Contents

Preface........................................................................................................................................................................ xi

Audience........................................................................................................................................................................ xi
Documentation Accessibility........................................................................................................................................ xi
Related Documents.................................................................................................................................................... xi
Documentation Updates................................................................................................................................................ xi
Conventions.................................................................................................................................................................. xii

What’s New in Oracle Identity Manager Connector for SAP User Management?............................................................... xiii

Software Updates............................................................................................................................................................ xiii
Documentation-Specific Updates................................................................................................................................... xx

1 About the Connector

1.1 Certified Components............................................................................................................................................. 1-1
1.2 Usage Recommendation.......................................................................................................................................... 1-3
1.3 Certified Languages.................................................................................................................................................. 1-3
1.4 Connector Architecture and Supported Deployment Configurations................................................................. 1-4
1.4.1 Basic User Management...................................................................................................................................... 1-6
1.4.2 User Management with SoD............................................................................................................................... 1-6
1.4.3 User Management with Compliant User Provisioning....................................................................................... 1-8
1.4.4 User Management with Both SoD and Compliant User Provisioning............................................................ 1-10
1.4.5 Guidelines on Using a Deployment Configuration......................................................................................... 1-10
1.4.6 Considerations to Be Addressed When You Enable Compliant User Provisioning........................................ 1-12
1.5 Features of the Connector....................................................................................................................................... 1-12
1.5.1 Support for Both SAP R/3 and SAP CUA........................................................................................................ 1-13
1.5.2 Mapping Standard and Custom Attributes for Reconciliation and Provisioning........................................ 1-13
1.5.3 SoD Validation of Entitlement Requests........................................................................................................... 1-13
1.5.4 Routing of Provisioning Requests Through SAP GRC Compliant User Provisioning............................. 1-14
1.5.5 Full and Incremental Reconciliation.................................................................................................................. 1-14
1.5.6 Limited (Filtered) Reconciliation....................................................................................................................... 1-15
1.5.7 Batched Reconciliation........................................................................................................................................ 1-15
1.5.8 Enabling and Disabling Accounts..................................................................................................................... 1-15
1.5.9 Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts........................................................................ 1-15
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5.10 SNC Communication Between the Target System and Oracle Identity Manager</td>
<td>1-15</td>
</tr>
<tr>
<td>1.5.11 Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations</td>
<td>1-16</td>
</tr>
<tr>
<td>1.5.12 Configuring Password Changes for Newly Created Accounts</td>
<td>1-16</td>
</tr>
<tr>
<td>1.5.13 Specifying a SAP JCo Trace Level</td>
<td>1-16</td>
</tr>
<tr>
<td>1.5.14 Connection Pooling</td>
<td>1-16</td>
</tr>
<tr>
<td>1.5.15 Specifying the Use of a Logon Group on the Target System for Connector Operations</td>
<td>1-17</td>
</tr>
<tr>
<td>1.5.16 Transformation and Validation of Account Data</td>
<td>1-17</td>
</tr>
<tr>
<td>1.5.17 Transformation of Lookup Field Data</td>
<td>1-17</td>
</tr>
<tr>
<td>1.5.18 Support for Both Unicode and Non-Unicode Modes</td>
<td>1-17</td>
</tr>
<tr>
<td>1.6 Lookup Definitions Used During Connector Operations</td>
<td>1-17</td>
</tr>
<tr>
<td>1.6.1 Lookup Definitions Synchronized with the Target System</td>
<td>1-17</td>
</tr>
<tr>
<td>1.6.2 Preconfigured Lookup Definitions</td>
<td>1-20</td>
</tr>
<tr>
<td>1.7 Connector Objects Used During Reconciliation</td>
<td>1-23</td>
</tr>
<tr>
<td>1.7.1 User Attributes for Reconciliation</td>
<td>1-23</td>
</tr>
<tr>
<td>1.7.2 Reconciliation Rules</td>
<td>1-25</td>
</tr>
<tr>
<td>1.7.2.1 Reconciliation Rule</td>
<td>1-25</td>
</tr>
<tr>
<td>1.7.2.2 Viewing Reconciliation Rules in the Design Console</td>
<td>1-25</td>
</tr>
<tr>
<td>1.7.3 Reconciliation Action Rules</td>
<td>1-26</td>
</tr>
<tr>
<td>1.7.3.1 Reconciliation Action Rules for Reconciliation</td>
<td>1-26</td>
</tr>
<tr>
<td>1.7.3.2 Viewing Reconciliation Action Rules in the Design Console</td>
<td>1-26</td>
</tr>
<tr>
<td>1.8 Connector Objects Used During Provisioning</td>
<td>1-27</td>
</tr>
<tr>
<td>1.8.1 User Provisioning Functions</td>
<td>1-27</td>
</tr>
<tr>
<td>1.8.2 User Attributes for Provisioning</td>
<td>1-28</td>
</tr>
<tr>
<td>1.9 Roadmap for Deploying and Using the Connector</td>
<td>1-30</td>
</tr>
</tbody>
</table>

## 2 Deploying the Connector

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Preinstallation</td>
<td>2-1</td>
</tr>
<tr>
<td>2.1.1 Preinstallation on Oracle Identity Manager</td>
<td>2-1</td>
</tr>
<tr>
<td>2.1.1.1 Files and Directories on the Installation Media</td>
<td>2-1</td>
</tr>
<tr>
<td>2.1.1.2 Determining the Release Number of the Connector</td>
<td>2-3</td>
</tr>
<tr>
<td>2.1.1.3 Creating a Backup of the Existing Common.jar File</td>
<td>2-3</td>
</tr>
<tr>
<td>2.1.2 Preinstallation on the Target System</td>
<td>2-5</td>
</tr>
<tr>
<td>2.1.2.1 Creating a Target System User Account for Connector Operations</td>
<td>2-5</td>
</tr>
<tr>
<td>2.1.2.2 Downloading and Installing the SAP JCo</td>
<td>2-12</td>
</tr>
<tr>
<td>2.2 Installation</td>
<td>2-14</td>
</tr>
<tr>
<td>2.3 Postinstallation</td>
<td>2-17</td>
</tr>
<tr>
<td>2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later</td>
<td>2-18</td>
</tr>
<tr>
<td>2.3.1.1 Tagging Form Fields</td>
<td>2-18</td>
</tr>
<tr>
<td>2.3.1.2 Creating and Activating a Sandbox</td>
<td>2-19</td>
</tr>
<tr>
<td>2.3.1.3 Creating a New UI Form</td>
<td>2-19</td>
</tr>
<tr>
<td>2.3.1.4 Creating an Application Instance</td>
<td>2-20</td>
</tr>
<tr>
<td>2.3.1.5 Publishing a Sandbox</td>
<td>2-20</td>
</tr>
<tr>
<td>2.3.1.6 Harvesting Entitlements and Sync Catalog</td>
<td>2-20</td>
</tr>
<tr>
<td>2.3.1.7 Updating an Existing Application Instance with a New Form</td>
<td>2-20</td>
</tr>
</tbody>
</table>
2.3.2 Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later....... 2-21
2.3.3 Configuring Ports on the Target System................................................................. 2-22
2.3.4 Configuring the Target System................................................................................... 2-22
2.3.4.1 Gathering Required Information......................................................................... 2-23
2.3.4.2 Creating an Entry in the BAPIF4T Table................................................................. 2-23
2.3.4.3 Importing the Request .......................................................................................... 2-23
2.3.4.3.1 Extracting the Request Files ........................................................................... 2-24
2.3.4.3.2 Performing the Request Import Operation......................................................... 2-25
2.3.5 Setting Up the Configuration Lookup Definition in Oracle Identity Manager....... 2-25
2.3.5.1 Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts.............................. 2-26
2.3.5.2 Configuring Password Changes for Newly Created Accounts............................ 2-28
2.3.5.3 Setting Values in the Lookup.SAP.UM.Configuration Lookup Definition ...... 2-28
2.3.6 Enabling Request-Based Provisioning................................................................. 2-31
2.3.6.1 Enabling Request-Based Provisioning in Oracle Identity Manager Release 9.1.0.x ... 2-32
2.3.6.2 Enabling Request-Based Provisioning in Oracle Identity Manager Release 11.1.1 .... 2-37
2.3.6.2.1 Copying Predefined Request Datasets............................................................. 2-37
2.3.6.2.2 Importing Request Datasets into MDS............................................................. 2-38
2.3.6.2.3 Enabling the Auto Save Form Feature ............................................................ 2-39
2.3.6.2.4 Running the PurgeCache Utility .................................................................... 2-39
2.3.7 Changing to the Required Input Locale ................................................................. 2-39
2.3.8 Clearing Content Related to Connector Resource Bundles from the Server Cache 2-40
2.3.9 Enabling Logging...................................................................................................... 2-41
2.3.9.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.x ....................... 2-41
2.3.9.2 Enabling Logging on Oracle Identity Manager Release 11.1.x ......................... 2-43
2.3.10 Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition....................... 2-46
2.3.11 Setting Up the Lookup.SAP.UM.LookupMappings and Lookup.SAP.CUA.LookupMappings Lookup Definitions 2-46
2.3.12 Copying the SAPCUP.jar File for User Provisioning ............................................. 2-47
2.3.13 Configuring the Compliant User Provisioning Feature of the Connector .......... 2-47
2.3.13.1 Importing the XML File for the Compliant User Provisioning Feature .......... 2-48
2.3.13.2 Enabling Request-Based Provisioning for the Compliant User Provisioning Feature 2-51
2.3.13.3 Specifying Values for the GRC-ITRes IT Resource........................................... 2-57
2.3.13.4 Specifying Values in the Lookup.SAP.UM.Configuration Lookup Definition 2-58
2.3.13.5 Setting Up the Link with the Web Services for SAP Compliant User Provisioning... 2-58
2.3.13.6 Configuring Request Types and Workflows on SAP GRC Compliant User Provisioning 2-59
2.3.13.6.1 Creating Request Types............................................................................... 2-59
2.3.13.6.2 Creating Workflows.................................................................................... 2-61
2.3.13.7 Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition..... 2-66
2.3.14 Configuring SoD...................................................................................................... 2-68
2.3.14.1 Configuring SAP GRC to Act As the SoD Engine ............................................. 2-68
2.3.14.2 Specifying Values for SoD-Related Entries in the Lookup.SAP.UM.SoDConfiguration Lookup Definition 2-69
2.3.14.3 Modifying the SoD-Related Lookup Definitions .................................................. 2-70
2.3.14.4 Specifying Values for the GRC-ITRes IT Resource ........................................... 2-71
2.3.14.5 Verifying Entries Created in the Lookup.SAP.UM.System Lookup Definition 2-72
2.3.14.6 Specifying a Value for the TopologyName IT Resource Parameter ................. 2-73
2.3.14.7 Disabling and Enabling SoD .............................................................................. 2-73
2.3.14.7.1 Disabling and Enabling SoD on Oracle Identity Manager Release 9.1.0.x 2-73
2.3.14.7.2 Disabling and Enabling SoD on Oracle Identity Manager Release 11.1.x 2-79
2.3.15 Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System 2-80
2.3.15.1 Prerequisites for Configuring the Connector to Use SNC 2-81
2.3.15.2 Installing the Security Package ......................................................................... 2-81
2.3.15.3 Configuring SNC ............................................................................................. 2-82
2.3.16 Configuring the IT Resource .................................................................................. 2-83
2.3.16.1 Parameters for Enabling the Use of a Logon Group 2-84
2.3.16.2 Parameters for Enabling SNC-Based Communication 2-85
2.3.16.3 Parameters for Enabling Multiple Attempts to Update Multivalued Attributes 2-85
2.3.16.4 Mapping New Connection Properties 2-85
2.3.16.5 Specifying Values for the IT Resource Parameters 2-87
2.3.17 Addressing the Issue Related to Non-Unique Values in Lookup Definitions Synchronized with the Target System 2-91
2.3.18 Localizing Field Labels in UI Forms .................................................................. 2-92

3 Using the Connector

3.1 Performing Full Reconciliation ................................................................................ 3-1
3.2 Scheduled Task for Lookup Field Synchronization .................................................. 3-2
3.3 Guidelines on Performing Reconciliation .................................................................. 3-2
3.4 Configuring Reconciliation ..................................................................................... 3-2
3.4.1 Full Reconciliation vs. Incremental Reconciliation ................................................ 3-3
3.4.2 Limited Reconciliation ......................................................................................... 3-3
3.4.3 Reconciliation Scheduled Tasks ........................................................................... 3-4
3.4.3.1 SAP User Management User Recon ................................................................. 3-5
3.4.3.2 SAP User Management Delete Recon ............................................................... 3-5
3.4.3.3 SAP CUP Status Update Recon ........................................................................ 3-6
3.4.3.4 SAP CUP Delete Recon .................................................................................. 3-7
3.5 Configuring Scheduled Tasks .................................................................................. 3-8
3.6 Guidelines on Performing Provisioning ..................................................................... 3-10
3.7 Provisioning Operations Performed in an SoD-Enabled Environment .................... 3-12
3.7.1 Overview of the Provisioning Process in an SoD-Enabled Environment ............... 3-13
3.7.2 Guidelines on Performing Provisioning Operations .............................................. 3-13
3.7.3 Direct Provisioning in an SoD-Enabled Environment ............................................ 3-13
3.7.3.1 Prerequisites ................................................................................................... 3-14
3.7.3.2 Performing Direct Provisioning in Oracle Identity Manager Release 9.1.0.x or 11.1.1 3-15
3.7.3.3 Performing Direct Provisioning in Oracle Identity Manager Release 11.1.2 .... 3-25
3.7.4 Request-Based Provisioning in an SoD-Enabled Environment .............................. 3-26
3.7.4.1 End User's Role in Request-Based Provisioning ............................................. 3-26
3.7.4.1.1 End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x 3-26
3.7.4.1.2 End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.1 3-31
3.7.4.2 Approver's Role in Request-Based Provisioning .................................................. 3-32
3.7.4.2.1 Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x 3-33
3.7.4.2.2 Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.1 3-34
3.8 Switching Between SAP R/3 and SAP CUA Target Systems ........................................ 3-35
3.9 Switching Between SAP R/3 or SAP CUA Target System to an SAP CUP Target System on Oracle Identity Manager Release 11.1.x 3-36
3.10 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1 3-36
3.11 Enabling and Disabling the SoD Feature ........................................................................ 3-37
3.12 Enabling and Disabling the Compliant User Provisioning Feature ............................. 3-37

4 Extending the Functionality of the Connector
4.1 Determining the Names of Target System Attributes .................................................. 4-1
4.2 Adding New Attributes for Reconciliation ................................................................... 4-7
4.3 Adding New Standard and Custom Multivalued Attributes for Reconciliation ........... 4-13
4.4 Adding New Standard Attributes for Provisioning ....................................................... 4-19
4.5 Adding New Standard SAP GRC Compliant User Provisioning Attributes for Provisioning 4-25
4.6 Adding New Standard Multivalued Attributes for Provisioning .................................. 4-31
4.7 Adding Custom Attributes for Provisioning .................................................................. 4-39
4.8 Adding Custom Multivalued Attributes for Provisioning ............................................... 4-44
4.9 Configuring Validation of Data During Reconciliation and Provisioning ..................... 4-52
4.10 Configuring Transformation of Data During User Reconciliation ............................ 4-54
4.11 Configuring Transformation of Data During Lookup Field Synchronization ................ 4-56
4.12 Configuring Synchronization of New Lookup Definitions with the Target System .... 4-58
4.13 Modifying Field Lengths on the Process Form ......................................................... 4-61
4.14 Configuring the Connector for Multiple Installations of the Target System ............... 4-62
4.14.1 Enabling the Dependent Lookup Fields Feature ..................................................... 4-64

5 Known Issues

A Standard BAPIs Used During Connector Operations
A.1 Standard BAPIs Used on Both SAP R/3 and SAP CUA ................................................. A-1
A.2 Standard BAPIs Used on SAP R/3 ............................................................................... A-1
A.3 Standard BAPIs Used on SAP CUA ............................................................................ A-2
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–1</td>
<td>Connector Integrating SAP R/3 with Oracle Identity Manager</td>
<td>1-4</td>
</tr>
<tr>
<td>1–2</td>
<td>Connector Integrating SAP CUA with Oracle Identity Manager</td>
<td>1-5</td>
</tr>
<tr>
<td>1–3</td>
<td>Data Flow During the SoD Validation Process</td>
<td>1-7</td>
</tr>
<tr>
<td>1–4</td>
<td>Connector Integrating SAP GRC Compliant User Provisioning with Oracle Identity Manager and the Target System</td>
<td>1-8</td>
</tr>
<tr>
<td>1–5</td>
<td>Reconciliation Rule</td>
<td>1-26</td>
</tr>
<tr>
<td>1–6</td>
<td>Reconciliation Action Rules</td>
<td>1-27</td>
</tr>
<tr>
<td>2–1</td>
<td>Dialog Box Displayed on Running the SAP JCo Test</td>
<td>2-14</td>
</tr>
<tr>
<td>2–2</td>
<td>Reconciliation Rule with the Element for Linking</td>
<td>2-27</td>
</tr>
</tbody>
</table>
List of Tables

1–1  Certified Components ................................................................. 1-2
1–2  Entries in the Lookup.SAP.UM.LookupMappings and
    Lookup.SAP.CUA.LookupMappings Lookup Definitions 1-18
1–3  Preconfigured Lookup Definitions ........................................... 1-20
1–4  Entries in the Lookup.SAP.UM.ReconAttrMap Lookup Definition  1-24
1–5  Entries in the Lookup.SAP.UM.ReconChildAttrMap Lookup Definition  1-25
1–6  Action Rules for Reconciliation ................................................. 1-26
1–7  User Provisioning Functions ....................................................... 1-28
1–8  Entries in the Lookup.SAP.UM.ProvAttrMap Lookup Definition  1-28
1–9  Entries in the Lookup.SAP.UM.ProvChildAttrMap Lookup Definition  1-30
1–10 Entries in the Lookup.SAP.CUP.ProvAttrMap Lookup Definition  1-30
1–11 Entries in the Lookup.SAP.CUP.ProvisionRoleAttrMap Lookup Definition  1-30
2–1  Files and Directories On the Installation Media .......................... 2-2
2–2  Ports for SAP Services ............................................................... 2-22
2–3  Entries in the Lookup.SAP.UM.Configuration Lookup Definition  2-29
2–4  Log Levels and ODL Message Type:Level Combinations ............ 2-44
2–5  Parameters of the GRC-ITRes IT Resource ................................. 2-57
2–6  Entries in the Lookup.SAP.CUP.Configuration Lookup Definition  2-66
2–7  Entries in the Lookup.SAP.UM.SoDConfiguration Lookup Definition  2-69
2–8  Entries in the Lookup.SAP.UM.ProfileChildformMappings Lookup Definition  2-70
2–9  Entries in the Lookup.SAP.UM.RoleChildformMappings Lookup Definition  2-71
2–10 Parameters of the GRC-ITRes IT Resource ................................ 2-72
2–11 Entries in the Lookup.SAP.UM.ITResourceMapping Lookup Definition  2-86
2–12 Parameters of the IT Resource .................................................... 2-88
3–1  Attributes of the SAP User Management Lookup Recon Scheduled Task  3-2
3–2  Attributes of the SAP User Management User Recon Scheduled Task  3-5
3–3  Attributes of the SAP User Management Delete Recon Scheduled Task  3-6
3–4  Attributes of the SAP CUP Status Update Recon Scheduled Task  3-7
3–5  Attributes of the SAP CUP Delete Recon Scheduled Task  3-7
3–6  Scheduled Tasks for Lookup Field Synchronization and Reconciliation  3-8
4–1  Connector Objects and Their Associations .................................. 4-63
4–2  SQL Queries for Lookup Fields ................................................ 4-65
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

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

Access to Oracle Support

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

Related Documents

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

For generic information about connectors, see Oracle Fusion Middleware User's Guide for Oracle Identity Manager.

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

http://download.oracle.com/docs/cd/E14571_01/im.htm

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://download.oracle.com/docs/cd/E22999_01/index.htm
Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>boldface</td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td>italic</td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
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 9.1.2.6 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 9.1.2.6**
- **Software Updates in Release 9.1.2.5**
- **Software Updates in Release 9.1.2.4**
- **Software Updates in Release 9.1.2.2**
- **Software Updates in Release 9.1.2**
- **Software Updates in Release 9.1.1**
- **Software Updates in Release 9.1.0**

#### Software Updates in Release 9.1.2.6

The following are issues resolved in release 9.1.2.6:

<table>
<thead>
<tr>
<th>Bug Number</th>
<th>Issue</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>13361517</td>
<td>The connector did not allow addition of roles with the same name for different systems.</td>
<td>This issue has been resolved.</td>
</tr>
<tr>
<td>12675870</td>
<td>Two attributes were marked with <code>entitlement=true</code> property in child form.</td>
<td>This issue has been resolved. Now, only one attribute is marked with <code>entitlement=true</code> property in child form.</td>
</tr>
<tr>
<td>14209711</td>
<td>The valid-through date was not updated correctly when the user was enabled and disabled.</td>
<td>This issue has been resolved.</td>
</tr>
</tbody>
</table>
Software Updates in Release 9.1.2.5

The following are the software updates in release 9.1.2.5:

- Propagation of Password Changes to Child Systems in SAP CUA
- Resolved Issues in Release 9.1.2.5

Propagation of Password Changes to Child Systems in SAP CUA

From this release onward, the connector can be configured to propagate user password changes from the SAP CUA parent system to the child systems. To enable propagation of password changes to the child systems, you must set the value of the Is Password Propagate To Child System entry in the configuration lookup definition to Yes. In addition, you must configure the target system for password propagation by installing custom BAPIs.

See Section 2.3.4, "Configuring the Target System" for more information about configuring the target system to enable the connector to propagate password changes from the SAP CUA parent system to its child systems.

Resolved Issues in Release 9.1.2.5

The following table lists issues resolved in release 9.1.2.5:

<table>
<thead>
<tr>
<th>Bug Number</th>
<th>Issue</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>12586222</td>
<td>When running the SAP User Management Lookup Recon scheduled task against a set of different IT resources, the lookup definitions are populated. However, the values in the Code columns did not reflect the correct IT resource keys.</td>
<td>This issue has been resolved. The values in the Code columns reflect the correct IT resource keys. The ITResource APIs are used for this purpose.</td>
</tr>
<tr>
<td>10627537</td>
<td>During a reconciliation operation, two reconciliation events were generated for every SAP account.</td>
<td>This issue has been resolved. Instead of generating separate reconciliation events for the account lock status, the connector generates status in a single reconciliation event.</td>
</tr>
</tbody>
</table>

Software Updates in Release 9.1.2.4

The following table lists issues resolved in release 9.1.2.4:

<table>
<thead>
<tr>
<th>Bug Number</th>
<th>Issue</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| 9475592 and 10408848 | After the Disable User provisioning operation was performed, the value of the Valid Through field in Oracle Identity Manager did not match the value of the corresponding attribute in the target system. In addition, the Valid Through Updated task failed. | This issue has been resolved. After the Disable User provisioning operation, to ensure that the values of the Valid Through fields in the target system and Oracle Identity Manager match, the connector performs one of the following steps:
  - If the OIM User is logged into the target system while the Disable User provisioning operation is being performed, then the value of the Valid Through attribute in the target system is set to the current date.
  - If the OIM User is not logged into the target system while the Disable User provisioning operation is being performed, then the value of the Valid Through attribute in the target system is set to a date in the past. |
The following are the software updates in release 9.1.2.2:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning

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

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

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

See Section 3.7.4, "Request-Based Provisioning in an SoD-Enabled Environment" for more information.

