From this release onward, you can specify the trace level as a parameter of the IT resource.

See Table 2–11, " Parameters of the IT Resource" for more information.

Support for Specifying the Use of a Logon Group on the Target System for Connector Operations

In SAP, a logon group is used as a load-sharing mechanism. When a user logs in to a logon group, the system internally routes the connection request to the logon group member with the least load. From this release onward, you can configure the connector to use a logon group for logging in to the target system for reconciliation and provisioning operations.

See Section 2.3.12.1, "Parameters for Enabling the Use of a Logon Group" for more information.

Support for Enabling and Disabling Accounts

Valid From and Valid Through are two user attributes on the target system. For a particular user in SAP, if the Valid Through date is less than the current date, then the account is in the Disabled state. Otherwise, the account is in the Enabled state. From this release onward, the same behavior is duplicated in Oracle Identity Manager.

See Section 1.4.8, "Enabling and Disabling Accounts" for more information.

Support for Connection Pooling

The connector supports the connection pooling feature introduced in Oracle Identity Manager release 9.1.0.2. In earlier releases, a connection with the target system was established at the start of a reconciliation run and closed at the end of the reconciliation run. With the introduction of connection pooling, multiple connections are established by Oracle Identity Manager and held in reserve for use by the connector.

See Section 1.4.14, "Connection Pooling" for more information.

Testing Utility Deprecated

The testing utility is not included in this release of the connector.

Software Updates in Release 9.1.2

The following is the software update in release 9.1.2:

- Changes in the Certified Oracle Identity Manager and Target System Releases
- Support for Integration with SAP GRC Compliant User Provisioning
- Reconciliation and Provisioning of Custom Multivalued Attributes
- Dependent Lookup Fields Feature Is Disabled by Default
- Support for Configuring Transformation of Data During Lookup Field Synchronization

Changes in the Certified Oracle Identity Manager and Target System Releases

Section 1.1, "Certified Components" lists the Oracle Identity Manager and target system releases certified from this release onward.

Support for Integration with SAP GRC Compliant User Provisioning

In an SAP environment, you can set up SAP GRC Compliant User Provisioning as the front end for receiving account creation and modification provisioning requests. From this release onward, the connector can be used to integrate Oracle Identity Manager with SAP GRC Compliant User Provisioning. In this deployment configuration, Oracle Identity Manager acts as the medium for sending provisioning requests to Compliant User Provisioning.

Reconciliation and Provisioning of Custom Multivalued Attributes

From this release onward, the connector allows you to add custom multivalued attributes that you create on the target system for reconciliation and provisioning with Oracle Identity Manager. See the following sections for information about the procedure:

- Section 4.3, "Adding New Standard and Custom Multivalued Attributes for Reconciliation"
- Section 4.8, "Adding Custom Multivalued Attributes for Provisioning"

Dependent Lookup Fields Feature Is Disabled by Default

In this release, the Dependent Lookup Fields feature is disabled by default. You can enable this feature after you deploy the Oracle Identity Manager release 9.1.0.2 bundle patch that addresses Bug 9181280. See Section 4.14.1, "Enabling the Dependent Lookup Fields Feature" for more information.

Support for Configuring Transformation of Data During Lookup Field Synchronization

From this release onward, you can configure transformation of lookup field data synchronized from the target system. Section 1.4.17, "Transformation of Lookup Field Data" provides a pointer to additional information about this feature.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 9.1.0
- Documentation-Specific Updates in Release 9.1.1
- Documentation-Specific Updates in Release 9.1.2

Documentation-Specific Updates in Release 9.1.0

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 information about the organization of content in this guide.

Documentation-Specific Updates in Release 9.1.1

The following documentation-specific updates have been made in release 9.1.1:

- The "Configuring the Connector for Multiple Trusted Source Reconciliation" section has been removed from Chapter 4, "Extending the Functionality of the Connector". The connector does not support this feature.
- The list of standard BAPIs used during connector operations has been added in Appendix A.

Documentation-Specific Updates in Release 9.1.2

Minor changes have been made in the structure and location of some sections.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to use SAP R/3 and SAP CUA systems as managed (target) resources of Oracle Identity Manager.

> **Note:** In this guide, the term **target system** collectively refers to both SAP R/3 and SAP CUA. Where information is specific to either SAP R/3 or SAP CUA, the name of the target system has been used.

In the account management (target resource) mode of the connector, data about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. This data is used to provision (allocate) new resources or update resources already assigned to OIM Users. In addition, you can use Oracle Identity Manager to provision or update SAP R/3 or SAP CUA resources assigned to OIM Users. These provisioning operations performed on Oracle Identity Manager translate into the creation of or updates to target system accounts.

This chapter contains the following sections:

- Section 1.1, "Certified Components"
- Section 1.2, "Certified Languages"
- Section 1.3, "Connector Architecture and Supported Deployment Configurations"
- 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 certified components for the connector.

Table 1–1 Certified Components

Component	Requirement
Oracle Identity Manager	Oracle Identity Manager release 9.1.0.2 BP 04 or later See the following Oracle Technology Network Web page for information about certified components of Oracle Identity Manager: `http://www.oracle.com/technology/software/products/ias/files/idm_certification_101401.html`
JDK	JDK 1.5 or later
Target systems	The target system can be any one of the following: ▪ SAP R/3 4.7 SP 45 (running on WAS 6.20) BASIS SP 48 ▪ mySAP ERP 2004 (ECC 5.0 running on WAS 6.40) BASIS SP 22 ▪ mySAP ERP 2005 (ECC 6.0 running on WAS 7.00) BASIS SP 13 **Note:** From version 6.40 onward, SAP WAS is also known as "SAP NetWeaver."
SoD engine	If you want to configure and use the SoD feature of Oracle Identity Manager with this target system, then install the version of SAP GRC that is supported by Oracle Identity Manager: SAP GRC versions 5.2 SP4 or later and 5.3 SP5 or later
SAP GRC Compliant User Provisioning	If you want to configure and use the Compliant User Provisioning feature of the connector, then you must also configure the Compliant User Provisioning module included in SAP GRC versions 5.2 SP4 or later and 5.3 SP5 or later.
External code	The connector works with SAP JCo 3.0. The following SAP custom code files are required: ▪ sapjco3.jar version 3.0 ▪ **Additional file for Microsoft Windows:** sapjco3.dll version 3.0 **Additional file for AIX, Solaris, and Linux:** libsapjco3.so version 3.0

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 and Supported Deployment Configurations

In its basic mode of operation, the connector sets up Oracle Identity Manager as the front end for sending account creation or modification provisioning requests to either SAP R/3 or SAP CUA. While deploying the connector, you can opt for enabling either direct provisioning or request-based provisioning in Oracle Identity Manager. In direct provisioning, only Oracle Identity Manager administrators can create and manage target system resources. In request-based provisioning, users can raise requests for creating and managing their accounts. Other users designated as administrators or approvers act upon these requests.

An access policy change is the third form of provisioning operation supported by the connector. If a change in an access policy requires corresponding changes in resources provisioned to a set of users, then the required provisioning operations on the target system are automatically initiated from Oracle Identity Manager.

Account data added or modified through provisioning operations performed directly on the target system can be reconciled into Oracle Identity Manager.

Figure 1–1 shows the connector integrating SAP R/3 with Oracle Identity Manager.

Figure 1–1 Connector Integrating SAP R/3 with Oracle Identity Manager

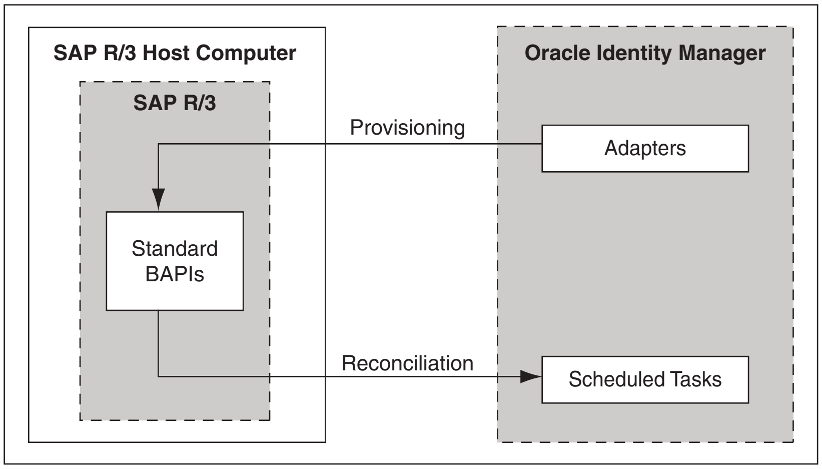
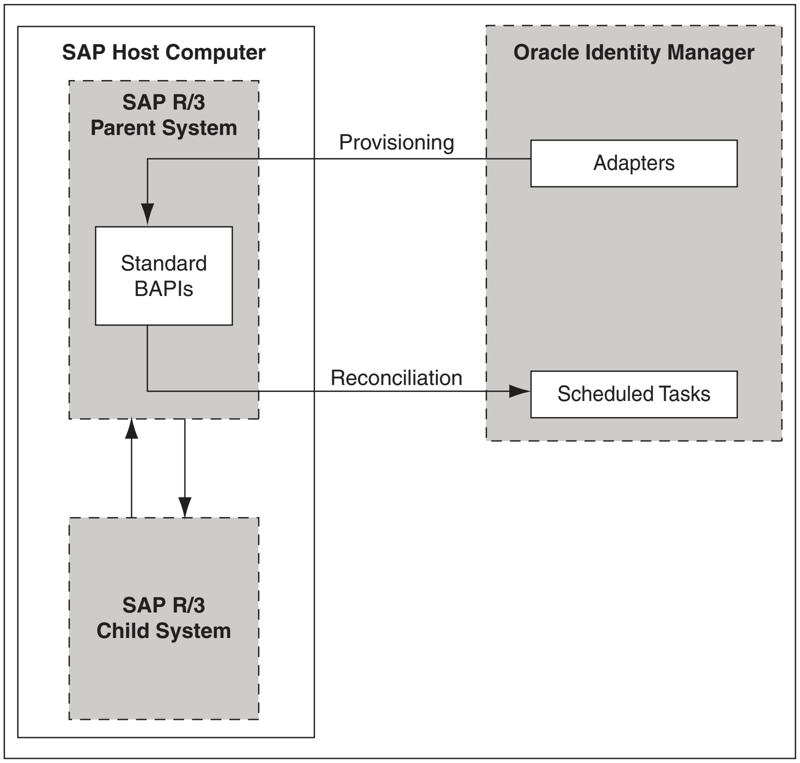


Figure 1–2 shows the connector integrating SAP CUA with Oracle Identity Manager.

Figure 1–2 Connector Integrating SAP CUA with Oracle Identity Manager



As shown in these figures, either SAP R/3 or SAP CUA is configured as a target resource of Oracle Identity Manager. Through provisioning operations performed on Oracle Identity Manager, accounts are created and updated on the target system for OIM Users. Through reconciliation, account data that is created and updated directly on the target system is fetched into Oracle Identity Manager and stored against the corresponding OIM Users.

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

> **See Also:** Appendix A, "Standard BAPIs Used During Connector Operations"

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

Each record fetched from the target system is compared with SAP UM resources that are already provisioned to OIM Users. If a match is found, then the update made to the SAP record from the target system is copied to the SAP UM resource in Oracle Identity Manager. If no match is found, 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 UM resource to the OIM User.

Besides enabling direct integration with the target system, the connector can also be used to act as an interface with the Risk Analysis and Remediation and Compliant

User Provisioning modules of SAP GRC. The target system (SAP R/3 or SAP CUA) and these two modules of SAP GRC together provide various deployment configurations. The following sections provide information about the supported deployment configurations of the connector:

- Section 1.3.1, "Basic User Management"
- Section 1.3.2, "User Management with SoD"
- Section 1.3.3, "User Management with Compliant User Provisioning"
- Section 1.3.4, "User Management with Both SoD and Compliant User Provisioning"
- Section 1.3.5, "Guidelines on Using a Deployment Configuration"
- Section 1.3.6, "Considerations to Be Addressed When You Enable Compliant User Provisioning"

1.3.1 Basic User Management

When you configure the connector for basic user management, the connector accepts provisioning data submitted through Oracle Identity Manager and propagates this data to the target system. For example, when a Create User provisioning operation is performed on Oracle Identity Manager, the outcome is the creation of an account on the target system.

Account data added or modified through provisioning operations performed directly on the target system can be reconciled into Oracle Identity Manager.

Figure 1–1 and Figure 1–2 show the architecture of the connector in this deployment configuration.

The steps performed during a provisioning operation can be summarized as follows:

1. The provisioning operation is initiated through direct provisioning, request-based provisioning, or an access policy change.
2. Provisioning data is sent to the target system.
3. The required change is made on the target system, and the outcome of the operation is sent back to and stored in Oracle Identity Manager.

1.3.2 User Management with SoD

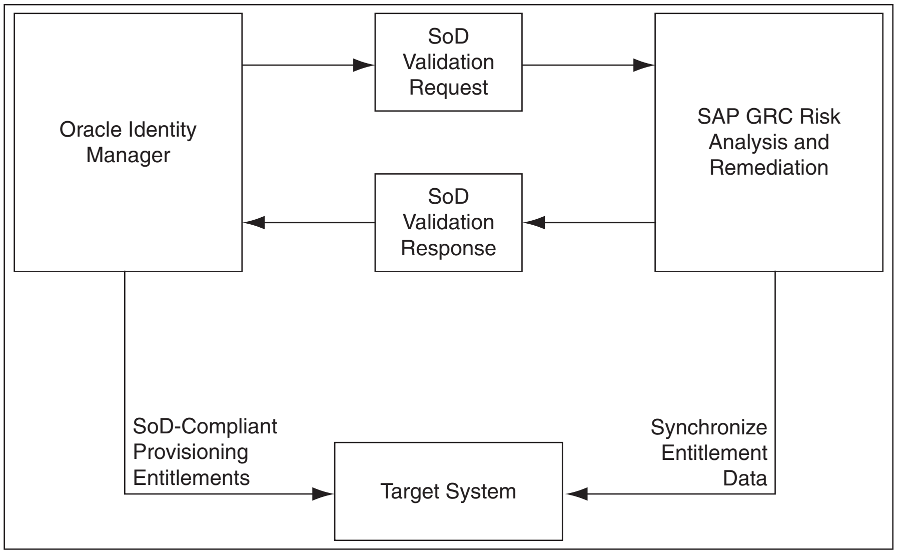
You might have the Risk Analysis and Remediation module of SAP GRC configured to implement segregation of duties (SoD) in your SAP operating environment. In this scenario, the connector can be used as the interface between Oracle Identity Manager and the SoD module. You can configure the connector so that provisioning requests sent from Oracle Identity Manager are first run through the SoD validation process of SAP GRC Risk Analysis and Remediation. Provisioning requests that clear this validation process are then propagated from Oracle Identity Manager to the target system.

Reconciliation does not involve SAP GRC Risk Analysis and Remediation. Account data added or modified through provisioning operations performed directly on the target system can be reconciled into Oracle Identity Manager.

In this guide, the phrase **configuring SoD** is used to mean configuring the integration between Oracle Identity Manager and SAP GRC Risk Analysis and Remediation.

Figure 1–3 shows data flow in this mode of the connector.

Figure 1–3 Data Flow During the SoD Validation Process


Oracle Identity Manager
SoD Validation Request
SAP GRC Risk Analysis and Remediation
SoD Validation Response
SoD-Compliant Provisioning Entitlements
Synchronize Entitlement Data
Target System

The steps performed during a provisioning operation can be summarized as follows:

> **See Also:** The "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in *Oracle Identity Manager Tools Reference* for detailed information about the provisioning process flow

1. The provisioning operation is initiated through direct provisioning, request-based provisioning, or an access policy change.
2. The resource approval workflow of Oracle Identity Manager sends this request to the SoD engine (SAP GRC Risk Analysis and Remediation).
3. The SoD engine uses predefined rules to check if the entitlement assignment would lead to SoD violations. The outcome of this check is then sent back to Oracle Identity Manager.
4. If the request fails SoD validation, then the approval workflow can be configured to take remediation steps. If the request passes SoD validation and if the approver in Oracle Identity Manager approves the request, then the resource provisioning workflow is initiated.
5. This resource provisioning workflow can be configured to perform the SoD validation again. This is to ensure SoD compliance of the entitlement assignment immediately before the entitlement assignment is provisioned to the target system. You can also configure the SoD validation check in the resource provisioning workflow to be bypassed if this validation has been passed in the resource approval workflow.
6. The resource provisioning workflow performs the required change on the target system, and the outcome of the operation is sent back to and stored in Oracle Identity Manager.

1.3.3 User Management with Compliant User Provisioning

Compliant User Provisioning is a module in the SAP GRC suite. In an SAP environment, you can set up Compliant User Provisioning as the front end for receiving account creation and modification provisioning requests. In Compliant User

Provisioning, workflows for processing these requests can be configured and users designated as approvers act upon these requests.

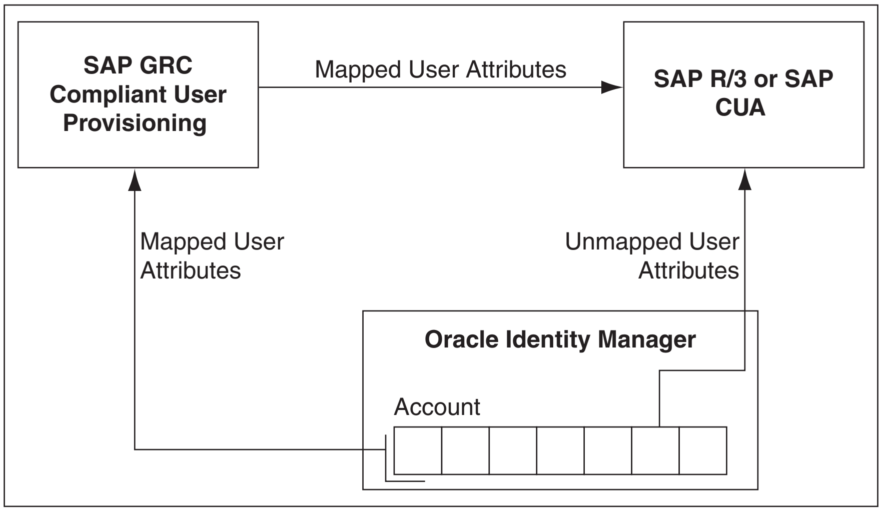
Note: In this guide, the phrase **configuring Compliant User Provisioning** has been used to mean configuring the integration between Oracle Identity Manager and SAP GRC Compliant User Provisioning.

In your operating environment, the Compliant User Provisioning module might be directly linked with the Risk Analysis and Remediation module. In other words, provisioning requests are first sent from Compliant User Provisioning to Risk Analysis and Remediation for SoD validation. Only requests that clear the validation process are implemented on the target system. In this scenario, it is recommended that you do *not* configure the SoD feature of the connector.

Reconciliation does not involve SAP GRC Compliant User Provisioning. Scheduled tasks on Oracle Identity Manager fetch data from the target system to Oracle Identity Manager.

Figure 1–4 shows data flow in this mode of the connector.

Figure 1–4 Connector Integrating SAP GRC Compliant User Provisioning with Oracle Identity Manager and the Target System



The following is the detailed sequence of steps performed during a provisioning operation:

1. The provisioning operation is initiated through direct provisioning, request-based provisioning, or an access policy change.
2. A BAPI is run on the target system to determine one of the following:
   - For a Create User operation, if the BAPI determines that the user exists on the target system, then an error message is displayed. If the user does not exist, then a request is created out of the provisioning data and sent to SAP GRC Compliant User Provisioning.
   - For a Modify User operation, if the BAPI determines that the user does *not* exist on the target system, then an error message is displayed. If the user

exists, then a request is created out of the provisioning data and sent to SAP GRC Compliant User Provisioning.

The connector sends requests and receives responses through the following Web services of SAP GRC:

- SAPGRC_AC_IDM_SUBMITREQUEST: This Web service is used to submit requests.
- SAPGRC_AC_IDM_REQUESTSTATUS: This Web service is used to fetch request statuses.
- SAPGRC_AC_IDM_AUDITTRAIL: This Web service is used to check if there are error messages in the SAP GRC Compliant User Provisioning logs.

The process form holds fields for both basic user management and Compliant User Provisioning. However, for a Create User operation, only the Compliant User Provisioning fields (attributes) on the process form are used. Mappings for these fields are stored in the Lookup.SAP.CUP.ProvisionAttrMap and Lookup.SAP.CUP.ProvisionRoleAttrMap lookup definitions. If you specify values for any attribute that is not present in these lookup definitions, then the connector ignores those attributes during the Create User operation.

> **Note:** SAP GRC Compliant User Provisioning does not process passwords. Therefore, any value entered in the Password field is ignored during Create User provisioning operations.
>
> See Section 3.6, "Guidelines on Performing Provisioning" for information about setting passwords when you configure Compliant User Provisioning.

For a Modify User operation, a request is created only for attributes whose mappings are present in these lookup definitions. If you specify values for attributes that are not present in these lookup definitions, then the connector directly sends them to the target system.

> **Note:** In a Modify User operation, you can specify values for attributes that are mapped with SAP GRC Compliant User Provisioning *and* attributes that are directly updated on the target system.

3. When the request is created on SAP GRC Compliant User Provisioning, data sent back by Compliant User Provisioning is stored in the following read-only fields in Oracle Identity Manager:

   - Request ID: This field holds the request ID that is generated on SAP GRC Compliant User Provisioning. The request ID does not change during the lifetime of the request.
   - Request Status: This field holds the status of the request on SAP GRC Compliant User Provisioning. You configure and run the SAP CUP Status Update Recon scheduled task to fetch the latest status of the request from the target system. Section 3.4.3.3, "SAP CUP Status Update Recon" describes this scheduled task.
   - CUP Requestor ID
   - CUP Requestor First Name

- CUP Requestor Last Name
- CUP Requestor Email

4. The request is passed through the workflow defined in SAP GRC Compliant User Provisioning. The outcome is one of the following:

   - If Compliant User Provisioning clears the request, then the outcome is the creation or modification of a user's account on the target system (SAP R/3 or SAP CUA). The status of the request is set to Closed and a message is recorded in the Oracle Identity Manager logs.
   - If Compliant User Provisioning rejects the provisioning request, then the status of the request is set to Reject and a message is recorded in the Oracle Identity Manager logs.
   - If an error occurs during communication between Compliant User Provisioning and the target system, then the request remains in the Open state. A message stating that the operation has failed is recorded in the audit log associated with the request. An error message is displayed on the console.

1.3.4 User Management with Both SoD and Compliant User Provisioning

You might have both SAP GRC Risk Analysis and Remediation and Compliant User Provisioning configured in your SAP operating environment. You should configure the connector features for both SoD and Compliant User Provisioning at the same time only if the Risk Analysis and Remediation and Compliant User Provisioning modules are discretely configured (that is, not linked) modules in your operating environment.

> **Note:** If SAP GRC Compliant User Provisioning is configured to send provisioning requests to SAP GRC Risk Analysis and Remediation for SoD validation, then you must not configure the SoD feature of the connector.

1.3.5 Guidelines on Using a Deployment Configuration

When you integrate Oracle Identity Manager with your SAP operating environment, you might have one of the following requirements in mind:

- Use Oracle Identity Manager as the provisioning source for account management on SAP resources.
- Leverage workflows and access policies configured in SAP GRC Compliant User Provisioning, with Oracle Identity Manager as the provisioning source for account management on SAP resources.
- Use SAP GRC Risk Analysis and Remediation for SoD enforcement and SAP GRC Compliant User Provisioning for user approval of provisioning requests sent through Oracle Identity Manager. Overall account management on SAP resources is performed through Oracle Identity Manager.

The following sections describe guidelines on the supported deployment configurations:

> **Note:** There are no special guidelines for the Basic User Management configuration and the User Management with SoD configuration.

User Management with SoD and Compliant User Provisioning

The following are deployment guidelines that you must apply for a scenario in which SAP GRC Risk Analysis and Remediation and SAP GRC Compliant User Provisioning are enabled and discretely configured modules:

- Configure both SoD and Compliant User Provisioning features of the connector.
- On SAP GRC Compliant User Provisioning, configure the no-stage approval for account creation. In other words, account creation requests must be auto-approved on Compliant User Provisioning.

  If a role or profile is provisioned on Oracle Identity Manager but rejected on SAP GRC Compliant User Provisioning, then the role or profile is revoked from Oracle Identity Manager at the end of the next user reconciliation run. Therefore, you can have approval workflows defined for role and profile provisioning requests on SAP GRC Compliant User Provisioning.

Summary of the account management process:

1. Data from a provisioning operation on Oracle Identity Manager is first sent to the SAP GRC Risk Analysis and Remediation module for SoD validation.
2. After the SoD validation checks are cleared, the provisioning request is sent to SAP GRC Compliant User Provisioning.
3. After the SAP GRC Compliant User Provisioning workflow clears the request, the provisioning request is implemented on the target system.
4. Scheduled tasks run from Oracle Identity Manager reconcile the outcome of the operation from the target system into Oracle Identity Manager.

User Management with Compliant User Provisioning

The following are deployment guidelines that you must apply for a scenario in which SAP GRC Compliant User Provisioning is configured and enabled in your SAP operating environment:

> **Note:** SAP GRC Risk Analysis and Remediation is either configured as a linked module of SAP GRC Compliant User Provisioning or it is not used at all.

- On SAP GRC Compliant User Provisioning, configure the no-stage approval for account creation. In other words, account creation requests must be auto-approved on Compliant User Provisioning.

  The scenario described earlier in this section explains this guideline.
- Configure the Compliant User Provisioning feature of the connector.
- Do *not* configure the SoD feature of the connector.

Summary of the account management process:

1. Data from a provisioning operation on Oracle Identity Manager is sent to SAP GRC Compliant User Provisioning.
2. The workflow defined in SAP GRC Compliant User Provisioning sends the request to the SAP GRC Risk Analysis and Remediation module for SoD validation.
3. After the SoD validation checks are cleared, the provisioning request is implemented on the target system.

4. Scheduled tasks run from Oracle Identity Manager reconcile the outcome of the operation from the target system into Oracle Identity Manager.

1.3.6 Considerations to Be Addressed When You Enable Compliant User Provisioning

Keep in mind the following considerations when you enable the Compliant User Provisioning feature of the connector:

- Multiple requests are generated from Oracle Identity Manager in response to some provisioning operations. For example, if you assign multiple roles to a user in a particular provisioning operation, then one request is created and sent to Compliant User Provisioning for each role.
- For a particular account, Oracle Identity Manager keeps track of the latest request only. This means, for example, if more than one attribute of an account has been modified in separate provisioning operations, then Oracle Identity Manager keeps track of data related to the last operation only.
- A Modify User operation can involve changes to multiple process form fields or child form fields. For each field that is modified, one request is created and sent to SAP GRC Compliant User Provisioning. Only information about the last request sent to Compliant User Provisioning is stored in Oracle Identity Manager.
- Only parent or child form requests can be submitted in a single operation. You cannot submit both parent and child form requests at the same time.
- Enable linking of SAP HRMS and SAP R/3 or SAP CUA accounts only if a no-stage workflow has been defined for the Create User provisioning operations.

  Section 1.4.9, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts" describes the feature of the connector that stores the link between an SAP HRMS account created for an individual and the corresponding SAP R/3 or SAP CUA account created for the same individual. When you configure the Compliant User Provisioning feature, you should enable linking only if a no-stage approval has been defined for the Create User request type in SAP GRC Compliant User Provisioning. A no-stage approval is one in which no approvers are involved. All requests sent through a no-stage approval are automatically approved.

1.4 Features of the Connector

The following are features of the connector:

- Section 1.4.1, "Support for Both SAP R/3 and SAP CUA"
- Section 1.4.2, "Mapping Standard and Custom Attributes for Reconciliation and Provisioning"
- Section 1.4.3, "SoD Validation of Entitlement Requests"
- Section 1.4.4, "Routing of Provisioning Requests Through SAP GRC Compliant User Provisioning"
- Section 1.4.5, "Full and Incremental Reconciliation"
- Section 1.4.6, "Limited (Filtered) Reconciliation"
- Section 1.4.7, "Batched Reconciliation"
- Section 1.4.8, "Enabling and Disabling Accounts"
- Section 1.4.9, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts"

- Section 1.4.10, "SNC Communication Between the Target System and Oracle Identity Manager"
- Section 1.4.11, "Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations"
- Section 1.4.12, "Configuring Password Changes for Newly Created Accounts"
- Section 1.4.13, "Specifying a SAP JCo Trace Level"
- Section 1.4.14, "Connection Pooling"
- Section 1.4.15, "Specifying the Use of a Logon Group on the Target System for Connector Operations"
- Section 1.4.16, "Transformation and Validation of Account Data"
- Section 1.4.17, "Transformation of Lookup Field Data"

1.4.1 Support for Both SAP R/3 and SAP CUA

The connector can be used to integrate Oracle Identity Manager with either or both SAP R/3 and SAP CUA. From release 9.1.1 onward, this connector replaces release 9.1.0 of both the SAP User Management and SAP CUA connectors.

Most of the features of the connector are the same for both target systems. Where there are differences, these differences have been called out in this guide.

1.4.2 Mapping Standard and Custom Attributes for Reconciliation and Provisioning

You can create mappings for attributes that are not included in the list of default attribute mappings. These attributes can be part of the standard set of attributes provided by the target system or custom attributes that you add on the target system.

See Chapter 4, "Extending the Functionality of the Connector" for more information.

1.4.3 SoD Validation of Entitlement Requests

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. 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 are configured for the SoD validation capabilities of SAP GRC. You can use them 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 detailed information about the SoD feature

Section 2.3.10, "Configuring SoD" in this guide

1.4.4 Routing of Provisioning Requests Through SAP GRC Compliant User Provisioning

You can configure the connector to work with SAP GRC Compliant User Provisioning. See Section 1.3.3, "User Management with Compliant User Provisioning" for detailed information about this feature.

1.4.5 Full and Incremental Reconciliation

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

At the end of a reconciliation run, an attribute of the scheduled task holds the time stamp at which the reconciliation run began. If that attribute is set to 0, then full reconciliation is performed. If that attribute holds a non-zero value, then incremental reconciliation is performed.

During full reconciliation, a single reconciliation event is generated for a particular target system account. However, during incremental reconciliation, two reconciliation events are generated for each account:

- The first reconciliation event contains all account data other than the Locked/Unlocked status.
- The second reconciliation event contains the Locked/Unlocked status.

You can switch from incremental to full reconciliation at any time after you deploy the connector. See Section 3.1, "Performing Full Reconciliation" for more information.

1.4.6 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 3.4.2, "Limited Reconciliation" for more information.

1.4.7 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 the description of the Batch Size attribute in Section 3.4.3, "Reconciliation Scheduled Tasks" for more information.

1.4.8 Enabling and Disabling Accounts

Valid From and Valid Through are two user attributes on the target system. For a particular user in SAP, if the Valid Through date is less than the current date, then the account is in the Disabled state. Otherwise, the account is in the Enabled state. The same behavior is duplicated in Oracle Identity Manager through reconciliation. In addition, you can set the value of the Valid Through date to a current date or a date in the past through a provisioning operation.

> **Note:** The Enabled or Disabled state of an account is not related to the Locked or Unlocked status of the account.

1.4.9 Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts

An SAP HRMS account created for an individual can be linked with the SAP R/3 or SAP CUA account created for the same user. For a particular user, an attribute of SAP HRMS holds the user ID of the corresponding SAP R/3 or SAP CUA account.

You can duplicate this link in Oracle Identity Manager by using the following entries of the Lookup.SAP.UM.Configuration lookup definition:

- Support HRMS 0105 Infotype Linking
- Validate Personnel Number before Linking
- Overwrite Link

See Section 2.3.2.1, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts" for more information.

1.4.10 SNC Communication Between the Target System and Oracle Identity Manager

You can configure Secure Network Communication (SNC) to secure communication between Oracle Identity Manager and the target system.

See Section 2.3.11, "Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System" for more information.

1.4.11 Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations

You can specify a list of accounts that must be excluded from all reconciliation and provisioning operations. Accounts whose user IDs you specify in the exclusion list are not affected by reconciliation and provisioning operations.

See Section 2.3.7, "Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition" for more information.

1.4.12 Configuring Password Changes for Newly Created Accounts

When you log in to SAP by using a newly created account, you are prompted to change your password at first logon. For accounts created through Oracle Identity Manager, password management can be configured using one of the following approaches:

- Configure the connector so that users with newly created accounts are prompted to change their passwords at first logon.
- Configure the connector so that the password set while creating the account on Oracle Identity Manager is set as the new password on the target system. The user is not prompted to change the password at first logon.

This feature is configured using the Dummy password parameter of the IT resource and the Change Password entry of the Lookup.SAP.UM.Configuration lookup definition. In addition, the Password Disabled entry of this lookup definition allows you to specify whether or not the password must be optional during Create User provisioning operations.

See Also:

Section 2.3.12, "Configuring the IT Resource"

Section 2.3.2.2, "Configuring Password Changes for Newly Created Accounts"

1.4.13 Specifying a SAP JCo Trace Level

The connector uses the SAP JCo for reconciliation and provisioning operations. The JCo trace level is a numeric specification of the level of trace data that must be logged when the SAP JCo is used. You can specify the trace level as a parameter of the IT resource.

See Table 2–11, " Parameters of the IT Resource" for more information.

1.4.14 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target system. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools are created, one for each target system installation.

The configuration properties of the connection pool are part of the IT resource definition. Section 2.3.12, "Configuring the IT Resource" provides information about setting up the connection pool.

1.4.15 Specifying the Use of a Logon Group on the Target System for Connector Operations

In SAP, a logon group is used as a load-sharing mechanism. When a user logs in to a logon group, the system internally routes the connection request to the logon group member with the least load. You can configure the connector to use a logon group for logging in to the target system for reconciliation and provisioning operations.

See Section 2.3.12.1, "Parameters for Enabling the Use of a Logon Group" for more information.

1.4.16 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:

- Section 4.9, "Configuring Validation of Data During Reconciliation and Provisioning"

- Section 4.10, "Configuring Transformation of Data During User Reconciliation"

1.4.17 Transformation of Lookup Field Data

You can configure transformation of lookup field data that is brought into Oracle Identity Manager during lookup field synchronization. Section 4.11, "Configuring Transformation of Data During Lookup Field Synchronization" for more information.

1.5 Lookup Definitions Used During Connector Operations

Lookup definitions used during connector operations can be categorized as follows:

- Section 1.5.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.5.2, "Preconfigured Lookup Definitions"

1.5.1 Lookup Definitions Synchronized with the Target System

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 automatically created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

> **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.UM.LookupMappings and Lookup.SAP.CUA.LookupMappings lookup definitions are 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 these lookup definitions 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 these lookup definitions. The Decode column holds a list of the parameters required to fetch lookup field values from the target system.

Table 1–2 Entries in the Lookup.SAP.UM.LookupMappings and Lookup.SAP.CUA.LookupMappings Lookup Definitions

Code Key	Decode
Lookup.SAP.UM.CommType	BAPI_HELPVALUES_GET;GETDETAIL;ADDRESS;COMM_TYPE;COMM_TYPE;COMM_TEXT
Lookup.SAP.UM.Company	BAPI_HELPVALUES_GET;GETDETAIL;COMPANY;COMPANY;COMPANY;COMPANY;USCOMPANY_ADDR;SH
Lookup.SAP.UM.ContractualUserType	BAPI_HELPVALUES_GET;GETDETAIL;UCLASSSYS;LIC_TYPE;USERTYP;UTYPTEXT;LANGU;I;EQ;EN
Lookup.SAP.UM.DateFormat	BAPI_HELPVALUES_GET;GETDETAIL;DEFAULTS;DATFM;_LOW;_TEXT
Lookup.SAP.UM.DecimalNotation	BAPI_HELPVALUES_GET;GETDETAIL;DEFAULTS;DCPFM;_LOW;_TEXT

Table 1–2 (Cont.) Entries in the Lookup.SAP.UM.LookupMappings and Lookup.SAP.CUA.LookupMappings Lookup Definitions

Code Key	Decode
Lookup.SAP.UM.LangComm	BAPI_HELPVALUES_GET;GETDETAIL;ADDRESS;LANGU_P;SPRAS;SPTXT
Lookup.SAP.UM.Parameter	BAPI_HELPVALUES_GET;GETDETAIL;PARAMETER;PARID;PARAMID;PARTEXT
Lookup.SAP.UM.Profile	**For SAP R/3:** BAPI_HELPVALUES_GET;GETDETAIL;PROFILES;BAPIPROF;PROFN;PTEXT **For SAP CUA:** RFC_READ_TABLE;USRSYSPRFT;PROFN;PTEXT;SUBSYSTEM;USRSYSPRF;LANGU = 'EN'
Lookup.SAP.UM.Roles	**For SAP R/3:** BAPI_HELPVALUES_GET;GETDETAIL;ACTIVITYGROUPS;AGR_NAME;AGR_NAME;TEXT;AGR_COLL;SH **For SAP CUA:** RFC_READ_TABLE;USRSYSACTT;AGR_NAME;TEXT;SUBSYSTEM;USRSYSACT;LANGU = 'EN'
Lookup.SAP.UM.System	**For SAP R/3:** SYSTEMNAME **For SAP CUA:** RFC_READ_TABLE;USZBVLNDRC;RCVSYSTEM;RCVSYSTEM
Lookup.SAP.UM.TimeZone	BAPI_HELPVALUES_GET;CHANGE;ADDRESS;TIME_ZONE;TZONE;DESCRIPT
Lookup.SAP.UM.UserGroups	BAPI_HELPVALUES_GET;GETDETAIL;GROUPS;USERGROUP;USERGROUP;TEXT
Lookup.SAP.UM.UserTitle	BAPI_HELPVALUES_GET;GETDETAIL;ADDRESS;TITLE_P;TITLE_MEDI;TITLE_MEDI;ADDR2_SH_TITLE;SH

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

- Code Key format: *`IT_RESOURCE_KEY~LOOKUP_FIELD_ID`*

  Note: For multivalued attributes (roles and profiles), the format is as follows:

  `IT_RESOURCE_KEY~SYSTEM_NAME~LOOKUP_FIELD_ID`

  In this format:

  – *`IT_RESOURCE_KEY`* is the numeric code assigned to the IT resource in Oracle Identity Manager.

  – *`LOOKUP_FIELD_ID`* is the target system code assigned to the lookup field entry.

  Sample value: `1~PRT`

- Decode format: *`IT_RESOURCE_NAME~LOOKUP_FIELD_ENTRY`*

  In this format:

- *IT_RESOURCE_NAME* is the name of the IT resource in Oracle Identity Manager.
- *LOOKUP_FIELD_ENTRY* is the value or description of the lookup field entry on the target system.

Sample value: `SAP IT~Printer`

The SAP User Management Lookup Recon scheduled task is used to synchronize values of these lookup definitions with the target system. Section 3.2, "Scheduled Task for Lookup Field Synchronization" provides 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.

During lookup field synchronization, new entries are appended to the existing set of entries in the lookup definitions. You can switch from an SAP R/3 target to a SAP CUA target, or you can switch between multiple installations of the same target system. Because the IT resource key is part of each entry created in each lookup definition, only lookup field entries that are specific to the IT resource you select during a provisioning operation are displayed.

1.5.2 Preconfigured Lookup Definitions

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 Preconfigured Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.SAP.UM.Configuration	This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.	Some of the entries in this lookup definition are preconfigured. See Section 2.3.2, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager" for information about the entries for which you can set values.
Lookup.SAP.CUP.Configuration	This lookup definition holds connector configuration entries that are used during reconciliation and provisioning by the Compliant User Provisioning feature. **Note:** This lookup definition is created only after you configure the Compliant User Provisioning feature.	Some of the entries in this lookup definition are preconfigured. See Section 2.3.9.7, "Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition" for information about the entries for which you can set values.
Lookup.SAP.UM.Constants	This lookup definition stores values that are used internally by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector.	You must not modify the entries in this lookup definition.

Table 1–3 (Cont.) Preconfigured Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.SAP.CUP.Constants	This lookup definition stores values that are used internally by the Compliant User Provisioning feature of the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector. **Note:** This lookup definition is created only after you configure the Compliant User Provisioning feature.	You must not modify the entries in this lookup definition.
Lookup.SAP.UM.ExclusionList	This lookup definition holds user IDs of target system accounts for which you do not want to perform reconciliation and provisioning.	You can enter user IDs in this lookup definition. See Section 2.3.7, "Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition" for more information.
Lookup.SAP.UM.ITResourceMapping	The IT resource is a set of the connection properties required to establish a connection with the target system. The entries listed in this lookup definition are mappings between: - Code Key: Some of the connection properties defined for the ServerDataProvider and DestinationDataProvider interfaces of SAP JCo 3.0 - Decode: Parameters of the IT resource	See Table 2–10 for a listing of the entries in this lookup definition. If you want to add more SAP JCo parameters for establishing a connection between Oracle Identity Manager and the target system installation, then see Section 2.3.12.4, "Mapping New Connection Properties" for information.
Lookup.SAP.CUA.LookupMappings and Lookup.SAP.UM.LookupMappings	These lookup definitions hold data required to synchronize other lookup definitions with the target system.	These lookup definitions are preconfigured. You can add entries in this lookup definition, but you must not modify existing entries. See the earlier section for a listing of the entries in these lookup definitions. See Section 4.12, "Configuring Synchronization of New Lookup Definitions with the Target System" for more information about adding entries.
Lookup.SAP.UM.LookupReconTransformation	This lookup definition is used to configure transformation of data during lookup field synchronization.	See Section 4.11, "Configuring Transformation of Data During Lookup Field Synchronization" for more information about adding entries in this lookup definition.
Lookup.SAP.UM.ProvAttrMap	This lookup definition holds mappings between process form fields and single-valued target system attributes.	This lookup definition is preconfigured. Table 1–8 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for provisioning. See Section 4.4, "Adding New Standard Attributes for Provisioning" for more information.

Table 1–3 (Cont.) Preconfigured Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.SAP.CUP.ProvisionAttrMap	This lookup definition holds mappings between process form fields and single-valued attributes on SAP GRC Compliant User Provisioning. **Note:** This lookup definition is created only after you configure the Compliant User Provisioning feature.	This lookup definition is preconfigured. Table 1–10 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new attributes for provisioning. See Section 4.5, "Adding New Standard SAP GRC Compliant User Provisioning Attributes for Provisioning" for more information.
Lookup.SAP.UM.ProvChildAttrMap	This lookup definition holds mappings between process form fields and multivalued target system attributes.	This lookup definition is preconfigured. Table 1–9 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new multivalued target system attributes for provisioning. See Section 4.6, "Adding New Standard Multivalued Attributes for Provisioning" for more information.
Lookup.SAP.CUP.ProvisionRoleAttrMap	This lookup definition holds mappings between process form fields and multivalued attributes on SAP GRC Compliant User Provisioning. **Note:** This lookup definition is created only after you configure the Compliant User Provisioning feature.	This lookup definition is preconfigured. Table 1–9 lists the default entries in this lookup definition.
Lookup.SAP.UM.ProvCheckBoxMapping	This lookup definition is used to map check box attributes of the target system with their values when selected and deselected. It is used during provisioning.	By default, there are no entries in this lookup definition. You must add entries only if you want to add a check box attribute on the target system for provisioning. See Step 4 in Section 4.4, "Adding New Standard Attributes for Provisioning" for more information.
Lookup.SAP.UM.ProvValidation	This lookup definition is used to configure validation of attribute values entered on the process form during provisioning operations.	You manually create entries in this lookup definition. See Section 4.9, "Configuring Validation of Data During Reconciliation and Provisioning" for more information.
Lookup.SAP.UM.ReconAttrMap	This lookup definition holds mappings between resource object fields and single-valued target system attributes.	This lookup definition is preconfigured. Table 1–4 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for reconciliation. See Section 4.2, "Adding New Attributes for Reconciliation" for more information.
Lookup.SAP.UM.ReconChildAttrMap	This lookup definition holds mappings between resource object fields and multivalued target system attributes.	This lookup definition is preconfigured. Table 1–5 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for reconciliation. See Section 4.3, "Adding New Standard and Custom Multivalued Attributes for Reconciliation" for more information.

Table 1–3 (Cont.) Preconfigured Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.SAP.UM.CustomChildAttrMap	This lookup definition holds mappings between resource object fields and custom multivalued target system attributes.	You can add entries in this lookup definition if you want to map custom target system attributes for reconciliation. See Section 4.3, "Adding New Standard and Custom Multivalued Attributes for Reconciliation" for more information.
Lookup.SAP.UM.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. Table 2–8 lists the entries in this lookup definition.
Lookup.SAP.UM.ReconChecKBoxMapping	This lookup definition maps check box attributes of the target system with their values when selected and deselected. It is used during reconciliation.	By default, there are no entries in this lookup definition. You must add entries only if you want to add a check box attribute on the target system for reconciliation. See Step 7 in Section 4.2, "Adding New Attributes for Reconciliation" for more information.
Lookup.SAP.UM.ReconTransformation	This lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation.	You manually create entries in this lookup definition. See Section 4.10, "Configuring Transformation of Data During User Reconciliation" for more information.
Lookup.SAP.UM.ReconValidation	This lookup definition that you can use to configure validation of attribute values that are fetched from the target system during reconciliation.	You manually create entries in this lookup definition. See Section 4.9, "Configuring Validation of Data During Reconciliation and Provisioning" for more information.
Lookup.SAP.UM.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. Table 2–7 lists the entries in this lookup definition.
Lookup.SAP.UM.SoDConfiguration	This lookup definition holds configuration values that are used by the connector during SoD operations.	See Section 2.3.10.2, "Specifying Values for SoD-Related Entries in the Lookup.SAP.UM.SoDConfiguration Lookup Definition" for information about specifying values for the entries in this lookup definition.
Lookup.SAP.UM.CustomAttrMap	This lookup definition holds details of custom attributes that you want to include for reconciliation.	See Step 6 in Section 4.2, "Adding New Attributes for Reconciliation" for information about creating entries in this lookup definition.

1.6 Connector Objects Used During Reconciliation

The SAP User Management User Recon scheduled task is used to initiate a reconciliation run. This scheduled task is discussed in Section 3.4.3, "Reconciliation Scheduled Tasks".

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

The Lookup.SAP.UM.ReconAttrMap lookup definition maps resource object fields and target system attributes. The Code Key column stores the names of resource object fields. The format of the Decode column is as follows:

```
FIELD_TYPE;FIELD_NAME;STRUCTURE_NAME
```

In this format, *FIELD_TYPE* can be TEXT, LOOKUP, CHECKBOX, or DATE.

Table 1–4 lists entries in this lookup definition.

Table 1–4 Entries in the Lookup.SAP.UM.ReconAttrMap Lookup Definition

Resource Object Field	Target System Attribute
Accounting Number	TEXT;ACCNT;LOGONDATA
Alias	TEXT;USERALIAS;ALIAS
Building	TEXT;BUILDING_P;ADDRESS
Communication Type	LOOKUP;COMM_TYPE;ADDRESS
Company	LOOKUP;COMPANY;COMPANY
Contractual User Type	LOOKUP;LIC_TYPE;UCLASS|UCLASSSYS
Cost Center	TEXT;KOSTL;DEFAULTS
Date Format	LOOKUP;DATFM;DEFAULTS
Decimal Notation	LOOKUP;DCPFM;DEFAULTS
Department	TEXT;DEPARTMENT;ADDRESS
E Mail	TEXT;E_MAIL;ADDRESS
Fax Extension	TEXT;FAX_EXTENS;ADDRESS
Fax Number	TEXT;FAX_NUMBER;ADDRESS
First Name	TEXT;FIRSTNAME;ADDRESS
Floor	TEXT;FLOOR_P;ADDRESS
Function	TEXT;FUNCTION;ADDRESS
Lang Communication	LOOKUP;LANGU_P;ADDRESS
Last Name	TEXT;LASTNAME;ADDRESS
Logon Language	LOOKUP;LANGU;DEFAULTS
Room Number	TEXT;ROOM_NO_P;ADDRESS
Start Menu	TEXT;START_MENU;DEFAULTS
Telephone Extension	TEXT;TEL1_EXT;ADDRESS
Telephone Number	TEXT;TEL1_NUMBR;ADDRESS
Time Zone	LOOKUP;TZONE;LOGONDATA
Title	LOOKUP;TITLE_P;ADDRESS

Table 1–4 (Cont.) Entries in the Lookup.SAP.UM.ReconAttrMap Lookup Definition

Resource Object Field	Target System Attribute
User Group	LOOKUP;CLASS;LOGONDATA
User Type	TEXT;USTYP;LOGONDATA
Valid From	DATE;GLTGV;LOGONDATA
Valid Through	DATE;GLTGB;LOGONDATA

The Lookup.SAP.UM.ReconChildAttrMap lookup definition maps resource object fields and multivalued target system attributes. Table 1–5 lists entries in this lookup definition.

The format of Decode entries in this lookup definition is as follows:

```
FIELD_TYPE;FIELD_NAME;TABLE_NAME;OIM_CHILD_TABLE_NAME
```

In this format, *`FIELD_TYPE`* can be `TEXT`, `LOOKUP`, `CHECKBOX`, or `DATE`.

Table 1–5 Entries in the Lookup.SAP.UM.ReconChildAttrMap Lookup Definition

Child Form Field	Target System Attribute
End Date	DATE;TO_DAT;ACTIVITYGROUPS;User Role
Profile Name	LOOKUP;PROFILE | BAPIPROF;PROFILES;User Profile
Profile System Name	LOOKUP;SUBSYSTEM;PROFILES;User Profile
Role Name	LOOKUP;AGR_NAME;ACTIVITYGROUPS;User Role
Role System Name	LOOKUP;SUBSYSTEM;ACTIVITYGROUPS;User Role
Start Date	DATE;FROM_DAT;ACTIVITYGROUPS;User Role

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"
- Section 1.6.2.2, "Viewing Reconciliation Rules in the Design Console"

1.6.2.1 Reconciliation Rule

The following is the process-matching rule:

Rule name: SAP UM Recon Rule

Rule element: User Login Equals User ID

In this rule element:

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

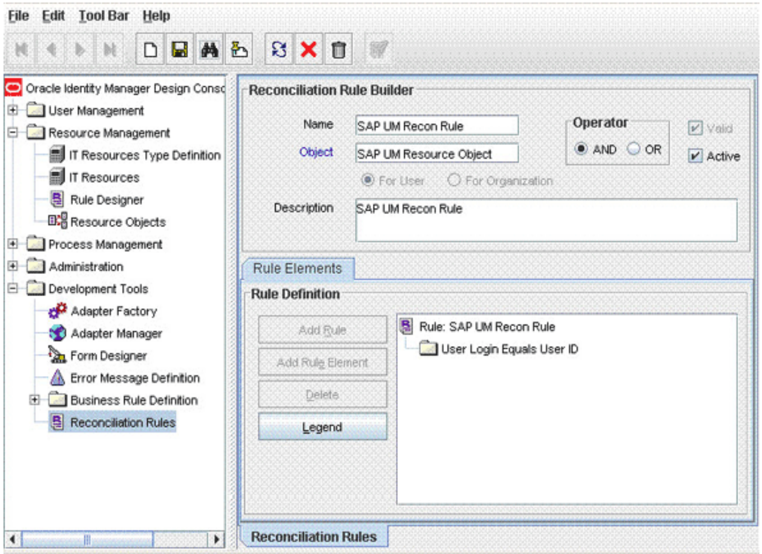
1.6.2.2 Viewing Reconciliation Rules in the Design Console

After you deploy the connector, you can view the reconciliation rule for 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 **and open SAP UM Recon Rule**. Figure 1–5 shows this reconciliation rule.

Figure 1–5 Reconciliation Rule



Name: SAP UM Recon Rule

Object: SAP UM Resource Object

● For User ○ For Organization

Description: SAP UM Recon Rule

Operator: ● AND ○ OR

☑ Valid

☑ Active

Rule: SAP UM Recon Rule
- User Login Equals User ID

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 Reconciliation"
- Section 1.6.3.2, "Viewing Reconciliation Action Rules in the Design Console"

1.6.3.1 Reconciliation Action Rules for Reconciliation

Table 1–6 lists the action rules for reconciliation.

Table 1–6 Action Rules for Reconciliation

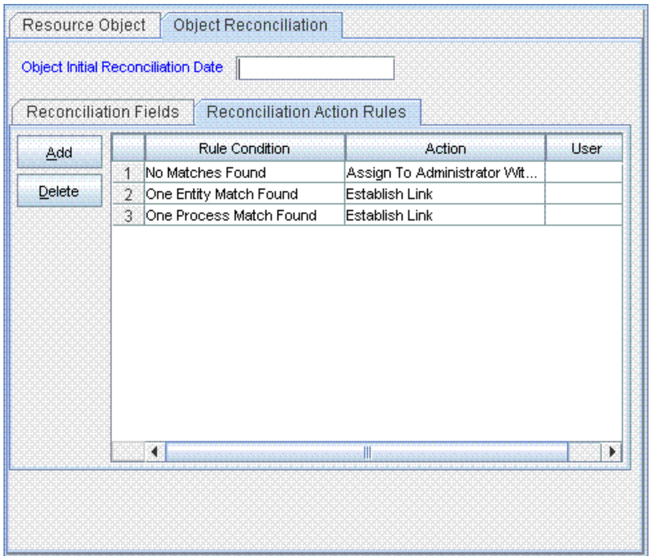
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

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 reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. If you want to view the reconciliation action rules for reconciliation, then search for and open the **SAP UM Resource Object** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–6 shows the reconciliation action rules for reconciliation.

Figure 1–6 Reconciliation Action Rules



	Rule Condition	Action	User
1	No Matches Found	Assign To Administrator Wit...	
2	One Entity Match Found	Establish Link	
3	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 1–7 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 1–7 User Provisioning Functions

Function	Adapter
Create a user account	SAPU Create User
Update a user account	SAPU Modify User
Update the user ID of an account	SAPU Update User ID
Delete a user account	SAPU Delete User
Lock or unlock a user account	SAPU Lock UnLock User
Enable a user account	SAPU Enable User
Disable a user account	SAPU Disable User
Link a user account with an SAP HRMS account	SAPU Create Link
Change the password of an account	SAPU Modify Password
Add (provision) a multivalued attribute (for example, role or profile)	SAPU Add Multivalue Data
Add (provision) a custom multivalued attribute	SAPU Add Custom Multivalue Data
Remove (revoke) a multivalued attribute (for example, role or profile)	SAPU Remove Multivalue Data
Update a multivalued attribute (for example, role or profile)	SAPU Update Multivalue Data
Remove (revoke) a multivalued attribute	SAPU Remove Custom Multivalue Data
Update a custom attribute added on the target system	SAPU Custom Attr Modify

1.7.2 User Attributes for Provisioning

The Lookup.SAP.UM.ProvAttrMap lookup definition maps process form fields with single-valued target system attributes. The Code Key column holds the names of process form fields. The format of values in the Decode column is as follows:

```
FIELD_TYPE;FIELD_NAME;STRUCTURE_NAME;FIELD_NAME_X;STRUCTURE_NAME_X
```

In this format:

- `FIELD_TYPE` can be `TEXT`, `DATE`, `CHECKBOX`, or `LOOKUP`.
- `FIELD_NAME` is the name of the field.
- `STRUCTURE_NAME` is the name of the structure.
- `FIELD_NAME_X` is the name of the field used to indicate whether or not the value in `FIELD_NAME` must be applied.
- `STRUCTURE_NAME_X` is the name of the structure that holds `FIELD_NAME_X`.

Table 1–8 lists the entries in this lookup definition.

Table 1–8 Entries in the Lookup.SAP.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Attribute
Accounting Number	TEXT;ACCNT;LOGONDATA;ACCNT;LOGONDATAX
Alias	TEXT;USERALIAS;ALIAS;BAPIALIAS;ALIASX
Building	TEXT;BUILDING_P;ADDRESS;BUILDING_P;ADDRESSX
Communication Type	LOOKUP;COMM_TYPE;ADDRESS;COMM_TYPE;ADDRESSX
Company	LOOKUP;COMPANY;COMPANY;COMPANY;COMPANYX
Contractual User Type	LOOKUP;LIC_TYPE;UCLASS;UCLASS;UCLASSX
Cost Center	TEXT;KOSTL;DEFAULTS;KOSTL;DEFAULTSX
Date Format	LOOKUP;DATFM;DEFAULTS;DATFM;DEFAULTSX
Decimal Notation	LOOKUP;DCPFM;DEFAULTS;DCPFM;DEFAULTSX
Department	TEXT;DEPARTMENT;ADDRESS;DEPARTMENT;ADDRESSX
E Mail	TEXT;E_MAIL;ADDRESS;E_MAIL;ADDRESSX
Fax Extension	TEXT;FAX_EXTENS;ADDRESS;FAX_EXTENS;ADDRESSX
Fax Number	TEXT;FAX_NUMBER;ADDRESS;FAX_NUMBER;ADDRESSX
First Name	TEXT;FIRSTNAME;ADDRESS;FIRSTNAME;ADDRESSX
Floor	TEXT;FLOOR_P;ADDRESS;FLOOR_P;ADDRESSX
Function	TEXT;FUNCTION;ADDRESS;FUNCTION;ADDRESSX
Language Communication	LOOKUP;LANGU_P;ADDRESS;LANGU_P;ADDRESSX
Last Name	TEXT;LASTNAME;ADDRESS;LASTNAME;ADDRESSX
Logon Language	LOOKUP;LANGU;DEFAULTS;LANGU;DEFAULTSX
Password	TEXT;BAPIPWD;PASSWORD;BAPIPWD;PASSWORDX
Room Number	TEXT;ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX
Start Menu	TEXT;START_MENU;DEFAULTS;START_MENU;DEFAULTSX
Telephone Extension	TEXT;TEL1_EXT;ADDRESS;TEL1_EXT;ADDRESSX
Telephone Number	TEXT;TEL1_NUMBR;ADDRESS;TEL1_NUMBR;ADDRESSX
Time Zone	LOOKUP;TZONE;LOGONDATA;TZONE;LOGONDATAX
Title	LOOKUP;TITLE_P;ADDRESS;TITLE_P;ADDRESSX
User Group	LOOKUP;CLASS;LOGONDATA;CLASS;LOGONDATAX
User ID	TEXT;USERNAME;NONE;NONE;NONE
User Type	TEXT;USTYP;LOGONDATA;USTYP;LOGONDATAX
Valid From	DATE;GLTGV;LOGONDATA;GLTGV;LOGONDATAX
Valid Through	DATE;GLTGB;LOGONDATA;GLTGB;LOGONDATAX

The Lookup.SAP.UM.ProvChildAttrMap lookup definition maps process form fields with multivalued target system attributes. The Code Key column holds the names of the child form fields. The format of the Decode column is the same as that for the Lookup.SAP.UM.ProvAttrMap lookup definition.

Table 1–9 lists the entries in this lookup definition.

Table 1–9 Entries in the Lookup.SAP.UM.ProvChildAttrMap Lookup Definition

Child Form Field	Target System Attribute
End Date	TEXT;TO_DAT;ACTIVITYGROUPS
Profile Name	LOOKUP;PROFILE|BAPIPROF;PROFILES
Profile System Name	LOOKUP;SUBSYSTEM;PROFILES
Role Name	LOOKUP;AGR_NAME;ACTIVITYGROUPS
Role System Name	LOOKUP;SUBSYSTEM;ACTIVITYGROUPS
Start Date	TEXT;FROM_DAT;ACTIVITYGROUPS

In the Compliant User Provisioning feature, the Lookup.SAP.CUP.ProvAttrMap lookup definition maps process form fields with single-valued attributes in SAP GRC Compliant User Provisioning. Table 1–10 lists entries in this lookup definition.

Table 1–10 Entries in the Lookup.SAP.CUP.ProvAttrMap Lookup Definition

Process Form Field	Target System Attribute
CUP Requestor ID	requestorId;TEXT;STANDARD;NONE;MANDATORY
CUP Requestor First Name	requestorFirstName;TEXT;STANDARD;NONE;MANDATORY
CUP Requestor Last Name	requestorLastName;TEXT;STANDARD;NONE;MANDATORY
CUP Requestor Email	requestorEmailAddress;TEXT;STANDARD;NONE;MANDATORY
E Mail	emailAddress;TEXT;STANDARD;E_MAIL;MANDATORY
First Name	firstName;TEXT;STANDARD;FIRSTNAME;MANDATORY
Last Name	lastName;TEXT;STANDARD;LASTNAME;MANDATORY
User ID	userId;TEXT;STANDARD;NONE;MANDATORY
Valid From	validFrom;DATE;STANDARD;GLTGV;NONE
Valid Through	validTo;DATE;STANDARD;GLTGB;MANDATORY

In the Compliant User Provisioning feature, the Lookup.SAP.CUP.ProvisionRoleAttrMap lookup definition maps process form fields with multivalued attributes (roles and profiles) in SAP GRC Compliant User Provisioning. Table 1–10 lists entries in this lookup definition.

