Oracle® Identity Manager

Connector Guide for SAP User Management

11.1.1

E29159-20

February 2021

Oracle Identity Manager Connector Guide for SAP User Management, 11.1.1

E29159-20

Primary Author: Gowri.G.R

Contents

Preface

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

1 About the Connector

2 Deploying the Connector

3 Using the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to onboard SAP User Management and SAP Access Control User Management applications to Oracle Identity Governance.

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 that have purchased support 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, visit the following Oracle Help Center page:

`http://docs.oracle.com/cd/E52734_01/index.html`

For information about Oracle Identity Manager Connectors documentation, visit the following Oracle Help Center page:

`http://docs.oracle.com/cd/E22999_01/index.htm`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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

This chapter provides an overview of the updates made to the software and documentation for release 11.1.1.7.0 of the SAP User Management connector.

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

- Software Updates

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

- Documentation-Specific Updates

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

Software Updates

The following section discusses software updates:

- Software Updates in Release 11.1.1.7.0
- Software Updates in Release 11.1.1.6.0
- Software Updates in Release 11.1.1.5.0

Software Updates in Release 11.1.1.7.0

There are no software updates in this release of the connector.

Software Updates in Release 11.1.1.6.0

The following are issues resolved in release 11.1.1.6.0:

Bug Number	Issue	Resolution
17388531	Account and role provisioning works fine without configuring the connector server.However, provisioning a role fails when the connector server is configured.	This issue has been resolved.
17575026	Failure of child data reconciliation during a reconciliation operation.	This issue has been resolved.

Bug Number	Issue	Resolution
17581363	Failure in updation of the SAP User Management Unique ID in the process form.	This issue has been resolved.
17642440	Missing few Users created during different times of the same day during reconciliation operation.	This issue has been resolved.
17911657	In non CUA mode, SAP role reconciliation is omitting composite roles.	This issue has been resolved.
17288932	SSL support for SAP GRC 5.3	This issue has been resolved.
18461406	When the CUA mode is enabled and a role lookup reconciliation is performed, roles are reconciled with English labels instead of French labels.	This issue has been resolved.
19078269	Unable to connect to SAP in load balance scenario. However, connection to concrete SAP is successful.	This issue has been resolved.
16506322	The task responses are displayed only in English even when the connector is configured for any other native language.	This issue has been resolved.
18815353	"Display" and "Help" label descriptions are not displayed appropriately.	This issue has been resolved.
17748964	AC: SAP User Management unique Id does not get updated in the process form.	This issue has been resolved.
17668632	Failure in updation of SoDCheckResult due to an issue with field label mapping.	This issue has been resolved.
17401315	During user reconciliation in SAP User Management, two resource objects are created for the same account in Oracle Identity Manager.	This issue has been resolved.
19620263	Performing a Remove Role operation on Oracle Identity Manager does not remove simple roles associated to composite roles.	This issue has been resolved.
18342752	When a User from CUA is disabled and re-enabled in Oracle Identity Manager, the User is still displayed as disabled in SAP.	This issue has been resolved.
19551686	SAP User Management reconciliation finds modified Users only once in every three reconciliation operations.	This issue has been resolved.

Software Updates in Release 11.1.1.5.0

This is the first release of the Oracle Identity Manager Connector for SAP User Management based on Identity Connector Framework (ICF). The following are the software updates in release 11.1.1.5.0:

- Support for SAP BusinessObjects Access Control Version 10
- ICF Based Connector
- Support for Connector Server

- Support for Connection Pooling
- Support for Transformation and Validation
- Support for Resource Exclusion Lists

Support for SAP BusinessObjects Access Control Version 10

From this release onward, the connector supports the following new components:

- Risk Analysis and Remediation, also known as Analyze and Manage Access Risk (AMAR)
- Compliant User Provisioning, also known as Provision and Manage Users (PMU)

Throughout this guide, SAP BusinessObjects AC Access Risk Analysis refers to Risk Analysis and Remediation and SAP BusinessObjects AC Access Request Management refers to Compliant User Provisioning.

ICF Based Connector

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager and Oracle Waveset connectors require.

The Oracle Identity Manager Connector for SAP User Management is an ICF-based connector. The ICF uses classpath isolation, which allows the SAP User Management connector to co-exist with legacy versions of the connector.

For more information about the ICF, see Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

Support for Connector Server

Connector Server is a component provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally-deployed bundles. In other words, a connector server enables remote execution of an Oracle Identity Manager connector.

See the following sections for more information:

- Installing and Configuring the Connector Server
- Installing the Connector in the Connector Server

Support for Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. 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 will be created, one for each target system installation.

See Setting up the Lookup Definition for Connection Pooling for more information.

Support for Transformation and Validation

You can configure transformation of data, such as process form field data or any other object, that is brought into Oracle Identity Manager during reconciliation. In addition, you can configure validation of data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning.

See the following sections for more information:

- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During User Reconciliation

Support for Resource Exclusion Lists

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

See Validation Groovy Script for Resource Exclusion in *Oracle Fusion Middleware Performing Self Service Tasks for Oracle Identity Manager* for more information.

Documentation-Specific Updates

The following section discusses documentation-specific updates:

- Documentation-Specific Updates in Release 11.1.1.7.0
- Documentation-Specific Updates in Release 11.1.1.6.0
- Documentation-Specific Updates in Release 11.1.1.5.0

Documentation-Specific Updates in Release 11.1.1.7.0

The following documentation-specific updates have been made in revision "20" of the guide:

The "Target systems" and "SAP Governance, Risk and Compliance Access Control (GRC AC)" rows of Table 1-1 have been updated.

The following documentation-specific updates have been made in revision "19" of the guide:

- Information about Oracle Identity Governance cluster has been added to Table 1-2, Table 1-6, and Enabling Logging.
- Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System has been updated.
- Postcloning Steps has been added.

The following documentation-specific update has been made in revision "18" of the guide:

The "Target systems" and "SAP Governance, Risk and Compliance Access Control (GRC AC)" rows of Table 1-1 have been updated.

The following documentation-specific updates have been made in revision "17" of the guide:

- Creating a Target System User Account for the SAP HR Target has been updated.
- Assigning Roles to a User Account in a SAP Business Objects Access Control System for Connector Operations has been updated.
- The FAQs section under Known Issues has been updated to include information about the SoD Check Tracking ID field.

The following documentation-specific updates have been made in revision "16" of the guide:

- The following updates have been made to Table 1-1:
  - The "Oracle Identity Governance or Oracle Identity Manager" row has been updated to include support for Oracle Identity Governance 12*c* (12.2.1.4.0).
  - The "Target Systems" row has been modified to include support for SAP S/ 4HANA 1809 with component S4CORE 103 SP 0000.
  - The "SAP Governance, Risk and Compliance Access Control (GRC AC)" row has been modified to include support for the following installations:
    - SAP BusinessObjects Access Control 12.0 on SAP NetWeaver 7.52 for S/4 HANA 1610 with SAPBASIS 752 with component GRCFND_A V1200 SP 03 NetWeaver 7.52 with plugin GRCPINWV1100_731 SP 20
    - SAP BusinessObjects Access Control 10.1 on SAP NetWeaver 7.52 for S/4 HANA 1610 with SAPBASIS 7.52 with component GRCFND_A V1100 SP 19 NetWeaver 7.52 with plugin GRCPINWV1100_731 SP 20
- Usage Recommendation has been modified to include support for Oracle Identity Governance 12*c* (12.2.1.4.0).
- The following steps have been modified:
  - Step 3 of Creating a Target System User Account for the SAP UM (SAP ERP or SAP CUA) Target
  - Step 1 of Installing the Security Package
  - Step 3.b of Configuring SNC
  - Step 4 of Downloading and Installing the SAP JCo
  - Step 2 of Installing the Connector in the Connector Server
- A "Note" regarding entitlements has been added to SoD Validation of Entitlement Requests.
- Information pertaining to 12*c* has been modified in Usage Recommendation.
- Title for Support for SAP Governance, Risk, and Compliance Version 10 or Later has been updated.
- The Description column for the wsdlFilePath row of Table 1-2 and Table 1-6 have been modified.
- A "Note" regarding cluster setup has been added to Step 6 of Downloading and Installing the SAP JCo.
- Installing the Connector in Oracle Identity Manager has been modified.

- Information pertaining to the Filter attribute has been removed from Table 3-4.
- A guideline regarding the SAP BusinessObjects Access version has been added to Frequently Asked Questions (FAQs).
- Table 3-5, Table 3-6, and Table 3-7 have been modified.

The following documentation-specific updates have been made in revision "15" of the guide:

- The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been modified to include support for Oracle Identity Governance 12*c* Release BP02 (12.2.1.3.2).
- The "Target Systems" row of Table 1-1 has been modified to include support for NetWeaver 7.51 and S/4 HANA.
- The "Connector Server" row of Table 1-1 has been modified to include support for 11.2.1.0 and 12.2.1.3.0.
- The "SAP Governance, Risk and Compliance Access Control (GRC AC)" row of Table 1-1 has been modified to include support for the following:
  - SAP BusinessObjects Access Control 10 on SAP NetWeaver 7.4 with SAP BASIS 7.40
  - SAP BusinessObjects Access Control 10 on SAP NetWeaver AS ABAP 7.02 Support Pack 7
- Usage Recommendation has been modified to include information about 12*c*.
- Support for SAP Governance, Risk, and Compliance Version 10 or Later has been modified to include connector support for new components.
- Code Key "ReportFormat" has been added to Table 1-6.
- Summary of the account management process has been added to User Management with SoD.
- Creating a Target System User Account for the SAP UM (SAP ERP or SAP CUA) Target has been modified.
- Step 2 has been added to Performing the Postupgrade Steps.
- Postupgrade Steps While Upgrading the SAP BusinessObjects AC Access Request Management from Release 11.1.1.6.0 to Release 11.1.1.7.0 has been added.
- A known issue and a workaround about an application server error whenever any jar is updated or modified is added to Known Issues.
- Troubleshooting the Connector has been added.

The following documentation-specific update has been made in revision "14" of the guide:

- The "Oracle Identity Manger" row of Table 1-1 has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and also updated for Oracle Identity Governance 12*c* (12.2.1.3.0) certification.

The following documentation-specific updates have been made in revision "13" of the guide:

- OIM interface names have been corrected throughout the guide.

- Information pertaining to procedures performed on the target system has been replaced with a high-level summary in the following sections:
  - Creating a Target System User Account for the SAP UM (SAP ERP or SAP CUA) Target
  - Creating a Target System User Account for the SAP HR Target
  - Creating an Entry in the BAPIF4T Table
  - Configuring Request Types and Workflows on SAP BusinessObjects AC Access Request Management
  - Downloading WSDL files from SAP BusinessObjects AC
  - Determining the Names of Target System Attributes

The following documentation-specific update has been made in revision "12" of the guide:

The "Oracle Identity Manager" row of Table 1-1 has been updated.

The following documentation-specific updates have been made in revision "10" of the guide:

- The "JDK" and "SAP Governance, Risk and Compliance Access Control (GRC AC)" rows of Table 1-1 have been updated.
- Information pertaining to SAP BusinessObjects Access Control 5.3 has been removed throughout the guide.
- Information pertaining to SAP BusinessObjects Access Control 10 artifacts has been added throughout the guide.
- Known Issues and FAQs has been modified to remove all bugs that are no longer issues.
- Standard BAPIs Used During Connector Operations has been added.

Documentation-Specific Updates in Release 11.1.1.6.0

The following documentation-specific updates have been made in revision "8" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of Table 1-1 has been updated.
- Information specific to Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) has been added to Usage Recommendation.

The following documentation-specific updates have been made in revision "7" of release 11.1.1.6.0:

- The "Target systems" row of Table 1-1 has been updated.
- A "Note" has been added at the beginning of Extending the Functionality of the Connector .
- A "Note" regarding field length has been added to Postinstallation.
- Step 5 of Performing the Postupgrade Steps has been removed.
- An issue regarding connector upgrade has been added to Known Issues.

The following documentation-specific updates have been made in revision "6" of release 11.1.1.6.0:

- A "Note" on SAP NetWeaver 7.31 certified connector version has been modified in Table 1-1.
- The "Connector Server" row has been added to Table 1-1.
- In Table 1-2, the following rows have been added:
  - singleRoles
  - compositeRoles
  - disableLockStatus
  - roles
- In Table 1-8, the following rows have been modified:
  - AC Request
  - Unique ID
- In Table 1-10, the "Unique ID" row has been added.
- The connector version has been modified from "11.1.1.5.0" to "11.1.1.6.0" in the following Sections:
  - Steps 3 and 4 of Downloading and Installing the SAP JCo
  - Steps 2 and 3 of Installing the Connector in Oracle Identity Manager
  - Upgrading the Connector
- Synchronizing the SAPUM Process Form Field Length Needs with the Target Field Length has been added.
- Step 3 has been added to Installing the Connector in the Connector Server.
- Steps 1 and 2 have been added to Performing the Postupgrade Steps.

Documentation-Specific Updates in Release 11.1.1.5.0

- The following documentation-specific update has been made in the revision "5" of release 11.1.1.5.0:

  Configuring Password Changes for Newly Created Accounts has been modified.
- The following documentation-specific update has been made in the revision "4" of release 11.1.1.5.0:

  has been modified.
- The following documentation-specific update has been made in the revision "3" of release 11.1.1.5.0:

  The "Target System" and "GRC AC" rows of Table 1-1 have been updated.
- The following documentation-specific updates have been made in the revision "2" of release 11.1.1.5.0:
  - The "destination" and "masterSystem" rows of Table 2-5 have been updated.
  - The "Oracle Identity Manager" row of Table 1-1 has been modified to include Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0).
  - Information specific to Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) has been added to Step 5 of Localizing Field Labels in UI Forms.

1
About the Connector

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

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

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

This chapter contains the following sections:

- Certified Components
- Usage Recommendation
- Certified Languages
- Connector Architecture and Supported Deployment Configurations
- Features of the SAP UM Connector
- Lookup Definitions Used During Connector Operations
- Connector Objects Used During Target Resource Reconciliation
- Connector Objects Used During Provisioning
- Roadmap for Deploying and Using the Connector

1.1 Certified Components

These are the software components and their versions required for installing and using the connector.

Table 1-1 lists certified components for the connector.

Table 1-1 Certified Components

Component	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.2) and any later BP in this release track • Oracle Identity Manager 11*g* Release 1 PS1 BP07 (11.1.1.5.7) with patch 16627402 and any later BP in this release track • Oracle Identity Manager 11*g* Release 1 PS2 BP01 (11.1.1.7.1) and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 BP05 (11.1.2.0.5) with patch 16627415 and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 PS1 (11.1.2.1.0) and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) and any later BP in this release track

Table 1-1 (Cont.) Certified Components

Component	Requirement
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." • SAP NetWeaver 7.0 with SAP BASIS 7.00 and SAP Business Suite release: BS 2005 with the following constituents: SAP ERP 6.0 (EHP2 and EHP3) SAP CRM 5.0, 6.0) SAP SRM 5.0, 6.0 SAP SCM 5.0, 5.1 • SAP NetWeaver 7.0 EHP1 with SAP BASIS 7.01 and SAP Business Suite release: BS 2007 with the following constituents: SAP ERP 6.0 EHP 4 (EHP 4) SAP CRM 7.0 SAP SRM 7.0 SAP SCM 7.0 • SAP NetWeaver 7.0 EHP2 with SAP BASIS 7.02 and SAP Business Suite release: BS 7i 2010 with the following constituents: SAP ERP 6.0 EHP 5 (EHP 5) SAP CRM 7.0 EHP1 SAP SRM 7.0 EHP1 SAP SCM 7.0 EHP1 • SAP NetWeaver 7.0 EHP3 with SAP BASIS 7.31 and SAP Business Suite release: BS 7i 2011 with the following constituents: SAP ERP 6.0 EHP 6 (EHP 6) SAP CRM 7.0 EHP2 SAP SRM 7.0 EHP2 SAP SCM 7.0 EHP2 **Note:** SAP NetWeaver 7.31 Certified Connector Version is SAP UM 11.1.1.6.0 or later. • SAP NetWeaver 7.31 with SAP BASIS 7.31 and SAP Business Suite release: BS 7i 2011 with the following constituents: SAP ERP 6.0 EHP 6 SAP CRM 7.0 EHP2 SAP SRM 7.0 EHP2 SAP SCM 7.0 EHP2 • SAP NetWeaver 7.4 with SAP BASIS 7.40 and SAP Business Suite release: BS 7i 2013 with the following constituents: SAP Enhancement Package 7 for SAP ERP 6.0 SAP Enhancement Package 3 for SAP CRM 7.0 SAP Enhancement Package 3 for SAP SRM 7.0 SAP Enhancement Package 3 for SAP SCM 7.0 • SAP NetWeaver 7.5 with SAP BASIS 7.50 and SAP Business Suite release: BS 7i 2016 with the following constituents: SAP Enhancement Package 8 for SAP ERM 6.0 SAP Enhancement Package 4 for SAP CRM 7.0

Table 1-1   (Cont.) Certified Components

Component	Requirement
	SAP Enhancement Package 4 for SAP SRM 7.0 • SAP NetWeaver 7.51 with SAP BASIS 7.51 SAP S/4 HANA 1610 with component S4CORE Release 101 SP 0000 • SAP ABAP Platform 1809 SAP S/4HANA 1809 with component S4CORE Release 103 SP 0000 SAP BW/4 HANA 2.0 with component DW4CORE Release 200 SP 0001 SAP BPC 11.1 with component BPC4HANA Release 200 SP 0001 • SAP ABAP Platform 1909 SAP S/4HANA 1909 with component S4CORE Release 104 SP 0000 • SAP ABAP Platform 2020 SAP S/4HANA 2020 with component S4CORE Release 105 SP 0000
Other Considerations	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.
Connector Server	11.1.2.1.0 and 12.2.1.3.0
Connector Server JDK	JDK 1.6 Update 24 or later and JKD1.7 or later, or JRockit 1.6 or later
External Code	The connector works with SAP JCo 3.0.2 or later. The following SAP custom code files are required: • sapjco3.jar version 3.0.2 or later • Additional file for Microsoft Windows: sapjco3.dll version 3.0 Additional file for AIX, Solaris, and Linux: libsapjco3.so version 3.0 **Note:** There are different distribution packages (JCo) 3.0 available for various supported platforms and processors. See, JCo documentation for more information about using JCo 3.0 packages as per your environment.

Table 1-1 (Cont.) Certified Components

Component	Requirement
SAP Governance, Risk and Compliance Access Control (GRC AC)	If you want to configure and use the Access Risk Analysis or Access Request Management feature of this target system, then install one of the following: • SAP Access Control 12.0 on SAP NetWeaver 7.52 with component GRCFND_A V1200 SP 06 for SAP S/4 HANA 2020 with SAP_BASIS 755 with plugin GRCPINW V1200_750 SP 11 • SAP Access Control 12.0 on SAP NetWeaver 7.52 with component GRCFND_A V1200 SP 06 for SAP S/4 HANA 1909 with SAP_BASIS 754 with plugin GRCPINW V1200_750 SP 00 • SAP Access Control 12.0 on SAP NetWeaver 7.52 with component GRCFND_A V1200 SP 03 for SAP S/4 HANA 1610 with SAP_BASIS 751 with plugin GRCPINW V1100_731 SP 20 **Note**: As per SNOTE 2699347 GRC Plug-ins should be at least on version 10.1 (ex: GRCPINW V1100 and GRCPIERP V1100) to be supported for GRC 12.0 Version. • SAP Access Control 10.1 on SAP NetWeaver 7.52 with component GRCFND_A V1100 SP 19 for SAP S/4 HANA 1610 with SAP_BASIS 751 with plugin GRCPINW V1100_731 SP 20 • SAP Access Control 10.1 on SAP NetWeaver 7.5 with component GRCFND_A V1100 SP 19 for SAP ERP 6.0 EHP8 with SAP_BASIS 750 with plugin GRCPINW V1100_731 SP 20 **Note**: As per SNOTE 352498 Access Control 10.1 GRCFND_A needs to be installed on NW740 (at least Support package level 02) and it is compatible with GRCPINW (700, 710, 730, 731). Also, apply the following SNOTEs: – 1843287: Error while inserting the request reason in an Access Request – 2500120: To update the User Alias via SOAPUI and OIM – 2399698: For WebService grac_risk_analysis_wout_no_ws, ReportFormat is mandatory field from SP17 • SAP Access Control 10.1 on SAP NetWeaver 7.5 with component GRCFND_A V1100 SP 12 for SAP ERP 6.0 EHP8 with SAP_BASIS 750 with plugin GRCPINW V1100_731 SP 14 **Note**: As per SNOTE 352498 Access Control 10.1 GRCFND_A needs to be installed on NW740 (at least Support package level 02) and it is compatible with GRCPINW (700, 710, 730, 731). Also, apply SNOTE 2335094 before performing SoD Violation. • SAP Access Control 10.1 on SAP NetWeaver 7.4 with component GRCFND_A V1100 SP 10 for SAP ERP 6.0 EHP7 with SAP_BASIS 740 with plugin GRCPINW V1000_731 SP 04 • SAP BusinessObjects Access Control 10 on SAP NetWeaver 7.4 with SAP_BASIS 7.40 Install the VIRACLP 530_700_19, VIRAE 530_700_19, VIRCC 530_700_19, VIRFF 530_700_19, and VIRRE 530_700_19 components. Use ECC 6.0 with RTA components VIRSAHR 530_700 SP 19 and VIRSANH 530_731 • SAP BusinessObjects Access Control 10 on SAP NetWeaver AS ABAP 7.02 Support Pack 7 Install the GRCFND_A SP 10 component. Use ECC 6.0 with RTA component GRCPIERP SP 13. **Note**: If you are using any other SAP application, then you must install the RTA component which is compatible with that SAP application.

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:

> **Note:**
>
> - In Oracle Identity Manager, you can install and configure both SAP User Management and SAP User Management Engine connectors.
>
>   You can configure the connectors with SAP GRC AC target system to use either the Access Risk Analysis or the Access Request Management feature.
> - At some places in this section, SAP User Management connector releases 9.1.2.x and 9.0.4.x have been referred to as release 9.x.

- If you are using Oracle Identity Governance 12*c*PS4(12.2.1.4.0), 12*c*PS3 Release BP02 (12.2.1.3.2) and any later BP in this release track, SAP NetWeaver 7.5 SPS 00 with SAP S/4 HANA 1610 and SAP BusinessObjects AC 10.1 or later, then you must use the SAP User Management 11.1.1.7.1 (one-off p28807748_111170_Generic.zip) or latest 12.2.1.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 PS1 BP07 (11.1.1.5.7) and any later BP in this release track (such as Oracle Identity Manager 11*g* Release 1 PS1 BP08 (11.1.1.5.8) or later, or Oracle Identity Manager 11*g* Release 2 BP05 (11.1.2.0.5)), or Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.*x* version of this connector.
- If you are using an Oracle Identity Manager release 9.1.0.2 BP04 or later and earlier than Oracle Identity Manager 11*g* Release 1 PS1 BP07 (11.1.1.5.7), then you must use the 9.1.2 version of this connector.
- If you are using an Oracle Identity Manager release 9.1.0.1 or later and earlier than Oracle Identity Manager 9.1.0.2 BP04, then you must use the 9.0.4 version of this connector.

1.3 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish

- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.4 Connector Architecture and Supported Deployment Configurations

The SAP UM connector is implemented by using the Identity Connector Framework (ICF).

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

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

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

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

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

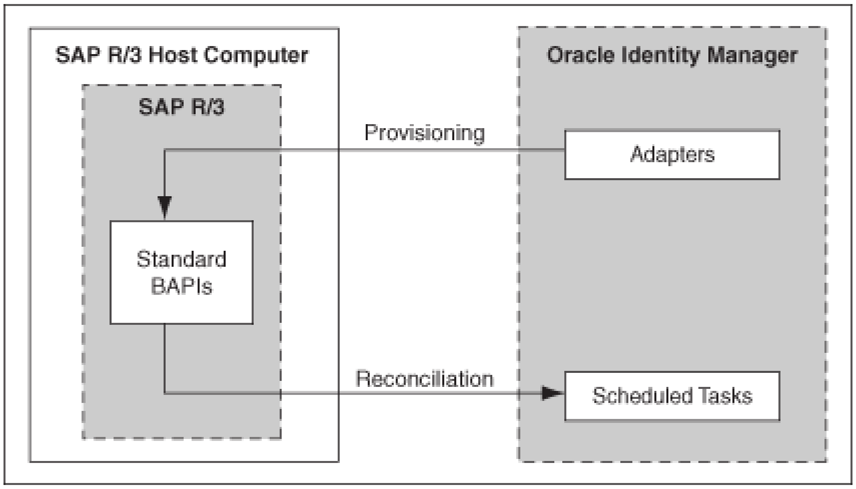
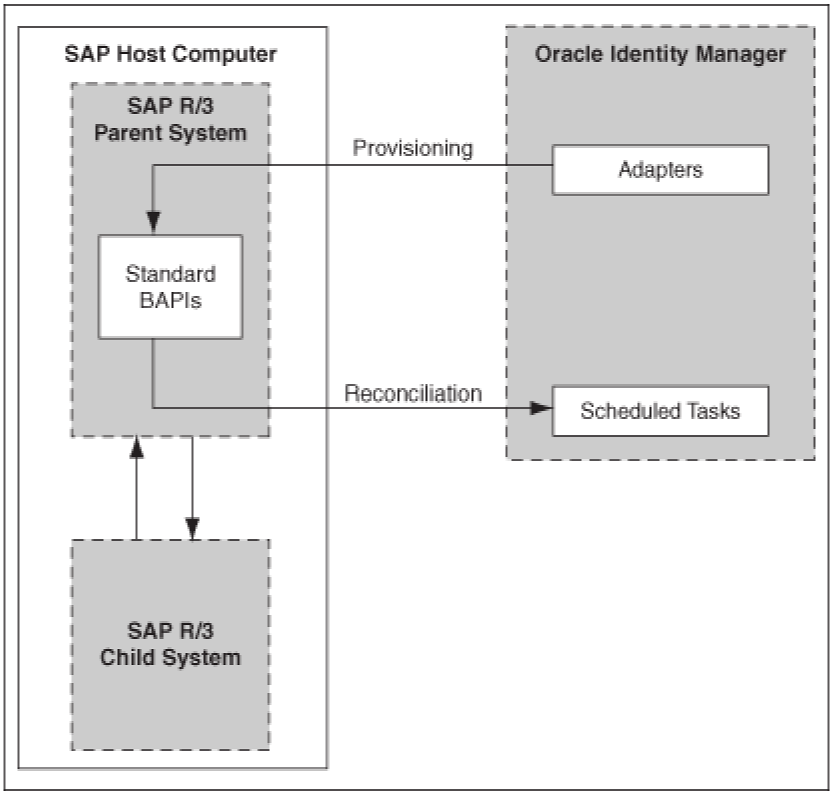


Figure 1-2 shows the connector integrating SAP CUA with Oracle Identity Manager.

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



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

> **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.

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 Access Risk Analysis and Access Request Management modules of SAP BusinessObjects AC. The target system (SAP R/3 or SAP CUA) and these two modules of SAP BusinessObjects AC together provide various deployment configurations. The following sections provide information about the supported deployment configurations of the connector:

- Basic User Management
- User Management with SoD
- Audit Trail Details in Connector Logs
- User Management with Access Request Management
- User Management with Both SoD and Access Request Management
- Guidelines on Using a Deployment Configuration
- Considerations to Be Addressed When You Enable Access Request Management
- Guidelines on Configuring Security

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

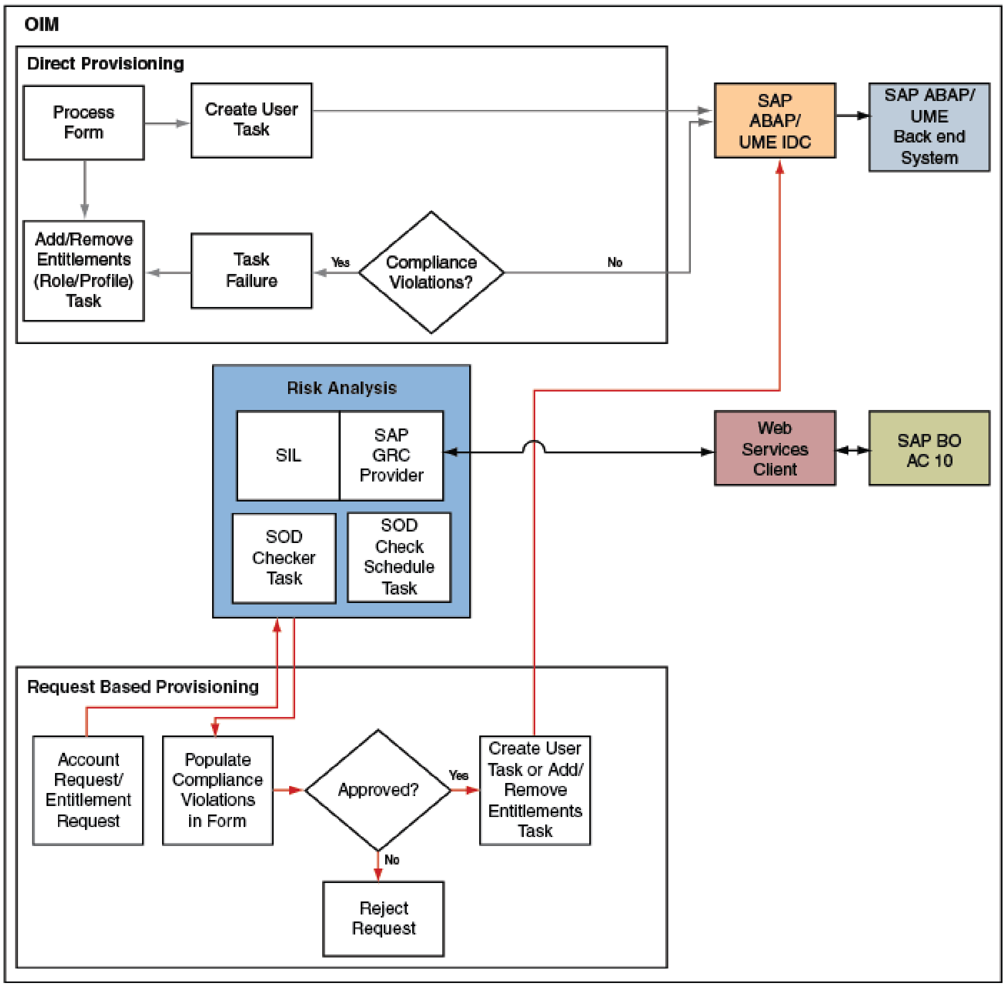
You might have the Access Risk Analysis module of SAP BusinessObjects AC configured to implement segregation of duties (SoD) in your SAP operating environment. In this scenario, the connector can be used as the interface between Oracle Identity Manager and the SoD module. You can configure the connector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

Reconciliation does not involve SAP BusinessObjects AC Access Risk Analysis. 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 BusinessObjects AC Access Risk Analysis.

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:

> **See Also:**
>
> Using Segregation of Duties (SoD) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the provisioning process flow

1. The provisioning operation is initiated through direct provisioning, request-based provisioning, or an access policy change.
2. The resource approval workflow of Oracle Identity Manager sends this request to the SoD engine (SAP BusinessObjects AC Access Risk Analysis).
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.

Summary of the account management process:

1. Data from a provisioning operation on Oracle Identity Governance is first sent to the SAP BusinessObjects Access Risk Analysis module for SoD validation.
2. After the SoD validation checks are cleared, the provisioning request is sent to SAP BusinessObjects Access Request Management.
3. After the SAP BusinessObjects Access Request Management workflow clears the request, the provisioning request is implemented on the target system.
4. Scheduled tasks run from Oracle Identity Governance to reconcile the outcome of the operation from the target system into Oracle Identity Governance.

1.4.3 Audit Trail Details in Connector Logs

The audit trail details can be captured in the connector logs when Access Request Management is configured.

Here are a few samples of Audit trail in the connector logs:

- Create User

```
logAuditTrial : Audit Trial:
{Result=[Createdate:20130409,Priority:HIGH,Requestedby:,johndoe
(JOHNDOE),Requestnumber:9000001341,Status:Decision
pending,Submittedby:,johndoe (JOHNDOE),auditlogData:
{,ID:000C290FC2851ED2A899DA29DAA1B1E2,Description:,Display String:Request
9000001341 of type New Account Submitted by  johndoe ( JOHNDOE ) for
JK1APRIL9 JK1APRIL9 ( JK1APRIL9 ) with Priority HIGH}], Status=0_Data
Populated successfully}
```

- Request Status Schedule Job

```
logAuditTrial : Audit Trial:
{Result=[Createdate:20130409,Priority:HIGH,Requestedby:,johndoe
(JOHNDOE),Requestnumber:9000001341,Status:Approved,Submittedby:,johndoe
(JOHNDOE),auditlogData:
{,ID:000C290FC2851ED2A899DA29DAA1B1E2,Description:,Display
String:Request 9000001341 of type New Account
Submitted by  johndoe ( JOHNDOE ) for JK1APRIL9 JK1APRIL9 ( JK1APRIL9 )
with Priority HIGH,ID:000C290FC2851ED2A899DAF9961C91E2,Description:,Display
String:Request is pending for approval at path GRAC_DEFAULT_PATH
stage GRAC_MANAGER,ID:000C290FC2851ED2A89A1400B60631E2,Description:,Display
String:Approved by JOHNDOE at Path GRAC_DEFAULT_PATH and
Stage GRAC_MANAGER,ID:000C290FC2851ED2A89A150972D091E2,Description:,Display
String:Auto provisioning
activity at end of request at Path GRAC_DEFAULT_PATH and
Stage GRAC_MANAGER,ID:000C290FC2851ED2A89A150972D111E2,Description:,Display
String:Approval path processing is finished,
end of path reached,ID:000C290FC2851ED2A89A150972D151E2,Description:,Display
String:Request is closed}], Status=0_Data Populated successfully}
```

- Modify User

```
logAuditTrial : Audit Trial:
{Result=[Createdate:20130409,Priority:HIGH,Requestedby:,johndoe
(JOHNDOE),Requestnumber:9000001342,Status:Decision
pending,Submittedby:,johndoe (JOHNDOE),auditlogData:
{,ID:000C290FC2851ED2A89A3ED3B1D7B1E2,Description:,Display String:Request
9000001342 of type Change Account Submitted by  johndoe ( JOHNDOE ) for
JK1FirstName JK1APRIL9 ( JK1APRIL9 ) with Priority HIGH}], Status=0_Data
Populated successfully}
```

1.4.4 User Management with Access Request Management

Access Request Management is a module in the SAP BusinessObjects AC suite. In an SAP environment, you can set up Access Request Management as the front end for receiving account creation and modification provisioning requests. In Access Request Management, workflows for processing these requests can be configured and users designated as approvers act upon these requests.