Software Updates in Release 9.1.2
The following are the software updates 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.

Bug Number | Issue | Resolution
--- | --- | ---
10373020 | Suppose you assign more than one instance of a role with different Start Date and End Date values to a user account. If you reconciled the user account, then only the role instance with the latest date as the Start Date value was reconciled. | This issue has been resolved. The connector reconciles all instances of a role assigned to the user. Reconcile future dated roles and Reconcile past dated roles entries have been added in the Lookup.SAP.UM.Configuration lookup definition. You use these entries to specify whether you want reconcile future-date or past-dated roles. See Section 2.3.5.3, "Setting Values in the Lookup.SAP.UM.Configuration Lookup Definition" for more information about these entries.
11070597 | The connector did not log BAPI attributes. | This issue has been resolved. The connector now logs BAPI attributes.
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 1.5.17, "Transformation of Lookup Field Data" provides a pointer to additional information about this feature.

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 1.5.1, "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 1.7.1, "User Attributes for Reconciliation"
- Section 1.8.2, "User Attributes for Provisioning"

New Provisioning Functions
In Section 1.8.1, "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 1.5.12, "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.
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 2.3.10, "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 1.5.9, "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 2–12, "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 2.3.16.1, "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 1.5.8, "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 1.5.14, "Connection Pooling" for more information.
Testing Utility Deprecated
The testing utility is not included in this release of the connector.

Software Updates in Release 9.1.0
This is the first release of the Oracle Identity Manager Connector for SAP User Management. 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 1.5.3, "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 1.6, "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:


---

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 1.7.2, "Reconciliation Rules" for more information.

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

Documentation-Specific Updates
The following sections discuss documentation-specific updates:

■ Documentation-Specific Updates in Release 9.1.2.6
■ Documentation-Specific Updates in Release 9.1.2.5
■ Documentation-Specific Updates in Release 9.1.2.4
■ Documentation-Specific Updates in Release 9.1.2.2
■ Documentation-Specific Updates in Release 9.1.2
■ Documentation-Specific Updates in Release 9.1.1
■ Documentation-Specific Updates in Release 9.1.0

Documentation-Specific Updates in Release 9.1.2.6
The following are documentation-specific updates in revision "16" of release 9.1.2.6:

■ The "Oracle Identity Manager" row of Section 1.1, "Certified Components" has been modified.
■ Section 1.2, "Usage Recommendation" has been added.

The following are documentation-specific updates in revision "15" of release 9.1.2.6:

■ The "Oracle Identity Manager" row in Table 1–1, "Certified Components" has been modified.
■ A note has been added in the following rows of Table 2–1, "Files and Directories On the Installation Media":
  – Files in the Datasets directory
  – xml/SAP-UserMgmt-RequestApproval-ConnectorConfig.xml
  – xml/SAP-UserMgmt-CUP-RequestApproval-ConnectorConfig.xml
■ The following sections have been added:
  – Section 2.3.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
  – Section 2.3.2, "Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later"
  – Section 2.3.18, "Localizing Field Labels in UI Forms"
  – Section 3.7.3.2, "Performing Direct Provisioning in Oracle Identity Manager Release 9.1.0.x or 11.1.1"
  – Section 3.7.3.3, "Performing Direct Provisioning in Oracle Identity Manager Release 11.1.2"
Instructions specific to Oracle Identity Manager release 11.1.2.x have been added in the following sections:

- Section 2.2, "Installation"
- Section 2.3.16, "Configuring the IT Resource"
- Section 3.5, "Configuring Scheduled Tasks"

**Documentation-Specific Updates in Release 9.1.2.5**
The following are documentation-specific update in release 9.1.2.5:

- In Chapter 4, "Extending the Functionality of the Connector," Table 4–1 the comments on creating a copy for the Resource Object, Process Definition, and Process Form connector objects have been updated.
- In Chapter 5, "Known Issues," bug 13429841 has been added.

**Documentation-Specific Updates in Release 9.1.2.4**
The following are the documentation-specific updates in this release:

- In Chapter 5, "Known Issues," the issue tracked by bug 10361925 has been added.
- Section 2.1.2.1, "Creating a Target System User Account for Connector Operations," has been modified.
- Section 2.3.12, "Copying the SAPCUP.jar File for User Provisioning" has been added.
- In Section 2.3.13.5, "Setting Up the Link with the Web Services for SAP Compliant User Provisioning," the note has been modified.

**Documentation-Specific Updates in Release 9.1.2.2**
There are no documentation-specific updates in this release.

**Documentation-Specific Updates in Release 9.1.2**
Minor changes have been made in the structure and location of some sections.

**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 9.1.0**
This is the first release of the Oracle Identity Manager Connector for SAP User Management. 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 1.9, "Roadmap for Deploying and Using the Connector" for information about the organization of content in this guide.
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, "Usage Recommendation"
- Section 1.3, "Certified Languages"
- Section 1.4, "Connector Architecture and Supported Deployment Configurations"
- Section 1.5, "Features of the Connector"
- Section 1.6, "Lookup Definitions Used During Connector Operations"
- Section 1.7, "Connector Objects Used During Reconciliation"
- Section 1.8, "Connector Objects Used During Provisioning"
- Section 1.9, "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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Oracle Identity Manager | You can use one of the following releases of Oracle Identity Manager:  
  - Oracle Identity Manager release 9.1.0.2 BP04 and any later BP in this release track  
    **Note:** In this guide, Oracle Identity Manager release 9.1.0.x has been used to denote Oracle Identity Manager release 9.1.0.2 BP04 and future releases in the 9.1.0.x series that the connector supports.  
  - Oracle Identity Manager 11g release 1 (11.1.1.3.0) and any later BP in this release track  
    **Note:** In this guide, Oracle Identity Manager release 11.1.1 has been used to denote Oracle Identity Manager release 11g release 1 (11.1.1) and future releases in the 11.1.1.x series that the connector supports.  
  - Oracle Identity Manager 11g release 1 PS1 (11.1.1.5.0) and any later BP in this release track  
  - Oracle Identity Manager 11g release 1 PS2 (11.1.1.7.0) and any later BP in this release track  
  - Oracle Identity Manager 11g release 2 BP04 (11.1.2.0.4) and any later BP in this release track  
    **Note:** In this guide, Oracle Identity Manager release 11.1.2 has been used to denote Oracle Identity Manager release 11g release 2 BP04 (11.1.2.0.4) and future releases in the 11.1.2.x series that the connector supports.  
  The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at [http://www.oracle.com/technetwork/documentation/oim1014-097544.html](http://www.oracle.com/technetwork/documentation/oim1014-097544.html) |
| JDK                     | The JDK requirement is as follows:  
  **Note:** JRockit is not supported because it is incompatible with the SAP JCo libraries.  
  - For Oracle Identity Manager release 9.1.0.x, use Sun/IBM JDK 1.5 or later.  
  - For Oracle Identity Manager release 11.1.x, use Sun/IBM JDK 1.6 update 18 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 or later  
  - mySAP ERP 2004 (ECC 5.0 running on WAS 6.40) BASIS SP 22 or later  
  - mySAP ERP 2005 (ECC 6.0 running on WAS 7.00) BASIS SP 13 or later  
  **Note:** From version 6.40 onward, SAP WAS is also known as ”SAP NetWeaver.”  
  In general:  
  - SAP applications installed on the ABAP stack are supported.  
  - Applications installed on the JAVA stack are not supported.  
  - Some SAP applications can be installed on the ABAP+JAVA stack. While installing such an application, you specify either ABAP or JAVA as the data source. The connector supports SAP applications that use the ABAP data source. |
1.2 Usage Recommendation

Depending on the Oracle Identity Manager version that you are using, you must deploy and use one of the following connectors:

- If you are using an Oracle Identity Manager release that is 9.1.0.1 or later and earlier than Oracle Identity Manager Release 9.1.0.2 BP04, then use the 9.0.4.x version of this connector.

- If you are using Oracle Identity Manager Release 9.1.0.2 BP04 or later and earlier than Oracle Identity Manager 11g PS1 BP07 (11.1.1.5.7) with patch 16627402, then use the latest 9.1.2.x version of this connector.

- If you are using Oracle Identity Manager 11g Release 1 PS1 BP07 (11.1.1.5.7) with patch 16627402 or later, or Oracle Identity Manager 11g Release 2 BP05 (11.1.2.0.5) with patch 16627415 or later, then use the latest 11.1.1.x version of this connector.

1.3 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
1.4 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.
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.

**Note:** The connector does not support direct administration of accounts on child systems in SAP CUA. As shown in Figure 1–2, all connector operations are performed between Oracle Identity Manager and the SAP R/3 parent system. When required, user data changes resulting from these connector operations are propagated from the parent system to the child system.

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 1.4.1, "Basic User Management"
- Section 1.4.2, "User Management with SoD"
- Section 1.4.3, "User Management with Compliant User Provisioning"
- Section 1.4.4, "User Management with Both SoD and Compliant User Provisioning"
- Section 1.4.5, "Guidelines on Using a Deployment Configuration"
- Section 1.4.6, "Considerations to Be Addressed When You Enable Compliant User Provisioning"

### 1.4.1 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.

### 1.4.2 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**

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. 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.

### 1.4.3 User Management with Compliant User Provisioning

Compliant User Provisioning (CUP) 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.

1.4.4 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.

1.4.5 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.

1.4.6 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 1.5.9, “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.

1.5 Features of the Connector

The following are features of the connector:

- Section 1.5.1, “Support for Both SAP R/3 and SAP CUA”

- Section 1.5.2, “Mapping Standard and Custom Attributes for Reconciliation and Provisioning”

- Section 1.5.3, “SoD Validation of Entitlement Requests”

- Section 1.5.4, “Routing of Provisioning Requests Through SAP GRC Compliant User Provisioning”
1.5.1 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.

1.5.2 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.

1.5.3 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.
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.

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.

In Oracle Identity Manager release 11.1.1, object forms have been replaced by request datasets. A request dataset is an XML file that specifies information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. The default approval workflow and associated request dataset are configured for the SoD validation capabilities of SAP GRC. You can use them to develop your own approval workflows and request datasets. See Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager for more information about request datasets.

1.5.4 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 1.4.3, "User Management with Compliant User Provisioning" for detailed information about this feature.

1.5.5 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.
1.5.6 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.

1.5.7 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.

1.5.8 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.

1.5.9 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 2.3.5.1, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts" for more information.

1.5.10 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 2.3.15, "Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System" for more information.
1.5.11 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 2.3.10, "Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition" for more information.

1.5.12 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 2.3.16, "Configuring the IT Resource"

Section 2.3.5.2, "Configuring Password Changes for Newly Created Accounts"

1.5.13 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 2–12, "Parameters of the IT Resource" for more information.

1.5.14 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 2.3.16, "Configuring the IT Resource" provides information about setting up the connection pool.

1.5.15 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 2.3.16.1, "Parameters for Enabling the Use of a Logon Group" for more information.

1.5.16 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"

1.5.17 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.

1.5.18 Support for Both Unicode and Non-Unicode Modes

An SAP application can be run in either Unicode or non-Unicode mode. The connector supports both modes.

1.6 Lookup Definitions Used During Connector Operations

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

- Section 1.6.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.6.2, "Preconfigured Lookup Definitions"

1.6.1 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.
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>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup.SAP.UM.CommType</td>
<td>BAPI_HELPVALUES_GET;GETDETAIL;ADDRESS;COMM_TYPE;COMM_TYPE;COMM_TEXT</td>
</tr>
<tr>
<td>Lookup.SAP.UM.Company</td>
<td>BAPI_HELPVALUES_GET;GETDETAIL;COMPANY;COMPANY;COMPANY;COMPANY_ADDR;SH</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ContractualUserType</td>
<td>BAPI_HELPVALUES_GET;GETDETAIL;UCLASSSYS;LIC_TYPE;USER_TYP;UTYPTEXT;LANGU;J;EQ;EN</td>
</tr>
<tr>
<td>Lookup.SAP.UM.DateFormat</td>
<td>BAPI_HELPVALUES_GET;GETDETAIL;DEFAULTS;DATFM;_LOW;_TEXT</td>
</tr>
<tr>
<td>Lookup.SAP.UM.DecimalNotation</td>
<td>BAPI_HELPVALUES_GET;GETDETAIL;DEFAULTS;DCPFM;_LOW;_TEXT</td>
</tr>
<tr>
<td>Lookup.SAP.UM.LangComm</td>
<td>BAPI_HELPVALUES_GET;GETDETAIL;ADDRESS;LANGU_P;SPRAS;SPTXT</td>
</tr>
<tr>
<td>Lookup.SAP.UM.Parameter</td>
<td>BAPI_HELPVALUES_GET;GETDETAIL;PARAMETER;PARID;PARAM_ID;PARTEXT</td>
</tr>
<tr>
<td>Lookup.SAP.UM.Profile</td>
<td>For SAP R/3:</td>
</tr>
<tr>
<td></td>
<td>BAPI_HELPVALUES_GET;GETDETAIL;PROFILES;BAPIPROF;PROFN;PTEXT</td>
</tr>
<tr>
<td></td>
<td>For SAP CUA:</td>
</tr>
<tr>
<td></td>
<td>RFC_READ_TABLE;USRSYSPRFT;PROFN;PTEXT;SUBSYSTEM;USRSYSPRFT;LANGU = 'EN'</td>
</tr>
<tr>
<td>Lookup.SAP.UM.Roles</td>
<td>For SAP R/3:</td>
</tr>
<tr>
<td></td>
<td>BAPI_HELPVALUES_GET;GETDETAIL;ACTIVITYGROUPS;AGR_NAME;AGR_NAME;TEXT;AGR_COLL;SH</td>
</tr>
<tr>
<td></td>
<td>For SAP CUA:</td>
</tr>
<tr>
<td></td>
<td>RFC_READ_TABLE;USRSYSACCT;AGR_NAME;TEXT;SUBSYSTEM;USRYSACCT;LANGU = 'EN'</td>
</tr>
<tr>
<td>Lookup.SAP.UM.System</td>
<td>For SAP R/3:</td>
</tr>
<tr>
<td></td>
<td>SYSTEMNAME</td>
</tr>
<tr>
<td></td>
<td>For SAP CUA:</td>
</tr>
<tr>
<td></td>
<td>RFC_READ_TABLE;USZBVLNDR;RCVSYSTEM;RCVSYSTEM</td>
</tr>
</tbody>
</table>
The following is the format of entries in each lookup definition 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.
### 1.6.2 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>
<thead>
<tr>
<th>Lookup Definition</th>
<th>Description of Values</th>
<th>Method to Specify Values for the Lookup Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup.SAP.UM.Configuration</td>
<td>This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.</td>
<td>Some of the entries in this lookup definition are preconfigured. See Section 2.3.5, &quot;Setting Up the Configuration Lookup Definition in Oracle Identity Manager&quot; for information about the entries for which you can set values.</td>
</tr>
<tr>
<td>Lookup.SAP.CUP.Configuration</td>
<td>This lookup definition holds connector configuration entries that are used during reconciliation and provisioning by the Compliant User Provisioning feature. <strong>Note:</strong> This lookup definition is created only after you configure the Compliant User Provisioning feature.</td>
<td>Some of the entries in this lookup definition are preconfigured. See Section 2.3.13.7, &quot;Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition&quot; for information about the entries for which you can set values.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.Constants</td>
<td>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.</td>
<td>You must not modify the entries in this lookup definition.</td>
</tr>
<tr>
<td>Lookup.SAP.CUP.Constants</td>
<td>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. <strong>Note:</strong> This lookup definition is created only after you configure the Compliant User Provisioning feature.</td>
<td>You must not modify the entries in this lookup definition.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ExclusionList</td>
<td>This lookup definition holds user IDs of target system accounts for which you do not want to perform reconciliation and provisioning.</td>
<td>You can enter user IDs in this lookup definition. See Section 2.3.10, &quot;Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition&quot; for more information.</td>
</tr>
</tbody>
</table>
## Lookup Definitions Used During Connector Operations

### Lookup.SAP.UM.ITResourceMapping
- **Description of Values**: 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
- **Method to Specify Values for the Lookup Definition**: See Table 2–11 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 2.3.16.4, “Mapping New Connection Properties” for information.

### Lookup.SAP.CUA.LookupMappings and Lookup.SAP.UM.LookupMappings
- **Description of Values**: These lookup definitions hold data required to synchronize other lookup definitions with the target system.
- **Method to Specify Values for the Lookup Definition**: 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
- **Description of Values**: This lookup definition is used to configure transformation of data during lookup field synchronization.
- **Method to Specify Values for the Lookup Definition**: 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
- **Description of Values**: This lookup definition holds mappings between process form fields and single-valued target system attributes.
- **Method to Specify Values for the Lookup Definition**: 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.

### Lookup.SAP.CUP.ProvisionAttrMap
- **Description of Values**: 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.
- **Method to Specify Values for the Lookup Definition**: 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
- **Description of Values**: This lookup definition holds mappings between process form fields and multivalued target system attributes.
- **Method to Specify Values for the Lookup Definition**: 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 Definitions Used During Connector Operations

#### Lookup Definition Description of Values Method to Specify Values for the Lookup Definition

<table>
<thead>
<tr>
<th>Lookup Definition</th>
<th>Description of Values</th>
<th>Method to Specify Values for the Lookup Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup.SAP.CUP.ProvisionRoleAttrMap</td>
<td>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.</td>
<td>This lookup definition is preconfigured. Table 1–9 lists the default entries in this lookup definition.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ProvCheckBoxMapping</td>
<td>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.</td>
<td>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 Section 4.4, &quot;Adding New Standard Attributes for Provisioning&quot; for more information.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ProvValidation</td>
<td>This lookup definition is used to configure validation of attribute values entered on the process form during provisioning operations.</td>
<td>You manually create entries in this lookup definition. See Section 4.9, &quot;Configuring Validation of Data During Reconciliation and Provisioning&quot; for more information.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ReconAttrMap</td>
<td>This lookup definition holds mappings between resource object fields and single-valued target system attributes.</td>
<td>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, &quot;Adding New Attributes for Reconciliation&quot; for more information.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ReconChildAttrMap</td>
<td>This lookup definition holds mappings between resource object fields and multivalued target system attributes.</td>
<td>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, &quot;Adding New Standard and Custom Multivalued Attributes for Reconciliation&quot; for more information.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.CustomChildAttrMap</td>
<td>This lookup definition holds mappings between resource object fields and custom multivalued target system attributes.</td>
<td>You can add entries in this lookup definition if you want to map custom target system attributes for reconciliation. See Section 4.3, &quot;Adding New Standard and Custom Multivalued Attributes for Reconciliation&quot; for more information.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.RoleChildFormMappings</td>
<td>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.</td>
<td>This lookup definition is preconfigured. Table 2–9 lists the entries in this lookup definition.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ReconCheckBoxMapping</td>
<td>This lookup definition maps check box attributes of the target system with their values when selected and deselected. It is used during reconciliation.</td>
<td>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, &quot;Adding New Attributes for Reconciliation&quot; for more information.</td>
</tr>
</tbody>
</table>
1.7 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 Fusion Middleware User’s Guide for Oracle Identity Manager for conceptual information about reconciliation.

This section discusses the following topics:

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

1.7.1 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

Table 1–3 (Cont.) Preconfigured Lookup Definitions

<table>
<thead>
<tr>
<th>Lookup Definition</th>
<th>Description of Values</th>
<th>Method to Specify Values for the Lookup Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup.SAP.UM.ReconTransformation</td>
<td>This lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation.</td>
<td>You manually create entries in this lookup definition. See Section 4.10, &quot;Configuring Transformation of Data During User Reconciliation&quot; for more information.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ReconValidation</td>
<td>This lookup definition is used to configure validation of attribute values that are fetched from the target system during reconciliation.</td>
<td>You manually create entries in this lookup definition. See Section 4.9, &quot;Configuring Validation of Data During Reconciliation and Provisioning&quot; for more information.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ProfileChildformMappings</td>
<td>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.</td>
<td>This lookup definition is preconfigured. Table 2–8 lists the entries in this lookup definition.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.SoDConfiguration</td>
<td>This lookup definition holds configuration values that are used by the connector during SoD operations.</td>
<td>See Section 2.3.14.2, &quot;Specifying Values for SoD-Related Entries in the Lookup.SAP.UM.SoDConfiguration Lookup Definition&quot; for information about specifying values for the entries in this lookup definition.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.CustomAttrMap</td>
<td>This lookup definition holds details of custom attributes that you want to include for reconciliation.</td>
<td>See Step 6 in Section 4.2, &quot;Adding New Attributes for Reconciliation&quot; for information about creating entries in this lookup definition.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Resource Object Field</th>
<th>Target System Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Number</td>
<td>TEXT; ACCNT; LOGONDATA</td>
</tr>
<tr>
<td>Alias</td>
<td>TEXT; USERALIAS; ALIAS</td>
</tr>
<tr>
<td>Building</td>
<td>TEXT; BUILDING_P; ADDRESS</td>
</tr>
<tr>
<td>Communication Type</td>
<td>LOOKUP; COMM_TYPE; ADDRESS</td>
</tr>
<tr>
<td>Company</td>
<td>LOOKUP; COMPANY; COMPANY</td>
</tr>
<tr>
<td>Contractual User Type</td>
<td>LOOKUP; LIC_TYPE; UCLASS</td>
</tr>
<tr>
<td>Cost Center</td>
<td>TEXT; KOSTL; DEFAULTS</td>
</tr>
<tr>
<td>Date Format</td>
<td>LOOKUP; DATFM; DEFAULTS</td>
</tr>
<tr>
<td>Decimal Notation</td>
<td>LOOKUP; DCPFM; DEFAULTS</td>
</tr>
<tr>
<td>Department</td>
<td>TEXT; DEPARTMENT; ADDRESS</td>
</tr>
<tr>
<td>E Mail</td>
<td>TEXT; E_MAIL; ADDRESS</td>
</tr>
<tr>
<td>Fax Extension</td>
<td>TEXT; FAX_EXTENS; ADDRESS</td>
</tr>
<tr>
<td>Fax Number</td>
<td>TEXT; FAX_NUMBER; ADDRESS</td>
</tr>
<tr>
<td>First Name</td>
<td>TEXT; FIRSTNAME; ADDRESS</td>
</tr>
<tr>
<td>Floor</td>
<td>TEXT; FLOOR_P; ADDRESS</td>
</tr>
<tr>
<td>Function</td>
<td>TEXT; FUNCTION; ADDRESS</td>
</tr>
<tr>
<td>Lang Communication</td>
<td>LOOKUP; LANGU_P; ADDRESS</td>
</tr>
<tr>
<td>Last Name</td>
<td>TEXT; LASTNAME; ADDRESS</td>
</tr>
<tr>
<td>Logon Language</td>
<td>LOOKUP; LANGU; DEFAULTS</td>
</tr>
<tr>
<td>Room Number</td>
<td>TEXT; ROOM_NO_P; ADDRESS</td>
</tr>
<tr>
<td>Start Menu</td>
<td>TEXT; START_MENU; DEFAULTS</td>
</tr>
<tr>
<td>Telephone Extension</td>
<td>TEXT; TEL1_EXT; ADDRESS</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>TEXT; TEL1_NUMBR; ADDRESS</td>
</tr>
<tr>
<td>Time Zone</td>
<td>LOOKUP; TZONE; LOGONDATA</td>
</tr>
<tr>
<td>Title</td>
<td>LOOKUP; TITLE_P; ADDRESS</td>
</tr>
<tr>
<td>User Group</td>
<td>LOOKUP; CLASS; LOGONDATA</td>
</tr>
<tr>
<td>User Type</td>
<td>TEXT; USTYP; LOGONDATA</td>
</tr>
<tr>
<td>Valid From</td>
<td>DATE; GLTGV; LOGONDATA</td>
</tr>
<tr>
<td>Valid Through</td>
<td>DATE; GLTGB; LOGONDATA</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Child Form Field</th>
<th>Target System Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>End Date</td>
<td>DATE;TO_DAT;ACTIVITYGROUPS;User Role</td>
</tr>
<tr>
<td>Profile Name</td>
<td>LOOKUP;PROFILE</td>
</tr>
<tr>
<td>Profile System Name</td>
<td>LOOKUP;SUBSYSTEM;PROFILES;User Profile</td>
</tr>
<tr>
<td>Role Name</td>
<td>LOOKUP;AGR_NAME;ACTIVITYGROUPS;User Role</td>
</tr>
<tr>
<td>Role System Name</td>
<td>LOOKUP;SUBSYSTEM;ACTIVITYGROUPS;User Role</td>
</tr>
<tr>
<td>Start Date</td>
<td>DATE;FROM_DAT;ACTIVITYGROUPS;User Role</td>
</tr>
</tbody>
</table>

1.7.2 Reconciliation Rules

See Also: Oracle Fusion Middleware User’s Guide for Oracle Identity Manager for generic information about reconciliation matching and action rules.