Table 1–11 Entries in the Lookup.SAP.CUP.ProvisionRoleAttrMap Lookup Definition

Process Form Field	Target System Attribute
End Date	validTo;DATE
Profile Name	roleId;LOOKUP
Profile System Name	sysId;LOOKUP
Role Name	roleId;LOOKUP
Role System Name	sysId;LOOKUP
Start Date	validFrom;DATE

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, "Known Issues" lists known issues associated with this release of the connector.

2 Deploying the Connector

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

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

> **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"
- Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File"

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-CI.xml	This XML file contains configuration information that is used during connector installation.
deploy/SAPCUP.jar	This JAR file contains class files that are used when you configure the Compliant User Provisioning feature.
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: *OIM_HOME*/xellerate/JavaTasks
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: *OIM_HOME*/xellerate/ScheduleTask
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: *OIM_HOME*/xellerate/ScheduleTask
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: *OIM_HOME*/xellerate/connectorResources **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
Sample/TransformLookup1.java	This file contains the code to work around the Oracle Identity Manager issue described by Bug 9237745. See Section 2.3.13, "Addressing the Issue Related to Non-Unique Values in Lookup Definitions Synchronized with the Target System" for more information.
xml/SAP-UserMgmt-Main-ConnectorConfig.xml	This XML file contains definitions for the following components of the connector: ▪ IT resource definition ▪ Process form ▪ Lookup definitions ▪ Resource object ▪ Process definition ▪ Scheduled tasks
xml/SAP-UserMgmt-RequestApproval-ConnectorConfig.xml	This file contains definitions of the connector components for request-based provisioning when you configure the Compliant User Provisioning feature. See Section 2.3.3, "Enabling Request-Based Provisioning" for instructions on importing this file.
xml/SAP-UserMgmt-CompliantUserProv-ConnectorConfig.xml	This file contains definitions of the connector components to configure the Compliant User Provisioning feature. See Section 2.3.9.1, "Importing the XML File for the Compliant User Provisioning Feature" for instructions on importing this file.
xml/SAP-UserMgmt-CUP-RequestApproval-ConnectorConfig.xml	This file contains definitions of the connector components for request-based provisioning when you configure the Compliant User Provisioning feature. See Section 2.3.9.2, "Enabling Request-Based Provisioning for the Compliant User Provisioning Feature" for instructions on importing this file.

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.

2.1.1.3 Creating a Backup of the Existing Common.jar File

The Common.jar file is in the deployment package of each release 9.1.x connector. With each new release, code corresponding to that particular release is added to the existing code in this file. For example, the Common.jar file shipped with Connector Y on 12-July contains:

- Code specific to Connector Y
- Code included in the Common.jar files shipped with all other release 9.1.x connectors that were released before 12-July.

If you have already installed a release 9.1.x connector that was released after this release of the SAP User Management connector, back up the existing Common.jar file, install the SAP User Management connector, and then restore the Common.jar file. The steps to perform this procedure are as follows:

> **Caution:** If you do not perform this procedure, then your release 9.1.x connectors might not work.

1. Determine the release date of your existing release 9.1.x connector as follows:
   a. Extract the contents of the following file in a temporary directory:

      OIM_HOME/xellerate/ScheduleTask/Common.jar

   b. Open the Manifest.mf file in a text editor.

   c. Note down the Build Date and Build Version values.
2. Determine the release date of this connector as follows:
   a. On the installation media for the connector, extract the contents of the lib/Common.jar and then open the Manifest.mf file in a text editor.

   b. Note down the Build Date and Build Version values.
3. If the Build Date and Build Version values for the SAP User Management connector are less than the Build Date and Build Version values for the connector that is already installed, then:
   a. Copy the *OIM_HOME*/xellerate/ScheduleTask/Common.jar to a temporary location.

   b. After you perform the procedure described in Section 2.2, "Installation" overwrite the new Common.jar file in the *OIM_HOME*/xellerate/ScheduleTask directory with the Common.jar file that you backed up in the preceding step.

2.1.2 Preinstallation on the Target System

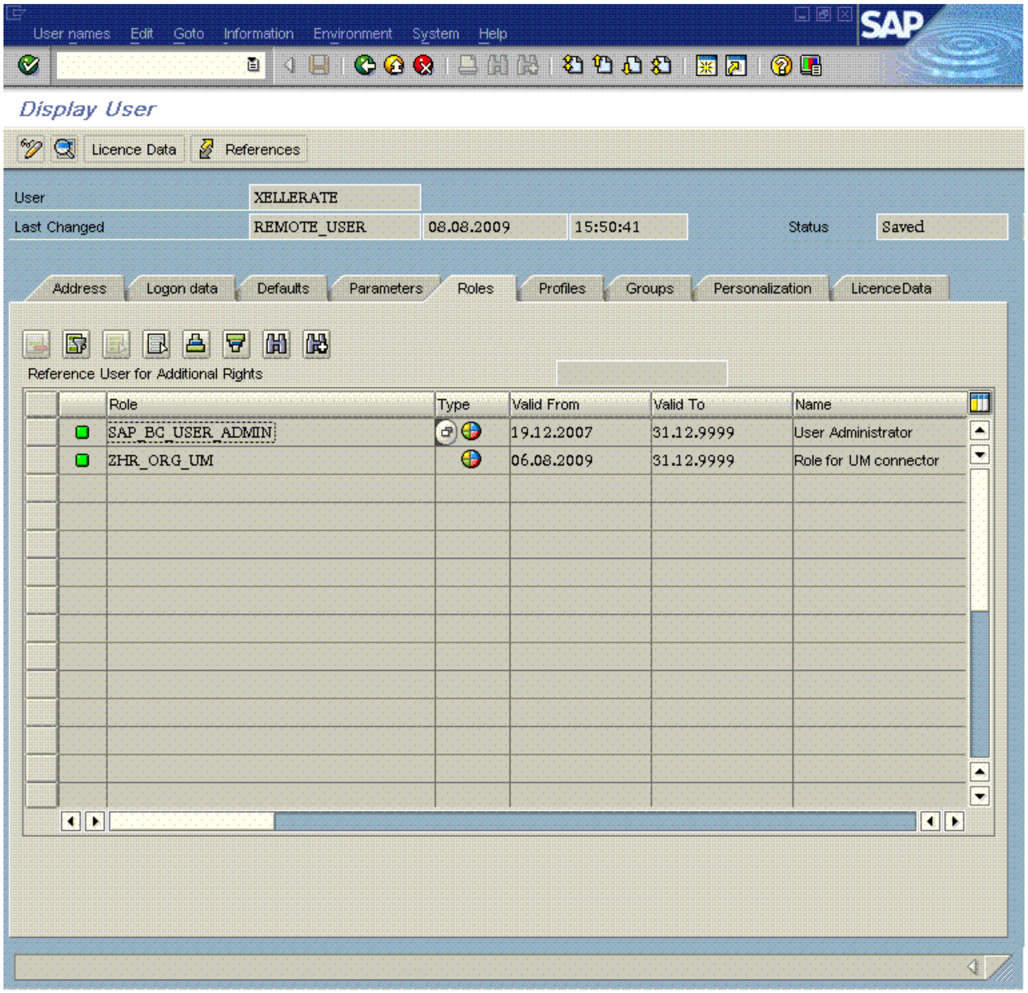
Preinstallation on the target system involves performing the following procedures:

- Section 2.1.2.1, "Creating a Target System User Account for Connector Operations"
- Section 2.1.2.2, "Downloading and Installing the SAP JCo"

2.1.2.1 Creating a Target System User Account for Connector Operations

The connector uses a target system account to connect to the target system during reconciliation. This target system account must be a user to whom you assign a customized role (for example, ZHR_ORG_UM) with the PLOG and P_ORIGIN authorization objects.

For the target system account that is to be created, the Roles tab of the Maintain User form is displayed in the following screenshot:

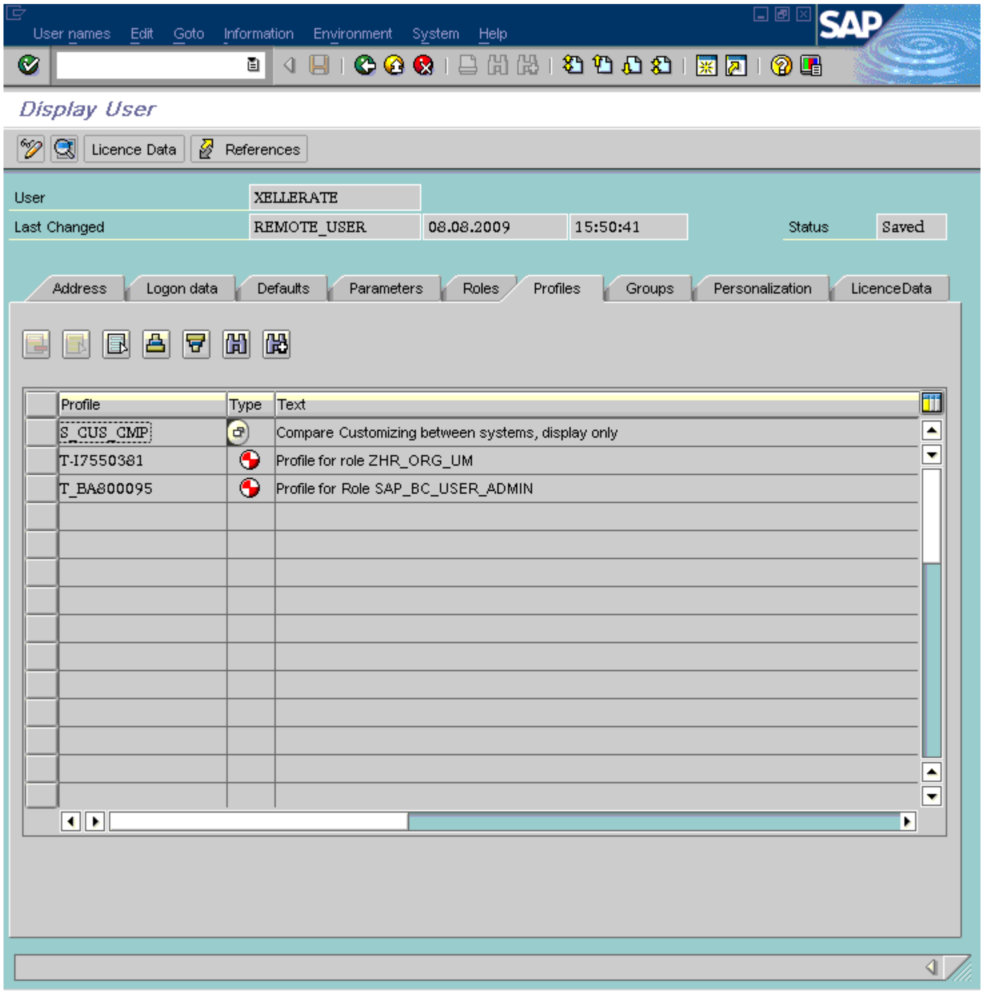


User	XELLERATE		
Last Changed	REMOTE_USER	08.08.2009	15:50:41
Status	Saved		

Reference User for Additional Rights

	Role	Type	Valid From	Valid To	Name
🟩	SAP_BC_USER_ADMIN		19.12.2007	31.12.9999	User Administrator
🟩	ZHR_ORG_UM		06.08.2009	31.12.9999	Role for UM connector

For the target system account that is to be created, the Profiles tab of the Maintain User form is displayed in the following screenshot:

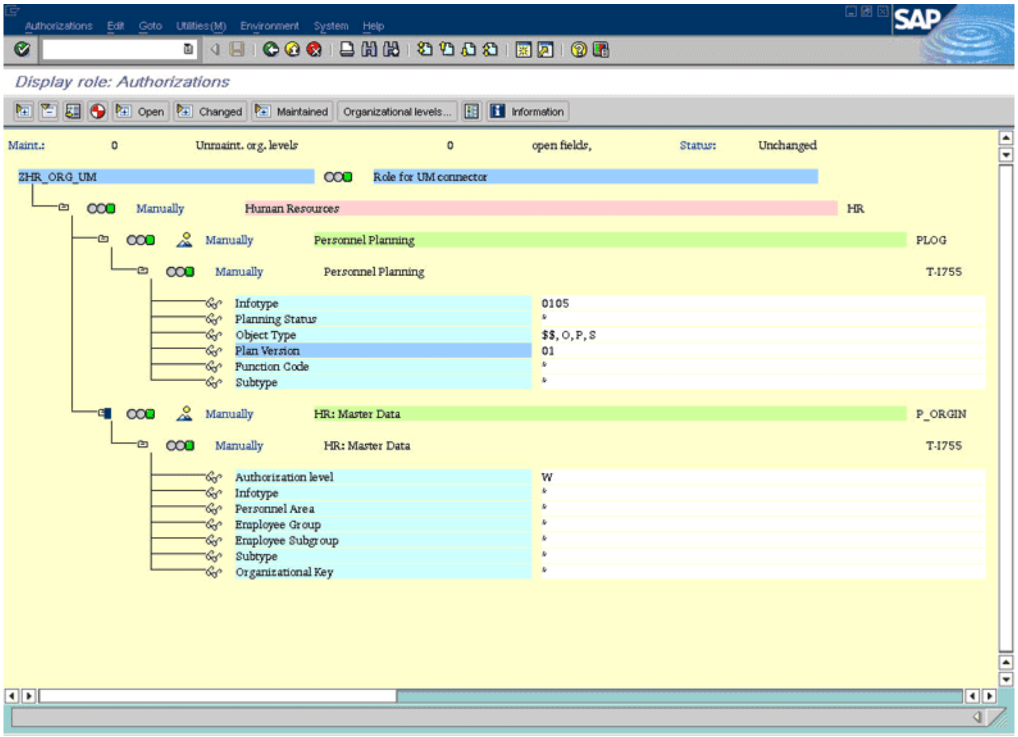


Display User

User	XELLERATE				
Last Changed	REMOTE_USER	08.08.2009	15:50:41	Status	Saved

Profile	Type	Text
S_CUS_CMP		Compare Customizing between systems, display only
T-I7550381		Profile for role ZHR_ORG_UM
T_BA800095		Profile for Role SAP_BC_USER_ADMIN

The following screenshot shows the authorization object that you must assign to the role:



Display role: Authorizations

Maint.: 0 Unmaint. org. levels 0 open fields, Status: Unchanged

ZHR_ORG_UM Role for UM connector

Manually Human Resources HR

Manually Personnel Planning PLOG

Manually Personnel Planning T-I755

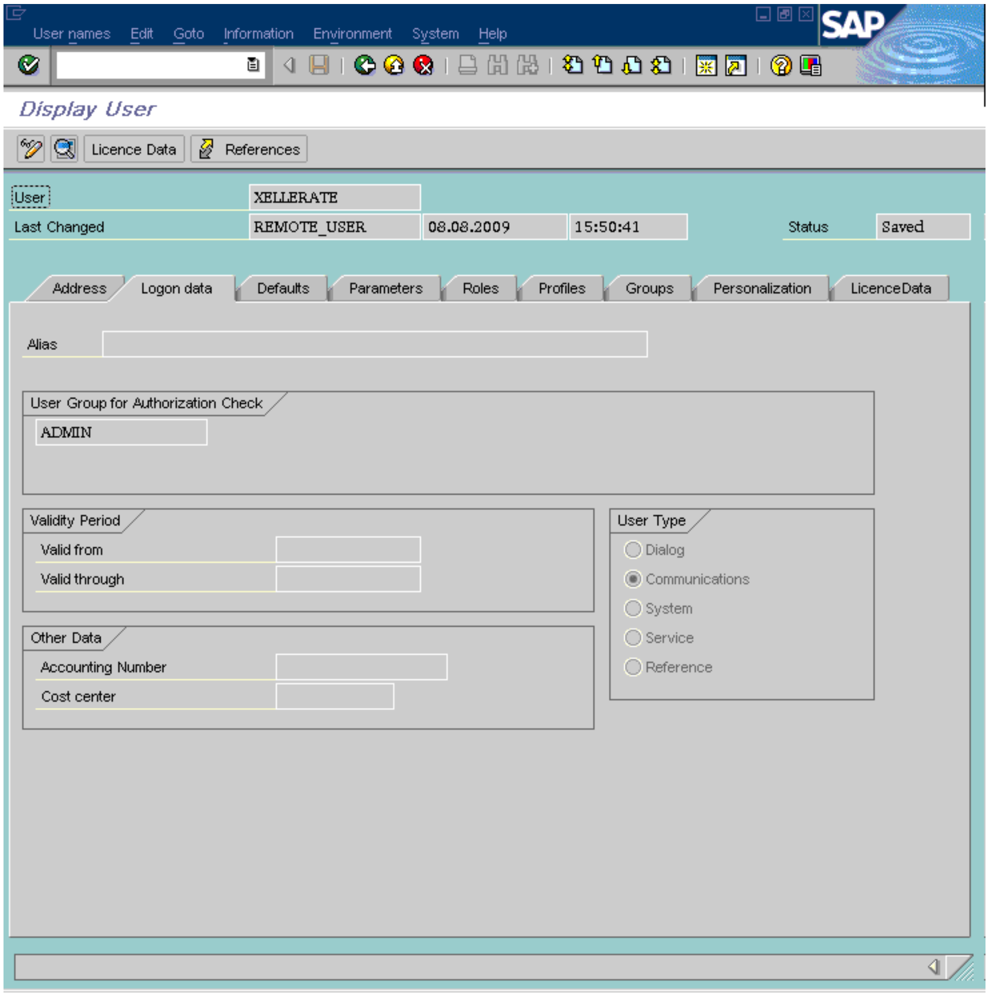
Infotype	0105
Planning Status	*
Object Type	$$, O, P, S
Plan Version	01
Function Code	*
Subtype	*

Manually HR: Master Data P_ORGIN

Manually HR: Master Data T-I755

Authorization level	W
Infotype	*
Personnel Area	*
Employee Group	*
Employee Subgroup	*
Subtype	*
Organizational Key	*

There are no changes to the logon data, as shown in the following screenshot:



Display User

User	XELLERATE				
Last Changed	REMOTE_USER	08.08.2009	15:50:41	Status	Saved

Alias

User Group for Authorization Check

ADMIN

Validity Period

Valid from

Valid through

Other Data

Accounting Number

Cost center

User Type

○ Dialog

● Communications

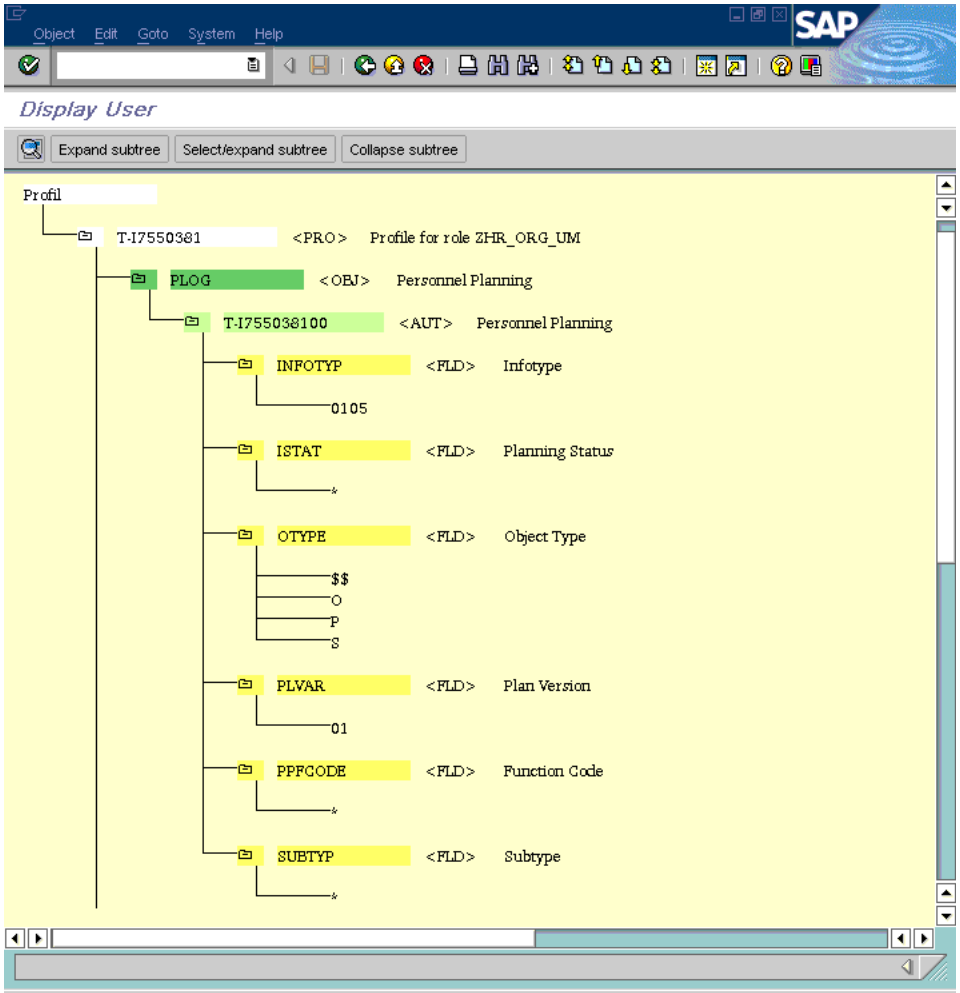
○ System

○ Service

○ Reference

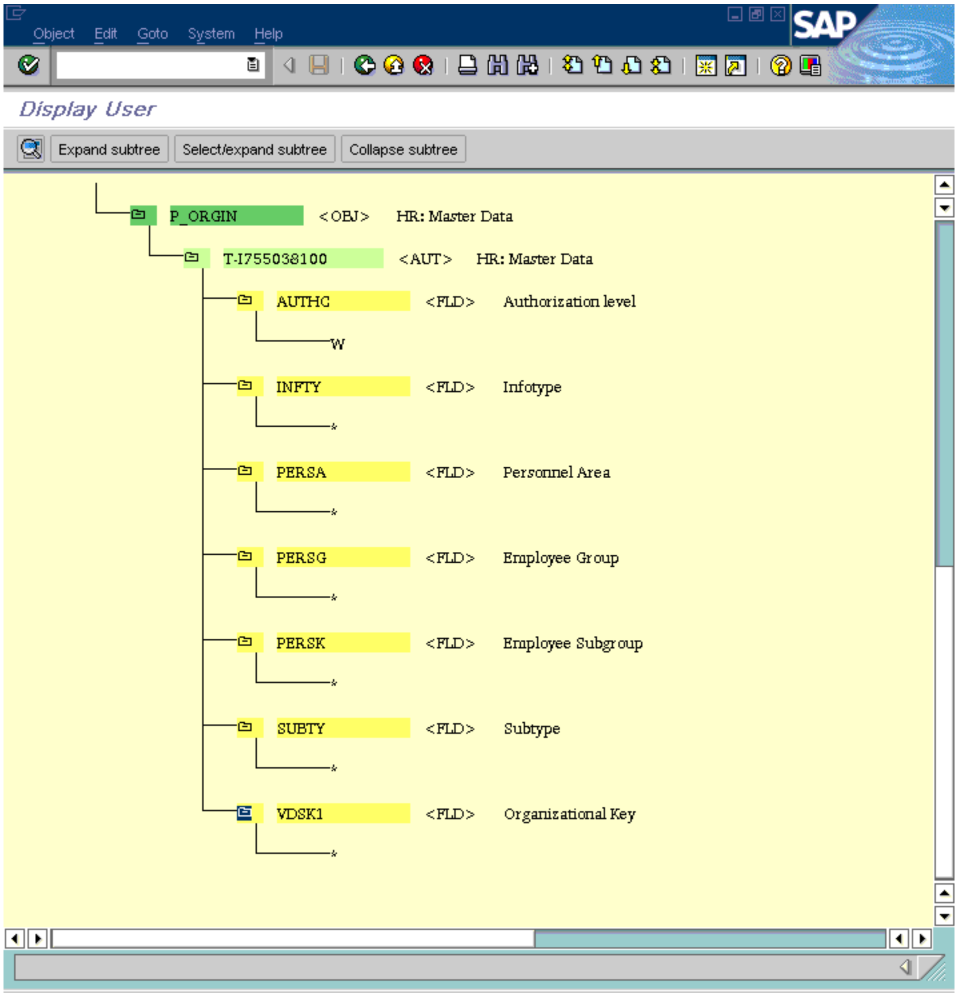
The following screenshot displays details of the PLOG authorization object:

Note: You must configure the PLOG authorization object so that the values assigned to this object match the ones shown in the screenshot. Only the Plan Version (PLVAR) object can be set according to your requirements.



```
Profil
  T-I7550381        <PRO>   Profile for role ZHR_ORG_UM
    PLOG            <OBJ>   Personnel Planning
      T-I755038100  <AUT>   Personnel Planning
        INFOTYP     <FLD>   Infotype
          0105
        ISTAT       <FLD>   Planning Status
          *
        OTYPE       <FLD>   Object Type
          $$
          O
          P
          S
        PLVAR       <FLD>   Plan Version
          01
        PPFCODE     <FLD>   Function Code
          *
        SUBTYP      <FLD>   Subtype
          *
```

The following screenshot displays details of the P_ORIGIN authorization object:



Display User

```
P_ORGIN        <OBJ>  HR: Master Data
  T-I755038100   <AUT>  HR: Master Data
    AUTHC          <FLD>  Authorization level
      W
    INFTY          <FLD>  Infotype
      *
    PERSA          <FLD>  Personnel Area
      *
    PERSG          <FLD>  Employee Group
      *
    PERSK          <FLD>  Employee Subgroup
      *
    SUBTY          <FLD>  Subtype
      *
    VDSK1          <FLD>  Organizational Key
      *
```

2.1.2.2 Downloading and Installing the SAP JCo

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. On a Microsoft Windows platform, ensure that the msvcr80.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.

6. Restart the server for the changes in the environment variable to take effect.

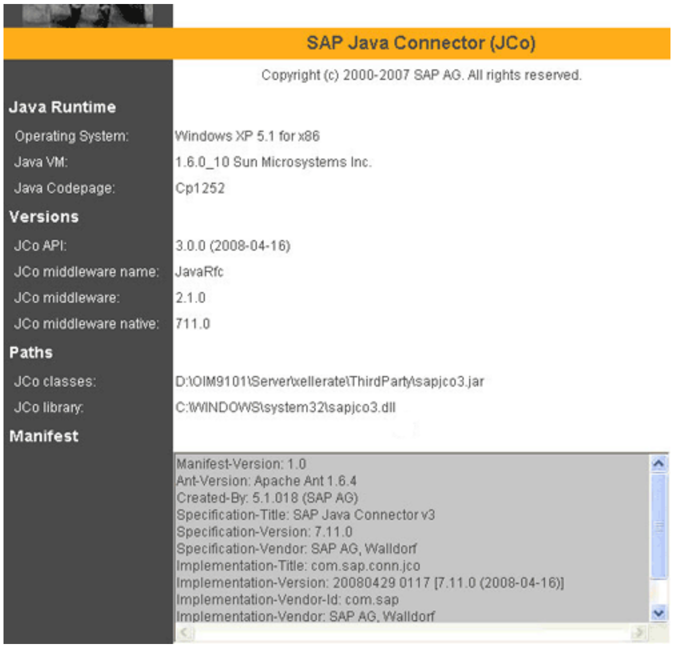
   Note: You can either restart the server now or after the connector is installed.

7. 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



SAP Java Connector (JCo)

Copyright (c) 2000-2007 SAP AG. All rights reserved.

Java Runtime	
Operating System:	Windows XP 5.1 for x86
Java VM:	1.6.0_10 Sun Microsystems Inc.
Java Codepage:	Cp1252
Versions	
JCo API:	3.0.0 (2008-04-16)
JCo middleware name:	JavaRfc
JCo middleware:	2.1.0
JCo middleware native:	711.0
Paths	
JCo classes:	D:\OIM9101\Server\xellerate\ThirdParty\sapjco3.jar
JCo library:	C:\WINDOWS\system32\sapjco3.dll
Manifest	

```
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.6.4
Created-By: 5.1.018 (SAP AG)
Specification-Title: SAP Java Connector v3
Specification-Version: 7.11.0
Specification-Vendor: SAP AG, Walldorf
Implementation-Title: com.sap.conn.jco
Implementation-Version: 20080429 0117 [7.11.0 (2008-04-16)]
Implementation-Vendor-Id: com.sap
Implementation-Vendor: SAP AG, Walldorf
```

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 2.3.3, "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 *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

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

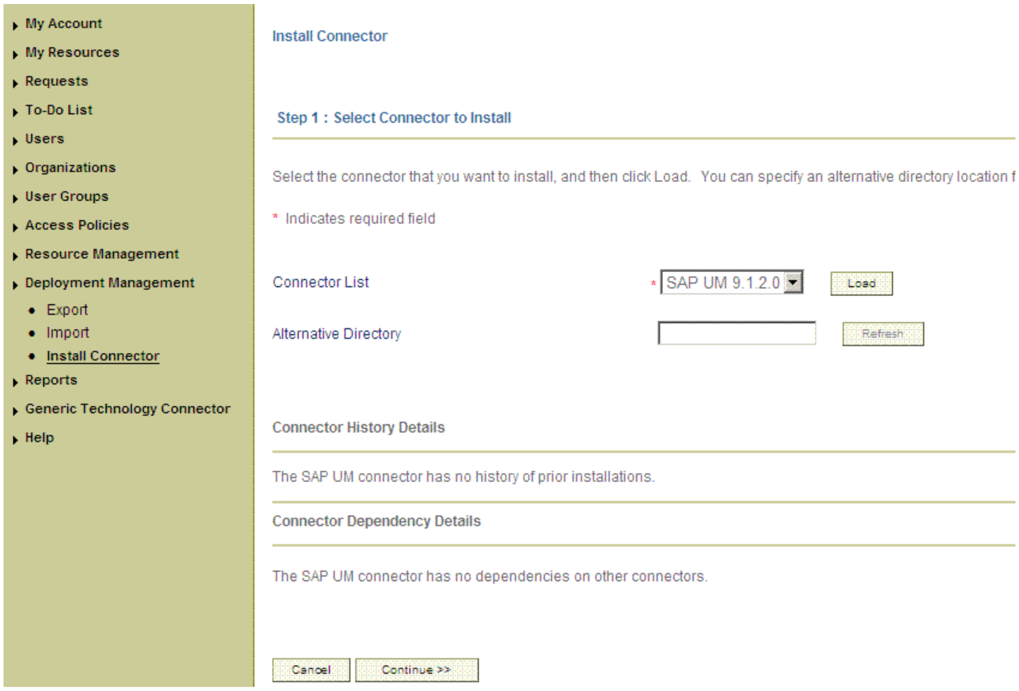
a. In the **Alternative Directory** field, enter the full path and name of that directory.

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

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

5. Click **Load**.

   The following screenshot shows this Administrative and User Console page:



Install Connector

Step 1 : Select Connector to Install

Select the connector that you want to install, and then click Load. You can specify an alternative directory location f

* Indicates required field

Connector List * SAP UM 9.1.2.0

Alternative Directory

Connector History Details

The SAP UM connector has no history of prior installations.

Connector Dependency Details

The SAP UM connector has no dependencies on other connectors.

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

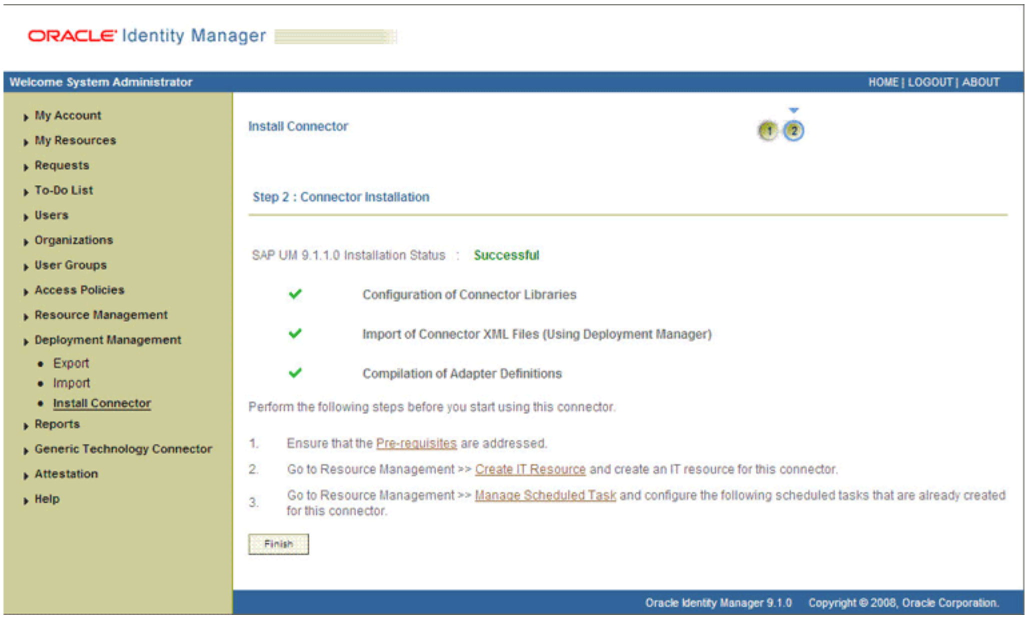
   The following tasks are performed in sequence:

   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. If a task fails, then make the required correction and perform one of the following steps:



Install Connector

Step 2 : Connector Installation

SAP UM 9.1.1.0 Installation Status : Successful

✓ Configuration of Connector Libraries

✓ Import of Connector XML Files (Using Deployment Manager)

✓ Compilation of Adapter Definitions

Perform the following steps before you start using this connector.

1. Ensure that the Pre-requisites are addressed.
2. Go to Resource Management >> Create IT Resource and create an IT resource for this connector.
3. Go to Resource Management >> Manage Scheduled Task and configure the following scheduled tasks that are already created for this connector.

- 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 2.3.5, "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.

Restoring the Common.jar File

If required, restore the Common.jar file that you had backed up by following the procedure described in Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File".

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- Section 2.3.1, "Configuring Ports on the Target System"
- Section 2.3.2, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager"
- Section 2.3.3, "Enabling Request-Based Provisioning"
- Section 2.3.4, "Changing to the Required Input Locale"
- Section 2.3.5, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.6, "Enabling Logging"
- Section 2.3.7, "Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition"
- Section 2.3.8, "Setting Up the Lookup.SAP.UM.LookupMappings and Lookup.SAP.CUA.LookupMappings Lookup Definitions"
- Section 2.3.9, "Configuring the Compliant User Provisioning Feature of the Connector"
- Section 2.3.10, "Configuring SoD"
- Section 2.3.11, "Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System"
- Section 2.3.12, "Configuring the IT Resource"
- Section 2.3.13, "Addressing the Issue Related to Non-Unique Values in Lookup Definitions Synchronized with the Target System"

2.3.1 Configuring Ports on the Target System

To enable communication between the target system and Oracle Identity Manager, you must ensure that the ports listed in Table 2–2 are open.

Table 2–2 Ports for SAP Services

Service	Port Number Format	Default Port
Dispatcher	32*SYSTEM_NUMBER*	3200

Table 2–2 (Cont.) Ports for SAP Services

Service	Port Number Format	Default Port
Gateway (for non-SNC communication)	33*SYSTEM_NUMBER*	3300
Gateway (for SNC communication)	48*SYSTEM_NUMBER*	4800
Message server	36*SYSTEM_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.

2.3.2 Setting Up the Configuration Lookup Definition in Oracle Identity Manager

> **Note:** In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

The following sections discuss the entries in the Lookup.SAP.UM.Configuration lookup definition:

- Section 2.3.2.1, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts"
- Section 2.3.2.2, "Configuring Password Changes for Newly Created Accounts"
- Section 2.3.2.3, "Setting Values in the Lookup.SAP.UM.Configuration Lookup Definition"
- Section 2.3.9.7, "Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition"

2.3.2.1 Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts

An SAP HRMS account created for a particular user can be linked with the SAP R/3 or SAP CUA account created for the same user. For a particular user, an attribute of SAP HRMS holds the user ID of the corresponding SAP R/3 or SAP CUA account.

You can duplicate this link in Oracle Identity Manager by using the following entries of the Lookup.SAP.UM.Configuration lookup definition:

- Support HRMS 0105 Infotype Linking: You enter `yes` as the value if you want to enable linking.
- Validate Personnel Number before Linking: You enter `yes` as the value if your operating environment contains multiple SAP HRMS installations. If there is only one SAP HRMS installation, then enter no.
- Overwrite Link: You enter `yes` as the value if you want existing links in SAP to be overwritten by the ones set up through provisioning operations.

If you enable linking, then you must also add the SAP Linked User ID Equals User ID element to the reconciliation rule as follows:

1. In the Design Console, expand **Development Tools** and then double-click **Reconciliation Rules**.
2. Search for and open **SAP UM Recon Rule**.
3. In the Operator region, select **OR**.
4. Click **Add Rule Element**.
5. In the Add Rule Element dialog box, enter the following data:

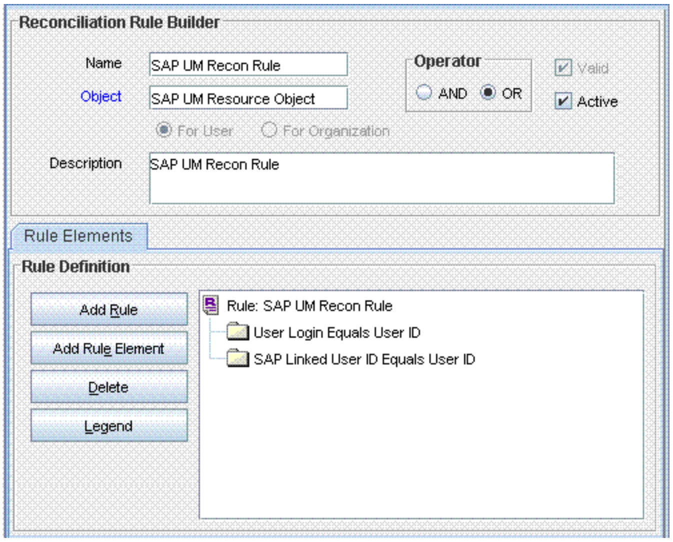
User Profile Data: SAP Linked User ID

Operator: Equals

Attribute: User ID

6. Save and close the dialog box.
7. Click the Save icon to save changes to the reconciliation rule. Figure 2–2 shows the reconciliation rule with the element for linking added.

Figure 2–2 Reconciliation Rule with the Element for Linking



Reconciliation Rule Builder

Name: SAP UM Recon Rule

Object: SAP UM Resource Object

● For User ○ For Organization

Operator: ○ AND ● OR

☑ Valid

☑ Active

Description: SAP UM Recon Rule

Rule Elements

Rule Definition

Rule: SAP UM Recon Rule
- User Login Equals User ID
- SAP Linked User ID Equals User ID

The following example describes the manner in which the linking process is performed:

1. An OIM User record is created for user John Doe through trusted source reconciliation with SAP HRMS. During creation, the user ID value is put in the User ID and Personnel Number attributes of the record.

> **Note:** The Personnel Number field is a hidden UDF on the OIM User form.

2. To provision an SAP R/3 or SAP CUA account for John, you enter and submit the required data on the Administrative and User Console. The remaining steps are performed if you have set the value of Support HRMS 0105 Infotype Linking to `yes`.
3. The connector looks for the user's SAP HRMS account. If you entered `yes` as the value of Validate Personnel Number before Linking, then the connector checks for a match for the Personnel Number attribute on SAP HRMS.
4. After a match is found with an existing SAP HRMS account, the connector performs one of the following steps:
   - If the value of Overwrite Link is `yes`, then the connector posts the User ID value of the SAP R/3 or SAP CUA account into the 0001 subtype in the Communication (0105) infotype of the SAP HRMS account. This is regardless of whether that infotype contains a value.

- If the value of Overwrite Link is no, then the connector posts the User ID value of the SAP R/3 or SAP CUA account into the 0001 subtype in the Communication (0105) infotype of the SAP HRMS account only if that subtype does not hold a value.

The Create Link task is one of the tasks that are run during the Create User provisioning operation. If you set the Support HRMS 0105 Infotype Linking entry to no, then the status of this task is automatically set to Completed even though it is not run. You can, if required, remove this task so that it is not displayed in the list of tasks that are run. Use the Design Console for this operation.

> **See Also:** *Oracle Identity Manager Design Console Guide* for information about removing process tasks

2.3.2.2 Configuring Password Changes for Newly Created Accounts

When you log in to SAP by using a newly created account, you are prompted to change your password at first logon. For accounts created through Oracle Identity Manager, password management can be configured by using the Dummy password parameter of the IT resource and the Change Password entry of the Lookup.SAP.UM.Configuration lookup definition.

You can apply one of the following approaches:

- Configure the connector so that users with newly created accounts are prompted to change their passwords at first logon.

  To achieve this, set the Change Password entry to no. With this setting, the password entered on the process form for a new user account is used to set the password for the new account on the target system. When the user logs in to the target system, the user is prompted to change the password.

  > **Note:** If the password feature is disabled for users on the target system, then set this entry to no.

- Configure the connector so that the password set while creating the account on Oracle Identity Manager is set as the new password on the target system. The user is not prompted to change the password at first logon.

  To achieve this, set the Change Password entry to yes and enter a string in the Dummy password parameter of the IT resource. With these settings, when you create a user account through Oracle Identity Manager, the user is first created with the dummy password. Immediately after that, the connector changes the password of the user to the one entered on the process form. When the user logs in to the target system, the user is not prompted to change the password.

- Configure the connector so that a password is optional during Create User provisioning operations.

  To achieve this, set the Password Disabled entry to yes.

2.3.2.3 Setting Values in the Lookup.SAP.UM.Configuration Lookup Definition

Table 2–3 describes the entries in the Lookup.SAP.UM.Configuration lookup definition.

> **Note:** You must not change any of the Code Key values of this lookup definition.

Table 2–3 Entries in the Lookup.SAP.UM.Configuration Lookup Definition

Code Key	Description
Change Password	See Section 2.3.2.2, "Configuring Password Changes for Newly Created Accounts" for information about the value to be specified for this entry. Default value: `yes`
Check Box Lookup for Prov	This entry holds the name of the lookup definition that is used to map check box attributes of the target system with their values when selected and deselected. This lookup definition is used during provisioning. By default, there are no entries in this lookup definition. You must add entries only if you want to add a check box attribute on the target system for provisioning. Information about using this feature is given in one of the steps in Section 4.4, "Adding New Standard Attributes for Provisioning." Value: `Lookup.SAP.UM.ProvCheckBoxMapping`
Check Box Lookup for Recon	This entry holds the name of the lookup definition that is used to map check box attributes of the target system with their values when selected and deselected. This lookup definition is used during reconciliation. By default, there are no entries in this lookup definition. You must add entries only if you want to add a check box attribute on the target system for reconciliation. Information about using this feature is given in one of the steps in Section 4.2, "Adding New Attributes for Reconciliation". Value: `Lookup.SAP.UM.ReconCheckBoxMapping`
Constants Lookup	This entry holds the name of the lookup definition that stores values used by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector. Value: `Lookup.SAP.UM.Constants`
Custom Attribute Mapping Lookup	This entry holds the name of the lookup definition that you can use to configure custom attribute values for reconciliation. For more information, see the sections that describe procedures to add attributes for reconciliation in Chapter 4. Value: `Lookup.SAP.UM.CustomAttrMap`
Custom Child Attribute Mapping Lookup	This entry holds the name of the lookup definition that you can use to configure custom multivalued attribute values for reconciliation. For more information, see the sections that describe procedures to add attributes for reconciliation in Chapter 4. Value: `Lookup.SAP.UM.CustomChildAttrMap`
CUP Configuration Lookup	This entry holds the name of the lookup definition that stores configuration values for the Compliant User Provisioning feature. Value: `Lookup.SAP.CUP.Configuration`
CUP Mode Enabled	Enter `yes` if you want to enable the Compliant User Provisioning feature. Otherwise, enter `no`.
Exclusion List Lookup	This entry holds the name of the lookup definition in which you enter user IDs of target system accounts for which you do not want to perform reconciliation and provisioning. See Section 2.3.7, "Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition" for more information. Value: `Lookup.SAP.UM.ExclusionList`
Is CUA Enabled	Enter `yes` if the target system is SAP CUA. Enter `no` if the target system is SAP R/3. Default value: `no`

Table 2–3 (Cont.) Entries in the Lookup.SAP.UM.Configuration Lookup Definition

Code Key	Description
IT Resource Mapping	This entry holds the name of the lookup definition that stores default mappings between SAP JCo connection parameters and IT resource parameters. If your target system installation uses JCo parameters that are not covered in this lookup definition, then you can add them. See Section 2.3.12.4, "Mapping New Connection Properties" for more information about this lookup definition. Value: `Lookup.SAP.UM.ITResourceMapping`
Overwrite Link	See Section 2.3.2.1, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts" for information about the value to be specified for this entry. Default value: `yes`
Password Disabled	Enter `no` if you want to make it mandatory for a password to be specified during Create User provisioning operations. Enter `yes` if you want to make the password optional. If you want to use the Compliant User Provisioning feature of the connector, then set the value to `yes`. See Section 2.3.9.4, "Specifying Values in the Lookup.SAP.UM.Configuration Lookup Definition" for more information.
Provisioning Attribute Map Lookup	This entry holds the name of the lookup definition that maps process form fields to target system attributes. See Section 1.7.2, "User Attributes for Provisioning" for more information. Value: `Lookup.SAP.UM.ProvAttrMap`
Provisioning Child Attribute Map Lookup	This entry holds the name of the lookup definition that maps child form fields to multivalued attributes on the target system. See Section 1.7.2, "User Attributes for Provisioning" for more information. Value: `Lookup.SAP.UM.ProvChildAttrMap`
Support HRMS 0105 Infotype Linking	See Section 2.3.2.1, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts" for information about the value to be specified for this entry. Default value: `yes`
Transform Lookup For Recon	This entry holds the name of the lookup definition that you can use to configure transformation of attribute values that are fetched from the target system during reconciliation. See Section 4.10, "Configuring Transformation of Data During User Reconciliation" for more information. Value: `Lookup.SAP.UM.ReconTransformation`
Transform Lookup For Lookup Recon	This entry holds the name of the lookup definition that you can use to configure transformation of lookup field values fetched from the target system during lookup field synchronization. See Section 4.11, "Configuring Transformation of Data During Lookup Field Synchronization" for more information. Value: `Lookup.SAP.UM.LookupReconTransformation`
Use Transformation For Recon	Enter `yes` if you want to configure transformation of attribute values that are fetched from the target system during reconciliation. See Section 4.10, "Configuring Transformation of Data During User Reconciliation" for more information. Default value: `no`

Table 2–3 (Cont.) Entries in the Lookup.SAP.UM.Configuration Lookup Definition

Code Key	Description
Use Transformation For Lookup Recon	Enter `yes` if you want to configure transformation of lookup field values that are fetched from the target system during lookup field synchronization. See Section 4.11, "Configuring Transformation of Data During Lookup Field Synchronization" for more information. Default value: `no`
Use Validation For Prov	Enter yes if you want to configure validation of attribute values entered on the process form during provisioning operations. See Section 4.9, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. Default value: `no`
Use Validation For Recon	Enter yes if you want to configure validation of attribute values that are fetched from the target system during reconciliation. See Section 4.9, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. Default value: `no`
Validate Personnel Number before Linking	See Section 2.3.2.1, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts" for information about the value to be specified for this entry. Default value: `no`
Validation Lookup For Prov	This entry holds the name of the lookup definition that you can use to configure validation of attribute values entered on the process form during provisioning operations. See Section 4.9, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. Value: `Lookup.SAP.UM.ProvValidation`
Validation Lookup For Recon	This entry holds the name of the lookup definition that you can use to configure validation of attribute values entered on the process form during provisioning operations. See Section 4.9, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. Value: `Lookup.SAP.UM.ReconValidation`

2.3.3 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 can be viewed and approved by approvers designated in Oracle Identity Manager.

Note: Do *not* enable request-based provisioning if you want to use the direct provisioning feature of the connector. See *Oracle Identity Manager Connector Concepts* for information about direct provisioning.

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.

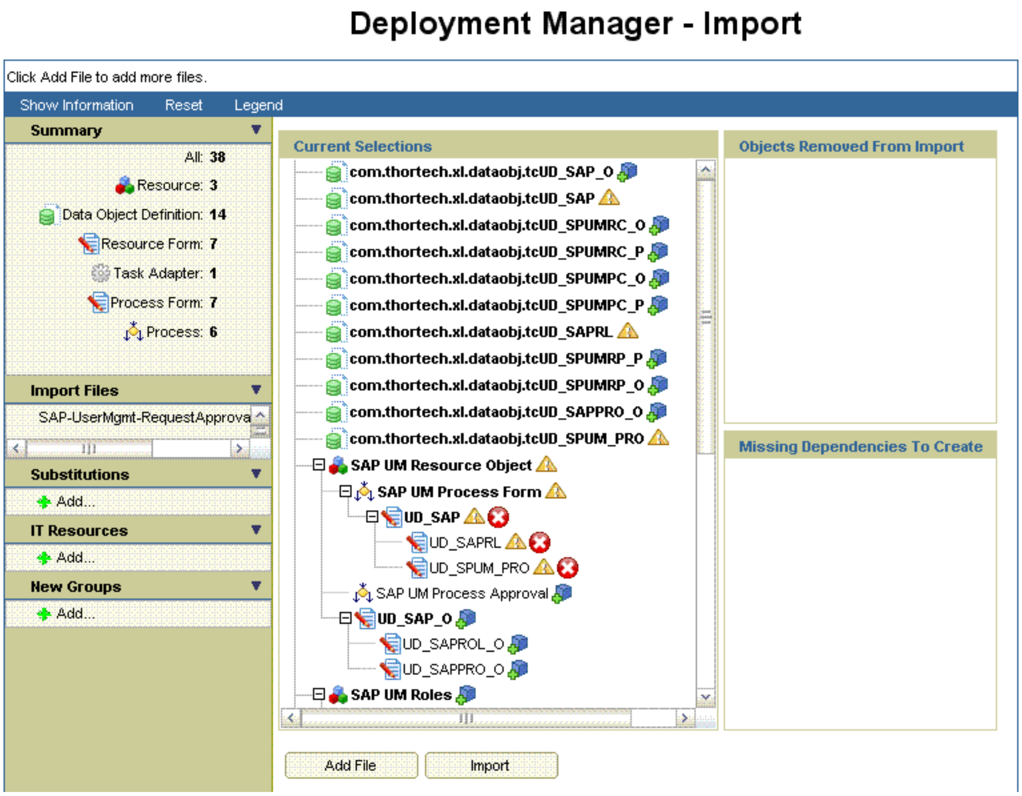
To enable request-based provisioning:

> **Note:** In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

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.

   The following screenshot shows this page:


Deployment Manager - Import
Click Add File to add more files.
Show Information
Reset
Legend
Summary
All: 38
Resource: 3
Data Object Definition: 14
Resource Form: 7
Task Adapter: 1
Process Form: 7
Process: 6
Import Files
SAP-UserMgmt-RequestApprova
Substitutions
Add...
IT Resources
Add...
New Groups
Add...
Current Selections
com.thortech.xl.dataobj.tcUD_SAP_O
com.thortech.xl.dataobj.tcUD_SAP
com.thortech.xl.dataobj.tcUD_SPUMRC_O
com.thortech.xl.dataobj.tcUD_SPUMRC_P
com.thortech.xl.dataobj.tcUD_SPUMPC_O
com.thortech.xl.dataobj.tcUD_SPUMPC_P
com.thortech.xl.dataobj.tcUD_SAPRL
com.thortech.xl.dataobj.tcUD_SPUMRP_P
com.thortech.xl.dataobj.tcUD_SPUMRP_O
com.thortech.xl.dataobj.tcUD_SAPPRO_O
com.thortech.xl.dataobj.tcUD_SPUM_PRO
SAP UM Resource Object
SAP UM Process Form
UD_SAP
UD_SAPRL
UD_SPUM_PRO
SAP UM Process Approval
UD_SAP_O
UD_SAPROL_O
UD_SAPPRO_O
SAP UM Roles
Objects Removed From Import
Missing Dependencies To Create
Add File
Import

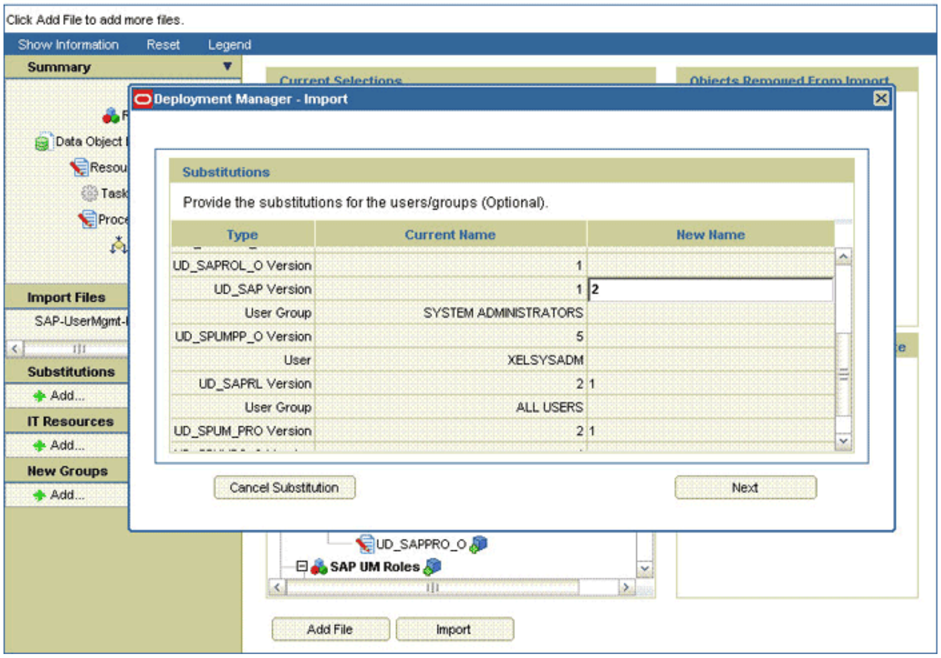
8. Note down the names of the forms that show errors, that is, the red cross sign against their names.

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



Click Add File to add more files.

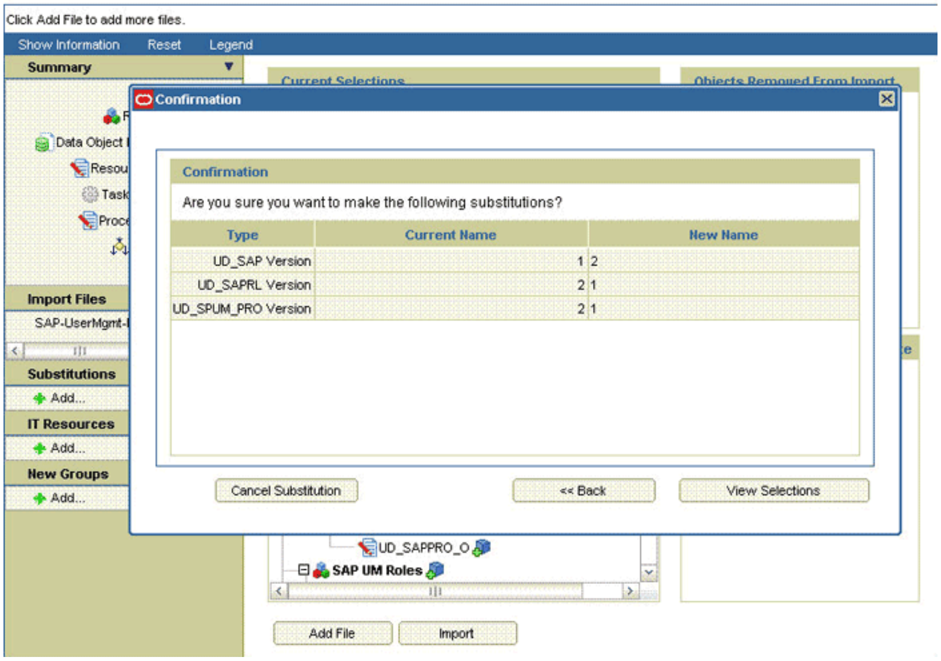
Substitutions

Provide the substitutions for the users/groups (Optional).

Type	Current Name	New Name
UD_SAPROL_O Version	1	
UD_SAP Version	1	2
User Group	SYSTEM ADMINISTRATORS	
UD_SPUMPP_O Version	5	
User	XELSYSADM	
UD_SAPRL Version	2	1
User Group	ALL USERS	
UD_SPUM_PRO Version	2	1

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

Deployment Manager - Import



Click Add File to add more files.

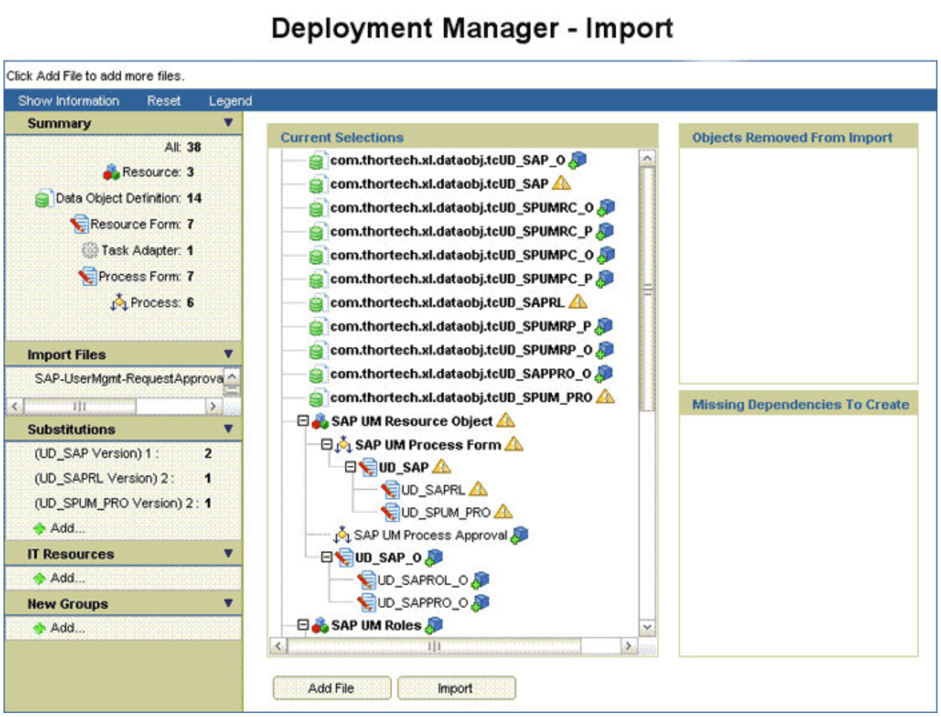
Confirmation

Are you sure you want to make the following substitutions?

Type	Current Name	New Name
UD_SAP Version	1	2
UD_SAPRL Version	2	1
UD_SPUM_PRO Version	2	1

12. Click **View Selections**.

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


Deployment Manager - Import
Click Add File to add more files.
Show Information
Reset
Legend
Summary
All: 38
Resource: 3
Data Object Definition: 14
Resource Form: 7
Task Adapter: 1
Process Form: 7
Process: 6
Import Files
SAP-UserMgmt-RequestApprova
Substitutions
(UD_SAP Version) 1 : 2
(UD_SAPRL Version) 2 : 1
(UD_SPUM_PRO Version) 2 : 1
Add...
IT Resources
Add...
New Groups
Add...
Current Selections
com.thortech.xl.dataobj.tcUD_SAP_O
com.thortech.xl.dataobj.tcUD_SAP
com.thortech.xl.dataobj.tcUD_SPUMRC_O
com.thortech.xl.dataobj.tcUD_SPUMRC_P
com.thortech.xl.dataobj.tcUD_SPUMPC_O
com.thortech.xl.dataobj.tcUD_SPUMPC_P
com.thortech.xl.dataobj.tcUD_SAPRL
com.thortech.xl.dataobj.tcUD_SPUMRP_P
com.thortech.xl.dataobj.tcUD_SPUMRP_O
com.thortech.xl.dataobj.tcUD_SAPPRO_O
com.thortech.xl.dataobj.tcUD_SPUM_PRO
SAP UM Resource Object
SAP UM Process Form
UD_SAP
UD_SAPRL
UD_SPUM_PRO
SAP UM Process Approval
UD_SAP_O
UD_SAPROL_O
UD_SAPPRO_O
SAP UM Roles
Objects Removed From Import
Missing Dependencies To Create
Add File
Import

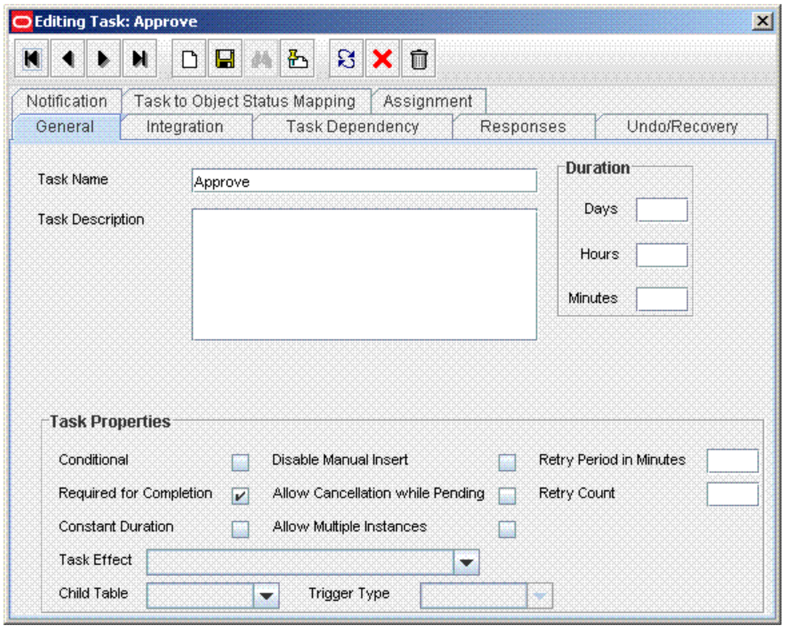
13. Click **Import**.