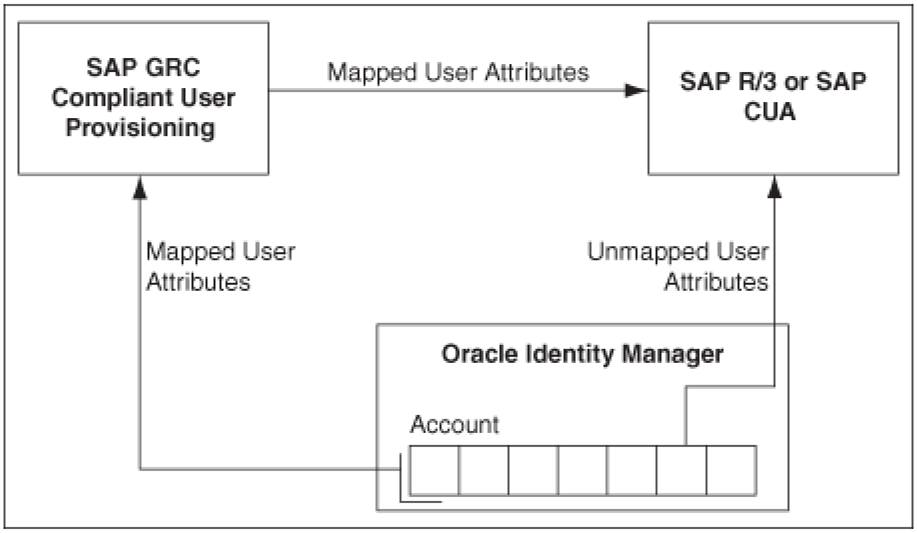
> **Note:**
>
> In this guide, (for the SAP UM AC Connector that uses the SAPUM-AC-Connector-CI.xml file) the phrase **configuring Access Request Management** has been used to mean configuring the integration between Oracle Identity Manager and SAP BusinessObjects AC Access Request Management.
>
> This connector works as a normal SAP UM connector as there is no interaction with GRC target.

In your operating environment, the Access Request Management module might be directly linked with the Access Risk Analysis module. In other words, provisioning requests are first sent from Access Request Management to Access Risk Analysis 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 BusinessObjects AC Access Request Management. 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.

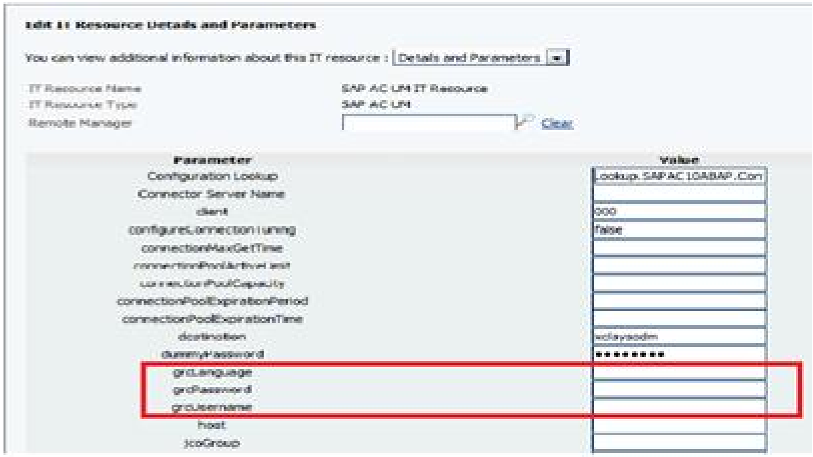
Figure 1-4 Connector Integrating SAP BusinessObjects AC Access Request Management with Oracle Identity Manager and the Target System



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.

   Figure 1-5 IT Resource Configuration Showing GRC in the SAP AC UM Flow

   Edit IT Resource Details and Parameters

   You can view additional information about this IT resource : Details and Parameters

IT Resource Name	SAP AC UM IT Resource
IT Resource Type	SAP AC UM
Remote Manager	Clear

Parameter	Value
Configuration Lookup	Lookup.SAPAC10ABAP.Con
Connector Server Name	
client	000
configureConnectionTuning	false
connectionMaxGetTime	
connectionPoolActiveLimit	
connectionPoolCapacity	
connectionPoolExpirationPeriod	
connectionPoolExpirationTime	
destination	xclaysodm
dummyPassword	********
grcLanguage	
grcPassword	
grcUsername	
host	
jcoGroup	

2. The connector sends requests and receives responses through the following Web services of SAP BusinessObjects AC:
   - 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 BusinessObjects AC Access Request Management logs.

The process form holds fields for both basic user management and Access Request Management. However, for a Create User operation, Access Request Management fields (attributes) on the process form are also used. Mappings for these fields are stored in the Lookup.SAPAC10ABAP.UM.ProvAttrMap lookup definition based on GRC target version.

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 BusinessObjects AC Access Request Management does not process passwords. Therefore, any value entered in the Password field is ignored during Create User provisioning operations.
>
> See Guidelines on Performing Provisioning for information about setting passwords when you configure Access Request Management.

In a Modify User operation, you can specify values for attributes that are mapped with SAP BusinessObjects AC Access Request Management.

3. When the request is created on SAP BusinessObjects AC Access Request Management, data sent back by Access Request Management is stored in the following read-only fields in Oracle Identity Manager:
   - AC Request ID: This field holds the request ID that is generated on SAP BusinessObjects AC Access Request Management. The AC Request ID does not change during the lifetime of the request.
   - AC Request Status: This field holds the status of the request on SAP BusinessObjects AC Access Request Management. You configure and run the SAP AC Request Status scheduled job to fetch the latest status of the request from the target system.
   - AC Request Type: This field holds the type of request, such as New Account, Change Account, Delete Account, New, and Change.
4. The request is passed through the workflow defined in SAP BusinessObjects AC Access Request Management. The outcome is one of the following:
   - If Access Request Management 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 OK in case of SAP BusinessObjects AC 10. Then, a message is recorded in the Oracle Identity Manager logs.
   - If Access Request Management rejects the provisioning request, then the status of the request is set to Failed in case of SAP BusinessObjects AC 10. Then, a message is recorded in the Oracle Identity Manager logs.
   - If Access Request Management cancels the provisioning request, then the status of the request is set to ABORTED in case of SAP BusinessObjects AC 10. Then, a message is recorded in the Oracle Identity Manager logs.

- If an error occurs during communication between Access Request Management 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.

Summary of the account management process:

1. Data from a provisioning operation on Oracle Identity Governance is sent to SAP BusinessObjects Access Request Management.
2. The workflow defined in SAP BusinessObjects Access Request Management sends the request to the SAP BusinessObjects Access Risk Analysis 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 Governance reconcile the outcome of the operation from the target system into Oracle Identity Governance.

1.4.5 User Management with Both SoD and Access Request Management

You might have both SAP BusinessObjects AC Access Risk Analysis and Access Request Management configured in your SAP operating environment. You should configure the connector features for both SoD and Access Request Management at the same time only if the Access Risk Analysis and Access Request Management modules are separately configured, such as User Management with SoD and Access Request Management (that is, not linked) modules are separately configured in your operating environment.

> **Note:**
>
> If SAP BusinessObjects AC Access Request Management is configured to send provisioning requests to SAP BusinessObjects AC Access Risk Analysis for SoD validation, then you must not configure the SoD feature of the connector.

1.4.6 Guidelines on Using a Deployment Configuration

These are the guidelines that you must apply while performing provisioning operations.

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 BusinessObjects AC Access Request Management, with Oracle Identity Manager as the provisioning source for account management on SAP resources.
- Use SAP BusinessObjects AC Access Risk Analysis for SoD enforcement and SAP BusinessObjects AC Access Request Management 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:**
>
> You must separately configure User Management with SoD, and Access Request Management.

- User Management with SoD and Access Request Management
- User Management with Access Request Management

1.4.6.1 User Management with SoD and Access Request Management

The following are deployment guidelines that you must apply for a scenario in which SAP BusinessObjects AC Access Risk Analysis and SAP BusinessObjects AC Access Request Management are enabled and discretely configured modules:

- Configure both SoD and Access Request Management features of the connector.
- On SAP BusinessObjects AC Access Request Management, configure the no-stage approval for account creation. In other words, account creation requests must be auto-approved on Access Request Management.

  If a role or profile is provisioned on Oracle Identity Manager but rejected on SAP BusinessObjects AC Access Request Management, 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 BusinessObjects AC Access Request Management.

Summary of the account management process:

1. Data from a provisioning operation on Oracle Identity Manager is first sent to the SAP BusinessObjects AC Access Risk Analysis module for SoD validation.
2. After the SoD validation checks are cleared, the provisioning request is sent to SAP BusinessObjects AC Access Request Management.
3. After the SAP BusinessObjects AC Access Request Management 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.

1.4.6.2 User Management with Access Request Management

The following are deployment guidelines that you must apply for a scenario in which SAP BusinessObjects AC Access Request Management is configured and enabled in your SAP operating environment:

> **Note:**
>
> SAP BusinessObjects AC Access Risk Analysis is either configured as a linked module of SAP BusinessObjects AC Access Request Management or it is not used at all.
>
> You must separately configure User Management with SoD, and Access Request Management.

- On SAP BusinessObjects AC Access Request Management, configure the no-stage approval for account creation. In other words, account creation requests must be auto-approved on Access Request Management.

  The scenario described earlier in this section explains this guideline.
- Configure the Access Request Management 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 BusinessObjects AC Access Request Management.
2. The workflow defined in SAP BusinessObjects AC Access Request Management sends the request to the SAP BusinessObjects AC Access Risk Analysis 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.

1.4.7 Considerations to Be Addressed When You Enable Access Request Management

These are the consideration you must keep in mind when you enable the Access Request Management 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 Access Request Management 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 BusinessObjects AC Access Request Management. Only information about the last request sent to Access Request Management 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.

  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 Access Request Management feature, you should enable linking only if a no-stage approval has been defined for the Create User request type in SAP BusinessObjects AC Access Request Management. A no-stage approval is one in which no approvers are involved. All requests sent through a no-stage approval are automatically approved.

1.4.8 Guidelines on Configuring Security

These are the guidelines that you must apply while configuring security.

- Secure communication

  It is important to protect sensitive data by securing the communication between Oracle Identity Manager and the SAP system.

  If you are using SAP User Management as the target system, then you must configure SNC (Secure Network Communication). See Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System for more information.

  If you are using SAP BusinessObjects AC as the target system, then you must enable SSL between Oracle Identity Manager and SAP BusinessObjects AC. See Enabling SSL Communication in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for the instructions.
- Password management

  For accounts created through Oracle Identity Manager, you can configure the connector so that users with newly created accounts are prompted to change their passwords at first logon or the password set while creating the account on Oracle Identity Manager is set as the new password on the target system.

  See Configuring Password Changes for Newly Created Accounts for more information.

1.5 Features of the SAP UM Connector

The following are features of the connector:

- Support for SAP Governance, Risk, and Compliance Version 10 or Later
- Support for Connector Server
- Mapping Standard and Custom Attributes for Reconciliation and Provisioning
- SoD Validation of Entitlement Requests
- Routing of Provisioning Requests Through SAP BusinessObjects AC Access Request Management
- Full and Incremental Reconciliation

- Limited (Filtered) Reconciliation
- Batched Reconciliation
- Enabling and Disabling Accounts
- Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts
- SNC Communication Between the Target System and Oracle Identity Manager
- Configuring Password Changes for Newly Created Accounts
- Specifying a SAP JCo Trace Level
- Connection Pooling
- Specifying the Use of a Logon Group on the Target System for Connector Operations
- Transformation and Validation of Account Data
- Support for Resource Exclusion Lists
- Support for Both Unicode and Non-Unicode Modes

1.5.1 Support for SAP Governance, Risk, and Compliance Version 10 or Later

You can use this connector for risk analysis and remdiation and for provisioning and managing users.

The connector supports the following new components:

- Risk Analysis and Remediation, also known as Access Risk Analysis (ARA)
- Compliant User Provisioning, also known as Access Request Management (ARM)

Throughout this guide, SAP GRC Access Risk Analysis refers to Risk Analysis and Remediation and SAP GRC Access Request Management refers to Compliant User Provisioning.

1.5.2 Support for Connector Server

Connector Server is a component provided by ICF.

By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles. In other words, a connector server enables remote execution of an Oracle Identity Manager connector. See the following sections for more information:

- Installing and Configuring the Connector Server
- Installing the Connector in the Connector Server

1.5.3 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 Extending the Functionality of the Connector for more information.

1.5.4 SoD Validation of Entitlement Requests

You can validate an entitlement request in Oracle Identity Manager with an SoD Engine.

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 can be configured to work with SAP BusinessObjects AC as the SoD engine. To enable this, changes have been made in the approval and provisioning workflows of the connector.

  > **Note:**
  >
  > The default approval workflow and associated object form are configured for the SoD validation capabilities of SAP BusinessObjects AC. 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 BusinessObjects AC. You can use them to develop your own approval workflows and request datasets.

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

See Configuring SoD (Segregation of Duties) for detailed information about the SoD feature.

> **Note:**
>
> If you are using SAP User Management with SOD, ensure to request entitlements from the **Entitlements** tab.

1.5.5 Routing of Provisioning Requests Through SAP BusinessObjects AC Access Request Management

You can configure the connector to work with SAP BusinessObjects AC Access Request Management.

See User Management with Access Request Management for detailed information about this feature.

1.5.6 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.

You can switch from incremental to full reconciliation at any time after you deploy the connector. See Full Reconciliation and Incremental Reconciliation for more information.

1.5.7 Limited (Filtered) Reconciliation

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

See Limited Reconciliation for more information.

1.5.8 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 Batched Reconciliation for more information.

1.5.9 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.

1.5.10 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.SAPABAP.Configuration lookup definition:

- validatePERNR
- overwriteLink

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

1.5.11 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 Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System 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 dummyPassword parameter of Basic Configuration Parameters and the ChangePasswordAtNextLogon entry of Advanced Settings parameters.

> **See Also:**
>
> Configuring the IT Resource
>
> 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 2-5 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. Setting up the Lookup Definition for Connection Pooling 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 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:

- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During User Reconciliation

1.5.17 Support for Resource Exclusion Lists

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

See Validation Groovy Script for Resource Exclusion in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for more information about configuring resource exclusion lists.

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 reconciliation and provisioning are preconfigured. Preconfigured lookup definitions are automatically created in Oracle Identity Manager after 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.

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

- Lookup Definitions Synchronized with the Target System
- Preconfigured Lookup Definitions
- Preconfigured Lookup Definitions for SAP BusinessObjects AC 10
- Lookup Definitions Synchronized with the Target System for SAP AC

1.6.1 Lookup Definitions Synchronized with the Target System

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

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 following lookup definitions are populated with values fetched from the target system by the scheduled jobs for lookup field synchronization, for the SAP UM and the SAP AC UM connectors:

- For the SAP UM Connector
  - Lookup.SAPABAP.CommType
  - Lookup.SAPABAP.Company
  - Lookup.SAPABAP.ContractualUserType
  - Lookup.SAPABAP.DateFormat
  - Lookup.SAPABAP.DecimalNotation
  - Lookup.SAPABAP.LangComm
  - Lookup.SAPABAP.Parameter
  - Lookup.SAPABAP.Priority
  - Lookup.SAPABAP.Profile
  - Lookup.SAPABAP.Roles

  - Lookup.SAPABAP.System
  - Lookup.SAPABAP.TimeZone
  - Lookup.SAPABAP.UserGroups
  - Lookup.SAPABAP.UserLock
  - Lookup.SAPABAP.UserTitle
  - Lookup.SAPABAP.UserType
- For the SAP AC UM Connector
  - Lookup.SAPACABAP.CommType
  - Lookup.SAPACABAP.Bproc
  - Lookup.SAPACABAP.Company
  - Lookup.SAPACABAP.ContractualUserType
  - Lookup.SAPACABAP.DateFormat
  - Lokup.SAPACABAP.Funcarea
  - Lookup.SAPACABAP.DecimalNotation
  - Lookup.SAPACABAP.LangComm
  - Lookup.SAPACABAP.Parameter
  - Lookup.SAPACABAP.Priority
  - Lookup.SAPACABAP.Profile
  - Lookup.SAPACABAP.ReqInitSystem
  - Lookup.SAPACABAP.Roles
  - Lookup.SAPACABAP.System
  - Lookup.SAPACABAP.Status.ReconAttrMap
  - Lookup.SAPACABAP.TimeZone
  - Lookup.SAPACABAP.UserGroups
  - Lookup.SAPACABAP.UserLock
  - Lookup.SAPACABAP.UserTitle
  - Lookup.SAPACABAP.UserType

The scheduled jobs for lookup field synchronization are used to synchronize values of these lookup definitions, in the preceding list, with the target system. See Scheduled Jobs for Lookup Field Synchronization for more information about scheduled jobs for lookup field synchronization.

After lookup definition synchronization, data is stored in the following format:

- Code Key format: *IT_RESOURCE_KEY~LOOKUP_FIELD_ID_OR_NAME*

  In this format:

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

The following is a sample value for the Code Key column in the Lookup.SAPABAP.UM.DateFormat lookup definition:

```
22~6
```

- 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.

  The following is a sample value for the Decode column in the Lookup.SAPABAP.DateFormat lookup definition:

  ```
  SAPUM63~YYYY-MM-DD
  ```

While performing a provisioning operation on Oracle Identity System Administration, 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

Preconfigured lookup definitions are 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.

The other lookup definitions are as follows:

- Lookup.SAPABAP.Configuration
- Lookup.SAPABAP.UM.Configuration
- Lookup.SAPABAP.UM.ProvAttrMap
- Lookup.SAPABAP.UM.ReconAttrMap
- Lookup.SAPABAP.UM.ReconTransformation
- Lookup Definitions for Validation of Data
- Lookup Definitions for Exclusion Lists
- Lookup.SAPABAP.UM.RoleChildformMappings
- Lookup.SAPABAP.UM.ProfileChildformMappings
- Preconfigured Lookup Definitions for Access Request Control

1.6.2.1 Lookup.SAPABAP.Configuration

The Lookup.SAPABAP.Configuration lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

Table 1-2 lists the default entries in this lookup definition.

Table 1-2 Entries in the Lookup.SAPABAP.Configuration Lookup Definition

Code Key	Decode	Description
aliasUser	none	This entry holds the logon user alias.
batchSize	100	Enter the number of records in each batch that must be included fetched from the target system during a reconciliation run.
Bundle Name	org.identityconnectors.sap	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.11170	This entry holds the version of the connector bundle class. Do *not* modify this entry.
changePasswordAtNextLogon	no	See Configuring Password Changes for Newly Created Accounts for information about the value to be specified for this entry.
codePage	none	This entry holds initial codepage in SAP notation.
compositeRoles	yes/no	Enter `yes` if you want to fetch composite roles from target. Otherwise enter `no`. **Note:** Both singleRoles and compositeRoles decode values cannot be "no", at least one of the values should be "yes".
Connector Name	org.identityconnectors.sap.SAPConnector	This entry holds the name of the connector class. Do *not* modify this entry.
cuaChildInitialPasswordChangeFuncModule	ZXLCBAPI_ZXLCUSR_PW_CHANGE	Name of the Remote Enabled function module that changes the initial password for a user on all CUA child systems. This attribute is not used unless CUA is enabled. If the value is not set, then the password changes will only apply to the CUA system. Setting productive passwords on CUA child systems will also automatically fail without this setting. Do *not* modify this entry.
cuaChildPasswordChangeFuncModule	ZXLCBAPI_ZXLCUSR_PASSWORDCHNGE	Name of the Remote Enabled function module which changes the productive password for a user on a CUA child system. This attribute is not used unless CUA is enabled. **Note:** If the default value is used, then only the password stored on the CUA central system will be changed.
disableLockStatus	64	Lock Status of an SAP User
enableCUA	no	Enter `yes` if the target system is SAP CUA. Otherwise, enter `no`.
entitlementRiskAnalysisAccessURL	None	This entry holds the URL for Entitlement Risk Analysis web service.

Table 1-2 (Cont.) Entries in the Lookup.SAPABAP.Configuration Lookup Definition

Code Key	Decode	Description
entitlementRiskAnalysisWS	oracle.iam.grc.sod.scomp.impl.grcsap.util.webservice.sap.ac10.RiskAnalysisWithoutNo	This entry holds the Webservice client class to get risk analysis for an user account.
gatewayHost	none	This entry holds the name or IP address of the gateway host.
gatewayService	none	This entry holds the name of the gateway service.
getSSO2	none	Get or do not get a SSO ticket after logon. The value of this entry can be `1` or `0`.
groups	GROUPS~USERGROUP	This field is an embedded object defined in the attribute mapping. In the decode entry, GROUPS is a table name and USERGROUP is a field name on the target system.
lCheck	none	Enable or disable logon check at open time. The value of this entry can be set to `1` to enable logon check or `0` to disable logon check.
mySAPSSO2	none	Specifies the SAP Cookie Version 2 to be used as logon ticket.
overwriteLink	no	See Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts for information about the value to be specified for this entry.
parameters	PARAMETER1~PARID;PARVA	This field is an embedded object defined in the attribute mapping. In the decode entry, PARAMETER1 is a table name, and PARID and PARVA are field names on the target system.
passwordPropagateToChildSystem	no	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`.
ProfileAttributeLabel	Profile Name	This field holds the label name of the profile name field in the child form.
Profile attribute name	USERPROFILE	This field holds a list of field names for the Profile duty type. The values of this list are separated by a semicolon (;).
Profile form names	UD_SPUMPC_P;UD_SPUM_PRO	This field holds a list of all profile child form names used during direct and request-based provisioning.
profiles	PROFILES~SUBSYSTEM;PROFILE	This field is an embedded object defined in the attribute mapping. In the decode entry, PROFILES is a table name, and SUBSYSTEM and PROFILE are field names on the target system.
reconcilefuturedatedroles	yes	Enter `yes` if you want to reconcile future-dated roles. Otherwise, enter `no`.
reconcilepastdatedroles	yes	Enter `yes` if you want to reconcile past-dated roles. Otherwise, enter `no`.
repositoryDestination	none	Specifies the destination to be used as repository.
repositoryPassword	none	Specifies the password for a repository user. This entry is mandatory if a repository user is used.

Table 1-2 (Cont.) Entries in the Lookup.SAPABAP.Configuration Lookup Definition

Code Key	Decode	Description
repositorySNCMode	none	This entry is optional. If SNC is used for this destination, you can turn off SNC for repository connections by setting this entry to `0`.
repositoryUser	none	This entry is optional. If the repository destination is not set, and this entry is set, this entry will be used as user for repository calls. With this entry, you can use a different user for repository lookups.
riskLevel	3	In SAP BusinessObjects AC target, each business risk is assigned a criticality level. You can control the risk analysis data returned by the target by specifying a risk level in this entry.
RoleAttributeLabel	USERROLE	This entry holds the label name of the role name field in the child form
Role attribute name	Profile Name	This field holds a list of field names for the Role duty type. The values of this list are separated by a semicolon (;).
Role form names	UD_SPUMRC_P;UD_SAPRL	This field holds a list of all role child form names used during direct and request-based provisioning.
roles	ACTIVITYGROUPS~SUBSYSTEM;AGR_NAME;TO_DAT;FROM_DAT;ORG_FLAG	This field is an embedded object defined in the attribute mapping. In the decode entry, ACTIVITYGROUPS is a table name on the target system. SUBSYSTEM, TO_DAT, FROM_DAT, and AGR_NAME are field names on the target system.
sapSystemTimeZone	PST	This entry holds the SAP target system time zone.
singleRoles	yes/no	Enter `yes` if you want to fetch single roles from target. Otherwise enter `no`.
SOD Configuration lookup	Lookup.SAPABAP.Configuration	This entry holds the name of the lookup definition that contains SoD configuration properties.
tpHost	none	This entry holds the host name of the external server program.
tpName	none	This entry holds the program ID of the external server program.
type	none	This entry holds the type of the remote host. This entry can have the following values: • For SAP R/2: 2 • For SAP R/3: 3 • For external remote host: `E`
User Configuration Lookup	Lookup.SAPABAP.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.
validatePERNR	no	See Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts for information about the value to be specified for this entry.

Table 1-2 (Cont.) Entries in the Lookup.SAPABAP.Configuration Lookup Definition

Code Key	Decode	Description
wsdlFilePath	< file directory>	Enter the absolute path of the directory containing the following file: GRAC_RISK_ANALYSIS_WOUT_NO_WS.WSDL. **Note**: • Download the WSDL file from the GRC system and save it any of the Oracle Identity Governance system directories. • In an Oracle Identity Governance cluster, copy the WSDL file to each node of the cluster and make sure that the folder structure is the same for each node.
ApplicationType	none	This entry holds the name of the type of application.
BusinessProcess	none	This entry holds the name of the business process.
OrgLevel	none	This entry holds the name of the organization.
ReportFormat	none	This entry holds the format of the report.
RiskLevel	none	This entry holds the value of the risk level.
RoleType	none	This entry holds the name of the type of role.
RuleId	none	This entry holds the name of the rule id.
RuleSetId	none	This entry holds the value of the rule set id.
SimulationRiskOnly	none	This entry holds the value that is set for the SimulationriskOnly parameter.
UserGroup	none	This entry holds the name of the user group.
UserType	none	This entry holds the name of the type of user.
HitCount	none	This entry supports an interger type value. It hold the value of the hit count.
AdditionalAttr	none	This is a multivalued attribute. **Note:** If you want to configure more than one value for multi valued attribute, separate the Decode values with a comma (,).
OrgRule	none	This is a multivalued attribute. **Note:** If you want to configure more than one value for multi valued attribute, separate the Decode values with a comma (,).
OrgVal	none	This is a multivalued attribute. **Note:** If you want to configure more than one value for multi valued attribute, separate the Decode values with a comma (,).
ReportType	none	This is a multivalued attribute. **Note:** If you want to configure more than one value for multi valued attribute, separate the Decode values with a comma (,).

Table 1-2 (Cont.) Entries in the Lookup.SAPABAP.Configuration Lookup Definition

Code Key	Decode	Description
RiskId	none	This is a multivalued attribute. **Note:** If you want to configure more than one value for multi valued attribute, separate the Decode values with a comma (,).

1.6.2.2 Lookup.SAPABAP.UM.Configuration

The Lookup.SAPABAP.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a target resource.

Table 1-3 lists the default entries in this lookup definition.

Table 1-3 Entries in the Lookup.SAPABAP.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.SAPABAP.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.SAPABAP.UM.ProvAttrMap for more information about this lookup definition.
Provisioning Validation Lookup	Lookup.SAPABAP.UM.ProvValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.
Recon Attribute Map	Lookup.SAPABAP.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.SAPABAP.UM.ReconAttrMap for more information about this lookup definition.
Recon Transformation Lookup	Lookup.SAPABAP.UM.ReconTransformation	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See Configuring Transformation of Data During User Reconciliation for more information about adding entries in this lookup definition.
Recon Validation Lookup	Lookup.SAPABAP.UM.ReconValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the target system during reconciliation. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

1.6.2.3 Lookup.SAPABAP.UM.ProvAttrMap

The Lookup.SAPABAP.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during provisioning. This lookup definition is preconfigured. Table 1-14 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

1.6.2.4 Lookup.SAPABAP.UM.ReconAttrMap

The Lookup.SAPABAP.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured. Table 1-10 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Connector for more information.

1.6.2.5 Lookup.SAPABAP.UM.ReconTransformation

The Lookup.SAPABAP.UM.ReconTransformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See Configuring Transformation of Data During User Reconciliation for more information about adding entries in this lookup definition.

1.6.2.6 Lookup Definitions for Validation of Data

The Lookup.SAPABAP.UM.ProvValidation and Lookup.SAPABAP.UM.ReconValidation lookup definitions are used to configure validation of attribute values entered on the process form during provisioning and reconciliation operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

1.6.2.7 Lookup Definitions for Exclusion Lists

This section describes the lookup definitions that hold resources for which you do not want to perform provisioning and reconciliation operations. Exclusions can be applied to any attribute in the process form or reconciliation profile. The Code Key value must be one of the Code Key values in Lookup.SAPABAP.UM.ReconAttrMap or Lookup.SAPABAP.UM.ProvAttrMap lookup definitions.

You can use one of the following lookups:

- Lookup.SAPABAP.ReconExclusionList
- Lookup.SAPABAP.ProvExclusionList

The following is the format of the values stored in these lookups:

Code Key	Decode	Sample Values
User Name	User ID of a user	Code Key: userName Decode: User001
User Name with the [PATTERN] suffix	A regular expression supported by the representation in the `java.util.regex.Pattern` class	Code Key: userName[PATTERN] To exclude users matching any of the user ID 's User001, User002, User088, then: Decode: User001|User002|User088 To exclude users whose user ID 's start with 00012, then: Decode: 00012* **See Also:** For information about the supported patterns, visit `http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html`

See Configuring Resource Exclusion Lists for more information about adding entries in this lookup definition.

1.6.2.8 Lookup.SAPABAP.UM.RoleChildformMappings

The Lookup.SAPABAP.UM.RoleChildformMappings lookup definition contains information about the actual and dummy child form mapped fields that are used during request-based provisioning of role entitlements. This lookup definition is preconfigured. Do not add or modify entries in this lookup definition.

If you are using a cloned connector for request-based provisioning of entitlements, then you must update the respective child form field names manually in this lookup definition.

This lookup definition contains the following entries:

Code Key	Decode
UD_SPUMRC_P_SYSTEMNAME	UD_SAPRL_SYSTEMNAME
UD_SPUMRC_P_STARTDATE	UD_SAPRL_STARTDATE,DATE
UD_SPUMRC_P_ENDDATE	UD_SAPRL_ENDDATE,DATE
UD_SPUMRC_P_USERROLE	UD_SAPRL_USERROLE

1.6.2.9 Lookup.SAPABAP.UM.ProfileChildformMappings

The Lookup.SAPABAP.UM.ProfileChildformMappings lookup definition contains information about the actual and dummy child form mapped fields that are used during request-based provisioning of profile entitlements. This lookup definition is preconfigured. Do not add or modify entries in this lookup definition.

If you are using a cloned connector for request-based provisioning of entitlements, then you must update the respective child form field names manually in this lookup definition.

This lookup definition contains the following entries:

Code Key	Decode
UD_SPUMPC_P_SYSTEMNAME	UD_SPUM_PRO_SYSTEMNAME
UD_SPUMPC_P_USERPROFILE	UD_SPUM_PRO_USERPROFILE

1.6.2.10 Preconfigured Lookup Definitions for Access Request Control

This section discusses the other lookup definitions that are created in Oracle Identity Manager when you deploy the Access Request Control connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed. The other lookup definitions are as follows:

- Lookup.SAPACABAP.Status.Configuration
- Lookup.SAPACABAP.Status.ReconAttrMap

1.6.2.10.1 Lookup.SAPACABAP.Status.Configuration

The Lookup.SAPACABAP.Status.Configuration lookup definition holds status configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a target resource.

Table 1-4 Entries in the Lookup.SAPACABAP.Status.Configuration Lookup Definition

Code	Decode	Description
Provisioning Attribute Map	Lookup.SAPACABAP.Status.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes
Provisioning Validation Lookup	Lookup.SAPACABAP.Status.ProvValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations
Recon Attribute Map	Lookup.SAPACABAP.Status.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.SAPACABAP.Status.ReconAttrMap for more information about this lookup definition.

1.6.2.10.2 Lookup.SAPACABAP.Status.ReconAttrMap

The Lookup.SAPACABAP.Status.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured.

Table 1-5   Entries in the Lookup.SAPACABAP.Status.ReconAttrMap Lookup Definition

Code	Decode
AC Request ID	__UID__
AC Request Status	RequestStatus
AC Request Type	RequestType
User ID	User ID

1.6.3 Preconfigured Lookup Definitions for SAP BusinessObjects AC 10

Preconfigured lookup definitions are 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.

This section discusses the lookup definitions for SAP BusinessObjects AC 10 that are created in Oracle Identity Manager when you deploy the connector. The lookup definitions are as follows:

- Lookup.SAPAC10ABAP.Configuration
- Lookup.SAPAC10ABAP.Configuration
- Lookup.SAPAC10ABAP.UM.ProvAttrMap
- Lookup.SAPAC10ABAP.UM.ReconAttrMap
- Lookup.SAPAC10ABAP.UM.ProvValidation
- Lookup.SAPAC10ABAP.ItemProvAction
- Lookup.SAPAC10ABAP.RequestType
- Lookup.SAPAC10ABAP.UM.ReconTransformation
- Lookup.SAPAC10ABAP.UM.ReconValidation

1.6.3.1 Lookup.SAPAC10ABAP.Configuration

The Lookup.SAPAC10ABAP.Configuration lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

Table 1-6 lists the default entries in this lookup definition.