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

- Section 1.7.2.1, "Reconciliation Rule"
- Section 1.7.2.2, "Viewing Reconciliation Rules in the Design Console"

1.7.2.1 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.

1.7.2.2 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:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand Development Tools.
4. Search for and open SAP UM Recon Rule. Figure 1–5 shows this reconciliation rule.

Note: Perform the following procedure only after the connector is deployed.
1.7.3 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. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Fusion Middleware User’s Guide for Oracle Identity Manager*
- For Oracle Identity Manager release 11.1.x: *Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager*

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

- Section 1.7.3.1, "Reconciliation Action Rules for Reconciliation"
- Section 1.7.3.2, "Viewing Reconciliation Action Rules in the Design Console"

### 1.7.3.1 Reconciliation Action Rules for Reconciliation

Table 1–6 lists the action rules for reconciliation.

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Matches Found</td>
<td>Assign to Administrator With Least Load</td>
</tr>
<tr>
<td>One Entity Match Found</td>
<td>Establish Link</td>
</tr>
<tr>
<td>One Process Match Found</td>
<td>Establish Link</td>
</tr>
</tbody>
</table>

### 1.7.3.2 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.
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**

![Reconciliation Action Rules](image)

### 1.8 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 Fusion Middleware User’s Guide for Oracle Identity Manager* for conceptual information about provisioning

This section discusses the following topics:

- Section 1.8.1, "User Provisioning Functions"
- Section 1.8.2, "User Attributes for Provisioning"

#### 1.8.1 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 Fusion Middleware User’s Guide for Oracle Identity Manager* for generic information about process tasks and adapters
1.8.2 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:

\[\text{FIELD\_TYPE};\,\text{FIELD\_NAME};\,\text{STRUCTURE\_NAME};\,\text{FIELD\_NAME\_X};\,\text{STRUCTURE\_NAME\_X}\]

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>
<thead>
<tr>
<th>Process Form Field</th>
<th>Target System Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Number</td>
<td>TEXT;ACCNT;LOGONDATA;ACCNT;LOGONDATAX</td>
</tr>
<tr>
<td>Alias</td>
<td>TEXT;USERALIAS;ALIAS;BAPIALIAS;ALIASX</td>
</tr>
<tr>
<td>Building</td>
<td>TEXT;BUILDING_P;ADDRESS;BUILDING_P;ADDRESSX</td>
</tr>
</tbody>
</table>
Table 1–8  (Cont.) Entries in the Lookup.SAP.UM.ProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Process Form Field</th>
<th>Target System Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Type</td>
<td>LOOKUP;COMM_TYPE;ADDRESS;COMM_TYPE;ADDRESSX</td>
</tr>
<tr>
<td>Company</td>
<td>LOOKUP;COMPANY;COMPANY;COMPANY;COMPANY;COMPANYX</td>
</tr>
<tr>
<td>Contractual User Type</td>
<td>LOOKUP;LIC_TYPE;UCLASS;UCLASS;UCLASSX</td>
</tr>
<tr>
<td>Cost Center</td>
<td>TEXT;KOSTL;DEFAULTS;KOSTL;DEFAULTSX</td>
</tr>
<tr>
<td>Date Format</td>
<td>LOOKUP;DATFM;DEFAULTS;DATFM;DEFAULTSX</td>
</tr>
<tr>
<td>Decimal Notation</td>
<td>LOOKUP;DCP FM;DEFAULTS;DCP FM;DEFAULTSX</td>
</tr>
<tr>
<td>Department</td>
<td>TEXT;DEPARTMENT;ADDRESS;DEPARTMENT;ADDRESSX</td>
</tr>
<tr>
<td>E Mail</td>
<td>TEXT;E_MAIL;ADDRESS;E_MAIL;ADDRESSX</td>
</tr>
<tr>
<td>Fax Extension</td>
<td>TEXT;FAX_EXTENS;ADDRESS;FAX_EXTENS;ADDRESSX</td>
</tr>
<tr>
<td>Fax Number</td>
<td>TEXT;FAX_NUMBER;ADDRESS;FAX_NUMBER;ADDRESSX</td>
</tr>
<tr>
<td>First Name</td>
<td>TEXT;FIRSTNAME;ADDRESS;FIRSTNAME;ADDRESSX</td>
</tr>
<tr>
<td>Floor</td>
<td>TEXT;FLOOR_P;ADDRESS;FLOOR_P;ADDRESSX</td>
</tr>
<tr>
<td>Function</td>
<td>TEXT;FUNCTION;ADDRESS;FUNCTION;ADDRESSX</td>
</tr>
<tr>
<td>Language Communication</td>
<td>LOOKUP;LANGU_P;ADDRESS;LANGU_P;ADDRESSX</td>
</tr>
<tr>
<td>Last Name</td>
<td>TEXT;LASTNAME;ADDRESS;LASTNAME;ADDRESSX</td>
</tr>
<tr>
<td>Logon Language</td>
<td>LOOKUP;LANGU;DEFAULTS;LANGU;DEFAULTSX</td>
</tr>
<tr>
<td>Password</td>
<td>TEXT;BAPIPWD;PASSWORD;BAPIPWD;PASSWORDX</td>
</tr>
<tr>
<td>Room Number</td>
<td>TEXT;ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX</td>
</tr>
<tr>
<td>Start Menu</td>
<td>TEXT;START_MENU;DEFAULTS;START_MENU;DEFAULTSX</td>
</tr>
<tr>
<td>Telephone Extension</td>
<td>TEXT;TEL1_EXT;ADDRESS;TEL1_EXT;ADDRESSX</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>TEXT;TEL1_NUMBR;ADDRESS;TEL1_NUMBR;ADDRESSX</td>
</tr>
<tr>
<td>Time Zone</td>
<td>LOOKUP;TZONE;LOGONDATA;TZONE;LOGONDATAAX</td>
</tr>
<tr>
<td>Title</td>
<td>LOOKUP;TITLE_P;ADDRESS;TITLE_P;ADDRESSX</td>
</tr>
<tr>
<td>User Group</td>
<td>LOOKUP;CLASS;LOGONDATA;CLASS;LOGONDATAAX</td>
</tr>
<tr>
<td>User ID</td>
<td>TEXT;USERNAME;NONE;NONE;NONE</td>
</tr>
<tr>
<td>User Type</td>
<td>TEXT;USTYP;LOGONDATA;USTYP;LOGONDATAAX</td>
</tr>
<tr>
<td>Valid From</td>
<td>DATE;GLTGV;LOGONDATA;GLTGV;LOGONDATA</td>
</tr>
<tr>
<td>Valid Through</td>
<td>DATE;GLTGB;LOGONDATA;GLTGB;LOGONDATA</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Child Form Field</th>
<th>Target System Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>End Date</td>
<td>TEXT;TO_DAT;ACTIVITYGROUPS</td>
</tr>
<tr>
<td>Profile Name</td>
<td>LOOKUP;PROFILE</td>
</tr>
<tr>
<td>Profile System Name</td>
<td>LOOKUP;SUBSYSTEM;PROFILES</td>
</tr>
<tr>
<td>Role Name</td>
<td>LOOKUP;AGR_NAME;ACTIVITYGROUPS</td>
</tr>
<tr>
<td>Role System Name</td>
<td>LOOKUP;SUBSYSTEM;ACTIVITYGROUPS</td>
</tr>
<tr>
<td>Start Date</td>
<td>TEXT;FROM_DAT;ACTIVITYGROUPS</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>Process Form Field</th>
<th>Target System Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>End Date</td>
<td>validTo;DATE</td>
</tr>
<tr>
<td>Profile Name</td>
<td>roeldid;LOOKUP</td>
</tr>
<tr>
<td>Profile System Name</td>
<td>sysId;LOOKUP</td>
</tr>
<tr>
<td>Role Name</td>
<td>roeldid;LOOKUP</td>
</tr>
<tr>
<td>Role System Name</td>
<td>sysId;LOOKUP</td>
</tr>
<tr>
<td>Start Date</td>
<td>validFrom;DATE</td>
</tr>
</tbody>
</table>

1.9 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.
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>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration/SAPUM-CI.xm</td>
<td>This XML file contains configuration information that is used during connector installation.</td>
</tr>
</tbody>
</table>
| Files in the DataSets directory | These XML files specify the information to be submitted by the requester during a request-based provisioning operation.  
**Note:** These XML files are specific to Oracle Identity Manager releases prior to 11.1.2. |
| 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 to the following location:  
- For Oracle Identity Manager release 9.1.0.x:  
  `OIM_HOME/xellerate/JavaTasks`  
- For Oracle Identity Manager release 11.1.x: Oracle Identity Manager database |
| lib/SAPCommon.jar | This JAR file contains the class files that are common to all SAP connectors. During connector deployment, this file is copied to the following location:  
- For Oracle Identity Manager release 9.1.0.x:  
  `OIM_HOME/xellerate/ScheduleTask`  
- For Oracle Identity Manager release 11.1.x: Oracle Identity Manager database |
| lib/Common.jar | This JAR file contains the class files that are common to all connectors. During connector deployment, this file is copied to the following location:  
- For Oracle Identity Manager release 9.1.0.x:  
  `OIM_HOME/xellerate/ScheduleTask`  
- For Oracle Identity Manager release 11.1.x: Oracle Identity Manager database |
| 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 to the following location:  
- For Oracle Identity Manager release 9.1.0.x:  
  `OIM_HOME/xellerate/connectorResources`  
- For Oracle Identity Manager release 11.1.x: Oracle Identity Manager database  
**Note:** A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages. |
| Sample/TransformLookup1.java | This file contains the code to work around the Oracle Identity Manager issue described by Bug 9237745. See Section 2.3.17, "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 connector objects:  
- IT resource definition  
- Process form  
- Lookup definitions  
- Resource object  
- Process definition  
- Scheduled tasks |
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.

Note: If you are using Oracle Identity Manager release 9.1.0.x, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.x, then skip this section.

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 the current release of the SAP User Management connector, then back up the existing Common.jar file, install the SAP User Management connector, and restore the Common.jar file. The steps to perform this procedure are as follows:

---

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

<table>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xml/SAP-UserMgmt-RequestApproval-ConnectorConfig.xml</td>
<td>This file contains definitions of the connector components for request-based provisioning when you configure the Compliant User Provisioning feature. See Section 2.3.6, “Enabling Request-Based Provisioning” for instructions on importing this file.</td>
</tr>
<tr>
<td>Note: This XML file is specific to Oracle Identity Manager releases prior to 11.1.2.</td>
<td></td>
</tr>
<tr>
<td>xml/SAP-UserMgmt-CompliantUserProv-ConnectorConfig.xml</td>
<td>This file contains definitions of the connector components to configure the Compliant User Provisioning feature. See Section 2.3.13.1, “Importing the XML File for the Compliant User Provisioning Feature” for instructions on importing this file.</td>
</tr>
<tr>
<td>xml/SAP-UserMgmt-CUP-RequestApproval-ConnectorConfig.xml</td>
<td>This file contains definitions of the connector components for request-based provisioning when you configure the Compliant User Provisioning feature. See Section 2.3.13.2, “Enabling Request-Based Provisioning for the Compliant User Provisioning Feature” for instructions on importing this file.</td>
</tr>
<tr>
<td>Note: This XML file is specific to Oracle Identity Manager releases prior to 11.1.2.</td>
<td></td>
</tr>
</tbody>
</table>
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:
      \texttt{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 Build Date and Build Version values of the current release of the
   SAP User Management connector as follows:
   a. On the installation media for the connector, extract the contents of the
      \texttt{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:
   - If you are using Oracle Identity Manager release 9.1.x, then:
     a. Copy the \texttt{OIM_HOME/xellerate/JavaTasks/Common.jar} file to a
        temporary location.
     b. After you perform the procedure described in Section 2.2, "Installation"
        overwrite the new Common.jar file in the
        \texttt{OIM_HOME/xellerate/JavaTasks} directory with the Common.jar file that
        you backed up in the preceding step.
   - If you are using Oracle Identity Manager release 11.1.x, then run the Oracle
     Identity Manager Upload JARs utility to post the Common.jar file to the
     Oracle Identity Manager database. This utility is copied into the following
     location when you install Oracle Identity Manager:

     \texttt{For Microsoft Windows:}
     \texttt{OIM_HOME/server/bin/UploadJars.bat}

     \texttt{For UNIX:}
     \texttt{OIM_HOME/server/bin/UploadJars.sh}

\textbf{Caution:} If you do not perform this procedure, then your release 9.1.x connectors might not work.

\textbf{Note:} On Oracle Identity Manager release 11.1.x, use the Oracle Identity Manager Download JARs utility to download the
Common.jar file from the database, and then extract the contents of this file into a temporary directory.

See \textit{Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager} for instructions about using the Download JARs utility.

\textbf{Note:} Before you use this utility, verify that the WL_HOME
environment variable is set to the directory in which Oracle WebLogic Server is installed.
When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

**See Also:** *Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility

### 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 each connector operation. This target system account must be one of the following:

- If you are using a target system in which the SAP HRMS module is enabled, then the 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. Note that the P_ORIGIN authorization object is related to the SAP HRMS module. Therefore, you can assign a customized role with the P_ORIGIN authorization object only if the SAP HRMS module is enabled.

- If you are using a target system in which the SAP HRMS module is not enabled, then the target system account must be a user to whom you assign a customized role (for example, ZHR_ORG_UM) with the following authorization objects:
  - PLOG
  - Authorization objects that run BAPIs corresponding to each provisioning function.

For example, consider a provisioning function that adds a multivalued attribute (such as role) to a user. If you want the connector to perform this provisioning operation, then you must create a target system user account to which you assign a customized role with the PLOG authorization object and an authorization object that runs the BAPIs to create, modify, or display roles.

For the target system account that is to be created, the Roles tab of the Maintain User form is displayed in the following screenshot: 
For the target system account that is to be created, the Profiles tab of the Maintain User form is displayed in the following screenshot:
The following screenshot shows the authorization objects, PLOG and P_ORIGIN that are assigned to a customized role (ZHR_ORG_UM) when the SAP HRMS module is enabled in the target system:
The following screenshot shows the authorization object (PLOG) that is assigned to a customized role (ZHR_ORG_UM) when the SAP HRMS module is not enabled in the target system:

The following screenshot shows the authorization objects (that run BAPIs corresponding to the add multivalued attribute (for example, role) provisioning function) that are assigned to a customized role (ZBC_ROLES_UM) when the SAP HRMS module is not enabled in the target system:
There are no changes to the logon data, as shown in the following screenshot:
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. The Plan Version (PLVAR) object can be set according to your requirements.
The following screenshot displays details of the P_ORIGIN authorization object:
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 an Oracle Identity Manager cluster, 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 SAP JAVA Connector page by selecting Application Platform, Connectivity, Connectors, SAP Java Connector, and Tools & Services.
   b. 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.
   c. 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.
   
   In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

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 msvc.exe 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.
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 2.3.6, "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:

   ![Figure 2–1 Dialog Box Displayed on Running the SAP JCo Test](image)

   **Java Runtime**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Windows XP SP 3 for x86</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java VM</td>
<td>1.6.0_10 Sun Microsystems Inc.</td>
</tr>
<tr>
<td>Java Codepage</td>
<td>Cpt1252</td>
</tr>
<tr>
<td>Versions</td>
<td>3.0.0 (2008-04-16)</td>
</tr>
<tr>
<td>JCo middleware name</td>
<td>LocalEc</td>
</tr>
<tr>
<td>JCo middleware</td>
<td>2.1.0</td>
</tr>
<tr>
<td>JCo middleware name</td>
<td>21.0</td>
</tr>
<tr>
<td>Paths</td>
<td>C:\OIM\JCo\3rdParty\com.sap.com\jco3.jar</td>
</tr>
<tr>
<td>JCo Classpath</td>
<td>C:\OIM\JCo\3rdParty\com.sap.com\jco3.jar</td>
</tr>
</tbody>
</table>

**Note:**

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

- For Oracle Identity Manager release 9.1.0.x:
  
  OIM_HOME/xellerate/ConnectorDefaultDirectory

- For Oracle Identity Manager release 11.1.x:
  
  OIM_HOME/server/ConnectorDefaultDirectory

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

   - For Oracle Identity Manager release 9.1.0.x or 11.1.1:
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 Fusion Middleware System Administrator’s Guide for Oracle Identity Manager.

- For Oracle Identity Manager release 11.1.2:
  a. Log in to Oracle Identity System Administration by using the user account described in the "Creating the User Account for Installing Connectors" section Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager.
  b. In the left pane, under System Management, click Manage Connector.

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

- For Oracle Identity Manager release 9.1.0.x:
  Click Deployment Management, and then click Install Connector.

- For Oracle Identity Manager release 11.1.1:
  On the Welcome to Identity Manager Advanced Administration page, under the System Management section, click Install Connector.

- For Oracle Identity Manager release 11.1.2:
  In the Manage Connector page, click Install.

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:

For Oracle Identity Manager release 9.1.0.x:

OIM_HOME/xellerate/ConnectorDefaultDirectory

For Oracle Identity Manager release 11.1.x:

OIM_HOME/server/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 for Oracle Identity Manager release 9.1.0.x:
6. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

- Configuration of connector libraries
- Import of the connector XML files (by using the Deployment Manager)
- 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:
Postinstallation steps are divided across the following sections:

- Section 2.3.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
- Section 2.3.2, "Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later"

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 2.3.8, "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 cluster, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. 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 Oracle Identity Manager 11.1.2 or Later"
- Section 2.3.2, "Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later"
2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2 or later, you must create additional metadata such as a UI form and an application instance. In addition, you must run entitlement and catalog synchronization jobs. These procedures are described in the following sections:

- **Section 2.3.1.1, “Tagging Form Fields”**
- **Section 2.3.1.2, "Creating and Activating a Sandbox"**
- **Section 2.3.1.3, "Creating a New UI Form"**
- **Section 2.3.1.4, "Creating an Application Instance"**
- **Section 2.3.1.5, "Publishing a Sandbox"**
- **Section 2.3.1.6, "Harvesting Entitlements and Sync Catalog"**
- **Section 2.3.1.7, "Updating an Existing Application Instance with a New Form"**

### 2.3.1.1 Tagging Form Fields

You must add properties to certain form fields. To do so:

1. Log in to Oracle Identity Manager Design Console.
2. Open SAP UM Role Form (UD_SAPRL).
3. Create a new form version.
4. In the **Properties** tab, for the **Role Name** field, add Entitlement = true property.

5. Click **Make Version Active**.

6. Open SAP UM Profile Form (UD_SPUM_PRO).

7. Create a new form version.

8. In the **Properties** tab, for the **Profile Name** field, add Entitlement = true property.

9. Click **Make Version Active**.

10. Open SAP UM User Form (UD_SAP).

11. Create a new form version.

12. In the **Properties** tab, add the following properties:

   For the **IT Resource** field, add ITResource = true property.

   For the **User ID** field, add AccountName = true and AccountId = true properties.

13. Click **Make Version Active**.

### 2.3.1.2 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see the "Managing Sandboxes" section in the *Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager*.

1. On the upper navigation bar, click **Sandboxes**. The Manage Sandboxes page is displayed.

2. On the toolbar, click **Create Sandbox**. The Create Sandbox dialog box is displayed.

3. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.

4. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.

5. Click **Save and Close**. A message is displayed with the sandbox name and creation label.

6. Click **OK**. The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.

7. Select the sandbox that you created.

8. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.

9. On the toolbar, click **Activate Sandbox**.

   The sandbox is activated.

### 2.3.1.3 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see the "Managing Forms" chapter in the *Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager*.

1. In the left pane, under Configuration, click **Form Designer**.

2. Under Search Results, click **Create**.
3. Select the resource type for which you want to create the form, for example, *SAP UM*.

4. Enter a form name and click **Create**.

### 2.3.1.4 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see the "Managing Application Instances" chapter in the *Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager*.

1. In the System Administration page, under Configuration in the left pane, click **Application Instances**.

2. Under Search Results, click **Create**.

3. Enter appropriate values for the fields displayed on the Attributes form and click **Save**.

4. In the Form drop-down list, select the newly created form and click **Apply**.

5. Publish the application instance for a particular organization.

### 2.3.1.5 Publishing a Sandbox

To publish the sandbox that you created in Section 2.3.1.2, "Creating and Activating a Sandbox":

1. Close all the open tabs and pages.

2. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Section 2.3.1.2, "Creating and Activating a Sandbox."

3. On the toolbar, click **Publish Sandbox**. A message is displayed asking for confirmation.

4. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

### 2.3.1.6 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Section 3.2, "Scheduled Task for Lookup Field Synchronization."