    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.



Task Name: Approve

Task Description:

Duration

Days:

Hours:

Minutes:

Task Properties

Conditional ☐

Required for Completion ☑

Constant Duration ☐

Disable Manual Insert ☐

Allow Cancellation while Pending ☐

Allow Multiple Instances ☐

Retry Period in Minutes:

Retry Count:

Task Effect:

Child Table:

Trigger Type:

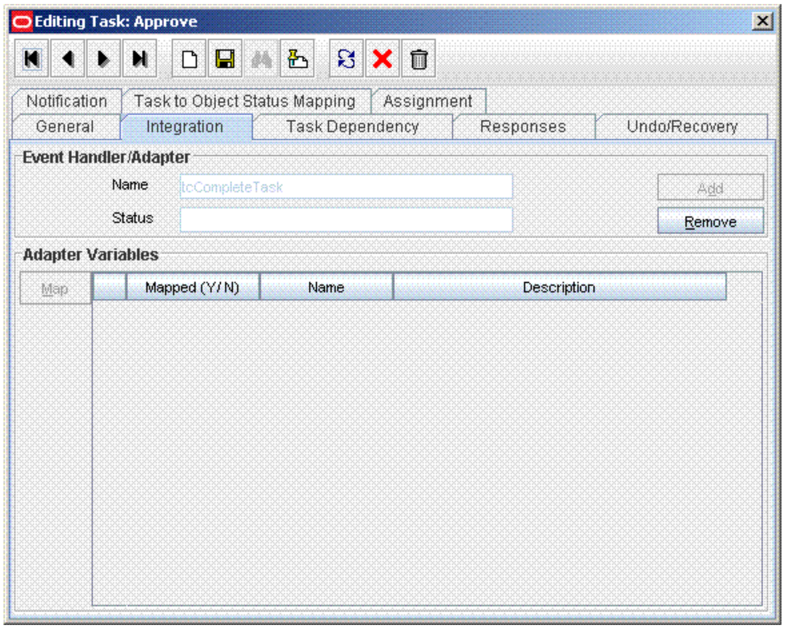
4. On the Integration tab of the Editing Task dialog box, click **Add**.

5. In the Handler Selection dialog box:

   a. Select **System**.

   b. Select the **tcCompleteTask** handler.

   c. Click the Save icon, and then close the dialog box.



Event Handler/Adapter

Name: tcCompleteTask

Status:

Adapter Variables

	Mapped (Y/N)	Name	Description

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.

2.3.4 Changing to the Required Input Locale

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

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.

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

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

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

2.3.6 Enabling Logging

> **Note:** In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

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.OIMCP.SAPU=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.OIMCP.SAPU=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.OIMCP.SAPU=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.OIMCP.SAPU=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="OIMCP.SAPU">
        <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="OIMCP.SAPU">
        <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.OIMCP.SAPU=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.OIMCP.SAPU=INFO
     ```

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

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

2.3.7 Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition

> **Note:** In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

In the Lookup.SAP.UM.ExclusionList lookup definition, enter the user IDs of target system accounts for which you do not want to perform reconciliation and provisioning:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAP.UM.ExclusionList** lookup definition.
3. Click **Add**.
4. In the Code Key and Decode columns, enter the first user ID that you want to exclude. You must enter the same value in both columns.

   > **Note:** You must enter the user ID in the same case (uppercase and lowercase) in which it is stored on the target system.

5. Repeat Steps 3 and 4 for all the user IDs that you want to exclude.
6. Click the Save icon.

2.3.8 Setting Up the Lookup.SAP.UM.LookupMappings and Lookup.SAP.CUA.LookupMappings Lookup Definitions

While logging in to SAP, you can specify a two-letter language code for the UI. Some of the entries in the Lookup.SAP.UM.LookupMappings and Lookup.SAP.CUA.LookupMappings lookup definitions require you to specify this language code.

The determine the language code and make the required change in the lookup definition:

1. To determine the two-letter language code set on the target system:
   a. In the SAP logon dialog box, right-click the system that you are using.
   b. Select Properties from the shortcut menu.
   c. In the Properties dialog box, click **Advanced**.

      In the Advanced Options dialog box, the Language field displays the two-letter language code set for your installation of the target system.
2. Log in to the Design Console.
3. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
4. Search for and open the **Lookup.SAP.UM.LookupMappings** or **Lookup.SAP.CUA.LookupMappings** lookup definition.

5. In the following entries, change **EN** to the two-letter language code that you determined in Step 1:

Code Key	Decode
Lookup.SAP.UM.ContractualUserType	BAPI_HELPVALUES_GET;GETDETAIL;UCLASSSYS;LIC_TYPE;USERTYP;USERTYPTEXT;LANGU;I;EQ;**EN**
Lookup.SAP.UM.Profile	For SAP CUA: RFC_READ_TABLE;USRSYSPRFT;PROFN;PTEXT;SUBSYSTEM;USRSYSPRF;LANGU = '**EN**'
Lookup.SAP.UM.Roles	For SAP CUA: RFC_READ_TABLE;USRSYSACTT;AGR_NAME;TEXT;SUBSYSTEM;USRSYSACT;LANGU = '**EN**'

6. Save and close the lookup definition.

2.3.9 Configuring the Compliant User Provisioning Feature of the Connector

Oracle Identity Manager can be configured as the medium for sending provisioning requests to SAP GRC Compliant User Provisioning. A request from Oracle Identity Manager is sent to Compliant User Provisioning, which forwards the provisioning data contained within the request to the target system (SAP R/3 or SAP CUA). The outcome is the creation of or modification to the user's account on the target system.

Note: Before you configure the Compliant User Provisioning feature, it is recommended that you read the guidelines described in Section 1.3.5, "Guidelines on Using a Deployment Configuration."

The following sections provide information about configuring the Compliant User Provisioning feature:

- Section 2.3.9.1, "Importing the XML File for the Compliant User Provisioning Feature"
- Section 2.3.9.2, "Enabling Request-Based Provisioning for the Compliant User Provisioning Feature"
- Section 2.3.9.3, "Specifying Values for the SAP GRC IT Resource IT Resource"
- Section 2.3.9.4, "Specifying Values in the Lookup.SAP.UM.Configuration Lookup Definition"
- Section 2.3.9.5, "Setting Up the Link with the Web Services for SAP GRC Compliant User Provisioning"
- Section 2.3.9.6, "Configuring Request Types and Workflows on SAP GRC Compliant User Provisioning"
- Section 2.3.9.7, "Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition"

2.3.9.1 Importing the XML File for the Compliant User Provisioning Feature

The xml/SAP-UserMgmt-CompliantUserProv-ConnectorConfig.xml file on the installation media contains definitions of the connector objects that are used by the Compliant User Provisioning feature. You must import the XML file to create these connector objects in Oracle Identity Manager.

To import the XML file:

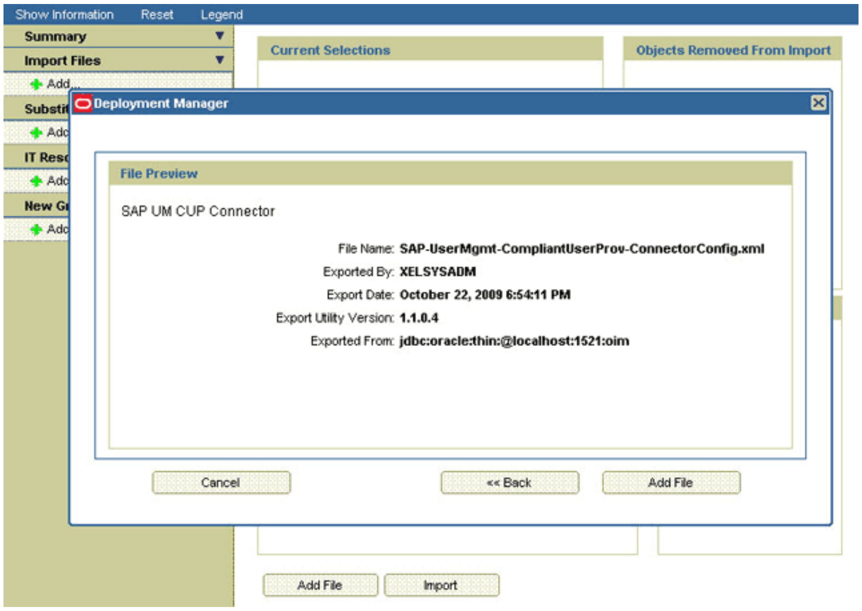
Note:

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.

In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

---

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-CompliantUserProv-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. The following screenshot shows this page:



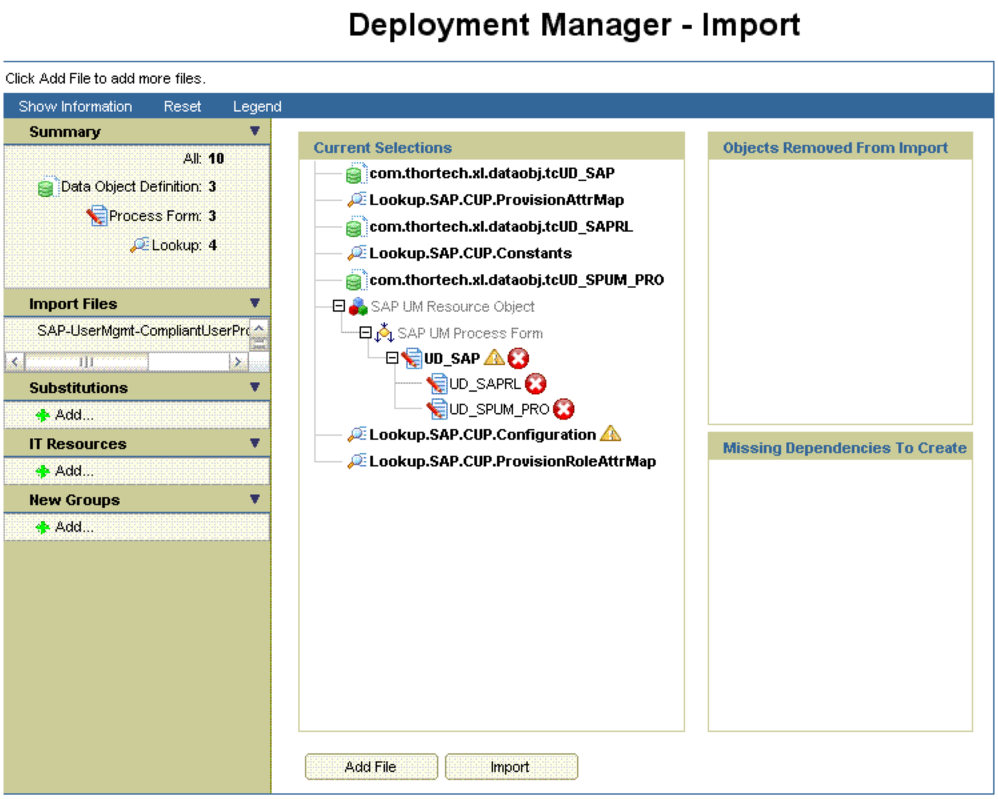
SAP UM CUP Connector

File Name: SAP-UserMgmt-CompliantUserProv-ConnectorConfig.xml
Exported By: XELSYSADM
Export Date: October 22, 2009 6:54:11 PM
Export Utility Version: 1.1.0.4
Exported From: jdbc:oracle:thin:@localhost:1521:oim

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.

   The following screenshot shows this page:



Deployment Manager - Import

Click Add File to add more files.

All: 10
Data Object Definition: 3
Process Form: 3
Lookup: 4

SAP-UserMgmt-CompliantUserPr

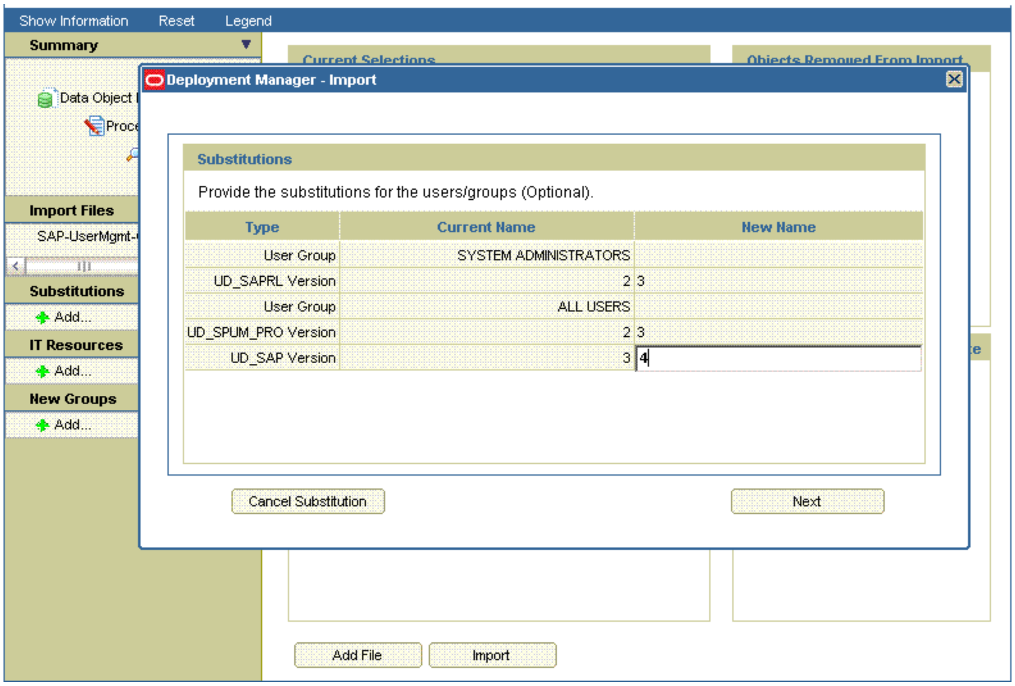
- com.thortech.xl.dataobj.tcUD_SAP
- Lookup.SAP.CUP.ProvisionAttrMap
- com.thortech.xl.dataobj.tcUD_SAPRL
- Lookup.SAP.CUP.Constants
- com.thortech.xl.dataobj.tcUD_SPUM_PRO
- SAP UM Resource Object
  - SAP UM Process Form
    - UD_SAP ⚠ ☒
      - UD_SAPRL ☒
      - UD_SPUM_PRO ☒
- Lookup.SAP.CUP.Configuration ⚠
- Lookup.SAP.CUP.ProvisionRoleAttrMap

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.

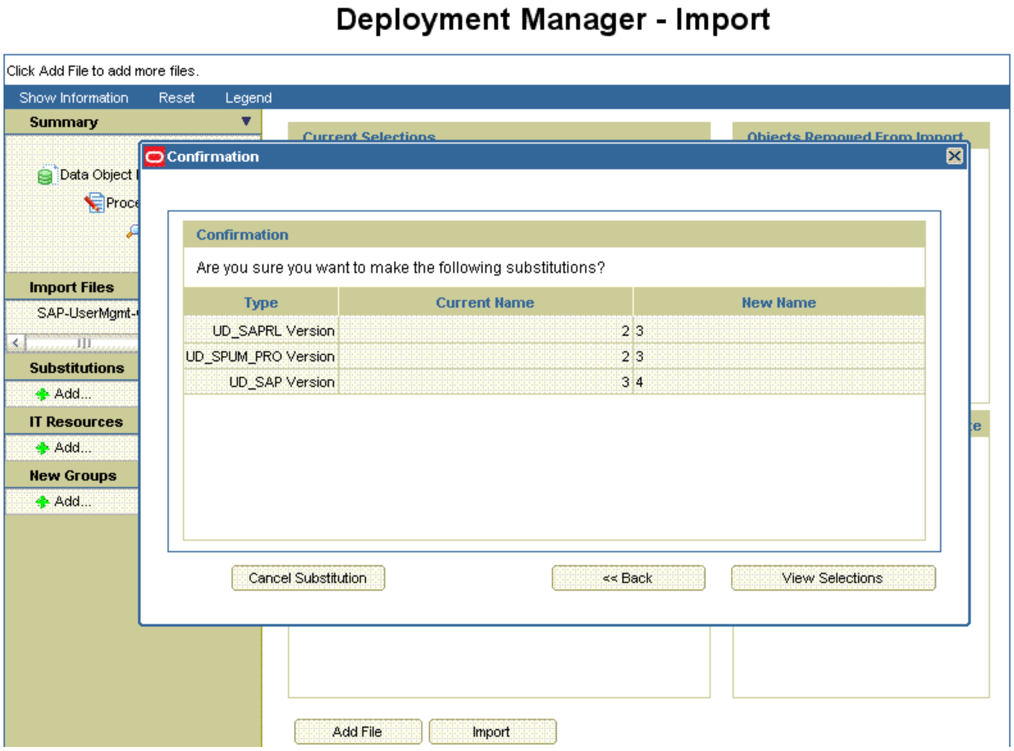


Substitutions

Provide the substitutions for the users/groups (Optional).

Type	Current Name	New Name
User Group	SYSTEM ADMINISTRATORS	
UD_SAPRL Version	2	3
User Group	ALL USERS	
UD_SPUM_PRO Version	2	3
UD_SAP Version	3	4

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


Deployment Manager - Import

Click Add File to add more files.

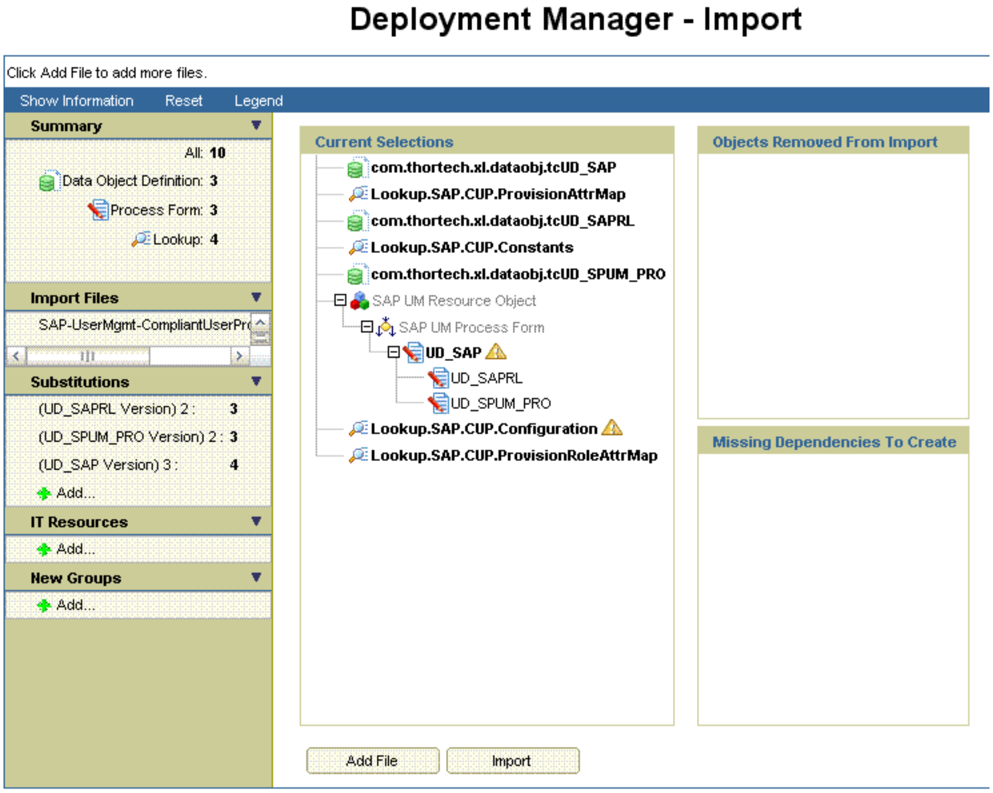
Confirmation

Are you sure you want to make the following substitutions?

Type	Current Name	New Name
UD_SAPRL Version	2	3
UD_SPUM_PRO Version	2	3
UD_SAP Version	3	4

12. Click **View Selections**.

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



All: 10
Data Object Definition: 3
Process Form: 3
Lookup: 4

SAP-UserMgmt-CompliantUserPr

(UD_SAPRL Version) 2 : 3
(UD_SPUM_PRO Version) 2 : 3
(UD_SAP Version) 3 : 4

com.thortech.xl.dataobj.tcUD_SAP
Lookup.SAP.CUP.ProvisionAttrMap
com.thortech.xl.dataobj.tcUD_SAPRL
Lookup.SAP.CUP.Constants
com.thortech.xl.dataobj.tcUD_SPUM_PRO
SAP UM Resource Object
SAP UM Process Form
UD_SAP
UD_SAPRL
UD_SPUM_PRO
Lookup.SAP.CUP.Configuration
Lookup.SAP.CUP.ProvisionRoleAttrMap

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**.

2.3.9.2 Enabling Request-Based Provisioning for the Compliant User Provisioning Feature

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 can be viewed and approved by approvers designated in Oracle Identity Manager.

> **Note:** Do *not* enable request-based provisioning if you want to use only the direct provisioning feature of the connector after enabling the Compliant User Provisioning feature.

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.

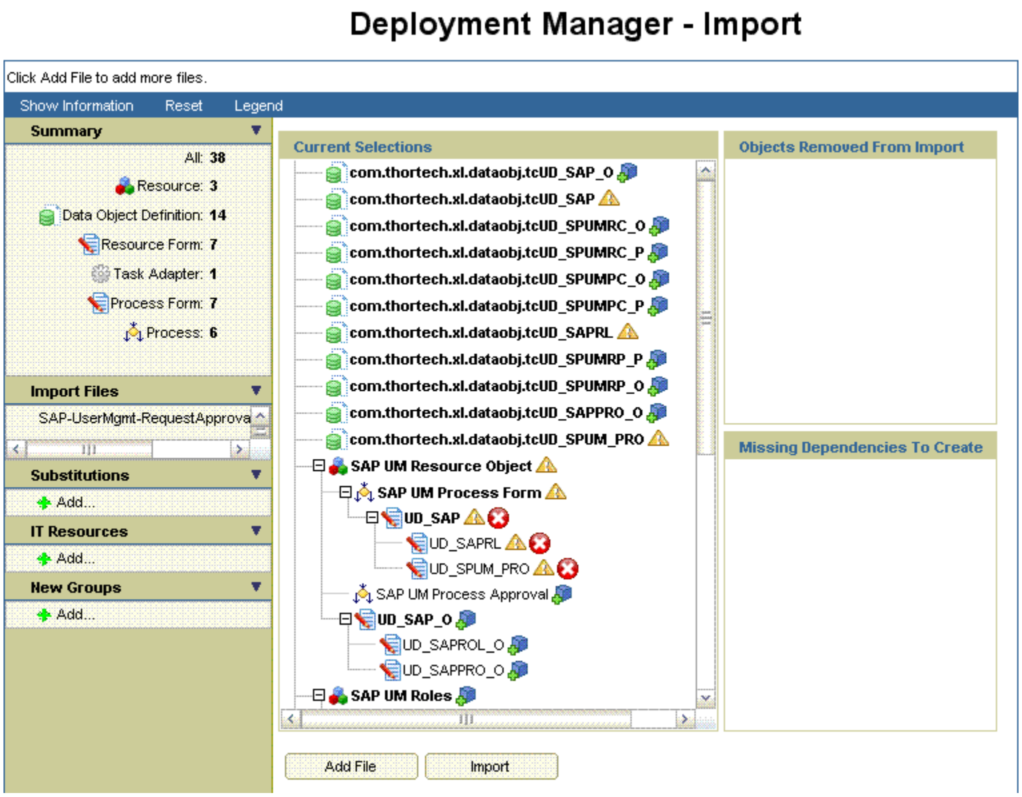
To enable request-based provisioning:

> **Note:** In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

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-CUP-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.

   The following screenshot shows this page:



Deployment Manager - Import

Click Add File to add more files.

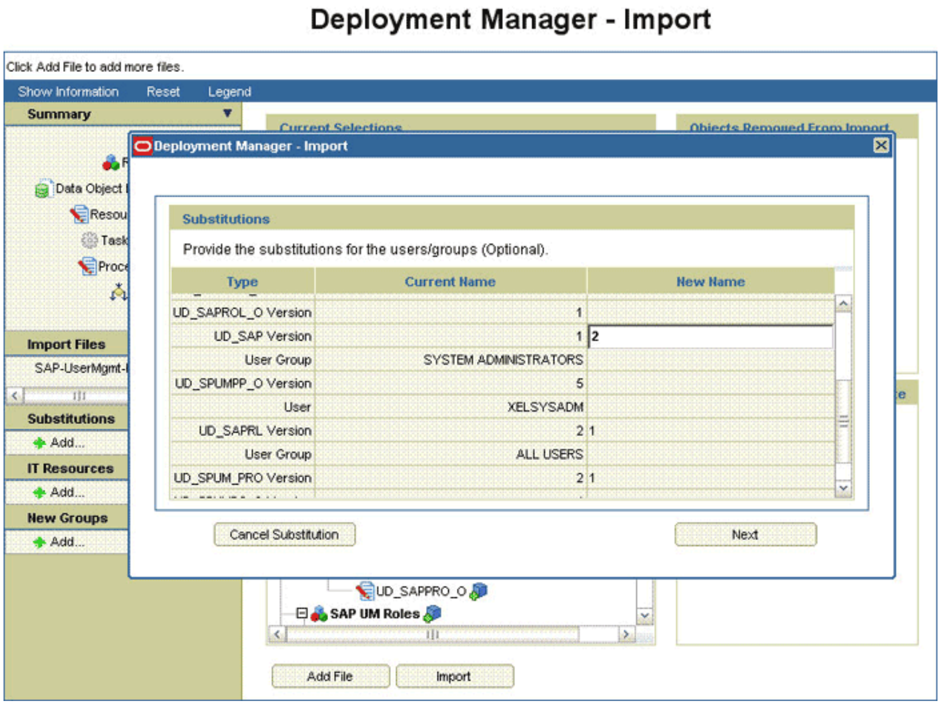
Show Information
Reset
Legend
Summary
All: 38
Resource: 3
Data Object Definition: 14
Resource Form: 7
Task Adapter: 1
Process Form: 7
Process: 6
Import Files
SAP-UserMgmt-RequestApprova
Substitutions
Add...
IT Resources
Add...
New Groups
Add...
Current Selections
com.thortech.xl.dataobj.tcUD_SAP_O
com.thortech.xl.dataobj.tcUD_SAP
com.thortech.xl.dataobj.tcUD_SPUMRC_O
com.thortech.xl.dataobj.tcUD_SPUMRC_P
com.thortech.xl.dataobj.tcUD_SPUMPC_O
com.thortech.xl.dataobj.tcUD_SPUMPC_P
com.thortech.xl.dataobj.tcUD_SAPRL
com.thortech.xl.dataobj.tcUD_SPUMRP_P
com.thortech.xl.dataobj.tcUD_SPUMRP_O
com.thortech.xl.dataobj.tcUD_SAPPRO_O
com.thortech.xl.dataobj.tcUD_SPUM_PRO
SAP UM Resource Object
SAP UM Process Form
UD_SAP
UD_SAPRL
UD_SPUM_PRO
SAP UM Process Approval
UD_SAP_O
UD_SAPROL_O
UD_SAPPRO_O
SAP UM Roles
Objects Removed From Import
Missing Dependencies To Create
Add File
Import

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

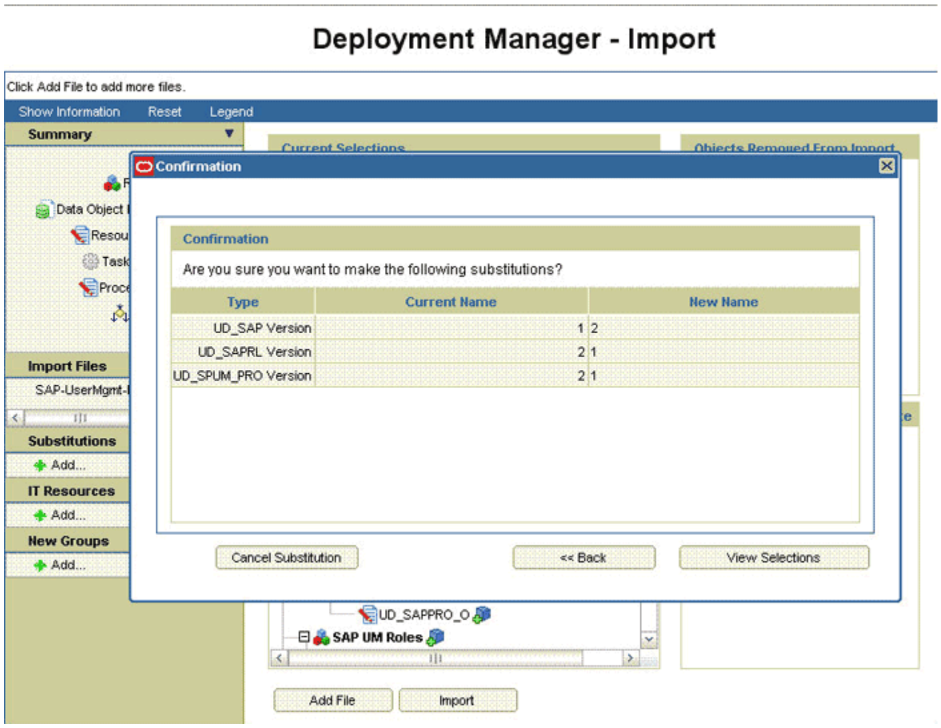
Click Add File to add more files.

Substitutions

Provide the substitutions for the users/groups (Optional).

Type	Current Name	New Name
UD_SAPROL_O Version	1	
UD_SAP Version	1	2
User Group	SYSTEM ADMINISTRATORS	
UD_SPUMPP_O Version	5	
User	XELSYSADM	
UD_SAPRL Version	2	1
User Group	ALL USERS	
UD_SPUM_PRO Version	2	1

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



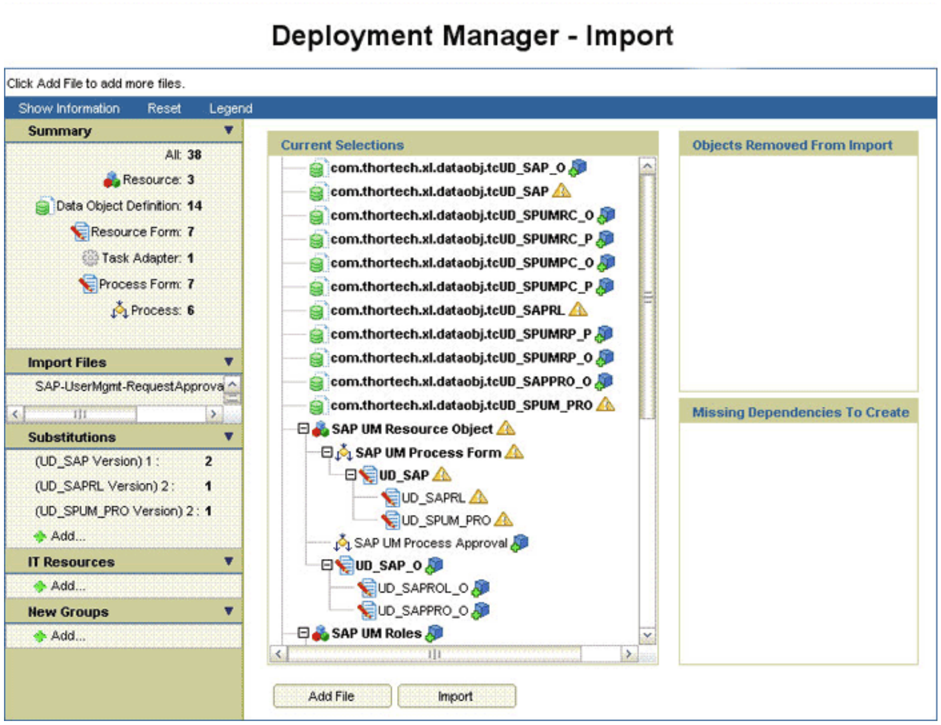
Confirmation

Are you sure you want to make the following substitutions?

Type	Current Name	New Name
UD_SAP Version	1	2
UD_SAPRL Version	2	1
UD_SPUM_PRO Version	2	1

12. Click **View Selections**.

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



Summary

All: 38
Resource: 3
Data Object Definition: 14
Resource Form: 7
Task Adapter: 1
Process Form: 7
Process: 6

Import Files

SAP-UserMgmt-RequestApprova

Substitutions

(UD_SAP Version) 1 : 2
(UD_SAPRL Version) 2 : 1
(UD_SPUM_PRO Version) 2 : 1

Current Selections

```
com.thortech.xl.dataobj.tcUD_SAP_O
com.thortech.xl.dataobj.tcUD_SAP
com.thortech.xl.dataobj.tcUD_SPUMRC_O
com.thortech.xl.dataobj.tcUD_SPUMRC_P
com.thortech.xl.dataobj.tcUD_SPUMPC_O
com.thortech.xl.dataobj.tcUD_SPUMPC_P
com.thortech.xl.dataobj.tcUD_SAPRL
com.thortech.xl.dataobj.tcUD_SPUMRP_P
com.thortech.xl.dataobj.tcUD_SPUMRP_O
com.thortech.xl.dataobj.tcUD_SAPPRO_O
com.thortech.xl.dataobj.tcUD_SPUM_PRO
⊟ SAP UM Resource Object
   ⊟ SAP UM Process Form
      ⊟ UD_SAP
           UD_SAPRL
           UD_SPUM_PRO
     SAP UM Process Approval
   ⊟ UD_SAP_O
        UD_SAPROL_O
        UD_SAPPRO_O
⊟ SAP UM Roles
```

13. Click **Import**.

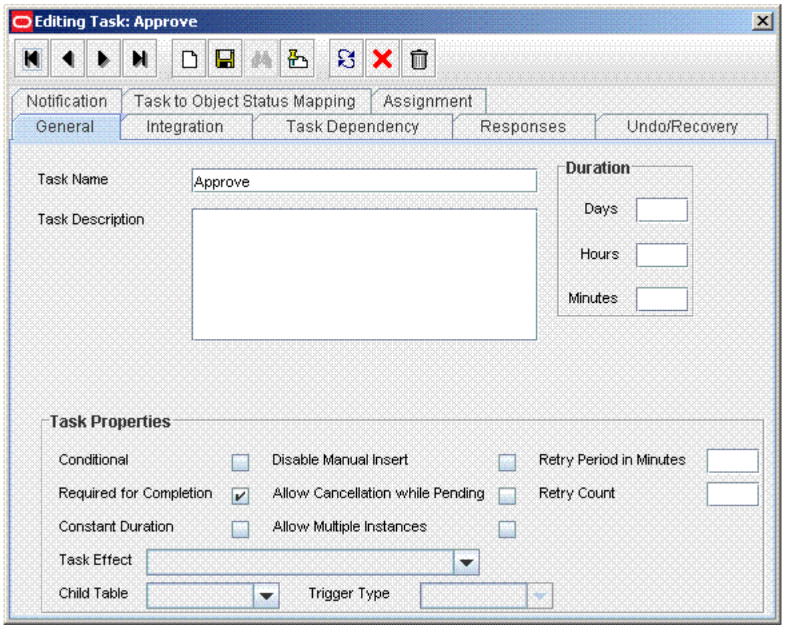
    In the message that is displayed, click **Import** to confirm that you want to import the XML file and then click **OK**.

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.

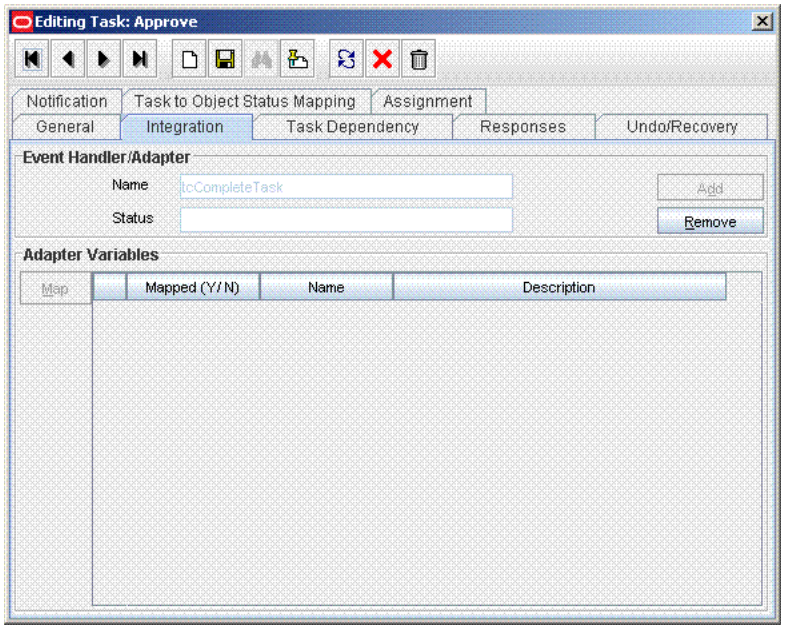


Task Name: Approve

Task Description:

Conditional	□	Disable Manual Insert	□	Retry Period in Minutes	
Required for Completion	☑	Allow Cancellation while Pending	□	Retry Count	
Constant Duration	□	Allow Multiple Instances	□		

4. On the Integration tab of the Editing Task dialog box, click **Add**.
5. In the Handler Selection dialog box:
   a. Select **System**.
   b. Select the **tcCompleteTask** handler.
   c. Click the Save icon, and then close the dialog box.



Name: tcCompleteTask

Status:

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.

2.3.9.3 Specifying Values for the SAP GRC IT Resource IT Resource

The SAP GRC IT Resource IT resource holds information that is used during communication with SAP GRC Compliant User Provisioning. To set values for the parameters of this 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 GRC IT Resource` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2–9 describes each parameter.

   Note: Entries in this table are sorted in alphabetical order of parameter names.

   Table 2–9 lists the parameters of the SAP GRC IT resource.

Table 2–4 Parameters of the SAP GRC IT Resource IT Resource

Parameter	Description
dbuser	You need not enter a value for this parameter.
dbpassword	You need not enter a value for this parameter.
jdbcURL	Enter the JDBC URL for connecting to the database used by SAP GRC. Sample value: `jdbc:oracle:thin:@10.123.123.123`
password	Enter the password of the account created on SAP GRC for API calls.
port	Enter the number of the port at which SAP GRC is listening. Sample value: `8090`
server	Enter the IP address of the host computer on which SAP GRC is running. Sample value: `10.231.231.231`
Source Datastore Name	You need not enter a value for this parameter.
sslEnable	Enter `true` if SAP GRC accepts only HTTPS communication requests. Otherwise, enter `false`. Sample value: `false`
username	Enter the user name of an account created on SAP GRC. This account is used to call SAP GRC APIs that are used during request validation. Sample value: `jdoe`

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

2.3.9.4 Specifying Values in the Lookup.SAP.UM.Configuration Lookup Definition

Specify values for the following entries in the Lookup.SAP.UM.Configuration lookup definition:

> **See Also:** Section 2.3.2.3, "Setting Values in the Lookup.SAP.UM.Configuration Lookup Definition" for information about setting up this lookup definition.

- CUP request mode: Enter `yes` to specify that you want to use the Compliant User Provisioning feature.
- Password Disabled: Enter `yes` to specify that passwords need not be specified during Create User provisioning operations. If you enter a password, then it is ignored.

2.3.9.5 Setting Up the Link with the Web Services for SAP GRC Compliant User Provisioning

To set up the link with the Web services for SAP GRC Compliant User Provisioning:

1. Search for and download the axis-bin-1_4.zip file from the following Web site:

   `http://www.apache.org`

2. Extract the contents of the axis2-1.4-bin.zip file to a temporary directory.
3. The following files are in the *TEMPORARY_DIRECTORY*/axis-1_4/lib directory:

   wsdl4j-1.5.1.jar

   axis.jar

jaxrpc.jar

saaj.jar

commons-discovery-0.2.jar

commons-logging-1.0.4.jar

Copy these JAR files into the *OIM_HOME*/xellerate/ext directory and one of the following directories:

- For IBM Websphere Application Server: *WEBSPHERE_HOME*/lib
- For JBoss Application Server: *JBOSS_HOME*/server/default/lib
- For Oracle Application Server: *ORACLE_HOME*/j2ee/home/lib
- For Oracle WebLogic Server: *WEBLOGIC_DOMAIN_HOME*/lib

4. Copy the deploy/SAPCUP.jar file from the installation media to one of the directories mentioned in the preceding step. If you are using Oracle WebLogic Server, then you must also copy the SAPCUP.jar file to the *WEBLOGIC_HOME*/wlserver_10.3/server/lib directory.

5. If Oracle Identity Manager is running on Oracle Application Server, then perform the following additional steps:

   a. In the temporary directory, extract the contents of the *ORACLE_HOME*/j2ee/home/oc4j.jar file.

   b. In a text editor, open the boot.xml file. This file is bundled in the oc4j.jar file.

   c. In the boot.xml file, add the following lines under the <system-class-loader> tag:

   ```
   <code-source path="lib/wsdl4j-1.5.1.jar"/>
   <code-source path="lib/log4j-1.2.8.jar"/>
   <code-source path="lib/saaj.jar"/>
   <code-source path="lib/axis.jar"/>
   <code-source path="lib/commons-discovery-0.2.jar"/>
   <code-source path="lib/commons-logging-1.0.4.jar"/>
   <code-source path="lib/jaxrpc.jar"/>
   <code-source path="lib/SAPCUP.jar"/>
   ```

   d. Save and close the boot.xml file.

   e. Re-create the oc4j.jar file with the updated boot.xml file bundled inside.

   f. Copy the log4j-1.2.8.jar file from the *OIM_HOME*/xellerate/ext directory into the *ORACLE_HOME*/j2ee/home/lib directory.

2.3.9.6 Configuring Request Types and Workflows on SAP GRC Compliant User Provisioning

You must create and configure request types and workflows on SAP GRC Compliant User Provisioning for provisioning operations.

The following sections describe these procedures in detail:

- Section 2.3.9.6.1, "Creating Request Types"
- Section 2.3.9.6.2, "Creating Workflows"

2.3.9.6.1 Creating Request Types

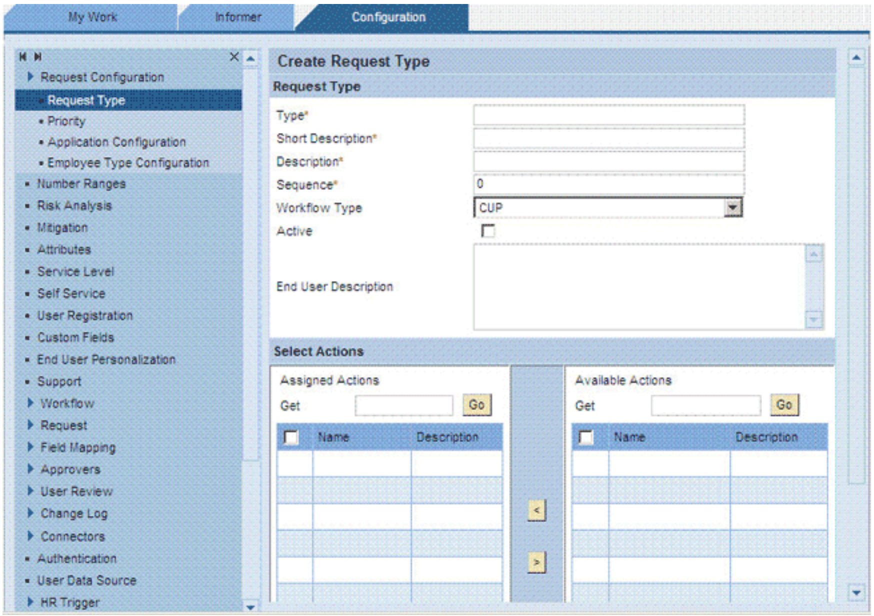
In SAP GRC Compliant User Provisioning, a request type defines the action that is performed when a request is processed. Oracle Identity Manager is a requester. It works with request types defined in SAP GRC Compliant User Provisioning. The Lookup.SAP.CUP.Configuration lookup definition maps request types to provisioning operations submitted through Oracle Identity Manager.

You can create request types in SAP GRC Compliant User Provisioning. Compliant User Provisioning also allows you to set default values for some user attributes. You can define these user defaults and then create user default mappings that specify conditions under which the user defaults must be applied.

To create a request type:

1. Log in to SAP GRC Access Control as an administrator.
2. On the Configuration tab, expand **Request Configuration**, click **Request Type**, and then click **Create**.

   The following screenshot shows this page:



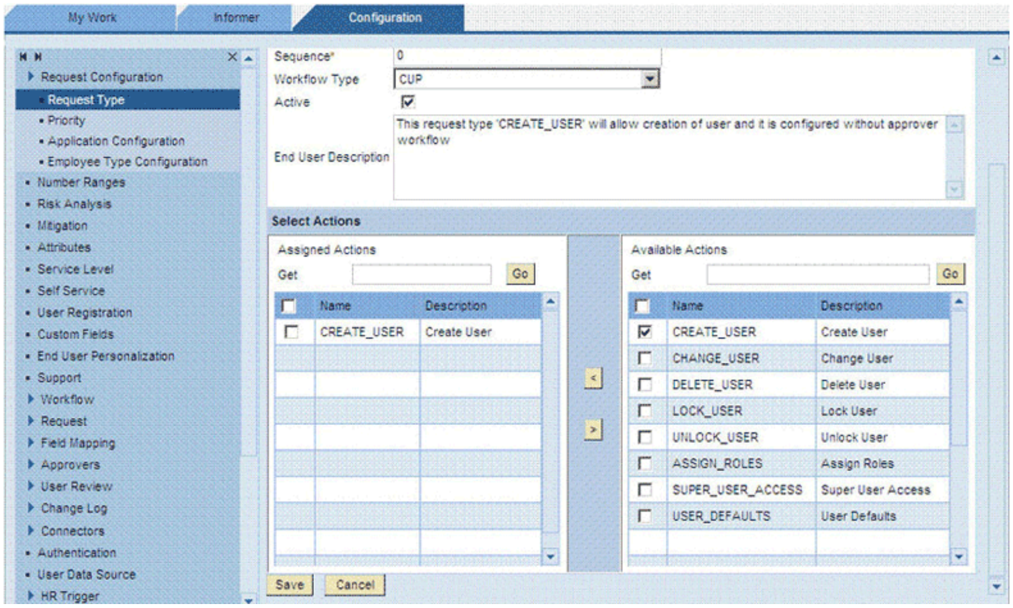
Sequence* 0

Workflow Type CUP

3. Enter the following information about the request type:
   - Type: Enter a unique name for the request type. The name must be in uppercase.
   - Short Description: Enter a short description for the request type.
   - Description: Enter a description for the request type.
   - Sequence: Enter a numeric value for the sequence in which this request type must be displayed on the Request Access page. If you assign 0, then the request type does not appear on the Request Access page. However, if the request type is Active, then it appears in the Request Type list throughout SAP GRC Compliant User Provisioning.
   - Workflow Type: Select **CUP** as the workflow type.
   - Active: Select the check box to make the request type active.
   - End User Description: Enter a description for display to users.

4. The Select Actions region displays assigned actions and available actions. Assigned actions are actions that will be performed during provisioning. Available actions are actions that are available to be performed during provisioning. You can use the arrow icons to move actions from the Available Actions list to the Assigned Actions list.

   Select an action, and then click the left arrow to assign the action.



Sequence* 0

Workflow Type CUP

Active ☑

End User Description: This request type 'CREATE_USER' will allow creation of user and it is configured without approver workflow

Select Actions

Assigned Actions

☐	Name	Description
☐	CREATE_USER	Create User

Available Actions

☐	Name	Description
☑	CREATE_USER	Create User
☐	CHANGE_USER	Change User
☐	DELETE_USER	Delete User
☐	LOCK_USER	Lock User
☐	UNLOCK_USER	Unlock User
☐	ASSIGN_ROLES	Assign Roles
☐	SUPER_USER_ACCESS	Super User Access
☐	USER_DEFAULTS	User Defaults

5. Click **Save**.

2.3.9.6.2 Creating Workflows

A workflow defined in SAP GRC Compliant User Provisioning acts upon a particular type of request. A workflow consists of an initiator, stage, and path. You can set up one workflow that contains all the request types. Alternatively, you can create a separate workflow for each request type.

An initiator is a combination of a request type and the workflow designed to handle that request type. Initiators and workflows function as matched pairs. A particular initiator can call only one workflow.

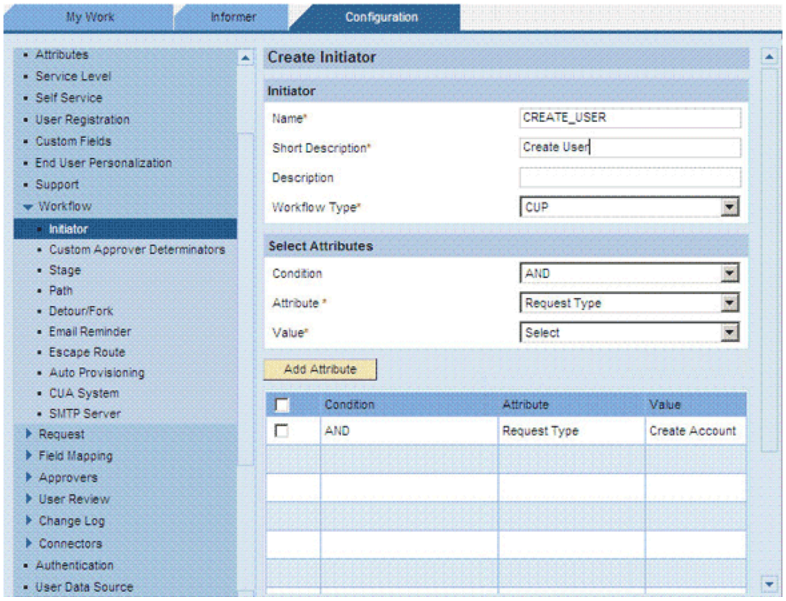
To create the initiator:

1. Log in to the SAP GRC Access Control as an administrative user.
2. On the Configuration tab, click **Workflow**, select **Initiator**, and then click **Create**.
3. Enter the following information about the initiator:
   - Name: Enter a name for the initiator. The name must be in uppercase. For example, enter `CHANGE_USER`.
   - Short Description: Enter a short description for the initiator.
   - Description: Enter a description for the initiator.
   - Workflow Type: Select **CUP** as the workflow type.
   - Select attribute information for the initiator:
   - Condition: Select **AND**, **NOT**, or **OR** as the condition. For this example, the OR condition is selected.

- Attribute: Select **Request Typ**e as the attribute.
- Value: Select a request type.

4. Click **Add Attribute**, and then repeat Step 3 for each request type that you create.
5. Click **Save**.

   The following screenshot shows this page:



Name*	CREATE_USER
Short Description*	Create User
Description	
Workflow Type*	CUP
Condition	AND
Attribute *	Request Type
Value*	Select

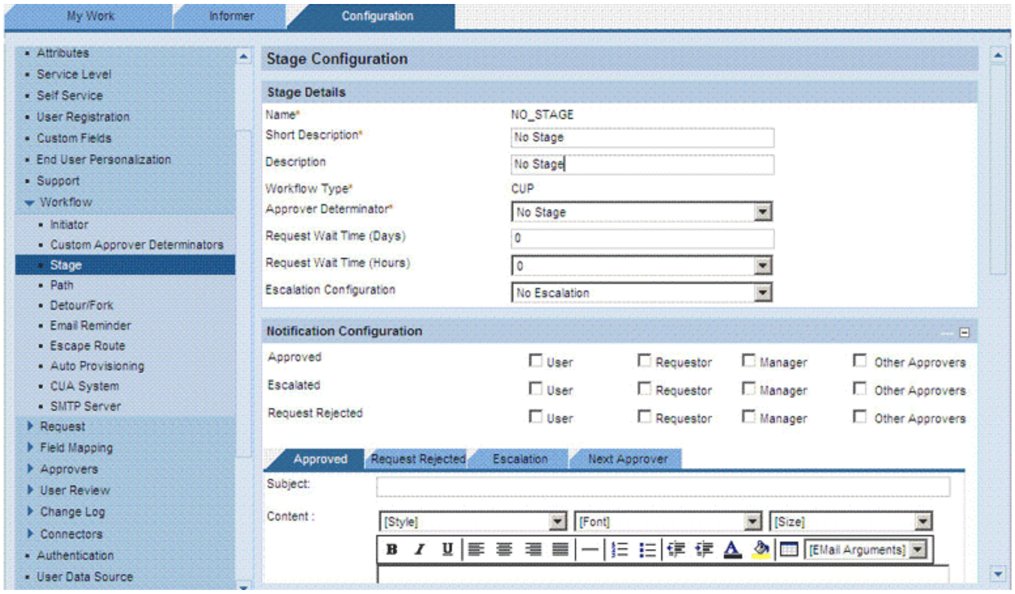
☐	Condition	Attribute	Value
☐	AND	Request Type	Create Account

A stage is a decision point in a workflow. At each stage in a workflow, an approver must approve or deny the request. The stage also specifies the action to be taken based on the decision of the approver. The request process proceeds beyond a stage only after the approver responds by approving or rejecting the request.

To create the stage:

1. Click **Workflow**, select **Stage**, and then click **Create**.
2. Enter the following information about the stage:
   - Name: Enter a name for the initiator. The name must be in uppercase, and it must not contain spaces. For example, enter `NO_STAGE`.
   - Short Description: Enter a short description for the initiator.
   - Description: Enter a description for the initiator.
   - Workflow Type: Select **CUP** as the workflow type.
   - Approver Determinator: From this list, it is recommended that you select **No Stage** for all operations other than the Add Role operation. See Section 1.3.6, "Considerations to Be Addressed When You Enable Compliant User Provisioning" for information about this guideline.

     The following screenshot shows this page:



Stage Configuration

Stage Details

Name*	NO_STAGE
Short Description*	No Stage
Description	No Stage
Workflow Type*	CUP
Approver Determinator*	No Stage
Request Wait Time (Days)	0
Request Wait Time (Hours)	0
Escalation Configuration	No Escalation

Notification Configuration

Approved	□ User	□ Requestor	□ Manager	□ Other Approvers
Escalated	□ User	□ Requestor	□ Manager	□ Other Approvers
Request Rejected	□ User	□ Requestor	□ Manager	□ Other Approvers

- Request Wait Time (Days): Enter the number of days for which Compliance User Provisioning must wait for an approver to respond to a request before escalating the request. In this example it is 0, because no escalation is configured.
- Request Wait Time (Hours): Enter the number of hours for which Compliance User Provisioning must wait for an approver to respond to a request before escalating the request. In this example it is 0, because no escalation is configured.
- Escalation Configuration: From the list, select **No Escalation**.
- Notification Configuration: Specify whether and to whom the system notifies about actions taken at this point in the stage.
- Additional Configuration: Define any additional functionality required at this stage.
- Additional Security Configuration: Specify whether or not approvers must reaffirm their actions by entering their password.

  The following actions can be configured to require password reaffirmation:

  - Approve
  - Reject
  - Create User (automatic creation of a user record)

3. Click **Save**.

A path defines the sequence of stages in a workflow. The stages in a workflow are related to other stages by the path.

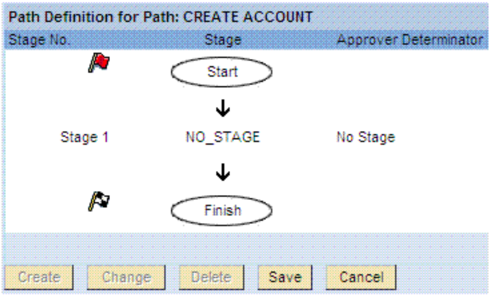
To create the path:

1. Click **Workflow**, select **Path**, and then click **Create**.
2. Enter the following information about the path:
   - Name: Enter a name for the path. The name must be in uppercase, and it must not contain spaces.
   - Short Description: Enter a short description for the path.

- Description: Enter a description for the path.
- Workflow Type: Select **CUP** as the workflow type.
- Number of Stages: Enter the number of stages that you want to include in the path.
- Initiator: From the list, select the initiator that you created earlier.
- Active: Select **Active** to make the path active.

3. Click Save to create the path.

   The following screenshot shows this page:



Path Definition for Path: CREATE ACCOUNT

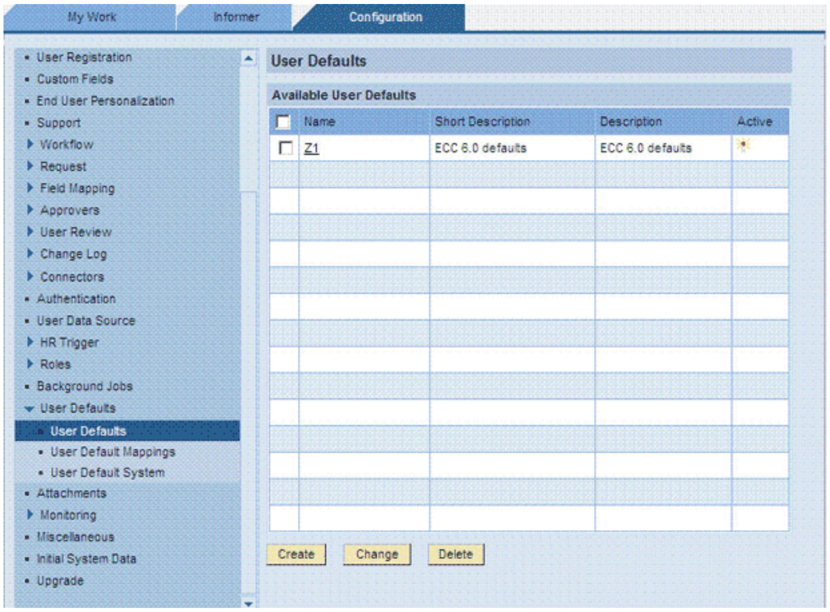
Stage No.	Stage	Approver Determinator
	Start	
Stage 1	NO_STAGE	No Stage
	Finish	

You can define a set of user defaults and also create user default mappings that define conditions under which the user defaults must be applied.

To define user defaults:

1. On the Configuration tab, expand **User Defaults** and then click **User Defaults**.

   The following screenshot shows this page:



User Defaults

Available User Defaults

□	Name	Short Description	Description	Active
□	Z1	ECC 6.0 defaults	ECC 6.0 defaults	✓

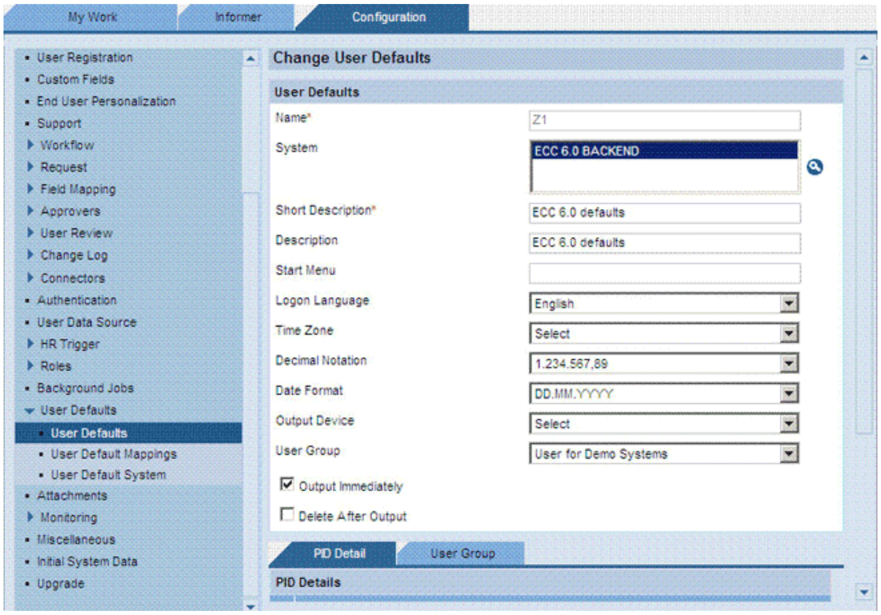
2. Enter values in the following fields:

   - Name: Enter a name for this set of user defaults.
   - System: Select the SAP R/3 or SAP CUA system.
   - Short Description: Enter a short description for this set of user defaults.