Table 1-6   Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode	Description
aliasUser	None	This entry holds the logon user alias
appLookupAccessURL	None	URL for Application Lookup web service

Table 1-6 (Cont.) Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode	Description
appLookupWS	oracle.iam.ws.sap.ac10.SelectApplication	Web service client to get all applications configured in SAP BusinessObjects AC
assignRoleReqType	002~Change Account~002~006	Name of the request type to be used for assign role request in SAP BusinessObjects AC The format of the decode value is as follows: `RequestType~RequestTypeName~ItemProvActionForSystem~ItemProvActionForRole` The value of RequestType is available in Lookup.SAPAC10ABAP.RequestType. The values of ItemProvActionForSystem and ItemProvActionForRole are available in Lookup.SAPAC10ABAP.ItemProvAction.
auditLogsAccessURL	None	URL for Audit Logs web service
auditLogsWS	oracle.iam.ws.sap.ac10.AuditLogs	Web service client to get audit logs
batchSize	100	Enter the number of records in each batch that must be fetched from the target system during a reconciliation run
Bundle Name	org.identityconnectors.sapacum	Name of the connector bundle package
Bundle Version	1.0.11170	Version of the connector bundle class
changePasswordAtNextLogon	No	See Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts for information about the value that must be specified for this entry
codePage	None	This entry holds the initial code page in SAP notation
compositeRoles	No	Enter `yes` if you want to fetch composite roles from target. Otherwise enter `no` **Note:** Both singleRoles and compositeRoles decode values cannot be "no", at least one of the values should be "yes".
Connector Name	org.identityconnectors.sapacum.SAPACUMConnector	Name of the connector class

Table 1-6 (Cont.) Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode	Description
createUserReqType	001~New Account~001	Name of the request type to use for create user request in SAP BusinessObjects AC The format of the decode value is as follows: `RequestType~RequestTypeName~ItemProvActionForSystem` The value of RequestType is available in Lookup.SAPAC10ABAP.RequestType. The value of ItemProvActionForSystem is available in Lookup.SAPAC10ABAP.ItemProvAction.
cuaChildInitialPasswordChangeFuncModule	ZXLCBAPI_ZXLCUSR_PW_CHANGE	Name of the Remote Enabled function module that changes the initial password for a user on all CUA child systems This attribute is not used unless CUA is enabled. If the value is not set, then the password changes will only apply to the CUA system. Setting productive passwords on CUA child systems will also automatically fail without this setting. Do not modify this entry.
cuaChildPasswordChangeFuncModule	ZXLCBAPI_ZXLCUSR_PASSWORDCHNGE	Name of the Remote Enabled function module that changes the productive password for a user on a CUA child system. This attribute is not used unless CUA is enabled. **Note:** If the default value is used, then only the password stored on the CUA central system will be changed.
deleteUserReqType	003~Delete Account~003	Name of the request type to use for delete user request in SAP BusinessObjects AC
disableLockStatus	64	Lock Status of an SAP User
enableCUA	No	Enter `yes` if the target system is SAP CUA. Otherwise, enter `no.`
gatewayHost	None	This entry holds the name or IP address of the gateway host
gatewayService	None	This entry holds the name of the gateway service
getSSO2	None	This entry specifies whether to get or not get an SSO ticket after logon. The value of this entry can be `1` or `0`

Table 1-6 (Cont.) Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode	Description
groups	GROUPS~USERGROUP	This field is an embedded object that is defined in the attribute mapping. In the decode entry, GROUPS is a table name and USERGROUP is a field name on the target system.
ignoreOpenStatus	Yes	Specify whether new requests can be sent for a particular user, even if the last request for the user is in the Open status
lCheck	None	Enable or disable logon check at open time. The value of this entry can be set to 1 to enable logon check or `0` to disable logon check.
lockUserReqType	004~Lock Account~004	Name of the request type to use for lock user request in SAP BusinessObjects AC
logAuditTrial	Yes	Specify whether complete audit trial needs to be logged whenever status request web service is invoked
modifyUserReqType	002~Change Account~002	Name of the request type to use for modify user request in SAP BusinessObjects AC
mySAPSSO2	None	Specifies the SAP Cookie Version 2 that must be used as a logon ticket
otherLookupAccessURL	None	URL for Other Lookup web service
otherLookupWS	oracle.iam.ws.sap.ac10.SearchLookup	Web service client to get other lookup field details
overwriteLink	No	See Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts Accounts" for information about the value that must be specified for this entry.
parameters	PARAMETER1~PARID;PARVA	This field is an embedded object that is defined in the attribute mapping. In the decode entry, PARAMETER1 is a table name, and PARID and PARVA are the field names on the target system.
passwordPropagateToChildSystem	No	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`
profiles	PROFILES~SUBSYSTEM;PROFILE	This field is an embedded object defined in the attribute mapping. In the decode entry, PROFILES is a table name, and SUBSYSTEM and PROFILE are the field names on the target system.
provActionAttrName	provAction;ReqLineItem	Name of the Provision Action target system attribute
provItemActionAttrName	provItemAction;ReqLineItem	Name of the Provision Item Action target system attribute

Table 1-6 (Cont.) Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode	Description
reconcilefuturedatedroles	Yes	Enter `yes` if you want to reconcile future-dated roles. Otherwise, enter `no`.
reconcilepastdatedroles	Yes	Enter `yes` if you want to reconcile past-dated roles. Otherwise, enter `no`.
removeRoleReqType	002~Change Account~002~009	Name of the request type to use for remove user request in SAP BusinessObjects AC
ReportFormat	No	This entry holds the format of the report. **Note:** For webService grac_risk_analysis_wout_no_ws, ReportFormat is a mandatory field from SP17 onwards. Default Value: 1 **Note:** This parameter is applicable only for SAP UM with SoD.
repositoryDestination	None	Specifies the destination to be used as repository.
repositoryPassword	None	Specifies the password for a repository user. This entry is mandatory if a repository user is used.
repositorySNCMode	None	This entry is optional. If SNC is used for this destination, you can turn off SNC for repository connections by setting the value of this entry to `0`.
repositoryUser	None	This entry is optional. If the repository destination is not set, and this entry is set, this entry will be used as user for repository calls. With this entry, you can use a different user for repository lookups.
requestStatusAccessURL	None	URL for Status Request web service
requestStatusValue	OK	The value that gets updated in the AC Request Status field on the process form.
requestStatusWS	oracle.iam.ws.sap.ac10.RequestStatus	Web service client to get status of provisioning request
requestTypeAttrName	Reqtype;Header	Name of the request type attribute used to differentiate request flows from the SAPUMCREATE adapter
riskLevel	High	In SAP BusinessObjects AC, each business risk is assigned a criticality level. You can control the risk analysis data returned by SAP BusinessObjects by specifying a risk level.
roleLookupAccessURL	None	URL for Role Lookup web service
roleLookupWS	oracle.iam.ws.sap.ac10.SearchRoles	Web service client to get all roles

Table 1-6 (Cont.) Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode	Description
roles	ACTIVITYGROUPS~SUBSYSTEM;AGR_NAME;TO_DAT;FROM_DAT;ORG_FLAG	This field is an embedded object defined in the attribute mapping. In the decode entry, ACTIVITYGROUPS is a table name on the target system. SUBSYSTEM, TO_DAT, FROM_DAT, AGR_NAME and ORG_FLAG are the field names on the target system.
sapSystemTimeZone	PST	This entry holds the SAP target system time zone.
singleRoles	yes	Enter `yes` if you want to fetch single roles from the target. Otherwise enter `no.`
Status Configuration Lookup	Lookup.SAPACABAP.Status.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.
tpHost	None	This entry holds the host name of the external server program.
tpName	None	This entry holds the program ID of the external server program.
type	None	This entry holds the type of the remote host. This entry can hold the following values: • For SAP R/2: 2 • For SAP R/3: 3 • For external remote host: E
unlockUserReqType	005~unlock user~005	Name of the request type to use for unlock user request in SAP BusinessObjects AC
userAccessAccessURL	None	URL for User Access web service
userAccessWS	oracle.iam.ws.sap.ac10.UserAccess	Web service client to get status of user access
User Configuration Lookup	Lookup.SAPAC10ABAP.UM.Configuration	Name of the lookup definition that contains user-specific configuration properties See Lookup.SAPAC10ABAP.Configuration for more information.
validatePERNR	No	See Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts for information about the value that must be specified for this entry.

Table 1-6 (Cont.) Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode	Description
wsdlFilePath	Absolute path of the files	Enter the absolute path of the directory containing the following files: GRAC_USER_ACCESS_WS.WSDL GRAC_SEARCH_ROLES_WS.WSDL GRAC_SELECT_APPL_WS.WSDL GRAC_REQUEST_STATUS_WS.WSDL GRAC_LOOKUP_WS.WSDL GRAC_AUDIT_LOGS_WS.WSDL Note: • Download the WSDL files from the GRC system and save it any of the Oracle Identity Governance system directories. • In an Oracle Identity Governance cluster, copy the WSDL files to each node of the cluster and make sure that the folder structure is the same for each node.

1.6.3.2 Lookup.SAPAC10ABAP.Configuration

The Lookup.SAPABAP.AC10.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a target resource.

Table 1-7 lists the default entries in this lookup definition.

Table 1-7 Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.SAPAC10ABAP.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.SAPAC10ABAP.UM.ProvAttrMap for more information about this lookup definition.
Provisioning Validation Lookup	Lookup.SAPAC10ABAP.UM.ProvValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations. See Lookup.SAPAC10ABAP.UM.ProvValidation for more information about this lookup definition.
Recon Attribute Map	Lookup.SAPAC10ABAP.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.SAPAC10ABAP.UM.ReconAttrMap for more information about this lookup definition.

Table 1-7 (Cont.) Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode	Description
Recon Transformation Lookup	Lookup.SAPAC10ABAP.UM.ReconTransformation	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See Configuring Transformation of Data During User Reconciliation for more information about adding entries in this lookup definition.
Recon Validation Lookup	Lookup.SAPAC10ABAP.UM.ReconValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the target system during reconciliation. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

1.6.3.3 Lookup.SAPAC10ABAP.UM.ProvAttrMap

The Lookup.SAPAC10ABAP.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during provisioning. This lookup definition is preconfigured. Table 1-8 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

Table 1-8 Entries in the Lookup.SAPAC10ABAP.UM.ProvAttrMap Lookup Definition

Code Key	Decode
AC Business Process[Lookup]	bproc;Header
Accounting Number	accno;UserInfo
AC Functional Area[Lookup]	funcarea;Header
AC Manager	manager;UserInfo
AC Manager email	managerEmail;UserInfo
AC Manager First Name	managerFirstname;UserInfo
AC Manager Last Name	managerLastname;UserInfo
AC Priority[Lookup]	priority;Header
AC Request Due Date[Date]	reqDueDate;Header
AC Request Id[WRITEBACK]	RequestId
AC Requestor email	email;Header
AC Requestor ID	requestorId;Header
AC Request Reason	requestReason;Header

Table 1-8 (Cont.) Entries in the Lookup.SAPAC10ABAP.UM.ProvAttrMap Lookup Definition

Code Key	Decode
AC Request Status[WRITEBACK]	RequestStatus
AC Request Type[WRITEBACK]	RequestType
AC System[Lookup]	reqInitSystem;Header
Alias	alias;UserInfo
Building	BUILDING_P;ADDRESS;BUILDING_P;ADDRESSX
Communication Type	commMethod;UserInfo
Company[Lookup]	COMPANY;COMPANY;COMPANY;COMPANYX
Contractual User Type[Lookup]	LIC_TYPE;UCLASS;UCLASS;UCLASSX
Cost Center	costcenter;UserInfo
Date Format	dateFormat;UserInfo
Decimal Notation	decNotation;UserInfo
Department	DEPARTMENT;ADDRESS;DEPARTMENT;ADDRESSX
E Mail	email;UserInfo
Fax Extension	FAX_EXTENS;ADDRESS;FAX_EXTENS;ADDRESSX
Fax Number	fax;UserInfo
First Name	fname;UserInfo
Floor	FLOOR_P;ADDRESS;FLOOR_P;ADDRESSX
Function	FUNCTION;ADDRESS;FUNCTION;ADDRESSX
Group Name[Lookup]	CLASS;LOGONDATA;CLASS;LOGONDATAX
Language Communication[Lookup]	LANGU_P;ADDRESS;LANGU_P;ADDRESSX
Last Name	lname;UserInfo
Logon Language	logonLang;UserInfo
Password	__PASSWORD__
Personnel Number	PERNR
Room Number	ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX
Start Menu	startMenu;UserInfo
Telephone Extension	TEL1_EXT;ADDRESS;TEL1_EXT;ADDRESSX
Telephone Number	telnumber;UserInfo
Time Zone[Lookup]	TZONE;LOGONDATA;TZONE;LOGONDATAX
Title[Lookup]	title;UserInfo
UD_UMAC_GRP~User Group[Lookup]	userGroup;UserGroup
UD_UMAC_PRM~Parameter ID[Lookup]	Parameter~parameter~parameter;Parameter

Table 1-8 (Cont.) Entries in the Lookup.SAPAC10ABAP.UM.ProvAttrMap Lookup Definition

Code Key	Decode
UD_UMAC_PRM~Parameter Value	Parameter~parameter~parameterValue;Parameter
UD_UMAC_ROL~End Date[Date]	roles~ACTIVITYGROUPS~ValidTo;ReqLineItem
UD_UMAC_ROL~Role Name[Lookup]	roles~ACTIVITYGROUPS~itemName;ReqLineItem
UD_UMAC_ROL~Role System Name[Lookup]	roles~ACTIVITYGROUPS~connector;ReqLineItem
UD_UMAC_ROL~Start Date[Date]	roles~ACTIVITYGROUPS~validFrom;ReqLineItem
UD_UMAC_PRO~Profile Name[Lookup]	profile~PROFILES~itemName;ReqLineItem
UD_UMAC_PRO~Profile System Name[Lookup]	profile~PROFILES~connector;ReqLineItem
Unique ID	__UID__
User Group[Lookup]	userGroup;UserInfo
User ID	userId;UserInfo
User Lock	userLock;None
User Type	userType;UserInfo
Valid From[Date]	validFrom;UserInfo
Valid Through[Date]	validTo;UserInfo

1.6.3.4 Lookup.SAPAC10ABAP.UM.ReconAttrMap

The Lookup.SAPAC10ABAP.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured. Table 1-9 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Connector for more information.

Table 1-9 Entries in the Lookup.SAPAC10ABAP.UM.ReconAttrMap Lookup Definition

Code Key	Decode
Accounting Number	ACCNT;LOGONDATA
Alias	USERALIAS;ALIAS
Building	BUILDING_P;ADDRESS
Communication Type[Lookup]	COMM_TYPE;ADDRESS

Table 1-9 (Cont.) Entries in the Lookup.SAPAC10ABAP.UM.ReconAttrMap Lookup Definition

Code Key	Decode
Company[Lookup]	COMPANY;COMPANY
Contractual User Type[Lookup]	LIC_TYPE;UCLASS|UCLASSSYS
Cost Center	KOSTL;DEFAULTS
Date Format[Lookup]	DATFM;DEFAULTS
Decimal Notation[Lookup]	DCPFM;DEFAULTS
Department	DEPARTMENT;ADDRESS
E Mail	E_MAIL;ADDRESS
Fax Extension	FAX_EXTENS;ADDRESS
Fax Number	FAX_NUMBER;ADDRESS
First Name	FIRSTNAME;ADDRESS
Floor	FLOOR_P;ADDRESS
Function	FUNCTION;ADDRESS
Group~User Group[Lookup]	groups~GROUPS~USERGROUP
Group Name[Lookup]	CLASS;LOGONDATA
Language Communication[Lookup]	LANGU_P;ADDRESS
Last Name	LASTNAME;ADDRESS
Logon Language	LANGU;DEFAULTS
Parameter~Parameter ID[Lookup]	parameters~PARAMETER1~PARID
Parameter~Parameter Value	parameters~PARAMETER1~PARVA
Profile~Profile Name[Lookup]	profiles~PROFILES~PROFILE
Profile~Profile System Name[Lookup]	profiles~PROFILES~SUBSYSTEM
Role~End Date[Date]	roles~ACTIVITYGROUPS~TO_DAT
Role~Role Name[Lookup]	roles~ACTIVITYGROUPS~AGR_NAME
Role~Role System Name[Lookup]	roles~ACTIVITYGROUPS~SUBSYSTEM
Role~Start Date[Date]	roles~ACTIVITYGROUPS~FROM_DAT
Room Number	ROOM_NO_P;ADDRESS
Start Menu	START_MENU;DEFAULTS
Status	__ENABLE__
Telephone Extension	TEL1_EXT;ADDRESS
Telephone Number	TEL1_NUMBR;ADDRESS
Time Zone[Lookup]	TZONE;LOGONDATA
Title[Lookup]	TITLE_P;ADDRESS

Table 1-9 (Cont.) Entries in the Lookup.SAPAC10ABAP.UM.ReconAttrMap Lookup Definition

Code Key	Decode
Unique ID	__UID__
User ID	__UID__
User Lock	__LOCK_OUT__
User Type	USTYP;LOGONDATA
Valid From[Date]	GLTGV;LOGONDATA
Valid Through[Date]	GLTGB;LOGONDATA

1.6.3.5 Lookup.SAPAC10ABAP.UM.ProvValidation

The Lookup.SAPAC10ABAP.UM.ProvValidation lookup definition is used to configure validation of attribute values entered on the process form during provisioning operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information.

1.6.3.6 Lookup.SAPAC10ABAP.ItemProvAction

The Lookup.SAPABAP.AC10.ItemProvAction lookup definition holds Item provision action code from SAP BusinessObjects AC 10. This code used to create a request in SAP BusinessObjects AC 10 to add or remove roles.

The Item provision action is used to configure the Decode values of the following Code Key entries in the Lookup.SAPAC10ABAP.Configuration lookup definition:

- assignRoleReqType
- removeRoleReqType

The Lookup.SAPAC10ABAP.ItemProvAction lookup definition is populated by the SAP AC ItemProvAction Lookup Reconciliation scheduled job. By default, there are no entries in the lookup definition.

1.6.3.7 Lookup.SAPAC10ABAP.RequestType

The Lookup.SAPAC10ABAP.RequestType lookup definition is used to configure the Decode values of the following Code Key entries in the Lookup.SAPAC10ABAP.Configuration lookup definition:

- assignRoleReqType
- createUserReqType
- deleteUserReqType
- lockUserReqType
- modifyUserReqType
- removeRoleReqType
- unlockUserReqType

The Lookup.SAPAC10ABAP.RequestType lookup definition is populated by the SAP AC RequestType Lookup Reconciliation scheduled job. By default, there are no entries in the lookup definition.

1.6.3.8 Lookup.SAPAC10ABAP.UM.ReconTransformation

The Lookup.SAPAC10ABAP.UM.ReconTransformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation.

See Configuring Transformation of Data During User Reconciliation for more information.

1.6.3.9 Lookup.SAPAC10ABAP.UM.ReconValidation

The Lookup.SAPAC10ABAP.UM.ReconValidation lookup definition is used to configure validation of attribute values that are entered on the process form during reconciliation operations.

See Configuring Validation of Data During Reconciliation and Provisioning for more information.

1.6.4 Lookup Definitions Synchronized with the Target System for SAP AC

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

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 following lookup definitions are populated with values fetched from the target system by the scheduled jobs for lookup field synchronization

- Lookup.SAPACABAP.Bproc
- Lookup.SAPACABAP.CommType
- Lookup.SAPACABAP.Company
- Lookup.SAPACABAP.ContractualUserType
- Lookup.SAPACABAP.DateFormat
- Lookup.SAPACABAP.DecimalNotation
- Lookup.SAPACABAP.Funcarea
- Lookup.SAPACABAP.LangComm
- Lookup.SAPACABAP.Parameter
- Lookup.SAPACABAP.Priority
- Lookup.SAPACABAP.Profile

- Lookup.SAPACABAP.ReqInitSystem
- Lookup.SAPACABAP.Roles
- Lookup.SAPACABAP.System
- Lookup.SAPACABAP.TimeZone
- Lookup.SAPACABAP.UM.ProvExclusionList
- Lookup.SAPACABAP.UM.ReconExclusionList
- Lookup.SAPACABAP.UserGroups
- Lookup.SAPACABAP.UserLock
- Lookup.SAPACABAP.UserTitle
- Lookup.SAPACABAP.UserType

The scheduled jobs for lookup field synchronization are used to synchronize values of these lookup definitions, in the preceding list, with the target system. See Scheduled Jobs for Lookup Field Synchronization for more information about scheduled jobs for lookup field synchronization.

After lookup definition synchronization, data is stored in the following format:

- Code Key format: *IT_RESOURCE_KEY~LOOKUP_FIELD_ID_OR_NAME*

  In this format:

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

  – *LOOKUP_FIELD_ID_OR_NAME* is the target system code or name assigned to the lookup field entry.

  The following is a sample value for the Code Key column in the Lookup.SAPABAP.UM.DateFormat lookup definition:

  ```
  22~6
  ```

- 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.

  The following is a sample value for the Decode column in the Lookup.SAPABAP.DateFormat lookup definition:

  ```
  SAPUM63~YYYY-MM-DD
  ```

While performing a provisioning operation on the Oracle Identity System Administration, 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.

1.7 Connector Objects Used During Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified accounts on the target system and using this data to add or modify resources assigned to OIM users.

The SAP UM User Recon scheduled job is used to initiate a reconciliation run. This scheduled job is discussed in SAP UM User Recon.

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for conceptual information about reconciliation

This section discusses the following topics:

- User Attributes for Reconciliation
- Reconciliation Rules
- Reconciliation Action Rules

1.7.1 User Attributes for Reconciliation

The Lookup.SAPABAP.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 for single-valued attribute is as follows:

FIELD_NAME;STRUCTURE_NAME

The format of the Decode column for multivalued attributes is as follows:

EMBEDDED_OBJECT_NAME~OBJECT_CLASS~TARGET_FIELD_NAME

Table 1-10 lists entries in this lookup definition.

Table 1-10 Entries in the Lookup.SAPABAP.UM.ReconAttrMap Lookup Definition

Resource Object Field	Target System Attribute
Accounting Number	ACCNT;LOGONDATA
Alias	USERALIAS;ALIAS
Building	BUILDING_P;ADDRESS
Communication Type[Lookup]	COMM_TYPE;ADDRESS
Company[Lookup]	COMPANY;COMPANY

Table 1-10 (Cont.) Entries in the Lookup.SAPABAP.UM.ReconAttrMap Lookup Definition

Resource Object Field	Target System Attribute
Contractual User Type[Lookup]	LIC_TYPE;UCLASS|UCLASSSYS
Cost Center	KOSTL;DEFAULTS
Date Format[Lookup]	DATFM;DEFAULTS
Decimal Notation[Lookup]	DCPFM;DEFAULTS
Department	DEPARTMENT;ADDRESS
E Mail	E_MAIL;ADDRESS
Fax Extension	FAX_EXTENS;ADDRESS
Fax Number	FAX_NUMBER;ADDRESS
First Name	FIRSTNAME;ADDRESS
Floor	FLOOR_P;ADDRESS
Function	FUNCTION;ADDRESS
Group~User Group[Lookup]	groups~GROUPS~USERGROUP
Group Name[Lookup]	CLASS;LOGONDATA
Language Communication[Lookup]	LANGU_P;ADDRESS
Last Name	LASTNAME;ADDRESS
Logon Language[Lookup]	LANGU;DEFAULTS
Parameter~Parameter ID[Lookup]	parameters~PARAMETER1~PARID
Parameter~Parameter Value	parameters~PARAMETER1~PARVA
Profile~Profile Name[Lookup]	profiles~PROFILES~PROFILE
Profile~Profile System Name[Lookup]	profiles~PROFILES~SUBSYSTEM
Role~End Date[Date]	roles~ACTIVITYGROUPS~TO_DAT
Role~Role Name[Lookup]	roles~ACTIVITYGROUPS~AGR_NAME
Role~Role System Name[Lookup]	roles~ACTIVITYGROUPS~SUBSYSTEM
Role~Start Date[Date]	roles~ACTIVITYGROUPS~FROM_DAT
Room Number	ROOM_NO_P;ADDRESS
Start Menu	START_MENU;DEFAULTS
Status	__ENABLE__
Telephone Extension	TEL1_EXT;ADDRESS
Telephone Number	TEL1_NUMBR;ADDRESS
Time Zone[Lookup]	TZONE;LOGONDATA
Title[Lookup]	TITLE_P;ADDRESS
User ID	__UID__
User Lock	__LOCK_OUT__
User Type[Lookup]	USTYP;LOGONDATA
Valid From[Date]	GLTGV;LOGONDATA
Valid Through[Date]	GLTGB;LOGONDATA
Unique ID	__UID__

1.7.2 Reconciliation Rules

The connector uses reconciliation rules to determine the identity to which Oracle Identity Governance must assign a resource.

> **See Also:**
>
> Reconciliation Engine in *Oracle Fusion Middleware Developing and Customizing Applications 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:

- Reconciliation Rule
- 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

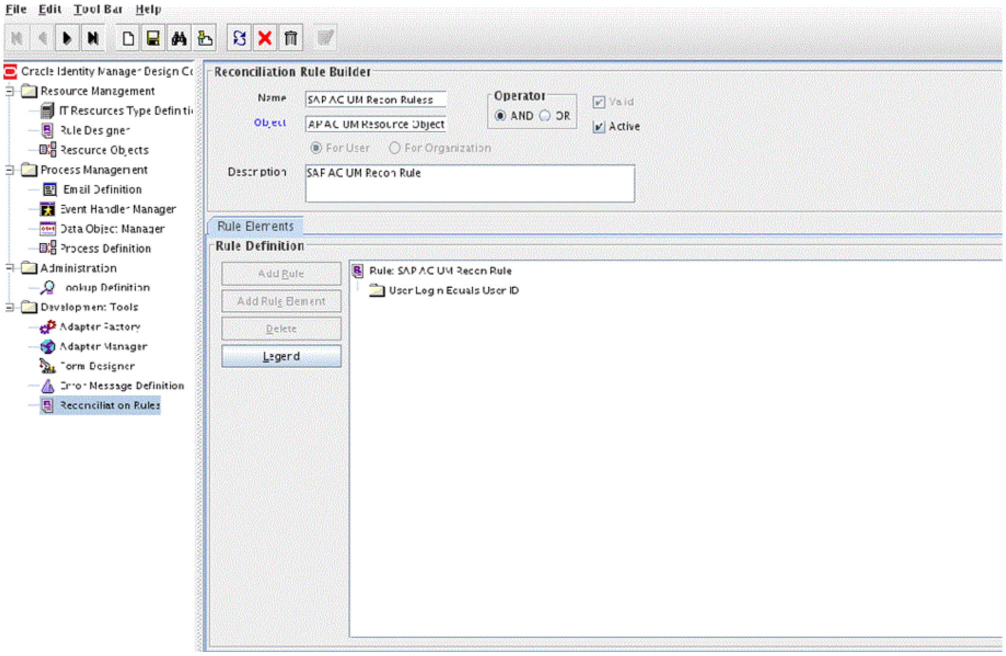
You can view reconciliation rules by using Oracle Identity Manager Design Console.

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

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

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for and open **SAP UM Recon Rule**. Figure 1-6 shows this reconciliation rule.

Figure 1-6   Reconciliation Rule



Name: SAP AC UM Recon Rules
Object: APAC UM Resource Object
Operator: ● AND ○ OR
☑ Valid
☑ Active
● For User ○ For Organization
Description: SAP AC UM Recon Rule

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

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. See Setting a Reconciliation Action Rule in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about modifying or creating reconciliation action rules.

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

- Reconciliation Action Rules for Reconciliation
- Viewing Reconciliation Action Rules in the Design Console

1.7.3.1 Reconciliation Action Rules for Reconciliation

Reconciliation action rules define that actions the connector must perform based on the reconciliation rules defined for Users.

Table 1-11 lists the action rules for reconciliation.

Table 1-11   Action Rules for Reconciliation

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load

Table 1-11 (Cont.) Action Rules for Reconciliation

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

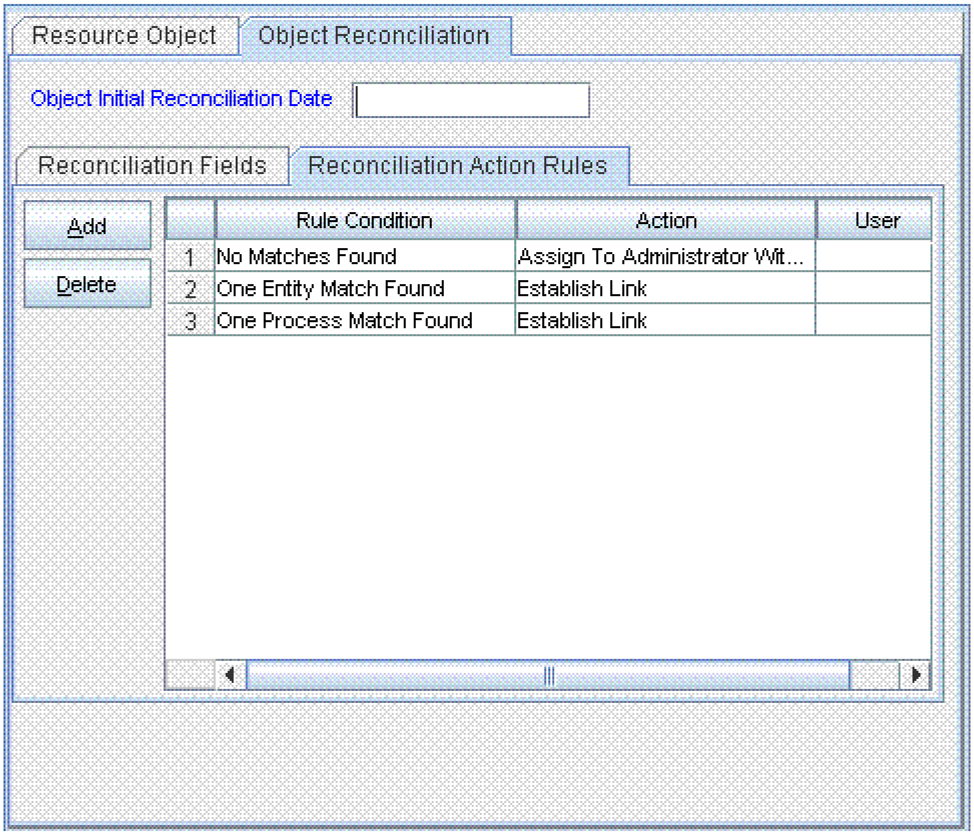
1.7.3.2 Viewing Reconciliation Action Rules in the Design Console

You can view reconciliation action rules on the Object Reconciliation tab of a resource object in Oracle Identity Manager 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 Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. If you want to view the reconciliation action rules for reconciliation, then search for and open the **SAP UM Resource Object** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1-7 shows the reconciliation action rules for reconciliation.

Figure 1-7 Reconciliation Action Rules



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

1.8 Connector Objects Used During Provisioning

Connector objects such as adapters are used for performing provisioning operations on the target system. These adapters perform provisioning functions on the fields defined in the lookup definition for provisioning.

This section discusses the following topics:

- User Provisioning Functions
- User Attributes for Provisioning

1.8.1 User Provisioning Functions

These are the supported provisioning functions and the adapters that perform these functions for the connector.

Table 1-12 and Table 1-13 list the user provisioning functions supported by the SAP UM and SAP AC UM connectors, and the adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.

> **See Also:**
>
> Using the Adapter Factory in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about process tasks and adapters

Table 1-12 User Provisioning Functions Supported by SAP UM

Function	Adapter
Create a user account	adpSAPUMCREATE
Update a user account	adpSAPUMUPDATE
Delete a user account	adpSAPUMDELETE
Enable a user account	adpSAPUMENABLE
Disable a user account	adpSAPUMDISABLE
Update multivalued attribute (for example, role or parameter)	adpSAPUMUPDATECHILD
Add multivalue attribute	adpSAPUMADDCHILD
Remove multivalue attribute	adpSAPUMREMOVECHILD
Prepopulates SAPUM form	adpSAPUMPREPOPULATE
request entitlement for SAP UM	adpSAPUMREQUESTENTITLEMENT

Table 1-13 User Provisioning Functions Supported by SAP AC UM

Function	Adapter
Create a user account	adpSAPACUMCREATEUSER

Table 1-13 (Cont.) User Provisioning Functions Supported by SAP AC UM

Function	Adapter
Update a user account	adpSAPACUMUPDATEUSER
Delete a user account	adpSAPACUMDELETEUSER
Enable a user account	adpSAPACUMENABLEUSER
Disable a user account	adpSAPACUMDISABLEUSER
Update multivalued attribute (for example, role or parameter)	adpSAPACUMUPDATECHILD
Add multivalue attribute	adpSAPACUMADDCHILD
Remove multivalue attribute	adpSAPACUMREMOVECHILD
Prepopulate SAP AC UM Form	adpSAPACUMPREPOPULATE

1.8.2 User Attributes for Provisioning

The Lookup.SAPABAP.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 the Decode column for single-valued attributes is as follows:

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

In this format:

- *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*.

The format of the Decode column for multivalued attributes is as follows:

```
EMBEDDED_OBJECT_NAME~OBJECT_CLASS~TARGET_FIELD_NAME
```

Table 1-14 lists the entries in this lookup definition.

Table 1-14 Entries in the Lookup.SAPABAP.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Attribute
Accounting Number	ACCNT;LOGONDATA;ACCNT;LOGONDATAX
Alias	USERALIAS;ALIAS;BAPIALIAS;ALIASX
Building	BUILDING_P;ADDRESS;BUILDING_P;ADDRESSX
Communication Type[Lookup]	COMM_TYPE;ADDRESS;COMM_TYPE;ADDRESSX
Company[Lookup]	COMPANY;COMPANY;COMPANY;COMPANYX
Contractual User Type[Lookup]	LIC_TYPE;UCLASS;UCLASS;UCLASSX
Cost Center	KOSTL;DEFAULTS;KOSTL;DEFAULTSX

Table 1-14 (Cont.) Entries in the Lookup.SAPABAP.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Attribute
Date Format[Lookup]	LOOKUP;DATFM;DEFAULTS;DATFM;DEFAULTSX
Decimal Notation[Lookup]	DCPFM;DEFAULTS;DCPFM;DEFAULTSX
Department	DEPARTMENT;ADDRESS;DEPARTMENT;ADDRESSX
E Mail	E_MAIL;ADDRESS;E_MAIL;ADDRESSX
Fax Extension	FAX_EXTENS;ADDRESS;FAX_EXTENS;ADDRESSX
Fax Number	FAX_NUMBER;ADDRESS;FAX_NUMBER;ADDRESSX
First Name	FIRSTNAME;ADDRESS;FIRSTNAME;ADDRESSX
Floor	FLOOR_P;ADDRESS;FLOOR_P;ADDRESSX
Function	FUNCTION;ADDRESS;FUNCTION;ADDRESSX
Group Name[Lookup]	CLASS;LOGONDATA;CLASS;LOGONDATAX
Language Communication[Lookup]	LANGU_P;ADDRESS;LANGU_P;ADDRESSX
Last Name	LASTNAME;ADDRESS;LASTNAME;ADDRESSX
Logon Language[Lookup]	LANGU;DEFAULTS;LANGU;DEFAULTSX
Password	__PASSWORD__
Personnel Number	PERNR
Room Number	ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX
Start Menu	START_MENU;DEFAULTS;START_MENU;DEFAULTSX
Telephone Extension	TEL1_EXT;ADDRESS;TEL1_EXT;ADDRESSX
Telephone Number	TEL1_NUMBR;ADDRESS;TEL1_NUMBR;ADDRESSX
Time Zone[Lookup]	TZONE;LOGONDATA;TZONE;LOGONDATAX
Title[Lookup]	TITLE_P;ADDRESS;TITLE_P;ADDRESSX
UD_SAP_GP~User Group[Lookup]	groups~GROUPS~USERGROUP
UD_SAP_PARA~Parameter ID[Lookup]	parameters~PARAMETER1~PARID
UD_SAP_PARA~Parameter Value	parameters~PARAMETER1~PARVA
UD_SAPRL~End Date[Date]	roles~ACTIVITYGROUPS~TO_DAT
UD_SAPRL~Role Name[Lookup]	roles~ACTIVITYGROUPS~AGR_NAME
UD_SAPRL~Start Date[Date]	roles~ACTIVITYGROUPS~FROM_DAT
UD_SPUM_PRO~Profile Name[Lookup]	profiles~PROFILES~PROFILE
Unique ID	__UID__
User ID	__NAME__
User Lock	User Lock;NONE;NONE;NONE
User Type[Lookup]	USTYP;LOGONDATA;USTYP;LOGONDATAX
Valid From[Date]	GLTGV;LOGONDATA;GLTGV;LOGONDATAX
Valid Through[Date]	GLTGB;LOGONDATA;GLTGB;LOGONDATAX

1.9 Roadmap for Deploying and Using the Connector

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

- Deploying the Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Using the Connector describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Extending the Functionality of the Connector describes procedures that you can perform if you want to extend the functionality of the connector.
- Known Issues and FAQs lists known issues and FAQs associated with this release of the connector.
- Troubleshooting the Connector describes the procedure to troubleshoot the connector.
- Files and Directories in the SAP UM Connector Package provides information about files and directories on the installation media.
- Standard BAPIs Used During Connector Operations provides information about standard BAPIs used during connector operations.