2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager* for more information about this scheduled job.

3. Run the Catalog Synchronization Job scheduled job. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager* for more information about this scheduled job.

### 2.3.1.7 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in Section 2.3.1.2, "Creating and Activating a Sandbox."
2. Create a new UI form for the resource as described in Section 2.3.1, "Creating a New UI Form."

3. Open the existing application instance.

4. In the Form field, select the new UI form that you created.

5. Save the application instance.

6. Publish the sandbox as described in Section 2.3.1.5, "Publishing a Sandbox."

2.3.2 Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later

In Oracle Identity Manager release 11.1.2.1.0 or later, you can reset password for an account after logging in as the user by navigating to My Access, Accounts tab.

The Reset Password option is enabled for only those accounts that follow the UD_FORMNAME_PASSWORD naming convention for the password field. Otherwise, this option would be disabled as shown in the following sample screenshot:

To enable the Reset Password option in Oracle Identity Manager release 11.1.2.1.0 or later:

1. Log in to Oracle Identity System Design Console.

2. Under Development Tools, click **Form Designer**.

3. Enter UD_SAP in the Table Name field and click the **Query for records** button.

4. Click **Create New Version**.

5. In the Create a New Version dialog box, specify the version name in the Label field, save the changes, and then close the dialog box.

6. From the **Current Version** list, select the newly created version.

7. Click the **Properties** tab.

8. Select the password field, and click **Add Property**.

9. From the Property Name list, select **AccountPassword**.

10. In the Property Value field, enter true.

11. Click **Save**.

The password field is tagged with the **AccountPassword = true** property as shown in the following screenshot:
12. Click Make Version Active.

13. Update the application instance with the new form as described in Section 2.3.1.7, "Updating an Existing Application Instance with a New Form."

2.3.3 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>
<thead>
<tr>
<th>Service</th>
<th>Port Number Format</th>
<th>Default Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dispatcher</td>
<td>32SYSTEM_NUMBER</td>
<td>3200</td>
</tr>
<tr>
<td>Gateway (for non-SNC communication)</td>
<td>33SYSTEM_NUMBER</td>
<td>3300</td>
</tr>
<tr>
<td>Gateway (for SNC communication)</td>
<td>48SYSTEM_NUMBER</td>
<td>4800</td>
</tr>
<tr>
<td>Message server</td>
<td>36SYSTEM_NUMBER</td>
<td>3600</td>
</tr>
</tbody>
</table>

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

2.3.4 Configuring the Target System

This section describes the procedures involved in configuring the target system to enable propagation user password changes from the SAP CUA parent system to its child systems. You may need the assistance of the SAP Basis administrator to perform some of these procedures.

Configuring the target system involves the following tasks:

- Section 2.3.4.1, "Gathering Required Information"
- Section 2.3.4.2, "Creating an Entry in the BAPIF4T Table"
- Section 2.3.4.3, "Importing the Request"
2.3.4.1 Gathering Required Information

The following information is required to configure the target system:

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

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

2.3.4.2 Creating an Entry in the BAPIF4T Table

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

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

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

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

2.3.4.3 Importing the Request

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

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Object Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>ZXLC</td>
</tr>
<tr>
<td>Function Group</td>
<td>ZXLCGRP</td>
</tr>
<tr>
<td></td>
<td>ZXLCHLVALUES</td>
</tr>
<tr>
<td></td>
<td>ZXLCPRF</td>
</tr>
<tr>
<td></td>
<td>ZXLCRL</td>
</tr>
<tr>
<td></td>
<td>ZXLCUSR</td>
</tr>
<tr>
<td>Message class</td>
<td>ZXLCBAPI</td>
</tr>
</tbody>
</table>
The xlsapcar.sar file contains the definitions for these objects. When you import the request represented by the contents of the xlsapcar.sar file, these objects are automatically created in SAP. This procedure does not result in any change in the existing configuration of SAP.

Importing the request into SAP involves the following steps:

- **Section 2.3.4.3.1, "Extracting the Request Files"
- **Section 2.3.4.3.2, "Performing the Request Import Operation"

**Note:** You must import the request represented by the contents of the xlsapcar.sar file to the parent and the child systems.

### 2.3.4.3.1 Extracting the Request Files

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

1. Download the SAPCAR utility from SAP website.

   The two files, Data file and Cofile, that constitute the request are compressed in the xlsapcar.sar. You can use the SAPCAR utility to extract these files.

2. Copy the xlsapcar.sar file into the directory in which you downloaded the SAPCAR utility.
The xlsapcar.sar file is in the BAPI directory inside the installation media directory.

3. In a command window, change to the directory in which you store the SAPCAR utility and the xlsapcar.sar file.

4. Enter the following command to extract the Data file and Cofile components of the request:

    sapcar -xvf xlsapcar.sar

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

7900863.147 (Cofile)
R900863.147 (Data file)

2.3.4.3.2 Performing the Request Import Operation

To perform the request import operation:

1. Copy the Data file and Cofile to the required locations on the SAP server.
2. Import the request into SAP.
3. Check the log file to determine whether or not the import was successful.

To display the log file:

a. Run the STMS transaction.

   The list of transport requests is displayed.

b. Select the transport request number corresponding to the request that you import.

   The transport request number is the same as the numeric part of the Cofile or Data file names. In Step 3 of the preceding procedure, for the sample Cofile (K900863.147) and Data file (R900863.147), the transport request number is 900863.

c. Click the log file icon.

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

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

2.3.5 Setting Up the Configuration Lookup Definition in Oracle Identity Manager

Note: In an Oracle Identity Manager cluster, 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 2.3.5.1, "Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts"
- Section 2.3.5.2, "Configuring Password Changes for Newly Created Accounts"
- Section 2.3.5.3, "Setting Values in the Lookup.SAP.UM.Configuration Lookup Definition"
- Section 2.3.13.7, "Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition"

2.3.5.1 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.
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.
2.3.5.2 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.

2.3.5.3 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.

See Also: See one of the following guides for information about removing process tasks:

- For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User’s Guide for Oracle Identity Manager
- For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager
### Table 2–3 Entries in the Lookup_SAP.UM.Configuration Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Password</td>
<td>See Section 2.3.5.2, &quot;Configuring Password Changes for Newly Created Accounts&quot; for information about the value to be specified for this entry. Default value: yes</td>
</tr>
<tr>
<td>Check Box Lookup for Prov</td>
<td>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, &quot;Adding New Standard Attributes for Provisioning.&quot; Value: Lookup.SAP.UM.ProvCheckBoxMapping</td>
</tr>
<tr>
<td>Check Box Lookup for Recon</td>
<td>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, &quot;Adding New Attributes for Reconciliation&quot;. Value: Lookup.SAP.UM.ReconCheckBoxMapping</td>
</tr>
<tr>
<td>Constants Lookup</td>
<td>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</td>
</tr>
<tr>
<td>Custom Attribute Mapping Lookup</td>
<td>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</td>
</tr>
<tr>
<td>Custom Child Attribute Mapping Lookup</td>
<td>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</td>
</tr>
<tr>
<td>CUP Configuration Lookup</td>
<td>This entry holds the name of the lookup definition that stores configuration values for the Compliant User Provisioning feature. Value: Lookup.SAP.CUP.Configuration</td>
</tr>
<tr>
<td>CUP Mode Enabled</td>
<td>Enter yes if you want to enable the Compliant User Provisioning feature. Otherwise, enter no.</td>
</tr>
<tr>
<td>Exclusion List Lookup</td>
<td>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 2.3.10, &quot;Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition&quot; for more information. Value: Lookup.SAP.UM.ExclusionList</td>
</tr>
<tr>
<td>Is CUA Enabled</td>
<td>Enter yes if the target system is SAP CUA. Enter no if the target system is SAP R/3. Default value: no</td>
</tr>
</tbody>
</table>
### Table 2–3  (Cont.) Entries in the Lookup.SAP.UM.Configuration Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 2.3.16.4](#), “Mapping New Connection Properties” for more information about this lookup definition.  
  Value: Lookup.SAP.UM.ITResourceMapping                                                                                                                                             |
| Overwrite Link                   | See [Section 2.3.5.1](#), “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 2.3.13.4](#), “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 1.8.2](#), “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 1.8.2](#), “User Attributes for Provisioning” for more information.  
  Value: Lookup.SAP.UM.ProvChildAttrMap                                                                                                                                             |
| Reconcile future dated roles     | Enter `Yes` if you want to reconcile future-dated roles. Otherwise, enter `No`.                                                                                                                                       |
| Reconcile past dated roles       | Enter `Yes` if you want to reconcile past-dated roles. Otherwise, enter `No`.                                                                                                                                       |
| SOD Configuration lookup         | This entry holds the name of the lookup definition that is used during SOD.  
  Value: Lookup.SAP.UM.SoDConfiguration                                                                                                                                          |
| Support HRMS 0105 Infotype Linking| See [Section 2.3.5.1](#), “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                                                                                                                                          |
Table 2–3 (Cont.) Entries in the Lookup.SAP.UM.Configuration Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Transformation For Recon</td>
<td>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</td>
</tr>
<tr>
<td>Use Transformation For Lookup Recon</td>
<td>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</td>
</tr>
<tr>
<td>Use Validation For Prov</td>
<td>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</td>
</tr>
<tr>
<td>Use Validation For Recon</td>
<td>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</td>
</tr>
<tr>
<td>Validate Personnel Number before Linking</td>
<td>See Section 2.3.5.1, ”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</td>
</tr>
<tr>
<td>Validation Lookup For Prov</td>
<td>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</td>
</tr>
<tr>
<td>Validation Lookup For Recon</td>
<td>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 reconciliation. See Section 4.9, ”Configuring Validation of Data During Reconciliation and Provisioning” for more information. Value: Lookup.SAP.UM.ReconValidation</td>
</tr>
<tr>
<td>Is Password Propagate To Child System</td>
<td>In the Decode column, enter Yes if you want the connector to propagate user password changes from the SAP CUA parent system to its child systems. Otherwise, enter No. Value: No</td>
</tr>
</tbody>
</table>

2.3.6 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.
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.

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

- Section 2.3.6.1, "Enabling Request-Based Provisioning in Oracle Identity Manager Release 9.1.0.x"
- Section 2.3.6.2, "Enabling Request-Based Provisioning in Oracle Identity Manager Release 11.1.1"

### 2.3.6.1 Enabling Request-Based Provisioning in Oracle Identity Manager Release 9.1.0.x

When you install the connector on Oracle Identity Manager release 9.1.0.x, request-based provisioning of accounts is automatically enabled. Perform the procedure described in this section only if you want to enable request-based provisioning of entitlements such as roles.

**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:**

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**.

Note: Perform the procedure described in this section only if you are using Oracle Identity Manager release prior to 11.1.2. Do not enable request-based provisioning if you want to use the direct provisioning feature of the connector. See Oracle Fusion Middleware User’s Guide for Oracle Identity Manager for information about direct provisioning.

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

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

12. Click **View Selections**.

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

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

To suppress the Standard Approval process definition:

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

1. On the Design Console, expand Process Management and double-click Process
   Definition.
2. Search for and open the Standard Approval process definition.
3. On the Tasks tab, double-click the Approve task.
4. On the Integration tab of the Editing Task dialog box, click **Add**.

5. In the Handler Selection dialog box:
   a. Select **System**.
   b. Select the **tcCompleteTask** handler.
   c. Click the Save icon, and then close the dialog box.

6. In the Editing Task dialog box, click the Save icon and close the dialog box.

7. Click the Save icon to save changes made to the process definition.
2.3.6.2 Enabling Request-Based Provisioning in Oracle Identity Manager Release 11.1.1

Note: Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 and you want to configure request-based provisioning.

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

To enable request-based provisioning, perform the following procedures:

- Section 2.3.6.2.1, "Copying Predefined Request Datasets"
- Section 2.3.6.2.2, "Importing Request Datasets into MDS"
- Section 2.3.6.2.3, "Enabling the Auto Save Form Feature"
- Section 2.3.6.2.4, "Running the PurgeCache Utility"

2.3.6.2.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation.

In an SAP environment, you can set up SAP R/3, SAP CUA, or Compliant User Provisioning (CUP) as the front end for provisioning requests. You can switch from an SAP R/3 target to a SAP CUP target. See Section 2.3.6.2.2, "Importing Request Datasets into MDS" for more information.

The following is the list of predefined request datasets available in the DataSets directory on the installation media:

For SAP R/3 or SAP CUA:

- ProvisionResourceSAP UM Resource Object.xml
- ModifyResourceSAP UM Resource Object.xml

For SAP CUP:

- SAP-UserMgmt-CUP-ModifyResourceSAP UM Resource Object.xml
- SAP-UserMgmt-CUP-ProvisionResourceSAP UM Resource Object.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/RESOURCE_NAME

For example:

E:\MyDatasets\custom\connector\SAPUM
The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

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

### 2.3.6.2.2 Importing Request Datasets into MDS

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

**Note:** You must import the appropriate request datasets depending on your target. For example, for SAP R/3 or SAP CUA target import the following request datasets:

- ProvisionResourceSAP UM Resource Object.xml
- ModifyResourceSAP UM Resource Object.xml

To import a request dataset definition into the MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager for detailed information about setting up the environment for MDS utilities.

**Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/RESOURCE_NAME directory. For example, while performing the procedure in Section 2.3.6.2.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\SAPUM directory, then set the value of the metada_from_loc property to E:\MyDatasets.

2. In a command window, change to the OIM_HOME/server/bin directory.

3. Run one of the following commands:

   - On Microsoft Windows
     
     `weblogicImportMetadata.bat`

   - On UNIX
     
     `weblogicImportMetadata.sh`

4. When prompted, enter values for the following:
■ Please enter your username [weblogic]
Enter the username used to log in to the Oracle WebLogic Server
Sample value: WL_User
■ Please enter your password [weblogic]
Enter the password used to log in to the Oracle WebLogic Server
■ Please enter your server URL [t3://localhost:7001]
Enter the URL of the application server in the following format:
t3://HOST_NAME_IP_ADDRESS:PORT
In this format, replace:
– HOST_NAME_IP_ADDRESS with the host name or IP address of the computer on which Oracle Identity Manager is installed.
– PORT with the port on which Oracle Identity Manager is listening.
The request dataset is imported into the MDS.

2.3.6.2.3 Enabling the Auto Save Form Feature
To enable the Auto Save Form feature:
1. Log in to the Design Console.
2. Expand Process Management, and then double-click Process Definition.
3. Search for and open the SAP UM Process Form process definition.
4. Select the Auto Save Form check box.
5. Click the Save icon.

2.3.6.2.4 Running the PurgeCache Utility
Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.8, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.
The procedure to enable enabling request-based provisioning ends with this step.

2.3.7 Changing to the Required Input Locale

Note: In an Oracle Identity Manager cluster, 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.
2.3.8 Clearing Content Related to Connector Resource Bundles from the Server Cache

**Note:** In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the `OIM_HOME/xellerate/connectorResources` directory for Oracle Identity Manager release 9.1.0.x and Oracle Identity Manager database for Oracle Identity Manager release 11.1.x. Whenever you add a new resource bundle to the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.x, then switch to the `OIM_HOME/xellerate/bin` directory.
   - If you are using Oracle Identity Manager release 11.1.x, then switch to the `OIM_HOME/server/bin` directory.

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

For Oracle Identity Manager release 9.1.0.x:

`OIM_HOME/xellerate/bin/SCRIPT_FILE_NAME`

For Oracle Identity Manager release 11.1.x:

`OIM_HOME/server/bin/SCRIPT_FILE_NAME`

2. Enter one of the following commands:

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

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

```
PurgeCache.bat MetaData
PurgeCache.sh MetaData
```

- For Oracle Identity Manager release 9.1.0.x:
  - On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`
  - On UNIX: `PurgeCache.sh ConnectorResourceBundle`
In this command, ConnectorResourceBundle is one of the content categories that you can delete from the server cache. See the following file for information about the other content categories:

OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.x:

On Microsoft Windows: PurgeCache.bat All

On UNIX: PurgeCache.sh All

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

t3:///OIM_HOST_NAME:OIM_PORT_NUMBER

In this format:

- Replace OIM_HOST_NAME with the host name or IP address of the Oracle Identity Manager host computer.
- Replace OIM_PORT_NUMBER with the port on which Oracle Identity Manager is listening.

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

2.3.9 Enabling Logging

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

- Section 2.3.9.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"
- Section 2.3.9.2, "Enabling Logging on Oracle Identity Manager Release 11.1.x"

2.3.9.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.x

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 might 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 written to the following file:
WEBLOGIC_HOME/user_projects/domains/DOMAIN_NAME/SERVER_NAME/SERVER_NAME.log

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:
WEBSHERE_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:

   ```xml
   <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:

   ```xml
   <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`

### 2.3.9.2 Enabling Logging on Oracle Identity Manager Release 11.1.x

---

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

---

Oracle Identity Manager release 11.1.x uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- `SEVERE.intValue()+100`
This level enables logging of information about fatal errors.

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

- **WARNING**
  This level enables logging of information about potentially harmful situations.

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

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

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

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

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

<table>
<thead>
<tr>
<th>Java Level</th>
<th>ODL Message Type:Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEVERE.intValue()+100</td>
<td>INCIDENT_ERROR:1</td>
</tr>
<tr>
<td>SEVERE</td>
<td>ERROR:1</td>
</tr>
<tr>
<td>WARNING</td>
<td>WARNING:1</td>
</tr>
<tr>
<td>INFO</td>
<td>NOTIFICATION:1</td>
</tr>
<tr>
<td>CONFIG</td>
<td>NOTIFICATION:16</td>
</tr>
<tr>
<td>FINE</td>
<td>TRACE:1</td>
</tr>
<tr>
<td>FINER</td>
<td>TRACE:16</td>
</tr>
<tr>
<td>FINEST</td>
<td>TRACE:32</td>
</tr>
</tbody>
</table>

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

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

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

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:
   a. Add the following blocks in the file:

      ```xml
      <log_handler name='sap-um-handler' level='[LOG_LEVEL]' class='oracle.core.ojdl.logging.ODLHandlerFactory'>
        <property name='logreader:' value='off'/>
        <property name='path' value='[FILE_NAME]' />
        <property name='format' value='ODL-Text' />
        <property name='useThreadName' value='true' />
        <property name='locale' value='en' />
      </log_handler>
      ```
Postinstallation

2. Save and close the file.

3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:
   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:
   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

   Replace `FILENAME` with the location and name of the file to which you want to redirect the output.

4. Restart the application server.
2.3.10 Setting Up the Lookup.SAP.UM.ExclusionList Lookup Definition

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.

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

2.3.11 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:
6. Save and close the lookup definition.

2.3.12 Copying the SAPCUP.jar File for User Provisioning

Note: Perform the procedure described in this section only if you are using IBM WebSphere Application Server.

You must copy the SAPCUP.jar file to avoid errors while performing regular provisioning operations. Copy the deploy/SAPCUP.jar file from the installation media to the WEBSHERE_HOME/lib directory.

If you are using Oracle Identity Manager release 11.1.x, then you must also copy the SAPCUP.jar file to the OIM_HOME/server/apps/oim.ear/APP-INF/lib directory.

2.3.13 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 1.4.5, "Guidelines on Using a Deployment Configuration."

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

- Section 2.3.13.1, "Importing the XML File for the Compliant User Provisioning Feature"
- Section 2.3.13.2, "Enabling Request-Based Provisioning for the Compliant User Provisioning Feature"
- Section 2.3.13.3, "Specifying Values for the GRC-ITRes IT Resource"
- Section 2.3.13.4, "Specifying Values in the Lookup.SAP.UM.Configuration Lookup Definition"
- Section 2.3.13.5, "Setting Up the Link with the Web Services for SAP Compliant User Provisioning"
2.3.13.1 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 an Oracle Identity Manager cluster, 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:
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](image)

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

12. Click View Selections.

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

14. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, “Creating a New UI Form” and Section 2.3.1.7, “Updating an Existing Application Instance with a New Form” for the procedures.

2.3.13.2 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:** Perform this procedure only if you are using Oracle Identity Manager release prior to 11.1.2. 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:

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

12. Click View Selections.

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

2. Search for and open the Standard Approval process definition.
3. On the Tasks tab, double-click the Approve task.
4. On the Integration tab of the Editing Task dialog box, click **Add**.

5. In the Handler Selection dialog box:
   a. Select **System**.
   b. Select the **tcCompleteTask** handler.
   c. Click the Save icon, and then close the dialog box.

6. In the Editing Task dialog box, click the Save icon and close the dialog box.

7. Click the Save icon to save changes made to the process definition.
2.3.13.3 Specifying Values for the GRC-ITRes IT Resource

The GRC-ITRes 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. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.x or 11.1.1:
     Log in to the Administrative and User Console
   - For Oracle Identity Manager release 11.1.2:
     Log in to Oracle Identity System Administration

2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.x, expand Resource Management, and then click Manage IT Resource.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Oracle Identity Manager Self Service page, click Advanced.
     b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click Manage IT Resource.
   - If you are using Oracle Identity Manager release 11.1.2, then:
     a. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the “Managing Sandboxes” section of Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager.
     b. In the left pane under Configuration, click IT Resource.

3. In the IT Resource Name field on the Manage IT Resource page, enter GRC-ITRes and then click Search.

4. Click the edit icon for the IT resource.

5. From the list at the top of the page, select Details and Parameters.

6. Specify values for the parameters of the IT resource. Table 2–10 describes each parameter.

\[
\textbf{Note:} \quad \text{Entries in this table are sorted in alphabetical order of parameter names.}
\]

Table 2–10 lists the parameters of the GRC-ITRes IT resource.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbuser</td>
<td>You need not enter a value for this parameter.</td>
</tr>
<tr>
<td>dbpassword</td>
<td>You need not enter a value for this parameter.</td>
</tr>
<tr>
<td>jdbcURL</td>
<td>Enter the JDBC URL for connecting to the database used by SAP GRC.</td>
</tr>
<tr>
<td>password</td>
<td>Enter the password of the account created on SAP GRC for API calls.</td>
</tr>
</tbody>
</table>
Table 2–5 (Cont.) Parameters of the GRC-ITRes IT Resource

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Enter the number of the port at which SAP GRC is listening. Sample value: 8090</td>
</tr>
<tr>
<td>server</td>
<td>Enter the IP address of the host computer on which SAP GRC is running. Sample value: 10.231.231.231</td>
</tr>
<tr>
<td>Source Datastore Name</td>
<td>You need not enter a value for this parameter.</td>
</tr>
<tr>
<td>sslEnable</td>
<td>Enter true if SAP GRC accepts only HTTPS communication requests. Otherwise, enter false. Sample value: false</td>
</tr>
<tr>
<td>username</td>
<td>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</td>
</tr>
</tbody>
</table>

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

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

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

- **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.

See Also: Section 2.3.5.3, "Setting Values in the Lookup.SAP.UM.Configuration Lookup Definition" for information about setting up this lookup definition.