- Description: Enter a description for this set of user defaults.

3. Specify default values for the Logon Language, Time Zone, Decimal Notation, Date Format, Output Device, and User Group attributes.

   The following screenshot shows this page:



Change User Defaults

User Defaults

Name*	Z1
System	ECC 6.0 BACKEND
Short Description*	ECC 6.0 defaults
Description	ECC 6.0 defaults
Start Menu	
Logon Language	English
Time Zone	Select
Decimal Notation	1.234.567,89
Date Format	DD.MM.YYYY
Output Device	Select
User Group	User for Demo Systems

☑ Output Immediately

☐ Delete After Output

4. Click **Save**.

To define a user default mapping:

1. On the Configuration tab, expand **User Defaults** and then click **User Default Mappings**.

2. Enter values in the following fields:

   - Name: Enter a name for this set of user defaults.
   - Short Description: Enter a short description for this set of user defaults.
   - Description: Enter a description for this set of user defaults.
   - User Defaults: Select the default that you create.

3. In the Select Attributes region, use the Condition, Attribute, and Value lists to specify the attributes (conditions) under which the defaults must be applied.

   For example, suppose you select the following attributes:

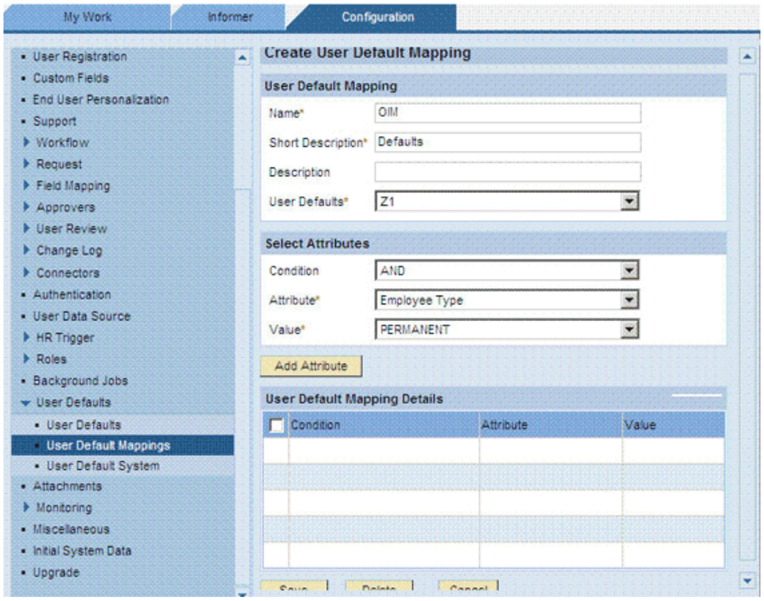
   Request Type: New

   Functional Area: Finance

   A request that has these two attributes is automatically assigned the user defaults.

4. Click **Save**.

   The following screenshot shows this page:



Create User Default Mapping

User Default Mapping

Name* OIM

Short Description* Defaults

Description

User Defaults* Z1

Select Attributes

Condition AND

Attribute* Employee Type

Value* PERMANENT

User Default Mapping Details

□	Condition	Attribute	Value

2.3.9.7 Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition

Table 2–5 describes the entries in the Lookup.SAP.CUP.Configuration lookup definition.

> **Note:** You must not change any of the Code Key values of this lookup definition.

Table 2–5 Entries in the Lookup.SAP.CUP.Configuration Lookup Definition

Code Key	Description
Application	Enter the system name of the SAP R/3 or SAP CUA installation. Sample value: `E60`
Assign Role	Enter the name of the request type that you create for Modify User provisioning operations. See Section 2.3.9.6.1, "Creating Request Types" for more information. Sample value: `MODIFY_USER`
Child Attribute Lookup	This entry holds the name of the lookup definition that stores child form attribute mappings for the Compliant User Provisioning feature. Value: `Lookup.SAP.CUP.ProvisionRoleAttrMap`
Constants Lookup	This entry holds the name of the lookup definition that stores values used by the connector in the Compliant User Provisioning feature. The connector development team can use this lookup definition to make minor configuration changes in the connector. Value: `Lookup.SAP.CUP.Constants`
Create User	Enter the name of the request type that you create for Create User provisioning operations. See Section 2.3.9.6.1, "Creating Request Types" for more information. Sample value: `CREATE_USER`

Table 2–5 (Cont.) Entries in the Lookup.SAP.CUP.Configuration Lookup Definition

Code Key	**Description**
Delete User	Enter the name of the request type that you create for Delete User provisioning operations. See Section 2.3.9.6.1, "Creating Request Types" for more information. Sample value: `DELETE_USER`
Ignore OPEN status	Use this entry to specify that new requests can be sent for a particular user, even if the last request for the user is in the Open status. If you set this entry to `yes`, then data from each new request replaces data stored from the preceding request, regardless of the status of the preceding request. If you set this entry to `no`, then new requests cannot be sent for a particular user for as long as the last request is in the Open status. Default value: `no` **Note:** If Ignore OPEN status is set to `no` and a new request is submitted for a user before an existing request for the user is closed, then a message is displayed on the Administrative and User Console. At the same time, the `Request ID xxx is in OPEN status` message is recorded in the log file.
Ignore User Created Check For Add Role	When an Add Role request is submitted through Oracle Identity Manager, the connector first checks if the specified user exists on the target system. If an approver is defined for the Create User request type and if the Add Role request is sent *immediately* after the Create User request is sent, then the process task for adding the role might be rejected. This is because the user is not created on the target system until SAP GRC Compliant User Provisioning clears the Create User request. If you want the connector to skip the check for the user on the target system during Add Role operations, then enter `yes` as the value of the Ignore User Created Check For Add Role entry. With this setting, the role is granted to the account (resource) in Oracle Identity Manager without checking if the user exists on the target system. Enter `no` as the value if you do not want to enable this feature. Default value: `yes`
IT Resource	This entry holds the name of the SAP GRC IT resource. Default value: `SAP GRC IT Resource`
Lock User	Enter the name of the request type that you create for Modify User provisioning operations. See Section 2.3.9.6.1, "Creating Request Types" for more information. Sample value: `LOCK_USER`
Modify User	Enter the name of the request type that you create for Modify User provisioning operations. See Section 2.3.9.6.1, "Creating Request Types" for more information. Sample value: `MODIFY_USER`

Table 2–5 (Cont.) Entries in the Lookup.SAP.CUP.Configuration Lookup Definition

Code Key	Description
Parent Attribute Lookup	This entry holds the name of the lookup definition that stores process form attribute mappings for the Compliant User Provisioning feature. Value: `Lookup.SAP.CUP.ProvisionAttrMap`
Priority	Enter the priority level at which SAP GRC Compliant User Provisioning must process requests sent from Oracle Identity Manager: ■ Low ■ Medium ■ High ■ Critical
Unlock User	Enter the name of the request type that you create for Modify User provisioning operations. See Section 2.3.9.6.1, "Creating Request Types" for more information. Sample value: `UNLOCK_USER`

2.3.10 Configuring SoD

This section discusses the following procedures:

- Section 2.3.10.1, "Configuring SAP GRC to Act As the SoD Engine"
- Section 2.3.10.2, "Specifying Values for SoD-Related Entries in the Lookup.SAP.UM.SoDConfiguration Lookup Definition"
- Section 2.3.10.3, "Modifying the SoD-Related Lookup Definitions"
- Section 2.3.10.4, "Specifying Values for the SAP GRC IT Resource IT Resource"
- Section 2.3.10.5, "Verifying Entries Created in the Lookup.SAP.UM.System Lookup Definition"
- Section 2.3.10.6, "Specifying a Value for the TopologyName IT Resource Parameter"
- Section 2.3.10.7, "Disabling and Enabling SoD"

> **Note:** The ALL USERS group has INSERT, UPDATE, and DELETE permissions on the UD_SAP, UD_SAPRL, and UD_SPUM_PRO 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.

2.3.10.1 Configuring SAP GRC to Act As the SoD Engine

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

2.3.10.2 Specifying Values for SoD-Related Entries in the Lookup.SAP.UM.SoDConfiguration Lookup Definition

The Lookup.SAP.UM.SoDConfiguration lookup definition holds configuration values that are used by the connector during SoD operations. Table 2–6 lists the entries in this lookup definition.

Table 2–6 Entries in the Lookup.SAP.UM.SoDConfiguration Lookup Definition

Code Key	Decode
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`. Default value: `5.3`
is CUA Enabled	Enter `yes` if the target system is SAP CUA. Enter `no` if the target system is SAP R/3. Default value: `no`
Profile name	USERPROFILE
Profile System Name	SYSTEMNAME
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. Default value: `3`
Role name	USERROLE
Role System Name	SYSTEMNAME
SAP Profile Child Object Form	UD_SPUMPC_O
SAP Profile Child Process Form	UD_SPUMPC_P
SAP Profile Object Form	UD_SAPPRO_O
SAP Profile Process Form	UD_SPUM_PRO
SAP Role Child Object Form	UD_SPUMRC_O
SAP Role Child Process Form	UD_SPUMRC_P
SAP Role Object Form	UD_SAPROL_O
SAP Role Process Form	UD_SAPRL
SOD Check Result	SODCHECKRESULT
SOD Check Status	SODCHECKSTATUS

Table 2–6 (Cont.) Entries in the Lookup.SAP.UM.SoDConfiguration Lookup Definition

Code Key	Decode
SOD Check Timestamp	SODCHECKTIMESTAMP
SOD Check Tracking ID	SODCHECKTRACKINGID
SOD Check Violation	SODCHECKVIOLATION
Systems Lookup	Lookup.SAP.UM.System
User Resource Object	SAP UM Resource Object

To specify values for the entries in the Lookup.SAP.UM.SoDConfiguration lookup definition:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAP.UM.SoDConfiguration** lookup definition.
3. Click **Add**.
4. In the Decode column, specify values for the following Code Key entries:

   - GRC version
   - is CUA Enabled
   - Risk Level

   If you create a copy of the connector, then you must also specify values for some of the other entries in this lookup definition. See Section 4.14, "Configuring the Connector for Multiple Installations of the Target System" for more information.
5. Click the Save icon.

2.3.10.3 Modifying the SoD-Related Lookup Definitions

Table 2–7 lists entries in the Lookup.SAP.UM.ProfileChildformMappings lookup definition.

Table 2–7 Entries in the Lookup.SAP.UM.ProfileChildformMappings Lookup Definition

Code Key	Decode
UD_SPUMPC_P_SYSTEMNAME	UD_SPUM_PRO_SYSTEMNAME
UD_SPUMPC_P_USERPROFILE	UD_SPUM_PRO_USERPROFILE

Table 2–8 lists entries in the Lookup.SAP.UM.RoleChildformMappings lookup definition.

Table 2–8 Entries in the Lookup.SAP.UM.RoleChildformMappings Lookup Definition

Code Key	Decode
UD_SPUMRC_P_SYSTEMNAME	UD_SAPRL_SYSTEMNAME
UD_SPUMRC_P_USERROLE	UD_SAPRL_USERROLE
UD_SPUMRC_P_VALID_FROM	UD_SAPRL_STARTDT,DATE
UD_SPUMRC_P_VALID_TO	UD_SAPRL_ENDDT,DATE

If you make changes in the child process forms, then you must also make the required changes in these lookup definitions.

2.3.10.4 Specifying Values for the SAP GRC IT Resource IT Resource

The SAP GRC IT Resource IT resource holds information that is used by the connector during SoD operations. To set values for the parameters of this IT resource:

> **Note:** This IT resource is the same as the one used by the Compliant User Provisioning feature.

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 GRC IT Resource` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2–9 describes each parameter.

   > **Note:** Entries in this table are sorted in alphabetical order of parameter names.

   Table 2–9 lists the parameters of the SAP GRC IT Resource IT resource.

Table 2–9 Parameters of the SAP GRC IT Resource IT Resource

Parameter	Description
dbuser	Enter the user name of the schema owner on the database used by SAP GRC. This account is used to access the database used by SAP GRC. Sample value: `databaseusr1`
dbpassword	Enter the password of the schema owner on the database used by SAP GRC.
jdbcURL	Enter the JDBC URL for connecting to the database used by SAP GRC. Sample value: `jdbc:oracle:thin:@10.123.123.123`
password	Enter the password of the account created on SAP GRC for API calls.
port	Enter the number of the port at which SAP GRC is listening. Sample value: `8090`
server	Enter the IP address of the host computer on which SAP GRC is running. Sample value: `10.231.231.231`

Table 2–9 (Cont.) Parameters of the SAP GRC IT Resource IT Resource

Parameter	Description
Source Datastore Name	Enter the name of the source data store (the target system) that you defined on SAP GRC. You specify a source data store name while performing the procedure described in Section 2.3.10.1, "Configuring SAP GRC to Act As the SoD Engine". Sample value: `GRCSTMD122`
sslEnable	Enter `true` if SAP GRC accepts only HTTPS communication requests. Otherwise, enter `false`. Sample value: `false`
username	Enter the user name of an account created on SAP GRC. This account is used to call the SoD engine APIs that are used during SoD validation. Sample value: `jdoe`

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

2.3.10.5 Verifying Entries Created in the Lookup.SAP.UM.System Lookup Definition

The Lookup.SAP.UM.System lookup definition is automatically populated with system names when you run lookup field synchronization. After synchronization, you must open this lookup definition and ensure that only entries for systems that you want to use for the SoD validation process are retained in this table.

2.3.10.6 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:

- 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 information about this element.

See Section 2.3.12, "Configuring the IT Resource" for information about specifying values for parameters of the IT resource.

2.3.10.7 Disabling and Enabling SoD

This section describes the procedures to disable and enable SoD.

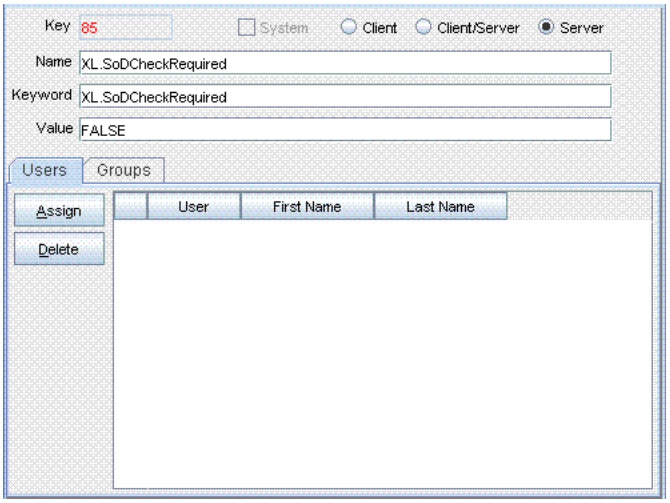
To disable SoD:

> **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.



Key 85 □ System ○ Client ○ Client/Server ● Server

Name XL.SoDCheckRequired

Keyword XL.SoDCheckRequired

Value FALSE

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.

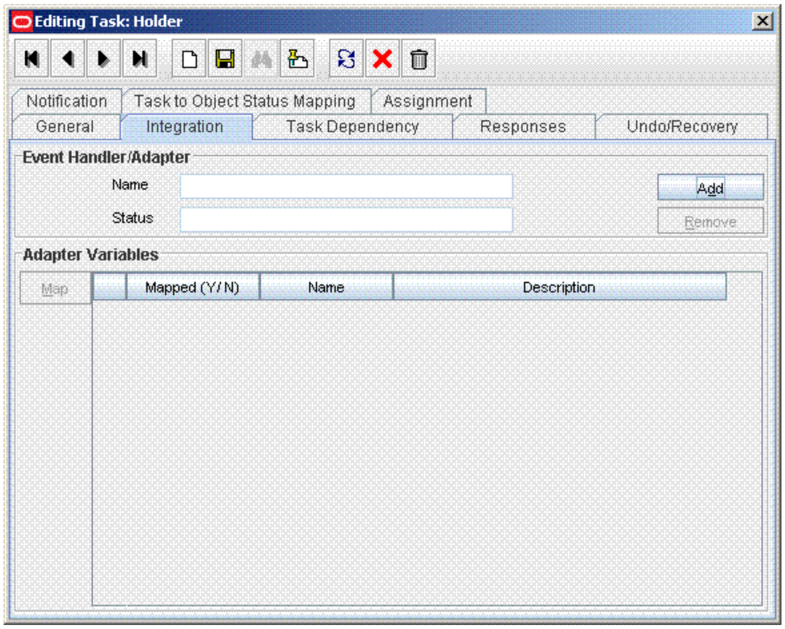
3. Disable the Holder andSODChecker process tasks as follows:

a. Expand **Process Management**, and double-click **Process Definition**.

b. Search for and open the **SAP UM Process Form** process definition.

c. On the Tasks tab, double-click the **Holder** task.

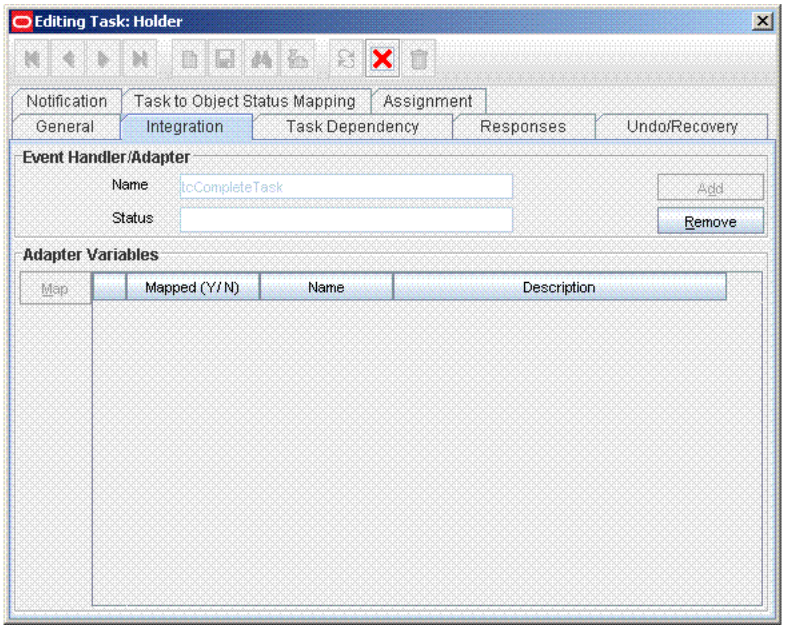
d. On the Integration tab of the Editing Task dialog box, click **Add**.



e. In the Handler Selection dialog box:

   Select **System**.

   Select the **tcCompleteTask handler**.



Name: tcCompleteTask

Status:

   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 t**cCompleteTask 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.

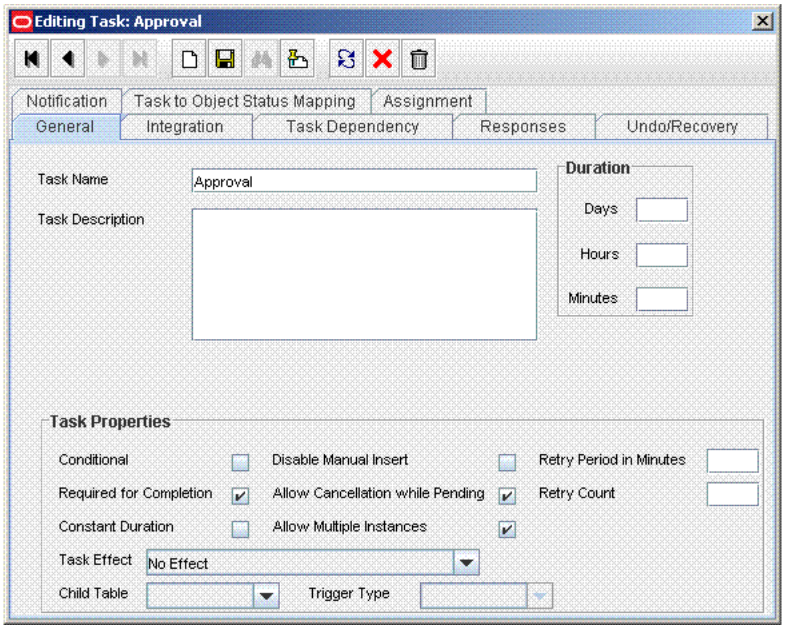
4. If you are going to perform the procedure described in Section 2.3.3, "Enabling Request-Based Provisioning", then in the SAP UM Process Approval, SAP UM Roles Approval, and SAP UM Process Approval process definitions, the human approval tasks must be made unconditional as follows:

   a. On the Design Console, expand **Process Management** and then double-click **Process Definition**.

   b. Search for and open the approval-type process definition for the connector that you are using.

   c. On the Task tab, search for the Approval task.

d. Make this task unconditional by deselecting the Conditional check box. See the following screenshot:



Task Name: Approval

Task Description:

Duration

Days:

Hours:

Minutes:

Task Properties

Conditional □

Disable Manual Insert □

Retry Period in Minutes:

Required for Completion ☑

Allow Cancellation while Pending ☑

Retry Count:

Constant Duration □

Allow Multiple Instances ☑

Task Effect: No Effect

Child Table:

Trigger Type:

e. Save the changes to the process definition.

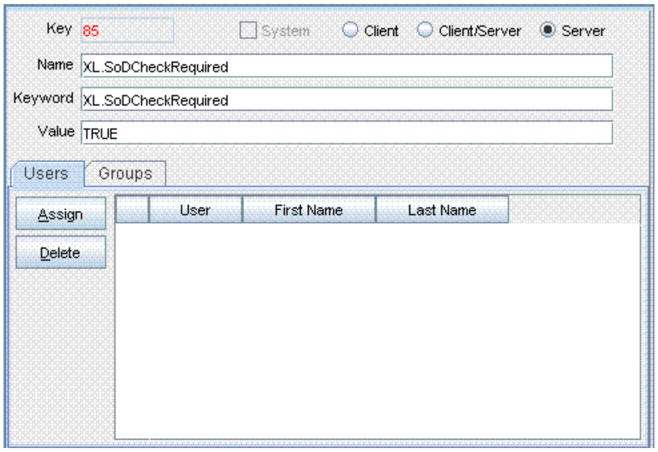
5. Restart Oracle Identity Manager.

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.



Key: 85

□ System ○ Client ○ Client/Server ● Server

Name: XL.SoDCheckRequired

Keyword: XL.SoDCheckRequired

Value: TRUE

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 andSODChecker process tasks as follows:

   a. Expand **Process Management** and double-click **Process Definition**.

   b. Search for and open the SAP UM Process Form 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.

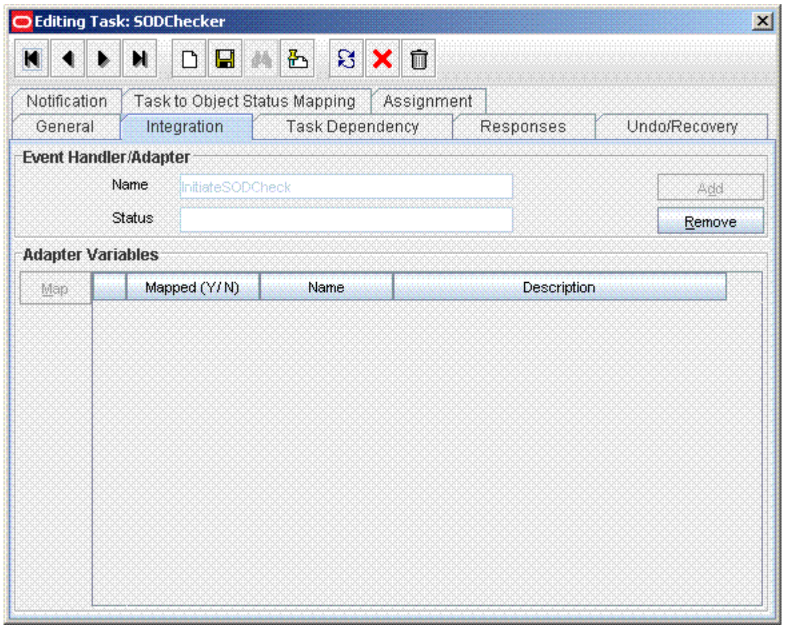
   f. On the Tasks tab, double-click **SODChecker**.

   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**.



Editing Task: SODChecker

Event Handler/Adapter

Name: InitiateSODCheck

Status:

      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.

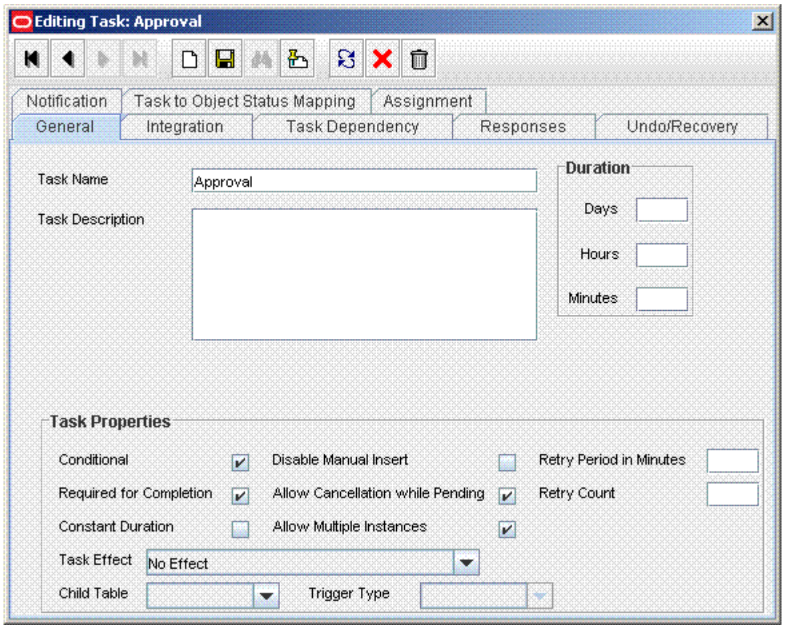
7. If you are going to perform the procedure described in Section 2.3.3, "Enabling Request-Based Provisioning", then in the SAP UM Process Approval, SAP UM Roles Approval, and SAP UM Process Approval process definitions, the human approval tasks must be made conditional as follows:

   a. Expand **Process Management**, and then double-click **Process Definition**.

b. Search for and open the approval-type process definition for the connector that you are using.

c. On the Task tab, search for the **Manager Approval** task.

d. Make this task conditional by selecting the **Conditional** check box. See the following screenshot:



Task Name: Approval

Task Description:

Duration
Days:
Hours:
Minutes:

Task Properties

Conditional ☑
Disable Manual Insert □
Retry Period in Minutes:
Required for Completion ☑
Allow Cancellation while Pending ☑
Retry Count:
Constant Duration □
Allow Multiple Instances ☑
Task Effect: No Effect
Child Table:
Trigger Type:

e. Save the changes to the process definition.

8. Restart Oracle Identity Manager.

2.3.11 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 communication between Oracle Identity Manager and the SAP system.

> **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 2.3.11.1, "Prerequisites for Configuring the Connector to Use SNC"
- Section 2.3.11.2, "Installing the Security Package"
- Section 2.3.11.3, "Configuring SNC"

2.3.11.1 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.

2.3.11.2 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 2.3.11.3, "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 and PATH environment variables for the user of the Java application server to the cryptographic library directory, which is the parent directory of the sec directory.

2.3.11.3 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:

   ```
   Sapgenpse 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 UM IT Resource IT resource object:

   - SAP lib
   - SAP mode
   - SAP myname
   - SAP partnername
   - SAP qop

2.3.12 Configuring the IT Resource

The following sections provide information about features that can be enabled using the IT resource:

- Section 2.3.12.1, "Parameters for Enabling the Use of a Logon Group"
- Section 2.3.12.2, "Parameters for Enabling SNC-Based Communication"
- Section 2.3.12.3, "Parameters for Enabling Multiple Attempts to Update Multivalued Attributes"
- Section 2.3.12.4, "Mapping New Connection Properties"

The following section describes the parameters of the IT resource:

- Section 2.3.12.5, "Specifying Values for the IT Resource Parameters"

2.3.12.1 Parameters for Enabling the Use of a Logon Group

In SAP, a logon group is used as a load-sharing mechanism. When a user logs in to a logon group, the system internally routes the connection request to the logon group member with the least load.

The following parameters of the IT resource are used to enable this feature. These parameters are explained in Table 2–11.

- App server host
- Logon group name
- Message server
- R3 name

In addition, perform the following procedure on the Oracle Identity Manager host computer to enable SAP JCo connectivity:

1. Open the following file in a text editor:

   For Microsoft Windows:

   C:\WINDOWS\system32\drivers\etc\services

   For Solaris or Linux, open the following file:

   /etc/services

2. Add an entry in the following format:

   > **Note:** Ensure that you add the entry in the correct ascending order of the port number as shown in the example.

   ```
   sapmsSYSTEM_ID         36SYSTEM_NUMBER/tcp
   ```

   For example:

   ```
   . . .
   ipx             213/udp             #IPX over IP
   ldap            389/tcp             #Lightweight Directory Access Protocol
   sapmsE60        3600/tcp
   . . .
   ```

3. Save and close the file.

4. Create the sapmsg.ini file and add the following lines in the file:

   ```
   [Message Server]
   o01=oss001.wdf.sap-ag.de
   SYSTEM_ID=HOST_NAME
   ```

   For example:

   ```
   [Message Server]
   o01=oss001.wdf.sap-ag.de
   E60=mysap08.corp.example.com
   ```

5. Save and close the file.

6. On the Oracle Identity Manager host computer, copy the file into the C:\Windows directory or the root directory (depending on the operating system running on the host).

2.3.12.2 Parameters for Enabling SNC-Based Communication

Secure Network Communication (SNC) is the SAP-proprietary mechanism for securing communication between SAP and applications with which SAP interacts. See Section 2.3.11, "Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System" for detailed information to enable SNC-based communication. The names of the SNC parameters are prefixed with `SNC`.

2.3.12.3 Parameters for Enabling Multiple Attempts to Update Multivalued Attributes

During provisioning operations, there is a possibility that more than one user tries to update the multivalued attribute (for example, a role) of a particular user. The following parameters of the IT resource are used to automatically manage simultaneous update attempts:

- Timeout count: Enter the time (in milliseconds) for which the connector must wait before retrying the operation to update a multivalued attribute on the target system.
- Timeout retry count: Enter the maximum number of retry attempts for updating a multivalued attribute on the target system.

2.3.12.4 Mapping New Connection Properties

The IT resource holds connection properties that are used by SAP JCo. These connection properties are the ones accepted by the SAP JCo. The Lookup.SAP.UM.ITResourceMapping lookup definition holds mappings between the connection properties accepted by the SAP JCo API and the names of IT resource parameters.

Note: See the Javadocs shipped with SAP JCo 3.0 for detailed information about connection properties used by the target system.

To meet the requirements of your operating environment, you might need to add connection properties to this default set of properties. For example, if the target system is behind a firewall, then you must also provide a value for the jco.client.saprouter connection property. To add a connection property, see Section 2.3.12.4, "Mapping New Connection Properties".

See Also: *Oracle Identity Manager Design Console Guide* for more information about this procedure

To map a new connection property:

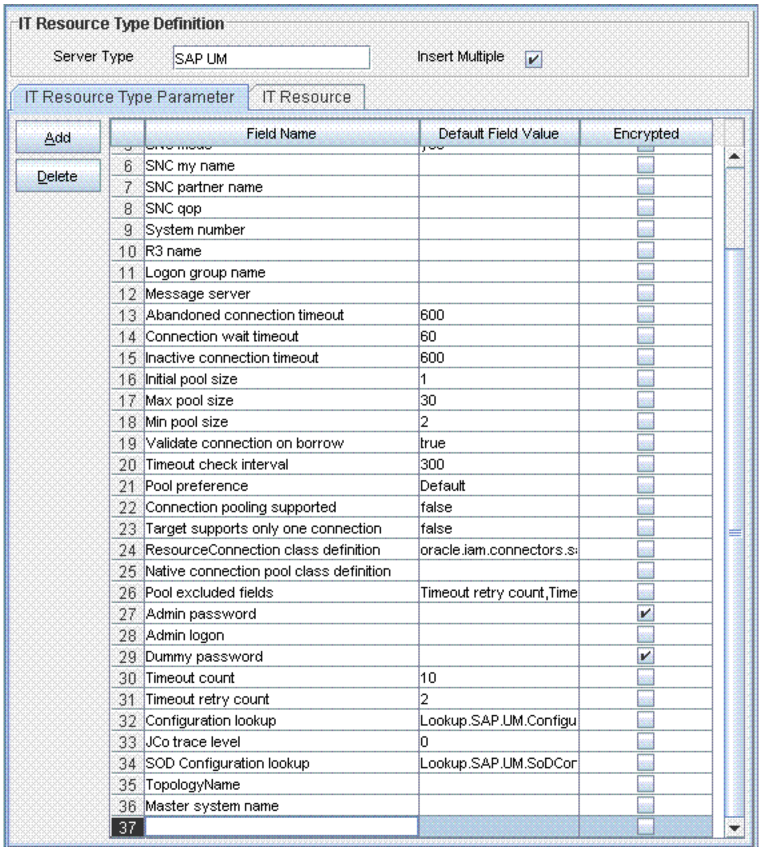
1. Add the connection property as a parameter in the SAP UM IT resource type definition as follows:

   a. On the Design Console, expand **Resource Management**, and then click **IT Resources Type Definition**.

   b. Search for and open the **SAP UM** IT resource type.

   c. Click **Add**.

   A new row is displayed in the IT Resource Type Parameter table.



IT Resource Type Definition

Server Type: SAP UM

Insert Multiple ☑

	Field Name	Default Field Value	Encrypted
6	SNC my name		□
7	SNC partner name		□
8	SNC qop		□
9	System number		□
10	R3 name		□
11	Logon group name		□
12	Message server		□
13	Abandoned connection timeout	600	□
14	Connection wait timeout	60	□
15	Inactive connection timeout	600	□
16	Initial pool size	1	□
17	Max pool size	30	□
18	Min pool size	2	□
19	Validate connection on borrow	true	□
20	Timeout check interval	300	□
21	Pool preference	Default	□
22	Connection pooling supported	false	□
23	Target supports only one connection	false	□
24	ResourceConnection class definition	oracle.iam.connectors.s	□
25	Native connection pool class definition		□
26	Pool excluded fields	Timeout retry count,Time	□
27	Admin password		☑
28	Admin logon		□
29	Dummy password		☑
30	Timeout count	10	□
31	Timeout retry count	2	□
32	Configuration lookup	Lookup.SAP.UM.Configu	□
33	JCo trace level	0	□
34	SOD Configuration lookup	Lookup.SAP.UM.SoDCor	□
35	TopologyName		□
36	Master system name		□
37			□

d. In the **Field Name** column, enter a name for the parameter.

e. Do not enter values in any other field.

f. Click the Save icon.

2. Specify a value for the new parameter in the IT resource. See Section 2.3.12.5, "Specifying Values for the IT Resource Parameters" for instructions.

3. In the Lookup.SAP.UM.ITResourceMapping lookup definition, create a mapping between the connection property and the IT resource parameter as follows:

   a. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.

   b. Search for and open the **Lookup.SAP.UM.ITResourceMapping** lookup definition.

   c. Click **Add**.

   d. In the **Code Key** column, enter the connection property defined in the ServerDataProvider or DestinationDataProvider interface of SAP JCo 3.0

   Table 2–10 lists the default entries in this lookup definition.

   Note: If you enable connection pooling, then you cannot create custom entries in this lookup definition.

Table 2–10 Entries in the Lookup.SAP.UM.ITResourceMapping Lookup Definition

SAP JCo Parameter	IT Resource Parameter
jco.client.ashost	App server host
jco.client.client	Client logon
jco.client.group	Logon group name
jco.client.lang	Language
jco.client.mshost	Message server
jco.client.passwd	Admin password
jco.client.r3name	R3 name
jco.client.snc_lib	SNC lib
jco.client.snc_mode	SNC mode
jco.client.snc_myname	SNC my name
jco.client.snc_partnername	SNC partner name
jco.client.snc_qop	SNC qop
jco.client.sysnr	System number
jco.client.trace	JCo trace level
jco.client.user	Admin logon

e. In the **Decode** column, enter the name of the IT resource parameter

f. Click the Save icon.

2.3.12.5 Specifying Values for the IT Resource Parameters

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.

You must use the Administrative and User Console to configure the IT resource. Values set for the connection pooling parameters will not take effect if you use the Design Console to configure 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. Table Table 2–11 describes each parameter.

> **Note:** Entries in this table are sorted in alphabetical order of parameter names.

Table 2–11 Parameters of the IT Resource

Parameter	Description
Admin logon	Enter the user ID of the target system user account that you create for connector operations See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for more information.
Admin password	Enter the password of the target system user account that you create for connector operations See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for more information.
App server host	If the target system provides the logon groups feature, then enter the system name as the value of this parameter. Otherwise, enter the host name or IP address of the target system.
Client logon	Enter the client ID of the target system.
Configuration Lookup	This parameter holds the name of the lookup definition containing configuration information. Value: `Lookup.SAP.UM.Configuration`
Dummy password	Enter the dummy password that you want the connector to use during a Create User provisioning operation. The connector first sets the password as this value and then changes it to the password specified on the process form. See Section 2.3.2.2, "Configuring Password Changes for Newly Created Accounts" for more information about this parameter.
JCo trace level	Enter a trace level from 0 through 10. The amount of data that is traced increases with the trace level that you select. In addition, a particular trace level also contains all the trace data from the lower trace levels. See the "Java Connectivity" section on the following Web site for more information about the JCo trace level parameter: `http://wiki.sdn.sap.com` Default value: `0`
Language	Enter the two-letter code for the language set on the target system. See Section 2.3.8, "Setting Up the Lookup.SAP.UM.LookupMappings and Lookup.SAP.CUA.LookupMappings Lookup Definitions" for more information.
Logon group name	Enter the name of the SAP R/3 or SAP CUA group.
Master system name	Enter the RFC Destination value that is used for identification of the SAP system.
Message server	Enter the host name of the message server.
R3 name	Enter the host name of the SAP R/3 or SAP CUA system.
SNC lib	Enter the full path and name of the crypto library on the target system host computer. This is required only if SNC is enabled. Sample value: `c://usr//sap/sapcrypto.dll`

Table 2–11 (Cont.) Parameters of the IT Resource

Parameter	Description
SNC mode	If SNC is enabled on the SAP server, then set this field to `yes`. Otherwise, set it to `no`. **Note:** It is recommended that you enable SNC to secure communication with the target system. Default value: `yes`
SNC my name	SNC system name Specify a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Manager. Sample value: `p:CN=TST,OU=SAP, O=ORA,c=IN`
SNC partner name	Enter the domain name of the target system host computer. Specify a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Manager. Sample value: `p:CN=I47,OU=SAP, O=ORA, c=IN`
SNC qop	Enter the protection level (quality of protection, QOP) at which data is transferred. The value can be any one of the following numbers: ■ 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. Default value: `3`
SOD Configuration lookup	This parameter holds the name of the lookup definition that stores configuration information for SAP GRC. Value: Lookup.SAP.UM.SoDConfiguration
System number	Enter the system number of the SAP R/3 or SAP CUA installation. You need not enter a value for this parameter if you are using a logon group. However, you must enter a value if you are not using a logon group.
Timeout count	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. See Section 2.3.12.3, "Parameters for Enabling Multiple Attempts to Update Multivalued Attributes" for more information. Default value: 10
Timeout retry count	Enter the number of times the connector method that is trying to add a role or profile to a user must be retried. See Section 2.3.12.3, "Parameters for Enabling Multiple Attempts to Update Multivalued Attributes" for more information. Default value: 2
TopologyName	Enter the value of the Topology Name element in the SIL configuration file. This parameter is used by the SoD feature. See *Oracle Identity Manager Tools Reference* for more information. Sample value: `oim1-grc1-sap1`
Connection Pooling Parameters	

Table 2–11 (Cont.) Parameters of the IT Resource

Parameter	Description
Abandoned connection timeout	Enter the time (in seconds) after which a connection must be automatically closed if it is not returned to the pool. **Note:** You must set this parameter to a value that is high enough to accommodate processes that take a long time to complete (for example, full reconciliation). Default value: `600`
Connection pooling supported	Enter `true` if you want to enable connection pooling for this target system installation. Otherwise, enter `false`. Default value: `false`
Connection wait timeout	Enter the maximum time (in seconds) for which the connector must wait for a connection to be available. Default value: 60
Inactive connection timeout	Enter the time (in seconds) of inactivity after which a connection must be dropped and replaced by a new connection in the pool. Default value: 600
Initial pool size	Enter the number of connections that must be established when the connection pool is initialized. The pool is initialized when it receives the first connection request from a connector. Default value: 1 Sample value: 3
Max pool size	Enter the maximum number of connections that must be established in the pool at any point of time This number includes the connections that have been borrowed from the pool. Default value: 100 Sample value: 30
Min pool size	Enter the minimum number of connections that must be in the pool at any point of time. This number includes the connections that have been borrowed from the pool. Default value: 5
Native connection pool class definition	This parameter holds the name of the wrapper to the native pool mechanism that implements the GenericPool. **Note:** Do not specify a value for this parameter.
Pool excluded fields	This parameter holds a comma-separated list of IT parameters whose change must not trigger a refresh of the connector pool. Value: `Timeout retry count,Timeout count,Configuration lookup,Dummy password,SOD Configuration lookup,TopologyName` **Note:** Do not change the value of this parameter unless you are adding or deleting a parameter from the IT resource. You must ensure that the total length of the list does not exceed 2000 characters. If you are adding a parameter to the IT resource, then that parameter name must be added to the above list with a comma separator. If you are deleting a parameter from the IT resource, then that parameter must be removed from the list if it exists in the list. You must restart Oracle Identity Manager for changes that you make to this parameter to take effect.
Pool preference	This parameter specifies the preferred connection pooling implementation. Value: `Default` **Note:** Do not change this value of this parameter.

Table 2–11 (Cont.) Parameters of the IT Resource

Parameter	Description
ResourceConnection class definition	This parameter holds the name of the implementation of the ResourceConnection class. Value: `oracle.iam.connectors.sap.common.connection.SAPResourceImpl` **Note:** Do not change the value of this parameter.
Target supports only one connection	This parameter indicates whether the target system can support one or more connections at a time. Value: `false` **Note:** Do not change the value of this parameter.
Timeout check interval	Enter the time interval (in seconds) at which the other timeouts specified by the other parameters must be checked Default value: 30
Validate connection on borrow	Specify whether or not a connection must be validated before it is lent by the pool. The value can be `true` or `false`. It is recommended that you set the value to `true`. Default value: `false`

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

2.3.13 Addressing the Issue Related to Non-Unique Values in Lookup Definitions Synchronized with the Target System

If Decode values in a lookup definition are not unique, then the wrong Code Key value might be saved in Oracle Identity Manager. This known issue in Oracle Identity Manager will be fixed when you deploy the Oracle Identity Manager release 9.1.0.2 bundle patch that addresses Bug 9237745.

Note: The bundle patch that addressed Bug 9237745 had not been released at the time of release of this connector.

To work around this issue, use the Transformation of Lookup Field Data feature of the connector as follows:

See Also: Section 1.4.17, "Transformation of Lookup Field Data"

1. Copy the Sample/TransformLookup1.java file from the installation media to a temporary directory.
2. Create a JAR file out of this Java file, and place the JAR file in the *OIM_HOME*/xellerate/ScheduleTask directory.
3. Open the Lookup.SAP.UM.Configuration lookup definition, and set the value of the Use Transformation For Lookup Recon entry to yes.
4. Open the Lookup.SAP.UM.LookupReconTransformation lookup definition, and add the following row:

   Code Key: ALL

   Decode: oracle.iam.connectors.common.transform.TransformLookup1

When you run lookup field synchronization, the Java program appends Code Key values to the Decode values. This ensures the uniqueness of each entry in the Decode column. The procedure to run lookup field synchronization is described later in this guide.

3 Using the Connector

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.

3.1 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Manager.

To perform a full reconciliation run, set the Last Execution Timestamp attribute of the SAP User Management User Recon and SAP User Management Delete Recon scheduled tasks to `0`. At the end of the reconciliation run, this attribute is automatically set to the time stamp at which the run started. From the next run onward, only records created or modified after this time stamp value are considered for reconciliation.

3.2 Scheduled Task for Lookup Field Synchronization

The SAP User Management Lookup Recon scheduled task is used for lookup field synchronization. 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 User Management Lookup Recon Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SAP UM IT Resource`
Lookup Name	Enter `Lookup.SAP.UM.LookupMappings` if the target system is SAP R/3. Enter `Lookup.SAP.CUA.LookupMappings` if the target system is SAP CUA. Default value: `Lookup.SAP.UM.LookupMappings`
Schedule Task Name	This attribute holds the name of the scheduled task. Value: `SAP User Management Lookup Recon`

3.3 Guidelines on Performing Reconciliation

Apply the following guidelines while configuring reconciliation:

- On SAP CUA, an account that is directly created on the target system must be assigned a master system before changes to that account can be detected and brought to Oracle Identity Manager during reconciliation.
- On a Microsoft Windows platform, if you encounter the org.quartz.SchedulerException exception during a reconciliation run, then download and install the Microsoft Visual C++ 2005 SP1 Redistributable Package from the Microsoft Web site.

3.4 Configuring Reconciliation

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

- Section 3.4.1, "Full Reconciliation vs. Incremental Reconciliation"
- Section 3.4.2, "Limited Reconciliation"
- Section 3.4.3, "Reconciliation Scheduled Tasks"

3.4.1 Full Reconciliation vs. Incremental Reconciliation

The Last Execution Timestamp attribute of the scheduled task 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 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.

3.4.2 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current incremental reconciliation run. For full reconciliation, all target system records are fetched into Oracle Identity Manager.

You can configure limited reconciliation to specify the subset of target system records that must be fetched into Oracle Identity Manager.

You configure limited reconciliation by specifying a query condition as the value of the Custom Query attribute of the SAP User Management User Recon scheduled task.

You must use the following format to specify a value for the Custom Query attribute:

```
RESOURCE_OBJECT_FIELD_NAME=VALUE
```

For example, suppose you specify the following as the value of the Custom Query attribute:

```
Last Name=Doe
```

With this query condition, only records for users whose last name is Doe are considered for reconciliation.

You can add multiple query conditions by using the ampersand (&) as the AND operator and the vertical bar (|) as the OR operator. For example, the following query condition is used to limit reconciliation to records of those users whose first name is John and last name is Doe:

```
First Name=John  & Last Name=Doe
```

> **Note:** This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure limited reconciliation:

1. Ensure that the attribute that you want to use in the query exists in the Lookup.SAP.UM.ReconAttrMap lookup definition.

   See Also: Table 1–4, " Entries in the Lookup.SAP.UM.ReconAttrMap Lookup Definition"

   If there is no entry in this lookup definition for the attribute that you want to use, then create an entry. See Section 4.2, "Adding New Attributes for Reconciliation" for more information.

2. Create the query condition. Apply the following guidelines to create the query condition:

   - Use only the equal sign (=), ampersand (&), and vertical bar (|) in the query condition. If any other special character is included, then it is treated as part of the attribute value that you specify.
   - Add a space before and after ampersands and vertical bars used in the query condition. For example:

     ```
     First Name=John & Last Name=Doe
     ```

This is to help the system distinguish between ampersands and vertical bars used in the query and the same characters included as part of attribute values specified in the query condition.

- 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 is not the same:

  ```
  First Name=John & Last Name=Doe
  ```

  ```
  First Name= John & Last Name= 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.

- Ensure that attribute names that you use in the query condition are in the same case (uppercase and lowercase) as the case of values in the Lookup.SAP.UM.ReconAttrMap lookup definition. For example, the following query condition would fail:

  ```
  fiRst Name = John
  ```

3. While configuring the SAP User Management User Recon scheduled task, specify the query condition as the value of the Custom Query attribute. The procedure is described later in this chapter.

3.4.3 Reconciliation Scheduled Tasks

You must specify values for the attributes of the following scheduled tasks:

> **Note:** Attribute values are predefined in the connector XML file that you import. Specify values only for the attributes that you want to change.

- Section 3.4.3.1, "SAP User Management User Recon"
- Section 3.4.3.2, "SAP User Management Delete Recon"
- Section 3.4.3.3, "SAP CUP Status Update Recon"
- Section 3.4.3.4, "SAP CUP Delete Recon"

3.4.3.1 SAP User Management User Recon

You use the SAP User Management User Recon scheduled task to reconcile user data from the target system. Table 3–2 describes the attributes of this scheduled task.

Table 3–2 Attributes of the SAP User Management User Recon Scheduled Task

Attribute	Description
Attribute Mapping Lookup	This attribute holds the name of the lookup definition that stores attribute mappings for reconciliation. Value: `Lookup.SAP.UM.ReconAttrMap`
Batch Size	Enter the number of records that must be included in each batch fetched from the target system during a reconciliation run. This attribute is used to implement batched reconciliation. Default value: `100`
Child Attribute Mapping Lookup	This attribute holds the name of the lookup definition that stores child attribute mappings for reconciliation. Value: `Lookup.SAP.UM.ReconChildAttrMap`
Custom Query	Enter the query that you want the connector to apply during reconciliation. See Section 3.4.2, "Limited Reconciliation" for more information.
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SAP UM IT Resource`
Last Execution Timestamp	This attribute holds the time stamp at which the last reconciliation run started. For the next reconciliation run, only target system records that have been added or modified after this time stamp are considered for reconciliation. For consecutive reconciliation runs, the connector automatically enters a value for this attribute. However, you can use this attribute to switch from incremental reconciliation to full reconciliation. See Section 3.4.1, "Full Reconciliation vs. Incremental Reconciliation" for more information. Default value: `0`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP UM Resource Object`
SAP System Time Zone	Enter the abbreviation for the time zone of the target system host computer. The value that you enter must be one of the time zones supported by the java.util.TimeZone class. **Note:** The connector does not validate the value that you enter. In addition, no error is thrown during reconciliation if the value entered is not a valid time zone. Sample value: `PST`
Schedule Task Name	This attribute holds the name of the scheduled task. Value: `SAP User Management User Recon`

3.4.3.2 SAP User Management Delete Recon

You use the SAP User Management Delete Recon scheduled task to reconcile deleted users from the target system. Table 3–3 describes the attributes of this scheduled task.

Table 3–3 Attributes of the SAP User Management Delete Recon Scheduled Task

Attribute	Description
Batch Size	Enter the number of records that must be included in each batch fetched from the target system during a reconciliation run. This attribute is used to implement batched reconciliation. Default value: `100`
Disable User	Enter `yes` if you want the connector to disable accounts (in Oracle Identity Manager) corresponding to accounts deleted on the target system. Enter `no` if you want the connector to revoke accounts in Oracle Identity Manager. Default value: `no`
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SAP UM IT Resource`
Last Execution Timestamp	This attribute holds the time stamp at which the last reconciliation run started. For the next reconciliation run, only target system records that have been added or modified after the recorded time stamp are considered for reconciliation. For consecutive reconciliation runs, the connector automatically enters a value for this attribute. However, you can use this attribute to switch from incremental reconciliation to full reconciliation. See Section 3.4.1, "Full Reconciliation vs. Incremental Reconciliation" for more information. Default value: `0`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP UM Resource Object`
SAP System Time Zone	Enter the abbreviation for the time zone of the target system host computer. The value that you enter must be one of the time zones supported by the java.util.TimeZone class. **Note:** The connector does not validate the value that you enter. In addition, no error is thrown during reconciliation if the value entered is not a valid time zone. Sample value: `PST`
Schedule Task Name	This attribute holds the name of the scheduled task. Default value: `SAP User Management Delete Recon`

3.4.3.3 SAP CUP Status Update Recon

> **Note:** Configure this scheduled task only if you enable the Compliant User Provisioning feature.

You use the SAP CUP Status Update Recon scheduled task to fetch the status of provisioning requests sent to SAP GRC Compliant User Provisioning. For a particular user, only the status of the latest request is brought to Oracle Identity Manager. This request is the one currently stored on the process form. Table 3–4 describes the attributes of this scheduled task.

Table 3–4 Attributes of the SAP CUP Status Update Recon Scheduled Task

Attribute	Description
Constants Lookup	This attribute holds the name of the lookup definition that holds constant values used by the connector during reconciliation and provisioning. Default value: `Lookup.SAP.CUP.Constants`
IT Resource	Enter the name of the IT resource for the SAP GRC installation from which you want to fetch request status data. Default value: `SAP GRC IT Resource`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP UM Resource Object`
Schedule Task Name	This attribute holds the name of the scheduled task. Default value: `SAP CUP Status Update Recon`

3.4.3.4 SAP CUP Delete Recon

> **Note:** Configure this scheduled task only if you enable the Compliant User Provisioning feature.

You use the SAP CUP Delete Recon scheduled task to revoke accounts (resources) of users in Oracle Identity Manager for whom the Create User provisioning requests are rejected by SAP GRC Compliant User Provisioning.

When you perform a Create User provisioning operation, the account is allocated to the OIM User even before SAP GRC Compliant User Provisioning clears the provisioning request and creates an account on the target system. For a particular user, if account creation on the target system fails, then the account provisioned in Oracle Identity Manager is an invalid account. You use the SAP CUP Delete Recon scheduled task to identify and delete such accounts.

Table 3–5 Attributes of the SAP CUP Delete Recon Scheduled Task

Attribute	Description
Configuration Lookup	This attribute holds the name of the lookup definition that stores configuration values used by the connector during reconciliation and provisioning. You can set values for some of the entries in this lookup definition. Default value: `Lookup.SAP.UM.Configuration`
Constants Lookup	This attribute holds the name of the lookup definition that holds constant values used by the connector during reconciliation and provisioning. Default value: `Lookup.SAP.CUP.Constants`
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SAP UM IT Resource`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP UM Resource Object`
Schedule Task Name	This attribute holds the name of the scheduled task. Default value: `SAP CUP Delete Recon`

3.5 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 3–6 lists the scheduled tasks that you must configure.

Table 3–6 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
SAP User Management Lookup Recon	This scheduled task is used for lookup field synchronization. Section 3.2, "Scheduled Task for Lookup Field Synchronization" describes this scheduled task.
SAP User Management User Recon	This scheduled task is used for user record reconciliation. Section 3.4.3.1, "SAP User Management User Recon" describes this scheduled task.
SAP User Management Delete Recon	This scheduled task is used for reconciliation of deleted user records. Section 3.4.3.2, "SAP User Management Delete Recon" describes this scheduled task.
SAP CUP Status Update Recon	This scheduled task is used to fetch the status of provisioning requests sent to SAP GRC Compliant User Provisioning. Section 3.4.3.3, "SAP CUP Status Update Recon" describes this scheduled task. **Note:** This scheduled task is created only if you configure the Compliant User Provisioning feature.
SAP CUP Delete Recon	This scheduled task is used to revoke accounts (resources) of users in Oracle Identity Manager for whom the Create User provisioning requests are rejected by SAP GRC Compliant User Provisioning. Section 3.4.3.4, "SAP CUP Delete Recon" describes this scheduled task. **Note:** This scheduled task is created only if you configure the Compliant User Provisioning feature.

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.

   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 Task Scheduler Form" in *Oracle Identity Manager Design Console Guide* for information about this feature.

3.6 Guidelines on Performing Provisioning

> **See Also:** Section 1.3.5, "Guidelines on Using a Deployment Configuration"

Apply the following guidelines while performing provisioning operations in any of the supported deployment configurations:

- Through provisioning, if you want to create and disable an account at the same time, then you can set the value of the Valid Through attribute to a date in the past. For example, while creating an account on 31-Jul, you can set the Valid Through date to 30-Jul. With this value, the resource provisioned to the OIM User is in the Disabled state immediately after the account is created.

  However, on the target system, if you set the Valid Through attribute to a date in the past while creating an account, then the target system automatically sets Valid Through to the current date. The outcome of this Create User provisioning operation is as follows:

  – The value of the Valid Through attribute on Oracle Identity Manager and the target system do not match.

  – On the target system, the user can log in all through the current day. The user cannot log in from the next day onward.

  You can lock the user on the target system so that the user is not able to log in the day the account is created.
- Remember that if password or system assignment fails during a Create User provisioning operation, then the user is not created.
- When you try to provision a multivalued attribute, such as a role or profile, if the attribute has already been set for the user on the target system, then the status of the process task is set to Completed in Oracle Identity Manager. If required, you can configure the task so that it shows the status Rejected in this situation. See

Oracle Identity Manager Design Console Guide for information about configuring process tasks.

- When you perform the Lock User or Unlock User provisioning operation, remember that the connector makes the required change on the target system without checking whether the account is currently in the Locked or Unlocked state. This is because the target system does not provide a method to check the current state of the account.
- The target system does not accept non-English letters in the E-mail Address field. Therefore, during provisioning operations, you must enter only English language letters in the E-mail Address field on the process form.
- The process form provides lookup definitions for both the target system IT resource and the Compliant User Provisioning IT resource (SAP GRC IT Resource). If you configure the Compliant User Provisioning feature, then you must select IT resources in both lookup definitions. In the Basic User Management mode, you need not select an IT resource for Compliant User Provisioning.
- On a Microsoft Windows platform, if you encounter the java.lang.UnsatisfiedLinkError exception during a provisioning operation, then download and install the Microsoft Visual C++ 2005 SP1 Redistributable Package from the Microsoft Web site.

Apply the following guidelines while performing provisioning operations after configuring the Compliant User Provisioning feature of the connector:

- During a Create User operation performed when the Compliant User Provisioning is configured, first submit process form data. Submit child form data after the user is created on the target system. This is because when Compliant User Provisioning is enabled, the connector supports modification of either process form fields or child form fields in a single Modify User operation.
- The following fields on the process form are mandatory attributes on SAP GRC Compliant User Provisioning:

  > **Note:** When the Compliant User Provisioning feature is configured, you must enter values for these fields even though some of them are not marked as mandatory fields on the Administrative and User Console.

  - CUP Requestor ID
  - CUP Requestor First Name
  - CUP Requestor Last Name
  - CUP Requestor Email
  - GRC IT Resource
  - User ID
  - First Name
  - Last Name
  - E Mail

  The Valid From and Valid Through attributes are not mandatory attributes.

- As mentioned earlier in this guide, SAP GRC Compliant User Provisioning does not process passwords. Therefore, any value entered in the Password field is ignored during Create User provisioning operations. After a Create User operation is performed, the user for whom the account is created on the target system must apply one of the following approaches to set the password:
  - To use the Oracle Identity Manager password as the target system password, change the password through Oracle Identity Manager.
  - Directly log in to the target system, and change the password.
- You perform an Enable User operation by setting the Valid From field to a future date. Similarly, you perform a Disable User operation by setting the Valid Through field to the current date. Both operations are treated as Modify User operations.
- When you delete a user (account) on the Administrative and User Console (process form), a Delete User request is created.
- When you select the Lock User check box on the process from, a Lock User request is created.
- When you deselect the Lock User check box on the process from, an Unlock User request is created.
- The Enable User and Disable User operations are implemented through the Valid From and Valid Through fields on the process form.
- In a Modify User operation, you can specify values for attributes that are mapped with SAP GRC Compliant User Provisioning and attributes that are directly updated on the target system. A request is created SAP GRC Compliant User Provisioning only for attributes whose mappings are present in these lookup definitions. If you specify values for attributes that are not present in these lookup definitions, then the connector sends them to directly the target system.
- SAP GRC Compliant User Provisioning does not process passwords. Therefore, any value entered in the Password field is ignored during Create User provisioning operations. During a Modify User provisioning operation, the password is sent directly to the target system.

3.7 Provisioning Operations Performed in an SoD-Enabled Environment

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system 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 3.7.1, "Overview of the Provisioning Process in an SoD-Enabled Environment"
- Section 3.7.3, "Direct Provisioning in an SoD-Enabled Environment"

- Section 3.7.4, "Request-Based Provisioning in an SoD-Enabled Environment"

3.7.1 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.