2

Deploying the Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, and postinstallation.
This chapter contains the following sections:

- Preinstallation
- Installation
- Postinstallation
- Upgrading the Connector
- Postcloning Steps

> **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 for the SAP UM connector involves performing a series of tasks on the target system.

Preinstallation information is divided across the following sections:

- Downloading and Installing the SAP JCo
- Creating a Target System User Account for Connector Operations
- Assigning Roles to a User Account in a SAP Business Objects Access Control System for Connector Operations

2.1.1 Downloading and Installing the SAP JCo

The SAP Java Connector file is a middleware component that enables the development of SAP-compatible components and applications in Java. This component is required to support inbound and outbound SAP server communication during runtime.

> **Note:**
>
> Ensure that you are using version 3.0.2 or later of the sapjco3.jar file.
>
> To download files from the SAP Web site, you must have access to the SAP service marketplace with Software Download authorization.

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:
   1. Open the SAP JAVA Connector page by selecting **Application Platform, Connectivity, Connectors, SAP Java Connector,** and **Tools & Services.**
   2. 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.
   3. 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. Create a directory called sap-11.1.1.7.0 for the SAP User Management connector in the following directory:

   OIM_HOME/server/ConnectorDefaultDirectory/targetsystems-lib/

   The files in this directory are not shared with any other connectors, which avoids version conflicts among shared libraries.
4. Copy the sapjco3.jar file into the *OIM_HOME*/server/ThirdParty directory. Then, add its path to the *DOMAIN_HOME*\bin\startWebLogic file as follows:
   - On Microsoft Windows:

     In a text editor, open the *DOMAIN_HOME/*bin/startWebLogic.cmd file and add the following path:

     ```
     set
     CLASSPATH=MIDDLEWARE_HOME_PATH\Oracle_IDM1\server\ThirdParty\sapjco
     3.jar;%SAVE_CLASSPATH%
     ```

     Save and close the file. Restart the server for the changes in the CLASSPATH variable to take effect.
   - On Linux:

     In a text editor, open the *DOMAIN_HOME/*bin/startWebLogic.sh file and add the following path:

     ```
     CLASSPATH=MIDDLEWARE_HOME_PATH/Oracle_IDM1/server/ThirdParty/
     sapjco3.jar:"${SAVE_CLASSPATH}"
     ```

     For example, `CLASSPATH=/home/shareuser/SYR2PS1BP207/Middleware/Oracle_IDM1/server/ThirdParty/sapjco3.jar:"${SAVE_CLASSPATH}"`

Save and close the file. Restart the server for the changes in the CLASSPATH variable to take effect.

5. 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 libsapjco3.so file into the /usr/local/jco directory, and then add the path to this directory in the LD_LIBRARY_PATH environment variable.

6. On a Microsoft Windows platform, ensure that the msvcr80.dll and msvcp80.dll files are in the c:\WINDOWS\system32 directory. If required, both files can be downloaded from various sources on the Internet.

> **Note:**
>
> If you are using Cluster setup, add CLASSPATH and LD_LIBRARY_PATH to each node.

7. If you are using IBM WebSphere Application Server, perform the following steps:

   a. Copy the following files to WEBSPHERE_HOME/AppServer/lib:

      libsapjco3.so

      sapidoc3.jar

      sapjco3.jar

      For example, copy the preceding files to /home/shareuser/R2PS1ST1WAS/IBM/WebSphere/AppServer/lib

   b. Update the *PROFILE_HOME*/bin/setupCmdLine.sh file as shown in the following example:

      ```
      WAS_CLASSPATH="$WAS_HOME"/properties:"$WAS_HOME"/lib/
      startup.jar:"$WAS_HOME"/lib/bootstrap.jar:"$WAS_HOME"/lib/
      lmproxy.jar:"$WAS_HOME"/lib/urlprotocols.jar:"$WAS_HOME"/lib/
      sapjco3.jar:"$WAS_HOME"/lib/sapidoc3.jar:"$JAVA_HOME"/lib/tools.jar
      ```

8. 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.

9. 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
   ```

The JCo classes and JCo library paths must be displayed in this dialog box.

2.1.2 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.

This section provides information on the following topics:

- Creating a Target System User Account for the SAP UM (SAP ERP or SAP CUA) Target
- Creating a Target System User Account for the SAP HR Target

2.1.2.1 Creating a Target System User Account for the SAP UM (SAP ERP or SAP CUA) Target

Oracle Identity Governance requires a target system user account to access the target system during connector operations.

To create a target system user account for the SAP UM target:

1. Create a CPIC User with the `S_IDOC_ALL` profile.
2. Add the following authorizations along with the corresponding default parameter values:
   - S_RFC
   - S_TABU_DIS
   - S_TABU_NAM
   - S_USER_AGR
   - S_USER_AUT

- S_USER_GRP
- S_USER_PRO
- S_USER_SAS
- S_USER_SYS

3. Modify the parameter values as follows:

   For S_RFC

   - ACTVT: `16`
   - RFC_NAME: `*`
   - RFC_TYPE: `FUGR`

   For S_TABU_DIS

   - ACTVT: `03`
   - DICBERCLS: `SUSR`

   For S_TABU_NAM

   - ACTVT: `03`
   - TABLE: `USH*, USR*, USZ*`

   For S_USER_AGR

   - ACTVT: `03, 22`
   - ACT_GROUP: `*`

   For S_USER_AUT

   - ACTVT: `03`
   - AUTH: `*`
   - OBJECT: `*`

   For S_USER_GRP

   - ACTVT: `01, 02, 03, 05, 06, 08, 22, 78, PP`
   - CLASS: `*`

   For S_USER_PRO

   - ACTVT: `03, 22`
   - PROFILE: `*`

   For S_USER_SAS

   - ACTVT: `01, 06, 22`
   - ACT_GROUP: `*`
   - CLASS: `*`
   - PROFILE: `*`
   - SUBSYSTEM: `*`

   For S_USER_SYS

   - ACTVT: `78`

- SUBSYSTEM: *

2.1.2.2 Creating a Target System User Account for the SAP HR Target

The connector uses a target system account to connect to the target system during reconciliation. This target system account must be a CPIC user to whom you assign a customized role with the S_IDOC_ALL profile, S_RFC authorization object, and PLOG authorization object.

Create user of type CPIC with the following privileges:

1. Assign `S_IDOC_ALL` profile.
2. Assign authorization object S_RFC with values:
   - ACTVT: `16`
   - RFC_NAME: *
   - RFC_TYPE: `FUGR, FUNC`
3. Assign authorization object PLOG with values:
   - INFORTY: *
   - ISTAT: *
   - OTYPE: `$$, O, P, S`
   - PLVAR: `01, RS`
   - PPFCODE: *
   - SUBTYP: *
4. Assign authorization object P_ORGIN with values:
   - AUTHC: `R`
   - INFTY: `0000-0003, 0006, 0105`
   - PERSA: *
   - PERSG: *
   - PERSK: *
   - SUBTY: *
   - VDSK1: *
5. Assign authorization object P_ORGINCON with values:
   - AUTHC: `R`
   - INFTY: `0000-0003, 0006, 0105`
   - PERSA: *
   - PERSG: *
   - PERSK: *
   - SUBTY: *
   - VDSK1: *
   - PROFL: *

6. Assign authorization object P_PERNR with values:
   - AUTHC: `R`
   - PSIGN: `E, I`
   - INFTY: `0000-0003, 0006, 0105`
   - SUBTY: `*`
7. Assign authorization object B_ALE_RECV with values:
   - EDI_MES: `HRMD_A`

> **Note:**
>
> You must configure the PLOG authorization object so that the values assigned to this object match the ones shown in Step 2 through 6. Only the Plan Version (PLVAR) object can be set according to your requirements.

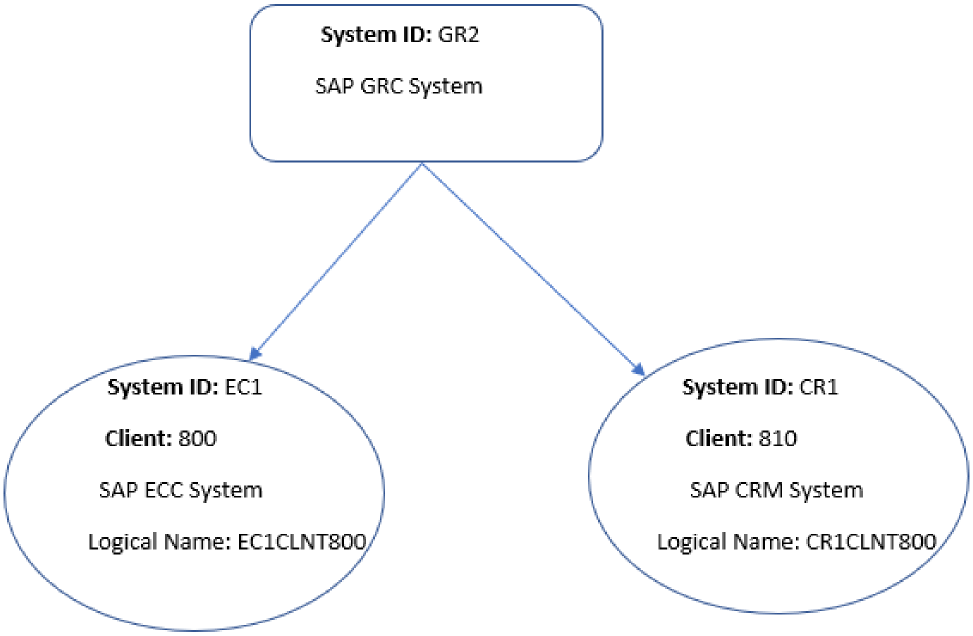
2.1.3 Assigning Roles to a User Account in a SAP Business Objects Access Control System for Connector Operations

You can perform connector operations such as Access Request Management and Access Risk Analysis through the SAP Business Objects Access Control system.

> **Note:**
>
> The naming convention of the connector name created in SAP Business Objects Access Control system should be synchronized with the logical name of the system to be integrated. To achieve this, a standard naming convention like *<SID>CLNT<XXX>* can be followed.

The below figure illustrates an example of the naming convention to be followed. According to this example, when a connector is created while integrating any system like ECC, CRM, SRM, or S/4 HANA with SAP Business Objects Access Control system, ensure to create an RFC destination of the system by following the standard naming convention which is synchronized with the logical name of the system.

Figure 2-1 Naming Convention For Connector Created in SAP Business Objects Access Control System



If you want to perform connector operations such as Access Request Management and Access Risk Analysis through the SAP Business Objects Access Control system, then assign the following minimum set of roles to a user account in SAP Business Objects Access Control:

Role Name	Description
SAP_BC_WEBSERVICE_CONSUMER	Web Service Consumer
SAP_GRC_NWBC	Governance, Risk, and Compliance
SAP_GRAC_ACCESS_APPROVER	Role for Access Request Approver
SAP_GRAC_RISK_OWNER	Risk Maintenance and Risk Analysis
SAP_GRAC_ROLE_MGMT_ROLE_OWNER	Role Owner

Apart from the default roles provided by SAP in the preceding table, you must add the additional authorizations to the user.

To create a target system user account for NW or S/4 HANA in an access control system:

1. Add the following authorizations along with the corresponding default parameter values:
   - GRFN_CONN
   - GRAC_SYS
   - GRAC_ROLER
   - GRAC_RISK

- GRAC_REQ
- GRAC_RA
- S_USER_GRP
- GRFN_USER
- GRAC_ROLED
- GRAC_ROLEP
- GRAC_EMPLY
- GRAC_USER
- S_CTS_ADMI
- S_CTS_SADM
- GRAC_ACTN
- GRAC_FFOWN

2. Modify the parameter values as follows:

   For GRFN_CONN

   - ACTVT: `16`
   - GRCFN_CONN: *

   For GRAC_SYS

   - ACTVT: `01, 02, 03, 78`
   - GRAC_APPTY: *
   - GRAC_ENVRM: *
   - GRAC_SYSID: *

   For GRAC_ROLER

   - ACTV: `16`
   - GRAC_OUNIT: *
   - GRAC_ROLE: *
   - GRAC_ROTYP: *
   - GRAC_SYSID: *

   For GRAC_RISK

   - ACTVT: `16`
   - GRAC_BPROC: *
   - GRAC_RISK: *
   - GRAC_RLVL: *
   - GRAC_RSET: *
   - GRAC_RTYPE: *

   For GRAC_REQ

   - ACTVT: `01, 02, 03`

- GRAC_BPROC: *
- GRAC_FNCAR: *
- GRAC_RQFOR: *
- GRAC_RQINF: *
- GRAC_RQTYPE: *

For GRAC_RA

- ACTVT: `16, 70`
- GRAC_OTYPE: *
- GRAC_RAMOD: `1, 2, 3, 4, 5`
- GRAC_REPT: `01, 02, 03, 04, 05`

For S_USER_GRP

- ACTVT: `03`
- CLASS: *

For GRFN_USER_GRP

- ACTVT: *

For GRAC_ROLED

- GRAC_ACTRD: `03, FS`
- GRAC_BPROC: *
- GRAC_LDSCP: *
- GRAC_RLSEN: *
- GRAC_RLTYP: *
- GRAC_ROLE: *

For GRAC_ROLEP

- ACTVT: `78`
- GRAC_BPROC: *
- GRAC_OUNIT: *
- GRAC_RLTYP: *
- GRAC_ROLE: *
- GRAC_SYSID: *

For GRAC_USER

- ACTVT: `01, 02, 03`
- GRAC_CLASS: *
- GRAC_OUNIT: *
- GRAC_SYSID: *
- GRAC_USER: *
- GRAC_UTYPE: *

For GRAC_EMPLY

- ACTVT: `01, 02, 03`
- GRAC_COMP: *
- GRAC_COSTC: *
- GRAC_DEPT: *
- GRAC_LOCTN: *

For GRAC_FFOWN

- ACTVT: *
- GRAC_OWN_T: *
- GRAC_SYSID: *
- GRAC_USER: *

For GRAC_ACTN

- GRAC_ACTN: `HOLD`
- GRFNMW_PRC: *

For S_CTS_SADM

- CTS_ADMFC: *
- DESTSYS: *
- DOMAIN: *

For S_CTS_ADMI

- CTS_ADMFCT: *

2.2 Installation

You must install the connector in Oracle Identity Manager. If necessary, you can also deploy the connector in a Connector Server.

The following topics provide details on installing the SAP UM connector:

- To run the connector code locally in Oracle Identity Manager, perform the procedure described in Installing the Connector in Oracle Identity Manager.
- To run the connector code remotely in a Connector Server, perform the procedures described in Installing the Connector in Oracle Identity Manager and Deploying the Connector Bundle in a Connector Server.

2.2.1 Installing the Connector in Oracle Identity Manager

In this scenario, you install the connector in Oracle Identity Manager using the Connector Installer:

> **Note:**
>
> 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 Enabling Request-Based Provisioning if you want to use the request-based provisioning feature for this target system.

To run the Connector Installer:

1. Download the connector package (ZIP file) from Oracle Technology Network and extract the connector package. Then, copy the contents into the following directory:

   OIM_HOME/server/ConnectorDefaultDirectory

2. If you are using Oracle Identity Manager release 11.1.1.*x*, perform the following steps:

   a. Log in to Oracle Identity System Administration by using the user account described in Creating the User Account for Installing Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

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

3. If you are using Oracle Identity Manager release 11.1.2.*x*, perform the following steps:

   a. Log in to Oracle Identity System Administration.

   b. In the left pane, under System Management, click **Manage Connector.**

4. In the Manage Connector page, click **Install.**

5. 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 in Step 1.

   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***.

6. Click **Load**.

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

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector XML files (by using the Deployment Manager)

   c. Compilation of adapters

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

- Retry the installation by clicking **Retry.**
- Cancel the installation and begin again from Step 5.

8. 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 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

      The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled jobs

      The procedure to configure these scheduled tasks is described later in this guide.

2.2.2 Deploying the Connector Bundle in a Connector Server

You can deploy the connector either locally in Oracle Identity Manager or remotely in the Connector Server. A Connector Server is an application that enables remote execution of an Identity Connector, such as the SAP User Management connector.

> **Note:**
>
> - To deploy the connector bundle remotely in a Connector Server, you must first deploy the connector in Oracle Identity Manager, as described in Installing the Connector in Oracle Identity Manager.
> - See Configuring the IT Resource for the Connector Server for related information.

This procedure can be divided into the following stages:

- Installing and Configuring the Connector Server
- Installing the Connector in the Connector Server
- Running the Connector Server

2.2.2.1 Installing and Configuring the Connector Server

Connector servers are available in two implementations:

- As a .Net implementation that is used by Identity Connectors implemented in .Net
- As a Java implementation that is used by Java-based Identity Connectors

The SAP User Management connector is implemented in Java, so you must deploy this connector to a Java Connector Server.

Use the following steps to install and configure the Java Connector Server:

> **Note:**
>
> Before you deploy the Java Connector Server, ensure that you install the JDK or JRE on the same computer where you are installing the Java Connector Server and that your *JAVA_HOME* or *JRE_HOME* environment variable points to this installation.

1. Create a new directory on the computer where you want to install the Java Connector Server.

   > **Note:**
   >
   > In this guide, *CONNECTOR_SERVER_HOME* represents this directory.

2. Unzip the Java Connector Server package in the new directory created in Step 1. You can download the Java Connector Server package from the Oracle Technology Network.
3. Open the ConnectorServer.properties file located in the `conf` directory. In the ConnectorServer.properties file, set the following properties, as required by your deployment.

Property	Description
connectorserver.port	Port on which the Java Connector Server listens for requests. Default value: `8759`
connectorserver.bundleDir	Directory where the connector bundles are deployed. Default value: `bundles`
connectorserver.libDir	Directory in which to place dependent libraries. Default value: `lib`

Property	Description
connectorserver.usessl	If set to **`true`**, the Java Connector Server uses SSL for secure communication. Default value: `false` If you specify **`true`**, use the following options on the command line when you start the Java Connector Server: • `-Djavax.net.ssl.keyStore` • `-Djavax.net.ssl.keyStoreType` (*optional*) • `-Djavax.net.ssl.keyStorePassword`
connectorserver.ifaddress	Bind address. To set this property, uncomment it in the file (if necessary). The bind address can be useful if there are more NICs installed on the computer.
connectorserver.key	Java Connector Server key.

4. Set the properties in the ConnectorServer.properties file, as follows:
   - To set the connectorserver.key, run the Java Connector Server with the `/setKey` option.

     > **Note:**
     >
     > For more information, see Running the Connector Server.

   - For all other properties, edit the ConnectorServer.properties file manually.
5. The conf directory also contains the logging.properties file, which you can edit if required by your deployment.

> **Note:**
>
> Oracle Identity Manager has no built-in support for testing the Connector Server configuration.

2.2.2.2 Installing the Connector in the Connector Server

> **See Also:**
>
> Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing and configuring connector server and running the connector server.

To deploy the SAP User Management connector into the Java Connector Server:

1. Stop the Java Connector Server.

> **Note:**
>
> You can download the necessary Java Connector Server from the Oracle Technology Network web page.

2. From the installation media, copy the SAP User Management the bundle\org.identityconnectors.sap-1.0.11170.jar file to the *CONNECTOR_SERVER_HOME*\lib directory.

> **Note:**
>
> - Copy SAP User Management third party libraries (sapjco3.jar) into the CONNECTOR_SERVER_HOME\lib directory.
> - Use org.identityconnectors.sapacum-1.0.11170.jar file if you are using SAP BusinessObjects AC system.

3. From the installation media, copy the SAP User Management the lib\sap-oim-integration.jar file to the *CONNECTOR_SERVER_HOME*\lib directory.

> **Note:**
>
> Use sapac-oim-integration.jar file if you are using SAP BusinessObjects AC system.

4. Start the Connector Server for the connector bundle to be picked up by the Connector Server.

2.2.2.3 Running the Connector Server

To run the Java Connector Server, use the ConnectorServer.bat script as follows:

1. Ensure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Installing and Configuring the Connector Server.
2. Change to the *CONNECTOR_SERVER_HOME*\bin directory and find the ConnectorServer.bat script.

   The ConnectorServer.bat supports the following options:

Option	Description

`/install [`*`serviceName`*`]`
`["-J `*`java-option`*`"]`
	Installs the Java Connector Server as a Windows service.
	Optionally, you can specify a service name and Java options. If you do not specify a service name, the default name is `ConnectorServerJava`.

Option	Description
/run ["-J *java-option*"]	Runs the Java Connector Server from the console. Optionally, you can specify Java options. For example, to run the Java Connector Server with SSL: ConnectorServer.bat /run "-J-Djavax.net.ssl.keyStore=mykeystore.jks" "-J-Djavax.net.ssl.keyStorePassword=***password***"
/setKey [*key*]	Sets the Java Connector Server key. The ConnectorServer.bat script stores the hashed value of the key in the connectorserver.key property in the ConnectorServer.properties file.
/uninstall [*serviceName*]	Uninstalls the Java Connector Server. If you do not specify a service name, the script uninstalls the ConnectorServerJava service.

3. If you need to stop the Java Connector Server, stop the respective Windows service.

2.3 Postinstallation

Postinstallation for the connector involves configuring Oracle Identity Manager, enabling logging to track information about all connector events, and configuring SoD. It also involves performing some optional configurations such as configuring ports on the target system, enabling the reset password option in OIM, setting up the configuration lookup definitions in OIM, changing the required input locale and so on.

Postinstallation steps are divided across the following sections:

- Configuring Ports on the Target System
- Configuring the Target System to Enable Propagation of User Password Changes
- Configuring Oracle Identity Manager 11.1.2 or Later
- Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later
- Setting Up the Configuration Lookup Definition in Oracle Identity Manager
- Enabling Request-Based Provisioning
- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Managing Logging
- Configuring the Access Request Management Feature of the Connector
- Configuring SoD (Segregation of Duties)
- Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System
- Configuring the IT Resource
- Configuring the IT Resource for the Connector Server
- Downloading WSDL files from SAP BusinessObjects AC
- Localizing Field Labels in UI Forms

- Synchronizing the SAPUM Process Form Field Length Needs with the Target Field Length

> **Note:**
>
> The field length of the values of an attribute coming from the SAPUM Process form should be in bounds of the length of values of attributes in the target system.

2.3.1 Configuring Ports on the Target System

You can configure ports to enable communication between the target system and Oracle Identity Manager.

To enable communication between the target system and Oracle Identity Manager, you must ensure that the ports listed in Table 2-1 are open.

Table 2-1 Ports for SAP Services

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

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

2.3.2 Configuring the Target System to Enable Propagation of User Password Changes

This section describes the procedures involved in configuring the target system to enable propagation of 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:

- Gathering Required Information
- Creating an Entry in the BAPIF4T Table
- Importing the Request

2.3.2.1 Gathering Required Information

The following information is required to configure the target system:

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.

- 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

2.3.2.2 Creating an Entry in the BAPIF4T Table

The User Group field is one of the fields that holds user data in SAP. F4 values are values of a field that you can view and select from a list. To view F4 values of the User Group field, you must create an entry in the BAPIF4T table by running the SM30 transaction. Ensure that the entry in the table includes XUCLASS as the data element and ZXL_PARTNER_BAPI_F4_AUTHORITY as the function name.

2.3.2.3 Importing the Request

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

Object Type	Object Name
Package	ZXLC
Function Group	ZXLCGRP ZXLCHLPVALUES ZXLCPRF ZXLCRL ZXLCUSR
Message class	ZXLCBAPI
Program	ZLCF4HLP_DATA_DEFINITIONS ZLCMS01CTCO ZLCMS01CTCO1 ZLCMS01CTP2 ZXLCGRP ZXLCHLPVALUES ZXLCPRF ZXLCRL ZXLCUSR
Search Help	ZXLC_ROLE ZXLC_SYS

Object Type	Object Name
Business object types	ZXLCGRP ZXLCHLP ZXLCPRF ZXLCRL ZXLCUSR
Table	ZXLCBAPIMODE ZXLCBAPIMODM ZXLCGROUPS ZXLCPRF ZXLCROLE ZXLCSTRING ZXLCSYSNAME

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 extracting the request files and performing the request import operation as follows:

1. Using SAPCAR utility, extract the Cofile and Data file from "xlsapcar.sar" as:

   xlsapcar.sar file location <Connecter Binaries>/sar

   - K900397.G10
   - R900397.G10
2. Import the request in target SAP system.

2.3.3 Configuring Oracle Identity Manager 11.1.2 or Later

You must create an UI form and an application instance for the resource against which you want to perform reconciliation and provisioning operations. In addition, you must run entitlement and catalog synchronization jobs.

These procedures are described in the following sections:

- Creating and Activating a Sandbox
- Creating a New UI Form
- Creating an Application Instance
- Publishing a Sandbox
- Harvesting Entitlements and Sync Catalog
- Updating an Existing Application Instance with a New Form

2.3.3.1 Creating and Activating a Sandbox

You must create and activate a sandbox to begin using the customization and form management features. You can then publish the sandbox to make the customizations available to other users.

See Managing Sandboxes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for instructions on creating and activating a sandbox.

2.3.3.2 Creating a New UI Form

You can use Form Designer in Oracle Identity System Administration to create and manage application instance forms.

See Managing Forms in *Oracle Fusion Middlware Administering Oracle Identity Manager* for instructions on creating a new UI form. While creating the UI form, ensure that you select the resource object corresponding to the Concur connector that you want to associate the form with. In addition, select the **Generate Entitlement Forms** check box..

2.3.3.3 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see Managing Application Instances in *Oracle Fusion Middlware Administering 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.

2.3.3.4 Publishing a Sandbox

Before publishing a sandbox, perform the following procedure as a best practice to validate all sandbox changes made till this stage as it is difficult to revert the changes after a sandbox is published:

1. In Identity System Administration, deactivate the sandbox.
2. Log out of Identity System Administration.
3. Log in to Identity Self Service using the xelsysadm user credentials and then activate the sandbox that you deactivated in Step 1.
4. In the Catalog, ensure that the Concur application instance form appears with correct fields.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for instructions on publishing a sandbox.

2.3.3.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Scheduled Jobs for Lookup Field Synchronization and Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

2.3.3.6 Updating an Existing Application Instance with a New Form

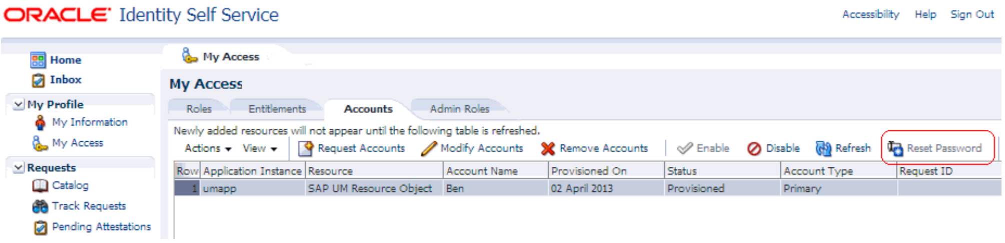
For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in Creating and Activating a Sandbox.
2. Create a new UI form for the resource as described in 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 Publishing a Sandbox.

2.3.4 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:



Newly added resources will not appear until the following table is refreshed.

Row	Application Instance	Resource	Account Name	Provisioned On	Status	Account Type	Request ID
1	umapp	SAP UM Resource Object	Ben	02 April 2013	Provisioned	Primary	

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 Administration.
2. In the left pane, under Configuration, 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:

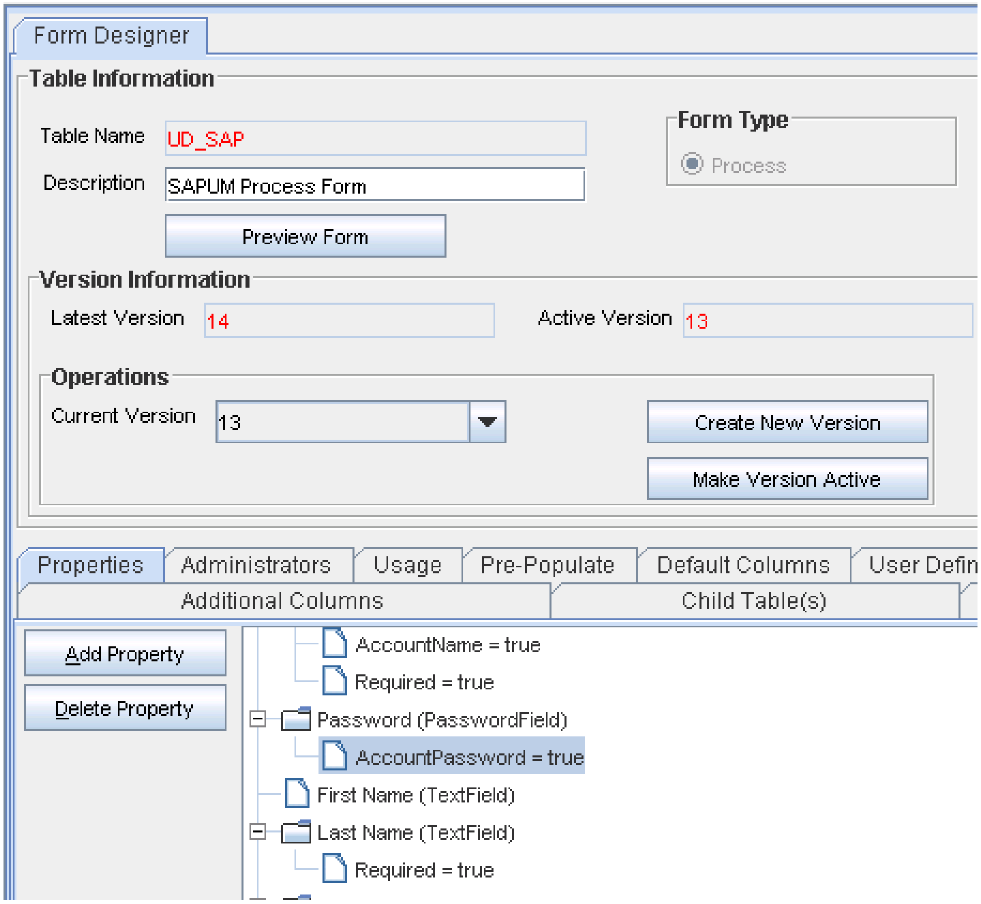
    

    Table Information

    Table Name: UD_SAP

    Description: SAPUM Process Form

    Form Type: ● Process

    Version Information

    Latest Version: 14

    Active Version: 13

    Operations

    Current Version: 13

    AccountName = true
    Required = true
    Password (PasswordField)
    AccountPassword = true
    First Name (TextField)
    Last Name (TextField)
    Required = true

12. Click **Make Version Active.**

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

2.3.5 Setting Up the Configuration Lookup Definition in Oracle Identity Manager

When you deploy the connector, configuration lookup definitions are created in Oracle Identity Manager.

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

- Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts
- Configuring Password Changes for Newly Created Accounts
- Setting up the Lookup Definition for Connection Pooling

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 parameters of the Advanced Settings section:

- validatePERNR: 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.
- overwriteLink: You enter `yes` as the value if you want existing links in SAP to be overwritten by the ones set up through provisioning operations.

The following topics provide detailed information about the linking process:

- About the Linking Process
- Enabling Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts

2.3.5.1.1 About the Linking Process

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.

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.

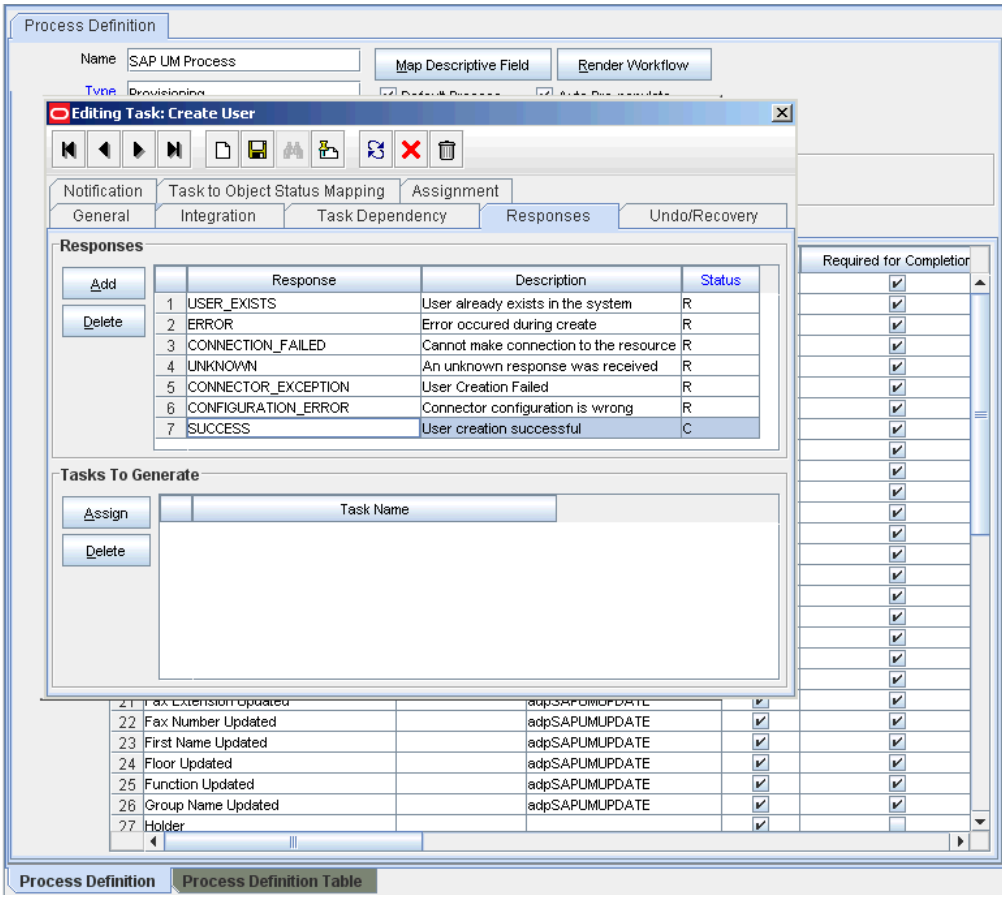
2. To provision an SAP R/3 or SAP CUA account for John, you enter and submit the required data on Oracle Identity System Administration.
3. The connector looks for the user's SAP HRMS account. If you entered `yes` as the value of validatePERNR attribute, then the connector checks for a match for the 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 overwriteLink advanced settings parameter 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 overwriteLink advanced settings parameter 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. 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.

2.3.5.1.2 Enabling Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts

To enable linking of SAP HRMS and SAP R/3 or SAP CUA accounts, perform the following steps:

1. In the Design Console, expand **Process Management** and then double-click **Process Definition.**
2. Search for and open the **SAP UM Process** form.
3. Double-click the **Create User** task to open the Editing Task:Create User dialog box.
4. In the Responses tab, select the **SUCCESS** response, as shown in the following screenshot.



Name: SAP UM Process

Type: Provisioning

Responses

	Response	Description	Status
1	USER_EXISTS	User already exists in the system	R
2	ERROR	Error occured during create	R
3	CONNECTION_FAILED	Cannot make connection to the resource	R
4	UNKNOWN	An unknown response was received	R
5	CONNECTOR_EXCEPTION	User Creation Failed	R
6	CONFIGURATION_ERROR	Connector configuration is wrong	R
7	SUCCESS	User creation successful	C

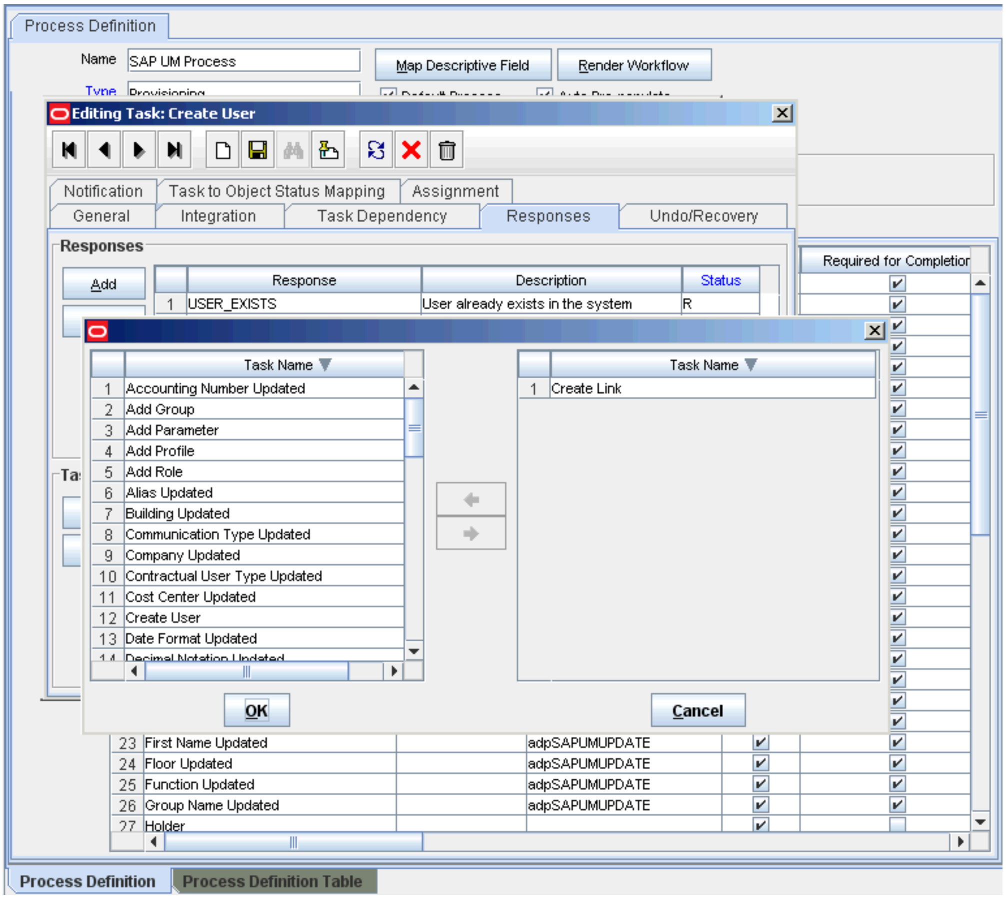
Tasks To Generate

	Task Name

					Required for Completion
21	Fax Extension Updated		adpSAPUMUPDATE	☑	☑
22	Fax Number Updated		adpSAPUMUPDATE	☑	☑
23	First Name Updated		adpSAPUMUPDATE	☑	☑
24	Floor Updated		adpSAPUMUPDATE	☑	☑
25	Function Updated		adpSAPUMUPDATE	☑	☑
26	Group Name Updated		adpSAPUMUPDATE	☑	☑
27	Holder			☑	□

5. Click **Assign.**

6. In the new dialog box, select the **Create Link** task, as shown in the following screenshot.



Name: SAP UM Process

Type: Provisioning

Responses

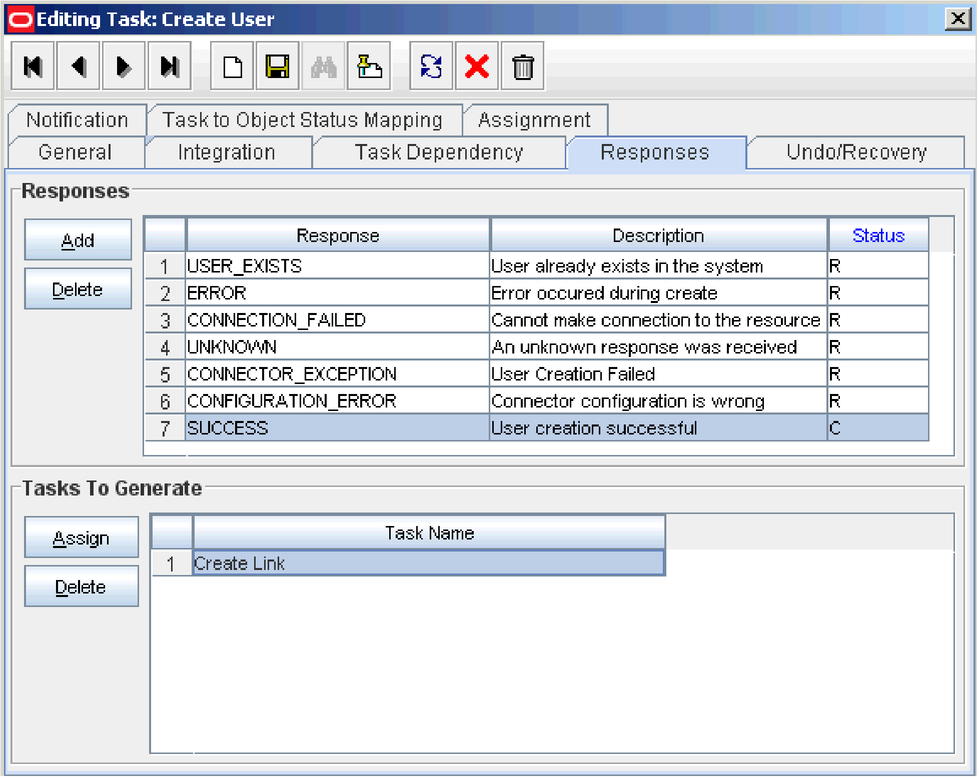
	Response	Description	Status
1	USER_EXISTS	User already exists in the system	R

	Task Name
1	Accounting Number Updated
2	Add Group
3	Add Parameter
4	Add Profile
5	Add Role
6	Alias Updated
7	Building Updated
8	Communication Type Updated
9	Company Updated
10	Contractual User Type Updated
11	Cost Center Updated
12	Create User
13	Date Format Updated
14	Decimal Notation Updated

	Task Name
1	Create Link

					Required for Completion
23	First Name Updated		adpSAPUMUPDATE	☑	☑
24	Floor Updated		adpSAPUMUPDATE	☑	☑
25	Function Updated		adpSAPUMUPDATE	☑	☑
26	Group Name Updated		adpSAPUMUPDATE	☑	☑
27	Holder			☑	□

7. The Create Link task will appear in the Tasks To Generate region for the SUCCESS response, as shown in the following screenshot.



Responses

	Response	Description	Status
1	USER_EXISTS	User already exists in the system	R
2	ERROR	Error occured during create	R
3	CONNECTION_FAILED	Cannot make connection to the resource	R
4	UNKNOWN	An unknown response was received	R
5	CONNECTOR_EXCEPTION	User Creation Failed	R
6	CONFIGURATION_ERROR	Connector configuration is wrong	R
7	SUCCESS	User creation successful	C

Tasks To Generate

	Task Name
1	Create Link

8. Save the changes and close the dialog box.

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 Governance, password management can be configured by using the changePasswordAtNextLogon parameter of the Advanced Settings section.

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 changePasswordAtNextLogon parameter to `yes`. 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.

- Configure the connector so that the password set while creating the account on Oracle Identity Governance 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 value of changePasswordAtNextLogon parameter to `no` and enter a string in the dummyPassword parameter of the Basic Configuration Section. With these settings, when you create a user account through Oracle Identity Governance, 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.

2.3.5.3 Setting up the Lookup Definition for Connection Pooling

By default, this connector uses the ICF connection pooling. Table 2-2 lists the connection pooling properties, their description, and default values set in ICF:

Table 2-2 Connection Pooling Properties

Property	Description
Pool Max Idle	Maximum number of idle objects in a pool. Default value: `10`
Pool Max Size	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`
Pool Min Evict Idle Time	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	Minimum number of idle objects in a pool. Default value: `1`

If you want to modify the connection pooling properties to use values that suit requirements in your environment, then:

1. Log in to the Design Console.
2. Expand **Administration,** and then double-click **Lookup Definition.**
3. Search for and open the configuration lookup definition for the target system your are using.

   For example, open Lookup.SAPABAP.Configuration.
4. On the Lookup Code Information tab, click **Add.**

   A new row is added.
5. In the **Code Key** column of the new row, enter `Pool Max Idle`.
6. In the **Decode** column of the new row, enter a value corresponding to the Pool Max Idle property.
7. Repeat Steps 4 through 6 for adding each of the connection pooling properties listed in Table 2-2.
8. Click the save icon.

2.3.6 Enabling Request-Based Provisioning

In request-based provisioning, an end user creates a request for a resource or entitlement by using Oracle Identity System Administration. 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 the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1.*x*.
>
> Do *not* enable request-based provisioning if you want to use the direct provisioning feature of the connector.

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.

The following sections discuss the steps to be performed to enable request-based provisioning:

- Approver's Role in Request-Based Provisioning
- Importing Request Datasets Using Deployment Manager
- End User's Role in Request-Based Provisioning
- Enabling the Auto Save Form Feature
- Running the PurgeCache Utility

2.3.6.1 Approver's Role in Request-Based Provisioning

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

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

   A message confirming that the task was approved is displayed.

2.3.6.2 Importing Request Datasets Using Deployment Manager

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

To import a request dataset XML file by using the Deployment Manager:

1. Log in to Oracle Identity System Administration.
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 request dataset XML file, SAPUM-Datasets.xml, which is in the xml directory of 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**.

8. Close the Deployment Manager dialog box.

   The request dataset is imported into Oracle Identity Manager.

2.3.6.3 End User's Role in Request-Based Provisioning

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

1. Log in to the Administrative User Console.

2. On the Welcome page, click **Advanced** in the upper-right corner of the page.

3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.

4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.

5. From the Request Template list, select **Provision Resource** and click **Next**.

6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.

7. From the **Available Users** list, select the user to whom you want to provision the account.

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.

8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.

9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.

10. From the Available Resources list, select **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

A message confirming that your request has been sent successfully is displayed along with the Request ID.

13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

2.3.6.4 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.

2.3.6.5 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See 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 Oracle Identity Manager database. 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, 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:
   >
   > `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`

   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.

2.3.9 Managing Logging

Oracle Identity Manager uses the Oracle Diagnostic Logging (ODL) logging service for recording all types of events pertaining to the connector.

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

2.3.9.1 Understanding Log Levels

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.

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 2-3.

Table 2-3 Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1

Table 2-3 (Cont.) Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

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

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

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

2.3.9.2 Enabling Logging

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

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

<logger name="ORG.IDENTITYCONNECTORS.SAP" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="sap-handler"/>
     <handler name="console-handler"/>
   </logger>
```