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

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

1. Copy the `deploy/SAPCUP.jar` file from the installation media to one of the following directories:

   - For IBM WebSphere Application Server: `WEBSHHERE_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

If you are using Oracle WebLogic Server, then you must also copy the SAPCUP.jar file to the WEBLOGIC_HOME/wlsserver_10.3/server/lib directory.

If you are using Oracle Identity Manager release 11.1.x, then you must also copy the SAPCUP.jar file to the OIM_HOME/server/apps/oim.ear/APP-INF/lib directory.

2. 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/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.

---

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

2.3.13.6 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 2.3.13.6.1, "Creating Request Types"
- Section 2.3.13.6.2, "Creating Workflows"

2.3.13.6.1 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:

![Create Request Type](image)

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.
5. Click Save.

2.3.13.6.2 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 Type 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:
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 1.4.6, “Considerations to Be Addressed When You Enable Compliant User Provisioning” for information about this guideline.

The following screenshot shows this page:
■ 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:

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:

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.
Postinstallation

Deploying the Connector

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:

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:
2.3.13.7 Setting Values in the Lookup.SAP.CUP.Configuration Lookup Definition

Table 2–6 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>
<thead>
<tr>
<th>Code Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Enter the system name of the SAP R/3 or SAP CUA installation.</td>
</tr>
<tr>
<td></td>
<td>Sample value: E60</td>
</tr>
<tr>
<td>Assign Role</td>
<td>Enter the name of the request type that you create for Modify User provisioning operations.</td>
</tr>
<tr>
<td></td>
<td>See Section 2.3.13.6.1, &quot;Creating Request Types&quot; for more information.</td>
</tr>
<tr>
<td></td>
<td>Sample value: MODIFY_USER</td>
</tr>
<tr>
<td>Child Attribute Lookup</td>
<td>This entry holds the name of the lookup definition that stores child form attribute mappings for the Compliant User Provisioning feature.</td>
</tr>
<tr>
<td></td>
<td>Value: Lookup.SAP.CUP.ProvisionRoleAttrMap</td>
</tr>
<tr>
<td>Constants Lookup</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Value: Lookup.SAP.CUP.Constants</td>
</tr>
<tr>
<td>Create User</td>
<td>Enter the name of the request type that you create for Create User provisioning operations.</td>
</tr>
<tr>
<td></td>
<td>See Section 2.3.13.6.1, &quot;Creating Request Types&quot; for more information.</td>
</tr>
<tr>
<td></td>
<td>Sample value: CREATE_USER</td>
</tr>
</tbody>
</table>
**Table 2–6  (Cont.) Entries in the Lookup.SAP.CUP.Configuration Lookup Definition**

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Description</th>
</tr>
</thead>
</table>
| Delete User               | Enter the name of the request type that you create for Delete User provisioning operations.  
  See Section 2.3.13.6.1, "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 GRC IT resource.  
  Default value: GRC-ITRes |
| Lock User                 | Enter the name of the request type that you create for Modify User provisioning operations.  
  See Section 2.3.13.6.1, "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 2.3.13.6.1, "Creating Request Types" for more information.  
  Sample value: MODIFY_USER |
This section discusses the following procedures:

- Section 2.3.14.1, "Configuring SAP GRC to Act As the SoD Engine"
- Section 2.3.14.2, "Specifying Values for SoD-Related Entries in the Lookup.SAP.CUP.SoDConfiguration Lookup Definition"
- Section 2.3.14.3, "Modifying the SoD-Related Lookup Definitions"
- Section 2.3.14.4, "Specifying Values for the GRC-ITRes IT Resource"
- Section 2.3.14.5, "Verifying Entries Created in the Lookup.SAP.CUP.System Lookup Definition"
- Section 2.3.14.6, "Specifying a Value for the TopologyName IT Resource Parameter"
- Section 2.3.14.7, "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.

### 2.3.14.1 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.

---

**Table 2–6 (Cont.) Entries in the Lookup.SAP.CUP.Configuration Lookup Definition**

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Attribute Lookup</td>
<td>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</td>
</tr>
<tr>
<td>Priority</td>
<td>Enter the priority level at which SAP GRC Compliant User Provisioning must process requests sent from Oracle Identity Manager:</td>
</tr>
<tr>
<td></td>
<td>■ Low</td>
</tr>
<tr>
<td></td>
<td>■ Medium</td>
</tr>
<tr>
<td></td>
<td>■ High</td>
</tr>
<tr>
<td></td>
<td>■ Critical</td>
</tr>
<tr>
<td>Unlock User</td>
<td>Enter the name of the request type that you create for Modify User provisioning operations. See Section 2.3.13.6.1, &quot;Creating Request Types&quot; for more information. Sample value: UNLOCK_USER</td>
</tr>
</tbody>
</table>
If you are using Oracle Identity Manager release 11.1.x, then see the "Configuring SAP GRC" section in the "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for information about this procedure.

2.3.14.2 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 2–7 lists the entries in this lookup definition.

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>entitlementRiskAnalysisWS</td>
<td>oracle.iam.grc.sod.scomp.impl.grcsap.util.webservice.sap.ac53.VirsaCCRiskAnalysis</td>
</tr>
<tr>
<td>GRC version</td>
<td>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</td>
</tr>
<tr>
<td>is CUA Enabled</td>
<td>Enter yes if the target system is SAP CUA. Enter no if the target system is SAP R/3. Default value: no</td>
</tr>
<tr>
<td>Profile attribute name</td>
<td>USERPROFILE</td>
</tr>
<tr>
<td>ProfileAttributeLabel</td>
<td>Profile Name</td>
</tr>
<tr>
<td>Profile form names</td>
<td>UD_SPUMPC_P;UD_SPUM_PRO</td>
</tr>
<tr>
<td>Profile name</td>
<td>USERPROFILE</td>
</tr>
<tr>
<td>Profile System Name</td>
<td>SYSTEMNAME</td>
</tr>
<tr>
<td>Risk Level</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>■ 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.</td>
</tr>
<tr>
<td></td>
<td>■ 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.</td>
</tr>
<tr>
<td></td>
<td>■ 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.</td>
</tr>
<tr>
<td></td>
<td>■ 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</td>
</tr>
<tr>
<td>Role attribute name</td>
<td>USERROLE</td>
</tr>
<tr>
<td>RoleAttributeLabel</td>
<td>Role Name</td>
</tr>
<tr>
<td>Role form names</td>
<td>UD_SPUMRC_P;UD_SAPRL</td>
</tr>
<tr>
<td>Role name</td>
<td>USERROLE</td>
</tr>
</tbody>
</table>
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.

### 2.3.14.3 Modifying the SoD-Related Lookup Definitions

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

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

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD_SPUMPC_P_SYSTEMNAME</td>
<td>UD_SPUM_PRO_SYSTEMNAME</td>
</tr>
</tbody>
</table>

---

Oracle Identity Manager Connector Guide for SAP User Management
Table 2–9 lists entries in the Lookup.SAP.UM.RoleChildformMappings lookup definition.

### Table 2–9 Entries in the Lookup.SAP.UM.RoleChildformMappings Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD_SPUMPC_P_USERPROFILE</td>
<td>UD_SPUM_PRO_USERPROFILE</td>
</tr>
<tr>
<td>UD_SPUMRC_P_SYSTEMNAME</td>
<td>UD_SAPRL_SYSTEMNAME</td>
</tr>
<tr>
<td>UD_SPUMRC_P_USERROLE</td>
<td>UD_SAPRL_USERROLE</td>
</tr>
<tr>
<td>UD_SPUMRC_P_VALID_FROM</td>
<td>UD_SAPRL_STARTDT,DATE</td>
</tr>
<tr>
<td>UD_SPUMRC_P_VALID_TO</td>
<td>UD_SAPRL_ENDDT,DATE</td>
</tr>
</tbody>
</table>

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

#### 2.3.14.4 Specifying Values for the GRC-ITRes IT Resource

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

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.x or 11.1.1: Log in to the Administrative and User Console
   - For Oracle Identity Manager release 11.1.2: Log in to Oracle Identity System Administration

2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.x, expand **Resource Management**, and then click **Manage IT Resource**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced**.
     b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the **Configuration** region, click **Manage IT Resource**.
   - If you are using Oracle Identity Manager release 11.1.2, then:
     a. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager.
b. In the left pane under Configuration, click **IT Resource**.

3. In the IT Resource Name field on the Manage IT Resource page, enter **GRC-ITRes** and then click **Search**.

4. Click the edit icon for the IT resource.

5. From the list at the top of the page, select **Details and Parameters**.

6. Specify values for the parameters of the IT resource. **Table 2–10** describes each parameter.

<table>
<thead>
<tr>
<th><strong>Table 2–10 Parameters of the GRC-ITRes IT Resource</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Configuration lookup</td>
</tr>
<tr>
<td>dbuser</td>
</tr>
<tr>
<td>dbpassword</td>
</tr>
<tr>
<td>jdbcURL</td>
</tr>
<tr>
<td>password</td>
</tr>
<tr>
<td>port</td>
</tr>
<tr>
<td>server</td>
</tr>
<tr>
<td>Source Datastore Name</td>
</tr>
<tr>
<td>sslEnable</td>
</tr>
<tr>
<td>username</td>
</tr>
</tbody>
</table>

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

**2.3.14.5 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.

### 2.3.14.6 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

For Oracle Identity Manager release 9.1.0.x:

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.

For Oracle Identity Manager release 11.1.x:

Enter `sodgrc` as the value of the TopologyName parameter.

See one of the following for more information about this element:

- For Oracle Identity Manager release 9.1.0.x, the "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in Oracle Identity Manager Tools Reference for Release 9.1.0.2.
- For Oracle Identity Manager release 11.1.x, the "Configuring SoD Validation" chapter in Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager.

See Section 2.3.16, "Configuring the IT Resource" for information about specifying values for parameters of the IT resource.

### 2.3.14.7 Disabling and Enabling SoD

This section describes the procedures to disable and enable SoD.

- Section 2.3.14.7.1, "Disabling and Enabling SoD on Oracle Identity Manager Release 9.1.0.x"
- Section 2.3.14.7.2, "Disabling and Enabling SoD on Oracle Identity Manager Release 11.1.x"

#### 2.3.14.7.1 Disabling and Enabling SoD on Oracle Identity Manager Release 9.1.0.x

The following sections describe the procedure to disable and enable SoD on Oracle Identity Manager on release 9.1.0.x:

- Disabling SoD on Oracle Identity Manager Release 9.1.0.x
- Enabling SoD on Oracle Identity Manager Release 9.1.0.x

**Disabling SoD on Oracle Identity Manager Release 9.1.0.x**

To disable SoD:

---

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

---

1. Log in to the Design Console.
2. Set the `XL.SoDCheckRequired` system property to `FALSE` as follows:
   a. Expand **Administration**, and double-click **System Configuration**.
   b. Search for and open the `XL.SoDCheckRequired` system property.
   c. Set the value of the system property to `FALSE`.
   d. Click the Save icon.

3. Disable the Holder and SODChecker process tasks as follows:
   a. Expand **Process Management**, and double-click **Process Definition**.
   b. Search for and open the SAP 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.

**Note:** You need not change the values of the `XL.SIL.Home.Dir` and Triggers Synchronous SoD checks offline system properties.
e. In the Handler Selection dialog box:
   Select System.
   Select the tcCompleteTask handler.

   ![Handler Selection dialog box](image)

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

f. In the Editing Task dialog box, click the Save icon and close the dialog box.

g. On the Tasks tab, double-click SODChecker.

h. On the Integration tab of the Editing Task dialog box, click Remove and then click the save icon.

i. Click Add.

j. In the Handler Selection dialog box:
Select **System**.

Select the **tcCompleteTask handler**.

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

**k.** Click the Save icon in the Editing Task dialog box, and then close the dialog box.

**l.** Click the Save icon to save the changes made to the process definition.

4. If you are going to perform the procedure described in Section 2.3.6, "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:

   ![Editing Task Approval](image)

   **e.** Save the changes to the process definition.

5. Restart Oracle Identity Manager.

**Enabling SoD on Oracle Identity Manager Release 9.1.0.x**

To enable SoD:

---

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

---

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **System Configuration**.

3. Set the XL.SoDCheckRequired system property to **TRUE** as follows:
   a. Search for and open the XL.SoDCheckRequired system property.
      b. Set the value of the system property to **TRUE**.
      c. Click the Save icon.

4. Search for and open the XL.SIL.Home.Dir system property.

5. Verify that the value of this system property is set to the full path and name of the **SIL_HOME** directory.

6. Enable the Holder and SODChecker process tasks as follows:
   a. Expand **Process Management** and double-click **Process Definition**.
   b. Search for and open the SAP 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**.
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 2.3.6, “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:
e. Save the changes to the process definition.

8. Restart Oracle Identity Manager.

2.3.14.7.2 Disabling and Enabling SoD on Oracle Identity Manager Release 11.1.x

This section describes the procedure to disable and enable SoD on Oracle Identity Manager release 11.1.x.

- Disabling SoD on Oracle Identity Manager Release 11.1.x
- Enabling SoD on Oracle Identity Manager Release 11.1.x

Disabling SoD on Oracle Identity Manager Release 11.1.x

To disable SoD:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Oracle Identity Manager Self Service page, click Advanced.
     c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click System Configuration.
   - For Oracle Identity Manager release 11.1.2:
     a. Log in to Oracle Identity System Administration.
     b. In the left pane, under System Management, click System Configuration.

2. In the Search System Configuration box, enter XL.SoDCheckRequired and then click Search.
   A list that matches your search criteria is displayed in the search results table.

3. Click the XL.SoDCheckRequired property name.
System properties for SoD are displayed on the right pane.

4. In the Value box, enter `FALSE` to disable SoD.
5. Click **Save**.
6. Restart Oracle Identity Manager.

**Enabling SoD on Oracle Identity Manager Release 11.1.x**

To enable SoD:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced**.
     c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the **System Management** region, click **System Configuration**.
   - For Oracle Identity Manager release 11.1.2:
     a. Log in to Oracle Identity System Administration.
     b. In the left pane, under **System Management**, click **System Configuration**.
   2. In the Search System Configuration box, enter `XL.SoDCheckRequired` and then **click** **Search**.

      A list that matches your search criteria is displayed in the search results table.

   3. Click the **XL.SoDCheckRequired** property name.

      System properties for SoD are displayed on the right pane.

   4. In the Value box, enter `TRUE` to enable SoD.
   5. Click **Save**.
   6. Restart Oracle Identity Manager.

**2.3.15 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 2.3.15.1, "Prerequisites for Configuring the Connector to Use SNC"**
- **Section 2.3.15.2, "Installing the Security Package"**
- **Section 2.3.15.3, "Configuring SNC"**
2.3.15.1 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.

2.3.15.2 Installing the Security Package

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

1. Download SAP Cryptolib for encrypted communication with Oracle Identity Manager.
   
   The necessary SAP Cryptolib for the encrypted communication of third-party software such as Oracle Identity Manager can be ordered from SAP official software partners listed at the SAP Service Marketplace.

2. Extract the contents of the SAP Cryptographic Library installation package. This package contains the following files:
   
   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

3. Copy the library and the sapgenpse.exe file into a local directory. For example: C:/usr/sap

4. 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.

5. 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.

6. 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 2.3.15.3, "Configuring SNC"

7. 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:

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

To:

```xml
<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>
</ias-instance>
```

**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.

8. 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.

### 2.3.15.3 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

### 2.3.16 Configuring the IT Resource

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

- Section 2.3.16.1, "Parameters for Enabling the Use of a Logon Group"
- Section 2.3.16.2, "Parameters for Enabling SNC-Based Communication"
- Section 2.3.16.3, "Parameters for Enabling Multiple Attempts to Update Multivalued Attributes"
- Section 2.3.16.4, "Mapping New Connection Properties"

The following section describes the parameters of the IT resource:

- Section 2.3.16.5, "Specifying Values for the IT Resource Parameters"
2.3.16.1 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 2–12.

- 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:\WINNDS\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.

   sapms\SYSTEM_ID 36\SYSTEM_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).
2.3.16.2 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 2.3.15, "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.

2.3.16.3 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.

2.3.16.4 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.

---

**Note:** If you enable connection pooling, then you cannot map new connection properties.

---

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.
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 2.3.16.5, "Specifying Values for the IT Resource Parameters" for instructions.

3. In the Lookup.SAP.JCo.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.JCo.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 2–11 lists the default entries in this lookup definition.

<table>
<thead>
<tr>
<th>SAP JCo Parameter</th>
<th>IT Resource Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>jco.client.ashost</td>
<td>App server host</td>
</tr>
<tr>
<td>jco.client.client</td>
<td>Client logon</td>
</tr>
<tr>
<td>jco.client.group</td>
<td>Logon group name</td>
</tr>
</tbody>
</table>
In the Decode column, enter the name of the IT resource parameter.

Click the Save icon.

### 2.3.16.5 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.

<table>
<thead>
<tr>
<th>SAP JCo Parameter</th>
<th>IT Resource Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>jco.client.lang</td>
<td>Language</td>
</tr>
<tr>
<td>jco.client.mshost</td>
<td>Message server</td>
</tr>
<tr>
<td>jco.client.passwd</td>
<td>Admin password</td>
</tr>
<tr>
<td>jco.client.r3name</td>
<td>R3 name</td>
</tr>
<tr>
<td>jco.client.snc_lib</td>
<td>SNC lib</td>
</tr>
<tr>
<td>jco.client.snc_mode</td>
<td>SNC mode</td>
</tr>
<tr>
<td>jco.client.snc_myname</td>
<td>SNC my name</td>
</tr>
<tr>
<td>jco.client.snc_partnername</td>
<td>SNC partner name</td>
</tr>
<tr>
<td>jco.client.snc_qop</td>
<td>SNC qop</td>
</tr>
<tr>
<td>jco.client.sysnr</td>
<td>System number</td>
</tr>
<tr>
<td>jco.client.trace</td>
<td>JCo trace level</td>
</tr>
<tr>
<td>jco.client.user</td>
<td>Admin logon</td>
</tr>
</tbody>
</table>

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. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.x or 11.1.1:
     - Log in to the Administrative and User Console
   - For Oracle Identity Manager release 11.1.2:
     - Log in to Oracle Identity System Administration

2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
If you are using Oracle Identity Manager release 9.1.0.x, expand **Resource Management**, and then click **Manage IT Resource**.

If you are using Oracle Identity Manager release 11.1.1, then:

- On the Welcome to Oracle Identity Manager Self Service page, click **Advanced**.
- On the Welcome to Oracle Identity Manager Advanced Administration page, in the **Configuration** region, click **Manage IT Resource**.

If you are using Oracle Identity Manager release 11.1.2, then:

- Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager*.
- In the left pane under Configuration, click **IT Resource**.

3. In the IT Resource Name field on the Manage IT Resource page, enter **SAP UM IT Resource** and then click **Search**.

4. Click the edit icon for the IT resource.

5. From the list at the top of the page, select **Details and Parameters**.

6. Specify values for the parameters of the IT resource. Table **Table 2–12** describes each parameter.

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

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 2.3.5.2, "Configuring Password Changes for Newly Created Accounts" for more information about this parameter. |
### Postinstallation

#### Deploying the Connector

2-89

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 2.3.11, "Setting Up the Lookup.SAP.UM.LookupMappings and Lookup.SAPCUA.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

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

### Table 2–12 (Cont.) Parameters of the IT Resource

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 2.3.11, "Setting Up the Lookup.SAP.UM.LookupMappings and Lookup.SAPCUA.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 |
| 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 |
<p>| SOD Configuration lookup   | This parameter holds the name of the lookup definition that stores configuration information for SAP GRC. Value: Lookup.SAP.UM.SoDConfiguration |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System number</td>
<td>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.</td>
</tr>
<tr>
<td>Timeout count</td>
<td>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 2.3.16.3, &quot;Parameters for Enabling Multiple Attempts to Update Multivalued Attributes&quot; for more information. Default value: 10</td>
</tr>
<tr>
<td>TopologyName</td>
<td>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. For Oracle Identity Manager release 9.1.0.x: Sample value: oim1-grc1-sap1 For Oracle Identity Manager release 11.1.1: Sample value: sodgrc</td>
</tr>
<tr>
<td>Abandoned connection timeout</td>
<td>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</td>
</tr>
<tr>
<td>Connection pooling supported</td>
<td>Enter true if you want to enable connection pooling for this target system installation. Otherwise, enter false. Default value: false</td>
</tr>
<tr>
<td>Connection wait timeout</td>
<td>Enter the maximum time (in seconds) for which the connector must wait for a connection to be available. Default value: 60</td>
</tr>
<tr>
<td>Inactive connection timeout</td>
<td>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</td>
</tr>
<tr>
<td>Initial pool size</td>
<td>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</td>
</tr>
<tr>
<td>Max pool size</td>
<td>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</td>
</tr>
</tbody>
</table>
Table 2–12 (Cont.) Parameters of the IT Resource

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min pool size</td>
<td>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</td>
</tr>
<tr>
<td>Native connection pool class definition</td>
<td>This parameter holds the name of the wrapper to the native pool mechanism that implements the GenericPool. <strong>Note:</strong> Do not specify a value for this parameter.</td>
</tr>
<tr>
<td>Pool excluded fields</td>
<td>This parameter holds a comma-separated list of IT parameters whose change must not trigger a refresh of the connector pool. <strong>Value:</strong> Timeout retry count, Timeout count, Configuration lookup, Dummy password, SOD Configuration lookup, TopologyName <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Pool preference</td>
<td>This parameter specifies the preferred connection pooling implementation. <strong>Value:</strong> Default <strong>Note:</strong> Do not change this value of this parameter.</td>
</tr>
<tr>
<td>ResourceConnection class definition</td>
<td>This parameter holds the name of the implementation of the ResourceConnection class. <strong>Value:</strong> oracle.iam.connectors.sap.common.connection.SAPResourceImpl <strong>Note:</strong> Do not change the value of this parameter.</td>
</tr>
<tr>
<td>Target supports only one connection</td>
<td>This parameter indicates whether the target system can support one or more connections at a time. <strong>Value:</strong> false <strong>Note:</strong> Do not change the value of this parameter.</td>
</tr>
<tr>
<td>Timeout check interval</td>
<td>Enter the time interval (in seconds) at which the other timeouts specified by the other parameters must be checked <strong>Default value:</strong> 30</td>
</tr>
<tr>
<td>Validate connection on borrow</td>
<td>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. <strong>Default value:</strong> false</td>
</tr>
</tbody>
</table>

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

### 2.3.17 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.
To work around this issue, use the Transformation of Lookup Field Data feature of the connector as follows:

**See Also:** Section 1.5.17, "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 for Oracle Identity Manager release 9.1.0.x and Oracle Identity Manager database for Oracle Identity Manager release 11.1.x.
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.