3.7.2 Guidelines on Performing Provisioning Operations

Apply the following guidelines while performing provisioning operations:

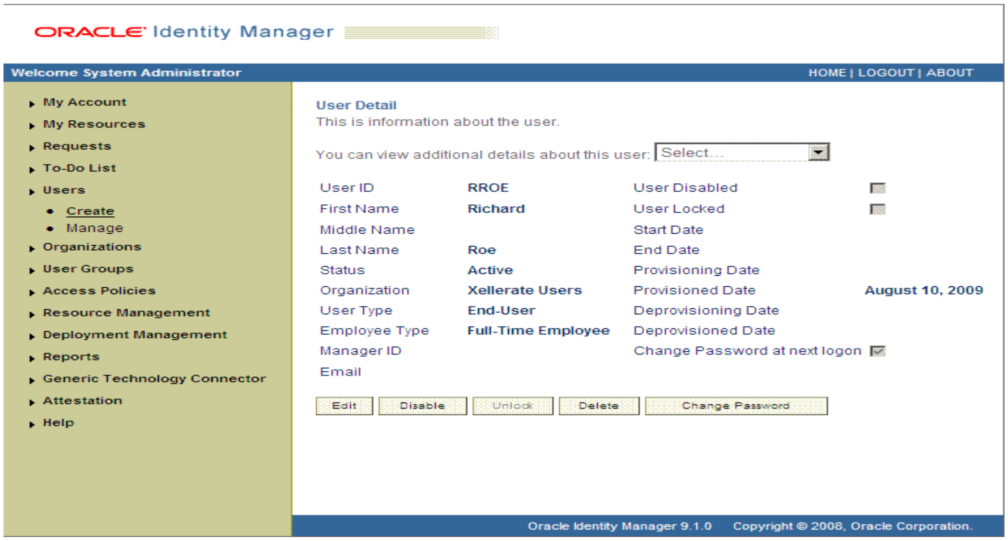
- When you assign a role to a user through provisioning, you set values for the following attributes:
  - Role System Name
  - Role Name
  - Start Date
  - End Date

  However, when you update a role assignment, you can specify values only for the Start Date and End Date attributes. You cannot set new values for the Role System Name and Role Name attributes. This also applies to new child forms that you add.
- You can only assign profiles. You cannot update an assigned profile.

3.7.3 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.
2. From the Users menu, select **Manage** if you want to provision a target system account to an existing OIM User.
3. 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.



User Detail

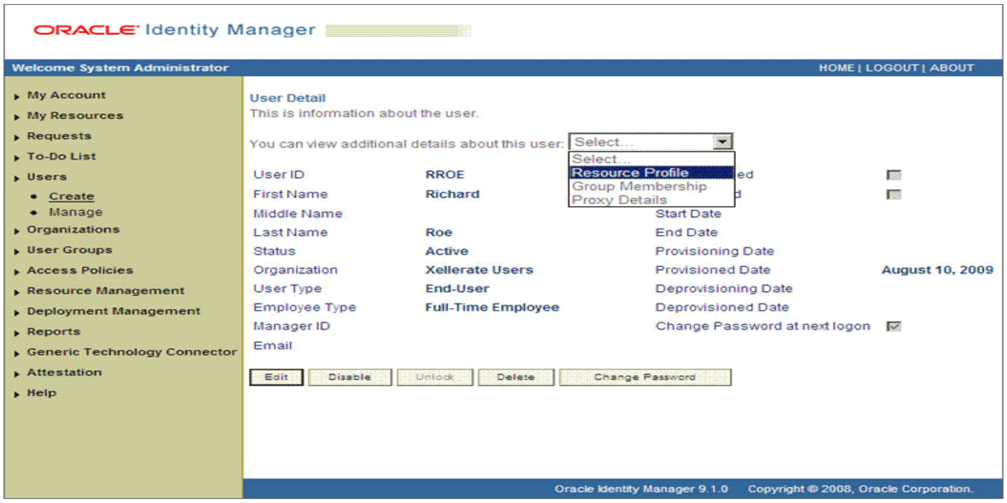
This is information about the user.

You can view additional details about this user: Select...

User ID	RROE	User Disabled	□
First Name	Richard	User Locked	□
Middle Name		Start Date	
Last Name	Roe	End Date	
Status	Active	Provisioning Date	
Organization	Xellerate Users	Provisioned Date	August 10, 2009
User Type	End-User	Deprovisioning Date	
Employee Type	Full-Time Employee	Deprovisioned Date	
Manager ID		Change Password at next logon	☑
Email			

4. 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.

5. 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.



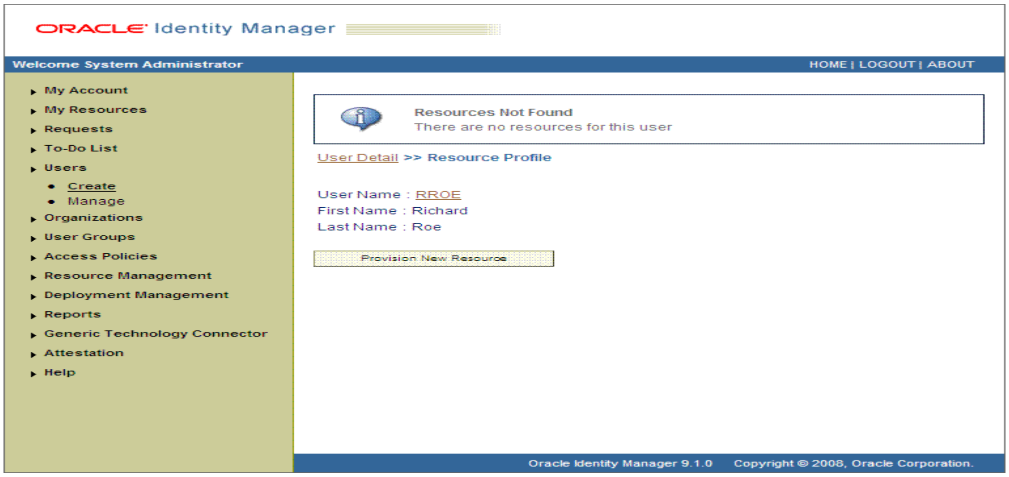
User Detail

This is information about the user.

You can view additional details about this user: Select...

User ID	RROE	ed	□
First Name	Richard	d	□
Middle Name		Start Date	
Last Name	Roe	End Date	
Status	Active	Provisioning Date	
Organization	Xellerate Users	Provisioned Date	August 10, 2009
User Type	End-User	Deprovisioning Date	
Employee Type	Full-Time Employee	Deprovisioned Date	
Manager ID		Change Password at next logon	☑
Email			

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

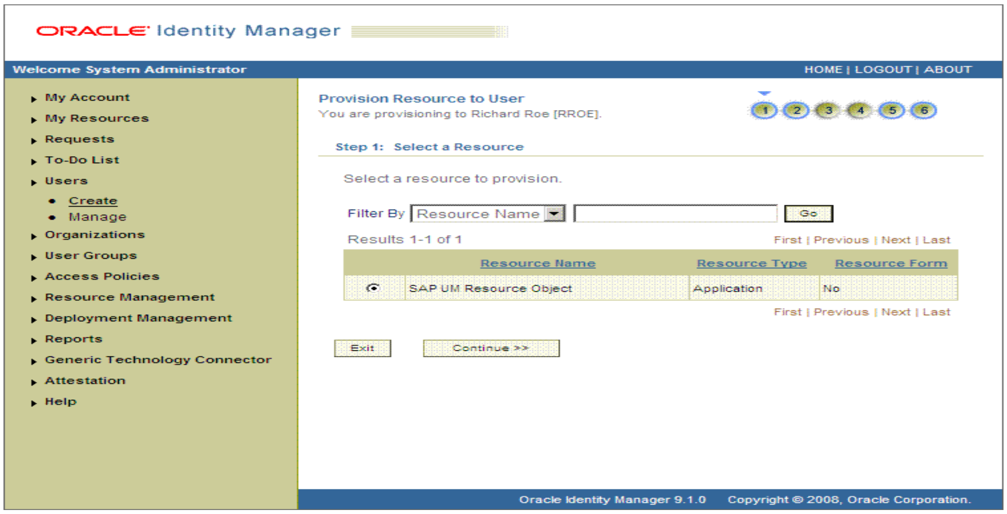


Resources Not Found
There are no resources for this user

User Detail >> Resource Profile

User Name : RROE
First Name : Richard
Last Name : Roe

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



Provision Resource to User
You are provisioning to Richard Roe [RROE].

Step 1: Select a Resource

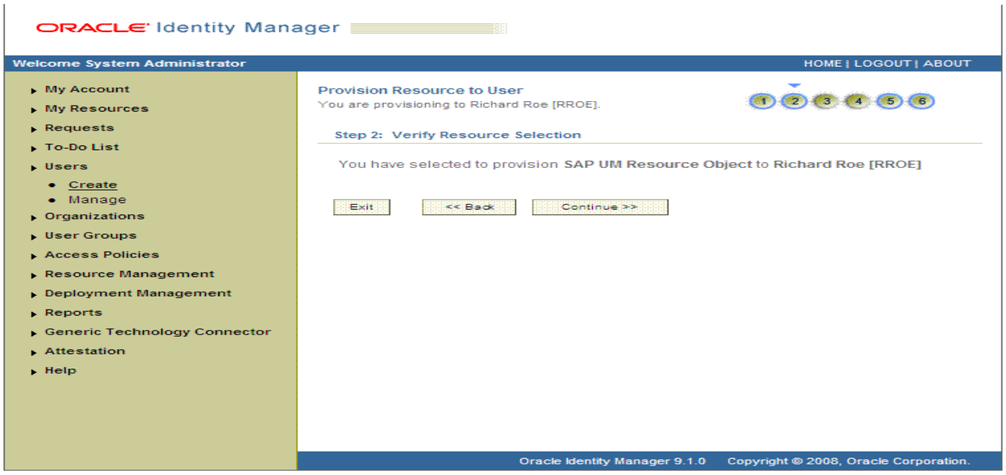
Select a resource to provision.

Filter By Resource Name

Results 1-1 of 1

	Resource Name	Resource Type	Resource Form
●	SAP UM Resource Object	Application	No

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

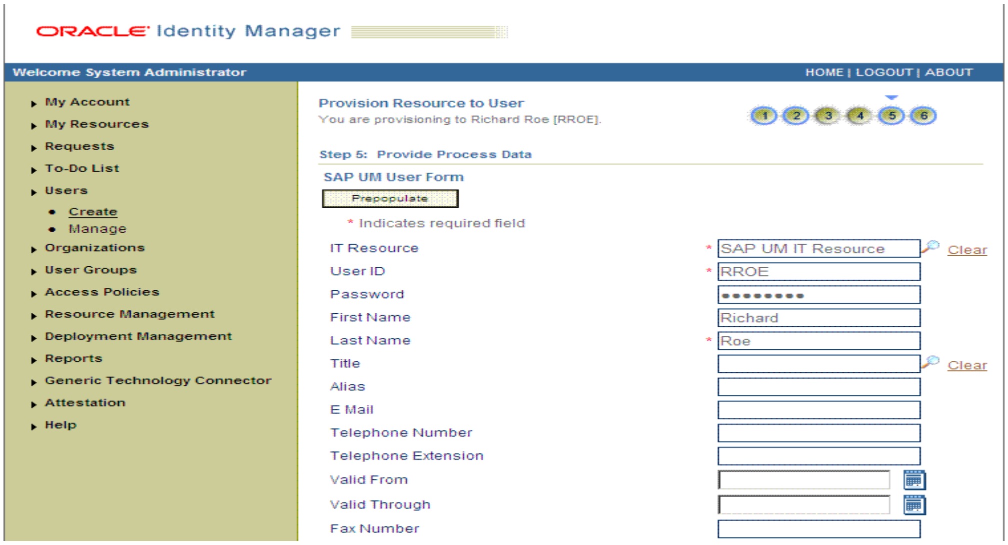


Provision Resource to User
You are provisioning to Richard Roe [RROE].

Step 2: Verify Resource Selection

You have selected to provision SAP UM Resource Object to Richard Roe [RROE]

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.



Provision Resource to User

You are provisioning to Richard Roe [RROE].

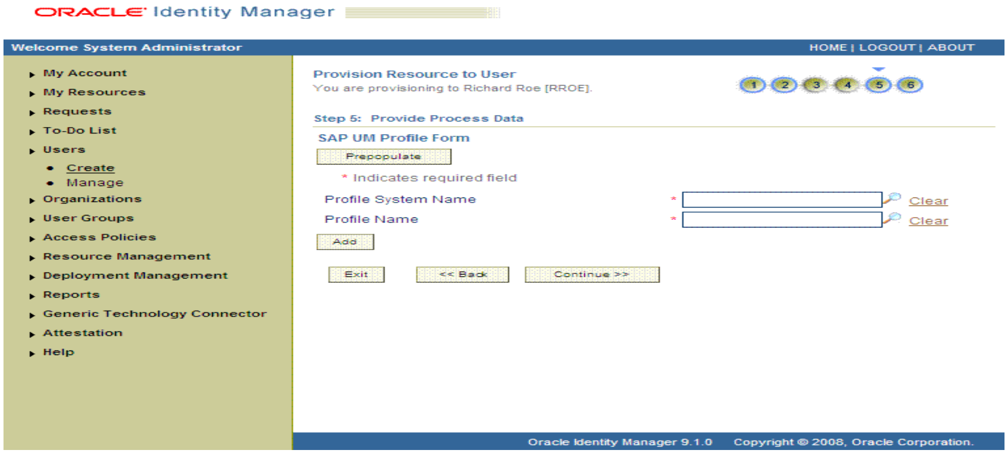
Step 5: Provide Process Data

SAP UM User Form

* Indicates required field

IT Resource *	SAP UM IT Resource
User ID *	RROE
Password	••••••••
First Name	Richard
Last Name *	Roe
Title	
Alias	
E Mail	
Telephone Number	
Telephone Extension	
Valid From	
Valid Through	
Fax Number	

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.



Provision Resource to User

You are provisioning to Richard Roe [RROE].

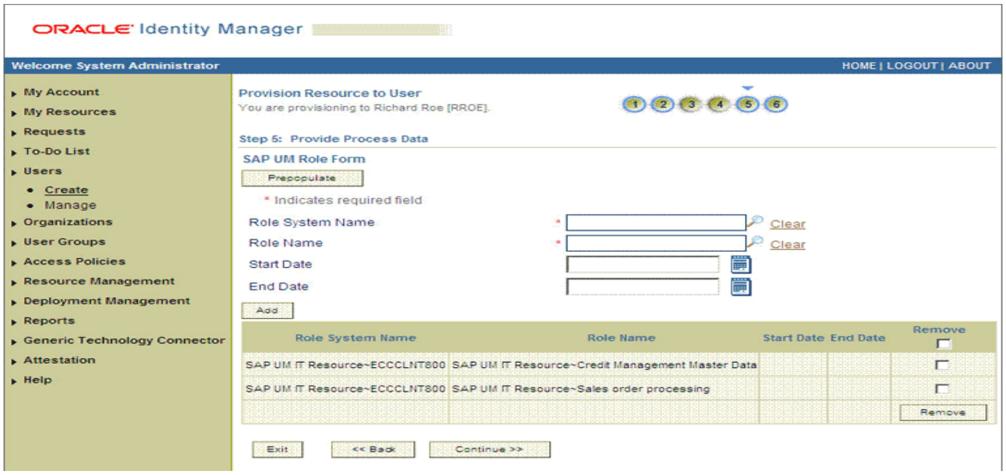
Step 5: Provide Process Data

SAP UM Profile Form

* Indicates required field

Profile System Name *	
Profile Name *	

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.



Provision Resource to User

You are provisioning to Richard Roe [RROE].

Step 5: Provide Process Data

SAP UM Role Form

* Indicates required field

Role System Name *

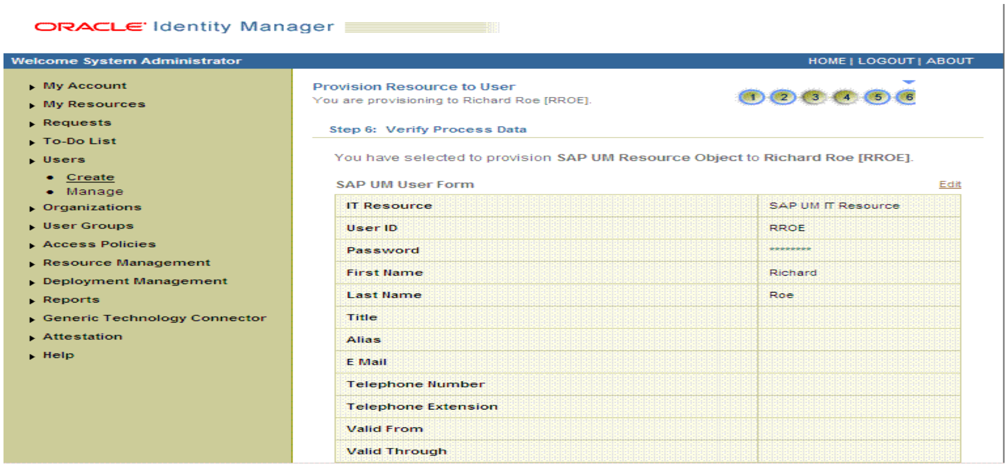
Role Name *

Start Date

End Date

Role System Name	Role Name	Start Date	End Date	Remove □
SAP UM IT Resource~ECCCLNT800	SAP UM IT Resource~Credit Management Master Data			□
SAP UM IT Resource~ECCCLNT800	SAP UM IT Resource~Sales order processing			□

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.



Provision Resource to User

You are provisioning to Richard Roe [RROE].

Step 6: Verify Process Data

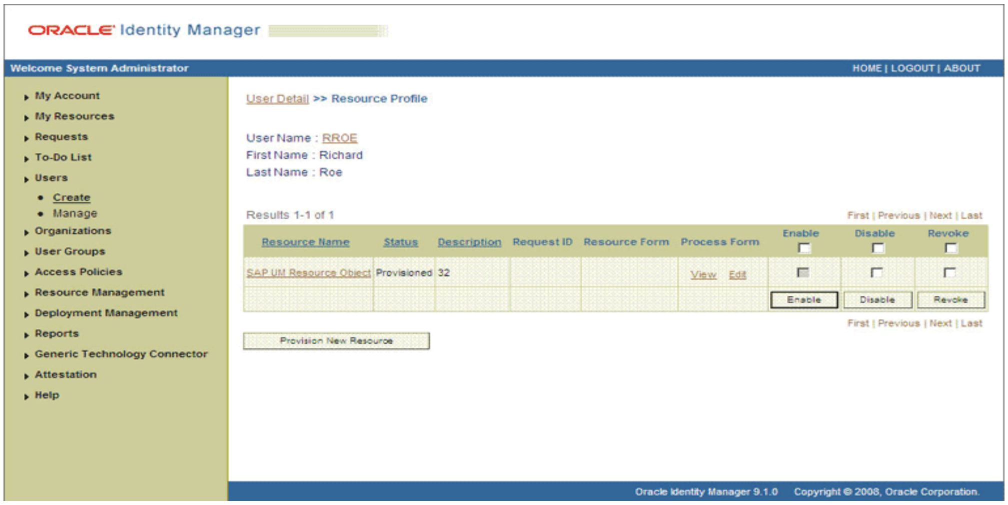
You have selected to provision **SAP UM Resource Object** to **Richard Roe [RROE]**.

SAP UM User Form

IT Resource	SAP UM IT Resource
User ID	RROE
Password	*********
First Name	Richard
Last Name	Roe
Title	
Alias	
E Mail	
Telephone Number	
Telephone Extension	
Valid From	
Valid Through	

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:



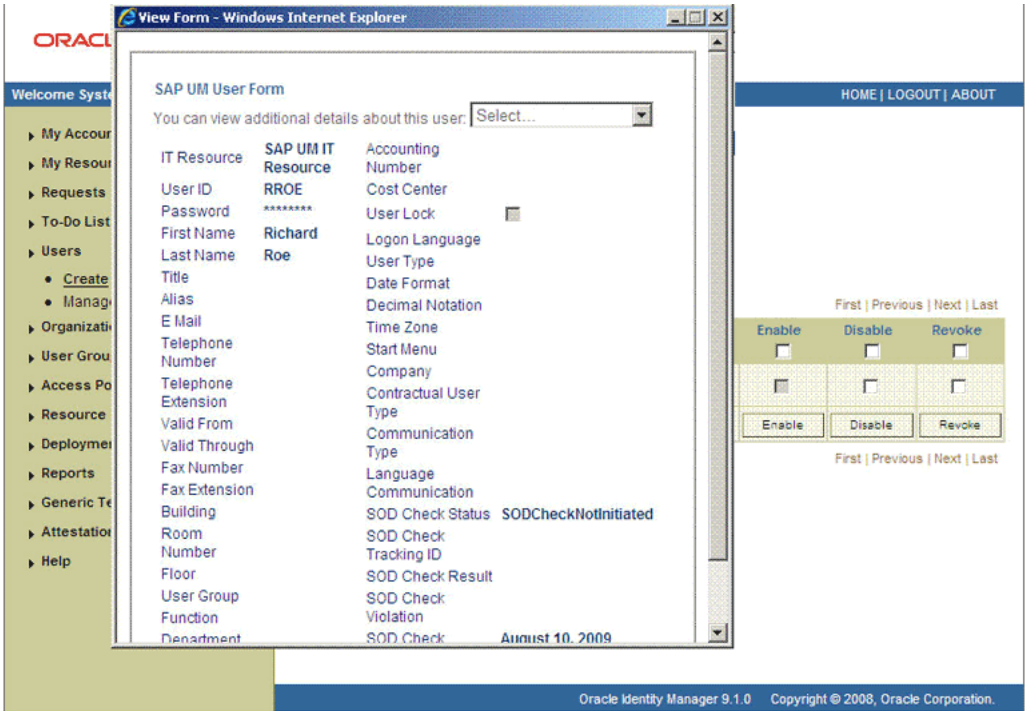
User Detail >> Resource Profile

User Name : RROE
First Name : Richard
Last Name : Roe

Results 1-1 of 1

Resource Name	Status	Description	Request ID	Resource Form	Process Form	Enable □	Disable □	Revoke □
SAP UM Resource Object	Provisioned	32			View Edit	□	□	□
						Enable	Disable	Revoke

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



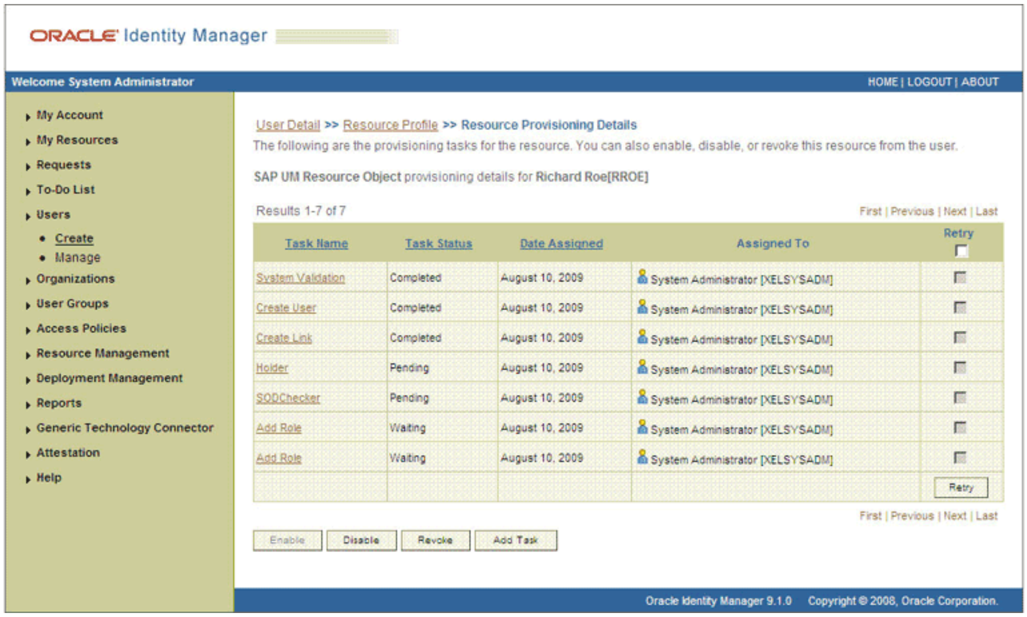
SAP UM User Form

You can view additional details about this user: Select...

IT Resource	SAP UM IT Resource	Accounting Number	
User ID	RROE	Cost Center	
Password	********	User Lock	□
First Name	Richard	Logon Language	
Last Name	Roe	User Type	
Title		Date Format	
Alias		Decimal Notation	
E Mail		Time Zone	
Telephone Number		Start Menu	
		Company	
Telephone Extension		Contractual User Type	
Valid From			
Valid Through		Communication Type	
Fax Number			
Fax Extension		Language Communication	
Building		SOD Check Status	SODCheckNotInitiated
Room Number		SOD Check Tracking ID	
Floor		SOD Check Result	
User Group		SOD Check Violation	
Function			
Department		SOD Check	August 10, 2009

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:



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 UM Resource Object provisioning details for Richard Roe[RROE]

Results 1-7 of 7

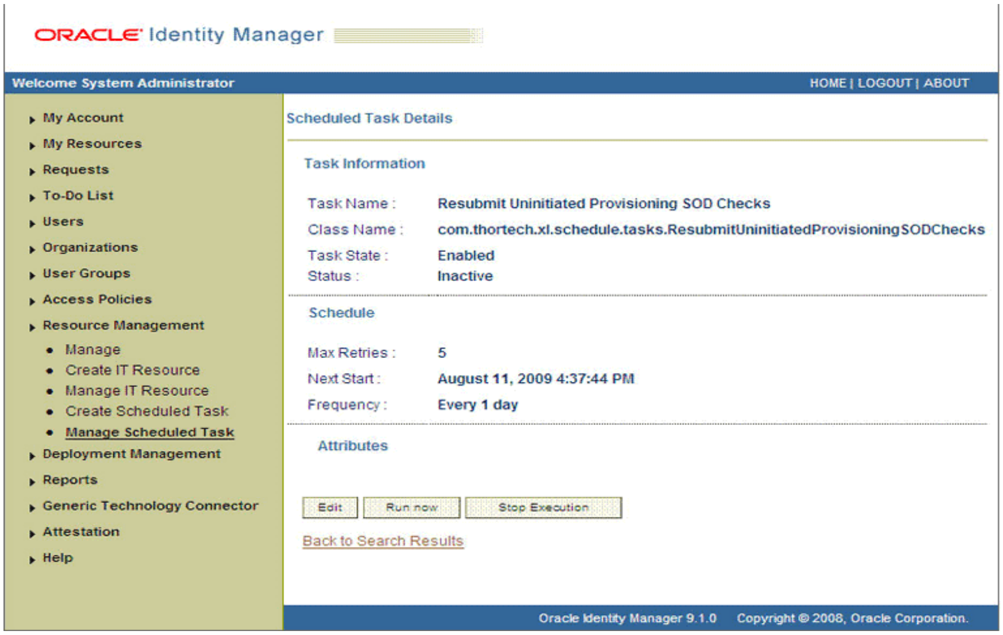
Task Name	Task Status	Date Assigned	Assigned To	Retry □
System Validation	Completed	August 10, 2009	System Administrator [XELSYSADM]	□
Create User	Completed	August 10, 2009	System Administrator [XELSYSADM]	□
Create Link	Completed	August 10, 2009	System Administrator [XELSYSADM]	□
Holder	Pending	August 10, 2009	System Administrator [XELSYSADM]	□
SODChecker	Pending	August 10, 2009	System Administrator [XELSYSADM]	□
Add Role	Waiting	August 10, 2009	System Administrator [XELSYSADM]	□
Add Role	Waiting	August 10, 2009	System Administrator [XELSYSADM]	□
				Retry

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.

16. 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:



Scheduled Task Details

Task Information

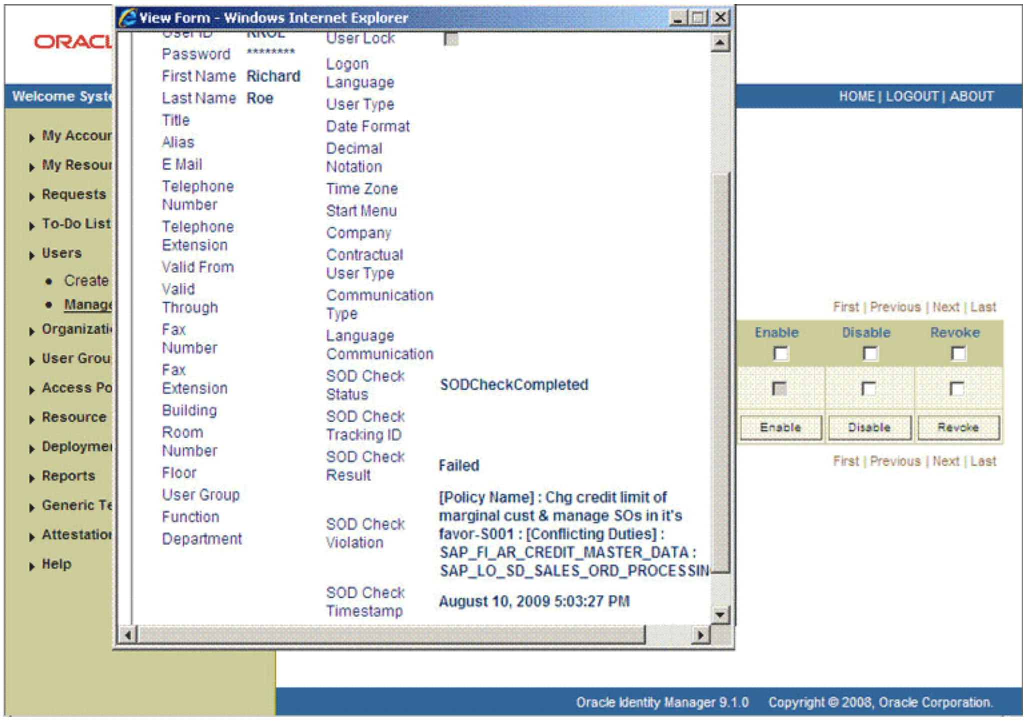
Task Name : Resubmit Uninitiated Provisioning SOD Checks
Class Name : com.thortech.xl.schedule.tasks.ResubmitUninitiatedProvisioningSODChecks
Task State : Enabled
Status : Inactive

Schedule

Max Retries : 5
Next Start : August 11, 2009 4:37:44 PM
Frequency : Every 1 day

Attributes

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:



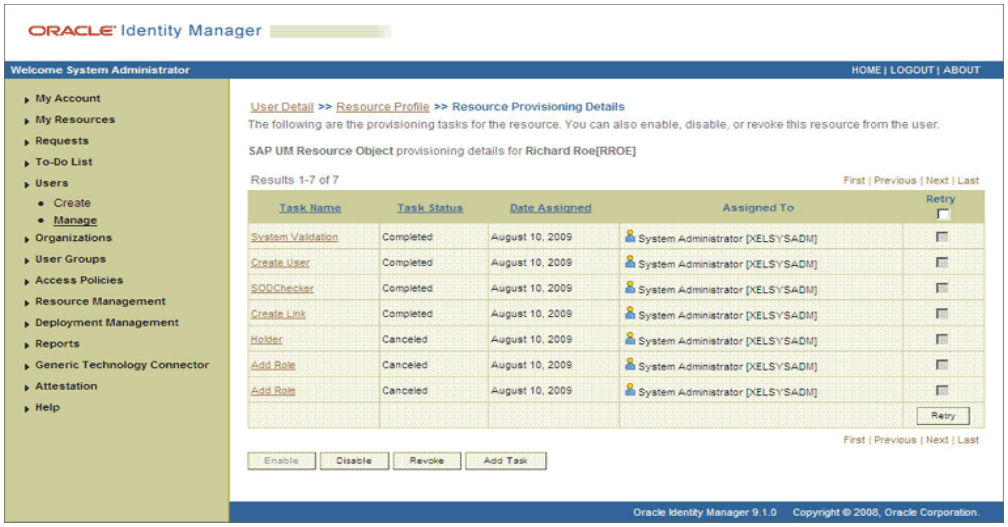
User ID RROLE
Password ********
First Name Richard
Last Name Roe
Title
Alias
E Mail
Telephone Number
Telephone Extension
Valid From
Valid Through
Fax Number
Fax Extension
Building
Room Number
Floor
User Group
Function
Department

User Lock
Logon Language
User Type
Date Format
Decimal Notation
Time Zone
Start Menu
Company
Contractual User Type
Communication Type
Language Communication
SOD Check Status SODCheckCompleted
SOD Check Tracking ID
SOD Check Result Failed
SOD Check Violation [Policy Name] : Chg credit limit of marginal cust & manage SOs in it's favor-S001 : [Conflicting Duties] : SAP_FI_AR_CREDIT_MASTER_DATA : SAP_LO_SD_SALES_ORD_PROCESSIN
SOD Check Timestamp August 10, 2009 5:03:27 PM

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:



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 UM Resource Object provisioning details for Richard Roe[RROE]

Results 1-7 of 7

Task Name	Task Status	Date Assigned	Assigned To	Retry □
System Validation	Completed	August 10, 2009	System Administrator [XELSYSADM]	□
Create User	Completed	August 10, 2009	System Administrator [XELSYSADM]	□
SODChecker	Completed	August 10, 2009	System Administrator [XELSYSADM]	□
Create Link	Completed	August 10, 2009	System Administrator [XELSYSADM]	□
Holder	Canceled	August 10, 2009	System Administrator [XELSYSADM]	□
Add Role	Canceled	August 10, 2009	System Administrator [XELSYSADM]	□
Add Role	Canceled	August 10, 2009	System Administrator [XELSYSADM]	□

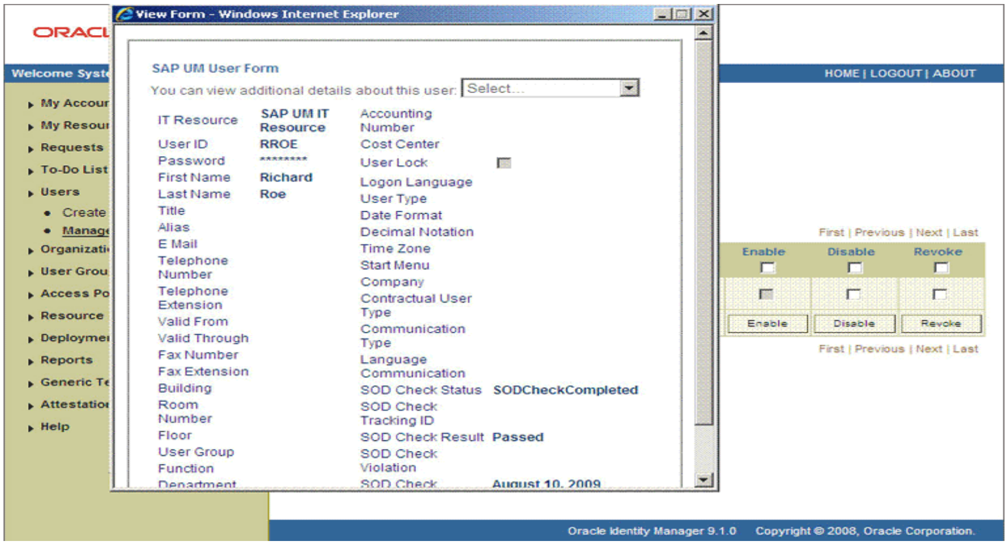
In this screenshot, the status of the Add User Role tasks is Canceled because the request failed the SoD validation process.

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:



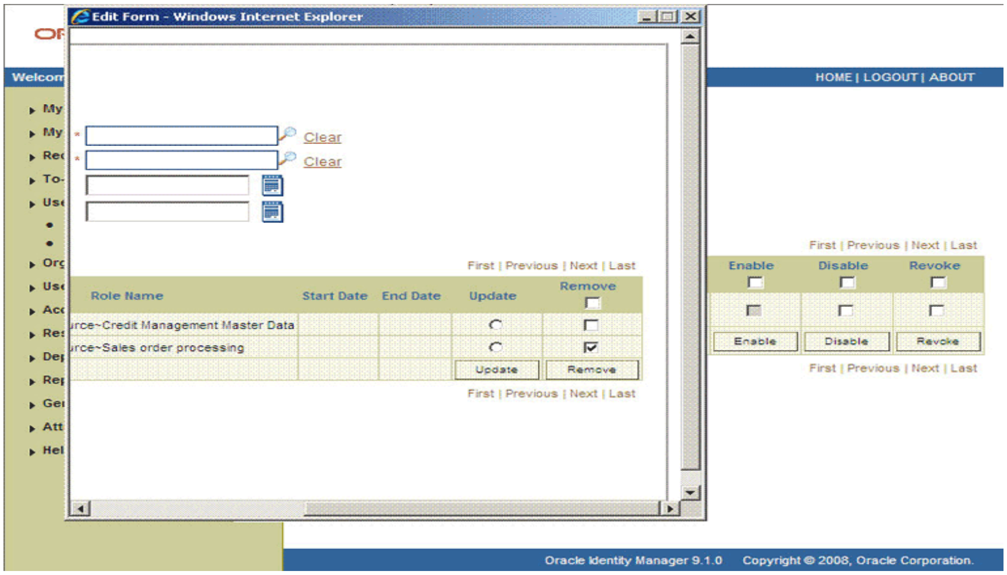
SAP UM User Form

You can view additional details about this user: Select...

IT Resource	SAP UM IT Resource	Accounting Number	
User ID	RROE	Cost Center	
Password	********	User Lock	□
First Name	Richard	Logon Language	
Last Name	Roe	User Type	
Title		Date Format	
Alias		Decimal Notation	
E Mail		Time Zone	
Telephone Number		Start Menu	
		Company	
Telephone Extension		Contractual User Type	
Valid From		Communication Type	
Valid Through			
Fax Number		Language Communication	
Fax Extension			
Building		SOD Check Status	SODCheckCompleted
Room Number		SOD Check Tracking ID	
Floor		SOD Check Result	Passed
User Group		SOD Check Violation	
Function			
Department		SOD Check	August 10, 2009

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

21. 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:


Edit Form - Windows Internet Explorer
OR
Welcom
HOME | LOGOUT | ABOUT
My
My
Rec
To-
Use
Org
Use
Acc
Res
Dep
Rep
Gei
Att
Hel
Clear
Clear
First | Previous | Next | Last
Update
Remove
Enable
Disable
Revoke
Oracle Identity Manager 9.1.0   Copyright © 2008, Oracle Corporation.

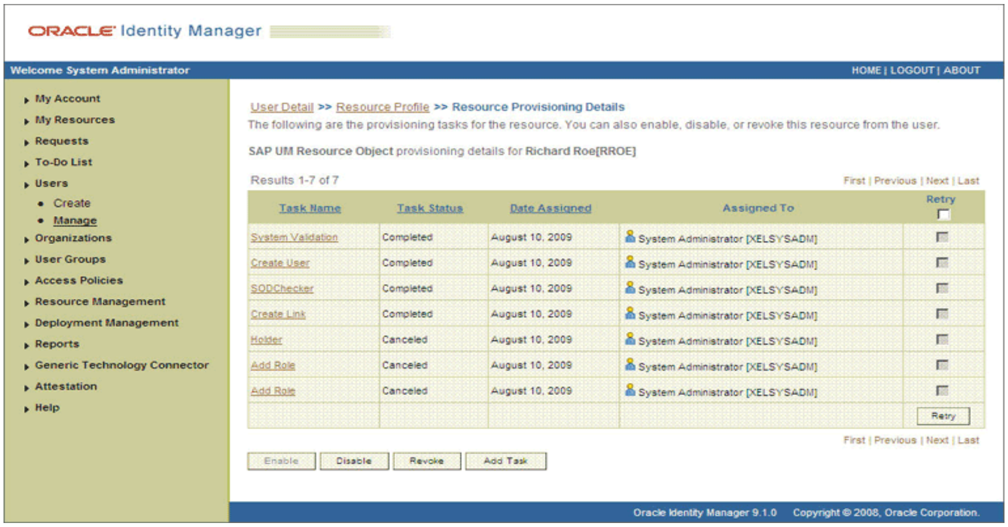
Role Name	Start Date	End Date	Update	Remove ☐
urce~Credit Management Master Data			○	☐
urce~Sales order processing			○	☑

Enable ☐	Disable ☐	Revoke ☐
☐	☐	☐

In this screenshot, the SOD Check Status field shows SoDCheckCompleted. Because no violation was detected by the SoD engine, the SoD Check Violation field shows `Passed`.

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

The following screenshot shows this page:



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 UM Resource Object provisioning details for Richard Roe[RROE]

Results 1-7 of 7

Task Name	Task Status	Date Assigned	Assigned To	Retry ☐
System Validation	Completed	August 10, 2009	System Administrator [XELSYSADM]	☐
Create User	Completed	August 10, 2009	System Administrator [XELSYSADM]	☐
SODChecker	Completed	August 10, 2009	System Administrator [XELSYSADM]	☐
Create Link	Completed	August 10, 2009	System Administrator [XELSYSADM]	☐
Holder	Canceled	August 10, 2009	System Administrator [XELSYSADM]	☐
Add Role	Canceled	August 10, 2009	System Administrator [XELSYSADM]	☐
Add Role	Canceled	August 10, 2009	System Administrator [XELSYSADM]	☐

On the Resource Provisioning Details page, the state of the Add User Role task is Completed.

3.7.4 Request-Based Provisioning in an SoD-Enabled Environment

See Also: Section 2.3.10, "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.

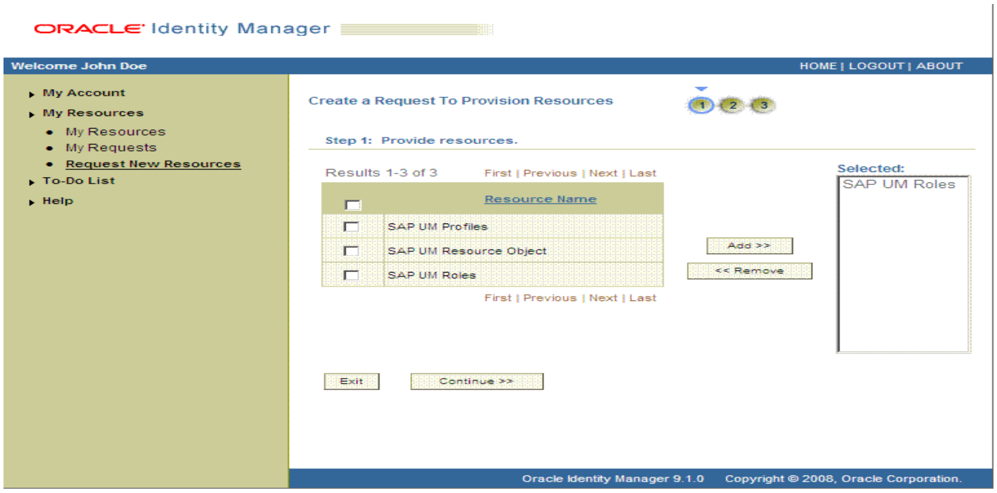
Request-based provisioning of entitlements: OIM Users who have been provisioned target system resources (either through direct or request-based provisioning) raise requests for provisioning entitlements.

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 UM 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:



Create a Request To Provision Resources

Step 1: Provide resources.

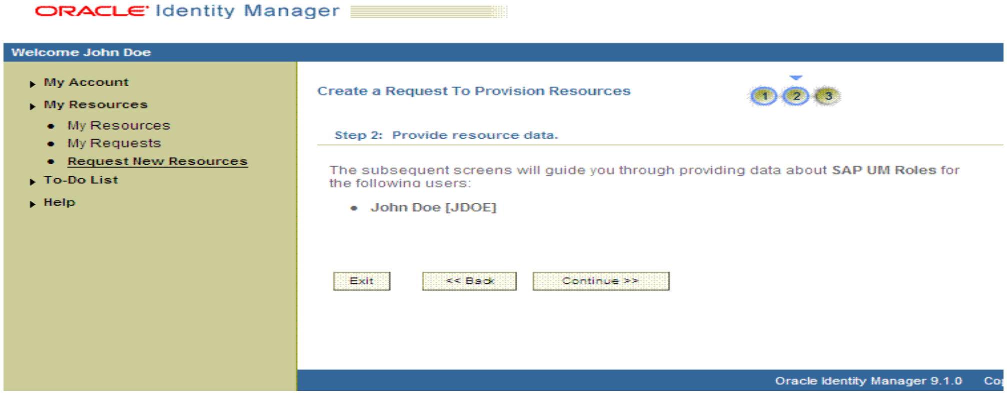
Results 1-3 of 3

□	Resource Name
□	SAP UM Profiles
□	SAP UM Resource Object
□	SAP UM Roles

Selected:
SAP UM Roles

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

   The following screenshot shows this page:



Create a Request To Provision Resources

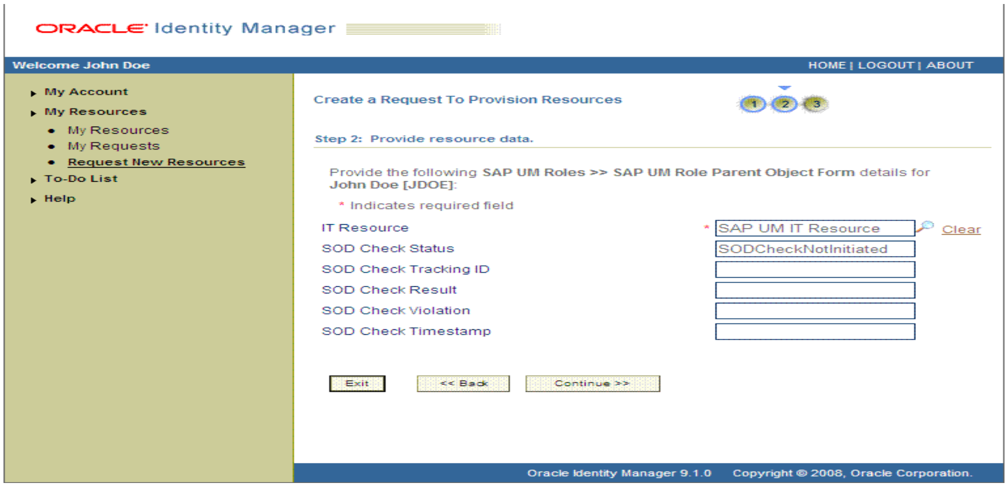
Step 2: Provide resource data.

The subsequent screens will guide you through providing data about **SAP UM Roles** for the following users:

- John Doe [JDOE]

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:



Create a Request To Provision Resources

Step 2: Provide resource data.

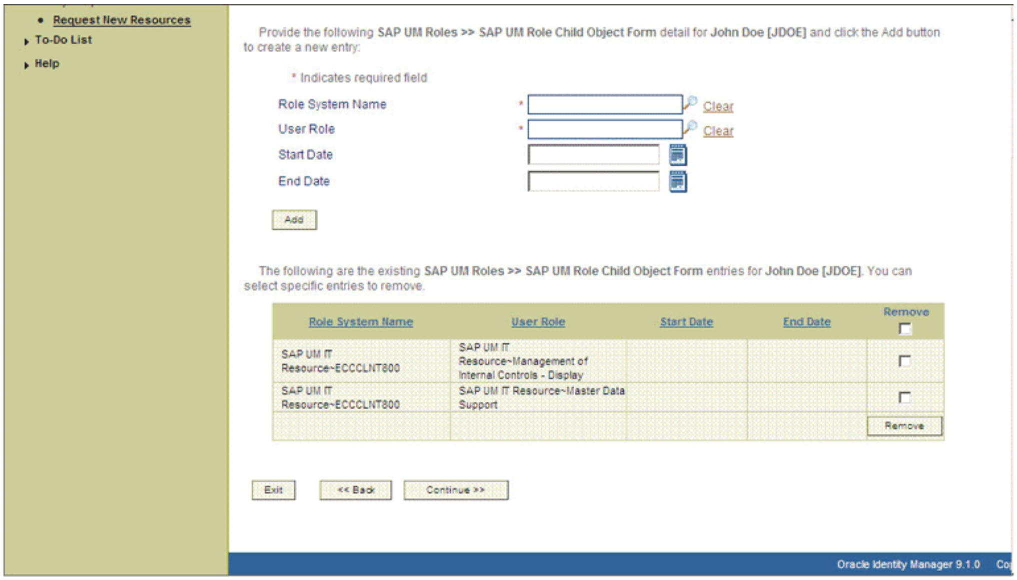
Provide the following **SAP UM Roles >> SAP UM Role Parent Object Form** details for **John Doe [JDOE]**:

* Indicates required field

IT Resource	* SAP UM IT Resource
SOD Check Status	SODCheckNotInitiated
SOD Check Tracking ID	
SOD Check Result	
SOD Check Violation	
SOD Check Timestamp	

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:



Provide the following **SAP UM Roles >> SAP UM Role Child Object Form** detail for **John Doe [JDOE]** and click the Add button to create a new entry:

* Indicates required field

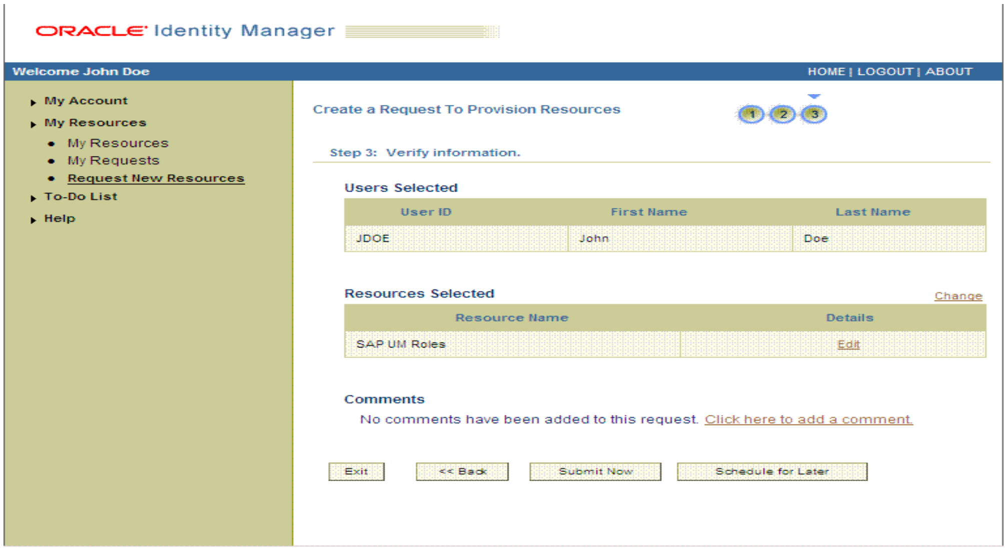
Role System Name	*
User Role	*
Start Date	
End Date	

The following are the existing **SAP UM Roles >> SAP UM Role Child Object Form** entries for **John Doe [JDOE]**. You can select specific entries to remove.

Role System Name	User Role	Start Date	End Date	Remove □
SAP UM IT Resource~ECCCLNT800	SAP UM IT Resource~Management of Internal Controls - Display			□
SAP UM IT Resource~ECCCLNT800	SAP UM IT Resource~Master Data Support			□

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:



Create a Request To Provision Resources

Step 3: Verify information.

Users Selected

User ID	First Name	Last Name
JDOE	John	Doe

Resources Selected — Change

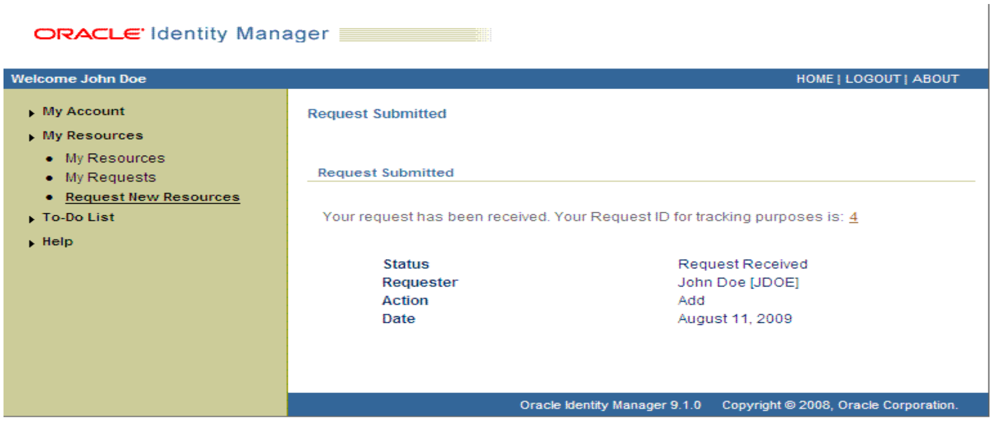
Resource Name	Details
SAP UM Roles	Edit

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:



Request Submitted

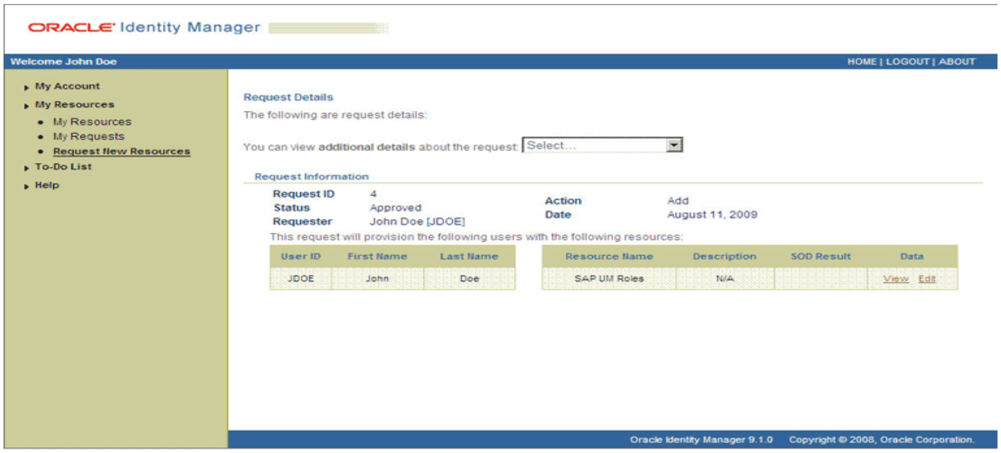
Request Submitted

Your request has been received. Your Request ID for tracking purposes is: 4

Status	Request Received
Requester	John Doe [JDOE]
Action	Add
Date	August 11, 2009

9. If you click the request ID, then the Request Details page is displayed.

   The following screenshot shows this page:



Request Details

The following are request details:

You can view **additional details** about the request:

Request Information

Request ID	4	Action	Add
Status	Approved	Date	August 11, 2009
Requester	John Doe [JDOE]		

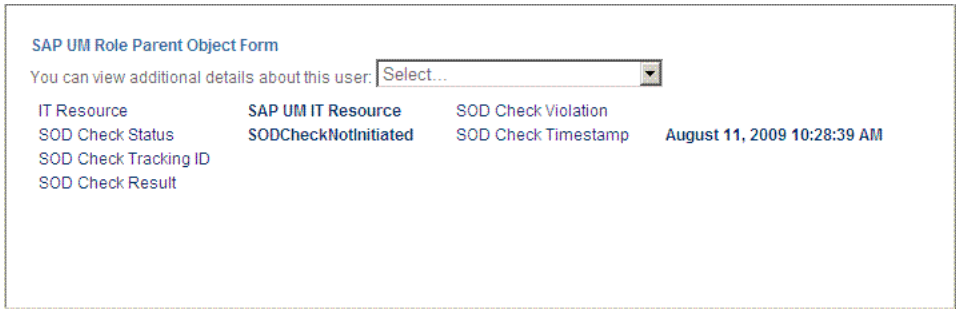
This request will provision the following users with the following resources:

User ID	First Name	Last Name
JDOE	John	Doe

Resource Name	Description	SOD Result	Data
SAP UM Roles	N/A		View Edit

On the page displayed when you click View, the SOD Status field shows SODCheckNotInitiated. The value in this field can be SoDCheckNotInitiated, SoDCheckResultPending, or SoDCheckCompleted.

The following screenshot shows this page:

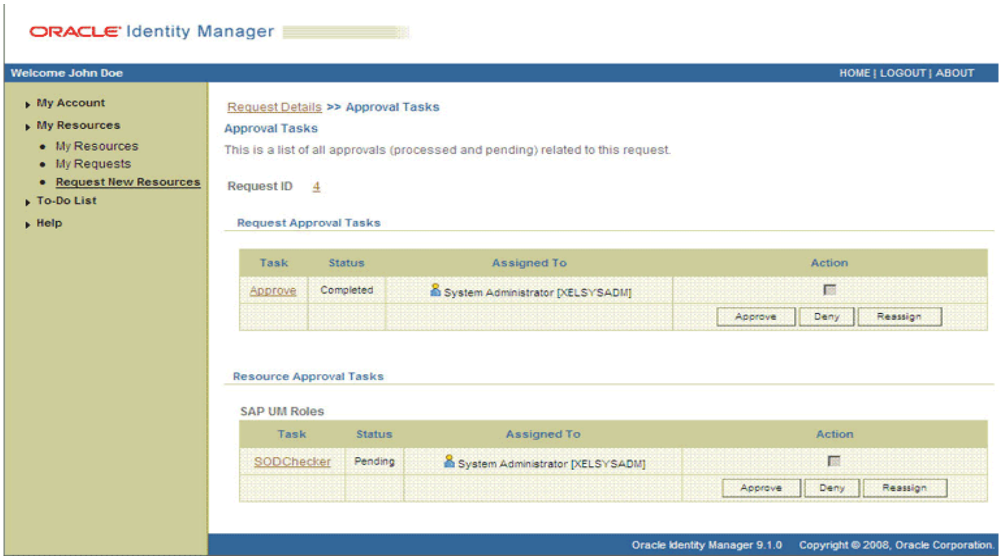


SAP UM Role Parent Object Form

You can view additional details about this user:

IT Resource	SAP UM IT Resource	SOD Check Violation	
SOD Check Status	SODCheckNotInitiated	SOD Check Timestamp	August 11, 2009 10:28:39 AM
SOD Check Tracking ID			
SOD Check Result			

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:



Request Details >> Approval Tasks

Approval Tasks

This is a list of all approvals (processed and pending) related to this request.

Request ID 4

Request Approval Tasks

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

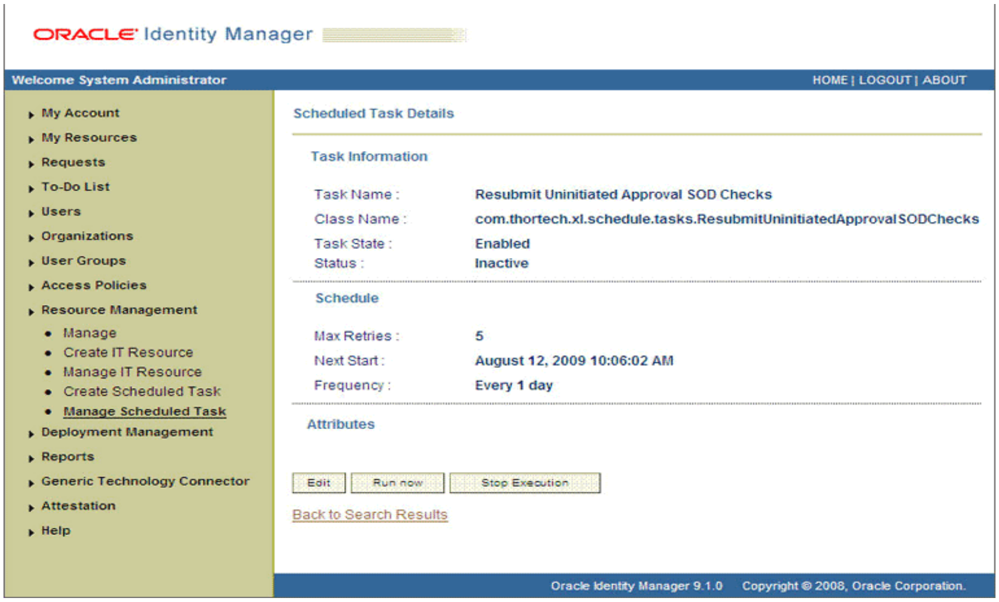
Resource Approval Tasks

SAP UM Roles

Task	Status	Assigned To	Action
SODChecker	Pending	System Administrator [XELSYSADM]	☐

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:



Scheduled Task Details

Task Information

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

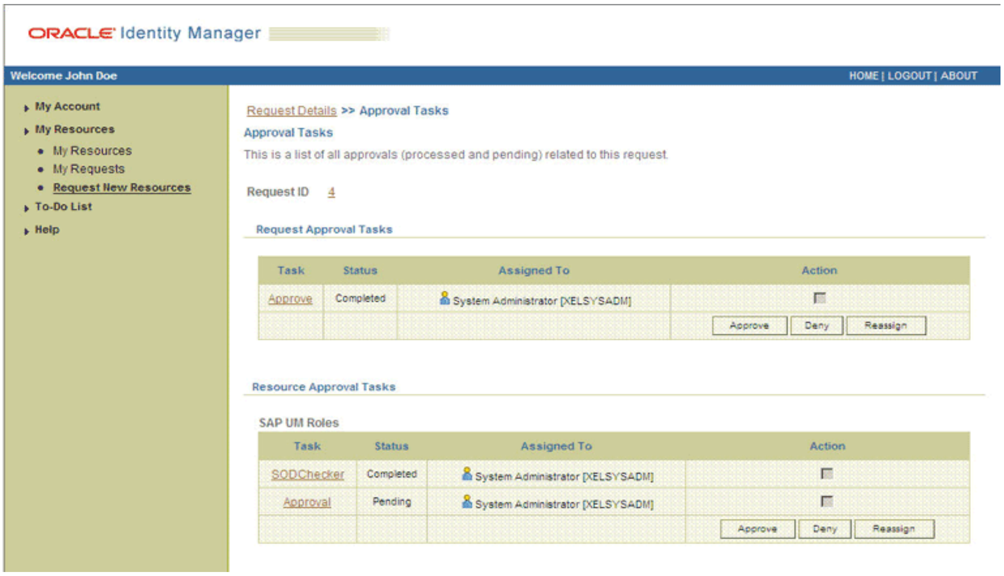
Schedule

Max Retries :	5
Next Start :	August 12, 2009 10:06:02 AM
Frequency :	Every 1 day

Attributes

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.