   If you are using SAP BusinessObjects AC, then add the following block:

```
<logger name="ORG.IDENTITYCONNECTORS.SAPAC" level="[Log_LEVEL]"
useParentHandlers="false">
     <handler name="sap-handler"/>
     <handler name="console-handler"/>
</logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2-3 lists the supported message type and level combinations.

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

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

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

<logger name="ORG.IDENTITYCONNECTORS.SAP" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="sap-handler"/>
     <handler name="console-handler"/>
   </logger>
```

If you are using SAP BusinessObjects AC, then add the following block:

```
<logger name="ORG.IDENTITYCONNECTORS.SAPAC" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="sap-handler"/>
     <handler name="console-handler"/>
</logger>
```

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

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

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

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

Note:

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

2.3.10 Configuring the Access Request Management Feature of the Connector

Access Request Management is a module in the SAP BusinessObjects AC suite. In an SAP environment, you can set up Access Request Management as the front end for receiving account creation and modification provisioning requests. In Access Request Management, workflows for processing these requests can be configured and users designated as approvers act upon these requests.

Oracle Identity Manager can be configured as the medium for sending provisioning requests to SAP BusinessObjects AC Access Request Management. A request from Oracle Identity Manager is sent to Access Request Management, 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 Access Request Management feature, it is recommended that you read the guidelines described in Guidelines on Using a Deployment Configuration

The following sections provide information about configuring the Access Request Management feature:

- Specifying Values for the GRC-ITRes IT Resource
- Configuring Request Types and Workflows on SAP BusinessObjects AC Access Request Management

2.3.10.1 Specifying Values for the GRC-ITRes IT Resource

The GRC-ITRes IT resource holds information that is used during communication with SAP BusinessObjects AC Access Request Management. 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 11.1.1.*x*:

     Log in to Oracle Identity System Administration.
   - For Oracle Identity Manager release 11.1.2.*x:*

     Log in to Oracle Identity System Administration.
2. If you are using Oracle Identity Manager release 11.1.1.*x*, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.

3. If you are using Oracle Identity Manager release 11.1.2.*x*, then, in the left pane under Configuration, click **IT Resource.**
4. In the IT Resource Name field on the Manage IT Resource page, enter `GRC-ITRes` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource.

   Table 2-4 lists the parameters of the GRC-ITRes IT resource.

Table 2-4   Parameters of the GRC-ITRes IT Resource

Parameter	Description
Configuration Lookup	Enter the name of the configuration lookup definition. For SAP BusinessObjects AC 10: `Lookup.SAPAC10ABAP.Configuration`
language	Enter the two-letter code for the language set on the target system. Sample value: `EN`
Connector Server Name	Name of the IT resource of the type "Connector Server." You create an IT resource for the Connector Server in Configuring the IT Resource for the Connector Server. **Note:** Enter a value for this parameter only if you have deployed the SAP User Management connector in the Connector Server.
password	Enter the password of the account created on Access Request Management system.
port	Enter the number of the port at which Access Request Management system is listening. Sample value: `8090`
server	Enter the IP address of the host computer on which Access Request Management system is listening. Sample value: `10.231.231.231`
username	Enter the user name of an account created on Access Request Management system. This account is used to call Access Request Management system APIs that are used during request validation. Sample value: `jdoe`

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

2.3.10.2 Configuring Request Types and Workflows on SAP BusinessObjects AC Access Request Management

You must create and configure request types and workflows on SAP BusinessObjects AC Access Request Management for provisioning operations.

1. Create a request type in SAP BusinessObjects AC Access Request Management.

   A request type In SAP BusinessObjects AC Access Request Management 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 BusinessObjects AC Access Request Management. The Lookup.SAPAC10ABAP.Configuration lookup definition maps request types to provisioning operations submitted through Oracle Identity Manager.

2. Create an access request workflow using the MSMP (Multi Step Multi process) Workflow Engine.

2.3.11 Configuring SoD (Segregation of Duties)

SoD is a process that ensures that every individual is given access to only one module of a business process and will not be able to access other modules to reduce risk of fraud and error.

This section discusses the following procedures:

- Configuring SAP BusinessObjects AC to Act As the SoD Engine
- Specifying Values for the GRC-ITRes IT Resource
- Verifying Entries Created in the Lookup.SAPABAP.System Lookup Definition
- Specifying a Value for the TopologyName IT Resource Parameter
- 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.
> - In the Lookup.SAPABAP.Configuration lookup definition, you must change the Decode value of the SOD Configuration lookup entry.
>
>   By default, the Decode value of this entry is Lookup.SAPAC10ABAP.Configuration.

2.3.11.1 Configuring SAP BusinessObjects AC to Act As the SoD Engine

To configure SAP BusinessObjects AC to act as the SoD engine, see Using Segregation of Duties in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* at for 11*g* Release 1 (11.1.2).

2.3.11.2 Specifying Values for the GRC-ITRes IT Resource

The GRC-ITRes IT resource holds information that is used by the connector during SoD operations. This IT resource is the same as the one used by the Access Request Management feature for both Oracle Identity Manager.

See Specifying Values for the GRC-ITRes IT Resource for the procedure to set values for the parameters of this IT resource.

2.3.11.3 Verifying Entries Created in the Lookup.SAPABAP.System Lookup Definition

The Lookup.SAPABAP.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.

2.3.11.4 Specifying a Value for the TopologyName IT Resource Parameter

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

- Oracle Identity Manager installation
- SAP BusinessObjects AC installation
- SAP ERP installation

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

For more inofmration about this element, see Using Segregation of Duties in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for 11*g* Release 1 (11.1.2.0).

See Configuring the IT Resource for information about specifying values for parameters of the IT resource.

2.3.11.5 Disabling and Enabling SoD

This section describes the procedure to disable and enable SoD on Oracle Identity Governance.

- Disabling SoD on Oracle Identity Manager
- Enabling SoD on Oracle Identity Manager

2.3.11.5.1 Disabling SoD on Oracle Identity Manager

To disable SoD:

1. If you are using the Oracle Identity Manager release 11.1.1.*x*, then perform the following steps:
   a. Log in to Oracle Identity System Administration.
   b. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management tab, click **System Configuration.**
2. If you are using the Oracle Identity Manager release 11.1.2.*x*, then perform the following steps:
   a. Log in to Oracle Identity System Administration.
   b. In the left pane, under System Management, click **System Configuration.**

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

   System properties for SoD are displayed on the right pane.
5. In the Value box, enter `FALSE` to disable SoD.
6. Click **Save.**
7. Restart Oracle Identity Manager.

2.3.11.5.2 Enabling SoD on Oracle Identity Manager

To enable SoD:

1. If you are using Oracle Identity Manager release 11.1.1.*x*, then perform the following steps:
   a. Log in to Oracle Identity System Administration.
   b. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management tab, click **System Configuration.**
2. If you are using Oracle Identity Manager release 11.1.2.*x*, then perform the following steps:
   a. Log in to Oracle Identity System Administration.
   b. In the left pane, under System Management, click **System Configuration.**
3. 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.
4. Click the **XL.SoDCheckRequired** property name.

   System properties for SoD are displayed on the right pane.
5. In the Value box, enter `TRUE` to enable SoD.
6. Click **Save.**
7. Restart Oracle Identity Manager.

2.3.12 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:**
>
> For more information, see the SAP SNC Documentation.

This section discusses the following topics:

- Prerequisites for Configuring the Connector to Use SNC
- Installing the Security Package
- Configuring SNC

2.3.12.1 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.

2.3.12.2 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 can be downloaded directly from the SAP Service Marketplace.

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

   - SAP Cryptographic Library (sapcrypto.dll for Microsoft Windows or libsapcrypto.so for UNIX)
   - A corresponding license ticket (`ticket`)
   - The configuration tool, sapgenpse

   > **Note:**
   >
   > In this guide, `sapgenpse.exe` is used for Microsoft Windows and `sapgenpse` is used for UNIX.

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 file.

5. Create the sec directory inside the directory into which you copy the library and the sapgenpse 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:**
   >
   > Configuring SNC

7. Set the SECUDIR environment variable for the Oracle WebLogic 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.

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.

   For Linux: Export LD_LIBRARY_PATH and PATCH

2.3.12.3 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.

   Use one of the following ways to set up SNC on the SAP application server:

   - Certificate or User Mapping
   - Rule based Certificate Mapping

   If you do not want to map each user with the certificate and use batch processing, define a general rule-based certificate mapping to enable NetWeaver map user certificates automatically.

   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 ITResource IT resource object:

   - sncLib
   - sncName
   - sncPartnerName
   - sncProtectionLevel

- useSNC

2.3.13 Configuring the IT Resource

An IT resource for your target system is created after you install the connector. You configure this IT resource to let the connector connect Oracle Identity Manager with your target system.

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

- Parameters for Enabling the Use of a Logon Group
- Parameters for Enabling SNC-Based Communication
- Parameters for Enabling Multiple Attempts to Update Multivalued Attributes

The following section describes the parameters of the IT resource:

- Specifying Values for the IT Resource Parameters

2.3.13.1 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 2-5.

- jcoGroup
- loadBalance
- msHost
- msServ

In addition, perform the procedure described in Enabling SAP JCo Connectivity on the Oracle Identity Manager host computer to enable SAP JCo connectivity.

2.3.13.1.1 Enabling SAP JCo Connectivity

Perform the following procedure on the Oracle Identity Manager host computer to enable SAP JCo connectivity:

1. Open the following file in a text editor:

   For Microsoft Windows:

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

   For Solaris or Linux, open the following file:

   /etc/services
2. Add an entry in the following format:

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

```
sapmsSYSTEM_ID          36SYSTEM_NUMBER/tcp
```

For example:

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

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

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

For example:

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

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

2.3.13.2 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 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`.

2.3.13.3 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.

2.3.13.4 Specifying Values for the IT Resource Parameters

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

> **Note:**
>
> The ALL USERS group has INSERT, UPDATE, and DELETE permissions on the default IT resource. This is to ensure that end users can select the IT resource during request-based provisioning. If you create another IT resource, then you must assign INSERT, UPDATE, and DELETE permissions for the ALL USERS group on the IT resource.
>
> You must use Oracle Identity System Administration 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 11.1.1.*x*:

     Log in to Oracle Identity System Administration.
   - For Oracle Identity Manager release 11.1.2.*x:*

     Log in to Oracle Identity System Administration.
2. If you are using Oracle Identity Manager release 11.1.1.*x*, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.*x,* then, in the left pane under Configuration, click **IT Resource.**
4. In the IT Resource Name field on the Manage IT Resource page, enter `SAP UM ITResource` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2-5 describes the parameters of the SAP UM IT resource and Table 2-6 describes the parameters of the SAP AC UM IT resource.

Table 2-5   Parameters of the SAP UM IT Resource

Parameter	Description	Mandatory?
client	SAP client setting Default value: `000`	Yes
Configuration Lookup	Name of the lookup definition containing configuration information Default value: `Lookup.SAPABAP.Configuration`	Yes
configureConnectionTuning	Allows the connection properties to be customized when the SAP Destination is configured Default value: `FALSE`	No
connectionMaxGetTime	Maximum time to wait for a connection (specified in milliseconds)	No
connectionPoolActiveTime	Maximum number of active connections that can be created for a destination simultaneously	No
connectionPoolCapacity	Maximum number of idle connections that can be kept open by the destination	No
connectionPoolExpirationPeriod	Released connections are checked for expiration after waiting for this time period (specified in milliseconds)	No
connectionPoolExpirationTime	Freed connections held by the destination that can be closed after this amount of time (specified in milliseconds)	No
Connector Server Name	Name of the IT resource of the type "Connector Server." You create an IT resource for the Connector Server in Configuring the IT Resource for the Connector Server. **Note:** Enter a value for this parameter only if you have deployed the SAP User Management connector in the Connector Server.	No
destination	This value must be unique. This is a mandatory connection parameter needed for SAPJCo to interact with the SAP System. Sample value: `dest or dest123` (any random value) The value specified has to be unique to each instance of the IT Resource.	Yes
dummyPassword	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 Configuring Password Changes for Newly Created Accounts for more information about this parameter.	Mandatory
host	Host name of the resource	Mandatory
jcoGroup	Group of SAP application servers	Optional
jcoSAPRouter	SAP router string to be used for a system protected by a firewall	Optional
jcoTrace	Level of SAP JCO tracing to enable. Enter 0 or any positive integer up to and including 10. Default value: `0`	Optional
jcoTraceDir	Absolute path to the directory where the trace files will be created	Optional
language	Enter the two-letter code for the language set on the target system Default value: `EN`	Optional
loadBalance	Enter `TRUE` to enable the use of Logon Group Default value: `FALSE`	Optional

Table 2-5 (Cont.) Parameters of the SAP UM IT Resource

Parameter	Description	Mandatory?
masterSystem	Enter the RFC Destination value that is used for identification of the SAP system. This value must be same as that of the Logical System name. Sample value: `EH6CLNT001` Here the sample value is based on the following format used in SAP system: <*SYSTEM_ID*>CLNT<*CLIENT_NUM*> In this sample value, EH6 is the System ID of the target system and 001 is the client number.	Mandatory
maxBAPIRetries	Maximum Number retries for BAPI execution Default value: 5	Optional
msHost	Enter the host name of the message server	Optional
msServ	(Optional) SAP message server port to be used instead of the default sapms	Optional
password	When using normal authentication, password of the User account	Mandatory
r3Name	Enter the host name of the SAP R/3 or SAP CUA system	Optional
retryWaitTime	Connection retry wait time Default value: `500`	Optional
sncLib	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`	Optional
sncName	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`	Optional
sncPartnerName	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`	Optional
sncProtection Level	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	Optional

Table 2-5 (Cont.) Parameters of the SAP UM IT Resource

Parameter	Description	Mandatory?
sncX509Cert	The X509 certificate that does not contain the BEGIN CERTIFICATE or END CERTIFICATE strings when using SNC **Note:** You must remove all new line characters from the certificate.	Optional
systemNumber	SAP system number Default value: `00`	Mandatory
TopologyName	Name of the topology of the target system host computer Default value: `sodgrc`	Optional
user	When using normal authentication, a user name that has permissions to create new accounts	Mandatory
useSNC	Enter `TRUE,` if you want to configure secure communication between Oracle Identity Manager and the target system. Otherwise, enter `FALSE.` Default value: `FALSE`	Optional

Table 2-6 Parameters of the SAP AC UM IT Resource

Parameter	Description
client	SAP client setting Default value: `000`
Configuration Lookup	Name of the lookup definition containing configuration information Default value: `Lookup.SAPAC10ABAP.Configuration`
configureConnectionTuning	Allows the connection properties to be customized when the SAP Destination is configured Default value: `FALSE`
connectionMaxGetTime	Maximum time to wait for a connection (specified in milliseconds)
connectionPoolActiveTime	Maximum number of active connections that can be created for a destination simultaneously
connectionPoolCapacity	Maximum number of idle connections that can be kept open by the destination
connectionPoolExpirationPeriod	Released connections are checked for expiration after waiting for this time period (specified in milliseconds)
connectionPoolExpirationTime	Freed connections held by the destination that can be closed after this amount of time (specified in milliseconds)
Connector Server Name	Name of the IT resource of the type "Connector Server." You create an IT resource for the Connector Server in Configuring the IT Resource for the Connector Server. **Note:** Enter a value for this parameter only if you have deployed the SAP User Management connector in the Connector Server.
destination	This value must be unique. This is a mandatory connection parameter needed for SAPJCo to interact with the SAP System. Sample value: `dest or dest123` (any random value) The value specified has to be unique to each instance of the IT Resource.

Table 2-6 (Cont.) Parameters of the SAP AC UM IT Resource

Parameter	Description
dummyPassword	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 Configuring Password Changes for Newly Created Accounts for more information about this parameter.
grcLanguage	Enter the two-letter code for the language set on the GRC system. Sample value: `EN`
grcPassword	Enter Password of the GRC System.
grcUsername	Enter User name of the GRC System.
host	Host name of the resource
jcoGroup	Group of SAP application servers
jcoSAPRouter	SAP router string to be used for a system protected by a fire wall
jcoTrace	Level of SAP JCO tracing to enable. Enter 0 or any positive integer up to and including 10. Default value: `0`
jcoTraceDir	Absolute path to the directory where the trace files will be created
language	Enter the two-letter code for the language set on the target system Default value: `EN`
loadBalance	Enter `TRUE` to enable the use of Logon Group Default value: `FALSE`
masterSystem	Enter the RFC Destination value that is used for identification of the SAP system. This value must be same as that of the Logical System name. Sample value: `EH6CLNT001` Here the sample value is based on the following format used in SAP system: *<SYSTEM_ID>*CLNT*<CLIENT_NUM>* In this sample value, EH6 is the System ID of the target system and 001 is the client number.
maxBAPIRetries	Maximum Number retries for BAPI execution. Default value: `5`
msHost	Enter the host name of the message server
msServ	(Optional) SAP message server port to be used instead of the default sapms
password	When using normal authentication, password of the User account
r3Name	Enter the host name of the SAP R/3 or SAP CUA system
retryWaitTime	Connection retry wait time Default value: `500`
sncLib	Enter the full path and name of the crypto library on the target system host computer This is required only if SNC is enabled. Sample value: `c://usr//sap/sapcrypto.dll`

Table 2-6 (Cont.) Parameters of the SAP AC UM IT Resource

Parameter	Description
sncName	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`
sncPartnerName	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`
sncProtection Level	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
sncX509Cert	The X509 certificate that does not contain the BEGIN CERTIFICATE or END CERTIFICATE strings when using SNC **Note:** You must remove all new line characters from the certificate.
systemNumber	SAP system number Default value: `00`
TopologyName	Name of the topology of the target system host computer Default value: `sodgrc`
user	When using normal authentication, a user name that has permissions to create new accounts
useSNC	Enter `FALSE,` if you want to configure secure communication between Oracle Identity Manager and the target system. Otherwise, enter `TRUE.` Default value: `FALSE`

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

2.3.14 Configuring the IT Resource for the Connector Server

During the installation of the connector, a default IT resource for the connector server for SAP UM is created with the name, SAP UM IT Resource.

To create the IT resource for the Connector Server:

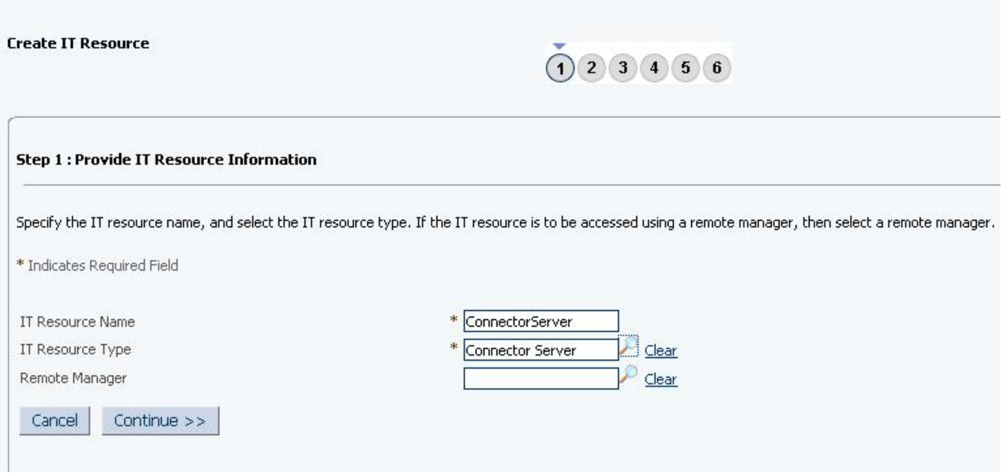
1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.*x*:

     Log in to Oracle Identity System Administration.
   - For Oracle Identity Manager release 11.1.2.*x:*

     Log in to Oracle Identity System Administration.

2. If you are using Oracle Identity Manager release 11.1.1.*x*, then:
   1. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   2. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Create IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.*x,* then:
   1. In the left pane under Configuration, click **IT Resource.**
   2. In the Manage IT Resource page, click **Create IT Resource.**
4. On the Step 1: Provide IT Resource Information page, perform the following steps:
   - **IT Resource Name**: Enter a name for the IT resource.
   - **IT Resource Type**: Select **Connector Server** from the IT Resource Type list.
   - **Remote Manager**: Do not enter a value in this field.
5. Click **Continue**. Figure 2-2 shows the IT resource values added on the Create IT Resource page.

Figure 2-2 Step 1: Provide IT Resource Information



Create IT Resource

Step 1 : Provide IT Resource Information

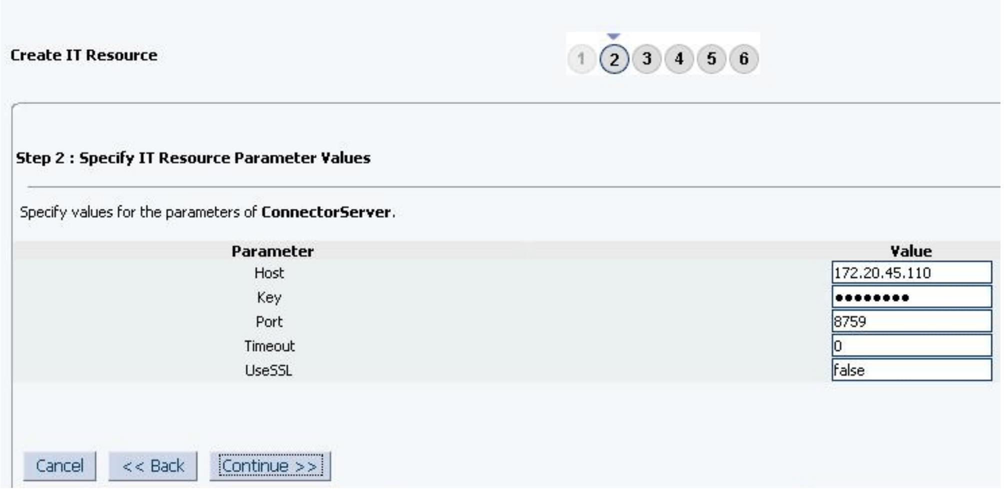
Specify the IT resource name, and select the IT resource type. If the IT resource is to be accessed using a remote manager, then select a remote manager.

* Indicates Required Field

IT Resource Name	* ConnectorServer	
IT Resource Type	* Connector Server	Clear
Remote Manager		Clear

6. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. Figure 2-3 shows the Step 2: Specify IT Resource Parameter Values page.

Figure 2-3   Step 2: Specify IT Resource Parameter Values



Create IT Resource

Step 2 : Specify IT Resource Parameter Values

Specify values for the parameters of **ConnectorServer**.

Parameter	Value
Host	172.20.45.110
Key	••••••••
Port	8759
Timeout	0
UseSSL	false

Table 2-7 provides information about the parameters of the IT resource.

> **Note:**
>
> See Step 8 of Installing and Configuring the Connector Server for the values to be specified for the parameters of the IT resource.