### 2.3.18 Localizing Field Labels in UI Forms

**Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2 or later and you want to localize UI form field labels.

To localize field label that you add to in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select oracle.iam.console.identity.sysadmin.ear.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:
   ```bash
   SAVED_LOCATION\xllfBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
   ```
6. Edit the BizEditorBundle.xlf file in the following manner:
   a. Search for the following text:
   ```xml
   <file source-language="en"
   ```
Postinstallation

Deploying the Connector

b. Replace with the following text:

```xml
<file source-language="en" target-language="LANG_CODE"
    original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
    datatype="x-oracle-adf">
<trans-unit id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_SAP_TITLE__c_description']}">
<source>Title</source>
<target>LANG_CODE</target>
</trans-unit>
<trans-unit id="sessiondef.oracle.iam.ui.runtime.form.model.umform.entity.umformEO.UD_SAP_TITLE__c_LABEL">
<source>Title</source>
<target>LANG_CODE</target>
</trans-unit>
```

In this text, replace LANG_CODE with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

```xml
<file source-language="en" target-language="ja"
    original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
    datatype="x-oracle-adf">
<trans-unit id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_SAP_TITLE__c_description']}">
<source>Title</source>
<target>日本語</target>
</trans-unit>
<trans-unit id="sessiondef.oracle.iam.ui.runtime.form.model.umform.entity.umformEO.UD_SAP_TITLE__c_LABEL">
<source>Title</source>
<target>日本語</target>
</trans-unit>
```

c. Search for the application instance code. This procedure shows a sample edit for SAP User Management application instance. The original code is:

```xml
<trans-unit id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_SAP_TITLE__c_description']}">
<source>Title</source>
<target>Title</target>
</trans-unit>
<trans-unit id="sessiondef.oracle.iam.ui.runtime.form.model.umform.entity.umformEO.UD_SAP_TITLE__c_LABEL">
<source>Title</source>
<target>Title</target>
</trans-unit>
```

d. Open the resource file from the connector package, for example SAPUM_ja.properties, and get the value of the attribute from the file, for example, global.udf. UD_SAP_TITLE = \\u5F79\u8077.

e. Replace the original code shown in Step 6.c with the following:

```xml
<trans-unit id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_SAP_TITLE__c_description']}">
<source>Title</source>
<target>日本語</target>
</trans-unit>
<trans-unit id="sessiondef.oracle.iam.ui.runtime.form.model.umform.entity.umformEO.UD_SAP_TITLE__c_LABEL">
<source>Title</source>
<target>日本語</target>
</trans-unit>
```

f. Repeat Steps 6.a through 6.d for all attributes of the process form.

g. Save the file as BizEditorBundle_LANG_CODE.xlf. In this file name, replace LANG_CODE with the code of the language to which you are localizing.

Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.
See Also: The "Deploying and Undeploying Customizations" chapter in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager, for more information about exporting and importing metadata files.

8. Log out of and log in to Oracle Identity Manager.
Using the Connector

This chapter is divided into the following sections:

- Section 3.1, "Performing Full Reconciliation"
- Section 3.2, "Scheduled Task for Lookup Field Synchronization"
- Section 3.3, "Guidelines on Performing Reconciliation"
- Section 3.4, "Configuring Reconciliation"
- Section 3.5, "Configuring Scheduled Tasks"
- Section 3.6, "Guidelines on Performing Provisioning"
- Section 3.7, "Provisioning Operations Performed in an SoD-Enabled Environment"
- Section 3.8, "Switching Between SAP R/3 and SAP CUA Target Systems"
- Section 3.9, "Switching Between SAP R/3 or SAP CUA Target System to an SAP CUP Target System on Oracle Identity Manager Release 11.1.x"
- Section 3.10, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"
- Section 3.11, "Enabling and Disabling the SoD Feature"
- Section 3.12, "Enabling and Disabling the Compliant User Provisioning Feature"

### 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...
Scheduled Task for Lookup Field Synchronization

onward, only records created or modified after this time stamp value are considered for reconciliation.

3.2 Scheduled Task for Lookup Field Synchronization

Note: It is assumed that you have performed all the procedures described in the preceding chapter.

In Oracle Identity Manager release 11.1.x, a scheduled job is an instance of a scheduled task. In this guide, the term scheduled task used in the context of Oracle Identity Manager release 9.1.0.x is the same as the term scheduled job in the context of Oracle Identity Manager release 11.1.x.

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

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Resource</td>
<td>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</td>
</tr>
<tr>
<td>Lookup Name</td>
<td>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</td>
</tr>
<tr>
<td>Schedule Task Name</td>
<td>This attribute holds the name of the scheduled task. Value: SAP User Management Lookup Recon</td>
</tr>
</tbody>
</table>

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:
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.
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"
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>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Mapping Lookup</td>
<td>This attribute holds the name of the lookup definition that stores attribute mappings for reconciliation.</td>
</tr>
<tr>
<td>Value: Lookup.SAP.UM.ReconAttrMap</td>
<td></td>
</tr>
<tr>
<td>Batch Size</td>
<td>Enter the number of records that must be included in each batch fetched from the target system during a reconciliation run.</td>
</tr>
<tr>
<td></td>
<td>This attribute is used to implement batched reconciliation.</td>
</tr>
<tr>
<td>Default value: 100</td>
<td></td>
</tr>
<tr>
<td>Child Attribute Mapping Lookup</td>
<td>This attribute holds the name of the lookup definition that stores child attribute mappings for reconciliation.</td>
</tr>
<tr>
<td>Value: Lookup.SAP.UM.ReconChildAttrMap</td>
<td></td>
</tr>
<tr>
<td>Custom Query</td>
<td>Enter the query that you want the connector to apply during reconciliation. See Section 3.4.2, &quot;Limited Reconciliation&quot; for more information.</td>
</tr>
<tr>
<td>IT Resource</td>
<td>Enter the name of the IT resource for the target system installation from which you want to reconcile user records.</td>
</tr>
<tr>
<td>Default value: SAP UM IT Resource</td>
<td></td>
</tr>
<tr>
<td>Last Execution Timestamp</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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, &quot;Full Reconciliation vs. Incremental Reconciliation&quot; for more information.</td>
</tr>
<tr>
<td>Default value: 0</td>
<td></td>
</tr>
<tr>
<td>Resource Object</td>
<td>This attribute holds the name of the resource object.</td>
</tr>
<tr>
<td>Default value: SAP UM Resource Object</td>
<td></td>
</tr>
<tr>
<td>SAP System Time Zone</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Sample value: PST</td>
<td></td>
</tr>
<tr>
<td>Schedule Task Name</td>
<td>This attribute holds the name of the scheduled task.</td>
</tr>
<tr>
<td>Value: SAP User Management User Recon</td>
<td></td>
</tr>
</tbody>
</table>

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.
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.
3.4.3.4 SAP CUP Delete Recon

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constants Lookup</td>
<td>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</td>
</tr>
<tr>
<td>IT Resource</td>
<td>Enter the name of the IT resource for the SAP GRC installation from which you want to fetch request status data. Default value: GRC-ITRes</td>
</tr>
<tr>
<td>Resource Object</td>
<td>This attribute holds the name of the resource object. Default value: SAP UM Resource Object</td>
</tr>
<tr>
<td>Schedule Task Name</td>
<td>This attribute holds the name of the scheduled task. Default value: SAP CUP Status Update Recon</td>
</tr>
</tbody>
</table>

#### 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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Lookup</td>
<td>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</td>
</tr>
<tr>
<td>Constants Lookup</td>
<td>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</td>
</tr>
<tr>
<td>IT Resource</td>
<td>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</td>
</tr>
<tr>
<td>Resource Object</td>
<td>This attribute holds the name of the resource object. Default value: SAP UM Resource Object</td>
</tr>
<tr>
<td>Schedule Task Name</td>
<td>This attribute holds the name of the scheduled task. Default value: SAP CUP Delete Recon</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Scheduled Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP User Management Lookup Recon</td>
<td>This scheduled task is used for lookup field synchronization. Section 3.2, “Scheduled Task for Lookup Field Synchronization” describes this scheduled task.</td>
</tr>
<tr>
<td>SAP User Management User Recon</td>
<td>This scheduled task is used for user record reconciliation. Section 3.4.3.1, “SAP User Management User Recon” describes this scheduled task.</td>
</tr>
<tr>
<td>SAP User Management Delete Recon</td>
<td>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.</td>
</tr>
<tr>
<td>SAP CUP Status Update Recon</td>
<td>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.</td>
</tr>
<tr>
<td>SAP CUP Delete Recon</td>
<td>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.</td>
</tr>
</tbody>
</table>

To configure a scheduled task:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.x or 11.1.1:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Oracle Identity Manager Self Service page, click Advanced in the upper-right corner of the page.
   - For Oracle Identity Manager release 11.1.2:
     a. Log in to Oracle Identity System Administration.
     b. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager.
     c. In the left pane, under System Management, click Scheduler.

2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.x, expand Resource Management, and then click Manage Scheduled Task.
   - If you are using Oracle Identity Manager release 11.1.1, then:
a. On the Welcome to Oracle Identity Manager Self Service page, click Advanced.

b. Click the System Management tab, and then click Scheduler.

c. On the left pane, click Advanced Search.

3. On the page that is displayed, you can use any combination of the search options provided to locate a scheduled task. Click Search after you specify the search criteria.

   The list of scheduled tasks that match your search criteria is displayed in the search results table.

4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.x, then in the search results table, click the Edit icon in the Edit column for the scheduled task.
   - If you are using Oracle Identity Manager release 11.1.x, then select the link for the scheduled task from the list of scheduled tasks displayed in the search results table.

5. Modify the details of the scheduled task. To do so:
   - If you are using Oracle Identity Manager release 9.1.0.x, then on the Edit Scheduled Task Details page, you can modify the following parameters:
     - **Status**: Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.
     - **Max Retries**: Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.
     - **Next Start**: Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
     - **Frequency**: Specify the frequency at which you want the task to run.
   - If you are using Oracle Identity Manager release 11.1.x, then on the Job Details tab, you can modify the following parameters:
     - **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
     - **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type.

---

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

6. After modifying the values for the scheduled task details listed in the previous step, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.x, then click Continue.
   - If you are using Oracle Identity Manager release 11.1.x, then perform the next step.
7. Specify values for the attributes of the scheduled task. To do so:
   - If you are using Oracle Identity Manager release 9.1.0.x, select each attribute from the Attribute list, specify a value in the field provided, and then click Update.
   - If you are using Oracle Identity Manager release 11.1.x, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

   **Note:** Attribute values are predefined in the connector XML file that is imported during the installation of the connector. Specify values only for the attributes that you want to change.

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

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

   - If you are using Oracle Identity Manager release 11.1.x, then click Apply to save the changes.

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

3.6 Guidelines on Performing Provisioning

**See Also:** Section 1.4.5, “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 one of the following guides for information about configuring process tasks:

– For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User’s Guide for Oracle Identity Manager

– For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager

■ 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.

■ 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
Provisioning Operations Performed in an SoD-Enabled Environment

- 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.

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 Fusion Middleware User’s Guide for Oracle Identity Manager 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 3.7.2, "Guidelines on Performing Provisioning Operations"
- 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

This section describes the prerequisites and the procedure to perform direct provisioning. It contains the following sections:

- Section 3.7.3.1, "Prerequisites"
3.7.3.1 Prerequisites

Note: Perform the procedure in this section only in the following situations:

- The first time you perform direct provisioning.
- If you switch from request-based provisioning to direct provisioning.

On Oracle Identity Manager release 9.1.0.x, when you run the Connector Installer, configurations for both direct provisioning and request-based provisioning of SAP user accounts are installed. Therefore, during direct provisioning, the process form is suppressed and object form is displayed. If you want to enable the use of the process form during direct provisioning, then perform the procedure described later in this section.

On Oracle Identity Manager release 11.1.x, when you run the Connector Installer, the configuration for direct provisioning of SAP user accounts is installed. Although the process form is displayed during direct provisioning, the connector cannot complete direct provisioning operations unless you enable the use of the process form. If you want to enable the use of the process form during direct provisioning, then perform the procedure described later in this section.

To enable the use of the process form during direct provisioning:

Note: Request-based provisioning is disabled after you perform this procedure.

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
   a. Expand Process Management, and then double-click Process Definition.
   b. Search for and open the SAP UM Process Form process definition.
   c. Deselect the Auto Save Form check box.
   d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
   a. Expand Resource Management, and then double-click Resource Objects.
   b. Search for and open the SAP UM Resource Object resource object.
   c. Deselect the Self Request Allowed check box.
   d. Click the Save icon.
3.7.3.2 Performing Direct Provisioning in Oracle Identity Manager Release 9.1.0.x or 11.1.1

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.

2. If you want to first create an OIM User and then provision a target system account:
   - If you are using Oracle Identity Manager release 9.1.0.x, then:
     a. From the Users menu, select Create.
     b. On the Create User page, enter values for the OIM User fields and then click Create User. The following screenshot shows the Create User page:

   ![Create User Page](image)

   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Users region, click Create User.
     b. On the Create User page, enter values for the OIM User fields, and then click Save.

3. If you want to provision a target system account to an existing OIM User, then:
   - If you are using Oracle Identity Manager release 9.1.0.x, then:
     a. From the Users menu, select Manage.
     b. Search for the OIM User by using the Search feature, and then click the link for the OIM User from the list of users displayed in the search results table.

   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, search for the OIM User by selecting Users from the drop-down list on the left pane.
     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.

4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
If you are using Oracle Identity Manager release 9.1.0.x, then:

a. 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:

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

If you are using Oracle Identity Manager release 11.1.1, then:

a. On the user details page, click the **Resources** tab.

b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

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

7. 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.
8. 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.

9. 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.
10. 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.

11. The "Provisioning has been initiated" message is displayed. To view the newly provisioned resource, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.x, then click **Back to User Resource Profile**. The Resource Profile page shows that the resource has been provisioned to the user. The following screenshot shows this page:
If you are using Oracle Identity Manager release 11.1.1, then:

a. Close the window displaying the "Provisioning has been initiated" message.

b. On the Resource tab of the user details page, click Refresh to view the newly provisioned resource.

12. To view the process form, perform one of the following steps:

If you are using Oracle Identity Manager release 9.1.0.x, then on the Resource Profile page, click the View link in the Process Form column. The View Form page is displayed.

In this screenshot, the SOD Check Status field shows SODCheckNotInitiated. The value in this field can be SODCheckNotInitiated, SODCheckResultPending, or SODCheckCompleted.
If you are using Oracle Identity Manager release 11.1.1, then on the Resources tab of the user details page, select the row displaying the newly provisioned resource, and then click Open. The Edit Form page is displayed.

13. To view the Resource Provisioning Details page, which shows the details of the process tasks that were run, perform the procedure in one of the following steps:

- If you are using Oracle Identity Manager release 9.1.0.x, then on the Resource Profile page, click the resource link in the Resource Name column.

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.

- If you are using Oracle Identity Manager release 11.1.1, then on the Resources tab of the user details page, from the Action menu, select Resource History.

14. The SODCheckNotInitiated status in the SOD Check Status field indicates that SoD validation has not started. If you are using Oracle Identity Manager release 9.1.0.x, then 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:
After the ResubmitUninitiatedProvisioningSODChecks scheduled task is run, the results of the SoD validation process are brought to Oracle Identity Manager. To view the process form, perform the procedure described in one of the following steps:

- If you are using Oracle Identity Manager release 9.1.0.x, then on the Resource Profile page, click the View link in the Process Form column. The View Form page is displayed.

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:

![Screenshot of Resource Provisioning Details page]

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

- If you are using Oracle Identity Manager release 11.1.1, then on the Resources tab of the user details page, select the row displaying the newly provisioned resource, and then click **Open**. The Edit Form page is displayed.

16. 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, perform the procedure in one of the following steps:

- If you are using Oracle Identity Manager release 9.1.0.x, then first click the **Edit** link in the Process Form column on the Resource Profile page.

- If you are using Oracle Identity Manager release 11.1.1, then on the Resource tab of the user details page, select the row containing the resource, and then click **Open**.

17. 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:
18. Rerun the ResubmitUninitiatedProvisioningSODChecks scheduled task to initiate the SoD validation process.

19. After the ResubmitUninitiatedProvisioningSODChecks scheduled task is run, the results of the SoD validation process are brought to Oracle Identity Manager. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

- If you are using Oracle Identity Manager release 9.1.0.x, then on the Resource Profile page, click the View link in the Process Form column. The process form is displayed.

   ![Resource Profile Page](image)

   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:

   ![Resource Provisioning Details Page](image)
On the Resource Provisioning Details page, the state of the Add User Role task is Completed.

- If you are using Oracle Identity Manager release 11.1.1, then on the Resources tab of the user details page, select the row containing the resource, and then click Open. The process form is displayed.

20. 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:

### 3.7.3.3 Performing Direct Provisioning in Oracle Identity Manager Release 11.1.2

To configure provisioning operations in Oracle Identity Manager release 11.1.2:

**Note:** The time required to complete a provisioning operation that you perform the first time by using this connector takes longer than usual.

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See the "Managing Users" chapter in Oracle Fusion Middleware User’s Guide for Oracle Identity Manager for more information about creating a user.
3. On the Account tab, click Request Accounts.
4. In the Catalog page, search for and add to cart the application instance and then click Checkout.
5. Specify value for fields in the application form and then click Ready to Submit.
6. Click Submit.
7. If you want to provision entitlements, then:
   a. On the Entitlements tab, click Request Entitlements.
   b. In the Catalog page, search for and add to cart the entitlement, and then click Checkout.
   c. Click Submit.
3.7.4 Request-Based Provisioning in an SoD-Enabled Environment

See Also: Section 2.3.14, "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.

3.7.4.1 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.

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

- Section 3.7.4.1.1, "End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x"
- Section 3.7.4.1.2, "End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.1"

3.7.4.1.1 End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x

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:
   The following screenshot shows this page:

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:
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:

   ![Screenshot of resource data page]

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:

   ![Screenshot of verification page]

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

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:

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:
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 show this scheduled task in the Design Console:

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.
3.7.4.1.2 End User’s Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.1

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

See Also: The "Creating and Searching Requests" chapter of Oracle Fusion Middleware User’s Guide for Oracle Identity Manager for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click Advanced on the top right corner of the page.
3. On the Welcome to Identity Manager Advanced Administration page, click the Administration tab, and then click the Requests tab.
4. From the Actions menu on the left pane, select Create Request.
   
   The Select Request Template page is displayed.
5. From the Request Template list, select Provision Resource and then click Next.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click Search. A list of users that match the search criterion you specified is displayed in the Available Users list.
7. From the Available Users list, select the user to whom you want to provision the account.
   
   If you want to create a provisioning request for more than one user, then from the Available Users list, select the users to whom you want to provision the account.
8. Click Move or Move All to include your selection in the Selected Users list, and then click Next.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select SAP UM Resource Object, move it to the Selected Resources list, and then click Next.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.

12. On the Justification page, you can specify values for the following fields, and then click **Finish**:
   - Effective Date
   - Justification

   On the resulting page, a message confirming that your request has been sent is displayed along with the Request ID.

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

14. On the Resource tab of the Request Details page, click the View Details link in the row containing the resource for which the request was created. The Resource Details page is displayed in a new window.

   One of the fields on this page is the SODCheckStatus field. The value in this field can be SoD Check Not Initiated or SoDCheckCompleted. When the request is placed, the SODCheckStatus field contains the SoDCheckCompleted status.

15. To view details of the approval, on the Request Details page, click the **Approval Tasks** tab.

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

### 3.7.4.2 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.

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

- **Section 3.7.4.2.1, “Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x”**
- **Section 3.7.4.2.2, “Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.1”**

### 3.7.4.2.1 Approver’s Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x

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

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 Screenshot](image)

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

The following screenshot shows this page:
5. On the Request Details page, the SOD Status column shows SODCheckCompleted.

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

3.7.4.2.2 Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.1

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

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

A message confirming that the task has been approved is displayed and the request status is changed to **Obtaining Operation Approval**.
6. Select the row containing the request which is approved, and then click **Approve Task**.
   A message confirming that the task has been approved is displayed and the request status is changed to **Request Completed**.
7. Click the **Administration** tab and search for the user(s) for whom the request is completed.
8. Select the user.
   The user detail information is displayed in the right pane.
9. Click the **Resources** tab to view the resource being provisioned.
10. Select the resource being provisioned, and then click **Open** to view the resource details.
11. On the Resources tab of the User Details page, from the **Action** menu, select **Resource History** to view the resource provisioning tasks.

### 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 2.3.5, "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 Switching Between SAP R/3 or SAP CUA Target System to an SAP CUP Target System on Oracle Identity Manager Release 11.1.x

On Oracle Identity Manager release 11.1.x, if you want to switch from an SAP R/3 or SAP CUA target system to a SAP CUP target system and vice versa, then perform the following steps:

1. Ensure that you have set the environment variable for running the MDS Delete utility. In the weblogic.properties file, ensure that values are set for the wls_servername, application_name, and metadata_files properties. See Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager for detailed information about setting up the environment for MDS utilities.

2. Delete the existing request datasets using the following command:
   - On Microsoft Windows
     weblogicDeleteMetadata.bat
   - On UNIX
     weblogicDeleteMetadata.sh

3. Run the PurgeCache utility to clear the cache for the content category Metadata. See Section 2.3.8, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

4. If you are using Oracle Identity Manager release 11.1.1, then import the request datasets for the target system to which you want to switch. Perform the procedure described in Section 2.3.6.2.2, "Importing Request Datasets into MDS."

5. Run the PurgeCache utility to clear the cache for the content category Metadata. See Section 2.3.8, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

**Note:** It is assumed that you have performed the procedure described in Section 2.3.6, "Enabling Request-Based Provisioning."

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

1. Log in to the Design Console.

2. Disable the Auto Save Form feature as follows:
   a. Expand Process Management, and then double-click Process Definition.
   b. Search for and open the SAP UM Process Form process definition.
   c. Deselect the Auto Save Form check box.
   d. Click the Save icon.

3. If the Self Request Allowed feature is enabled, then:
   a. Expand Resource Management, and then double-click Resource Objects.
   b. Search for and open the SAP UM Resource Object resource object.
c. Deselect the **Self Request Allowed** check box.