Request Details >> Approval Tasks

Approval Tasks

This is a list of all approvals (processed and pending) related to this request.

Request ID 4

Request Approval Tasks

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

Resource Approval Tasks

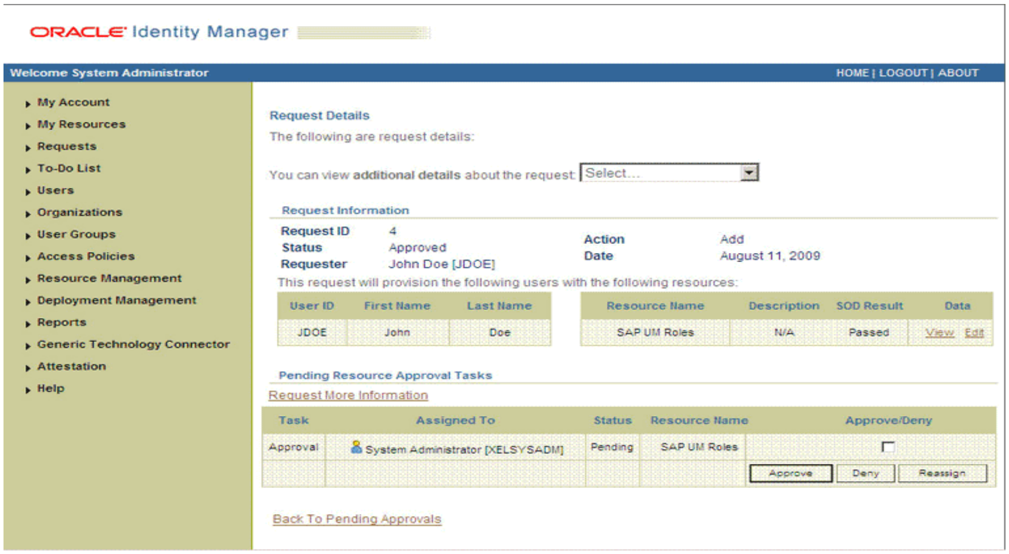
SAP UM Roles

Task	Status	Assigned To	Action
SODChecker	Completed	System Administrator [XELSYSADM]	□
Approval	Pending	System Administrator [XELSYSADM]	□

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.



Request Details

The following are request details:

You can view additional details about the request: Select...

Request Information

Request ID	4	Action	Add
Status	Approved	Date	August 11, 2009
Requester	John Doe [JDOE]		

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

User ID	First Name	Last Name	Resource Name	Description	SOD Result	Data
JDOE	John	Doe	SAP UM Roles	N/A	Passed	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	□

Back To Pending Approvals

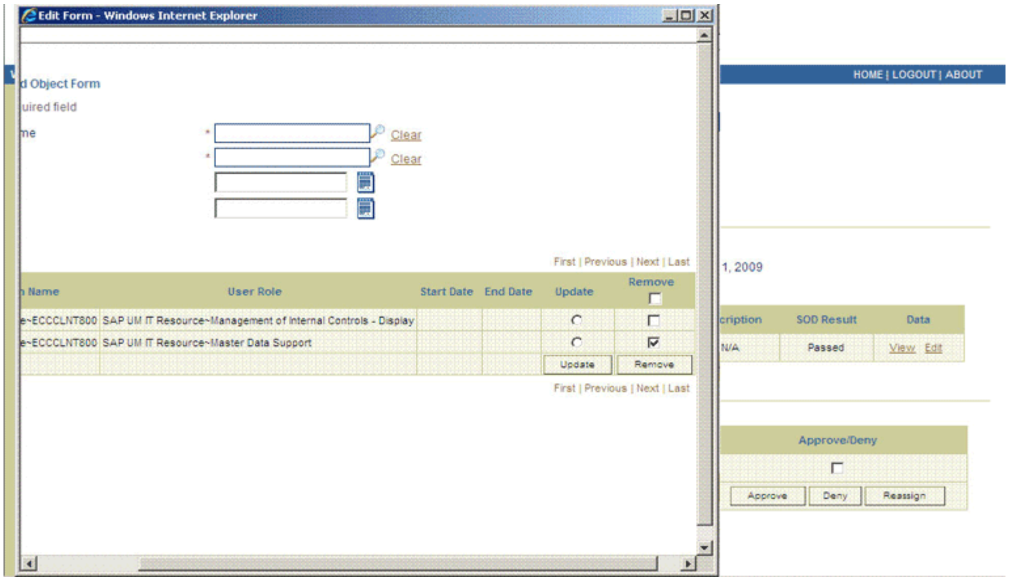
In addition, the approver can click the View link to view details of the SoD validation process.

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:



Edit Form - Windows Internet Explorer
d Object Form
uired field
me
Clear
Clear
First | Previous | Next | Last
HOME | LOGOUT | ABOUT
1, 2009

n Name	User Role	Start Date	End Date	Update	Remove □
e~ECCCLNT800	SAP UM IT Resource~Management of Internal Controls - Display			○	□
e~ECCCLNT800	SAP UM IT Resource~Master Data Support			○	☑
				Update	Remove

First | Previous | Next | Last

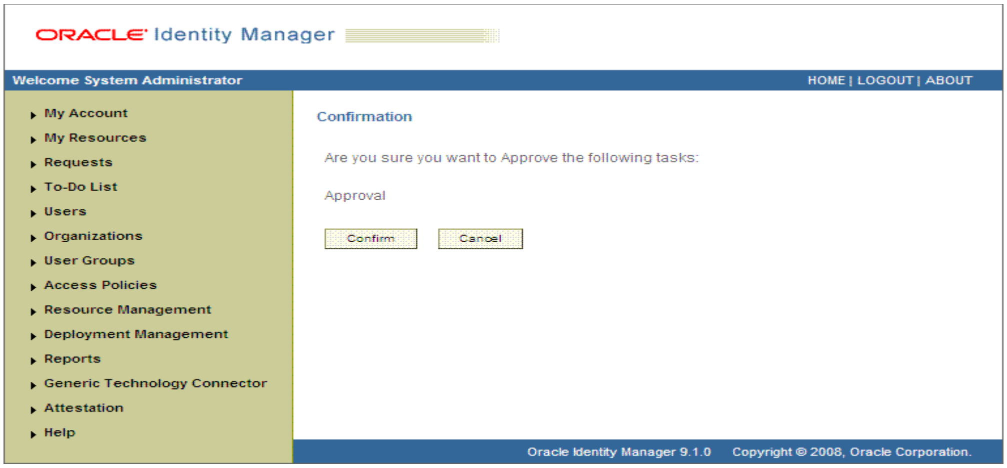
cription	SOD Result	Data
N/A	Passed	View Edit

Approve/Deny
□
Approve
Deny
Reassign

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:



Confirmation

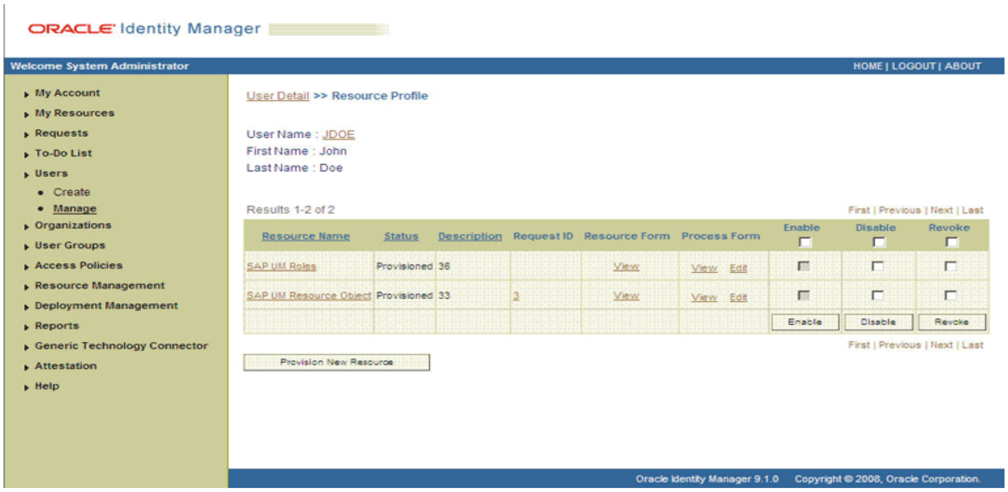
Are you sure you want to Approve the following tasks:

Approval

Confirm
Cancel
Oracle Identity Manager 9.1.0
Copyright © 2008, Oracle Corporation.

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:



User Detail >> Resource Profile

User Name : JDOE
First Name : John
Last Name : Doe

Results 1-2 of 2

Resource Name	Status	Description	Request ID	Resource Form	Process Form	Enable □	Disable □	Revoke □
SAP UM Roles	Provisioned	36		View	View Edit	□	□	□
SAP UM Resource Object	Provisioned	33	3	View	View Edit	□	□	□
						Enable	Disable	Revoke

3.8 Switching Between SAP R/3 and SAP CUA Target Systems

To switch target systems for reconciliation:

1. If you are switching to SAP CUA, then set the value of the Is CUA Enabled entry to `yes` in the Lookup.SAP.UM.Configuration lookup definition. If you are switching to SAP R/3, then set the value to `no`.

   See Section 2.3.2, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager" for more information.

2. In the SAP User Management User Recon and SAP User Management Delete Recon scheduled tasks, set values for the following attributes:

   - IT Resource: Enter the name of the required IT resource.
   - Last Execution Timestamp: Enter `0` as the value of this attribute. Alternatively, if you have saved the time stamp value from the previous reconciliation run on the same target system, then you can enter that value in the Time Stamp attribute. See Section 3.4.3, "Reconciliation Scheduled Tasks" for information about the scheduled task.

To switch target systems for provisioning:

1. If you are switching to SAP CUA, then set the value of the Is CUA Enabled entry to `yes` in the Lookup.SAP.UM.Configuration lookup definition. If you are switching to SAP R/3, then set the value to `no`.
2. If you have configured the target system for SoD, then set the Is CUA Enabled entry in the Lookup.SAP.UM.SoDConfiguration lookup definition to `yes` or `no` depending on the target system that you want to use.
3. In the SAP User Management Lookup Recon scheduled task, set values for the following attributes:

   - IT Resource: Enter the name of the required IT resource.
   - Lookup Name: Enter Lookup.SAP.CUA.LookupMappings if the target system is SAP CUA. Otherwise, enter Lookup.SAP.UM.LookupMappings.

4. Run the SAP User Management Lookup Recon scheduled task.
5. Start the provisioning operation on the Administrative and User Console by selecting the required IT resource.

3.9 Enabling and Disabling the SoD Feature

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 enabling and disabling the SoD feature in Oracle Identity Manager.

3.10 Enabling and Disabling the Compliant User Provisioning Feature

To enable or disable the Compliant User Provisioning feature of the connector:

- Set one of the following values for the CUP request mode entry in the Lookup.SAP.UM.Configuration lookup definition:

  Enter `yes` as the value of this entry to enable the Compliant User Provisioning feature.

  Enter `no` to disable this feature.

- If you are enabling Compliant User Provisioning, set `yes` as the value of the Password Disabled entry in the Lookup.SAP.UM.Configuration lookup definition.

See Section 2.3.2.3, "Setting Values in the Lookup.SAP.UM.Configuration Lookup Definition" for information about setting values in this lookup definition.

4

Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

4.1 Determining the Names of Target System Attributes

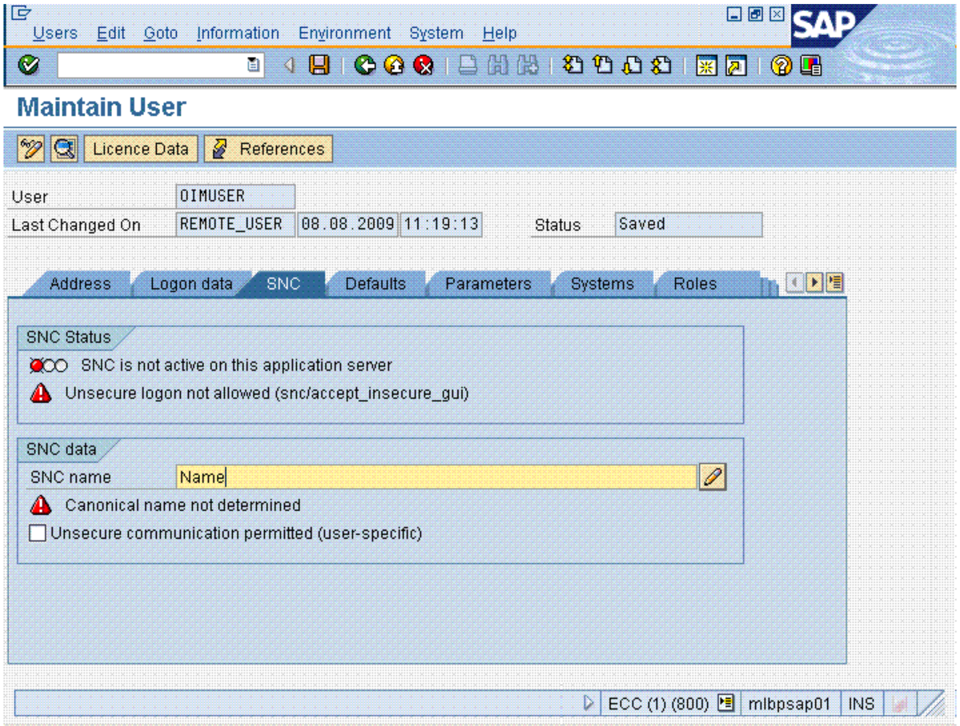
This section describes the procedure to determine the names of standard target system attributes that you want to add for reconciliation or provisioning. These attributes can be single-valued or multivalued. The names that you determine are used to build values for the Decode column of the lookup definitions that hold attribute mappings. These lookup definitions and their corresponding Decode column formats are listed in the following table:

Lookup Definition	Format of Value in the Decode Column
Lookup.SAP.UM.ReconAttrMap	*FIELD_TYPE;FIELD_NAME;STRUCTURE_NAME* *FIELD_TYPE* can be TEXT, DATE, CHECKBOX, or LOOKUP. See Section 1.6.1, "User Attributes for Reconciliation" for more information.
Lookup.SAP.UM.ReconChildAttrMap	*FIELD_TYPE;FIELD_NAME;TABLE_NAME;OIM_CHILD_TABLE_NAME* *FIELD_TYPE* can be TEXT, DATE, CHECKBOX, or LOOKUP. See Section 1.6.1, "User Attributes for Reconciliation" for more information.
Lookup.SAP.UM.ProvAttrMap and Lookup.SAP.UM.ProvChildAttrMap	*FIELD_TYPE;FIELD_NAME;STRUCTURE_NAME;FIELD_NAME_X;STRUCTURE_NAME_X* *FIELD_TYPE* can be TEXT, DATE, CHECKBOX, or LOOKUP. See Section 1.7.2, "User Attributes for Provisioning" for more information.

Note: You need not perform this procedure for custom attributes that you add on the target system. For custom attributes, the names are the same as those given in the custom BAPI that you create.

To determine the name of a target system attribute that you want to add for reconciliation or provisioning:

1. Log in to the SAP system.
2. Run transaction SU01.
3. In the **User** field, enter the user ID of the target system account that you have created for connector operations. See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for more information.
4. Click the Change icon.
5. Click the tab on which the attribute that you want to add is displayed. For example, if you want to add the SNC Name attribute, click the **SNC** tab.
6. In the field for the attribute that you want to add, enter a value. For example, enter a value in the SNC name field. The following screenshot shows this page:



User OIMUSER

Last Changed On REMOTE_USER 08.08.2009 11:19:13 Status Saved

SNC Status

SNC is not active on this application server

Unsecure logon not allowed (snc/accept_insecure_gui)

SNC data

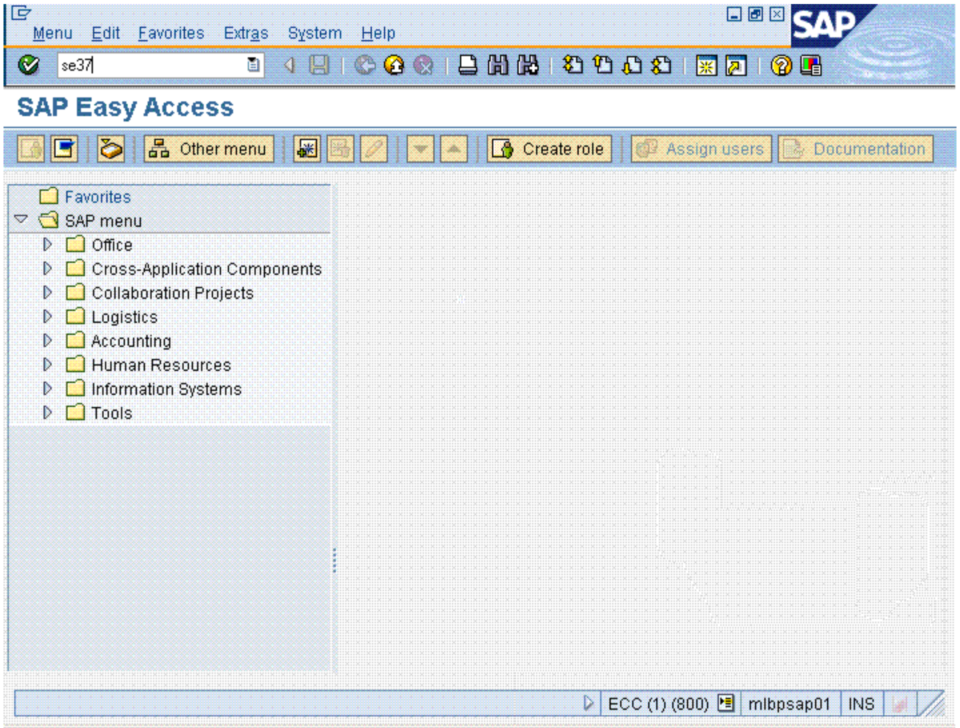
SNC name Name

Canonical name not determined

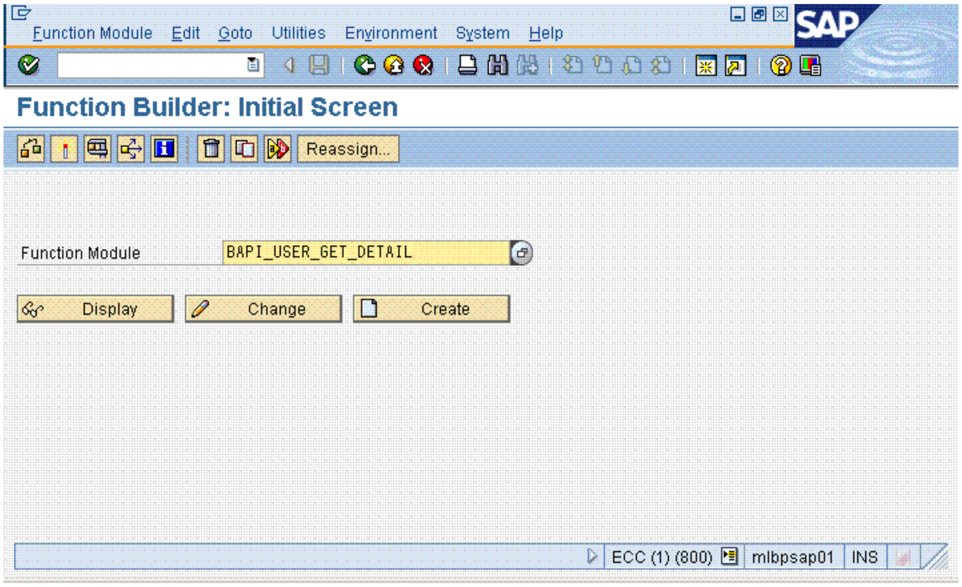
□ Unsecure communication permitted (user-specific)

7. Click the Save icon.

8. Run transaction SE37. The following screenshot shows this page:



9. In the **Function Module** field, enter `BAPI_USER_GET_DETAIL`. The following screenshot shows this page:


Function Module Edit Goto Utilities Environment System Help
SAP
Function Builder: Initial Screen
Reassign...
Display
Change
Create
ECC (1) (800)
mlbpsap01
INS

Function Module: BAPI_USER_GET_DETAIL

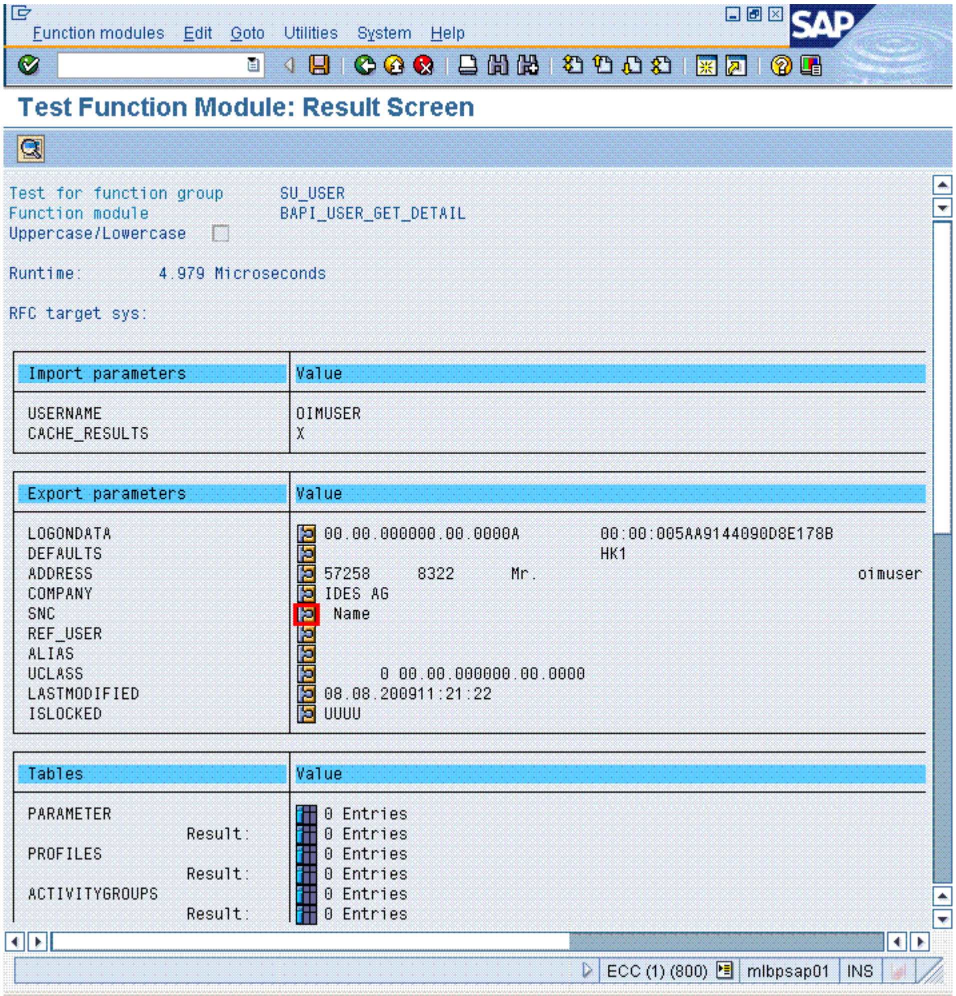
10. Click the Test/Execute icon.

11. In the USERNAME field, enter the user ID of the account described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations".

12. Click the Execute icon.

    Single-valued attributes are listed in the Export parameters table. Similarly, multivalued attributes are listed in the Tables table.

13. For the attribute that you are adding, click the icon displayed in the Value column. The following screenshot shows this page:



Test Function Module: Result Screen

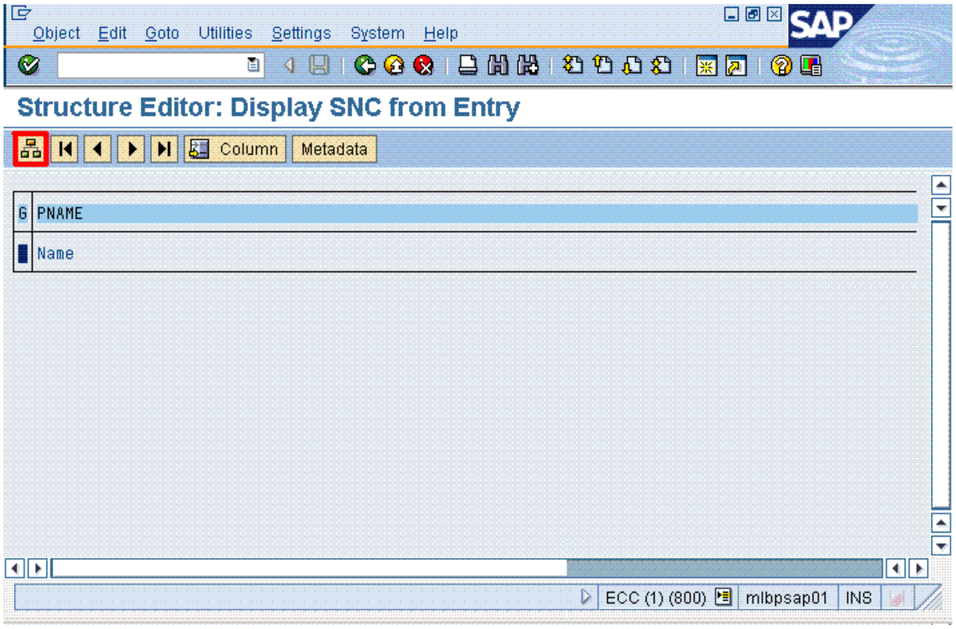
```
Test for function group      SU_USER
Function module              BAPI_USER_GET_DETAIL
Uppercase/Lowercase          □

Runtime:        4.979 Microseconds

RFC target sys:
```

Import parameters	Value
USERNAME	OIMUSER
CACHE_RESULTS	X

Export parameters	Value
LOGONDATA	00.00.000000.00.0000A 00:00:005AA9144090D8E178B
DEFAULTS	HK1
ADDRESS	57258 8322 Mr. oimuser
COMPANY	IDES AG
SNC	Name
REF_USER	
ALIAS	
UCLASS	0 00.00.000000.00.0000
LASTMODIFIED	08.08.200911:21:22
ISLOCKED	UUUU

Tables	Value
PARAMETER	0 Entries
Result:	0 Entries
PROFILES	0 Entries
Result:	0 Entries
ACTIVITYGROUPS	0 Entries
Result:	0 Entries

14. On the page that is displayed, click the Single Entry icon. The following screenshot shows this page:



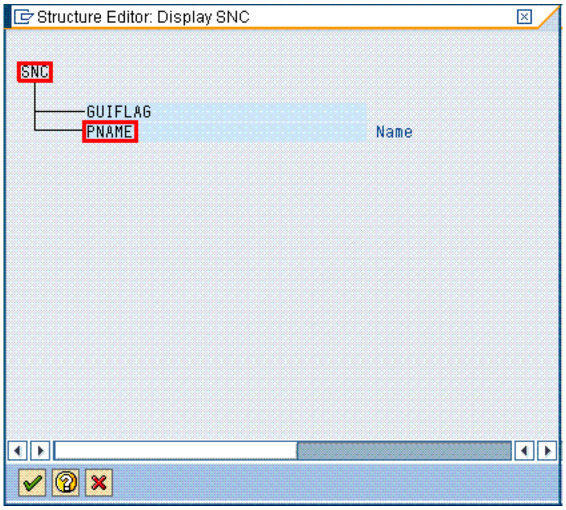
Structure Editor: Display SNC from Entry

G	PNAME
█	Name

15. The target system name for the attribute is displayed along with the value that you entered. Write down the names of the attribute (*FIELD_NAME*) and the structure (*STRUCTURE_NAME*).

> **Note:** The *FIELD_NAME* and *STRUCTURE_NAME* values can be used in the Decode value for both reconciliation and provisioning attribute mapping.
>
> You must write down the names in the same case (uppercase or lowercase) as given on the target system. This is because the attribute names are case-sensitive.

The following screenshot shows this page:



16. Using the values that you have written down, create the Decode column value for reconciliation. See the table at the start of this section for information about the required format of the Decode column.

> **Note:** If you are going to add the attribute for provisioning, then perform the remaining steps of this procedure.

17. To determine the names of the structureX and attributeX fields, which indicate that the attribute is ready for modification:

    a. Run transaction SE37.

    b. In the Function Module field, enter `BAPI_USER_CHANGE`.

    c. Click the Test/Execute icon.

    d. Click the icon in the Value column for the structureX containing the attributeX that you want to add.

    e. Write down the names of attributeX (*FIELD_NAME_X*) and structureX (*STRUCTURE_NAME_X*).

18. Using the values that you have written down, create the Decode column value for provisioning. See the table at the start of this section for information about the required format of the Decode column.

4.2 Adding New Attributes for Reconciliation

Note:

- You must ensure that new fields you add for reconciliation contain only string-format data. Binary fields must not be brought into Oracle Identity Manager natively.
- The procedure described in this section applies to both standard target system attributes and custom attributes that you create on the target system.
- If you want to add a multivalued field for reconciliation, then see "Adding New Standard and Custom Multivalued Attributes for Reconciliation" on page 4-13.

By default, the attributes listed in Table 1–4 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for reconciliation.

Summary of the procedure to add a new attribute for reconciliation

1. Add the new attribute on the process form.
2. Add the attribute to the list of reconciliation fields in the resource object.
3. Create a reconciliation field mapping for the attribute in the process definition.
4. If the new attribute is a standard attribute, create an entry for the field in the Lookup.SAP.UM.ReconAttrMap lookup definition.
5. If the new attribute is a custom attribute, then create an entry in the Lookup.SAP.UM.CustomAttrMap lookup definition.
6. If the new attribute is a check box, then create an entry in the Lookup.SAP.UM.ReconCheckBoxMapping lookup definition.

To add a new attribute for reconciliation:

Note:

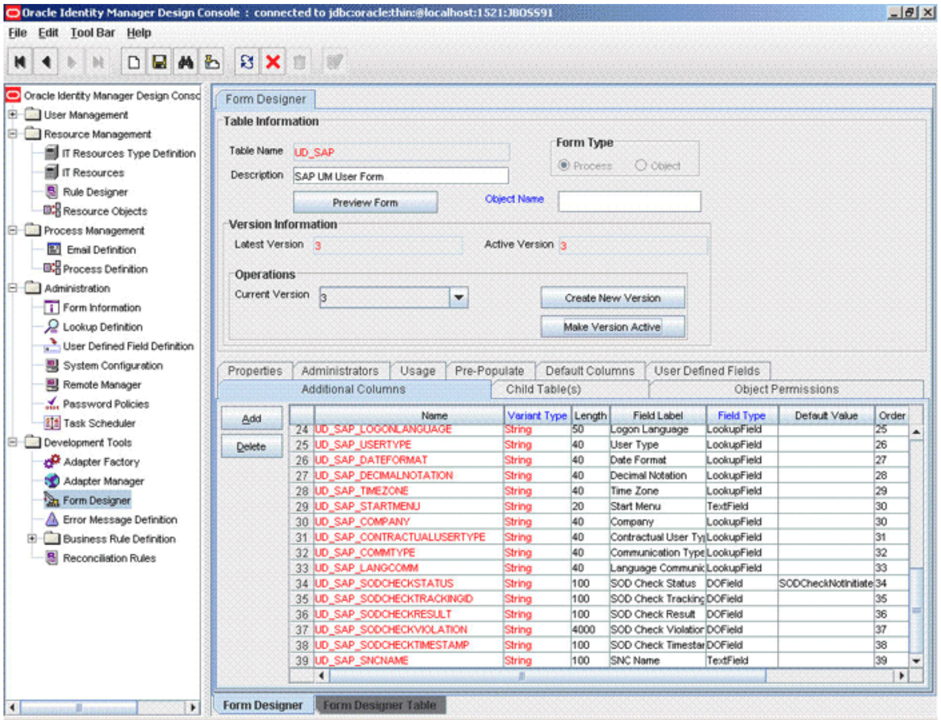
See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure.

If you have already added an attribute for provisioning, then you need not repeat steps performed as part of that procedure.

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:
   a. Expand **Development Tools**, and double-click **Form Designer**.
   b. Search for and open the **UD_SAP** process form.
   c. Click **Create New Version**, and then click **Add**.
   d. Enter the details of the field.

      For example, if you are adding the SNC Name field, enter `UD_SAP_SNCNAME` in the Name field and then enter other details such as Variable Type, Length, Field Label, and Field Type.

e. Click the Save icon, and then click **Make Version Active.** The following screenshot shows the new field added to the process form:



Oracle Identity Manager Design Console : connected to jdbc:oracle:thin:@localhost:1521:JBOSS91

Form Designer

Table Information

Table Name: UD_SAP

Description: SAP UM User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 3

Active Version: 3

Operations

Current Version: 3

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order
24	UD_SAP_LOGONLANGUAGE	String	50	Logon Language	LookupField		25
25	UD_SAP_USERTYPE	String	40	User Type	LookupField		26
26	UD_SAP_DATEFORMAT	String	40	Date Format	LookupField		27
27	UD_SAP_DECIMALNOTATION	String	40	Decimal Notation	LookupField		28
28	UD_SAP_TIMEZONE	String	40	Time Zone	LookupField		29
29	UD_SAP_STARTMENU	String	20	Start Menu	TextField		30
30	UD_SAP_COMPANY	String	40	Company	LookupField		30
31	UD_SAP_CONTRACTUALUSERTYPE	String	40	Contractual User Ty	LookupField		31
32	UD_SAP_COMMTYPE	String	40	Communication Type	LookupField		32
33	UD_SAP_LANGCOMM	String	40	Language Communic	LookupField		33
34	UD_SAP_SODCHECKSTATUS	String	100	SOD Check Status	DOField	SODCheckNotInitiate	34
35	UD_SAP_SODCHECKTRACKINGID	String	100	SOD Check Tracking	DOField		35
36	UD_SAP_SODCHECKRESULT	String	100	SOD Check Result	DOField		36
37	UD_SAP_SODCHECKVIOLATION	String	4000	SOD Check Violatior	DOField		37
38	UD_SAP_SODCHECKTIMESTAMP	String	100	SOD Check Timestar	DOField		38
39	UD_SAP_SNCNAME	String	100	SNC Name	TextField		39

3. Add the new attribute to the list of reconciliation fields in the resource object as follows:

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

   b. Search for and open the **SAP UM** resource object.

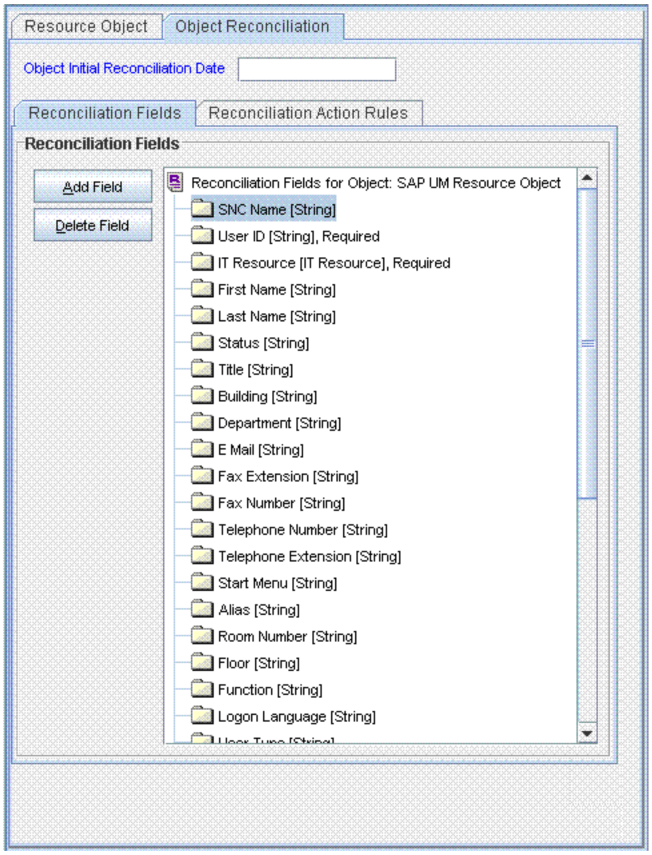
   c. On the Object Reconciliation tab, click **Add Field**.

   d. Enter the details of the field.

      For example, enter `SNC Name` in the **Field Name** field and select **String** from the Field Type list.

      Later in this procedure, you will enter the field name as the Code value of the entry that you create in the lookup definition for reconciliation.

   e. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:



4. Create a reconciliation field mapping for the new attribute in the process definition as follows:

   a. Expand **Process Management**, and double-click **Process Definition**.

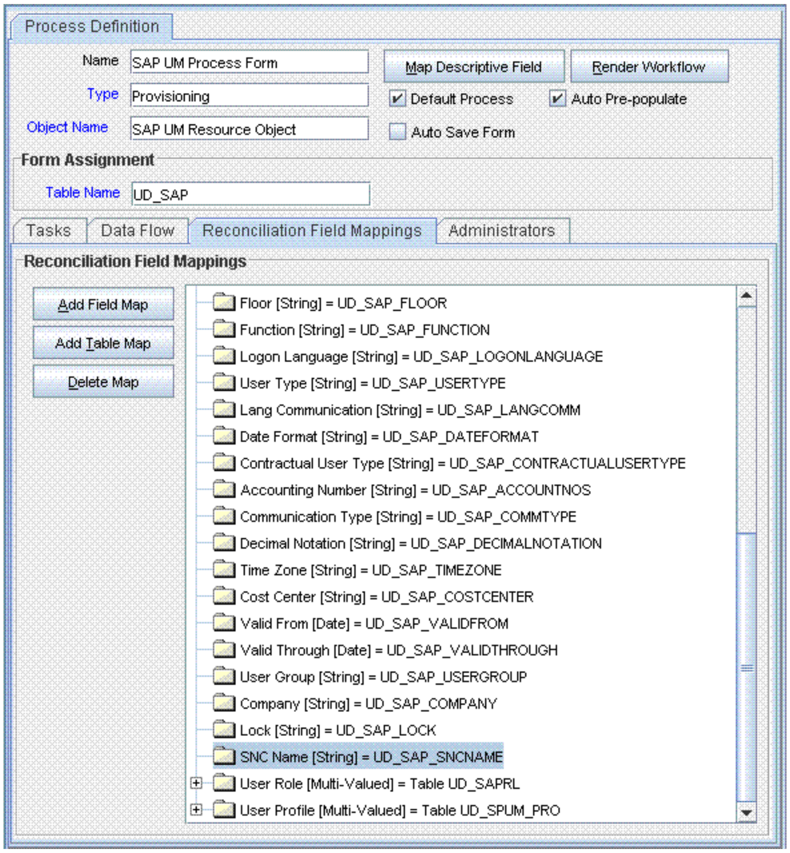
   b. Search for and open the **SAP UM Process Form** process definition.

   c. On the **Reconciliation Field Mappings** tab of the **SAP UM Process Form** process definition, click **Add Field Map**.

   d. In the Field Name field, select the value for the field that you want to add.

   e. Double-click the **Process Data Field** field, and then select **UD_SAP_SNCNAME**.

   f. Click the Save icon. The following screenshot shows the new reconciliation field mapped to a process data field in the process definition:



Name: SAP UM Process Form

Type: Provisioning

Object Name: SAP UM Resource Object

☑ Default Process ☑ Auto Pre-populate

☐ Auto Save Form

Form Assignment

Table Name: UD_SAP

Reconciliation Field Mappings

- Floor [String] = UD_SAP_FLOOR
- Function [String] = UD_SAP_FUNCTION
- Logon Language [String] = UD_SAP_LOGONLANGUAGE
- User Type [String] = UD_SAP_USERTYPE
- Lang Communication [String] = UD_SAP_LANGCOMM
- Date Format [String] = UD_SAP_DATEFORMAT
- Contractual User Type [String] = UD_SAP_CONTRACTUALUSERTYPE
- Accounting Number [String] = UD_SAP_ACCOUNTNOS
- Communication Type [String] = UD_SAP_COMMTYPE
- Decimal Notation [String] = UD_SAP_DECIMALNOTATION
- Time Zone [String] = UD_SAP_TIMEZONE
- Cost Center [String] = UD_SAP_COSTCENTER
- Valid From [Date] = UD_SAP_VALIDFROM
- Valid Through [Date] = UD_SAP_VALIDTHROUGH
- User Group [String] = UD_SAP_USERGROUP
- Company [String] = UD_SAP_COMPANY
- Lock [String] = UD_SAP_LOCK
- SNC Name [String] = UD_SAP_SNCNAME
- User Role [Multi-Valued] = Table UD_SAPRL
- User Profile [Multi-Valued] = Table UD_SPUM_PRO

5. Create an entry for the field in the lookup definition for reconciliation as follows:

   Note: Skip this step if you are adding a custom attribute.

   a. Expand **Administration**.

   b. Double-click **Lookup Definition.**

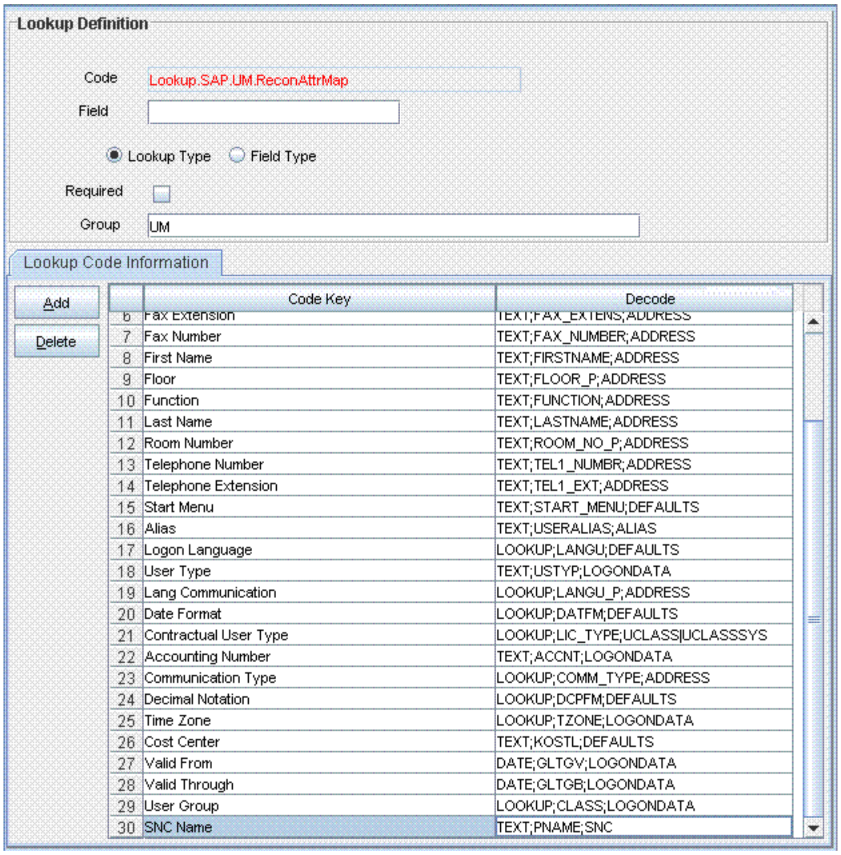
   c. Search for and open the Lookup.SAP.UM.ReconAttrMap lookup definition.

   Note: For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

   d. Click **Add** and enter the Code Key and Decode values for the field. The Code Key value must be the name of the field in the resource object. The Decode value is what you determine by performing the procedure described in Section 4.1, "Determining the Names of Target System Attributes".

   For example, enter `SNC Name` in the **Code Key** field and then enter `TEXT;PNAME;SNC` in the **Decode** field.

   e. Click the Save icon. The following screenshot shows the entry added to the lookup definition:



Lookup Definition

Code: Lookup.SAP.UM.ReconAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: UM

Lookup Code Information

	Code Key	Decode
6	Fax Extension	TEXT;FAX_EXTENS;ADDRESS
7	Fax Number	TEXT;FAX_NUMBER;ADDRESS
8	First Name	TEXT;FIRSTNAME;ADDRESS
9	Floor	TEXT;FLOOR_P;ADDRESS
10	Function	TEXT;FUNCTION;ADDRESS
11	Last Name	TEXT;LASTNAME;ADDRESS
12	Room Number	TEXT;ROOM_NO_P;ADDRESS
13	Telephone Number	TEXT;TEL1_NUMBR;ADDRESS
14	Telephone Extension	TEXT;TEL1_EXT;ADDRESS
15	Start Menu	TEXT;START_MENU;DEFAULTS
16	Alias	TEXT;USERALIAS;ALIAS
17	Logon Language	LOOKUP;LANGU;DEFAULTS
18	User Type	TEXT;USTYP;LOGONDATA
19	Lang Communication	LOOKUP;LANGU_P;ADDRESS
20	Date Format	LOOKUP;DATFM;DEFAULTS
21	Contractual User Type	LOOKUP;LIC_TYPE;UCLASS|UCLASSSYS
22	Accounting Number	TEXT;ACCNT;LOGONDATA
23	Communication Type	LOOKUP;COMM_TYPE;ADDRESS
24	Decimal Notation	LOOKUP;DCPFM;DEFAULTS
25	Time Zone	LOOKUP;TZONE;LOGONDATA
26	Cost Center	TEXT;KOSTL;DEFAULTS
27	Valid From	DATE;GLTGV;LOGONDATA
28	Valid Through	DATE;GLTGB;LOGONDATA
29	User Group	LOOKUP;CLASS;LOGONDATA
30	SNC Name	TEXT;PNAME;SNC

6. The target system allows you to create custom structures and tables that hold custom fields. If you are mapping a custom attribute for reconciliation, then create an entry for the attribute in the Lookup.SAP.UM.CustomAttrMap lookup definition as follows:

   Note:

   Skip this step if you are adding a standard attribute.

   Only single-valued custom attributes can be mapped for reconciliation.

   For a change in a custom attribute to be detected during incremental reconciliation, at least one standard attribute in the same record must be modified.

   - In the Code Key column of the Lookup.SAP.UM.CustomAttrMap lookup definition, enter the name of the resource object field that you created for the custom attribute.
   - In the Decode column of the lookup definition, enter a value in one of the following formats:
     - If you want a custom BAPI to fetch values from this attribute, then:

       CUSTOM_BAPI_NAME;FIELD_TYPE;TABLE_NAME;FIELD_NAME;KEY_USER_ID_FIELD

     - If you want a custom RFC table to fetch values from this attribute, then:

       RFC_READ_TABLE;*FIELD_TYPE;TABLE_NAME;FIELD_NAME;KEY_USER_ID_FIELD*

In these formats:

- *CUSTOM_BAPI_NAME* is the name of the custom BAPI that you created for fetching values from the custom attribute.
- *FIELD_TYPE* is the type of data that is stored in the custom attribute. It can be TEXT, DATE, or CHECKBOX.
- *TABLE_NAME* is the name of the custom table that contains the attribute.
- *FIELD_NAME* is the name of the attribute in the custom table.
- *KEY_USER_ID_FIELD* is the attribute in the custom table that holds user ID values.

The following is a sample value for the Decode column:

```
ZBAPI_CUSTFIELDS;TEXT;ZCUSTFIELDS;FIELD1;USERNAME
```

7. Oracle Identity Manager stores the state of a check box as either 1 (selected) or 0 (deselected). In SAP, the state of check boxes is stored using different characters. If you are adding a check box attribute on the target system for reconciliation, then:

   a. Search for and open the Lookup.SAP.UM.ReconCheckBoxMapping lookup definition.

   b. If the attribute is a standard check box attribute, then create one of the entries given in the following table:

Field Label in SAP	Value to Be Entered in the Code Key Column (Sample Resource Object Field Name)	Value to Be Entered in the Decode Column
Output Immediately	Output Immediately	GH
Delete After Output	Delete After Output	DK
Check Indicator	Check Indicator	X
Unsecure communication permitted (user-specific)	Unsecure communication permitted	X

   c. If the attribute is a standard check box attribute, then create the following entry in the Lookup.SAP.UM.ReconCheckBoxMapping lookup definition:

   - Code Key: Enter the name of the process form field that you created for the attribute.
   - Decode: Enter the characters for representing the check box state when it is selected and deselected. For example, suppose you use X to represent the selected state of the check box and Y to represent the deselected state, then enter XY in the Decode column.

   d. Save and close the lookup definition.

4.3 Adding New Standard and Custom Multivalued Attributes for Reconciliation

> **Note:**
>
> This section describes the procedure to add standard multivalued attributes of the target system for reconciliation. Addition of custom multivalued attributes is not supported.
>
> You must ensure that new fields you add for reconciliation contain only string-format data. Binary fields must not be brought into Oracle Identity Manager natively.

By default, the multivalued attributes listed in Table 1–5 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued fields for reconciliation.

Summary of the procedure to add a new multivalued attribute for reconciliation

1. Create a child form for the new multivalued attribute.
2. Associate the child form with the parent form.
3. Add the multivalued attribute to the list of reconciliation fields in the resource object.
4. Create a reconciliation field mapping for the multivalued attribute.
5. Create an entry for the multivalued attribute in the Lookup.SAP.UM.ReconChildAttrMap lookup definition.
6. If the attribute is a custom multivalued attribute, then add it in Lookup.SAP.UM.CustomChildAttrMap lookup definition.

To add a new multivalued attribute for reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Create a child form for the multivalued attribute as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Create a form by specifying a table name and description, and then click the Save icon.
   d. Click **Add** and enter the details of the attributes.
   e. Click the Save icon and then click **Make Version Active.** The following screenshot shows the multivalued attributes added on a new form:

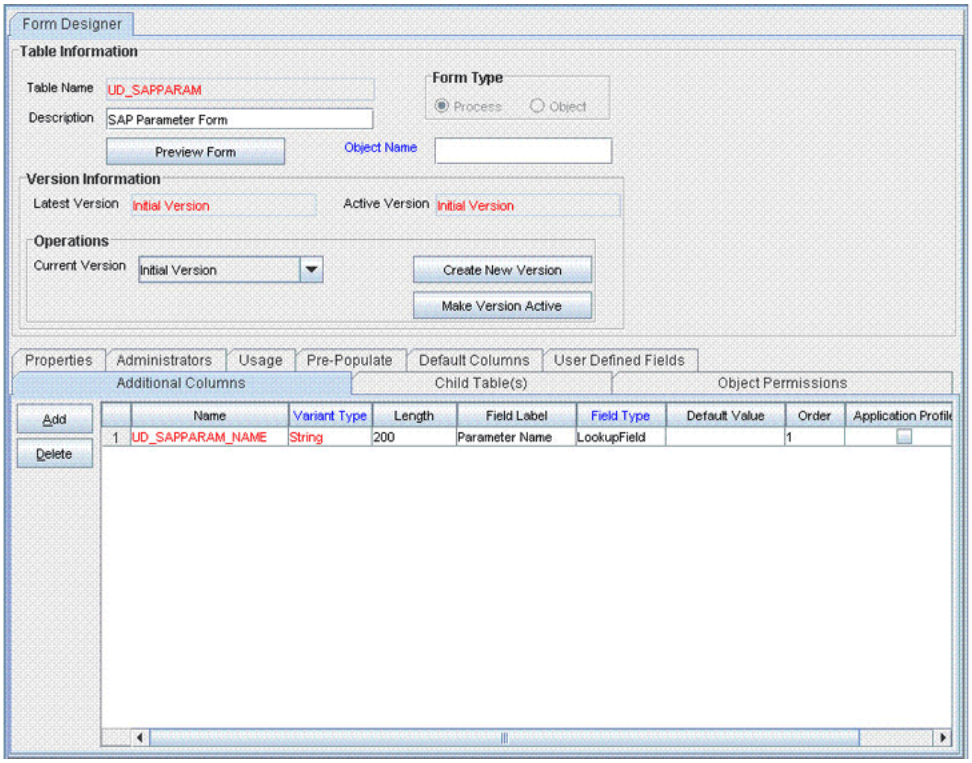


Table Information

Table Name: UD_SAPPARAM

Description: SAP Parameter Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: Initial Version

Active Version: Initial Version

Operations

Current Version: Initial Version

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile
1	UD_SAPPARAM_NAME	String	200	Parameter Name	LookupField		1	□

3. Associate the child form with the process form as follows:

   a. Search for and open the **UD_SAP** process form.

   b. Click **Create New Version**.

   c. Click the **Child Table(s)** tab.

   d. Click **Assign**.

   e. In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK**.

   f. Click the Save icon and then click **Make Version Active.** The following screenshot shows the child form added to the process form:

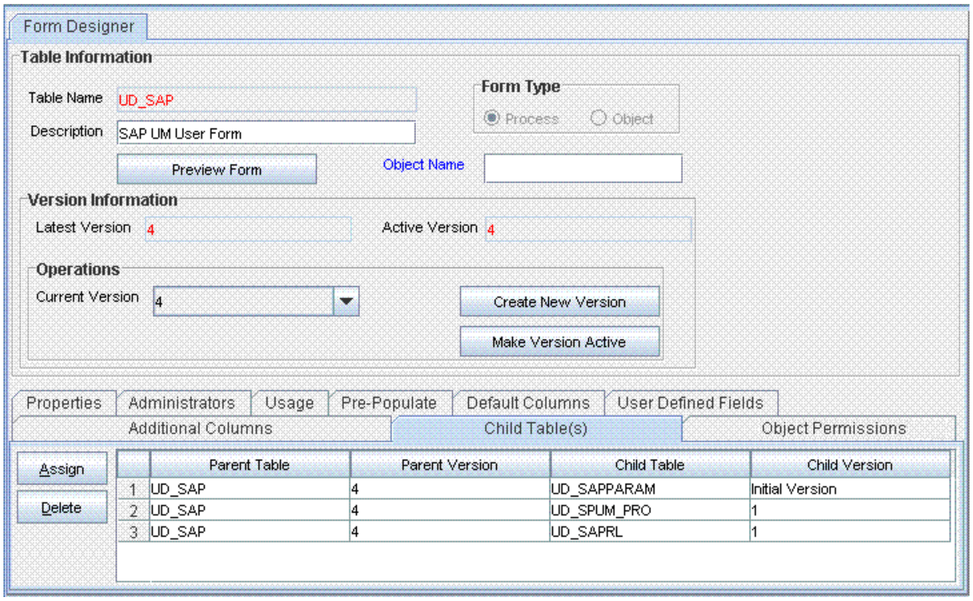


Table Information

Table Name: UD_SAP

Description: SAP UM User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 4

Active Version: 4

Operations

Current Version: 4

	Parent Table	Parent Version	Child Table	Child Version
1	UD_SAP	4	UD_SAPPARAM	Initial Version
2	UD_SAP	4	UD_SPUM_PRO	1
3	UD_SAP	4	UD_SAPRL	1

4. Add the new multivalued attribute to the list of reconciliation fields in the resource object as follows:

   a. Expand **Resource Management**.

   b. Double-click **Resource Objects**.

   c. Search for and open the **SAP UM** resource object.

   d. On the Object Reconciliation tab, click **Add Field**.

   e. In the Add Reconciliation Fields dialog box, enter the details of the field.

      For example, enter `User Parameter` in the **Field Name** field and select **Multi Valued Attribute** from the Field Type list.

   f. Click the Save icon and then close the dialog box.

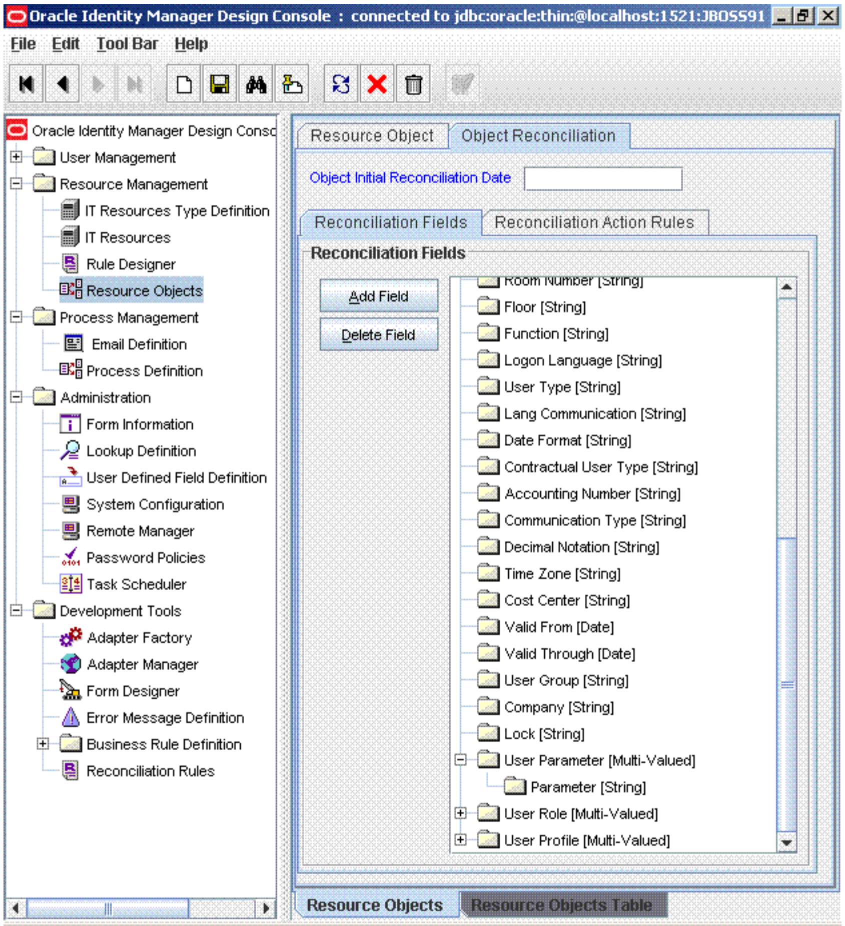
   g. Right-click the newly created attribute.

   h. Select **Define Property Fields**.

   i. In the Add Reconciliation Fields dialog box, enter the details of the newly created attribute.

      For example, enter `Parameter` in the Field Name field and select **String** from the Field Type list.

   j. Click the Save icon, and then close the dialog box. The following screenshot shows the new reconciliation field added in the resource object:



5. Create a reconciliation field mapping for the new multivalued attribute in the process definition as follows:

   a. Expand **Process Management**, and double-click **Process Definition**.

   b. Search for and open the **SAP UM Process Form** process definition.

   c. On the Reconciliation Field Mappings tab of the **SAP UM Process Form** process definition, click **Add Table Map**.