Table 2-7   Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: `myhost.com`
Key	Enter the key for the connector server.
Port	Enter the number of the port at which the connector server is listening. Default value: `8759`
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: `0` A value of 0 means that the connection never times out.
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter `false.` Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL between Oracle Identity Manager and Connector Server, see Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System.

7. On the Step 3: Set Access Permission to IT Resource page, the `SYSTEM ADMINISTRATORS` group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.

> **Note:**
>
> This step is optional.

If you want to assign groups to the IT resource and set access permissions for the groups, then:

a. Click **Assign Group**.

b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

c. Click **Assign**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

> **Note:**
>
> - This step is optional.
> - You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

a. Click **Update Permissions**.

b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

c. Click **Update**.

9. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

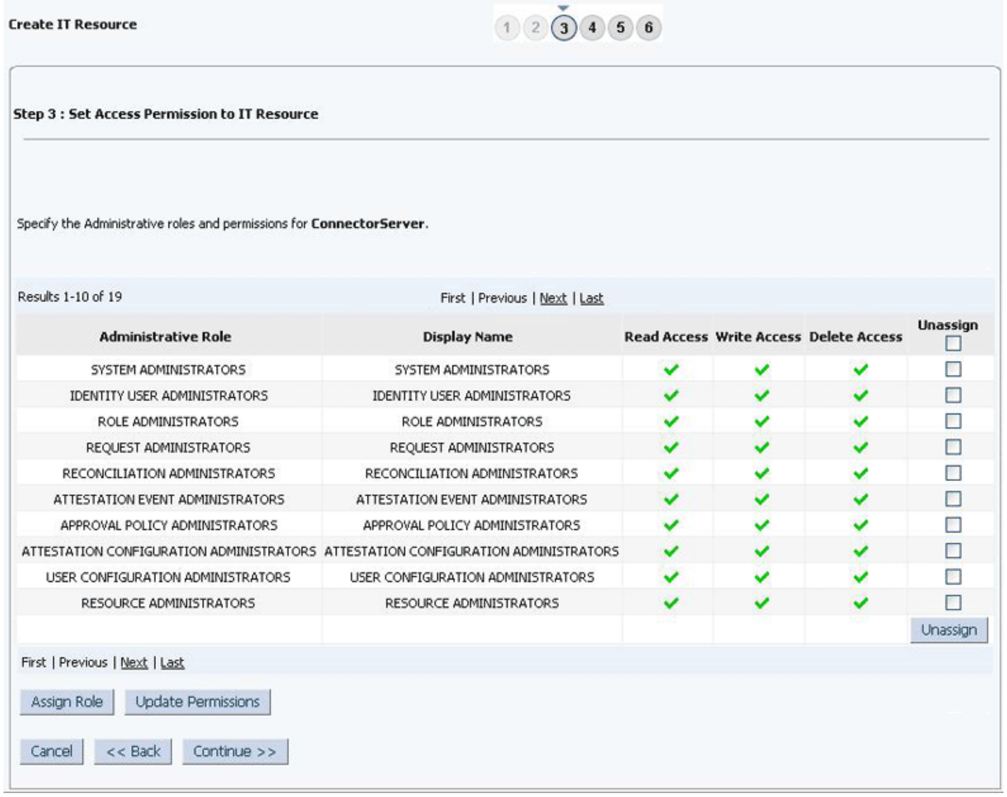
> **Note:**
>
> - This step is optional.
> - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

a. Select the **Unassign** check box for the group that you want to unassign.

b. Click **Unassign**.

10. Click **Continue**. Figure 2-4 shows the Step 3: Set Access Permission to IT Resource page.

Figure 2-4   Step 3: Set Access Permission to IT Resource



Create IT Resource

Step 3 : Set Access Permission to IT Resource

Specify the Administrative roles and permissions for **ConnectorServer**.

Results 1-10 of 19   First | Previous | Next | Last

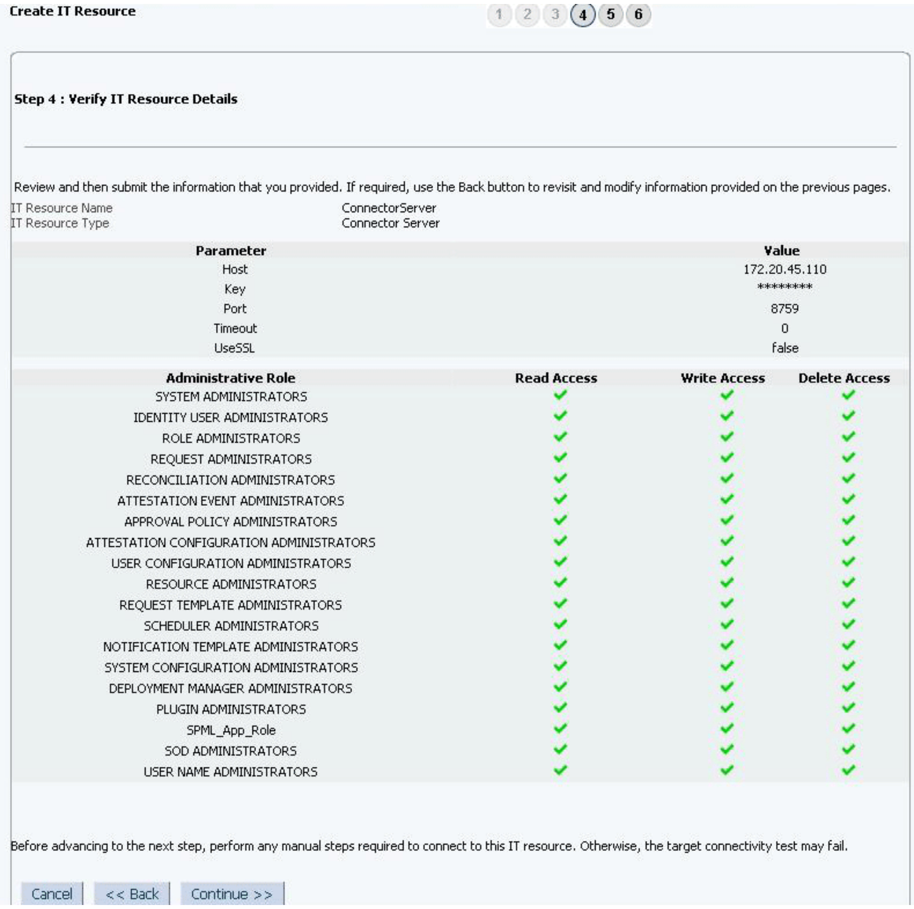
Administrative Role	Display Name	Read Access	Write Access	Delete Access	Unassign □
SYSTEM ADMINISTRATORS	SYSTEM ADMINISTRATORS	✓	✓	✓	□
IDENTITY USER ADMINISTRATORS	IDENTITY USER ADMINISTRATORS	✓	✓	✓	□
ROLE ADMINISTRATORS	ROLE ADMINISTRATORS	✓	✓	✓	□
REQUEST ADMINISTRATORS	REQUEST ADMINISTRATORS	✓	✓	✓	□
RECONCILIATION ADMINISTRATORS	RECONCILIATION ADMINISTRATORS	✓	✓	✓	□
ATTESTATION EVENT ADMINISTRATORS	ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓	□
APPROVAL POLICY ADMINISTRATORS	APPROVAL POLICY ADMINISTRATORS	✓	✓	✓	□
ATTESTATION CONFIGURATION ADMINISTRATORS	ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓	□
USER CONFIGURATION ADMINISTRATORS	USER CONFIGURATION ADMINISTRATORS	✓	✓	✓	□
RESOURCE ADMINISTRATORS	RESOURCE ADMINISTRATORS	✓	✓	✓	□
					Unassign

First | Previous | Next | Last

11. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.

12. To proceed with the creation of the IT resource, click **Continue**. Figure 2-5 shows Step 4: Verify IT Resource Details page.

Figure 2-5   Step 4: Verify IT Resource Details



Create IT Resource

Step 4 : Verify IT Resource Details

Review and then submit the information that you provided. If required, use the Back button to revisit and modify information provided on the previous pages.

IT Resource Name	ConnectorServer
IT Resource Type	Connector Server

Parameter	Value
Host	172.20.45.110
Key	********
Port	8759
Timeout	0
UseSSL	false

Administrative Role	Read Access	Write Access	Delete Access
SYSTEM ADMINISTRATORS	✓	✓	✓
IDENTITY USER ADMINISTRATORS	✓	✓	✓
ROLE ADMINISTRATORS	✓	✓	✓
REQUEST ADMINISTRATORS	✓	✓	✓
RECONCILIATION ADMINISTRATORS	✓	✓	✓
ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓
APPROVAL POLICY ADMINISTRATORS	✓	✓	✓
ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓
USER CONFIGURATION ADMINISTRATORS	✓	✓	✓
RESOURCE ADMINISTRATORS	✓	✓	✓
REQUEST TEMPLATE ADMINISTRATORS	✓	✓	✓
SCHEDULER ADMINISTRATORS	✓	✓	✓
NOTIFICATION TEMPLATE ADMINISTRATORS	✓	✓	✓
SYSTEM CONFIGURATION ADMINISTRATORS	✓	✓	✓
DEPLOYMENT MANAGER ADMINISTRATORS	✓	✓	✓
PLUGIN ADMINISTRATORS	✓	✓	✓
SPML_App_Role	✓	✓	✓
SOD ADMINISTRATORS	✓	✓	✓
USER NAME ADMINISTRATORS	✓	✓	✓

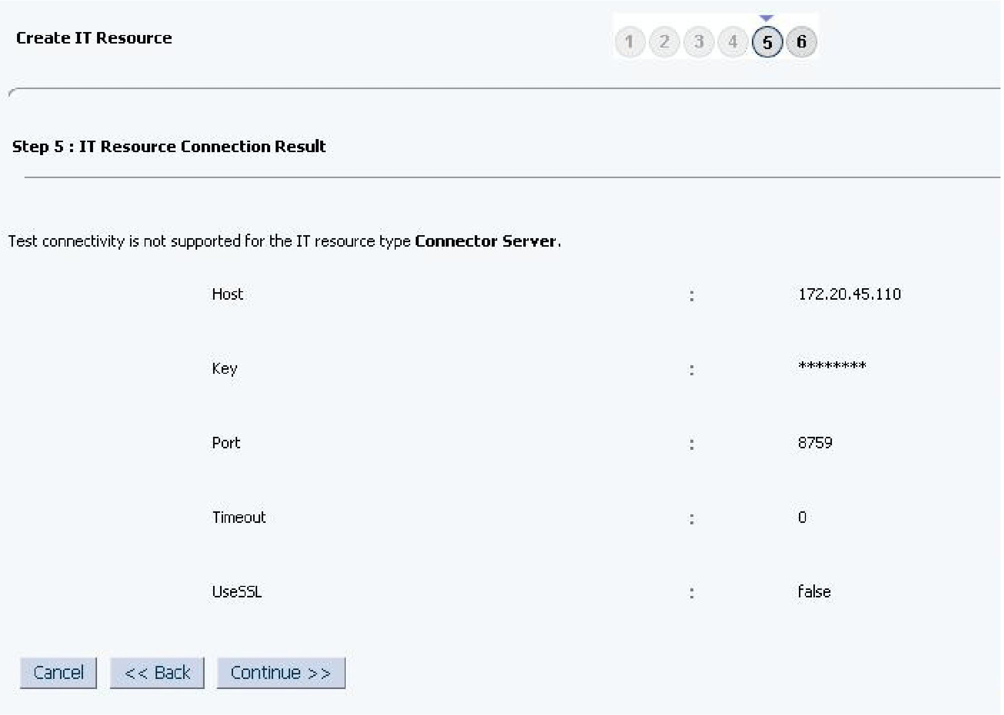
Before advancing to the next step, perform any manual steps required to connect to this IT resource. Otherwise, the target connectivity test may fail.

13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:

    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.

    Figure 2-6 shows the Step 5: IT Resource Connection Result page.

Figure 2-6   Step 5: IT Resource Connection Result



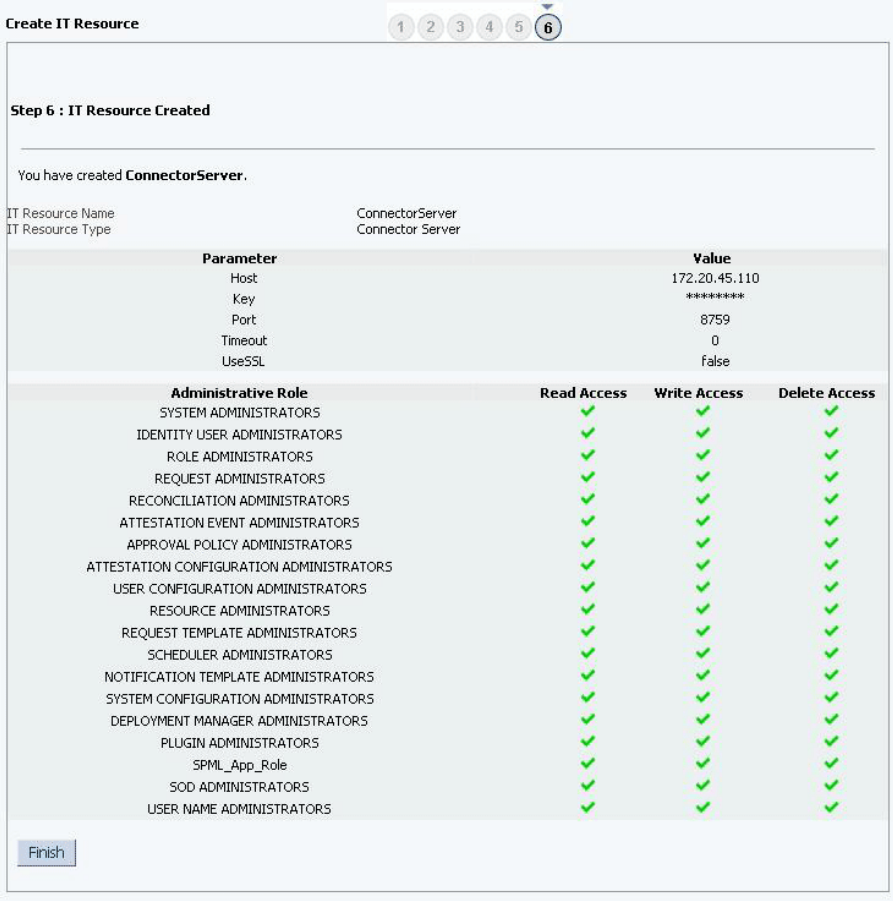
Step 5 : IT Resource Connection Result

Test connectivity is not supported for the IT resource type **Connector Server**.

Host	:	172.20.45.110
Key	:	********
Port	:	8759
Timeout	:	0
UseSSL	:	false

14. Click **Finish**. Figure 2-7 shows the IT Resource Created Page.

Figure 2-7   Step 6: IT Resource Created



Create IT Resource

Step 6 : IT Resource Created

You have created **ConnectorServer**.

IT Resource Name	ConnectorServer
IT Resource Type	Connector Server

Parameter	Value
Host	172.20.45.110
Key	********
Port	8759
Timeout	0
UseSSL	false

Administrative Role	Read Access	Write Access	Delete Access
SYSTEM ADMINISTRATORS	✓	✓	✓
IDENTITY USER ADMINISTRATORS	✓	✓	✓
ROLE ADMINISTRATORS	✓	✓	✓
REQUEST ADMINISTRATORS	✓	✓	✓
RECONCILIATION ADMINISTRATORS	✓	✓	✓
ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓
APPROVAL POLICY ADMINISTRATORS	✓	✓	✓
ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓
USER CONFIGURATION ADMINISTRATORS	✓	✓	✓
RESOURCE ADMINISTRATORS	✓	✓	✓
REQUEST TEMPLATE ADMINISTRATORS	✓	✓	✓
SCHEDULER ADMINISTRATORS	✓	✓	✓
NOTIFICATION TEMPLATE ADMINISTRATORS	✓	✓	✓
SYSTEM CONFIGURATION ADMINISTRATORS	✓	✓	✓
DEPLOYMENT MANAGER ADMINISTRATORS	✓	✓	✓
PLUGIN ADMINISTRATORS	✓	✓	✓
SPML_App_Role	✓	✓	✓
SOD ADMINISTRATORS	✓	✓	✓
USER NAME ADMINISTRATORS	✓	✓	✓

2.3.15 Downloading WSDL files from SAP BusinessObjects AC

In SAP BusinessObjects AC 10, you need to download the WSDL files from SAP BusinessObjects AC before configuring the web services.

Since the connector only supports basic authentication, select the User ID/Password check box for the following web services supported from OIM:

WSDL	Description
GRAC_AUDIT_LOGS_WS	Audit log web service
GRAC_LOOKUP_WS	Lookup service
GRAC_REQUEST_STATUS_WS	Request status web service
GRAC _RISK_ANALYSIS_WOUT_NO_WS	Risk analysis without request number. **Note:** For this WSDL, ReportFormat is a mandatory field from SP17.
GRAC_SELECT_APPL_WS	Select application web service
GRAC_USER_ACCES_WS	User access request service
GRAC_SEARCH_ROLES_W	Search role web service

When you download the WSDL file, ensure to save it with the same name as mentioned in the SOA Management page. In addition, ensure that the folder containing WSDL files have read permission.

2.3.16 Localizing Field Labels in UI Forms

You can localize UI form field labels by using the resource bundle corresponding to the language you want to use. The resource bundles are available in the connector installation media.

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

To localize field label that is added to the 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 one of the following files in a text editor:
   - For Oracle Identity Manager 11*g* Release 2 PS2 and later (11.1.2.2.0):

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
   - For releases prior to Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0):

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:
   a. Search for the following text:

      ```
      <file source-language="en"
      original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
      datatype="x-oracle-adf">
      ```

   b. Replace with the following text:

      ```
      <file source-language="en" target-language="LANG_CODE"
      original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
      datatype="x-oracle-adf">
      ```

      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:

      ```
      <file source-language="en" target-language="ja"
      original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
      datatype="x-oracle-adf">
      ```

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_SAP_TITLE__c_description']}">
<source>Title</source>
</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>
</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.b with the following:

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_SAP_TITLE__c_description']}">
<source>Title</source>
<target>\u5F79\u8077</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>\u5F79\u8077</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:**
>
> Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager,* for more information about exporting and importing metadata files

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

2.3.17 Synchronizing the SAPUM Process Form Field Length Needs with the Target Field Length

Ensure that the field length of the values of an attribute coming from the target system should be in bounds of the length of values of attributes in SAPUM process form.

2.4 Upgrading the Connector

If you have already deployed an earlier release of this connector, then upgrade the connector to the current release.

You can upgrade the SAP User Management connector while in production, and with no downtime. Your customizations will remain intact and the upgrade will be transparent to your users. All form field names are preserved from the legacy connector.

To upgrade the SAP User Management connector, perform the procedures described in the following sections:

- Preupgrade Steps for the SAP UM Connector
- Upgrade Steps for the SAP UM Connector
- Performing the Postupgrade Steps

Note:

- Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
- As a best practice, first perform the upgrade procedure in a test environment.
- Direct upgrade to release 11.1.1.7.0 or later from release 9.*x* of the connector is not supported. You must first upgrade to release 11.1.1.6.0 from release 9.*x* and then upgrade to release 11.1.1.7.0 or later.

2.4.1 Preupgrade Steps for the SAP UM Connector

Before you perform an upgrade operation or any of the upgrade procedures, you must perform the following actions:

- Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
- Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector.
- Run the Oracle Identity Manager Delete JARs utility to delete the old connector bundle to the Oracle Identity Manager database.

> **See Also:**
>
> Delete JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Delete JARs utility

2.4.2 Upgrade Steps for the SAP UM Connector

Depending on the environment in which you are upgrading the connector, perform one of the following steps:

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.
- Production Environment

  Perform the upgrade procedure by using the silent mode.

> **See Also:**
>
> Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the wizard and silent modes

2.4.3 Performing the Postupgrade Steps

Perform the procedure described in this section to complete the steps that are required to post-upgrade.

1. Run the Oracle Identity Manager Upload JARs utility to post the new connector bundle to the Oracle Identity Manager database.

   > **See Also:**
   >
   > Upload JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for detailed information about the Upload JARs utility

2. If the connector is deployed on a Connector Server, then:
   a. Stop the Connector Server.
   b. Replace the existing connector bundle and lib JARs located in the *CONNECTOR_SERVER_HOME*/bundles and *CONNECTOR_SERVER_HOME*/lib directories respectively with the new connector bundles (bundle/org.identityconnectors.sapacum-12.3.0.jar and bundle/org.identityconnectors.sapum-12.3.0.jar) and lib JARs (lib/sapac-oim-integration.jarlib/sapum-oim-integration.jar) from the connector installation media.

   c. Start the Connector Server.

3. Reconfigure the IT resource of the connector.

4. Upgrading the connector will generate duplicate entries in Lookups, you must manually delete these duplicate entries. Perform the postupgrade procedure documented in Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Manager*.

5. Perform the postupgrade steps. Depending on the version of the connector that you are using, perform one of the procedures described in the following sections:

   - Postupgrade Steps for Releases 9.*x* to 11.1.1.5.0, 9.*x* to 11.1.1.6.0, and 11.1.1.5.0 to 11.1.1.6.0 of the Connector
   - Postupgrade Steps for Release 11.1.1.6.0 of the Connector

6. Run the FVC utility. This utility is copied into the following directory when you install the design console:

   - For Microsoft Windows: *OIM_DC_HOME*/fvcuti.bat
   - For UNIX: *OIM_DC_HOME*/fvcutil.sh

   When you run this utility, you are prompted to enter the login credentials of the Oracle Identity manager administrator, and the logger level, and log file location.

7. Create a new version of the process form.

   If you are using Oracle Identity Manager release 11.1.2.*x*, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:

   a. Log in to Oracle Identity System Administration.

   b. Create and activate a sandbox. See Creating and Activating a Sandbox.

   c. Create a new UI form to view the upgraded fields. See Creating a New UI Form.

   d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in the preceding step), and then save the application instance.

   e. Publish the sandbox. Publishing a Sandbox.

8. Perform full reconciliation.

   This operation updates the Unique Id resource object field and the lock status of the users. The lock status will be updated as per the value specified in the fvc.properties file for Release 9.*x* through Release 11.1.1.5.0 of the connector.

   See Full and Incremental Reconciliationfor more information about this step.

   Perform the postupgrade procedure in Managing Connector Lifecycle of *Oracle Fusion Middlware Administering Oracle Identity Governance*.

9. After upgrading the connector, you can perform delete reconciliation.

   See Reconciliation Scheduled Jobs for the SAP UM Connector for more information about delete reconciliation.

2.4.3.1 Postupgrade Steps for Releases 9.*x* to 11.1.1.5.0, 9.*x* to 11.1.1.6.0, and 11.1.1.5.0 to 11.1.1.6.0 of the Connector

Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation.

To do so, in a text editor, open the fvc.properties file located in the *OIM_DC_HOME* directory.

If you are using the connector release 9*x*, include the following entries:

```
ResourceObject;SAPUM Resource Object
FormName;UD_SAP
FromVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_WAS_IN_THE_ACTIVE_STATUS_BEFORE_THE_
UPGRADE
ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_UPGR
ADE
Parent;UD_SAPUSER
```

Example:

```
ResourceObject;SAPUM Resource Object
FormName;UD_SAP
FromVersion;V_9.1.2.6
ToVersion;v_11.1.1.5.0
Parent;UD_SAPUSER
```

If you are using the connector release 11.1.1.*x*, include the following entries:

```
ResourceObject;SAPUM Resource Object
FormName;UD_SAP
FromVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_WAS_IN_THE_ACTIVE_STATUS_BEFORE_THE_
UPGRADE
ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_UPGR
ADE
Parent;UD_SAPUSER
```

Example:

```
ResourceObject;SAPUM Resource Object
FormName;UD_SAP
FromVersion;V_11.1.1.5.0
ToVersion;v_11.1.1.6.0
Parent;UD_SAPUSER
```

2.4.3.2 Postupgrade Steps for Release 11.1.1.6.0 of the Connector

Depending on the type of connector that you choose to upgrade, perform one of the following procedures:

- Postupgrade Steps While Upgrading the Basic User Management configuration from Release 11.1.1.6.0 to Release 11.1.1.7.0
- Postupgrade Steps While Upgrading the SoD validation of SAP BusinessObjects AC Access Risk Analysis from Release 11.1.1.6.0 to Release 11.1.1.7.0
- Postupgrade Steps While Upgrading the SAP BusinessObjects AC Access Request Management from Release 11.1.1.6.0 to Release 11.1.1.7.0

2.4.3.2.1 Postupgrade Steps While Upgrading the Basic User Management configuration from Release 11.1.1.6.0 to Release 11.1.1.7.0

Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation. To do so, in a text editor, open the fvc.properties file located in the OIM_DC_HOME directory.

If you are using the connector release 11.1.1.6.0, include the following entries:

```
ResourceObject;SAPUM Resource Object
FormName;UD_SAP
FromVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_WAS_IN_THE_ACTIVE_STATUS_BEFORE_THE_
UPGRADE
ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_UPGR
ADE
```

Example:

```
ResourceObject;SAPUM Resource Object
FormName;UD_SAP
FromVersion;V_11.1.1.6.0
ToVersion;v_11.1.1.7.0
```

> **Note:**
>
> While upgrading the connector, the following information will display. You must manually delete the following adapters and Event handlers:
>
> - The "sapacum ac remove child" and "sapacum add child" Adapters.
> - The "adpSAPACUMREMOVECHILD" and "adpSAPACUMADDCHILD" EventHandlers.

2.4.3.2.2 Postupgrade Steps While Upgrading the SoD validation of SAP BusinessObjects AC Access Risk Analysis from Release 11.1.1.6.0 to Release 11.1.1.7.0

Perform the procedure described in this section to complete the postupgrade steps for the SoD validation of SAP BusinessObjects AC Access Risk Analysis:

1. Re-configure the GRC-ITRes IT resource.
2. You must manually update the decode values of the following entries in the "Lookup.SAPABAP.Configuration" lookup definition:
   - wsdlFilePath
   - entitlementRiskAnalysisAccessURL
3. Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation. To do so, in a text editor, open the fvc.properties file located in the OIM_DC_HOME directory. If you are using the connector release 11.1.1.6.0, include the following entries:

   ```
   ResourceObject;SAPUM Resource Object
   FormName;UD_SAP
   ```

```
FromVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_WAS_IN_THE_ACTIVE_STATUS_BEFORE_
THE_UPGRADE
ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_
UPGRADE
```

Example:

```
ResourceObject;SAP UM Resource Object
FormName;UD_SAP
FromVersion;V_11.1.1.6.0
ToVersion;v_11.1.1.7.0
```

4. Create a new version of the process form, and run the "Resubmit Uninitiated Provisioning SODChecks" scheduler.

> **Note:**
>
> While upgrading the connector, the following information will display. You must manually delete the following adapters and Event handlers:
>
> - The "sapacum ac remove child" and "sapacum add child" Adapters.
> - The "adpSAPACUMREMOVECHILD" and "adpSAPACUMADDCHILD" EventHandlers.

2.4.3.2.3 Postupgrade Steps While Upgrading the SAP BusinessObjects AC Access Request Management from Release 11.1.1.6.0 to Release 11.1.1.7.0

Perform the procedure described in this section to complete the postupgrade steps for the SAP BusinessObjects AC Access Request Management:

1. Re-configure the SAPUM IT Resource IT resource.
2. You must manually update the decode value to `None` for the following entries in the "Lookup.SAPAC10ABAP.Configuration" lookup definition:
   - roleLookupAccessURL
   - otherLookupAccessURL
   - auditLogsAccessURL
   - appLookupAccessURL
   - wsdlFilePath
   - userAccessAccessURL
   - requestStatusAccessURL
3. Run the PostUpgradeScript_SAPUM.sql script as follows:
   a. Log into the Oracle Identity Manager database using the OIM DB User credentials.
   b. Run the PostUpgradeScript_SAPUM.sql. This script is located in the Upgrade directory on the installation media.

> **Note:**
>
> You must change the task name of the bulk adapter after upgrade. For example, replace the task name "UD_SAPACUM Updated" with "UD_SAPUM Updated."

4. Run the following lookups:
   - SAP AC UM BusinessProcess Lookup Reconciliation
   - SAP AC UM CommType Lookup Reconciliation
   - SAP AC UM Company Lookup Reconciliation
   - SAP AC UM ContractUserType Lookup Reconciliation
   - SAP AC UM DateFormat Lookup Reconciliation
   - SAP AC UM DecimalNot Lookup Reconciliation
   - SAP AC UM FunctionalArea Lookup Reconciliation
   - SAP AC UM ItemProvAction Lookup Reconciliation
   - SAP AC UM LangComm Lookup Reconciliation
   - SAP AC UM Parameter Lookup Reconciliation
   - SAP AC UM Priority Lookup Reconciliation
   - SAP AC UM ReqInitSystem Lookup Reconciliation
   - SAP AC UM RequestType Lookup Reconciliation
   - SAP AC UM Role Lookup Reconciliation
   - SAP AC UM TimeZone Lookup Reconciliation
   - SAP AC UM Title Lookup Reconciliation
   - SAP AC UM UserGroup Lookup Reconciliation
   - SAP AC UM UserType Lookup Reconciliation
5. Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation. To do so, in a text editor, open the fvc.properties file located in the OIM_DC_HOME directory. If you are using the connector release 11.1.1.6.0, include the following entries:

   ```
   ResourceObject;SAP AC UM Resource Object
   FormName;UD_SAP
   FromVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_WAS_IN_THE_ACTIVE_STATUS_BEFORE_
   THE_UPGRADE
   ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_
   UPGRADE
   FromVersion;V_11.1.1.6.0
   ToVersion;v_11.1.1.7.0
   ParentParent;UD_SAP_AC_MANAGER_FIRST_NAME;UD_SAP_AC_MNGR_FIRSTNAME
   ParentParent;UD_SAP_AC_MANAGER_LAST_NAME;UD_SAP_AC_MNGR_LASTNAME
   ParentParent;UD_SAP_AC_MANAGER_EMAIL;UD_SAP_AC_MNGR_EMAIL
   ```

   Example:

   ```
   ResourceObject;SAP AC UM Resource Object
   FormName;UD_SAP
   ```

```
FromVersion;V_11.1.1.6.0
ToVersion;v_11.1.1.7.0
ParentParent;UD_SAP_AC_MANAGER_FIRST_NAME;UD_SAP_AC_MNGR_FIRSTNAME
ParentParent;UD_SAP_AC_MANAGER_LAST_NAME;UD_SAP_AC_MNGR_LASTNAME
ParentParent;UD_SAP_AC_MANAGER_EMAIL;UD_SAP_AC_MNGR_EMAIL
```

2.5 Postcloning Steps

You can clone this connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

> **Note:**
>
> Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about cloning connectors and the postcloning steps.

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- IT Resource

  The cloned connector has its own set of IT resources. You must configure both the cloned connector IT resources and ensure you use the configuration lookup definition of the cloned connector.

- Scheduled Job

  The values of the Resource Object Name and IT Resource scheduled job attributes in the cloned connector refer to the values of the base connector. Therefore, these values (values of the Resource Object Name and IT resource scheduled job attributes that refer to the base connector) must be replaced with the new cloned connector artifacts.

- Adapter

  You must change the itResourceFieldName (Literal Value) in the Variable list of “sapum update” Adapter.For example UD_SAP_ITRESOURCECLONE To be the cloned IT Resource name , After Clone Update the itResourceFieldName (Literal Value) with Form name (e.g.: UD_SAP_ITRESOURCECLONE).

- Lookup Definition

  The cloned lookup definition (for example, Lookup.SAPABAP.ConfigurationCLONE) corresponding to the Lookup.SAPABAP.Configuration lookup definition has Code Key or Decode Key entries related to child form fields that still map to the old child form fields. You must change the values of these Code Key entries so that they map to the cloned child form fields.

For example, consider UD_CloneSAPRL and UD_CloneSAP_PRO to be the cloned child forms of the UD_SAPRL and UD_SAP_ PRO child forms respectively. After cloning, the Lookup.SAPABAP.ConfigurationCLONE lookup definition contains Code Key entries that correspond to the fields of the old child form UD_SAPRL and UD_SAP_ PRO respectively. To ensure that the Code Key entries point to the fields of the cloned child form (UD_CloneSAPRL and UD_CloneSAP_PRO), specify the following values in the corresponding Code Key or Decode Key columns:

- UD_SPUMPC_P; UD_CloneSAP_PRO
- UD_SPUMRC_P; UD_CloneSAPRL

> **Note:**
>
> You must update the respective child form field names manually in the required lookup definitions. For example, Lookup.SAPABAP.UM.ProvAttrMapClone.

- Process Tasks

  You must change the literal value of the **childTableName** adapter variable from UD_SAPRL and UD_SAP_PRO to the cloned form names UD_CLONESAPRL anUD_CLONESAP_PRO, respectively in the following process tasks:

  - Add Role
  - Update Role
  - Remove Role
  - Add Profile
  - Remove Profile
  - Add Group
  - Remove Group
  - Add Parameter
  - Remove Parameter
  - Update Parameter

  You must change the literal value of the parent form from **UD_SAP** to the cloned form name **UD_SAPCLONED** in the **UD_SAP** in the Bulk adapter process task.

- Localization Properties

  You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

  For example, the process form (UD_SAP) attributes are referenced in the Japanese properties file, SAPUM_ja.properties, as global.udf.UD_SAP_FIRST_NAME. During cloning, if you change the process form name from UD_SAPCL to global.udf.UD_SAPCL_FIRST_NAME, then you must add the process form attributes to global.udf.UD_SAP_FIRST_NAME.

- Replicate changes made to the form designer to a new UI form

To do so, perform the procedure described in Postupgrade Steps for Release 11.1.1.6.0 of the Connector.

3 Using the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter is divided into the following sections:

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

3.1 Scheduled Jobs for Lookup Field Synchronization

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

The following scheduled jobs are used for lookup field synchronization:

- SAP UM CommType Lookup Reconciliation
- SAP UM Company Lookup Reconciliation
- SAP UM ContractUserType Lookup Reconciliation
- SAP UM DateFormat Lookup Reconciliation
- SAP UM DecimalNot Lookup Reconciliation
- SAP UM LangComm Lookup Reconciliation
- SAP UM Parameter Lookup Reconciliation

- SAP UM Profile Lookup Reconciliation
- SAP UM Role Lookup Reconciliation
- SAP UM Systems Lookup Reconciliation
- SAP UM TimeZone Lookup Reconciliation
- SAP UM Title Lookup Reconciliation
- SAP UM UserGroup Lookup Reconciliation
- SAP UM UserType Lookup Reconciliation

> **Note:**
>
> Before running a scheduled job for lookup field synchronization, you must copy all the third-party libraries to the following directory:
>
> *OIM_HOME*/xellerate/ConnectorDefaultDirectory/targetsystems-lib/sap-11.1.1.5.0

You can specify values for the attributes of these scheduled jobs. Table 3-1 describes the attributes of these scheduled jobs. Configuring Scheduled Jobs describes the procedure to configure scheduled jobs.