**d. Click the Save icon.**

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

1. Log in to the Design Console.

2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **SAP UM Process Form** process definition.
   c. Select the **Auto Save Form** check box.
   **d. Click the Save icon.**

3. If you want to enable end users to raise requests for themselves, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **SAP UM Resource Object** resource object.
   c. Select the **Self Request Allowed** check box.
   **d. Click the Save icon.**

**3.11 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.

**3.12 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 2.3.5.3, "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:

- Section 4.1, "Determining the Names of Target System Attributes"
- Section 4.2, "Adding New Attributes for Reconciliation"
- Section 4.3, "Adding New Standard and Custom Multivalued Attributes for Reconciliation"
- Section 4.4, "Adding New Standard Attributes for Provisioning"
- Section 4.5, "Adding New Standard SAP GRC Compliant User Provisioning Attributes for Provisioning"
- Section 4.6, "Adding New Standard Multivalued Attributes for Provisioning"
- Section 4.7, "Adding Custom Attributes for Provisioning"
- Section 4.8, "Adding Custom Multivalued Attributes for Provisioning"
- Section 4.9, "Configuring Validation of Data During Reconciliation and Provisioning"
- Section 4.10, "Configuring Transformation of Data During User Reconciliation"
- Section 4.11, "Configuring Transformation of Data During Lookup Field Synchronization"
- Section 4.12, "Configuring Synchronization of New Lookup Definitions with the Target System"
- Section 4.13, "Modifying Field Lengths on the Process Form"
- Section 4.14, "Configuring the Connector for Multiple Installations of the Target System"

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:
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:

### Lookup Definition

<table>
<thead>
<tr>
<th>Lookup Definition</th>
<th>Format of Value in the Decode Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup.SAP.UM.ReconAttrMap</td>
<td><code>FIELD_TYPE;FIELD_NAME;STRUCTURE_NAME</code></td>
</tr>
<tr>
<td></td>
<td><code>FIELD_TYPE</code> can be TEXT, DATE, CHECKBOX, or LOOKUP.</td>
</tr>
<tr>
<td></td>
<td>See Section 1.7.1, &quot;User Attributes for Reconciliation&quot; for more information.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ReconChildAttrMap</td>
<td><code>FIELD_TYPE;FIELD_NAME;TABLE_NAME;OIM_CHILD_TABLE_NAME</code></td>
</tr>
<tr>
<td></td>
<td><code>FIELD_TYPE</code> can be TEXT, DATE, CHECKBOX, or LOOKUP.</td>
</tr>
<tr>
<td></td>
<td>See Section 1.7.1, &quot;User Attributes for Reconciliation&quot; for more information.</td>
</tr>
<tr>
<td>Lookup.SAP.UM.ProvAttrMap and Lookup.SAP.UM.ProvChildAttrMap</td>
<td><code>FIELD_TYPE;FIELD_NAME;STRUCTURE_NAME;FIELD_NAME_X;STRUCTURE_NAME_X</code></td>
</tr>
<tr>
<td></td>
<td><code>FIELD_TYPE</code> can be TEXT, DATE, CHECKBOX, or LOOKUP.</td>
</tr>
<tr>
<td></td>
<td>See Section 1.8.2, &quot;User Attributes for Provisioning&quot; for more information.</td>
</tr>
</tbody>
</table>

---

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

![Screenshot of structure editor](image)

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 one of the following guides for detailed information about the steps of this procedure:
- For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User’s Guide for Oracle Identity Manager
- For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager

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:

3. Add the new attribute to the list of reconciliation fields in the resource object as follows:
   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:
f. If you are using Oracle Identity Manager release 11.1.x, then click Create Reconciliation Profile. This copies changes made to the resource object into the MDS.

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


   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:
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:
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:

```
2BAPI_CUSTFIELDS;TEXT;2CUSTFIELDS;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:

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.

8. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.
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:
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:
Adding New Standard and Custom Multivalued Attributes for Reconciliation

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

   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:
   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:
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:
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.

8. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, “Creating a New UI Form” and Section 2.3.1.7, “Updating an Existing Application Instance with a New Form” for the procedures.

### 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:**
Adding New Standard Attributes for Provisioning

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:

3. Create an entry for the attribute in the lookup definition for provisioning as follows:
   a. Expand Administration.

   See one of the following guides for detailed information about the steps of this procedure:
   - For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User’s Guide for Oracle Identity Manager
   - For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager

If you have already added an attribute for reconciliation, then you need not repeat steps performed as part of that procedure.
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;ADDRESS;ROOM_NO;ADDRESS** in the **Decode** column. The following screenshot shows the entry added to the lookup definition:

   ![Lookup Definition](image)

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:
Adding New Standard Attributes for Provisioning

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:

   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:

<table>
<thead>
<tr>
<th>Field Label in SAP</th>
<th>Value to Be Entered in the Code Key Column (Sample Process Form Field Name)</th>
<th>Value to Be Entered in the Decode Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Immediately</td>
<td>Output Immediately</td>
<td>GH</td>
</tr>
<tr>
<td>Delete After Output</td>
<td>Delete After Output</td>
<td>DK</td>
</tr>
<tr>
<td>Check Indicator</td>
<td>Check Indicator</td>
<td>X</td>
</tr>
<tr>
<td>Unsecure communication permitted (user-specific)</td>
<td>Unsecure communication permitted</td>
<td>X</td>
</tr>
</tbody>
</table>

---

**See Also:** One of the following guides for detailed information about these steps:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Fusion Middleware User’s Guide for Oracle Identity Manager*
- For Oracle Identity Manager release 11.1.x: *Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager*
On the Integration tab of the Creating New Task dialog box, click **Add**.

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:

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:

<table>
<thead>
<tr>
<th>Variable Number</th>
<th>Variable Name</th>
<th>Map To</th>
<th>Qualifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>BapiFieldName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: ROOM_NO_P</td>
</tr>
<tr>
<td>Third</td>
<td>BapiStructure</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: ADDRESS</td>
</tr>
<tr>
<td>Fourth</td>
<td>ProcessKey</td>
<td>Process Data</td>
<td>Process Instance</td>
</tr>
<tr>
<td>Fifth</td>
<td>ITResNameU</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: UD_SAP_ITRESOURCE</td>
</tr>
<tr>
<td>Sixth</td>
<td>UserId</td>
<td>Process Data</td>
<td>User ID</td>
</tr>
</tbody>
</table>

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.

6. If you are using Oracle Identity Manager release prior to 11.1.2, perform the following steps:

a. When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. In a text editor, open the XML file located in the \OIM_HOME\DataSet\file directory for editing.

b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager* for more information about creating and updating request datasets.

For example, while performing Step 1 of this procedure, if you added City as an attribute on the process form, then enter the following line:

```xml
<AttributeReference
  name = "City"
  attr-ref = "City"
  type = "String"
  widget = "text"
  length = "50"
  available-in-bulk = "false"/>
```

In this AttributeReference element:

- For the name attribute, enter the value in the Name column of the process form without the tablename prefix.
- For example, if UD_SAP_CITY is the value in the Name column of the process form, then you must specify CITY is the value of the name attribute in the AttributeReference element.
- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 1.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 1.
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.

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:
Adding New Standard SAP GRC Compliant User Provisioning Attributes for Provisioning

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:

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:

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.
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:

   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:

Note: See one of the following guides for detailed information about the steps of this procedure:

- For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User’s Guide for Oracle Identity Manager
- For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager
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.UUM.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:

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: One of the following guides for detailed information about these steps:

- For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User's Guide for Oracle Identity Manager
- For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager

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:

   ![New Task Added](image)

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:
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:

<table>
<thead>
<tr>
<th>Variable Number</th>
<th>Variable Name</th>
<th>Map To</th>
<th>Qualifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>BapiFieldName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: ROOM_NO_P</td>
</tr>
<tr>
<td>Third</td>
<td>BapiStructure</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: ADDRESS</td>
</tr>
<tr>
<td>Fourth</td>
<td>ProcessKey</td>
<td>Process Data</td>
<td>Process Instance</td>
</tr>
<tr>
<td>Fifth</td>
<td>ITResNameU</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: UD_SAP_ITRESOURCE</td>
</tr>
<tr>
<td>Sixth</td>
<td>UserId</td>
<td>Process Data</td>
<td>User ID</td>
</tr>
</tbody>
</table>

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.

6. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI
   form and attach it to the application instance to make this new attribute visible.
   See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an
   Existing Application Instance with a New Form" for the procedures.
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 one of the following guides for detailed information about the steps of this procedure:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Fusion Middleware User’s Guide for Oracle Identity Manager*
- For Oracle Identity Manager release 11.1.x: *Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager*

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:
Adding New Standard Multivalued Attributes for Provisioning

**Note:** Only the most basic instructions to create a child form are given in this section. See one of the following guides for detailed instructions:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Fusion Middleware User’s Guide for Oracle Identity Manager*
- For Oracle Identity Manager release 11.1.x: *Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager*

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:
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:
Adding New Standard Multivalued Attributes for Provisioning


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:

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:

<table>
<thead>
<tr>
<th>Variable Number</th>
<th>Variable Name</th>
<th>Map To</th>
<th>Qualifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>UserId</td>
<td>Process Data</td>
<td>User ID</td>
</tr>
<tr>
<td>Third</td>
<td>MultiValueAttribute</td>
<td>Process Data / Child Form Name</td>
<td>Key Multi Valued Attribute present in child form For example: Parameter ID</td>
</tr>
<tr>
<td>Fourth</td>
<td>ChildPrimaryKey</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UD field of the child form For example: UD_SPUM_PARAM</td>
</tr>
<tr>
<td>Fifth</td>
<td>ChildTableName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UD field of the child form For example: UD_SPUM_PARAM</td>
</tr>
<tr>
<td>Sixth</td>
<td>BapiStructureName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: PARAMETER</td>
</tr>
<tr>
<td>Seventh</td>
<td>BapiFieldName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: PARID</td>
</tr>
<tr>
<td>Eighth</td>
<td>ProcessKey</td>
<td>Process Data</td>
<td>Process Instance</td>
</tr>
<tr>
<td>Ninth</td>
<td>ITResNameUD</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: UD_SAP_ITRESOURCE</td>
</tr>
</tbody>
</table>

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:

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:

![Creating New Task](image)

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:

<table>
<thead>
<tr>
<th>Variable Number</th>
<th>Variable Name</th>
<th>Map To</th>
<th>Qualifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>UserId</td>
<td>Process Data</td>
<td>User ID</td>
</tr>
</tbody>
</table>
| 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 |
| 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:
On the Integration tab of the Creating New Task dialog box, click **Add**.

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:

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:

<table>
<thead>
<tr>
<th>Variable Number</th>
<th>Variable Name</th>
<th>Map To</th>
<th>Qualifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>UserId</td>
<td>Process Data</td>
<td>User ID</td>
</tr>
<tr>
<td>Third</td>
<td>MultiValueAttribute</td>
<td>Process Data / Child</td>
<td>Key multivalued attribute present in the child form</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Form Name</td>
<td>For example: Parameter Id</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: Select the Old Value check box.</td>
</tr>
<tr>
<td>Fourth</td>
<td>ChildPrimaryKey</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BAPI field name of Key multivalued attribute taken from the child form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: PARID</td>
</tr>
<tr>
<td>Fifth</td>
<td>BapiStructureName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: PARAMETER</td>
</tr>
<tr>
<td>Sixth</td>
<td>ProcessKey</td>
<td>Process Data</td>
<td>Process Instance</td>
</tr>
<tr>
<td>Seventh</td>
<td>ITResNameUD</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: UD_SAP_ITRESOURCE</td>
</tr>
</tbody>
</table>

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.

11. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.

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 one of the following guides for detailed information about the steps of this procedure:

- For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User’s Guide for Oracle Identity Manager
- For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager

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:
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: One of the following guides for detailed information about these steps:
   * For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User's Guide for Oracle Identity Manager
   * For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager

   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:

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:

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:

<table>
<thead>
<tr>
<th>Variable Number</th>
<th>Variable Name</th>
<th>Map To</th>
<th>Qualifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>UserId</td>
<td>Process Data</td>
<td>User ID</td>
</tr>
<tr>
<td>Third</td>
<td>UserIDBAPIName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User ID field in the BAPI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: BNAME</td>
</tr>
<tr>
<td>Fourth</td>
<td>BAPIName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BAPI Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: ZXLCBAPI_ZXLCUSR_CHANG_ATTR</td>
</tr>
<tr>
<td>Fifth</td>
<td>BAPIStructureName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: ADDRESS</td>
</tr>
<tr>
<td>Sixth</td>
<td>BAPIFieldName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BAPI field name of custom attribute</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: JOB_DESC1</td>
</tr>
<tr>
<td>Seventh</td>
<td>FormFieldName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: Job Description</td>
</tr>
<tr>
<td>Eighth</td>
<td>FieldType</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: TEXT</td>
</tr>
<tr>
<td>Ninth</td>
<td>ProcessKey</td>
<td>Process Data</td>
<td>Process Instance</td>
</tr>
<tr>
<td>Tenth</td>
<td>ITResourceUDField</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: UD_SAP_ITRESOURCE</td>
</tr>
<tr>
<td>Eleventh</td>
<td>FieldValue</td>
<td>Process Data</td>
<td>Custom field in process form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: Job Description</td>
</tr>
</tbody>
</table>

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.

5. If you are using Oracle Identity Manager release prior to 11.1.2, perform the following steps:

a. When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. In a text editor, open the XML file located in the $OIM_HOME/DataSet/file directory for editing.

b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

See Also: The "Configuring Requests" chapter of the Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager for more information about creating and updating request datasets.
For example, while performing Step 1 of this procedure, if you added JobDesc as an attribute on the process for, then enter the following line:

```xml
<AttributeReference
name = "JobDesc"
attr-ref = "JobDesc"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

In this AttributeReference element:

- For the name attribute, enter the value in the Name column of the process form without the tablename prefix.
  
  For example, if UD_SAP_JOBDESC is the value in the Name column of the process form, then you must specify JobDesc is the value of the name attribute in the AttributeReference element.

- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 1.

- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 1.

- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 1.

- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 1.

- For the available-in-bulk attribute, specify true if the data value is available for bulk modification. Otherwise specify false.

While performing Step 1, if you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

d. Run the PurgeCache utility to clear content related to request datasets from the server cache.

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

e. Import into MDS, the request dataset definitions in XML format.

See Section 2.3.6.2.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

6. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible.

See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.

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.
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: 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.

Note: See one of the following guides for detailed information about the steps of this procedure:

- For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User’s Guide for Oracle Identity Manager
- For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager

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

   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:

\[
\text{LOOKUP; STRUCT; STRUCT\_ROL}
\]

The following screenshot shows the entry added to the lookup definition:

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:

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:

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.

To create mappings for the remaining adapter variables, use the data given in the following table:
Click the Save icon in the Editing Task dialog box, and then close the dialog box.

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

   Second

   Third

   Fourth

   Fifth

   Sixth

   Seventh

   Eighth

   Ninth

   Tenth

   Eleventh

   Twelfth

<table>
<thead>
<tr>
<th>Variable Number</th>
<th>Variable Name</th>
<th>Map To</th>
<th>Qualifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>UserId</td>
<td>Process Data</td>
<td>User ID</td>
</tr>
<tr>
<td>Third</td>
<td>Field Value</td>
<td>Process Data / Child Form Name</td>
<td>Key multivalued attribute present on the child form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: Structural Roles</td>
</tr>
<tr>
<td>Fourth</td>
<td>ChildPrimaryKey</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User-defined field of key multivalued attribute taken from the child form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: UD_SAP_STRUCT_ROLES</td>
</tr>
<tr>
<td>Fifth</td>
<td>ChildTableName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User-defined field of the child form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: UD_SAP_STRUCT</td>
</tr>
<tr>
<td>Sixth</td>
<td>BapiStructureName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: STRUCT_ROLE</td>
</tr>
<tr>
<td>Seventh</td>
<td>BapiFieldName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: STRUCT</td>
</tr>
<tr>
<td>Eighth</td>
<td>ProcessKey</td>
<td>Process Data</td>
<td>Process Instance</td>
</tr>
<tr>
<td>Ninth</td>
<td>ITResNameUD</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: UD_SAP_ITRESOURCE</td>
</tr>
<tr>
<td>Tenth</td>
<td>GetAttrBAPIName</td>
<td>Literal</td>
<td>BAPI name for the custom BAPI that will fetch the multivalued attribute from the target system</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: ZMPHC_RETURN_STRUCT_ROLES</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Eleventh</td>
<td>BAPIName</td>
<td>Literal</td>
<td>Name of the custom BAPI that will add the multivalued attribute</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: ZMPHC_STRUCT_ROLES</td>
</tr>
<tr>
<td>Twelfth</td>
<td>UserIDBAPIName</td>
<td>Literal</td>
<td>User ID field as it appears in the custom BAPI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example: USERNAME</td>
</tr>
</tbody>
</table>
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:

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:

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:

<table>
<thead>
<tr>
<th>Variable Number</th>
<th>Variable Name</th>
<th>Map To</th>
<th>Qualifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>UserId</td>
<td>Process Data</td>
<td>User ID</td>
</tr>
<tr>
<td>Third</td>
<td>FieldValue</td>
<td>Process Data / Child Form Name</td>
<td>Key multivalued attribute present on the child form For example: Structural Role Note: Select the Old Value check box.</td>
</tr>
<tr>
<td>Fourth</td>
<td>BapiFieldName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td>Fifth</td>
<td>BapiStructureName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td>Sixth</td>
<td>ProcessKey</td>
<td>Process Data</td>
<td>Process Instance</td>
</tr>
<tr>
<td>Seventh</td>
<td>ITResNameUD</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td>Eight</td>
<td>BAPIName</td>
<td>Literal</td>
<td>String</td>
</tr>
<tr>
<td>Nine</td>
<td>UserIDBAPIName</td>
<td>Literal</td>
<td>User ID field in BAPI For example: USERNAME</td>
</tr>
</tbody>
</table>

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.

10. If you are using Oracle Identity Manager release prior to 11.1.2, then:

a. When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. In a text editor, open the XML file located in the OIM_HOME/DataSet/file directory for editing.

b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

See Also: The "Configuring Requests" chapter of the Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager for more information about creating and updating request datasets

For example, while performing Step 1 of this procedure, if you added CustRoles as an attribute on the process for, then enter the following line:

<AttributeReference
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:

debugId: "123456789"; date: "2023-01-01 12:00:00"; level: "ERROR"; message: "Failed validation check for attribute 'First Name'. Value: 'John#Doe'; reason: 'Contains invalid character'"; severity: "ERROR"; source: "ReconciliationServer"; target: "SAProphe";

In this AttributeReference element:

- For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

  For example, if UD_SAPRL_CUSTROLES is the value in the Name column of the process form, then you must specify CUSTROLES is the value of the name attribute in the AttributeReference element.

- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 1.

- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 1.

- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 1.

- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 1.

- For the available-in-bulk attribute, specify true if the data value is available for bulk modification. Otherwise specify false.

While performing Step 1, if you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

d. Run the PurgeCache utility to clear content related to request datasets from the server cache.

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

e. Import into MDS, the request dataset definitions in XML format.

  See Section 2.3.6.2.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

11. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible.

  See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.
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 (#):

   ```java
   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 in the following directory:
   - For Oracle Identity Manager release 9.1.0.x:
     JavaTasks or ScheduleTask directory
   - For Oracle Identity Manager release 11.1.x:
     Oracle Identity Manager database

   Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:
For Microsoft Windows:

OIM_HOME/server/bin/UploadJars.bat

For UNIX:

OIM_HOME/server/bin/UploadJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

See Also: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager for detailed information about the Upload JARs utility.

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.
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:

   ```java
   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 in the following directory:

      For Oracle Identity Manager release 9.1.0.x:

      Note: This feature cannot be applied to the Locked/Unlocked status attribute of the target system.
JavaTasks or ScheduleTask directory
For Oracle Identity Manager release 11.1.x:
Oracle Identity Manager database
Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

---

**Note:** Before you use this utility, verify that the **WL_HOME** environment variable is set to the directory in which Oracle WebLogic Server is installed.

---

For Microsoft Windows:

```
OIM_HOME/server/bin/UploadJars.bat
```

For UNIX:

```
OIM_HOME/server/bin/UploadJars.sh
```

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

**See Also:** Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for detailed information about the Upload JARs utility

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 in the following directory:
   - For Oracle Identity Manager release 9.1.0.x:
     JavaTasks or ScheduleTask directory
   - For Oracle Identity Manager release 11.1.x:
     Oracle Identity Manager database

Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

```
Note: Before you use this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.
```

For Microsoft Windows:

```
OIM_HOME/server/bin/UploadJars.bat
```

For UNIX:

```
OIM_HOME/server/bin/UploadJars.sh
```

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

**See Also:** Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for detailed information about the Upload JARs utility

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 one of the following guides for detailed information about the steps of this procedure: |
| For Oracle Identity Manager release 9.1.0.x: Oracle Fusion Middleware User’s Guide for Oracle Identity Manager |
| For Oracle Identity Manager release 11.1.x: Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager |

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_CODEKEY;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:

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:
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:
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

<table>
<thead>
<tr>
<th>Connector Object</th>
<th>Name</th>
<th>Referenced By</th>
<th>Comments on Creating a Copy</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT resource</td>
<td>SAP UM IT Resource</td>
<td>SAP User Management User Recon (scheduled task)</td>
<td>Create a copy of the IT resource. See Section 2.3.16, &quot;Configuring the IT Resource&quot; for more information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAP User Management Delete Recon (scheduled task)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAP User Management Lookup Recon (scheduled task)</td>
<td></td>
</tr>
<tr>
<td>Resource object</td>
<td>SAP UM Resource Object</td>
<td>SAP User Management User Recon (scheduled task)</td>
<td>Create copies of the resource object only if there are differences in attributes between the various installations of the target system and if the same user ID exists in different target systems. See Section 3.4.3, &quot;Reconciliation Scheduled Tasks&quot; for more information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAP User Management Delete Recon (scheduled task)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAP User Management Lookup Recon (scheduled task)</td>
<td></td>
</tr>
<tr>
<td>Process definition</td>
<td>SAP UM Process Form</td>
<td>NA</td>
<td>Create copies of this process definition only if there are differences in attributes between the various installations of the target system and if the same user ID exists in different target systems.</td>
</tr>
<tr>
<td>Attribute Mapping Lookup Definition</td>
<td>Lookup.SAP.UM. ProvAttrMap</td>
<td>NA</td>
<td>Create copies of these lookup definition only if you want to map a different set of attributes for the various installations of the target system. See the following sections for more information: Section 1.7, &quot;Connector Objects Used During Reconciliation&quot; Section 1.8, &quot;Connector Objects Used During Provisioning&quot;</td>
</tr>
</tbody>
</table>
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 User Management 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.
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

<table>
<thead>
<tr>
<th>Form</th>
<th>Lookup Field</th>
<th>Oracle Database Query for the Lookup Field</th>
<th>Microsoft SQL Server Query for the Lookup Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD_SPUM_PROFILE</td>
<td>Profile System Name</td>
<td><code>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('$Form data.UD_SAP_ITRESOURCE$','~')</code></td>
<td><code>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)&gt;0</code></td>
</tr>
<tr>
<td>UD_SPUM_PROFILE</td>
<td>Profile Name</td>
<td><code>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('$Form data.UD_SPUM_PRO_SYSTEMNAME$', '~'))&gt;0</code></td>
<td><code>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('$Form data.UD_SPUM_PROFILESYSTEMNAME$' + '~', lkv_encoded)&gt;0</code></td>
</tr>
<tr>
<td>UD_SAPRL ROLE</td>
<td>Role System Name</td>
<td><code>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('$Form data.UD_SAPRL_SYSTEMNAME$', '~'))&gt;0</code></td>
<td><code>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)&gt;0</code></td>
</tr>
<tr>
<td>UD_SAPRL ROLE</td>
<td>Role Name</td>
<td><code>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('$Form data.UD_SAPRL_SYSTEMNAME$', '~'))&gt;0</code></td>
<td><code>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)&gt;0</code></td>
</tr>
<tr>
<td>UD_SAP ROLE</td>
<td>Title</td>
<td><code>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('$Form data.UD_SAP_ITRESOURCE$','~')</code></td>
<td><code>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)&gt;0</code></td>
</tr>
</tbody>
</table>