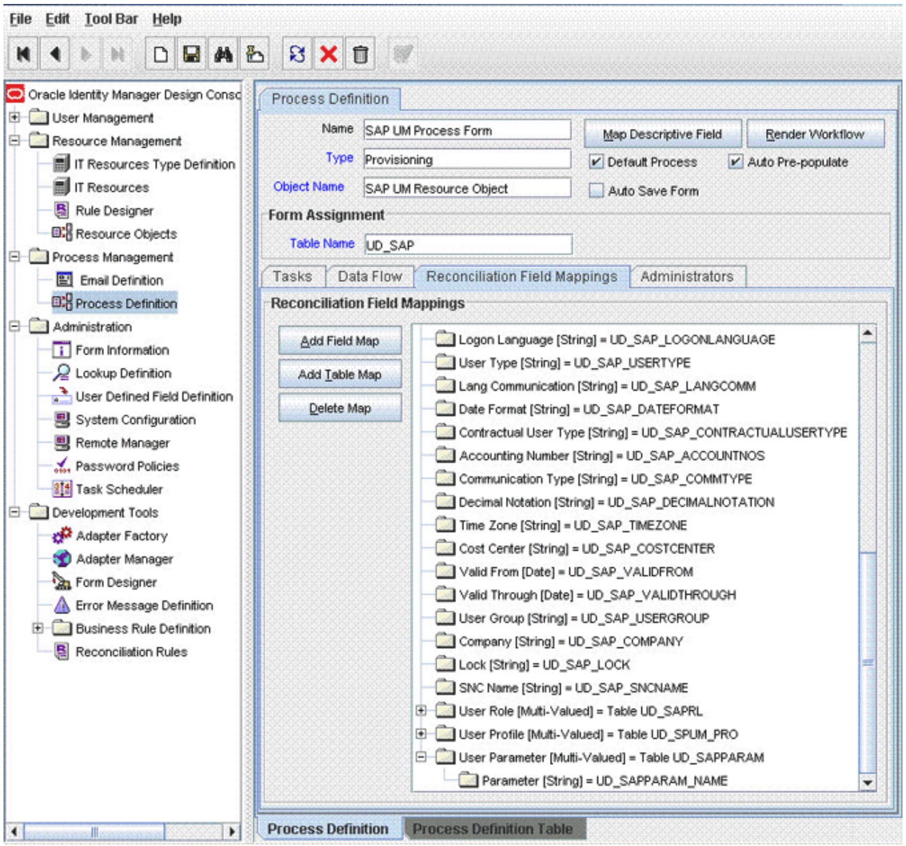
   d. In the Add Reconciliation Table Mapping dialog box, select the attribute name and table name from the list, click the Save icon, and then close the dialog box.

   e. Right-click the newly created attribute, and select **Define Property Field Map**.

   f. In the Field Name field, select the value for the attribute that you want to add.

   g. Double-click the Process Data Field field, and then select **UD_SAPPARAM_NAME**.

   h. Select **Key Field for Reconciliation Field Matching** and click the Save icon. The following screenshot shows the new reconciliation field mapped to a process data field in the process definition:



Name: SAP UM Process Form

Type: Provisioning

Object Name: SAP UM Resource Object

☑ Default Process ☑ Auto Pre-populate

☐ Auto Save Form

Table Name: UD_SAP

Reconciliation Field Mappings

- Logon Language [String] = UD_SAP_LOGONLANGUAGE
- User Type [String] = UD_SAP_USERTYPE
- Lang Communication [String] = UD_SAP_LANGCOMM
- Date Format [String] = UD_SAP_DATEFORMAT
- Contractual User Type [String] = UD_SAP_CONTRACTUALUSERTYPE
- Accounting Number [String] = UD_SAP_ACCOUNTNOS
- Communication Type [String] = UD_SAP_COMMTYPE
- Decimal Notation [String] = UD_SAP_DECIMALNOTATION
- Time Zone [String] = UD_SAP_TIMEZONE
- Cost Center [String] = UD_SAP_COSTCENTER
- Valid From [Date] = UD_SAP_VALIDFROM
- Valid Through [Date] = UD_SAP_VALIDTHROUGH
- User Group [String] = UD_SAP_USERGROUP
- Company [String] = UD_SAP_COMPANY
- Lock [String] = UD_SAP_LOCK
- SNC Name [String] = UD_SAP_SNCNAME
- User Role [Multi-Valued] = Table UD_SAPRL
- User Profile [Multi-Valued] = Table UD_SPUM_PRO
- User Parameter [Multi-Valued] = Table UD_SAPPARAM
  - Parameter [String] = UD_SAPPARAM_NAME

6. Create an entry for the new multivalued attribute in the lookup definition for reconciliation as follows:

   a. Expand **Administration**.

   b. Double-click **Lookup Definition.**

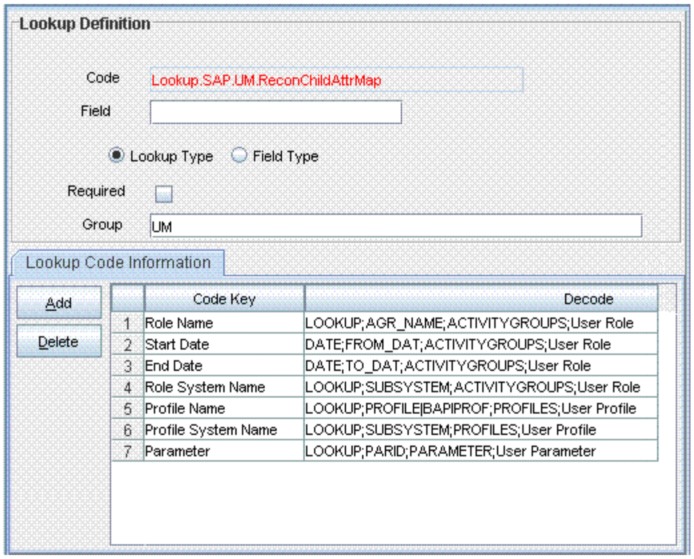
   c. Search for and open the **Lookup.SAP.UM.ReconChildAttrMap** lookup definition.

   Note: For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the attribute names are case-sensitive.

   ---

   d. Click **Add** and enter the Code Key and Decode values for the attribute, and then click the Save icon. The Code Key value must be the name of the field in the resource object. The Decode value is what you determine by performing the procedure described in Section 4.1, "Determining the Names of Target System Attributes".

   For example, enter `Parameter` in the Code Key field and then enter `LOOKUP;PARID;PARAMETER;User parameter` in the Decode field. The following screenshot shows the entry added to the lookup definition:



Code: Lookup.SAP.UM.ReconChildAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: UM

	Code Key	Decode
1	Role Name	LOOKUP;AGR_NAME;ACTIVITYGROUPS;User Role
2	Start Date	DATE;FROM_DAT;ACTIVITYGROUPS;User Role
3	End Date	DATE;TO_DAT;ACTIVITYGROUPS;User Role
4	Role System Name	LOOKUP;SUBSYSTEM;ACTIVITYGROUPS;User Role
5	Profile Name	LOOKUP;PROFILE|BAPIPROF;PROFILES;User Profile
6	Profile System Name	LOOKUP;SUBSYSTEM;PROFILES;User Profile
7	Parameter	LOOKUP;PARID;PARAMETER;User Parameter

7. If the attribute is a custom multivalued attribute, then add it in Lookup.SAP.UM.CustomChildAttrMap lookup definition as follows:

   Note: For a change in a custom attribute to be detected during incremental reconciliation, at least one standard attribute in the same record must be modified.

   a. Expand **Administration**.

   b. Double-click **Lookup Definition.**

   c. Search for and open the **Lookup.SAP.UM.CustomChildAttrMap** lookup definition.

   d. Click **Add.**

   e. In the **Code Key** column, enter the name of the resource object field that you create for the custom attribute.

   f. In the **Decode** column of the lookup definition, enter a value in one of the following formats:

   Note: For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the attribute names are case-sensitive.

   If you want a custom BAPI to fetch values from this attribute, then enter a value in the following format:

   CUSTOM_BAPI_NAME;*FIELD_TYPE*;*TABLE_NAME*;*FIELD_NAME*;*KEY_USER_ID_FIELD*;*CHILD_TABLE_NAME*

   If you want a custom RFC table to fetch values from this attribute, then enter a value in the following format:

   RFC_READ_TABLE;*FIELD_TYPE*;*TABLE_NAME*;*FIELD_NAME*;*KEY_USER_ID_FIELD*;*CHILD_TABLE_NAME*

In these formats:

- *CUSTOM_BAPI_NAME* is the name of the custom BAPI that you created for fetching values from the custom attribute.
- *FIELD_TYPE* is the type of data that is stored in the custom attribute. It can be TEXT, DATE, or CHECKBOX.
- *TABLE_NAME* is the name of the custom table that contains the attribute.
- *FIELD_NAME* is the name of the attribute in the custom table.
- *KEY_USER_ID_FIELD* is the attribute in the custom table that holds user ID values.
- *CHILD_TABLE_NAME* is the child table name of OIM

The following is a sample value for the Decode column:

```
ZBAPI_CUSTFIELDS;TEXT;ZCUSTFIELDS;FIELD1;USERNAME;CustomFields
```

g. Click the Save icon.

4.4 Adding New Standard Attributes for Provisioning

By default, the attributes listed in Table 1–8 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

> **Note:** Perform the procedure described in this section only if you want to map standard target system attributes for provisioning. If you want to add a standard multivalued attribute for provisioning, then see Section 4.6, "Adding New Standard Multivalued Attributes for Provisioning". If you want to add a custom attribute for provisioning, then see Section 4.7, "Adding Custom Attributes for Provisioning".

Summary of the procedure to add a new standard attribute for provisioning

1. Add the new standard attribute on the process form.
2. Create an entry for the attribute in the Lookup.SAP.UM.ProvAttrMap lookup definition.
3. If the attribute is a check box, then create an entry in the Lookup.SAP.UM.ProvCheckBoxMapping lookup definition.
4. Create a task to enable update of the attribute during provisioning operations.

To add a new standard attribute for provisioning:

> **Note:**
>
> See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure.
>
> If you have already added an attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new standard attribute on the process form as follows:

a. Expand **Development Tools**, and double-click **Form Designer**.

b. Search for and open the **UD_SAP** process form.

c. Click **Create New Version**, and then click **Add**.

d. Enter the details of the attribute.

For example, if you are adding the Room No field, enter `UD_SAP_ROOM_NO` in the Name field, and then enter the rest of the details of this field.

e. Click the Save icon, and then click **Make Version Active.** The following screenshot shows the new field added to the process form:

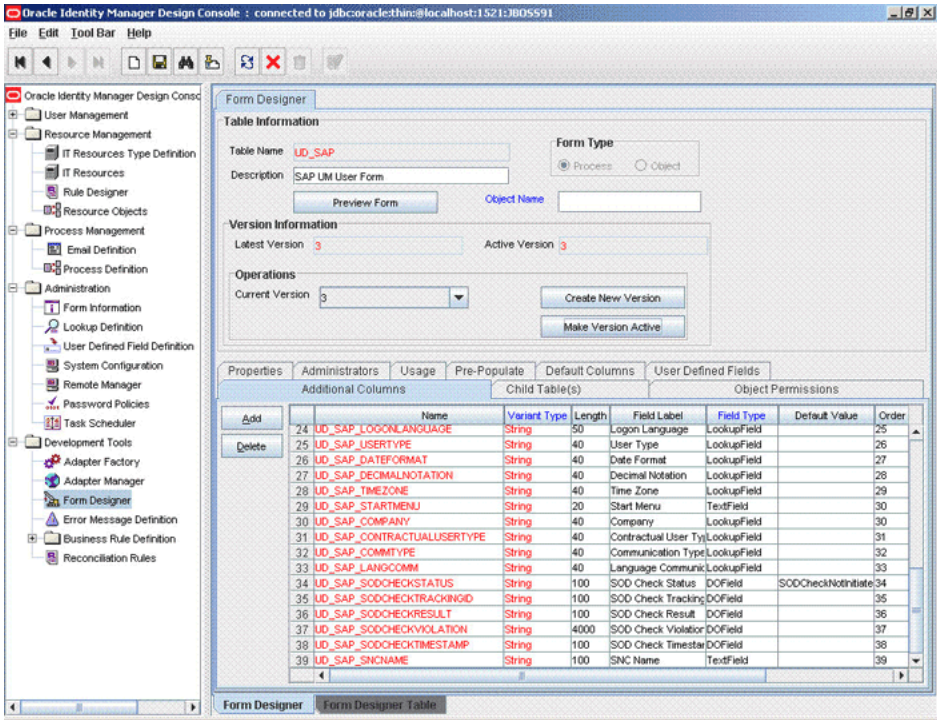


Table Information

Table Name: UD_SAP

Description: SAP UM User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 3

Active Version: 3

Operations

Current Version: 3

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order
24	UD_SAP_LOGONLANGUAGE	String	50	Logon Language	LookupField		25
25	UD_SAP_USERTYPE	String	40	User Type	LookupField		26
26	UD_SAP_DATEFORMAT	String	40	Date Format	LookupField		27
27	UD_SAP_DECIMALNOTATION	String	40	Decimal Notation	LookupField		28
28	UD_SAP_TIMEZONE	String	40	Time Zone	LookupField		29
29	UD_SAP_STARTMENU	String	20	Start Menu	TextField		30
30	UD_SAP_COMPANY	String	40	Company	LookupField		30
31	UD_SAP_CONTRACTUALUSERTYPE	String	40	Contractual User Ty	LookupField		31
32	UD_SAP_COMMTYPE	String	40	Communication Type	LookupField		32
33	UD_SAP_LANGCOMM	String	40	Language Communic	LookupField		33
34	UD_SAP_SODCHECKSTATUS	String	100	SOD Check Status	DOField	SODCheckNotInitiate	34
35	UD_SAP_SODCHECKTRACKINGID	String	100	SOD Check Tracking	DOField		35
36	UD_SAP_SODCHECKRESULT	String	100	SOD Check Result	DOField		36
37	UD_SAP_SODCHECKVIOLATION	String	4000	SOD Check Violatior	DOField		37
38	UD_SAP_SODCHECKTIMESTAMP	String	100	SOD Check Timestar	DOField		38
39	UD_SAP_SNCNAME	String	100	SNC Name	TextField		39

3. Create an entry for the attribute in the lookup definition for provisioning as follows:

a. Expand **Administration**.

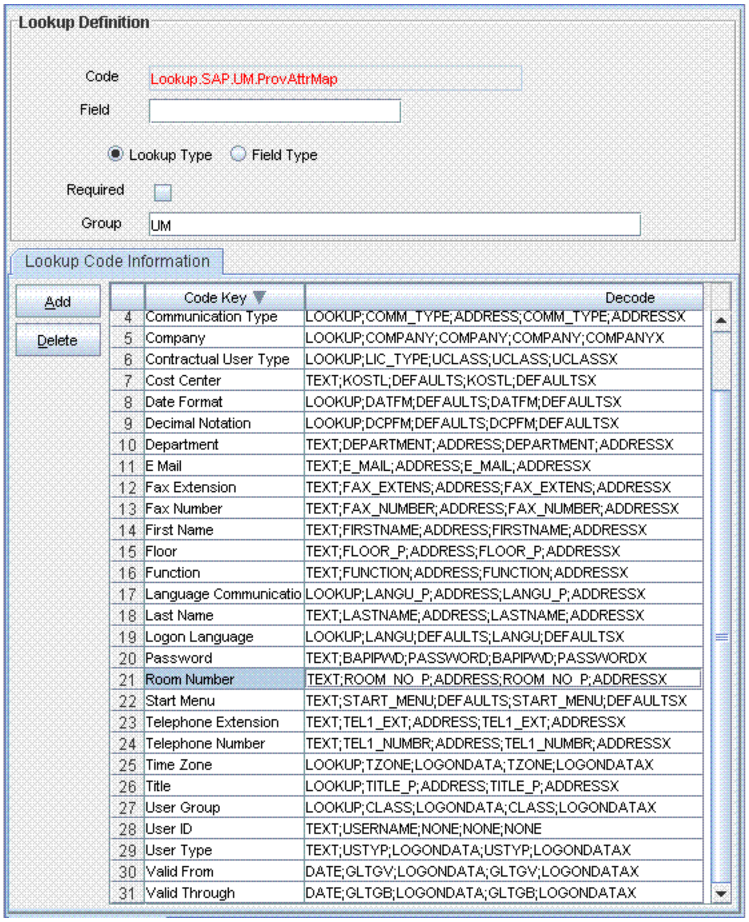
b. Double-click **Lookup Definition.**

c. Search for and open the Lookup.SAP.UM.ProvAttrMap lookup definition.

d. Click **Add** and then enter the Code Key and Decode values for the attribute.

The Code Key value must be the name of the field on the process form. The Decode value is what you determine by performing the procedure described in Section 4.1, "Determining the Names of Target System Attributes".

For example, enter `Room Number` in the **Code Key** column and then enter `TEXT;ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX` in the **Decode** column. The following screenshot shows the entry added to the lookup definition:



Lookup Definition

Code: Lookup.SAP.UM.ProvAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: UM

Lookup Code Information

	Code Key	Decode
4	Communication Type	LOOKUP;COMM_TYPE;ADDRESS;COMM_TYPE;ADDRESSX
5	Company	LOOKUP;COMPANY;COMPANY;COMPANY;COMPANYX
6	Contractual User Type	LOOKUP;LIC_TYPE;UCLASS;UCLASS;UCLASSX
7	Cost Center	TEXT;KOSTL;DEFAULTS;KOSTL;DEFAULTSX
8	Date Format	LOOKUP;DATFM;DEFAULTS;DATFM;DEFAULTSX
9	Decimal Notation	LOOKUP;DCPFM;DEFAULTS;DCPFM;DEFAULTSX
10	Department	TEXT;DEPARTMENT;ADDRESS;DEPARTMENT;ADDRESSX
11	E Mail	TEXT;E_MAIL;ADDRESS;E_MAIL;ADDRESSX
12	Fax Extension	TEXT;FAX_EXTENS;ADDRESS;FAX_EXTENS;ADDRESSX
13	Fax Number	TEXT;FAX_NUMBER;ADDRESS;FAX_NUMBER;ADDRESSX
14	First Name	TEXT;FIRSTNAME;ADDRESS;FIRSTNAME;ADDRESSX
15	Floor	TEXT;FLOOR_P;ADDRESS;FLOOR_P;ADDRESSX
16	Function	TEXT;FUNCTION;ADDRESS;FUNCTION;ADDRESSX
17	Language Communicatio	LOOKUP;LANGU_P;ADDRESS;LANGU_P;ADDRESSX
18	Last Name	TEXT;LASTNAME;ADDRESS;LASTNAME;ADDRESSX
19	Logon Language	LOOKUP;LANGU;DEFAULTS;LANGU;DEFAULTSX
20	Password	TEXT;BAPIPWD;PASSWORD;BAPIPWD;PASSWORDX
21	Room Number	TEXT;ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX
22	Start Menu	TEXT;START_MENU;DEFAULTS;START_MENU;DEFAULTSX
23	Telephone Extension	TEXT;TEL1_EXT;ADDRESS;TEL1_EXT;ADDRESSX
24	Telephone Number	TEXT;TEL1_NUMBR;ADDRESS;TEL1_NUMBR;ADDRESSX
25	Time Zone	LOOKUP;TZONE;LOGONDATA;TZONE;LOGONDATAX
26	Title	LOOKUP;TITLE_P;ADDRESS;TITLE_P;ADDRESSX
27	User Group	LOOKUP;CLASS;LOGONDATA;CLASS;LOGONDATAX
28	User ID	TEXT;USERNAME;NONE;NONE;NONE
29	User Type	TEXT;USTYP;LOGONDATA;USTYP;LOGONDATAX
30	Valid From	DATE;GLTGV;LOGONDATA;GLTGV;LOGONDATAX
31	Valid Through	DATE;GLTGB;LOGONDATA;GLTGB;LOGONDATAX

4. Oracle Identity Manager stores the state of a check box as either 1 (selected) or 0 (deselected). In SAP, the state of check boxes is stored using different characters. If you are adding a check box attribute on the target system for provisioning, then:

   a. Search for and open the Lookup.SAP.UM.ProvCheckBoxMapping lookup definition.

   b. Depending on the check box that you want to add, create one of the entries given in the following table:

Field Label in SAP	Value to Be Entered in the Code Key Column (Sample Process Form Field Name)	Value to Be Entered in the Decode Column
Output Immediately	Output Immediately	GH
Delete After Output	Delete After Output	DK
Check Indicator	Check Indicator	X
Unsecure communication permitted (user-specific)	Unsecure communication permitted	X

   c. Save and close the lookup definition.

5. Create a task to enable update of the attribute during provisioning operations.

If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of the attribute during provisioning operations, add a process task for updating the attribute:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

a. Expand **Process Management**, and double-click **Process Definition**.

b. Search for and open the **SAP UM Process Form** process definition.

c. Click **Add**.

d. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

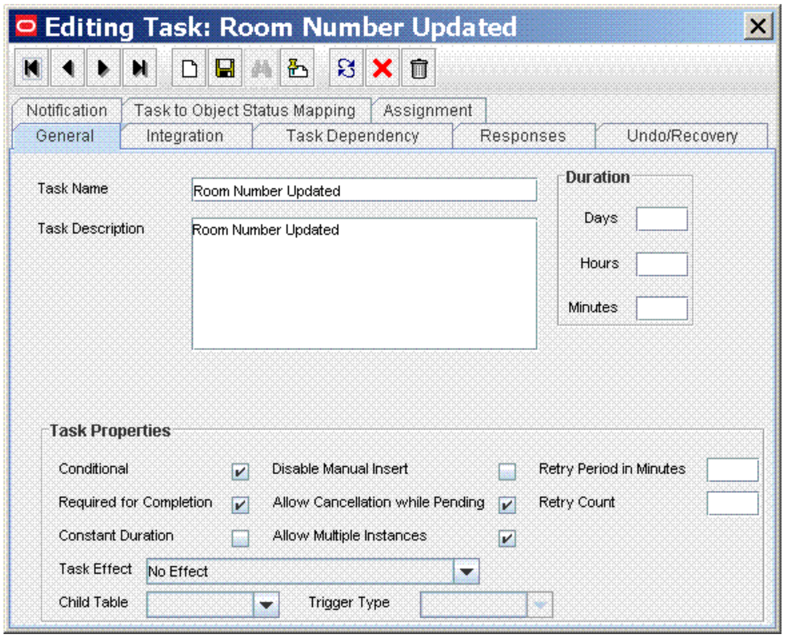
   Conditional

   Required for Completion

   Allow Cancellation while Pending

   Allow Multiple Instances

e. Click the Save icon. The following screenshot shows the new task added to the process definition:



Task Name: Room Number Updated

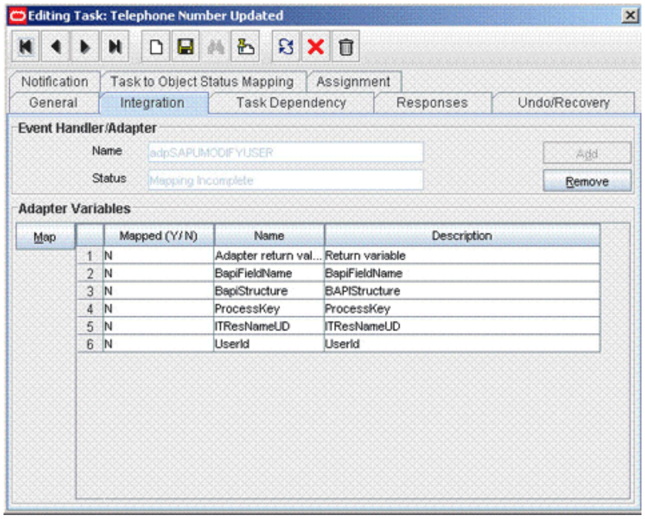
Task Description: Room Number Updated

Conditional ☑ Disable Manual Insert □
Required for Completion ☑ Allow Cancellation while Pending ☑
Constant Duration □ Allow Multiple Instances ☑
Task Effect: No Effect
Child Table:
Trigger Type:

f. On the Integration tab of the Creating New Task dialog box, click **Add**.

g. In the Handler Selection dialog box, select **Adapter**, click **adpSAPUMODIFYUSER**, and then click the Save icon.

   The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Name: adpSAPUMODIFYUSER

Status: Mapping Incomplete

	Mapped (Y/N)	Name	Description
1	N	Adapter return val...	Return variable
2	N	BapiFieldName	BapiFieldName
3	N	BapiStructure	BAPIStructure
4	N	ProcessKey	ProcessKey
5	N	ITResNameUD	ITResNameUD
6	N	UserId	UserId

h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the Save icon.

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	BapiFieldName	Literal	String For example: ROOM_NO_P
Third	BapiStructure	Literal	String For example: ADDRESS
Fourth	ProcessKey	Process Data	Process Instance
Fifth	ITResNameU	Literal	String For example: UD_SAP_ITRESOURCE
Sixth	UserId	Process Data	User ID

j. Click the Save icon in the Editing Task dialog box, and then close the dialog box.

k. Click the Save icon to save changes to the process definition.

4.5 Adding New Standard SAP GRC Compliant User Provisioning Attributes for Provisioning

By default, the attributes listed in Table 1–10 are mapped for sending requests from Oracle Identity Manager to SAP GRC Compliant User Provisioning. If required, you can map additional single-valued attributes.

Note: Perform the procedure described in this section only if you want to map additional standard Compliant User Provisioning attributes for requests sent from Oracle Identity Manager to Compliant User Provisioning.

Summary of the procedure to add a new SAP GRC Compliant User Provisioning attribute for provisioning

1. Determine the name of the attribute on Compliant User Provisioning.
2. Add the attribute on the process form.
3. Create an entry for the attribute in the Lookup.SAP.CUP.ProvAttrMap lookup definition.
4. Create a task to enable update of the attribute during provisioning operations.

To add a new SAP GRC Compliant User Provisioning attribute for provisioning:

1. To determine the name of the attribute on Compliant User Provisioning:

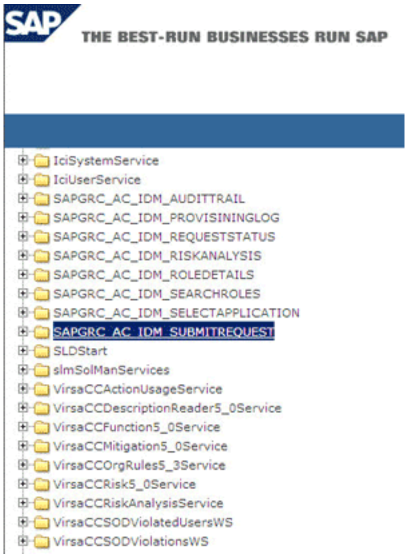
   a. In a browser, open the Web Services Navigator for SAP GRC Access Control.

      The URL that you use to open the Web Services Navigator is of the following format:

      ```
      http://SERVER:PORT/wsnavigator/enterwsdl.html
      ```

   b. In the list of Web services that is displayed, search for and click the **SAPGRC_AC_IDM_SUBMITREQUEST** Web service.

      The following screenshot shows this page:

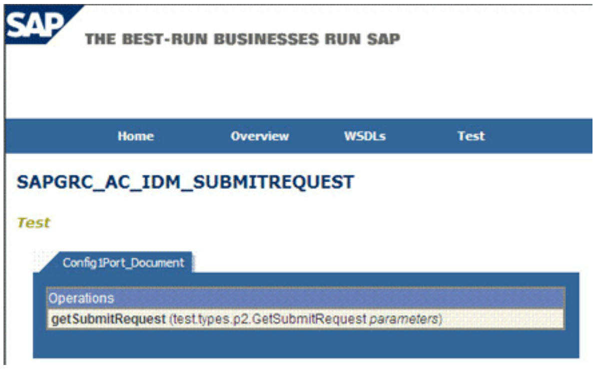


IciSystemService
IciUserService
SAPGRC_AC_IDM_AUDITTRAIL
SAPGRC_AC_IDM_PROVISININGLOG
SAPGRC_AC_IDM_REQUESTSTATUS
SAPGRC_AC_IDM_RISKANALYSIS
SAPGRC_AC_IDM_ROLEDETAILS
SAPGRC_AC_IDM_SEARCHROLES
SAPGRC_AC_IDM_SELECTAPPLICATION
SAPGRC_AC_IDM_SUBMITREQUEST
SLDStart
slmSolManServices
VirsaCCActionUsageService
VirsaCCDescriptionReader5_0Service
VirsaCCFunction5_0Service
VirsaCCMitigation5_0Service
VirsaCCOrgRules5_3Service
VirsaCCRisk5_0Service
VirsaCCRiskAnalysisService
VirsaCCSODViolatedUsersWS
VirsaCCSODViolationsWS

   c. Click the **Test** option on the menu bar.

   d. Click the **getSubmitRequest (test.types.p2.GetSubmitRequest parameters)** operation.

      The following screenshot shows this page:



SAPGRC_AC_IDM_SUBMITREQUEST

Test

Config1Port_Document

Operations

getSubmitRequest (test.types.p2.GetSubmitRequest *parameters*)

e. From the list of attributes that is displayed, copy the name of the attribute that you want to add. Do not copy the data type of the attribute. For example, copy `telephone`.

2. Log in to the Oracle Identity Manager Design Console.

> **Note:** See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure

3. If the attribute does not already exist on the process form, then add it on the process form as follows:

   a. Expand Development Tools, and double-click Form Designer.

   b. Search for and open the UD_SAP process form.

   c. Click Create New Version, and then click Add.

   d. Enter the details of the attribute.

   For example, if you are adding the Telephone field, enter UD_SAP_TELEPHONE in the Name field, and then enter the rest of the details of this field.

   The following screenshot shows this page:

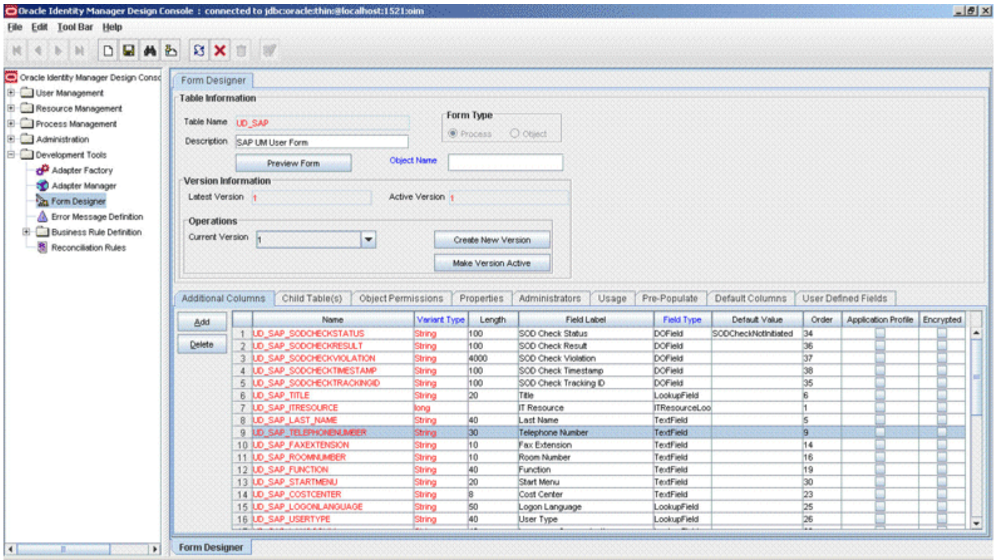


Table Information

Table Name: UD_SAP

Description: SAP UM User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 1

Active Version: 1

Operations

Current Version: 1

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encrypted
1	UD_SAP_SODCHECKSTATUS	String	100	SOD Check Status	DOField	SODCheckNotInitiated	34	☐	☐
2	UD_SAP_SODCHECKRESULT	String	100	SOD Check Result	DOField		36	☐	☐
3	UD_SAP_SODCHECKVIOLATION	String	4000	SOD Check Violation	DOField		37	☐	☐
4	UD_SAP_SODCHECKTIMESTAMP	String	100	SOD Check Timestamp	DOField		38	☐	☐
5	UD_SAP_SODCHECKTRACKINGID	String	100	SOD Check Tracking ID	DOField		35	☐	☐
6	UD_SAP_TITLE	String	20	Title	LookupField		6	☐	☐
7	UD_SAP_ITRESOURCE	long		IT Resource	ITResourceLoo		1	☐	☐
8	UD_SAP_LAST_NAME	String	40	Last Name	TextField		5	☐	☐
9	UD_SAP_TELEPHONENUMBER	String	30	Telephone Number	TextField		9	☐	☐
10	UD_SAP_FAXEXTENSION	String	10	Fax Extension	TextField		14	☐	☐
11	UD_SAP_ROOMNUMBER	String	10	Room Number	TextField		16	☐	☐
12	UD_SAP_FUNCTION	String	40	Function	TextField		19	☐	☐
13	UD_SAP_STARTMENU	String	20	Start Menu	TextField		30	☐	☐
14	UD_SAP_COSTCENTER	String	8	Cost Center	TextField		23	☐	☐
15	UD_SAP_LOGONLANGUAGE	String	50	Logon Language	LookupField		25	☐	☐
16	UD_SAP_USERTYPE	String	40	User Type	LookupField		26	☐	☐

e. Click the Save icon, and then click **Make Version Active**. The following screenshot shows the new field added to the process form:

4. Create an entry for the attribute in the Lookup.SAP.CUP.ProvAttrMap lookup definition as follows:

   a. Expand Administration.

   b. Double-click Lookup Definition.

   c. Search for and open the Lookup.SAP.CUP.ProvAttrMap lookup definition.

   d. Click Add and then enter the Code Key and Decode values for the attribute.

   The Code Key value must be the name of the field on the process form. The Decode value is in the following format:

   FIELD_NAME;FIELD_TYPE;STANDARD_OR_CUSTOM;BAPI_FIELD_NAME;MANDATORY_OR_NONE

   In this format:

   – *FIELD_TYPE* can be TEXT or DATE.

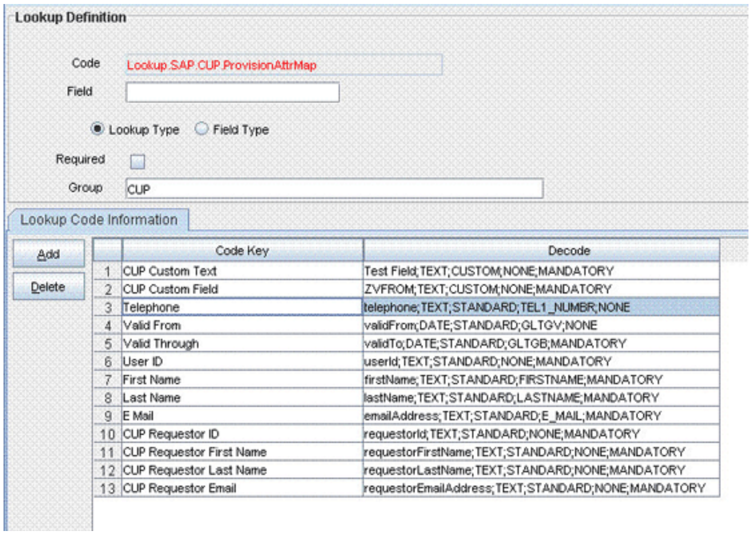
   – *FIELD_NAME* is the name of the attribute. You determine this name by performing the procedure described in Step 1.

   – *STANDARD_OR_CUSTOM* is used to specify whether the attribute is a standard or custom on SAP GRC Compliant User Provisioning.

   – *BAPI_FIELD_NAME* is the BAPI name of the field added in the Lookup.SAP.UM.ProvAttrMap lookup definition when you performed Step 3 of Section 4.4, "Adding New Standard Attributes for Provisioning." If the attribute that you are adding exists only on SAP GRC Compliant User Provisioning and not on the target system, then enter NONE as the value of *BAPI_FIELD_NAME*.

   – *MANDATORY_OR_NONE* is used to specify whether the attribute is a mandatory or nonmandatory attribute in the request submitted to SAP GRC Compliant User Provisioning.

   The following screenshot shows this page:



Lookup Definition

Code: Lookup.SAP.CUP.ProvisionAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: CUP

Lookup Code Information

	Code Key	Decode
1	CUP Custom Text	Test Field;TEXT;CUSTOM;NONE;MANDATORY
2	CUP Custom Field	ZVFROM;TEXT;CUSTOM;NONE;MANDATORY
3	Telephone	telephone;TEXT;STANDARD;TEL1_NUMBR;NONE
4	Valid From	validFrom;DATE;STANDARD;GLTGV;NONE
5	Valid Through	validTo;DATE;STANDARD;GLTGB;MANDATORY
6	User ID	userId;TEXT;STANDARD;NONE;MANDATORY
7	First Name	firstName;TEXT;STANDARD;FIRSTNAME;MANDATORY
8	Last Name	lastName;TEXT;STANDARD;LASTNAME;MANDATORY
9	E Mail	emailAddress;TEXT;STANDARD;E_MAIL;MANDATORY
10	CUP Requestor ID	requestorId;TEXT;STANDARD;NONE;MANDATORY
11	CUP Requestor First Name	requestorFirstName;TEXT;STANDARD;NONE;MANDATORY
12	CUP Requestor Last Name	requestorLastName;TEXT;STANDARD;NONE;MANDATORY
13	CUP Requestor Email	requestorEmailAddress;TEXT;STANDARD;NONE;MANDATORY

5. Create a process task to enable update of the attribute during provisioning operations if the following conditions are true:

- The task does not already exist.
- This attribute exists on both SAP GRC Compliant User Provisioning and the target system.

Note: If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of the attribute during provisioning operations, add a process task for updating the attribute:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

a. Expand **Process Management**, and double-click **Process Definition**.

b. Search for and open the **SAP UM Process Form** process definition.

c. Click **Add**.

d. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

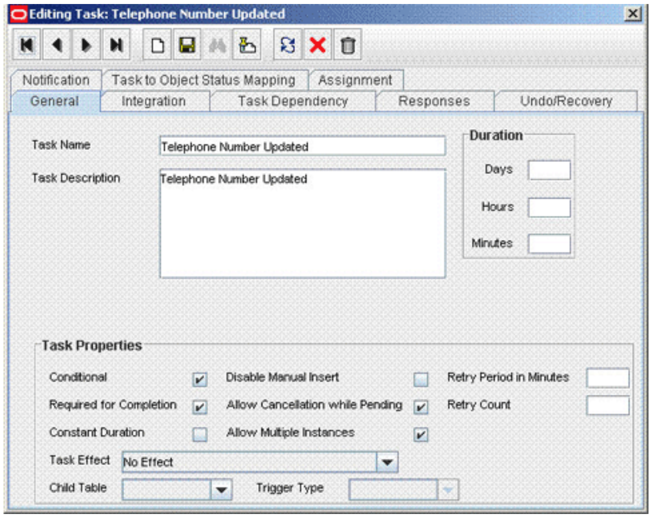
Conditional

Required for Completion

Allow Cancellation while Pending

Allow Multiple Instances

e. Click the Save icon. The following screenshot shows the new task added to the process definition:



Task Name: Telephone Number Updated

Task Description: Telephone Number Updated

Days:

Hours:

Minutes:

Conditional ☑

Disable Manual Insert ☐

Retry Period in Minutes:

Required for Completion ☑

Allow Cancellation while Pending ☑

Retry Count:

Constant Duration ☐

Allow Multiple Instances ☑

Task Effect: No Effect

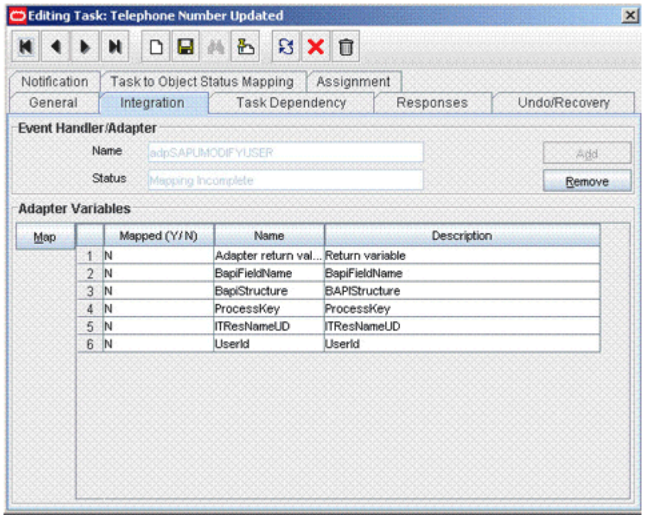
Child Table:

Trigger Type:

f. On the Integration tab of the Creating New Task dialog box, click **Add**.

g. In the Handler Selection dialog box, select **Adapter**, click **adpSAPUMODIFYUSER**, and then click the Save icon.

The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Event Handler/Adapter

Name: adpSAPUMODIFYUSER

Status: Mapping Incomplete

Adapter Variables

	Mapped (Y/N)	Name	Description
1	N	Adapter return val...	Return variable
2	N	BapiFieldName	BapiFieldName
3	N	BapiStructure	BAPIStructure
4	N	ProcessKey	ProcessKey
5	N	ITResNameUD	ITResNameUD
6	N	UserId	UserId

h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the Save icon.

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	BapiFieldName	Literal	String For example: ROOM_NO_P
Third	BapiStructure	Literal	String For example: ADDRESS
Fourth	ProcessKey	Process Data	Process Instance
Fifth	ITResNameU	Literal	String For example: UD_SAP_ITRESOURCE
Sixth	UserId	Process Data	User ID

j. Click the Save icon in the Editing Task dialog box, and then close the dialog box.

k. Click the Save icon to save changes to the process definition.

4.6 Adding New Standard Multivalued Attributes for Provisioning

> **Note:** This section describes the procedure to add standard multivalued attributes of the target system for provisioning. Addition of custom multivalued attributes is not supported.

By default, the multivalued attributes listed in Table 1–9 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can add new multivalued fields for provisioning.

Summary of the procedure to add a new multivalued attribute for provisioning

1. Create a child form for the new multivalued attribute.
2. Associate the child form with the process form.
3. Create an entry for the attribute in the Lookup.SAP.UM.ProvChildAttrMap lookup definition.
4. Create tasks for adding, modifying, and deleting values of the attribute during provisioning operations.

To add a new multivalued attribute for provisioning:

> **Note:**
>
> See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure.
>
> If you have already added a multivalued attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

1. Log in to the Oracle Identity Manager Design Console.
2. Create a child form for the new multivalued attribute as follows:
   a. Expand **Development Tools**, and then double-click **Form Designer**.
   b. In the **Table Name** field, enter a name for the child table. For example, enter `UD_USR_PARAM`.
   c. In the **Description** field, enter a description for the child form.
   d. In the Form Type region, select **Process**.
   e. Click the Save icon.
   f. On the Additional Columns tab, click **Add**.
   g. In the Name column, enter a name for the attribute.
   h. Enter values in the remaining columns, and then click the Save icon.
   i. If you want to add more fields, then click **Add** and enter values for each field.
3. Associate the child form with the process form as follows:

> **Note:** Only the most basic instructions to create a child form are given in this section. See *Oracle Identity Manager Design Console Guide* for detailed instructions.

a. Search for and open the **UD_SAP** form.

b. Click **Create New Version**.

c. Enter a version name, and then click the Save icon.

d. From the **Current Version** list, select the version that you created.

e. On the Child Tables tab, click **Assign**.

f. From the list on the left, select the child table and then move it to the list on the right. Then, click **OK**.

g. Click **Make Version Active**.

4. Create an entry for the attribute in the lookup definition for multivalued attribute provisioning as follows:

a. Expand **Administration**, and double-click **Lookup Definition**.

b. Search for and open the **Lookup.SAP.UM.ProvChildAttrMap** lookup definition.

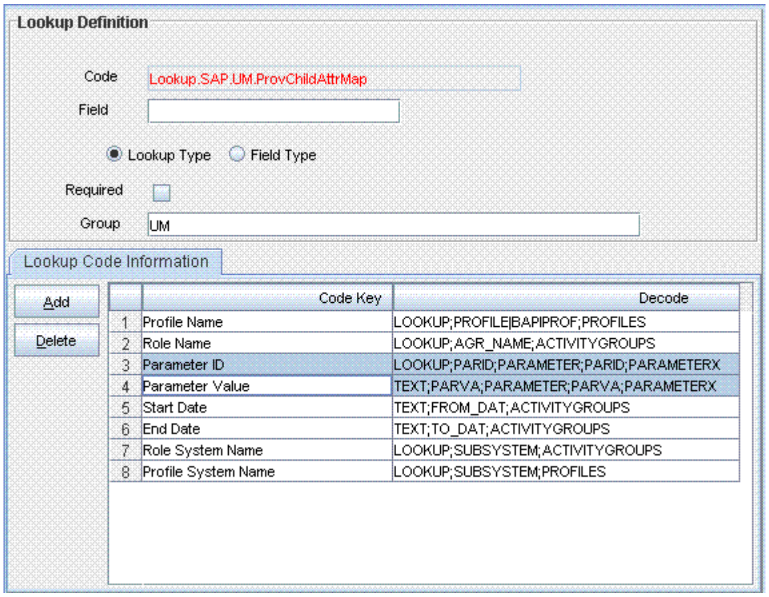
c. Click **Add** and then enter the Code Key and Decode values for the attribute.

The Code Key value must be the name of the field on the process form. The Decode value is what you determine by performing the procedure described in Section 4.1, "Determining the Names of Target System Attributes".

For example, suppose you want to add the Parameters child table, which has two attributes: Parameter ID and Parameter Value. For these attributes, you can create the following Decode entries:

```
LOOKUP;PARID;PARAMETER;PARID;PARAMETERX
TEXT;PARVA;PARAMETER;PARVA;PARAMETERX
```

The following screenshot shows the entry added to the lookup definition:



Code: Lookup.SAP.UM.ProvChildAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: UM

	Code Key	Decode
1	Profile Name	LOOKUP;PROFILE|BAPIPROF;PROFILES
2	Role Name	LOOKUP;AGR_NAME;ACTIVITYGROUPS
3	Parameter ID	LOOKUP;PARID;PARAMETER;PARID;PARAMETERX
4	Parameter Value	TEXT;PARVA;PARAMETER;PARVA;PARAMETERX
5	Start Date	TEXT;FROM_DAT;ACTIVITYGROUPS
6	End Date	TEXT;TO_DAT;ACTIVITYGROUPS
7	Role System Name	LOOKUP;SUBSYSTEM;ACTIVITYGROUPS
8	Profile System Name	LOOKUP;SUBSYSTEM;PROFILES

5. Expand **Process Management**, and double-click **Process Definition**.

6. Search for and open the **SAP UM Process Form** process definition.

7. In the process definition, create a process task for adding values in the attribute:

a. Click **Add**.

b. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

   Conditional

   Required for Completion

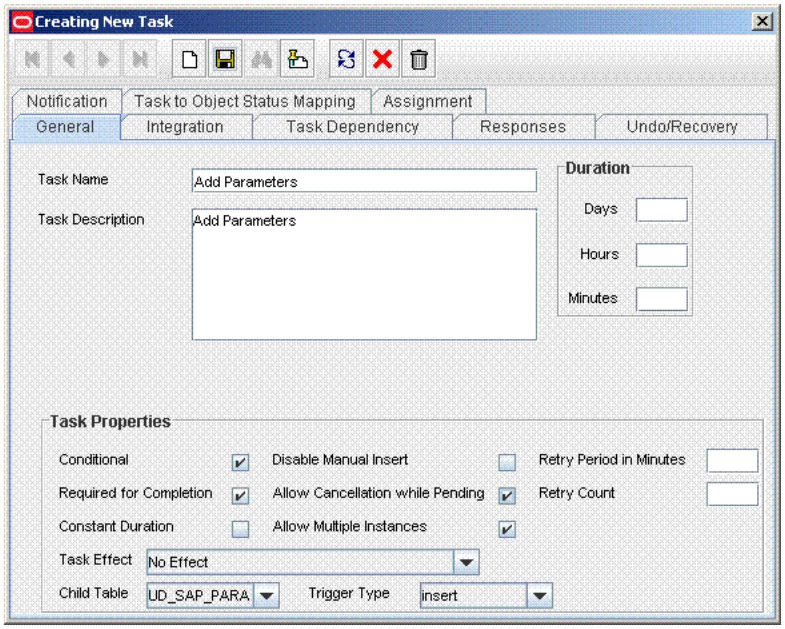
   Allow Cancellation while Pending

   Allow Multiple Instances

c. From the **Child Table** list, select the child table name.

d. From the **Trigger Type** list, select **Insert**.

e. Click the Save icon. The following screenshot shows the new task added to the process definition:



Task Name: Add Parameters

Task Description: Add Parameters

Duration

Days:

Hours:

Minutes:

Task Properties

Conditional	☑	Disable Manual Insert	□	Retry Period in Minutes	
Required for Completion	☑	Allow Cancellation while Pending	☑	Retry Count	
Constant Duration	□	Allow Multiple Instances	☑		

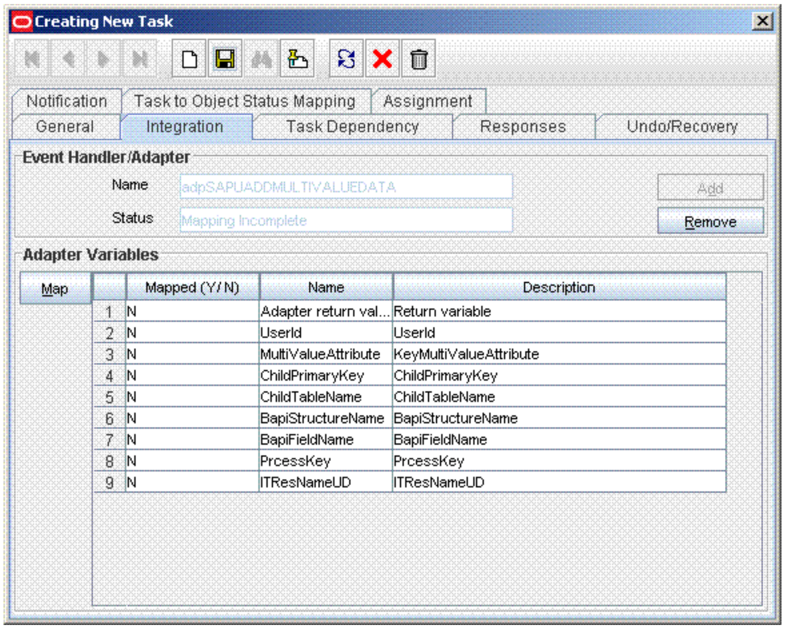
Task Effect: No Effect

Child Table: UD_SAP_PARA   Trigger Type: insert

f. On the Integration tab of the Creating New Task dialog box, click **Add**.

g. In the Handler Selection dialog box, select **Adapter**, click **adpSAPUAddMultiValueData**, and then click the Save icon.

   The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Event Handler/Adapter

Name: adpSAPUADDMULTIVALUEDATA

Status: Mapping Incomplete

Adapter Variables

	Mapped (Y/ N)	Name	Description
1	N	Adapter return val...	Return variable
2	N	UserId	UserId
3	N	MultiValueAttribute	KeyMultiValueAttribute
4	N	ChildPrimaryKey	ChildPrimaryKey
5	N	ChildTableName	ChildTableName
6	N	BapiStructureName	BapiStructureName
7	N	BapiFieldName	BapiFieldName
8	N	PrcessKey	PrcessKey
9	N	ITResNameUD	ITResNameUD

h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the Save icon.

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	UserId	Process Data	User ID
Third	MultiValueAttribute	Process Data / Child Form Name	Key Multi Valued Attribute present in child form For example: Parameter ID
Fourth	ChildPrimaryKey	Literal	String UD field of key multivalued Attribute taken from the child form For example: UD_SPUM_PARAM_ID
Fifth	ChildTableName	Literal	String UD field of the child form For example: UD_SPUM_PARAM
Sixth	BapiStructureName	Literal	String For example: PARAMETER
Seventh	BapiFieldName	Literal	String For example: PARID

Variable Number	Variable Name	Map To	Qualifier
Eighth	ProcessKey	Process Data	Process Instance
Ninth	ITResNameUD	Literal	String For example: UD_SAP_ITRESOURCE

j. Click the Save icon in the Editing Task dialog box, and then close the dialog box.

k. Click the Save icon to save changes to the process definition.

8. To enable updates of the multiValued attribute during provisioning operations, create a process task in the process definition as follows:

a. Click **Add**.

b. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

Conditional

Required for Completion

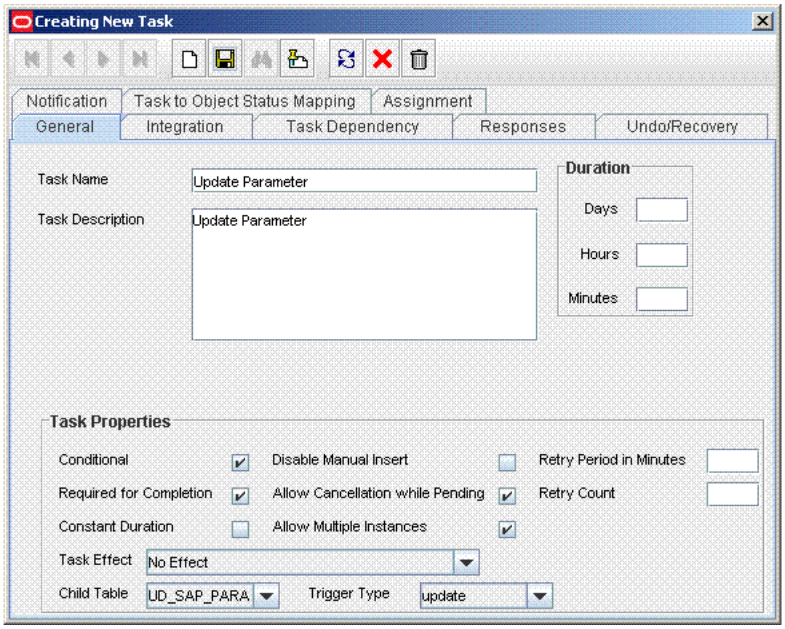
Allow Cancellation while Pending

Allow Multiple Instances

c. From the **Child Table** list, select the child table name.

d. From the **Trigger Type** list, select **Update**.

e. Click **the Save icon**. The following screenshot shows the new task added to the process definition:



Task Name: Update Parameter

Task Description: Update Parameter

Days:

Hours:

Minutes:

Conditional ☑ Disable Manual Insert □ Retry Period in Minutes:

Required for Completion ☑ Allow Cancellation while Pending ☑ Retry Count:

Constant Duration □ Allow Multiple Instances ☑

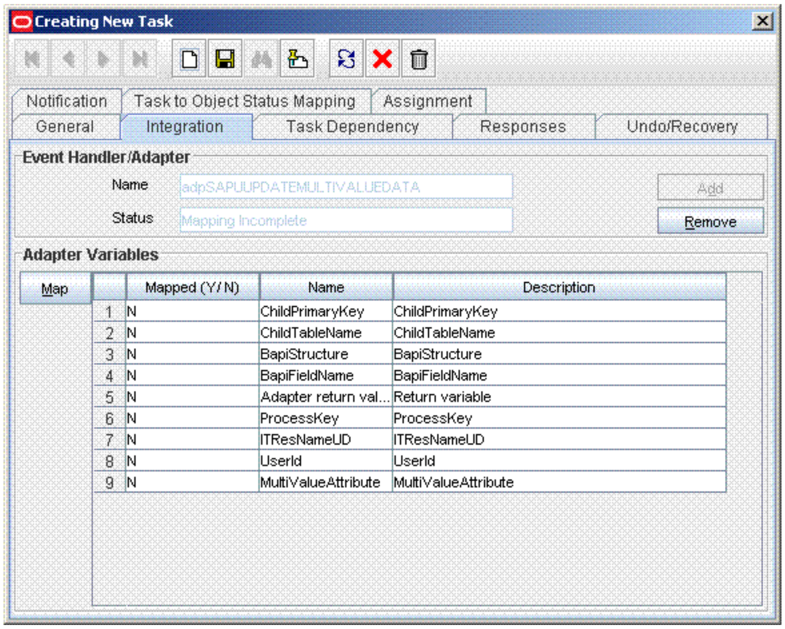
Task Effect: No Effect

Child Table: UD_SAP_PARA Trigger Type: update

f. On the Integration tab of the Creating New Task dialog box, click **Add**.

g. In the Handler Selection dialog box, select **Adapter**, click **adpSAPUUpdateMultiValueData**, and then click the Save icon.

The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Event Handler/Adapter

Name: adpSAPUUPDATEMULTIVALUEDATA

Status: Mapping Incomplete

Adapter Variables

	Mapped (Y/ N)	Name	Description
1	N	ChildPrimaryKey	ChildPrimaryKey
2	N	ChildTableName	ChildTableName
3	N	BapiStructure	BapiStructure
4	N	BapiFieldName	BapiFieldName
5	N	Adapter return val...	Return variable
6	N	ProcessKey	ProcessKey
7	N	ITResNameUD	ITResNameUD
8	N	UserId	UserId
9	N	MultiValueAttribute	MultiValueAttribute

h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the Save icon.

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	UserId	Process Data	User ID
Third	MultiValueAttribute	Process Data / Child Form Name	Key multivalued attribute present in the child form For example: Parameter Id
Fourth	ChildPrimaryKey	Literal	String UD field of key multivalued attribute taken from the child form For example: UD_SPUM_PARAM_ID
Fifth	ChildTableName	Literal	String UD field of the child form For example: UD_SPUM_PARAM
Sixth	BapiStructureName	Literal	String For example: PARAMETER
Seventh	BapiFieldName	Literal	String For example: PARID

Variable Number	Variable Name	Map To	Qualifier
Eighth	ProcessKey	Process Data	Process Instance
Ninth	ITResNameUD	Literal	String For example: UD_SAP_ITRESOURCE

j. Click the Save icon in the Editing Task dialog box, and then close the dialog box.

k. Click the Save icon to save changes to the process definition.

9. In the process definition, create a process task to delete values in the attribute:

a. Click **Add**.

b. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

Conditional

Required for Completion

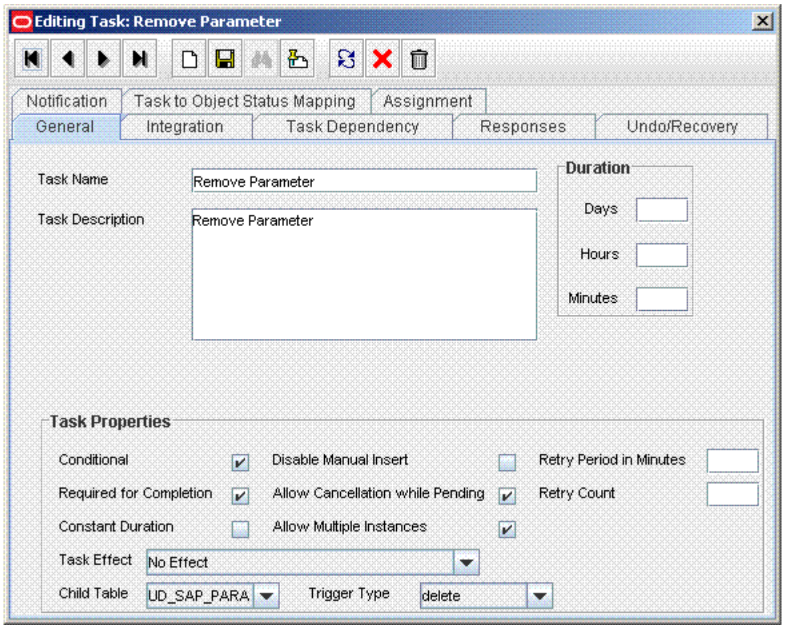
Allow Cancellation while Pending

Allow Multiple Instances

c. From the **Child Table** list, select the child table name.

d. From the **Trigger Type** list, select **Delete**.

e. Click the Save icon. The following screenshot shows the new task added to the process definition:



Editing Task: Remove Parameter

Task Name: Remove Parameter

Task Description: Remove Parameter

Duration — Days: Hours: Minutes:

Task Properties

Conditional ☑ Disable Manual Insert □ Retry Period in Minutes

Required for Completion ☑ Allow Cancellation while Pending ☑ Retry Count

Constant Duration □ Allow Multiple Instances ☑

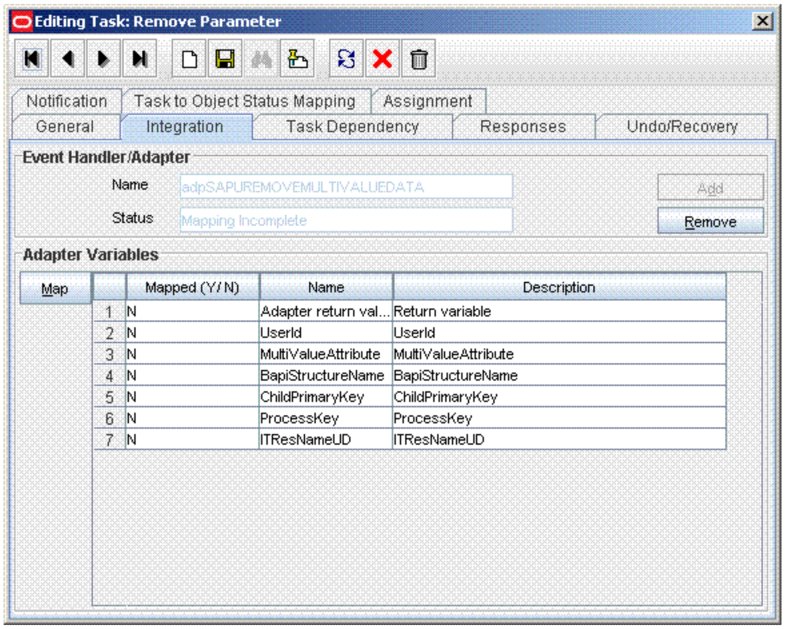
Task Effect: No Effect

Child Table: UD_SAP_PARA Trigger Type: delete

f. On the Integration tab of the Creating New Task dialog box, click **Add**.

g. In the Handler Selection dialog box, select **Adapter**, click **adpSAPURemoveMultiValueData**, and then click the Save icon.

The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Name: adpSAPUREMOVEMULTIVALUEDATA

Status: Mapping Incomplete

	Mapped (Y/N)	Name	Description
1	N	Adapter return val...	Return variable
2	N	UserId	UserId
3	N	MultiValueAttribute	MultiValueAttribute
4	N	BapiStructureName	BapiStructureName
5	N	ChildPrimaryKey	ChildPrimaryKey
6	N	ProcessKey	ProcessKey
7	N	ITResNameUD	ITResNameUD

h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the Save icon.