Table 3-1 Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job you are using, the default values are as follows: • For SAP UM CommType Lookup Reconciliation: `COMM_TYPE` • For SAP UM Company Lookup Reconciliation: `COMPANY` • For SAP UM ContractUserType Lookup Reconciliation: `USERTYP` • For SAP UM DateFormat Lookup Reconciliation: `_LOW` • For SAP UM DecimalNot Lookup Reconciliation: `_LOW` • For SAP UM LangComm Lookup Reconciliation: `SPRAS` • For SAP UM Parameter Lookup Reconciliation: `PARAMID` • For SAP UM Profile Lookup Reconciliation: `SUBSYSTEM` • For SAP UM Role Lookup Reconciliation: `SUBSYSTEM` • For SAP UM Systems Lookup Reconciliation: `RCVSYSTEM` • For SAP UM TimeZone Lookup Reconciliation: `TZONE` • For SAP UM Title Lookup Reconciliation: `TITLE_MEDI` • For SAP UM UserGroup Lookup Reconciliation: `USERGROUP` • For SAP UM UserType Lookup Reconciliation: `_LOW` **Note:** You must not change the value of this attribute.

Table 3-1 (Cont.) Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Decode Attribute	Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job you are using, the default values are as follows: • For SAP UM CommType Lookup Reconciliation: COMM_TEXT • For SAP UM Company Lookup Reconciliation: COMPANY • For SAP UM ContractUserType Lookup Reconciliation: UTYPTEXT • For SAP UM DateFormat Lookup Reconciliation: _TEXT • For SAP UM DecimalNot Lookup Reconciliation: _TEXT • For SAP UM LangComm Lookup Reconciliation: SPTXT • For SAP UM Parameter Lookup Reconciliation: PARTEXT • For SAP UM Profile Lookup Reconciliation: USRSYSPRF • For SAP UM Role Lookup Reconciliation: USRSYSACT • For SAP UM Systems Lookup Reconciliation: RCVSYSTEM • For SAP UM TimeZone Lookup Reconciliation: DESCRIPT • For SAP UM Title Lookup Reconciliation: TITLE_MEDI • For SAP UM UserGroup Lookup Reconciliation: TEXT • For SAP UM UserType Lookup Reconciliation: _TEXT
Filter	Enter a filter to filter out records to be stored in the lookup definition. For more information about the Filter attribute, see Limited Reconciliation.
IT Resource Name	Name of the IT resource for the target system installation from which you want to reconcile records. Default value: SAP UM ITResource

Table 3-1 (Cont.) Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Lookup Name	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. **Note:** If the lookup name that you specify as the value of this attribute is not present in Oracle Identity Manager, then this lookup definition is created while the scheduled job is run. Depending on the scheduled job you are using, the default values are as follows: • For SAP UM CommType Lookup Reconciliation: `Lookup.SAPABAP.CommType` • For SAP UM Company Lookup Reconciliation: `Lookup.SAPABAP.Company` • For SAP UM ContractUserType Lookup Reconciliation: `Lookup.SAPABAP.ContractualUserType` • For SAP UM DateFormat Lookup Reconciliation: `Lookup.SAPABAP.DateFormat` • For SAP UM DecimalNot Lookup Reconciliation: `Lookup.SAPABAP.DecimalNotation` • For SAP UM LangComm Lookup Reconciliation: `Lookup.SAPABAP.LangComm` • For SAP UM Parameter Lookup Reconciliation: `Lookup.SAPABAP.Parameter` • For SAP UM Profile Lookup Reconciliation: `Lookup.SAPABAP.Profile` • For SAP UM Role Lookup Reconciliation: `Lookup.SAPABAP.Roles` • For SAP UM Systems Lookup Reconciliation: `Lookup.SAPABAP.System` • For SAP UM TimeZone Lookup Reconciliation: `Lookup.SAPABAP.TimeZone` • For SAP UM Title Lookup Reconciliation: `Lookup.SAPABAP.UserTitle` • For SAP UM UserGroup Lookup Reconciliation: `Lookup.SAPABAP.UserGroups` • For SAP UM UserType Lookup Reconciliation: `Lookup.SAPABAP.UserType`
Object Class	Enter the name of the class of the object you want to reconcile. Depending on the scheduled job you are using, the default values are as follows: • For SAP UM CommType Lookup Reconciliation: `commtype` • For SAP UM Company Lookup Reconciliation: `company` • For SAP UM ContractUserType Lookup Reconciliation: `contractualusertype` • For SAP UM DateFormat Lookup Reconciliation: `dateformat` • For SAP UM DecimalNot Lookup Reconciliation: `decimalnotation` • For SAP UM LangComm Lookup Reconciliation: `languagecommunication` • For SAP UM Parameter Lookup Reconciliation: `parameters` • For SAP UM Profile Lookup Reconciliation: `profiles` • For SAP UM Role Lookup Reconciliation: `activityGroups` • For SAP UM Systems Lookup Reconciliation: `cuaSystems` • For SAP UM TimeZone Lookup Reconciliation: `timeZones` • For SAP UM Title Lookup Reconciliation: `title` • For SAP UM UserGroup Lookup Reconciliation: `__GROUP__` • For SAP UM UserType Lookup Reconciliation: `usertype`

Table 3-1 (Cont.) Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Object Type	Enter the name of the type of object you want to reconcile. Depending on the scheduled job you are using, the default values are as follows: • For SAP UM CommType Lookup Reconciliation: `commtype` • For SAP UM Company Lookup Reconciliation: `company` • For SAP UM ContractUserType Lookup Reconciliation: `contractualusertype` • For SAP UM DateFormat Lookup Reconciliation: `dateformat` • For SAP UM DecimalNot Lookup Reconciliation: `decimalnotation` • For SAP UM LangComm Lookup Reconciliation: `languagecommunication` • For SAP UM Parameter Lookup Reconciliation: `parameters` • For SAP UM Profile Lookup Reconciliation: `profiles` • For SAP UM Role Lookup Reconciliation: `activityGroups` • For SAP UM Systems Lookup Reconciliation: `cuaSystems` • For SAP UM TimeZone Lookup Reconciliation: `timeZones` • For SAP UM Title Lookup Reconciliation: `title` • For SAP UM UserGroup Lookup Reconciliation: `GROUP` • For SAP UM UserType Lookup Reconciliation: `usertype`

3.2 Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization

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

The following scheduled jobs are used for SAP BusinessObjects AC lookup field synchronization:

- SAP AC UM BusinessProcess Lookup Reconciliation
- SAP AC UM CommType Lookup Reconciliation
- SAP AC UM Company Lookup Reconciliation
- SAP AC UM ContractUserType Lookup Reconciliation
- SAP AC UM DateFormat Lookup Reconciliation
- SAP AC UM DecimalNot Lookup Reconciliation
- SAP AC FunctionalArea Lookup Reconciliation
- SAP AC UM ItemProvAction Lookup Reconciliation
- SAP AC UM LangComm Lookup Reconciliation
- SAP AC UM Parameter Lookup Reconciliation
- SAP AC UM Priority Lookup Reconciliation
- SAP AC UM Profile Lookup Reconciliation
- SAP AC UM ReqInitSystem Lookup Reconciliation
- SAP AC UM RequestType Lookup Reconciliation

- SAP AC UM Role Lookup Reconciliation
- SAP AC UM Systems Lookup Reconciliation
- SAP AC UM TimeZone Lookup Reconciliation
- SAP AC UM Title Lookup Reconciliation
- SAP AC UM User Delete Recon
- SAP AC UM UserGroup Lookup Reconciliation
- SAP AC UM User Recon
- SAP AC UM UserType Lookup Reconciliation

You can specify values for the attributes of these scheduled jobs. Table 3-2 describes the attributes of these scheduled jobs. Configuring Scheduled Jobs describes the procedure to configure scheduled jobs.

Table 3-2 Attributes of the Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job you are using, the default values are as follows: • SAP AC UM BusinessProcess Lookup Reconciliation: `LCODE` • SAP AC UM CommType Lookup Reconciliation: `COMM_TYPE` • SAP AC UM Company Lookup Reconciliation: `COMPANY` • SAP AC UM ContractUserType Lookup Reconciliation: `USERTYP` • SAP AC UM DateFormat Lookup Reconciliation: `_LOW` • SAP AC UM DecimalNot Lookup Reconciliation: `_LOW` • SAP AC UM FunctionalArea Lookup Reconciliation: `LCODE` • SAP AC UM ItemProvAction Lookup Reconciliation: `LCODE` • SAP AC UM LangComm Lookup Reconciliation: `SPRAS` • SAP AC UM Parameter Lookup Reconciliation: `PARAMID` • SAP AC UM Priority Lookup Reconciliation: `LCODE` • SAP AC UM Profile Lookup Reconciliation: `SUBSYSTEM` • SAP AC UM ReqInitSystem Lookup Reconciliation: `REQSYSCODE` • SAP AC UM RequestType Lookup Reconciliation: `LCODE` • SAP AC UM Role Lookup Reconciliation: `SUBSYSTEM` • SAP AC UM Systems Lookup Reconciliation: `RCVSYSTEM` • SAP AC UM TimeZone Lookup Reconciliation: `TZONE` • SAP AC UM Title Lookup Reconciliation: `TITLE_MEDI` • SAP AC UM UserGroup Lookup Reconciliation: `USERGROUP` • SAP AC UM UserType Lookup Reconciliation: `_LOW` **Note:** You must not change the value of this attribute.

Table 3-2 (Cont.) Attributes of the Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization

Attribute	Description
Decode Attribute	Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job you are using, the default values are as follows: • SAP AC UM BusinessProcess Lookup Reconciliation: LDECODE • SAP AC UM CommType Lookup Reconciliation: COMM_TEXT • SAP AC UM Company Lookup Reconciliation: COMPANY • SAP AC UM ContractUserType Lookup Reconciliation: UTYPTEXT • SAP AC UM DateFormat Lookup Reconciliation: _TEXT • SAP AC UM DecimalNot Lookup Reconciliation: _TEXT • SAP AC UM FunctionalArea Lookup Reconciliation: LDECODE • SAP AC UM ItemProvAction Lookup Reconciliation: LDECODE • SAP AC UM LangComm Lookup Reconciliation: SPTXT • SAP AC UM Parameter Lookup Reconciliation: PARTEXT • SAP AC UM Priority Lookup Reconciliation: LDECODE • SAP AC UM Profile Lookup Reconciliation: USRSYSPRF • SAP AC UM ReqInitSystem Lookup Reconciliation: REQSYSDECODE • SAP AC UM RequestType Lookup Reconciliation: LDECODE • SAP AC UM Role Lookup Reconciliation: USRSYSACT • SAP AC UM Systems Lookup Reconciliation: RCVSYSTEM • SAP AC UM TimeZone Lookup Reconciliation: DESCRIPT • SAP AC UM Title Lookup Reconciliation: TITLE_MEDI • SAP AC UM UserGroup Lookup Reconciliation: TEXT • SAP AC UM UserType Lookup Reconciliation: _TEXT
IT Resource Name	Name of the IT resource for the target system installation from which you want to reconcile records. Default value: `SAP AC UM IT Resource`

Table 3-2 (Cont.) Attributes of the Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization

Attribute	Description
Lookup Name	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. **Note:** If the lookup name that you specify as the value of this attribute is not present in Oracle Identity Manager, then this lookup definition is created while the scheduled job is run. Depending on the scheduled job you are using, the default values are as follows: • SAP AC UM BusinessProcess Lookup Reconciliation: `Lookup.SAPACABAP.Bproc` • SAP AC UM CommType Lookup Reconciliation: `Lookup.SAPACABAP.CommType` • SAP AC UM Company Lookup Reconciliation: `Lookup.SAPACABAP.Company` • SAP AC UM ContractUserType Lookup Reconciliation: `Lookup.SAPACABAP.ContractualUserType` • SAP AC UM DateFormat Lookup Reconciliation: `Lookup.SAPACABAP.DateFormat` • SAP AC UM DecimalNot Lookup Reconciliation: `Lookup.SAPACABAP.DecimalNotation` • SAP AC UM FunctionalArea Lookup Reconciliation: `Lookup.SAPACABAP.Funcarea` • SAP AC UM ItemProvAction Lookup Reconciliation: `Lookup.SAPAC10ABAP.ItemProvAction` • SAP AC UM LangComm Lookup Reconciliation: `Lookup.SAPACABAP.LangComm` • SAP AC UM Parameter Lookup Reconciliation: `Lookup.SAPACABAP.Parameter` • SAP AC UM Priority Lookup Reconciliation: `Lookup.SAPACABAP.Priority` • SAP AC UM Profile Lookup Reconciliation: `Lookup.SAPACABAP.Profile` • SAP AC UM ReqInitSystem Lookup Reconciliation: `Lookup.SAPACABAP.ReqInitSystem` • SAP AC UM RequestType Lookup Reconciliation: `Lookup.SAPAC10ABAP.RequestType` • SAP AC UM Role Lookup Reconciliation: `Lookup.SAPACABAP.Roles` • SAP AC UM Systems Lookup Reconciliation: `Lookup.SAPACABAP.System` • SAP AC UM TimeZone Lookup Reconciliation: `Lookup.SAPACABAP.TimeZone` • SAP AC UM Title Lookup Reconciliation: `Lookup.SAPACABAP.UserTitle` • SAP AC UM UserGroup Lookup Reconciliation: `Lookup.SAPACABAP.UserGroups` • SAP AC UM UserType Lookup Reconciliation: `Lookup.SAPACABAP.UserType`

Table 3-2 (Cont.) Attributes of the Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization

Attribute	Description
Object Class	Enter the name of the class of the object you want to reconcile. Depending on the scheduled job you are using, the default values are as follows: • SAP AC UM BusinessProcess Lookup Reconciliation: `BusProc` • SAP AC UM CommType Lookup Reconciliation: `commtype` • SAP AC UM Company Lookup Reconciliation: `company` • SAP AC UM ContractUserType Lookup Reconciliation: `contractualusertype` • SAP AC UM DateFormat Lookup Reconciliation: `dateformat` • SAP AC UM DecimalNot Lookup Reconciliation: `decimalnotation` • SAP AC UM FunctionalArea Lookup Reconciliation: `FunctionArea` • SAP AC UM ItemProvAction Lookup Reconciliation: `ItemProvActionType` • SAP AC UM LangComm Lookup Reconciliation: `languagecommunication` • SAP AC UM Parameter Lookup Reconciliation: `parameters` • SAP AC UM Priority Lookup Reconciliation: `PriorityType` • SAP AC UM Profile Lookup Reconciliation: `profiles` • SAP AC UM ReqInitSystem Lookup Reconciliation: `SYSTEM` • SAP AC UM RequestType Lookup Reconciliation: `RequestType` • SAP AC UM Role Lookup Reconciliation: `activityGroups` • SAP AC UM Systems Lookup Reconciliation: `cuaSystems` • SAP AC UM TimeZone Lookup Reconciliation: `timeZones` • SAP AC UM Title Lookup Reconciliation: `title` • SAP AC UM UserGroup Lookup Reconciliation: `__GROUP__` • SAP AC UM UserType Lookup Reconciliation: `usertype`
Object Type	Enter the name of the type of object you want to reconcile. Depending on the scheduled job you are using, the default values are as follows: • SAP AC UM BusinessProcess Lookup Reconciliation: `BusProc` • SAP AC UM CommType Lookup Reconciliation: `commtype` • SAP AC UM Company Lookup Reconciliation: `company` • SAP AC UM ContractUserType Lookup Reconciliation: `contractualusertype` • SAP AC UM DateFormat Lookup Reconciliation: `dateformat` • SAP AC UM DecimalNot Lookup Reconciliation: `decimalnotation` • SAP AC UM FunctionalArea Lookup Reconciliation: `FunctionArea` • SAP AC UM ItemProvAction Lookup Reconciliation: `ItemProvActionType` • SAP AC UM LangComm Lookup Reconciliation: `languagecommunication` • SAP AC UM Parameter Lookup Reconciliation: `parameters` • SAP AC UM Priority Lookup Reconciliation: `PriorityType` • SAP AC UM Profile Lookup Reconciliation: `profiles` • SAP AC UM ReqInitSystem Lookup Reconciliation: `SYSTEM` • SAP AC UM RequestType Lookup Reconciliation: `RequestType` • SAP AC UM Role Lookup Reconciliation: `activityGroups` • SAP AC UM Systems Lookup Reconciliation: `cuaSystems` • SAP AC UM TimeZone Lookup Reconciliation: `timeZones` • SAP AC UM Title Lookup Reconciliation: `title` • AP AC UM UserGroup Lookup Reconciliation: `GROUP` • SAP AC UM UserType Lookup Reconciliation: `usertype`

3.3 Guidelines on Performing Reconciliation

These are the guidelines that you must apply while performing reconciliation operations.

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

You can configure the connector to specify the type of reconciliation and its schedule.

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:

- Full Reconciliation and Incremental Reconciliation
- Batched Reconciliation
- Limited Reconciliation
- Reconciliation Scheduled Jobs for the SAP UM Connector

3.4.1 Full Reconciliation and Incremental 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, ensure that no value is specified for the Filter attribute. However, to reconcile user records, set the value for the Latest token attribute as `0` (Zero) in the scheduled job:

At the end of the reconciliation run, the Latest Token attribute of the scheduled job for user record reconciliation is automatically set to the time stamp at which the run ended. From the next run onward, only records created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

3.4.2 Batched Reconciliation

This section discusses the batchSize attribute of the Lookup.SAPABAP.Configuration lookup definition.

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid such problems.

To configure batched reconciliation, specify a value for the following attribute while performing the procedure described in Setting Up the Configuration Lookup Definition in Oracle Identity Manager:

batchSize: Use this attribute to specify the number of records that must be included in each batch.

After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then you only need to rerun the scheduled task without changing the values of the task attributes.

3.4.3 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

The connector provides a Filter attribute that allows you to use any of the resource attributes to filter the target system records.

The syntax for this parameter is as follows:

> **Note:**
>
> You can use a shortcut for the <and> and <or> operators. For example: `<filter1> & <filter2>` instead of `and` (`<filter1>, <filter2>`), analogically replace `or` with `|`.

```
syntax = expression ( operator expression )*
operator = 'and' | 'or'
expression = ( 'not' )? filter
filter = ('equalTo' | 'contains' | 'containsAllValues' | 'startsWith'
| 'endsWith'  | 'greaterThan' | 'greaterThanOrEqualTo' | 'lessThan'
| 'lessThanOrEqualTo' )  '(' 'attributeName' ',' attributeValue ')'
attributeValue = singleValue  |  multipleValues
singleValue = 'value'
multipleValues = '[' 'value_1' (',' 'value_n')* ']'
```

For example, to limit the number of reconciled accounts to only matching account names, you could use the following expression:

```
equalTo('FirstName;ADDRESS','AP10A1')
```

While deploying the connector, follow the instructions in Configuring Scheduled Jobs to specify attribute values.

3.4.4 Reconciliation Scheduled Jobs for the SAP UM Connector

You can use reconciliation scheduled job to reconcile user account data from the target system.

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

- SAP UM User Recon
- SAP UM User Delete Recon
- SAP AC UM User Recon
- SAP AC UM User Delete Recon
- SAP AC UM Request Status

3.4.4.1 SAP UM User Recon

You use the SAP UM User Recon scheduled job to reconcile user data from the target system. Table 3-3 describes the attributes of this scheduled job.

Table 3-3 Attributes of the SAP UM User Recon Scheduled Job

<table>
<tr><th>Attribute</th><th>Description</th></tr>
<tr><td>Filter</td><td>Expression for filtering records. Use the following syntax:
<pre>
syntax = expression (operator expression)*
operator = 'and' | 'or'
expression = ('not')? filter
filter = ('equalTo' | 'contains' | 'containsAllValues'
| 'startsWith' | 'endsWith' | 'greaterThan' | 'greaterThanOrEqualTo'
| 'lessThan' | 'lessThanOrEqualTo') '(' 'attributeName' ','
attributeValue')'
attributeValue = singleValue | multipleValues
singleValue = 'value'
multipleValues = '[' 'value_1' (',' 'value_n')* ']'
</pre>
Default value: None
See Limited Reconciliation for more information.</td></tr>
<tr><td>Incremental Recon Attribute</td><td>Time stamp at which the last reconciliation run started
Default value: <code>Last Updated</code>
<b>Note:</b> Do <i>not</i> enter a value for this attribute. The reconciliation engine automatically enters a value for this attribute.</td></tr>
<tr><td>IT Resource Name</td><td>Name of the IT resource instance that the connector must use to reconcile data
Sample value: <code>SAP UM IT Resource</code></td></tr>
</table>

Table 3-3 (Cont.) Attributes of the SAP UM User Recon Scheduled Job

Attribute	Description
Latest Token	This attribute holds the time stamp (in the *YYYYMMDDHHMMSS* format) at which the last reconciliation run ended. For the next reconciliation run, only target system records that have been added or modified after this time stamp are considered for reconciliation. For consecutive reconciliation runs, the connector automatically enters a value for this attribute. However, you can use this attribute to switch from incremental reconciliation to full reconciliation. See Full Reconciliation and Incremental Reconciliation for more information. **Note:** The reconciliation engine automatically enters a value in this attribute. Sample value: `20120417123006`
Object Type	Type of object you want to reconcile Default value: `User`
Resource Object Name	Name of the resource object against which reconciliation runs must be performed Default value: `SAP UM Resource Object`
Scheduled Task Name	Name of the scheduled task Default value: `SAP UM User Recon`

3.4.4.2 SAP UM User Delete Recon

You use the SAP UM User Delete Recon scheduled job to reconcile data about deleted users from the target system. Table 3-4 describes the attributes of this scheduled job.

Table 3-4 Attributes of the SAP UM User Delete Recon Scheduled Job

Attribute	Description
Disable User	Enter `yes` if you want the connector to disable accounts (in Oracle Identity Manager) corresponding to accounts deleted on the target system. Enter `no` if you want the connector to revoke accounts in Oracle Identity Manager. Default value: `no`
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data Sample value: `SAP UM ITResource`
Object Type	Type of object you want to reconcile Default value: `User`
Resource Object Name	Name of the resource object against which reconciliation runs must be performed Default value: `SAP UM Resource Object`
Scheduled Task Name	Name of the scheduled task Default value: `SAP UM User Delete Recon`

Table 3-4 (Cont.) Attributes of the SAP UM User Delete Recon Scheduled Job

Attribute	Description
Sync Token	Time stamp at which the last reconciliation run ended in *YYYYMMDDHHMMSS* format (for example, 20120417123006). For the next reconciliation run, only target system records that have been deleted after this time stamp are considered for reconciliation. If you set this attribute to an empty value, then incremental reconciliation operations fetch all the records (perform full reconciliation). **Note:** Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute.

3.4.4.3 SAP AC UM User Recon

You use the SAP AC UM User Recon scheduled job to reconcile users from SAP BusinessObjects AC target system. Table 3-5 describes the attributes of this scheduled job.

Table 3-5 Attributes of the SAP AC UM User Recon Scheduled Job

<table>
<tr><th>Attribute</th><th>Description</th></tr>
<tr><td>Filter</td><td>Expression for filtering records. Use the following syntax:
syntax = expression (operator expression)*
operator = 'and' | 'or'
expression = ('not')? filter
filter = ('equalTo' | 'contains' | 'containsAllValues'
| 'startsWith' | 'endsWith' | 'greaterThan' | 'greaterThanOrEqualTo'
| 'lessThan' | 'lessThanOrEqualTo') '(' 'attributeName' ','
attributeValue')'
attributeValue = singleValue | multipleValues
singleValue = 'value'
multipleValues = '[' 'value_1' (',' 'value_n')* ']'
Default value: None
See Limited Reconciliation for more information.</td></tr>
<tr><td>Incremental Recon Attribute</td><td>Time stamp at which the last reconciliation run started
Default value: Last Updated
<b>Note:</b> Do <i>not</i> enter a value for this attribute. The reconciliation engine automatically enters a value for this attribute.</td></tr>
<tr><td>IT Resource Name</td><td>Name of the IT resource instance that the connector must use to reconcile data
Sample value: SAP AC UM IT Resource</td></tr>
</table>

Table 3-5 (Cont.) Attributes of the SAP AC UM User Recon Scheduled Job

Attribute	Description
Latest Token	This attribute holds the time stamp (in the *YYYYMMDDHHMMSS* format) at which the last reconciliation run ended. For the next reconciliation run, only target system records that have been added or modified after this time stamp are considered for reconciliation. For consecutive reconciliation runs, the connector automatically enters a value for this attribute. However, you can use this attribute to switch from incremental reconciliation to full reconciliation. See Full Reconciliation and Incremental Reconciliation for more information. **Note:** The reconciliation engine automatically enters a value in this attribute. Sample value: `20120417123006`
Object Type	Type of object you want to reconcile Default value: `User`
Resource Object Name	Name of the resource object against which reconciliation runs must be performed Default value: `SAP AC UM Resource Object`
Scheduled Task Name	Name of the scheduled task Default value: `SAP AC UM User Recon`

3.4.4.4 SAP AC UM User Delete Recon

You use the SAP AC UM User Delete Recon scheduled job to reconcile deleted users from SAP BusinessObjects AC target system. Table 3-6 describes the attributes of this scheduled job.

Table 3-6 Attributes of the SAP AC UM User Delete Recon Scheduled Job

Attribute	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data Default value: = `SAP AC UM IT Resource`
Object Type	Type of object you want to reconcile Default value: `User`
Resource Object Name	Name of the resource object against which reconciliation runs must be performed Default value: `SAP AC UM Resource Object`
Scheduled Task Name	Name of the scheduled task Default value: `SAP AC UM User Delete Recon`
Sync Token	Time stamp at which the last reconciliation run ended in *YYYYMMDDHHMMSS* format (for example, 20120417123006). For the next reconciliation run, only targets ystem records that have been deleted after this time stamp are considered for reconciliation. If you set this attribute to an empty value, then incremental reconciliation operations fetch all the records (perform full reconciliation). **Note:** Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Default value: `<String>0</String>`

Table 3-6 (Cont.) Attributes of the SAP AC UM User Delete Recon Scheduled Job

Attribute	Description
Disable User	Enter `yes` if you want the connector to disable accounts (in Oracle Identity Manager)corresponding to accounts deleted on the target system. Enter no if you want theconnector to revoke accounts in Oracle Identity Manager. Default value: `no`

3.4.4.5 SAP AC UM Request Status

You use the SAP AC UM Request Status scheduled job to reconcile request status from SAP BusinessObjects AC target system. Table 3-7 describes the attributes of this scheduled job.

Table 3-7 Attributes of the SAP AC UM Request Status Scheduled Job

Attribute	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data Default value: `SAP AC UM IT Resource`
Object Type	Type of object you want to reconcile Default value: `STATUS`
Resource Object Name	Name of the resource object against which reconciliation runs must be performed Default value: `SAP AC UM Resource Object`
Scheduled Task Name	Name of the scheduled task Default value: `SAP AC UM Request Status`

3.5 Configuring Scheduled Jobs

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

See Scheduled Jobs for Lookup Field Synchronization, Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization, and Reconciliation Scheduled Jobs for the SAP UM Connector for information about scheduled jobs and their attributes.

To configure a scheduled job:

1. If you are using Oracle Identity Manager release 11.1.1.*x*, then you must perform the following steps:
   a. Log in to Oracle Identity System Administration.
   b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
2. If you are using Oracle Identity Manager release 11.1.2.*x*, then you must perform the following steps:
   a. Log in to Oracle Identity System Administration.

   b. In the left pane, under System Management, click **Scheduler.**

3. Search for and open the scheduled job as follows:
   a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
   b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   c. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the parameters of the scheduled job:
   - **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 Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

   In addition to modifying the job details, you can enable or disable a job.
5. On the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.
6. Click **Apply** to save the changes.

> **Note:**
>
> You can use the Scheduler Status page in Identity System Administration to either start, stop, or reinitialize the scheduler.

3.6 Guidelines on Performing Provisioning

These are the guidelines that you must apply while performing provisioning.
This section provides information on the following guidelines related to provisioning:

- Guidelines on Performing Provisioning in Supported Deployment Configuration
- Guidelines on Performing Provisioning After Configuring Access Request Management

3.6.1 Guidelines on Performing Provisioning in Supported Deployment Configuration

These are the guidelines that you must apply 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 Governance 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 Governance. If required, you can configure the task so that it shows the status Rejected in this situation. See Modifying Process Tasks in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for information about configuring process tasks.
- When you perform the Lock User or Unlock User provisioning operation, remember that the connector makes the required change on the target system without checking whether the account is currently in the Locked or Unlocked state. This is because the target system does not provide a method to check the current state of the account.
- The target system does not accept non-English letters in the E-mail Address field. Therefore, during provisioning operations, you must enter only English language letters in the E-mail Address field on the process form.
- 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.

3.6.2 Guidelines on Performing Provisioning After Configuring Access Request Management

These are the guidelines that you must apply while performing provisioning operations after configuring the Access Request Management feature of the connector.

- During a Create User operation performed when the Access Request Management is configured, first submit process form data. Submit child form data after the user is created on the target system. This is because when Access Request Management 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 parameters on SAP GRC Access Request Management:

  > **Note:**
  >
  > When the Access Request Management feature is configured, you must enter values for these fields even though some of them are not marked as mandatory fields on Oracle Identity System Administration.

  - AC Manager
  - AC Manager email
  - AC Priority
  - AC System
  - AC Requestor ID
  - AC Requestor email
  - AC Request Reason

  The following fields may be mandatory or optional based on the configuration in SAP GRC system:

  - AC Manager First Name
  - AC Manager Last Name
  - AC Manager Telephone
  - AC Request Due Date
  - AC Functional Area
  - AC Business Process
  - AC Requestor First Name
  - AC Requestor Last Name
  - AC Requestor Telephone
  - AC Company
- As mentioned earlier in this guide, SAP GRC Access Request Management 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 Governance password as the target system password, change the password through Oracle Identity Governance.
  - 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 Oracle Identity System Administration (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 parameters that are mapped with SAP GRC Access Request Management and parameters that are directly updated on the target system. A request is created SAP GRC Access Request Management only for parameters whose mappings are present in these lookup definitions. If you specify values for parameters that are not present in these lookup definitions, then the connector sends them to directly the target system.
- You cannot perform an assign or revoke groups operation in SAP UM AC account on GRC server. Groups must be managed in the SAP ECC system (backend ABAP system).

3.7 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2

You create a new user in Oracle Identity Self Service by using the Create User page. You provision or request for accounts on the Accounts tab of the User Details page.

To configure provisioning operations in Oracle Identity Manager release 11.1.2.*x:*

> **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 System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Managing Sandboxes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

3. Create an application instance and specify values for the following fields in the Create Application Instance page. See Creating Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
   - **Name:** The name of the application instance.
   - **Display Name:** The display name of the application instance.
   - **Description:** A description of the application instance.
   - **Resource Object:** The resource object name. Click the search icon next to this field to search for and select **SAP UM Resource Object.**
   - **IT Resource Instance:** The IT resource instance name. Click the search icon next to this field to search for and select **SAP UM IT Resource.**
   - **Form:** Select the form name, for example, **SAPUM.** To do so, click **Create.** against the Form list, specify the form name, and then create it. On the Create Application Instance page, click the Refresh icon next to the Form field. From this list, select the form name that you created.
4. Publish the sandbox.
5. Run lookup field synchronization.
6. Search for and run the Entitlement List scheduled job to populate the ENT_LIST table.
7. Publish the application instance (created in Step 3) to an organization. To do so:
   a. On the Organizations tab of the Application Instance page, click **Assign.**
   b. In the Select Organizations dialog box, select the organization to which you want to publish the application instance.
   c. Select the **Apply to entitlements** checkbox.
   d. Click **OK.**
8. Search for and run the Catalog Synchronization Job scheduled job.
9. Log in to Oracle Identity System Administration.
10. Create a user. See Managing Users in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
11. On the Account tab, click **Request Accounts.**
12. In the Catalog page, search for and add to cart the application instance created in Step 3, and then click **Checkout.**
13. Specify value for fields in the application form and then click **Ready to Submit.**
14. Click **Submit.**
15. 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.**

> **See Also:**
>
> - Scheduled Jobs for Lookup Field Synchronization
> - Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization
> - Configuring Scheduled Jobs

3.8 Performing Provisioning Operations 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

This section discusses the following topics:

- Overview of the Provisioning Process in an SoD-Enabled Environment
- Guidelines on Performing Provisioning Operations in an SoD-Enabled Environment
- Direct Provisioning in an SoD-Enabled Environment
- Request-Based Provisioning in an SoD-Enabled Environment

3.8.1 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. SAP BusinessObjects SoD Invocation Library (SIL) Provider passes the entitlement data to the Web service of SAP BusinessObjects AC.
3. After SAP BusinessObjects AC runs the SoD validation process on the entitlement data, the response from the process is returned to Oracle Identity Manager.
4. 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.

3.8.2 Guidelines on Performing Provisioning Operations in an SoD-Enabled Environment

These are the guidelines that you must apply while performing provisioning operations in an SoD-enabled environment.

- 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.

3.8.3 Direct Provisioning in an SoD-Enabled Environment

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

- Enabling the Use of the Process Form During Direct Provisioning in an SoD-Enable Environment
- Performing Direct Provisioning

3.8.3.1 Enabling the Use of the Process Form During Direct Provisioning in an SoD-Enable Environment

> **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.

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.