**Note:** Check with Oracle Support about the bundle patch that addresses Bug 9181280.
<table>
<thead>
<tr>
<th>Form</th>
<th>Lookup Field</th>
<th>Oracle Database Query for the Lookup Field</th>
<th>Microsoft SQL Server Query for the Lookup Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD_SAP</td>
<td>User Group</td>
<td>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($Form data.UD_SAP_ITRESOURCE$,'<del>')))=concat($Form data.UD_SAP_ITRESOURCE$,'</del>')</td>
<td>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)&gt;0</td>
</tr>
<tr>
<td>UD_SAP</td>
<td>Logon Language</td>
<td>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($Form data.UD_SAP_ITRESOURCE$,'<del>')))=concat($Form data.UD_SAP_ITRESOURCE$,'</del>')</td>
<td>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)&gt;0</td>
</tr>
<tr>
<td>UD_SAP</td>
<td>Date Format</td>
<td>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($Form data.UD_SAP_ITRESOURCE$,'<del>')))=concat($Form data.UD_SAP_ITRESOURCE$,'</del>')</td>
<td>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)&gt;0</td>
</tr>
<tr>
<td>UD_SAP</td>
<td>Decimal Notation</td>
<td>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($Form data.UD_SAP_ITRESOURCE$,'<del>')))=concat($Form data.UD_SAP_ITRESOURCE$,'</del>')</td>
<td>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)&gt;0</td>
</tr>
<tr>
<td>UD_SAP</td>
<td>Time Zone</td>
<td>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($Form data.UD_SAP_ITRESOURCE$,'<del>')))=concat($Form data.UD_SAP_ITRESOURCE$,'</del>')</td>
<td>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)&gt;0</td>
</tr>
</tbody>
</table>
### Table 4–2 (Cont.) SQL Queries for Lookup Fields

<table>
<thead>
<tr>
<th>Form</th>
<th>Lookup Field</th>
<th>Oracle Database Query for the Lookup Field</th>
<th>Microsoft SQL Server Query for the Lookup Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD_SAP</td>
<td>Company</td>
<td>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('$Form data.UD_SAP_ITRESOURCE$','<del>'))) = concat('$Form data.UD_SAP_ITRESOURCES$','</del>'))</td>
<td>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('$Form data.UD_SAP_ITRESOURCES$' + '~~', lkv_encoded) &gt; 0</td>
</tr>
<tr>
<td>UD_SAP</td>
<td>Contractual User Type</td>
<td>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('$Form data.UD_SAP_ITRESOURCE$','<del>'))) = concat('$Form data.UD_SAP_ITRESOURCES$','</del>'))</td>
<td>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('$Form data.UD_SAP_ITRESOURCES$' + '~~', lkv_encoded) &gt; 0</td>
</tr>
<tr>
<td>UD_SAP</td>
<td>Communication Type</td>
<td>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('$Form data.UD_SAP_ITRESOURCE$','<del>'))) = concat('$Form data.UD_SAP_ITRESOURCES$','</del>'))</td>
<td>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('$Form data.UD_SAP_ITRESOURCES$' + '~~', lkv_encoded) &gt; 0</td>
</tr>
<tr>
<td>UD_SAP</td>
<td>Language Communication</td>
<td>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('$Form data.UD_SAP_ITRESOURCE$','<del>'))) = concat('$Form data.UD_SAP_ITRESOURCES$','</del>'))</td>
<td>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('$Form data.UD_SAP_ITRESOURCES$' + '~~', lkv_encoded) &gt; 0</td>
</tr>
<tr>
<td>UD_SAP_PRO_0</td>
<td>Profile System Name</td>
<td>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('$Form data.UD_SAP_O_ITRESOURCE$','<del>'))) = concat('$Form data.UD_SAP_O_ITRESOURCES$','</del>'))</td>
<td>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('$Form data.UD_SAP_O_ITRESOURCES$' + '~~', lkv_encoded) &gt; 0</td>
</tr>
<tr>
<td>UD_SAP_PRO_0</td>
<td>Profile Name</td>
<td>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('$Form data.UD_SPUM_PRO_0_SYSTEMNAME$','~')) &gt; 0</td>
<td>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('$Form data.UD_SPUM_PRO_0_SYSTEMNAME$' + '~~', lkv_encoded) &gt; 0</td>
</tr>
</tbody>
</table>
### Table 4–2 (Cont.) SQL Queries for Lookup Fields

<table>
<thead>
<tr>
<th>Form</th>
<th>Lookup Field</th>
<th>Oracle Database Query for the Lookup Field</th>
<th>Microsoft SQL Server Query for the Lookup Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD_SAPRL_O Role System Name</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.System' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SAPRL_O_SYSTEMNAME$','<del>')))=concat('$Form data.UD_SAPRL_O_ITRESOURCES$','</del>')</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.System' and CHARINDEX('$Form data.UD_SAPRL_O_SYSTEMNAME$ + '~', lkv_encoded)&gt;0</td>
<td></td>
</tr>
<tr>
<td>UD_SAPRL_O Role Name</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.Roles' and instr(lkv_encoded, concat('$Form data.UD_SAPRL_O_SYSTEMNAME$','~'))&gt;0</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.Roles' and CHARINDEX('$Form data.UD_SAPRL_O_SYSTEMNAME$ + '~', lkv_encoded)&gt;0</td>
<td></td>
</tr>
<tr>
<td>UD_SAP_O Title</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.UserTitle' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SAP_O_ITRESOURCES$','<del>')))=concat('$Form data.UD_SAP_O_ITRESOURCES$','</del>')</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.UserTitle' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCES$ + '~', lkv_encoded)&gt;0</td>
<td></td>
</tr>
<tr>
<td>UD_SAP_O User Group</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.UserGroups' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SAP_O_ITRESOURCES$','<del>')))=concat('$Form data.UD_SAP_O_ITRESOURCES$','</del>')</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.UserGroups' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCES$ +('~', lkv_encoded)&gt;0</td>
<td></td>
</tr>
<tr>
<td>UD_SAP_O Logon Language</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.LangComm' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SAP_O_ITRESOURCES$','<del>')))=concat('$Form data.UD_SAP_O_ITRESOURCES$','</del>')</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.LangComm' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCES$ +('~', lkv_encoded)&gt;0</td>
<td></td>
</tr>
<tr>
<td>UD_SAP_O Date Format</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.DateFormat' and substr(lkv_encoded, 1, length(concat('$Form data.UD_SAP_O_ITRESOURCES$','<del>')))=concat('$Form data.UD_SAP_O_ITRESOURCES$','</del>')</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAPUUM.DateFormat' and CHARINDEX('$Form data.UD_SAP_O_ITRESOURCES$ +('~', lkv_encoded)&gt;0</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4–2 (Cont.) SQL Queries for Lookup Fields

<table>
<thead>
<tr>
<th>Form</th>
<th>Lookup Field</th>
<th>Oracle Database Query for the Lookup Field</th>
<th>Microsoft SQL Server Query for the Lookup Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD_SAP_O</td>
<td>Decimal Notation</td>
<td><code>select lkv_encoded, lkv_decoded from lkv 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_ITRESOURCES$','~')))=concat('Form data.UD_SAP_O_ITRESOURCES$','~')</code></td>
<td><code>select lkv_encoded, lkv_decoded from lkv where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.DecimalNotation' and CHARINDEX('Form data.UD_SAP_O_ITRESOURCES$' + '~', lkv_encoded)&gt;0</code></td>
</tr>
<tr>
<td></td>
<td>Time Zone</td>
<td><code>select lkv_encoded, lkv_decoded from lkv where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.TimeZone' and substr(lkv_encoded,1,length(concat('Form data.UD_SAP_O_ITRESOURCES$','~')))=concat('Form data.UD_SAP_O_ITRESOURCES$','~')</code></td>
<td><code>select lkv_encoded, lkv_decoded from lkv where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.TimeZone' and CHARINDEX('Form data.UD_SAP_O_ITRESOURCES$' + '~', lkv_encoded)&gt;0</code></td>
</tr>
<tr>
<td></td>
<td>Company</td>
<td><code>select lkvEncoded, lkvDecoded from lkv 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_ITRESOURCES$','~')))=concat('Form data.UD_SAP_O_ITRESOURCES$','~')</code></td>
<td><code>select lkvEncoded, lkvDecoded from lkv where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.Company' and CHARINDEX('Form data.UD_SAP_O_ITRESOURCES$' + '~', lkv_encoded)&gt;0</code></td>
</tr>
<tr>
<td></td>
<td>Contractual User Type</td>
<td><code>select lkvEncoded, lkvDecoded from lkv where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.ContractualUserType' and substr(lkv_encoded,1,length(concat('Form data.UD_SAP_O_ITRESOURCES$','~')))=concat('Form data.UD_SAP_O_ITRESOURCES$','~')</code></td>
<td><code>select lkvEncoded, lkvDecoded from lkv where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.ContractualUserType' and CHARINDEX('Form data.UD_SAP_O_ITRESOURCES$' + '~', lkv_encoded)&gt;0</code></td>
</tr>
<tr>
<td></td>
<td>Communication Type</td>
<td><code>select lkvEncoded, lkvDecoded from lkv 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_ITRESOURCES$','~')))=concat('Form data.UD_SAP_O_ITRESOURCES$','~')</code></td>
<td><code>select lkvEncoded, lkvDecoded from lkv where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.SAP.UM.CommType' and CHARINDEX('Form data.UD_SAP_O_ITRESOURCES$' + '~', lkv_encoded)&gt;0</code></td>
</tr>
</tbody>
</table>
Table 4–2 (Cont.) SQL Queries for Lookup Fields

<table>
<thead>
<tr>
<th>Form</th>
<th>Lookup Field</th>
<th>Oracle Database Query for the Lookup Field</th>
<th>Microsoft SQL Server Query for the Lookup Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD_SAP_O</td>
<td>Language Communication</td>
<td>select lkv_encoded, lkv_decoded from lkv. lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.UD.SAP_O.LangComm' and substr(lkv_encoded, 1, length(concat('UD_SAP_O_ITRESOURCES', '<del>')))=concat('UD_SAP_O_ITRESOURCES', '</del>')</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.M.LangComm' and CHARINDEX('UD_SAP_O_ITRESOURCES' + '~', lkv_encoded)&gt;0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD_SPUMRC_O</td>
<td>Role System Name</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.UD.SPUMRC_O.SYSTEM' and substr(lkv_encoded, 1, length(concat('UD_SPUMRC_O_SERVER', '<del>')))=concat('UD_SPUMRC_O_SERVER', '</del>')</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.M.System' and CHARINDEX('UD_SPUMRC_O_SERVER' + '~', lkv_encoded)&gt;0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD_SPUMRC_P</td>
<td>Profile System Name</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.UD.SPUMPC_O.SYSTEM' and substr(lkv_encoded, 1, length(concat('UD_SPUMPC_O_SERVER', '<del>')))=concat('UD_SPUMPC_O_SERVER', '</del>')</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.M.System' and CHARINDEX('UD_SPUMPC_O_SERVER' + '~', lkv_encoded)&gt;0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD_SPUMPC_O</td>
<td>Profile Name</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.UD.SPUMPC_O.PROFILE' and instr(lkv_encoded, concat('UD_SPUMPC_O_SYSTEMNAMES', '~'))&gt;0</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.M.Profile' and CHARINDEX('UD_SPUMPC_O_SYSTEMNAMES' + '~', lkv_encoded)&gt;0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD_SPUMRC_P</td>
<td>User Role</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.UD.SPUMRC_P.SYSTEM' and substr(lkv_encoded, 1, length(concat('UD_SPUMRC_P_SERVER', '<del>')))=concat('UD_SPUMRC_P_SERVER', '</del>')</td>
<td>select lkv_encoded, lkv_decoded from lkv lkv where lkv.lku_key=lku.lku_key and lkv_type_string_key='Lookup.SAPU.M.System' and CHARINDEX('UD_SPUMRC_P_SERVER' + '~', lkv_encoded)&gt;0</td>
</tr>
</tbody>
</table>

4-70 Oracle Identity Manager Connector Guide for SAP User Management
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**.
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.

- **Bug 9797993**
  
  On Oracle Identity Manager release 11.1.1, the SAP CUP Delete Recon scheduled task does not work.

- **Bug 9759483**
  
  The following issue is observed when you perform a request-based provisioning operation on Oracle Identity Manager release 11.1.1:

  In the Role Name lookup field or Profile Name lookup field, the results displayed when you search for a role or profile do not show descriptions (Decode values) of the roles or profiles. Only Code Key values are displayed.

- **Bug 10361925**
  
  The Compliant User Provisioning feature of the connector does not work if Oracle Identity Manager is running on IBM WebSphere Application Server.

- **Bug 13429841**
  
  **Limitation:**

  Whenever any jar is updated/modified, if application server is not restarted then it will throw the following error:

  ```java
  java.lang.UnsatisfiedLinkError: Native Library /usr/local/jco/libsapjco3.so
  java.lang.UnsatisfiedLinkError: Native Library /usr/local/jco/libsapjco3.dll
  ```
already loaded in another classloader. It is limitation from SAP JCO.

Analysis:
Whenever any jar is updated/modified, the application server tries to register SAP
destination data provider (SAP JCO) even though it is already registered.
Therefore the application server throws an error.

Workaround:
Restart the application server if any jar is updated or modified in Oracle Identity
Manager server.
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
A  additional files, 1-3
  Administrative and User Console, 2-32, 2-48, 2-52
  architecture, 1-4
  attributes, adding new, 4-7

B  BAPIF4T table, 2-23
  BAPIs, 1-5, 1-9, 1-18, 3-13, 4-2, 4-3, 4-11, 4-27, 4-43, 4-49, 4-51, 4-58, A-1
  batched reconciliation, 1-15, 3-5, 3-6

C  certified components, 1-1
  certified languages, 1-3
  changing input locale, 2-39
  clearing server cache, 2-40
  Compliant User Provisioning feature, 1-3, 1-6, 1-8, 1-10, 1-11, 1-12, 1-14, 1-20, 1-21, 1-22, 1-30, 2-2, 2-3, 2-29, 2-30, 2-47, 3-6, 3-7, 3-8, 3-11, 3-37, 4-25
  components, certified, 1-1
  configuring
    target system, 2-22
    configuring connector, 3-1
  connection pooling, 1-16, 2-85, 2-87, 2-90, 5-1
  connector architecture, 1-4
  connector features, 1-12
  connector files and directories, 2-1
  connector functionality, extending, 4-1
  Connector Installer, 2-14
  connector release number, determining, 2-3
  connector, configuring, 3-1
  custom multivalued target system attributes, 4-13, 4-44
  custom target system attributes, 1-13, 4-7, 4-39

D  dependent lookup fields, 4-64
  determining release number of connector, 2-3
  direct provisioning, 1-4, 1-6, 1-7, 1-8, 2-14, 2-32, 2-33, 2-49, 2-51, 2-52, 3-12, 3-13
  disabling accounts, 1-15, 1-28

E  enabling accounts, 1-15, 1-28
  enabling logging, 2-41
  exclusion list, 1-16, 1-20, 2-29, 2-46
  extending connector functionality, 4-1
  external code files, 1-3

F  features of connector, 1-12
  field mappings, 4-61
  files
    additional, 1-3
    external code, 1-3
  See also XML files
  filtered reconciliation, 1-15, 3-3
  full reconciliation, 1-14, 3-3

G  globalization features, 1-3

I  incremental reconciliation, 1-14, 3-3
  input locale, changing, 2-39
  installation, 2-14
  installing connector, 2-1, 2-14
  issues, 5-1
  IT resources, 2-83
  IT resources, parameters, 2-83

L  limitations, 5-1
  limited reconciliation, 1-15, 3-3
  logging enabling, 2-41
  login group, 1-17, 2-84
  lookup field synchronization, 1-17, 1-20, 3-2
  lookup fields, 1-17, 1-20, 3-2
  Lookup.SAP.CUA.LookupMappings, 1-18, 1-21, 2-46, 3-2, 3-35, 4-58
  Lookup.SAP.CUP.Configuration, 1-20, 2-29, 2-59, 2-66
  Lookup.SAP.CUP.Constants, 1-20, 2-83
  Lookup.SAP.CUP.ProvisionAttrMap, 1-9, 1-21, 2-68
Lookup.SAP.CUP.ProvisionRoleAttrMap, 1-9, 1-22, 1-30, 2-66
Lookup.SAP.UM.CommType, 1-18, 4-67, 4-69
Lookup.SAP.UM.Company, 1-18, 4-67, 4-69
Lookup.SAP.UM.Configuration, 1-15, 1-16, 1-20, 2-26, 2-28, 2-58, 2-88, 3-7, 3-35, 3-37, 4-54, 4-56, 4-57
Lookup.SAP.UM.Constants, 1-20, 2-29
Lookup.SAP.UM.ContractualUserType, 1-18, 2-47, 4-67, 4-69
Lookup.SAP.UM.CustomAttrMap, 1-23, 2-29, 4-7, 4-11
Lookup.SAP.UM.CustomChildAttrMap, 1-22
Lookup.SAP.UM.DateFormat, 1-18, 4-66, 4-68
Lookup.SAP.UM.DecimalNotation, 1-18, 4-66, 4-69
Lookup.SAP.UM.ExclusionList, 1-20, 2-29, 2-46
Lookup.SAP.UM.ITResourceMapping, 1-21, 2-30, 2-85, 2-86, 5-1
Lookup.SAP.UM.LangComm, 1-18
Lookup.SAP.UM.LookupMappings, 1-18, 1-21, 2-46, 3-2, 4-58
Lookup.SAP.UM.LookupReconTransformation, 1-21, 2-30, 2-92, 4-57
Lookup.SAP.UM.Parameter, 1-18
Lookup.SAP.UM.Profile, 1-18, 2-47, 4-65, 4-67, 4-70, 4-71
Lookup.SAP.UM.ProfileChildformMappings, 1-23, 2-70
Lookup.SAP.UM.ProvAttrMap, 1-21, 1-28, 2-30, 4-19, 4-21, 4-28
Lookup.SAP.UM.ProvCheckBoxMapping, 1-22, 2-29, 4-19, 4-21, 4-41
Lookup.SAP.UM.ProvChildAttrMap, 1-21, 1-29, 2-30, 4-2, 4-31, 4-32, 4-45, 4-46
Lookup.SAP.UM.ProvValidation, 1-22, 2-31, 4-54
Lookup.SAP.UM.ReconAttrMap, 1-22, 1-23, 3-3, 3-4, 3-5, 4-2, 4-7, 4-10
Lookup.SAP.UM.ReconCheckBoxMapping, 1-22, 2-29, 4-7, 4-12, 4-39
Lookup.SAP.UM.ReconChildAttrMap, 1-22, 1-24, 3-5, 4-2, 4-13, 4-17
Lookup.SAP.UM.ReconTransformation, 2-30, 4-56
Lookup.SAP.UM.ReconTransformationtransformatio n, 1-23
Lookup.SAP.UM.ReconValidation, 1-23, 2-31, 4-54
Lookup.SAP.UM.RoleChildformMappings, 1-22, 2-71
Lookup.SAP.UM.Roles, 1-18, 2-47, 4-65, 4-68, 4-70, 4-71
Lookup.SAP.UM.SoDConfiguration, 1-23, 2-69, 2-89
Lookup.SAP.UM.System, 1-18, 2-70, 2-72, 4-65, 4-67, 4-68, 4-70, 4-71
Lookup.SAP.UM.TimeZone, 1-19, 4-66, 4-69
Lookup.SAP.UM.UserGroups, 1-19, 4-66, 4-68
Lookup.SAP.UM.UserTitle, 1-19, 4-65, 4-68

M
multilanguage support, 1-3
multivalued attributes, 4-13

O
Oracle Identity Manager Administrative and User Console, 2-32, 2-48, 2-52
Oracle Identity Manager certified releases, 1-2

P
parameters of IT resources, 2-83
password field, 1-9, 1-16, 1-28, 1-29, 2-28, 2-29, 2-30, 2-58, 2-88
postinstallation, 2-17
preinstallation, 2-1
provisioning, 3-25
direct provisioning, 3-15
fields, 1-27
identity fields, 1-28
module, 1-27
provisioning triggered by policy changes, 3-12
request-based, 3-12
request-based provisioning, 2-31, 2-51
user provisioning, 1-27
user provisioning functions, 1-27

R
reconciliation, 1-1, 1-23, 1-26
adding new attributes, 4-7
batched, 1-15
full, 1-14, 3-3
incremental, 1-14, 3-3
reconciliation action rules, 1-26
reconciliation rule, 1-25
reconciliation, user attributes, 1-23
release number of connector, determining, 2-3
request-based provisioning, 1-4, 1-6, 1-7, 1-8, 2-3, 2-14, 2-31, 2-32, 2-33, 2-35, 2-49, 2-51, 2-52, 2-55, 2-87, 3-12, 3-26

S
SAP CUA, 1-1, 1-2, 1-4, 1-12, 1-13, 1-15, 1-19, 2-26, 2-29, 2-69, 2-89, 2-90, 3-2, 3-35
SAP GRC, 1-13, 2-68, 3-13, 3-21
SAP GRC Compliant User Provisioning, 1-3, 1-6, 1-8, 1-10, 1-11, 1-12, 1-14, 2-47, 3-7, 4-25
SAP GRC Risk Analysis and Remediation, 1-3, 1-6, 1-8, 1-10, 1-11, 2-68, 2-89
SAP GRC, configuring, 2-68
SAP HRMS, 1-12, 1-15, 1-28, 2-26, 2-30
SAP JCo, 1-3, 1-16, 1-21, 2-12, 2-30, 2-80, 2-84, 2-85
scheduled tasks
defining, 3-8
user reconciliation, 3-4
server cache, clearing, 2-40
SNC, 1-15, 2-22, 2-80
configuring, parameters, 2-82
prerequisites, 2-81
security package, installing, 2-81
SoD engine, 2-68
SoD feature, 1-3, 1-6, 1-8, 1-10, 1-11, 1-13, 1-22, 1-23, 2-68, 2-69, 2-89, 2-90, 3-12, 3-35, 3-37
SoD-enabled environment, 3-13, 3-26
direct provisioning, 3-13
provisioning process, overview, 3-13
request-based provisioning, 3-26
SSL, configuring for SoD validation, 2-58, 2-72
standard multivalued target system attributes, 4-13, 4-31
standard target system attributes, 1-13, 4-1, 4-7, 4-11, 4-12, 4-19

T
target resource reconciliation, 1-23
 multivalued attributes, 4-13
 reconciliation action rules, 1-26
target system user account, 2-5
target system, multiple installations, 4-62
target systems
 configuration, 2-22
target systems, certified, 1-2
transformation, 1-17, 2-30, 2-31, 4-54, 4-56
transport request
 creating, 2-23
 importing, 2-23

U
user reconciliation scheduled task, 3-4

V
validation, 1-17, 1-23, 4-52