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	UserId	Process Data	User ID
Third	MultiValueAttribute	Process Data / Child Form Name	Key multivalued attribute present in the child form For example: Parameter Id **Note:** Select the **Old Value** check box.
Fourth	ChildPrimaryKey	Literal	String BAPI field name of Key multivalued attribute taken from the child form For example: PARID
Fifth	BapiStructureName	Literal	String For example: PARAMETER
Sixth	ProcessKey	Process Data	Process Instance
Seventh	ITResNameUD	Literal	String For example: UD_SAP_ITRESOURCE

- **j.** Click the Save icon in the Editing Task dialog box, and then close the dialog box.
- **k.** Click the Save icon to save changes to the process definition.

10. Save the changes to the process definition.

4.7 Adding Custom Attributes for Provisioning

By default, the attributes listed in Table 1–8 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

> **Note:** Perform the procedure described in this section only if you want map for provisioning custom attributes that you add on the target system. If you want to add standard target system attributes for provisioning, then see Section 4.4, "Adding New Standard Attributes for Provisioning"

Summary of the procedure to add a custom attribute for provisioning

1. Add the custom attribute on the process form.
2. If the attribute is a check box, then create an entry in the Lookup.SAP.UM.ReconCheckBoxMapping lookup definition.
3. Create a task to enable update of the attribute during provisioning operations.

To add a custom attribute for provisioning:

> **Note:**
>
> See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure.
>
> If you have already added a custom attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

1. Log in to the Oracle Identity Manager Design Console.
2. Add the custom attribute on the process form as follows:
   - **a.** Expand **Development Tools**.
   - **b.** Double-click **Form Designer.**
   - **c.** Search for and open the **UD_SAP** process form.
   - **d.** Click **Create New Version**, and then click **Add**.
   - **e.** Enter the details of the attribute.

     For example, if you are adding the Job Description field, enter `UD_SAP_JOB_DESC` in the Name field, and then enter the rest of the details of this field.
   - **f.** Click the Save icon and then click **Make Version Active.** The following screenshot shows the new field added to the process form:

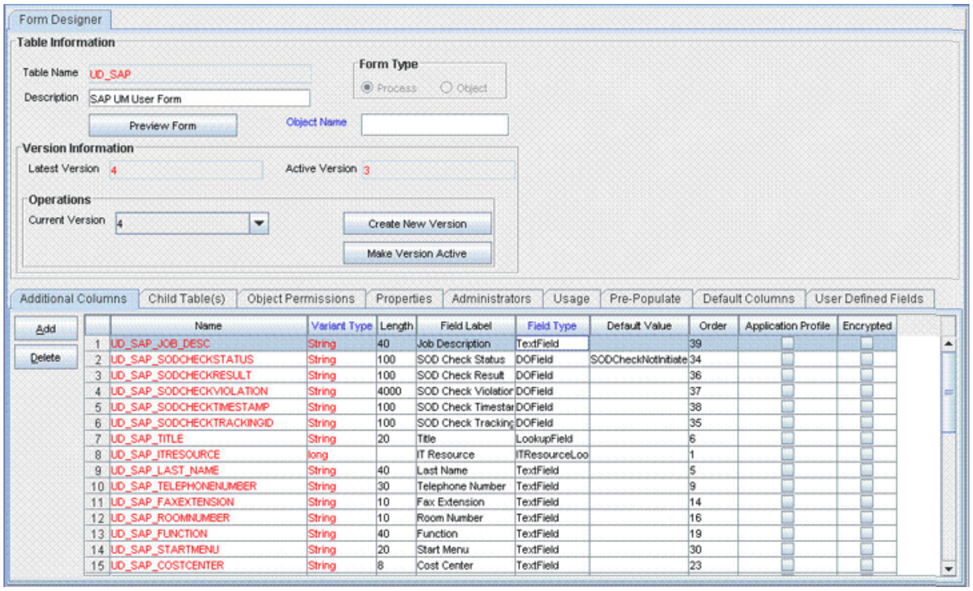


Table Information

Table Name: UD_SAP

Description: SAP UM User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 4

Active Version: 3

Operations

Current Version: 4

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encrypted
1	UD_SAP_JOB_DESC	String	40	Job Description	TextField		39	□	□
2	UD_SAP_SODCHECKSTATUS	String	100	SOD Check Status	DOField	SODCheckNotInitiate	34	□	□
3	UD_SAP_SODCHECKRESULT	String	100	SOD Check Result	DOField		36	□	□
4	UD_SAP_SODCHECKVIOLATION	String	4000	SOD Check Violatior	DOField		37	□	□
5	UD_SAP_SODCHECKTIMESTAMP	String	100	SOD Check Timestar	DOField		38	□	□
6	UD_SAP_SODCHECKTRACKINGID	String	100	SOD Check Tracking	DOField		35	□	□
7	UD_SAP_TITLE	String	20	Title	LookupField		6	□	□
8	UD_SAP_ITRESOURCE	long		IT Resource	ITResourceLoo		1	□	□
9	UD_SAP_LAST_NAME	String	40	Last Name	TextField		5	□	□
10	UD_SAP_TELEPHONENUMBER	String	30	Telephone Number	TextField		9	□	□
11	UD_SAP_FAXEXTENSION	String	10	Fax Extension	TextField		14	□	□
12	UD_SAP_ROOMNUMBER	String	10	Room Number	TextField		16	□	□
13	UD_SAP_FUNCTION	String	40	Function	TextField		19	□	□
14	UD_SAP_STARTMENU	String	20	Start Menu	TextField		30	□	□
15	UD_SAP_COSTCENTER	String	8	Cost Center	TextField		23	□	□

3. Oracle Identity Manager stores the state of a check box as either 1 (selected) or 0 (deselected). In SAP, the state of check boxes is stored using different characters. If you are adding a check box attribute on the target system for provisioning, then:

   a. Search for and open the Lookup.SAP.UM.ProvCheckBoxMapping lookup definition.

   b. Create the following entry in this lookup definition:

      – Code Key: Enter the name of the process form field that you created for the attribute.

      – Decode: Enter the characters for representing the check box state when it is selected and deselected. For example, suppose you use X to represent the selected state of the check box and Y to represent the deselected state, then enter `XY` in the Decode column.

   c. Save and close the lookup definition.

4. Create a task to enable setting of and updates to the custom attribute during provisioning operations.

   To enable the update of the attribute during provisioning operations, add a process task for updating the attribute:

   > **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

   a. Expand **Process Management**, and double-click **Process Definition**.

   b. Search for and open the **SAP UM Process Form** process definition.

   c. Click **Add**.

   d. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

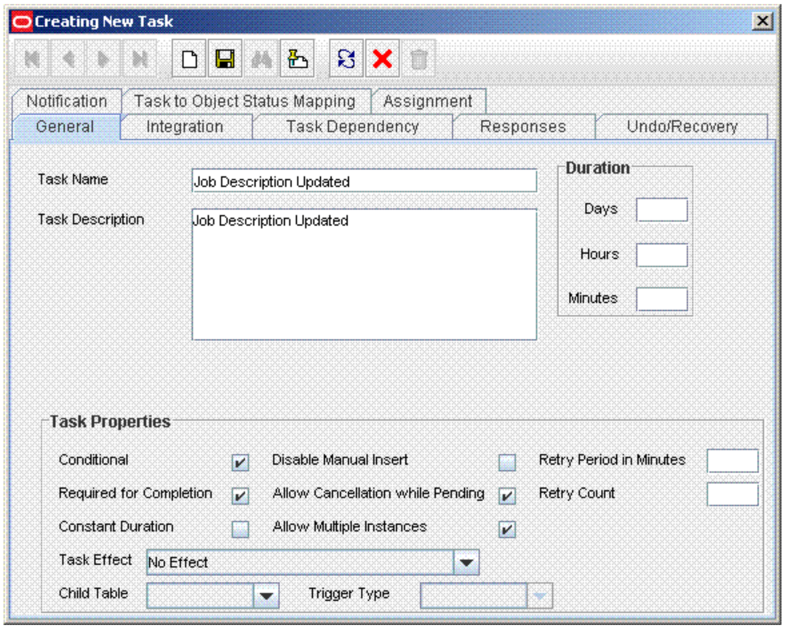
      Conditional

      Required for Completion

      Allow Cancellation while Pending

Allow Multiple Instances

e. Click the Save icon. The following screenshot shows the new task added to the process definition:



Task Name: Job Description Updated

Task Description: Job Description Updated

Days:

Hours:

Minutes:

Conditional ☑

Required for Completion ☑

Constant Duration □

Disable Manual Insert □

Allow Cancellation while Pending ☑

Allow Multiple Instances ☑

Retry Period in Minutes:

Retry Count:

Task Effect: No Effect

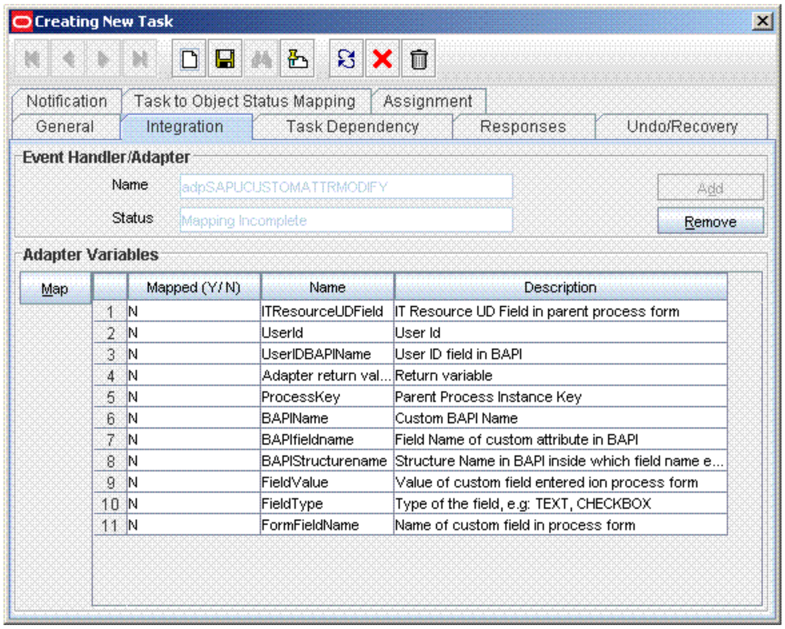
Child Table:

Trigger Type:

f. On the Integration tab of the Creating New Task dialog box, click **Add**.

g. In the Handler Selection dialog box, select **Adapter**, click **adpSAPUCustomAttrModify**, and then click the Save icon.

The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Name: adpSAPUCUSTOMATTRMODIFY

Status: Mapping Incomplete

	Mapped (Y/ N)	Name	Description
1	N	ITResourceUDField	IT Resource UD Field in parent process form
2	N	UserId	User Id
3	N	UserIDBAPIName	User ID field in BAPI
4	N	Adapter return val...	Return variable
5	N	ProcessKey	Parent Process Instance Key
6	N	BAPIName	Custom BAPI Name
7	N	BAPIfieldname	Field Name of custom attribute in BAPI
8	N	BAPIStructurename	Structure Name in BAPI inside which field name e...
9	N	FieldValue	Value of custom field entered ion process form
10	N	FieldType	Type of the field, e.g: TEXT, CHECKBOX
11	N	FormFieldName	Name of custom field in process form

h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the Save icon.

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	UserId	Process Data	User ID
Third	UserIDBAPIName	Literal	String User ID field in the BAPI For example: BNAME
Fourth	BAPIName	Literal	String BAPI Name For example: ZXLCBAPI_ZXLCUSR_CHANG_ATTR
Fifth	BAPIStructureName	Literal	String For example: ADDRESS
Sixth	BAPIFieldName	Literal	String BAPI field name of custom attribute For example: JOB_DESC1
Seventh	FormFieldName	Literal	String For example: Job Description
Eighth	FieldType	Literal	String For example: TEXT
Ninth	ProcessKey	Process Data	Process Instance
Tenth	ITResourceUDField	Literal	String For example: UD_SAP_ITRESOURCE
Eleventh	FieldValue	Process Data	Custom field in process form For example: Job Description

j. Click the Save icon in the Editing Task dialog box, and then close the dialog box.

k. Click the Save icon to save changes to the process definition.

4.8 Adding Custom Multivalued Attributes for Provisioning

By default, the attributes listed in Table 1–8 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

> **Note:** Perform the procedure described in this section only if you want to map for provisioning custom multivalued attributes that you add on the target system.

Summary of the procedure to add a new multivalued attribute for provisioning

1. Create a child form for the new multivalued attribute.
2. Associate the child form with the process form.
3. Create an entry for the attribute in the Lookup.SAP.UM.ProvChildAttrMap lookup definition.
4. Create tasks for adding and deleting values of the new multivalued attribute during provisioning operations.

To add a custom multivalued attribute for provisioning:

> **Note:** See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure.
>
> If you have already added a custom multivalued attribute form for reconciliation, then you need not repeat steps performed as part of that procedure.

1. Log in to the Oracle Identity Manager Design Console.
2. Add the custom attribute on the process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer.**
   c. Click **Create New Form**, enter the form name (for example, `UD_SAP_STRUCT`) and then click the Save icon.
   d. To add a column, click **Add**.
   e. Enter the details of the attribute.

      For example, if you are adding the Structural Role field, enter `UD_SAP_STRUCT_ROLE` in the Name field, and then enter the rest of the details of this field.

      Click the Save icon, and then click **Make Version Active**. The following screenshot shows the new field added to the process form:

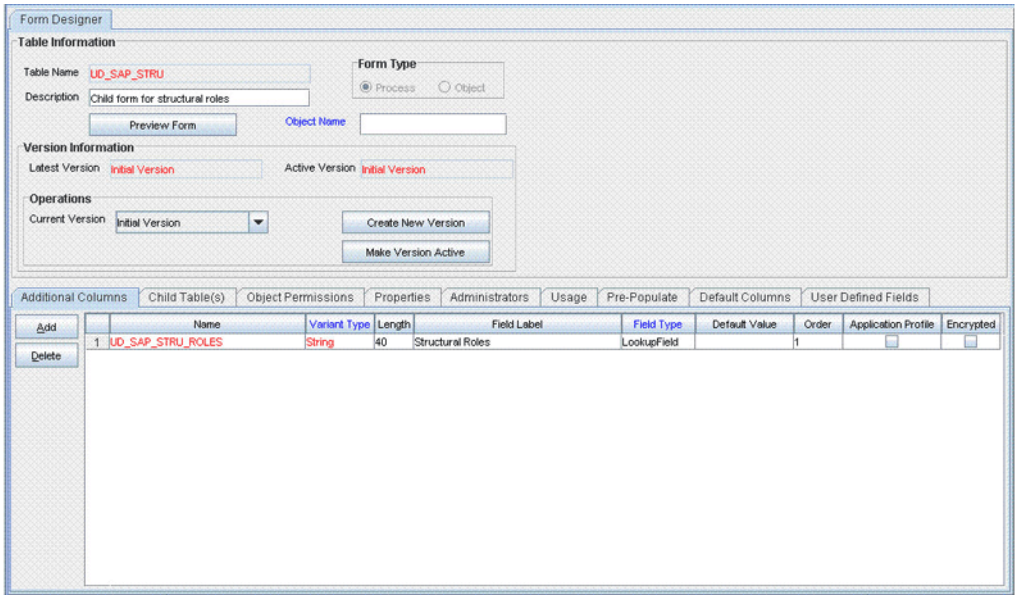


Table Name: UD_SAP_STRU

Description: Child form for structural roles

Form Type: ● Process ○ Object

Latest Version: Initial Version

Active Version: Initial Version

Current Version: Initial Version

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encrypted
1	UD_SAP_STRU_ROLES	String	40	Structural Roles	LookupField		1	□	□

3. Associate the child form with the process form as follows:

   Note: Only basic instructions to create a child form are given in this section. See *Oracle Identity Manager Design Console Guide* for detailed instructions.

   ---

   a. Search for and open the **UD_SAP** form.

   b. Click **Create New Version**.

   c. Enter a version name, and then click the Save icon.

   d. From the **Current Version** list, select the version that you created.

   e. On the Child Tables tab, click **Assign**.

   f. From the list on the left, select the child table and then move it to the list on the right. Then, click **OK**.

   g. Click **Make Version Active**.

4. Create an entry for the attribute in the lookup definition for multivalued attribute provisioning as follows:

   a. Expand **Administration**, and double-click **Lookup Definition**.

   b. Search for and open the **Lookup.SAP.UM.ProvChildAttrMap** lookup definition.

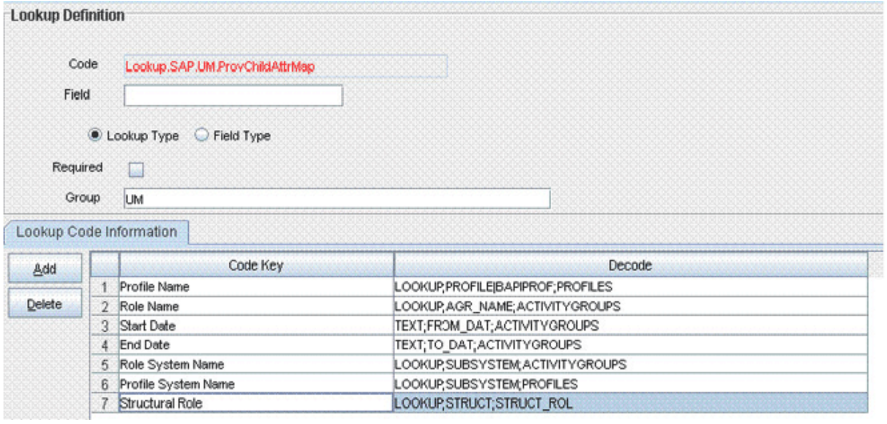
   c. Click **Add**, and then enter the Code Key and Decode values for the attribute.

   The Code Key value must be the name of the field on the process form. The Decode value is what you determine by performing the procedure described in Section 4.1, "Determining the Names of Target System Attributes."

   For example, suppose you want to add the Structural Roles child table, which has one attribute: `Structural Roles`. For this attribute, you create the following Decode entries:

   ```
   LOOKUP;STRUCT;STRUCT_ROL
   ```

The following screenshot shows the entry added to the lookup definition:



Lookup Definition

Code: Lookup.SAP.UM.ProvChildAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: UM

Lookup Code Information

	Code Key	Decode
1	Profile Name	LOOKUP;PROFILE|BAPIPROF;PROFILES
2	Role Name	LOOKUP;AGR_NAME;ACTIVITYGROUPS
3	Start Date	TEXT;FROM_DAT;ACTIVITYGROUPS
4	End Date	TEXT;TO_DAT;ACTIVITYGROUPS
5	Role System Name	LOOKUP;SUBSYSTEM;ACTIVITYGROUPS
6	Profile System Name	LOOKUP;SUBSYSTEM;PROFILES
7	Structural Role	LOOKUP;STRUCT;STRUCT_ROL

5. Expand **Process Management**, and double-click **Process Definition**.

6. Search for and open the **SAP UM Process Form** process definition.

7. In the process definition, create a process task for adding values in the attribute:

   a. Click **Add**.

   b. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

      Conditional

      Required for Completion

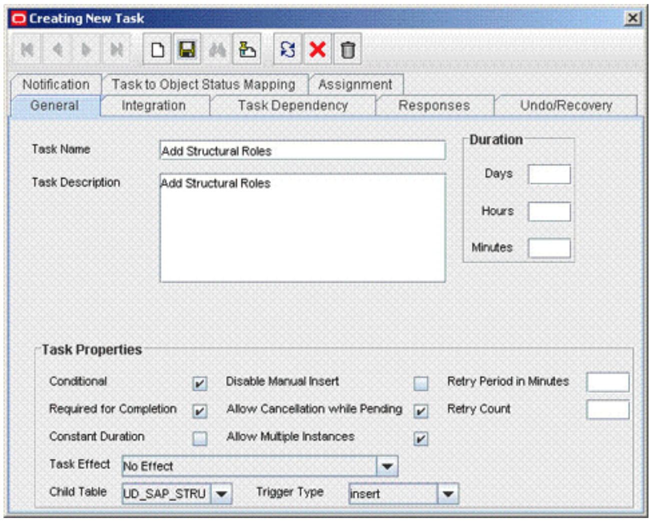
      Allow Cancellation while Pending

      Allow Multiple Instances

   c. From the **Child Table** list, select the child table name.

   d. From the Trigger Type list, select **Insert**.

   e. Click the Save icon. The following screenshot shows the new task added to the process definition:



Task Name: Add Structural Roles

Task Description: Add Structural Roles

Duration

Days:

Hours:

Minutes:

Task Properties

Conditional ☑

Required for Completion ☑

Constant Duration □

Disable Manual Insert □

Allow Cancellation while Pending ☑

Allow Multiple Instances ☑

Retry Period in Minutes:

Retry Count:

Task Effect: No Effect

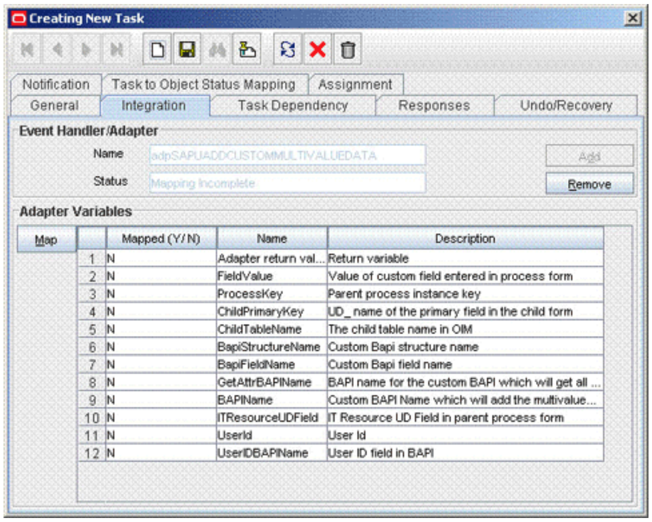
Child Table: UD_SAP_STRU

Trigger Type: Insert

   f. On the Integration tab of the Creating New Task dialog box, click **Add**.

g. In the Handler Selection dialog box, select **Adapter**, click **adpSAPUAddCustomMultiValueData**, and then click the Save icon.

The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Event Handler/Adapter

Name: adpSAPUADDCUSTOMMULTIVALUEDATA

Status: Mapping Incomplete

Adapter Variables

	Mapped (Y/N)	Name	Description
1	N	Adapter return val...	Return variable
2	N	FieldValue	Value of custom field entered in process form
3	N	ProcessKey	Parent process instance key
4	N	ChildPrimaryKey	UD_ name of the primary field in the child form
5	N	ChildTableName	The child table name in OIM
6	N	BapiStructureName	Custom Bapi structure name
7	N	BapiFieldName	Custom Bapi field name
8	N	GetAttrBAPIName	BAPI name for the custom BAPI which will get all ...
9	N	BAPIName	Custom BAPI Name which will add the multivalue...
10	N	ITResourceUDField	IT Resource UD Field in parent process form
11	N	UserId	User Id
12	N	UserIDBAPIName	User ID field in BAPI

h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the Save icon.

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	UserId	Process Data	User ID
Third	Field Value	Process Data / Child Form Name	Key multivalued attribute present on the child form For example: Structural Roles
Fourth	ChildPrimaryKey	Literal	String User-defined field of key multivalued attribute taken from the child form For example: UD_SAP_STRUCT_ROLES
Fifth	ChildTableName	Literal	String User-defined field of the child form For example: UD_SAP_STRUCT
Sixth	BapiStructureName	Literal	String For example: STRUCT_ROLE

Variable Number	Variable Name	Map To	Qualifier
Seventh	BapiFieldName	Literal	String For example: STRUCT
Eighth	ProcessKey	Process Data	Process Instance
Ninth	ITResNameUD	Literal	String For example: UD_SAP_ITRESOURCE
Tenth	GetAttrBAPIName	Literal	BAPI name for the custom BAPI that will fetch the multivalued attribute from the target system Example: ZMPHC_RETURN_STRUCT_ROLES **Note:** This is not a mandatory field. However, if it is not provided, then Oracle Identity Manager cannot check whether the attribute being added has already been added.
Eleventh	BAPIName	Literal	Name of the custom BAPI that will add the multivalued attribute Example: ZMPHC_STRUCT_ROLES
Twelfth	UserIDBAPIName	Literal	User ID field as it appears in the custom BAPI For example: USERNAME

j. Click the Save icon in the Editing Task dialog box, and then close the dialog box.

k. Click the Save icon to save the changes to the process definition.

8. In the process definition, create a process task to delete values in the attribute:

a. Click **Add**.

b. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

Conditional

Required for Completion

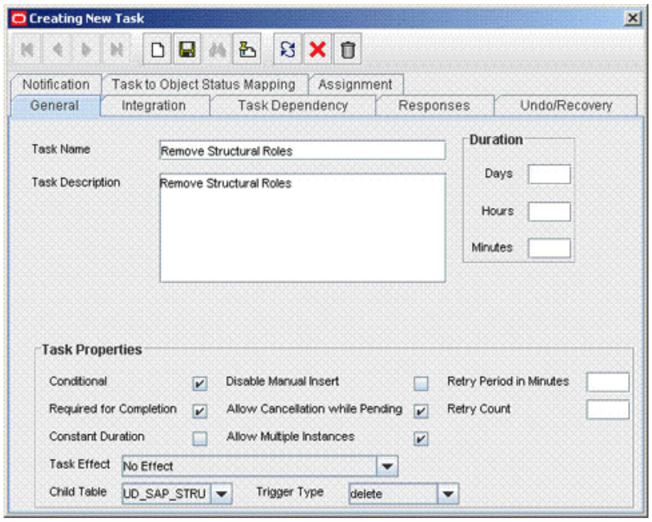
Allow Cancellation while Pending

Allow Multiple Instances

c. From the **Child Table** list, select the child table name.

d. From the Trigger Type list, select **Delete**.

e. Click the Save icon. The following screenshot shows the new task added to the process definition:



Task Name: Remove Structural Roles

Task Description: Remove Structural Roles

Duration

Days:

Hours:

Minutes:

Task Properties

Conditional ☑ Disable Manual Insert ☐ Retry Period in Minutes:

Required for Completion ☑ Allow Cancellation while Pending ☑ Retry Count:

Constant Duration ☐ Allow Multiple Instances ☑

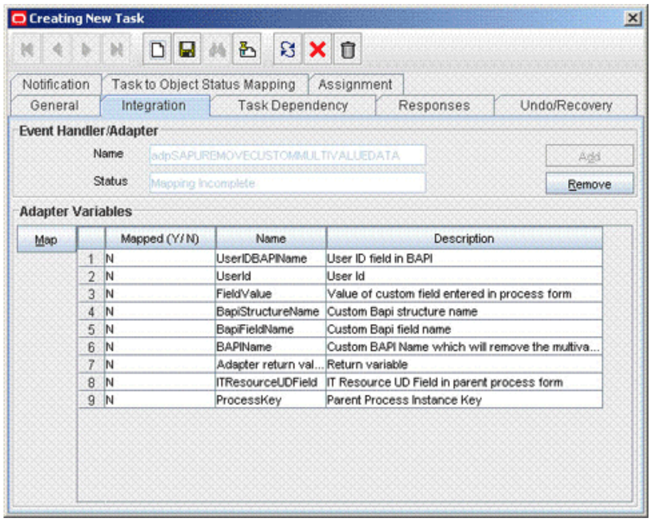
Task Effect: No Effect

Child Table: UD_SAP_STRU Trigger Type: delete

f. On the Integration tab of the Creating New Task dialog box, click **Add**.

g. In the Handler Selection dialog box, select **Adapter**, click **adpSAPURemoveMultiValueData**, and then click the Save icon.

The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Event Handler/Adapter

Name: adpSAPUREMOVECUSTOMMULTIVALUEDATA

Status: Mapping Incomplete

Adapter Variables

	Mapped (Y/ N)	Name	Description
1	N	UserIDBAPIName	User ID field in BAPI
2	N	UserId	User Id
3	N	FieldValue	Value of custom field entered in process form
4	N	BapiStructureName	Custom Bapi structure name
5	N	BapiFieldName	Custom Bapi field name
6	N	BAPIName	Custom BAPI Name which will remove the multiva...
7	N	Adapter return val...	Return variable
8	N	ITResourceUDField	IT Resource UD Field in parent process form
9	N	ProcessKey	Parent Process Instance Key

h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the Save icon.

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	UserId	Process Data	User ID
Third	FieldValue	Process Data / Child Form Name	Key multivalued attribute present on the child form For example: Structural Role **Note:** Select the Old Value check box.
Fourth	BapiFieldName	Literal	String BAPI field name of the key multivalued attribute taken from the child form For example: STRUCT
Fifth	BapiStructureName	Literal	String For example: STRUCT_ROLES
Sixth	ProcessKey	Process Data	Process Instance
Seventh	ITResNameUD	Literal	String For example: UD_SAP_ITRESOURCE
Eight	BAPIName	Literal	String For example: ZSDA_REMOV_STRUCT_ROLES Name of the custom BAPI that will remove the multivalued attribute
Nine	UserIDBAPIName	Literal	User ID field in BAPI For example: USERNAME

j. Click the Save icon in the Editing Task dialog box, and then close the dialog box.

9. Save the changes to the process definition.

4.9 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

For data that fails the validation check, the following message is displayed or recorded in the log file:

```
Value returned for field FIELD_NAME is false.
```

Note: This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

This validation class must implement the oracle.iam.connectors.common.validate.Validator interface and the validate method.

> **See Also:** The Javadocs shipped with the connector for more information about this interface

The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

```
public boolean validate(HashMap hmUserDetails,
              HashMap hmEntitlementDetails, String field) {
            /*
         * You must write code to validate attributes. Parent
         * data values can be fetched by using hmUserDetails.get(field)
         * For child data values, loop through the
         * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
         * Depending on the outcome of the validation operation,
         * the code must return true or false.
         */
         /*
         * In this sample code, the value "false" is returned if the field
         * contains the number sign (#). Otherwise, the value "true" is
         * returned.
         */
            boolean valid=true;
            String sFirstName=(String) hmUserDetails.get(field);
            for(int i=0;i<sFirstName.length();i++){
              if (sFirstName.charAt(i) == '#'){
                    valid=false;
                    break;
              }
            }
            return valid;
      }
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.
4. If you created the Java class for validating a process form field for reconciliation, then:
    a. Log in to the Design Console.
    b. Search for and open the **Lookup.SAP.UM.ReconValidation** lookup definition.
    c. In the Code Key, enter the resource object field name. In the Decode, enter the class name.
    d. Save the changes to the lookup definition.
    e. Search for and open the **Lookup.SAP.UM.Configuration** lookup definition.
    f. Set the value of the **Use Validation For Recon** entry to `yes`.
    g. Save the changes to the lookup definition.
5. If you created the Java class for validating a process form field for provisioning, then:
    a. Log in to the Design Console.
    b. Search for and open the **Lookup.SAP.UM.ProvValidation** lookup definition.

c. In the **Code Key** column, enter the process form field name. In the **Decode** column, enter the class name.

d. Save the changes to the lookup definition.

e. Search for and open the **Lookup.SAP.UM.Configuration** lookup definition.

f. Set the value of the **Use Validation For Prov** entry to `yes`.

g. Save the changes to the lookup definition.

4.10 Configuring Transformation of Data During User Reconciliation

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

> **Note:** This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure transformation of single-valued user data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class.

   This transformation class must implement the oracle.iam.connectors.common.transform.Transformation interface and the transform method.

   > **See Also:** The Javadocs shipped with the connector for more information about this interface

   The following sample transformation class creates a value for the Full Name attribute by using values fetched from the First Name and Last Name attributes of the target system:

```
package oracle.iam.connectors.common.transform;

import java.util.HashMap;

public class TransformAttribute implements Transformation {

      /*
      Description:Abstract method for transforming the attributes

      param hmUserDetails<String,Object>

      HashMap containing parent data details

      param hmEntitlementDetails <String,Object>

      HashMap containing child data details

      */
      public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails,String sField) {
      /*
       * You must write code to transform the attributes.
       Parent data attribute values can be fetched by
       using hmUserDetails.get("Field Name").
       *To fetch child data values, loop through the
       * ArrayList/Vector fetched by hmEntitlementDetails.get("Child
Table")
       * Return the transformed attribute.
       */
      String sFirstName= (String)hmUserDetails.get("First Name");
      String sLastName= (String)hmUserDetails.get("Last Name");
      String sFullName=sFirstName+"."+sLastName;
      return sFullName;
      }
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.
4. If you created the Java class for transforming a process form field for reconciliation, then:
    a. Log in to the Design Console.
    b. Search for and open the **Lookup.SAP.UM.ReconTransformation** lookup definition.
    c. In the **Code Key** column, enter the resource object field name. In the **Decode** column, enter the class name.
    d. Save the changes to the lookup definition.
    e. Search for and open the **Lookup.SAP.UM.Configuration** lookup definition.
    f. Set the value of the **Use Transformation For Recon** entry to `yes`.
    g. Save the changes to the lookup definition.

4.11 Configuring Transformation of Data During Lookup Field Synchronization

You can configure transformation of lookup field data synchronized from the target system.

To configure transformation of lookup field data fetched during lookup field synchronization:

1. Write code that implements the required transformation logic in a Java class.

    This transformation class must implement the oracle.iam.connectors.common.transform.Transformation interface and the transform method.

    > **See Also:** The Javadocs shipped with the connector for more information about this interface

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.
4. Run lookup field synchronization for the lookup definition containing the lookup field that you want to transform. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for more information.
5. Open the lookup definition in the Design Console, and copy the Code Key value for the entry whose Decode value you want to transform.

6. Search for and open the **Lookup.SAP.UM.LookupReconTransformation** lookup definition.
7. In the **Code Key** column, enter the Code Key string that you copy by performing Step 5. In the **Decode** column, enter the class name.
8. Save the changes to the lookup definition.
9. Search for and open the **Lookup.SAP.UM.Configuration** lookup definition.
10. Set the value of the **Use Transformation For Lookup Recon** entry to `yes`.
11. Save the changes to the lookup definition.

4.12 Configuring Synchronization of New Lookup Definitions with the Target System

Table 1–2 lists the lookup definitions that are synchronized with the target system. If you want to add to this list of lookup definitions, then:

> **Note:** See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure.

To configure synchronization of a new lookup definition with the target system:

1. Create the lookup definition in Oracle Identity Manager
2. Add the lookup definition to the process form.
3. Create an entry for the new lookup definition in the Lookup.SAP.UM.LookupMappings or Lookup.SAP.CUA.LookupMappings lookup definition.

   In the Code Key column of this lookup definition, enter a name for the new lookup definition.

   In the Decode column, create an entry in the following format:

   ```
   BAPI_HELPVALUES_GET;METHOD_NAME;PARAMETER_NAME;FIELD_NAME;FIELDNAME_VALUE_FOR_C
   ODEKEY;FIELDNAME_VALUE_FOR_DECODE
   ```

   In this format:

   – *`METHOD_NAME`* is the name of the method.

   – *`PARAMETER_NAME`* is the name of the parameter.

   – *`FIELD_NAME`* is the name of the field.

   – *`FIELDNAME_VALUE_FOR_CODEKEY`* is the name of the field from which the Code Key column on Oracle Identity Manager is to be populated.

   – *`FIELDNAME_VALUE_FOR_DECODE`* is the name of the field from which the Decode column on Oracle Identity Manager is to be populated.

   To determine the Decode value:

   > **Note:** The sample values given in this procedure are from existing values mapped for lookup field synchronization. When you perform this procedure, replace these sample values with values for the lookup definition that you want to synchronize.

a. Log in to the target system.

b. Run transaction SE37.

c. In the Function Module field, enter `BAPI_HELPVALUES_GET` and then click the Test/Execute icon.

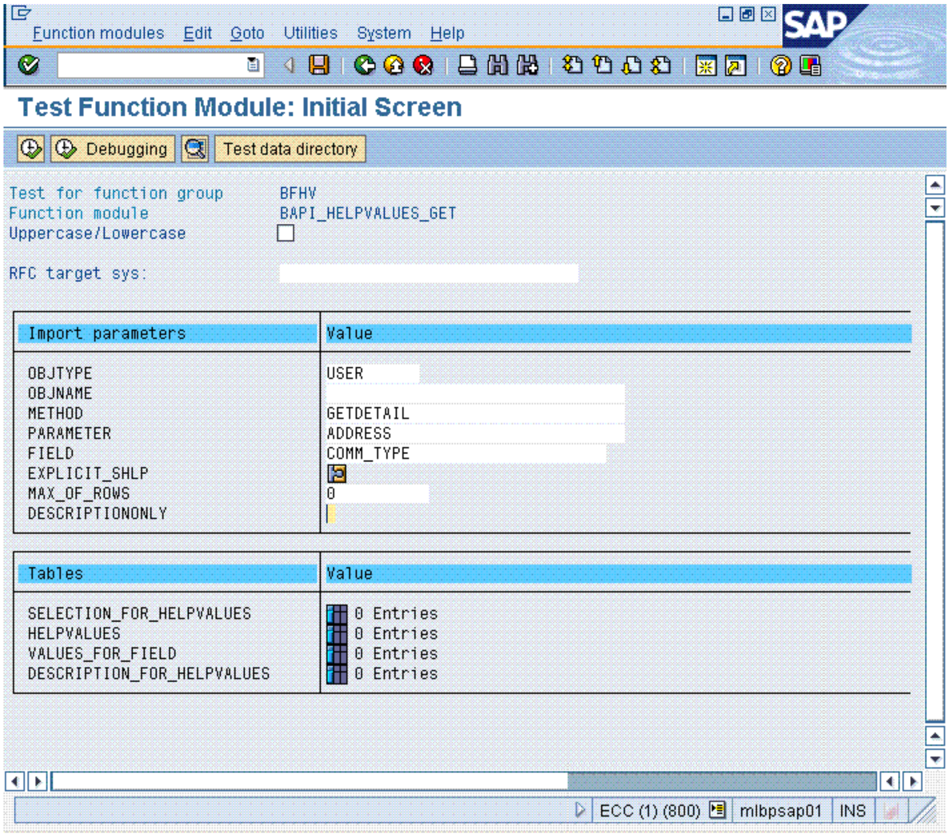
d. In the **OBJTYPE** field, enter `USER`.

e. In the **METHOD** field, enter the name of the BAPI method. For example, enter `GETDETAIL`. This is the replacement for *`METHOD_NAME`*.

f. In the **PARAMETER** field, enter the name of the parameter. For example, enter `ADDRESS`. This is the replacement for *`PARAMETER_NAME`*.

g. In the **FIELD** field, enter the name of the field. For example, enter `COMM_TYPE`. This is the replacement for *`FIELD_NAME`*.

The following screenshot shows this page:



Test Function Module: Initial Screen

Test for function group BFHV
Function module BAPI_HELPVALUES_GET
Uppercase/Lowercase □

RFC target sys:

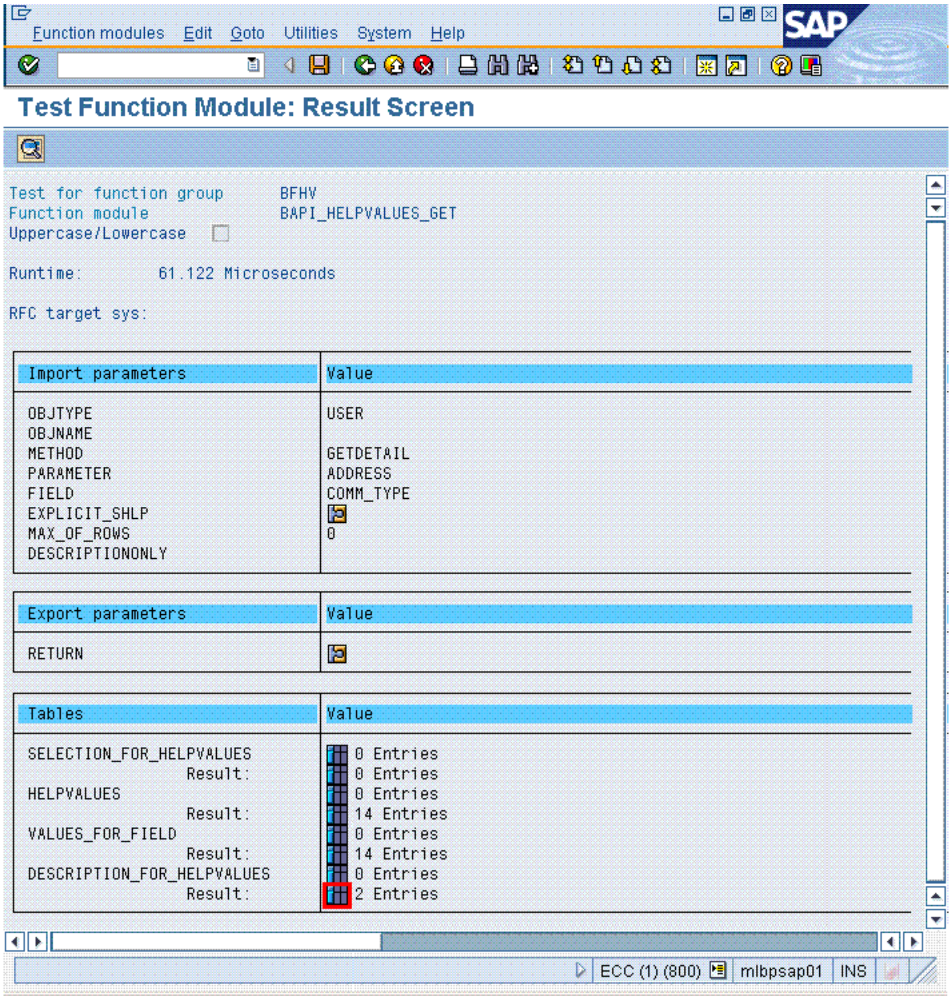
Import parameters	Value
OBJTYPE	USER
OBJNAME	
METHOD	GETDETAIL
PARAMETER	ADDRESS
FIELD	COMM_TYPE
EXPLICIT_SHLP	
MAX_OF_ROWS	0
DESCRIPTIONONLY	

Tables	Value
SELECTION_FOR_HELPVALUES	0 Entries
HELPVALUES	0 Entries
VALUES_FOR_FIELD	0 Entries
DESCRIPTION_FOR_HELPVALUES	0 Entries

h. Click the Execute icon.

i. In the table that is displayed, click the icon to display the entries in the DESCRIPTION_FOR_HELPVALUES column.

The following screenshot shows this page:



Test Function Module: Result Screen

```
Test for function group      BFHV
Function module              BAPI_HELPVALUES_GET
Uppercase/Lowercase       □

Runtime:          61.122 Microseconds

RFC target sys:
```

Import parameters	Value
OBJTYPE	USER
OBJNAME	
METHOD	GETDETAIL
PARAMETER	ADDRESS
FIELD	COMM_TYPE
EXPLICIT_SHLP	
MAX_OF_ROWS	0
DESCRIPTIONONLY	

Export parameters	Value
RETURN	

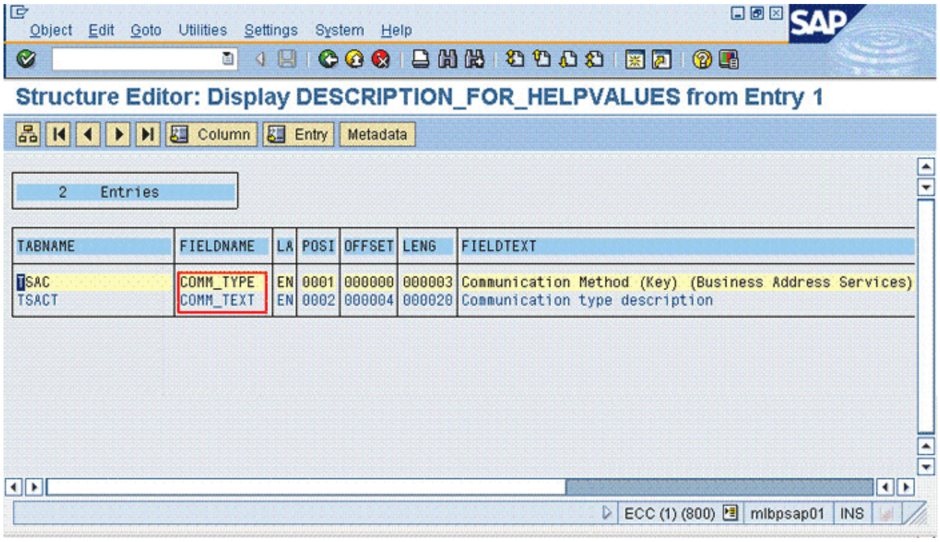
Tables	Value
SELECTION_FOR_HELPVALUES	0 Entries
Result:	0 Entries
HELPVALUES	0 Entries
Result:	14 Entries
VALUES_FOR_FIELD	0 Entries
Result:	14 Entries
DESCRIPTION_FOR_HELPVALUES	0 Entries
Result:	2 Entries

ECC (1) (800) | mlbpsap01 | INS

j. In the FIELDNAME column of the table that is displayed, copy the contents of the first row. For the COMM_TYPE example, this value is COMM_TYPE. This is the replacement for *FIELDNAME_VALUE_FOR_CODEKEY*.

In the FIELDNAME column of the table that is displayed, copy the contents of the second row. For the COMM_TYPE example, the second value is COMM_TEXT. This is the replacement for *FIELDNAME_VALUE_FOR_DECODE*.

The following screenshot shows this page:



Structure Editor: Display DESCRIPTION_FOR_HELPVALUES from Entry 1

2 Entries

TABNAME	FIELDNAME	LA	POSI	OFFSET	LENG	FIELDTEXT
TSAC	COMM_TYPE	EN	0001	000000	000003	Communication Method (Key) (Business Address Services)
TSACT	COMM_TEXT	EN	0002	000004	000020	Communication type description

For the sample values given in this procedure, the Decode entry that you would create is as follows:

```
BAPI_HELPVALUES_GET;GETDETAIL;ADDRESS;COMM_TYPE;COMM_TYPE;COMM_TEXT
```

4.13 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_SAP** 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**.

4.14 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

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

To meet the requirement posed by such a scenario, you can create copies of connector objects, such as the IT resource and resource object.

The decision to create a copy of a connector object might be based on a requirement. For example, an IT resource can hold connection information for one target system installation. Therefore, it is mandatory to create a copy of the IT resource for each target system installation.

With some other connector objects, you do not need to create copies at all. For example, a single attribute-mapping lookup definition can be used for all installations of the target system.

All connector objects are linked. For example, a scheduled task holds the name of the IT resource. Similarly, the IT resource holds the name of the configuration lookup definition, Lookup.SAP.UM.Configuration. If you create a copy of an object, then you must specify the name of the copy in associated connector objects. Table 4–1 lists associations between connector objects whose copies can be created and the other objects that reference these objects. When you create a copy of a connector object, use this information to change the associations of that object with other objects.

Note: On a particular Oracle Identity Manager installation, if you create a copy of a connector object, then you must set a unique name for it.

Table 4–1 Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
IT resource	SAP UM IT Resource	SAP User Management User Recon (scheduled task) SAP User Management Delete Recon (scheduled task) SAP User Management Lookup Recon (scheduled task)	Create a copy of the IT resource. See Section 2.3.12, "Configuring the IT Resource" for more information.
Resource object	SAP UM Resource Object	SAP User Management User Recon (scheduled task) SAP User Management Delete Recon (scheduled task) SAP User Management Lookup Recon (scheduled task)	It is optional to create a copy of the resource object. If you are reconciling the same set of attributes from all installations of the target system, then you need not create a copy of the resource object. In other words, create copies of the resource object only if there are differences in attributes between the various installations of the target system. See Section 3.4.3, "Reconciliation Scheduled Tasks" for more information.
Process definition	SAP UM Process Form	NA	Create copies of this process definition only if there are difference in attributes between the installations of the target system.
Attribute Mapping Lookup Definition	Lookup.SAP.UM. ProvAttrMap Lookup.SAP.UM. ProvChildAttrMap Lookup.SAP.UM. ReconAttrMap Lookup.SAP.UM. ReconChildAttrMap	NA	Create copies of this lookup definition only if you want to use a different set of configuration values for the various installations of the target system. See the following sections for more information: Section 1.6, "Connector Objects Used During Reconciliation" Section 1.7, "Connector Objects Used During Provisioning"
Process form	UD_SAP	NA	It is optional to create a copy of a process form. If you are provisioning different sets of attributes, then you need to create a copy of this connector object.
Configuration lookup definition	Lookup.SAP.UM. Configuration	SAP UM IT Resource (IT resource)	Create copies of this lookup definition only if you want to use a different set of configuration values for the various installations of the target system. See Section 2.3.2, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager" for more information.
Lookup mappings lookup definitions	Lookup.SAP.UM. LookupMappings Lookup.SAP.CUA.LookupMappings	SAP User Management Lookup Recon (scheduled task)	Create copies of these lookup definition only if you want to use a different set of lookup mappings for the various installations of the target system.

When you configure reconciliation:

To reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the scheduled task attribute that holds the IT resource name. For example, you enter the name of the IT resource as the value of the IT resource attribute of the SAP HRMS User Recon scheduled task.

When you perform provisioning operations:

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the target system installation to which you want to provision the user.

4.14.1 Enabling the Dependent Lookup Fields Feature

When you perform a provisioning operation, lookup fields on the Administrative and User Console allow you to select values from lists. Some of these lookup fields are populated with values copied from the target system.

In earlier releases of the connector, if you had multiple installations of the target system, then entries in the lookup field were linked with the target system installation from which the entries were copied. This allowed you to select lookup field values that were specific to the target system installation on which the provisioning operation was to be performed.

For release 9.1.2 of the connector, the Dependent Lookup Fields feature is disabled by default. You can enable this feature after you deploy the Oracle Identity Manager release 9.1.0.2 bundle patch that addresses Bug 9181280.

> **Note:** The bundle patch that addressed Bug 9181280 had not been released at the time of release of this connector.

To enable the Dependent Lookup Fields feature after you deploy the bundle patch that addresses Bug 9181280, you must make changes in the forms listed in Table 4–2. This table lists the forms, the lookup fields on the forms, and the lookup query that you must use for each lookup field. The procedure is described after the table.

Table 4–2 SQL Queries for Lookup Fields

Form	Lookup Field	Oracle Database Query for the Lookup Field	Microsoft SQL Server Query for the Lookup Field
UD_SPUM_PRO	Profile System Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))= concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' , lkv_encoded)>0
UD_SPUM_PRO	Profile Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Profile' and instr(lkv_encoded,concat('$Form data.UD_SPUM_PRO_SYSTEMNAME$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Profile' and CHARINDEX('$Form data.UD_SPUM_PRO_SYSTEMNAME$' + '~' , lkv_encoded)>0
UD_SAPRL	Role System Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))= concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' , lkv_encoded)>0
UD_SAPRL	Role Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Roles' and instr(lkv_encoded,concat('$Form data.UD_SAPRL_SYSTEMNAME$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Roles' and CHARINDEX('$Form data.UD_SAPRL_SYSTEMNAME$' + '~' , lkv_encoded)>0
UD_SAP	Title	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.UserTitle' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.UserTitle' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP	User Group	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.UserGroups' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.UserGroups' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0

Table 4–2 (Cont.) SQL Queries for Lookup Fields

Form	Lookup Field	Oracle Database Query for the Lookup Field	Microsoft SQL Server Query for the Lookup Field
UD_SAP	Logon Language	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.LangComm' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.LangComm' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP	Date Format	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.DateFormat' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.DateFormat' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP	Decimal Notation	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.DecimalNotation' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.DecimalNotation' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP	Time Zone	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.TimeZone' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.TimeZone' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP	Company	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Company' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Company' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0

Table 4–2 (Cont.) SQL Queries for Lookup Fields

Form	Lookup Field	Oracle Database Query for the Lookup Field	Microsoft SQL Server Query for the Lookup Field
UD_SAP	Contractual User Type	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.ContractualUserType' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.ContractualUserType' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP	Communication Type	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.CommType' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.CommType' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP	Language Communication	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.LangComm' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.LangComm' and CHARINDEX('$Form data.UD_SAP_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAPPRO_O	Profile System Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))= concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and CHARINDEX('$Form data. UD_SAP_O_ITRESOURCE$' + '~' , lkv_encoded)>0
UD_SAPPRO_O	Profile Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Profile' and instr(lkv_encoded,concat('$Form data.UD_SPUM_PRO_O_SYSTEMNAME$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Profile' and CHARINDEX('$Form data. UD_SPUM_PRO_O_SYSTEMNAME$' + '~' , lkv_encoded)>0
UD_SAPRL_O	Role System Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))= concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' , lkv_encoded)>0

Table 4–2 (Cont.) SQL Queries for Lookup Fields

Form	Lookup Field	Oracle Database Query for the Lookup Field	Microsoft SQL Server Query for the Lookup Field
UD_SAPRL_O	Role Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Roles' and instr(lkv_encoded,concat('$Form data.UD_SAPRL_O_SYSTEMNAME$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Roles' and CHARINDEX('$Form data.UD_SAPRL_O_SYSTEMNAME$' + '~' , lkv_encoded)>0
UD_SAP_O	Title	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.UserTitle' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.UserTitle' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP_O	User Group	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.UserGroups' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.UserGroups' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP_O	Logon Language	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.LangComm' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.LangComm' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP_O	Date Format	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.DateFormat' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.DateFormat' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP_O	Decimal Notation	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.DecimalNotation' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.DecimalNotation' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0

Table 4–2 (Cont.) SQL Queries for Lookup Fields

Form	Lookup Field	Oracle Database Query for the Lookup Field	Microsoft SQL Server Query for the Lookup Field
UD_SAP_O	Time Zone	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.TimeZone' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.TimeZone' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP_O	Company	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Company' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Company' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP_O	Contractual User Type	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.ContractualUserType' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.ContractualUserType' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP_O	Communication Type	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.CommType' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.CommType' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0
UD_SAP_O	Language Communication	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.LangComm' and substr(lkv_encoded,1,length(concat('$Form data.UD_SAP_O_ITRESOURCE$','~')))=concat('$Form data.UD_SAP_O_ITRESOURCE$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.LangComm' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCE$' + '~' ,lkv_encoded)>0

Table 4–2 (Cont.) SQL Queries for Lookup Fields

Form	Lookup Field	Oracle Database Query for the Lookup Field	Microsoft SQL Server Query for the Lookup Field
UD_SPUMRC_O	Role System Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SPUMRP_O_SERVER$','~')))=concat('$Form data.UD_SPUMRP_O_SERVER$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and CHARINDEX('$Form data.UD_SPUMRP_O_SERVER$' + '~' , lkv_encoded)>0
UD_SPUMRC_O	User 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.UM.Roles' and instr(lkv_encoded,concat('$Form data.UD_SPUMRC_O_SYSTEMNAME$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Roles' and CHARINDEX('$Form data.UD_SPUMRC_O_SYSTEMNAME$' + '~' , lkv_encoded)>0
UD_SPUMPC_O	Profile System Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SPUMPP_O_SERVER$','~')))=concat('$Form data.UD_SPUMPP_O_SERVER$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and CHARINDEX('$Form data.UD_SPUMPP_O_SERVER$' + '~' , lkv_encoded)>0
UD_SPUMPC_O	Profile Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Profile' and instr(lkv_encoded,concat('$Form data.UD_SPUMPC_O_SYSTEMNAME$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Profile' and CHARINDEX('$Form data.UD_SPUMPC_O_SYSTEMNAME$' + '~' , lkv_encoded)>0
UD_SPUMRC_P	User 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.UM.System' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SPUMRP_P_SERVER$','~')))=concat('$Form data.UD_SPUMRP_P_SERVER$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and CHARINDEX((select CONVERT(varchar,svr_key) from svr where svr_name='$Form data.UD_SPUMRP_P_SERVER$') + '~' ,lkv_encoded)>0

Table 4–2 (Cont.) SQL Queries for Lookup Fields

Form	Lookup Field	Oracle Database Query for the Lookup Field	Microsoft SQL Server Query for the Lookup Field
UD_SPUMRC_P	Role System Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Roles' and instr(lkv_encoded,concat('$Form data.UD_SPUMRC_P_SYSTEMNAME$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Roles' and CHARINDEX((select CONVERT(varchar,svr_key) from svr where svr_name='$Form data.UD_SPUMRC_P_SYSTEMNAME$') + '~' ,lkv_encoded)>0
UD_SPUMPC_P	Profile System Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SPUMPP_P_SERVER$','~')))=concat('$Form data.UD_SPUMPP_P_SERVER$','~')	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.System' and CHARINDEX((select CONVERT(varchar,svr_key) from svr where svr_name='$Form data.UD_SPUMPP_P_SERVER$') + '~' ,lkv_encoded)>0
UD_SPUMPC_P	Profile Name	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Profile' and instr(lkv_encoded,concat('$Form data.UD_SPUMPC_P_SYSTEMNAME$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Profile' and CHARINDEX((select CONVERT(varchar,svr_key) from svr where svr_name='$Form data.UD_SPUMPC_P_SYSTEMNAME$') + '~' ,lkv_encoded)>0

To enable lookup fields on each form:

> **Note:** You must enable lookup fields in the order given in Table 4–2.

1. On the Design Console, expand **Development Tools** and double-click **Form Designer**.
2. Search for and open the form. For example, open the UD_SAP form.
3. Click **Create New Version**, enter a new version number, and then save the version.
4. From the **Current Version** list, select the version that you created.
5. Open the **Properties** tab, and expand **Components**.
6. Add properties for each lookup field on the form as follows:
   a. Select the **Lookup Code** property, and then click **Delete Property**.
   b. Select the first lookup field on the form, and then click **Add Property**. For example, select Profile System Name on the UD_SAP form.
   c. In the Add Property dialog box:

      From the Property Name list, select **Lookup Column Name**.

      In the **Property Value** field, enter `lkv_encoded`.

      Click the Save icon, and then close the dialog box.
   d. Select the lookup field, and then click **Add Property**.

e. In the Add Property dialog box:

   From the Property Name list, select **Column Names**.

   In the **Property Value** field, enter `lkv_encoded`.

   Click the Save icon, and then close the dialog box.

f. Select the lookup field, and then click **Add Property**.

g. In the Add Property dialog box:

   From the Property Name list, select **Column Widths**.

   In the **Property Value** field, enter `234`.

h. Select the lookup field, and then click **Add Property**.

i. In the Add Property dialog box:

   From the Property Name list, select **Column Captions**.

   In the **Property Value** field, enter `lkv_decoded`.

   Click the Save icon, and then close the dialog box.

j. Select the lookup field, and then click **Add Property**.

k. In the Add Property dialog box:

   From the Property Name list, select **Lookup Query**.

   In the Property Value field, enter the query given in Table 4–2.

   Click the Save icon, and then close the dialog box.

7. Repeat Step 6 for each lookup field on the form.
8. Click the Save icon to save the changes to the form.
9. Click **Make Version Active**.

5 Known Issues

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

- **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 4.13, "Modifying Field Lengths on the Process Form" for information about working around this issue.

- **Bug 8670307**

  If you enable connection pooling, then custom entries created in the Lookup.SAP.UM.ITResourceMapping lookup definition do not take effect.

A Standard BAPIs Used During Connector Operations

Standard BAPIs used during connector operations can be categorized as follows:

- Section A.1, "Standard BAPIs Used on Both SAP R/3 and SAP CUA"
- Section A.2, "Standard BAPIs Used on SAP R/3"
- Section A.3, "Standard BAPIs Used on SAP CUA"

A.1 Standard BAPIs Used on Both SAP R/3 and SAP CUA

The following standard BAPIs are used during connector operations on both SAP R/3 and SAP CUA:

- BAPI_HELPVALUES_GET: Fetches lookup definition values
- BAPI_USER_GET_DETAIL: Fetches account details
- RFC_READ_TABLE: Queries the USR02 table for first-time reconciliation
- BAPI_USER_CREATE1: Creates accounts on the target system
- BAPI_USER_DELETE: Deletes accounts on the target system
- BAPI_USER_LOCK: Locks accounts
- BAPI_USER_UNLOCK: Unlocks accounts
- BAPI_USER_CHANGE: Modifies account details, also resets the password
- SUSR_USER_CHANGE_PASSWORD_RFC: Changes the password, so that user does not have change the password on first logon
- BAPI_USER_EXISTENCE_CHECK: Checks whether a user exists
- RFC_READ_TABLE: Queries the USH04 table to fetch deleted accounts during reconciliation

A.2 Standard BAPIs Used on SAP R/3

The following standard BAPI is used during connector operations on SAP R/3:

- RFC_READ_TABLE: Queries the USR04 table for incremental reconciliation, and queries the USH02 table for fetching the account lock status

A.3 Standard BAPIs Used on SAP CUA

The following standard BAPI is used during connector operations on SAP CUA:

- RFC_READ_TABLE: Fetches lookup definition values for roles, profiles, and child systems
- BAPI_USER_LOCACTGROUPS_READ: Fetches details of roles assigned to the user
- BAPI_USER_LOCPROFILES_READ: Fetches details of profiles assigned to the user
- RFC_READ_TABLE: Queries the USZBVSYS table during incremental reconciliation and queries the USH02 table for fetching the account lock status

Index