3.8.3.2 Performing Direct Provisioning

To provision a resource by using the direct provisioning approach:

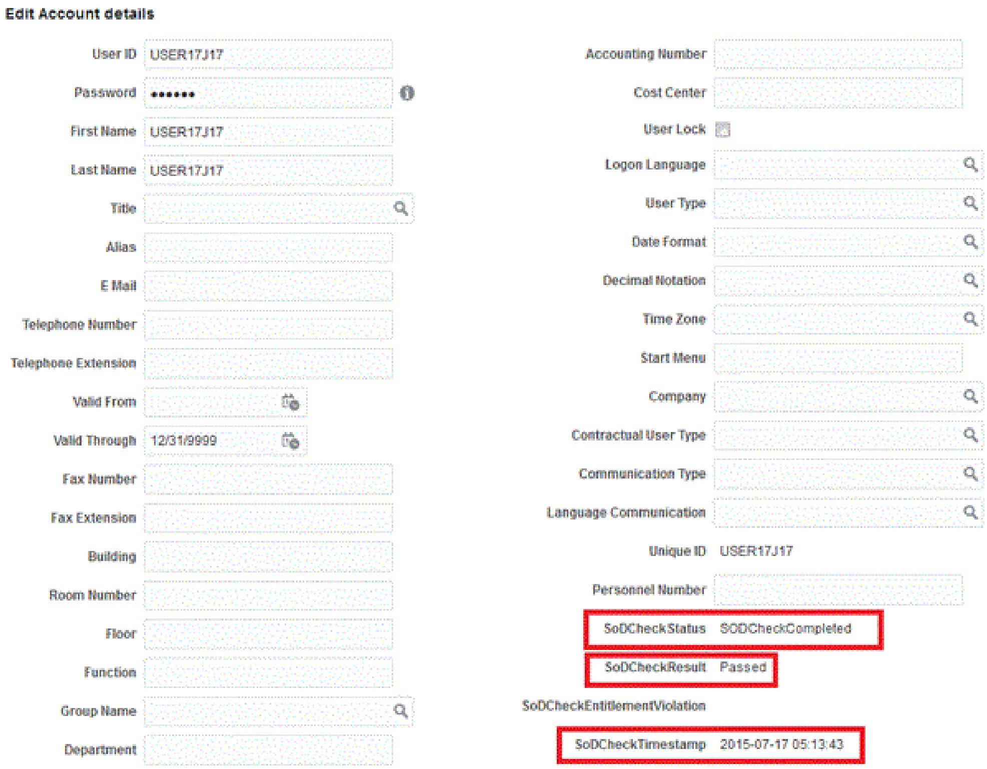
1. Log in to Oracle Identity System Administration.
2. If you want to first create an OIM User and then provision a target system account, then:
   a. On the Welcome to Identity Administration page, in the Users region, click **Create User.**
   b. On the Create User page, enter values for the OIM User fields, and then click **Save.**
3. If you want to provision a target system account to an existing OIM User, then:
   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. On the user details page, click the **Resources** tab.
5. 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.
6. On the Step 1: Select a Resource page, select **SAP UM Resource Object** from the list and then click **Continue**.
7. On the Step 2: Verify Resource Selection page, click **Continue**.
8. 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**.

9. 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**.
10. 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**.
11. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
12. The "Provisioning has been initiated" message is displayed. Close the window displaying this message.
13. On the Resource tab of the user details page, click **Refresh** to view the newly provisioned resource.
14. To view the Resource Provisioning Details page, which shows the details of the process tasks that were run:

    On the Resources tab of the user details page, from the Action menu, select **Resource History.**
15. The SOD Check Status field is updated with SOD Check Completed status.
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, 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:



Edit Account details

User ID	USER17J17	Accounting Number	
Password	••••••	Cost Center	
First Name	USER17J17	User Lock	☐
Last Name	USER17J17	Logon Language	
Title		User Type	
Alias		Date Format	
E Mail		Decimal Notation	
Telephone Number		Time Zone	
Telephone Extension		Start Menu	
Valid From		Company	
Valid Through	12/31/9999	Contractual User Type	
Fax Number		Communication Type	
Fax Extension		Language Communication	
Building		Unique ID	USER17J17
Room Number		Personnel Number	
Floor		SoDCheckStatus	SODCheckCompleted
Function		SoDCheckResult	Passed
Group Name		SoDCheckEntitlementViolation	
Department		SoDCheckTimestamp	2015-07-17 05:13:43

18. After invoking the risk analysis web service, the results of the SoD validation process are brought to Oracle Identity Manager. If you open the process form, the results will be displayed as shown in the screenshot in Step 17.

3.8.4 Request-Based Provisioning in an SoD-Enabled Environment

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.

> **Note:**
>
> Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1.*x*.
>
> See Configuring SoD (Segregation of Duties) for related information.

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.

The following sections provide more information about request-based provisioning:

- Creation of Request-Based Provisioning by End-Users
- Approving Request-Based Provisioning

3.8.4.1 Creation of Request-Based Provisioning by End-Users

The following are types of request-based provisioning:

- Request-based provisioning of accounts: OIM Users are created but not provisioned target system resources when they are created. Instead, the users themselves raise requests for provisioning accounts.
- Request-based provisioning of entitlements: OIM Users who have been provisioned target system resources (either through direct or request-based provisioning) raise requests for provisioning entitlements.

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

1. Log in to Oracle Identity System Administration.
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 in 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.

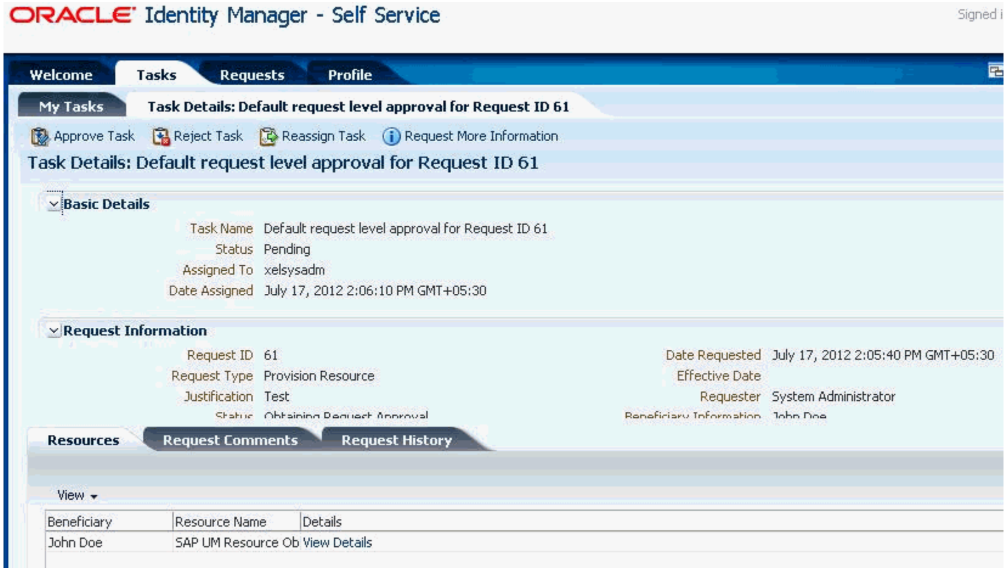
15. To view details of the approval, on the Request Details page, click the **Approval Tasks** tab.

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

3.8.4.2 Approving 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.



Task Details: Default request level approval for Request ID 61

Basic Details

Task Name: Default request level approval for Request ID 61
Status: Pending
Assigned To: xelsysadm
Date Assigned: July 17, 2012 2:06:10 PM GMT+05:30

Request Information

Request ID: 61
Request Type: Provision Resource
Justification: Test
Status: Obtaining Request Approval
Date Requested: July 17, 2012 2:05:40 PM GMT+05:30
Effective Date:
Requester: System Administrator
Beneficiary Information: John Doe

Beneficiary	Resource Name	Details
John Doe	SAP UM Resource Ob	View Details

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

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

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

1. Log in to Oracle Identity System Administration.

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.

3.9 Switching Between SAP ERP and SAP CUA Target Systems

You can switch your target systems between SAP ERP and SAP CUA for reconciliation and provisioning.

The following sections provide information about the procedure to switch between the SAP ERP and SAP CUA target systems:

- Switching Between the SAP R/3 and SAP CUA Target Systems for Reconciliation
- Switching Between the SAP R/3 and SAP CUA Target Systems for Provisioning

3.9.1 Switching Between the SAP R/3 and SAP CUA Target Systems for Reconciliation

To switch between SAP R/3 and SAP CUA target systems for reconciliation:

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

   See Setting Up the Configuration Lookup Definition in Oracle Identity Manager for more information.

2. In the SAP UM User Recon and SAP UM User Delete Recon scheduled jobs, set values for the following attributes:
    - IT Resource Name: Enter the name of the required IT resource.
    - Latest Token: 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 Reconciliation Scheduled Jobs for the SAP UM Connector for information about the scheduled task.

3.9.2 Switching Between the SAP R/3 and SAP CUA Target Systems for Provisioning

To switch between SAP R/3 and SAP CUA target systems for provisioning:

1. If you are switching to SAP CUA, then set the value of the enableCUA entry to `yes` in the Lookup.SAPABAP.Configuration lookup definition. If you are switching to SAP R/3, then set the value to `no`.
2. For every scheduled job used for lookup field synchronization, set the value of required IT resource in the IT Resource Name field and run it individually.

    Perform this step on all the scheduled jobs listed in Scheduled Jobs for Lookup Field Synchronization.
3. Start the provisioning operation on Oracle Identity System Administration by selecting the required IT resource.

3.10 Switching From an SAP R/3 or SAP CUA Target Systems to an SAP BusinessObjects AC Target System and Vice Versa

You can switch from an SAP R/3 or SAP CUA target system to an SAP BusinessObjects AC target system and viceversa.

If you want to switch from an SAP R/3 or SAP CUA target system to a SAP BusinessObjects AC 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 Exporting All MDS Data for Oracle Identity Manager in *Oracle Fusion Middleware Developing and Customizing Applications 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 Clearing Content Related to Connector Resource Bundles from the Server Cache for instructions.
4. Import the request datasets for the target system to which you want to switch. Perform the procedure described in Importing Request Datasets Using Deployment Manager.
5. Run the PurgeCache utility to clear the cache for the content category **Metadata**. See Clearing Content Related to Connector Resource Bundles from the Server Cache. for instructions.

3.11 Switching Between Request-Based Provisioning and Direct Provisioning

> **Note:**
>
> Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1. It is assumed that you have performed the procedure described in Enabling 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. Diret provisioning cannot be used if you enable request-based provisioning.

The following sections discuss the steps to be performed to switch between request-based provsioning and direct provisioning:

- Switching from Request-Based Provisioning to Direct Provisioning
- Switching from Direct Provisioning to Request-Based Provisioning

3.11.1 Switching from Request-Based Provisioning to Direct Provisioning

To switch from request-based provisioning to direct provisioning, do the following:

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.

3.11.2 Switching from Direct Provisioning to Request-Based Provisioning

To switch from direct provisioning to request-based provisioning, do the following:

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.

4 Extending the Functionality of the Connector

You can extend the functionality of the connector to address your specific business requirements.
This chapter discusses the following optional procedures:

> **Note:**
>
> From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See Managing Lookups in *Oracle Fusion Middleware Administering Oracle Identity Manager* guide for information about managing lookups by using the Form Designer in Oracle Identity System Administration.

- Determining the Names of Target System Attributes
- Adding New Attributes for Reconciliation
- Adding New Standard Attributes for Provisioning
- Adding New Standard SAP BusinessObjects AC Access Request Management Attributes for Provisioning
- Removing SAP BusinessObjects AC Access Request Management Attributes from Process Form
- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During User Reconciliation
- Configuring Resource Exclusion Lists
- Modifying Field Lengths on the Process Form
- About Configuring the Connector for Multiple Installations of the Target System

4.1 Determining the Names of Target System Attributes

You can determine the name of a target system attribute that you want to add for reconciliation or provisioning on the SAP system.

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

Lookup Definition	Format of Value in the Decode Column
Lookup.SAPABAP.UM.ReconAttrMap	*FIELD_NAME; STRUCTURE_NAME* For example: ACCNT;LOGONDATA
Lookup.SAPABAP.UM.ProvAttrMap	*FIELD_NAME;STRUCTURE_NAME;FIELD_NAME;STRUCTURE_NAME_X* For example: ACCNT;LOGONDATA;ACCNT;LOGONDATAX

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

To determine the name of the target system attribute on which the connector can perform reconciliation and provisioning operations:

1. Run the SE37 transaction.
2. Execute any one of the following function modules:
   - For reconciliation attributes: BAPI_USER_GET_DETAIL
   - For provisioning attributes: BAPI_USER_CHANGE
3. Enter the user ID of the account created in Creating a Target System User Account for Connector Operations

   The function module returns the list of all user attributes.
4. Select the attribute to view its details.
5. Select the structure icon to view further details in the Structure editor.

   The target system name for the attribute is displayed along with its value. Write down the names of the attribute (FIELD_NAME for reconciliation and FIELD_NAME_X for provisioning) and the structure (STRUCTURE_NAME for reconciliation and STRUCTURE_NAME_X for provisioning). Note that the attribute and structure names are case sensitive.

4.2 Adding New Attributes for Reconciliation

You can map new attributes between Oracle Identity manager and the target system 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.

By default, the attributes listed in Table 1-10 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for reconciliation.

To add a new attribute for reconciliation, perform the procedures listed in the following sections:

- Creating a New Version of the Process Form
- Adding the New Attribute to the Resource Object
- Creating a Reconciliation Field Mapping for the New Attribute in the Process Definition
- Creating an Entry for the Field in the Lookup Definition for Reconciliation
- Creating an Entry for the Attribute in the Lookup Definition
- Creating a New UI Form to make the New Attribute Visible

4.2.1 Creating a New Version of the Process Form

To create a new version of a process form:

1. Log in to Oracle Identity Manager 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**, and then click **Add**.
5. 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 Variant Type, Length, Field Label, and Field Type.
6. Click the Save icon, and then click **Make Version Active.** The following screenshot shows the new field added to the process form:

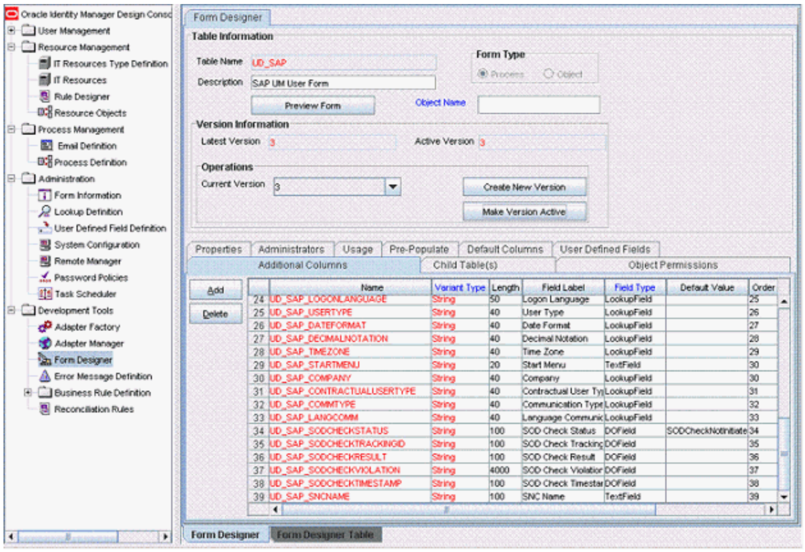


Table Information

Table Name: UD_SAP

Description: SAP UM User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 3   Active Version: 3

Operations

Current Version: 3

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

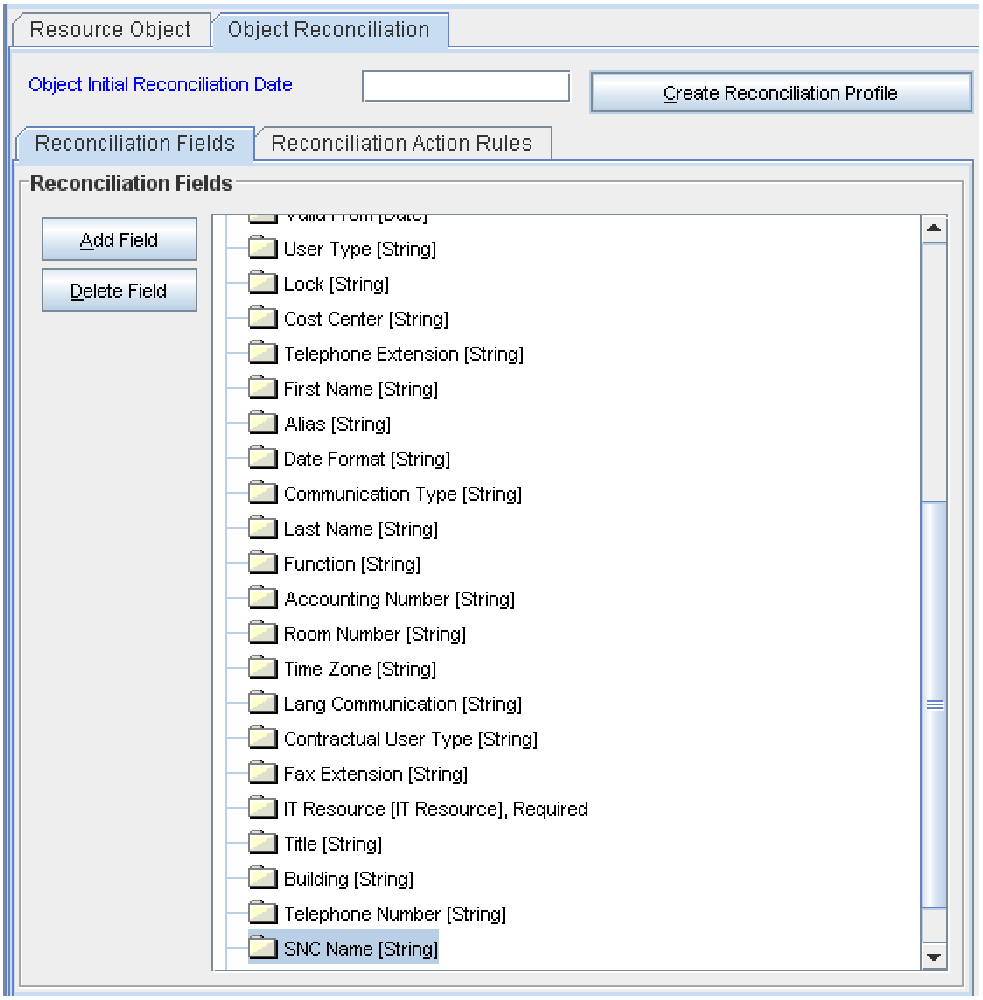
4.2.2 Adding the New Attribute to the Resource Object

To add the new attribute to the list of reconciliation fields in the resource object:

1. Expand **Resource Management**, and double-click **Resource Objects**.
2. Search for and open the **SAP UM** resource object.
3. On the Object Reconciliation tab, click **Add Field**.
4. 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.
5. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:

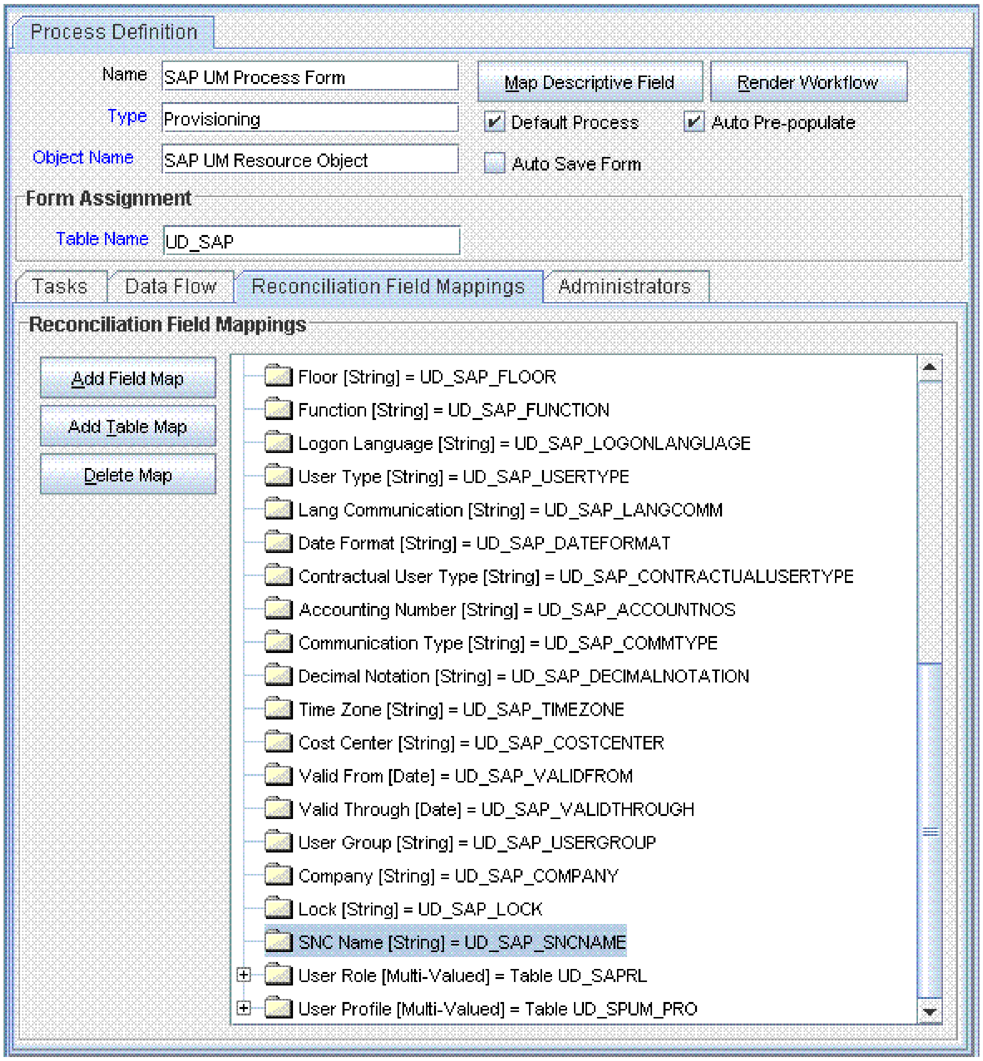


6. Click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

4.2.3 Creating a Reconciliation Field Mapping for the New Attribute in the Process Definition

To create a reconciliation field mapping for the new attribute in the process definition:

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open the **SAP UM Process Form** process definition.
3. On the **Reconciliation Field Mappings** tab of the **SAP UM Process Form** process definition, click **Add Field Map**.
4. In the Field Name field, select the value for the field that you want to add.
5. Double-click the **Process Data Field** field, and then select **UD_SAP_SNCNAME**.
6. Click the Save icon. The following screenshot shows the new reconciliation field mapped to a process data field in the process definition:



Name: SAP UM Process Form

Type: Provisioning

Object Name: SAP UM Resource Object

☑ Default Process

☑ Auto Pre-populate

□ Auto Save Form

Form Assignment

Table Name: UD_SAP

Reconciliation Field Mappings

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

4.2.4 Creating an Entry for the Field in the Lookup Definition for Reconciliation

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

To create an entry for the field in the lookup definition for reconciliation:

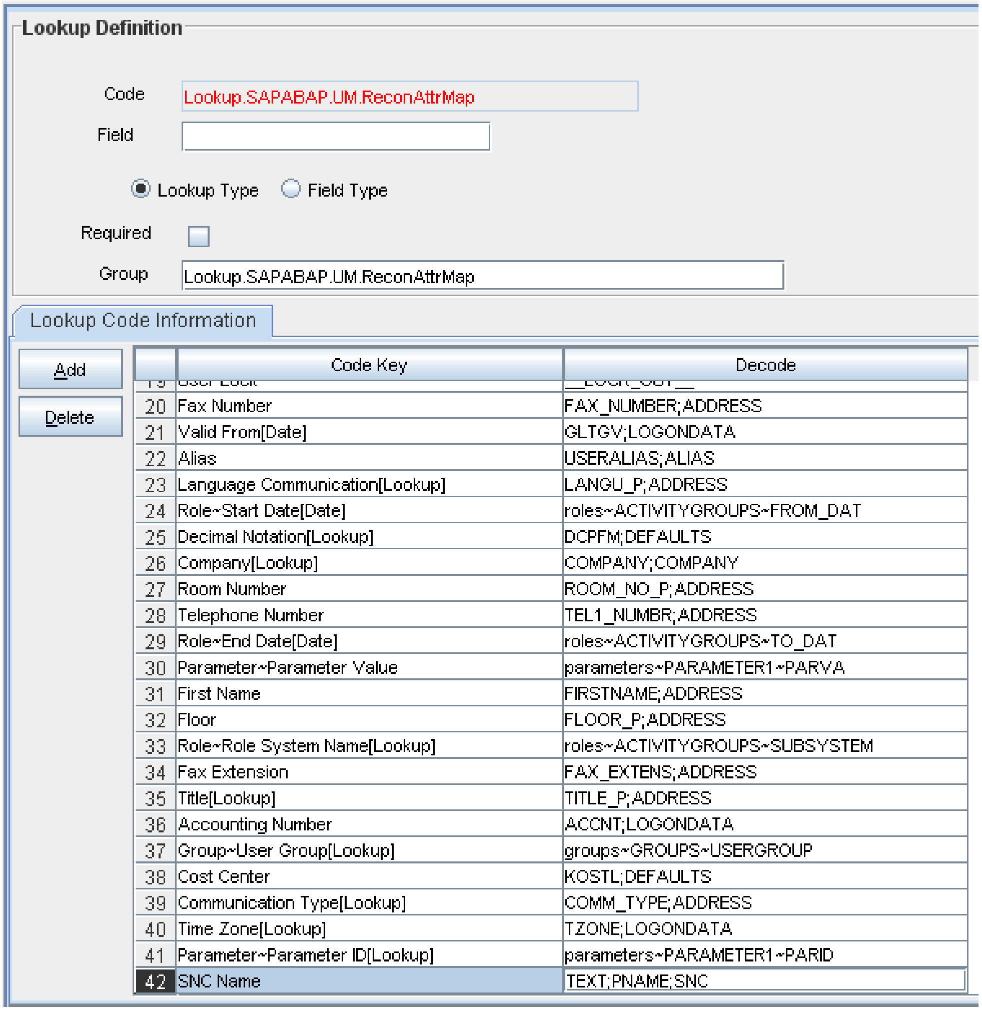
1. Expand **Administration**.
2. Double-click **Lookup Definition.**
3. Search for and open the Lookup.SAPABAP.UM.ReconAttrMap lookup definition.

> **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.

4. 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 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.

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



Lookup Definition

Code: Lookup.SAPABAP.UM.ReconAttrMap

Field:

● Lookup Type ○ Field Type

Required ☐

Group: Lookup.SAPABAP.UM.ReconAttrMap

	Code Key	Decode
19	User Lock	__LOCK_OUT__
20	Fax Number	FAX_NUMBER;ADDRESS
21	Valid From[Date]	GLTGV;LOGONDATA
22	Alias	USERALIAS;ALIAS
23	Language Communication[Lookup]	LANGU_P;ADDRESS
24	Role~Start Date[Date]	roles~ACTIVITYGROUPS~FROM_DAT
25	Decimal Notation[Lookup]	DCPFM;DEFAULTS
26	Company[Lookup]	COMPANY;COMPANY
27	Room Number	ROOM_NO_P;ADDRESS
28	Telephone Number	TEL1_NUMBR;ADDRESS
29	Role~End Date[Date]	roles~ACTIVITYGROUPS~TO_DAT
30	Parameter~Parameter Value	parameters~PARAMETER1~PARVA
31	First Name	FIRSTNAME;ADDRESS
32	Floor	FLOOR_P;ADDRESS
33	Role~Role System Name[Lookup]	roles~ACTIVITYGROUPS~SUBSYSTEM
34	Fax Extension	FAX_EXTENS;ADDRESS
35	Title[Lookup]	TITLE_P;ADDRESS
36	Accounting Number	ACCNT;LOGONDATA
37	Group~User Group[Lookup]	groups~GROUPS~USERGROUP
38	Cost Center	KOSTL;DEFAULTS
39	Communication Type[Lookup]	COMM_TYPE;ADDRESS
40	Time Zone[Lookup]	TZONE;LOGONDATA
41	Parameter~Parameter ID[Lookup]	parameters~PARAMETER1~PARID
42	SNC Name	TEXT;PNAME;SNC

4.2.5 Creating an Entry for the Attribute in the Lookup Definition

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.SAPABAP.UM.ReconAttrMap 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.SAPABAP.UM.ReconAttrMap lookup definition, enter the name of the resource object field that you created for the custom attribute.
- If you want a custom BAPI to fetch values from this attribute, then enter the following value in the Decode column of the lookup definition:

  `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 enter the following value in the Decode column of the lookup definition:

  `RFC_READ_TABLE;`*`FIELD_TYPE`*`;`*`TABLE_NAME`*`;`*`FIELD_NAME`*`;`*`KEY_USER_ID_FIELD`*
- In the Code Key column of the Lookup.SAPABAP.UM.ReconAttrMap lookup definition, enter the name of the resource object field that you created for the custom attribute.
- If you want a custom BAPI to fetch values from this attribute, then enter the following value in the Decode column of the lookup definition:

  `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 enter the following value in the Decode column of the lookup definition:

  `RFC_READ_TABLE;`*`FIELD_TYPE`*`;`*`TABLE_NAME`*`;`*`FIELD_NAME`*`;`*`KEY_USER_ID_FIELD`*

In these formats:

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

The following is a sample value for the Decode column:

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

4.2.6 Creating a New UI Form to Make the New Attribute Visible

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

4.3 Adding New Standard Attributes for Provisioning

You can map addition attributes for provisioning between Oracle Identity Manager and the target system.

By default, the attributes listed in Table 1-14 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

Perform the following procedures described in this section only if you want to map standard target system attributes for provisioning:

- Creating a New Version of the Process Form
- Creating an Entry for the Attribute in the Lookup Definition for Provisioning
- Creating a Task to Update the Attribute During Provisioning Operations
- Updating the Request Dataset
- Running the PurgeCache Utility
- Importing the Request Dataset Definitions
- Creating a New UI Form to make the New Attribute Visible

4.3.1 Creating a New Version of the Process Form

Create a new version on the process form as follows:

1. Log in to Oracle Identity Manager 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**, and then click **Add**.
5. 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.
6. Click the Save icon, and then click **Make Version Active.** The following screenshot shows the new field added to the process form:

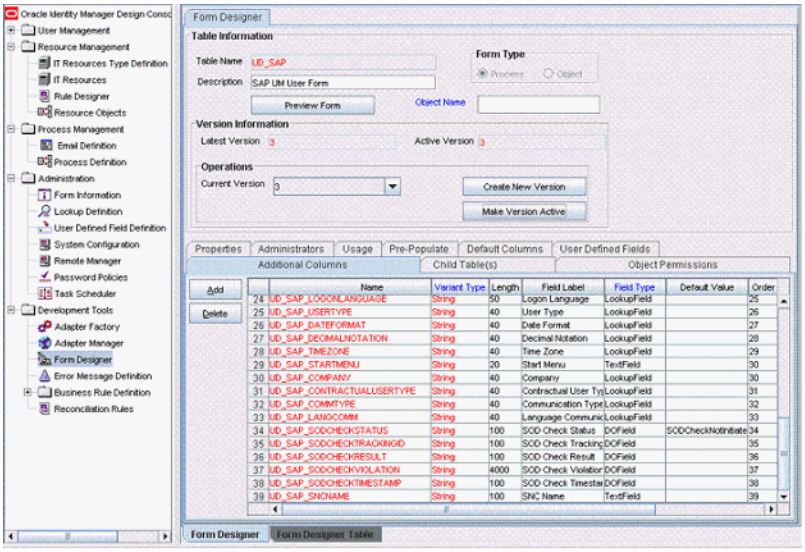


Table Information

Table Name: UD_SAP

Description: SAP UM User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 3

Active Version: 3

Operations

Current Version: 3

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

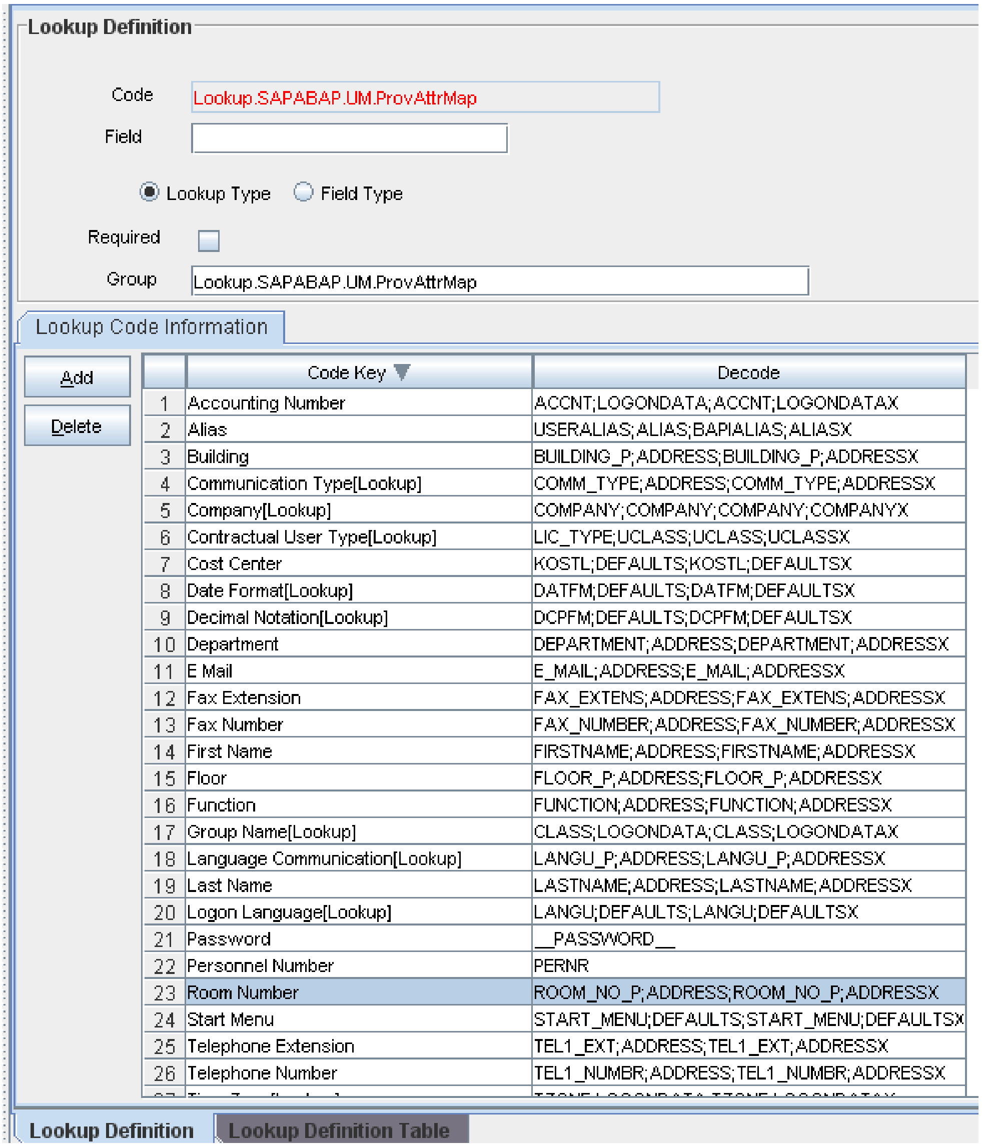
4.3.2 Creating an Entry for the Attribute in the Lookup Definition for Provisioning

Create an entry for the attribute in the lookup definition for provisioning as follows:

1. Expand **Administration**.
2. Double-click **Lookup Definition.**
3. Search for and open the Lookup.SAPABAP.UM.ProvAttrMap lookup definition.
4. 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 Determining the Names of Target System Attributes.

   For example, enter `Room Number` in the **Code Key** column and then enter `TEXT;ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX` in the **Decode** column. The following screenshot shows the entry added to the lookup definition:



Code: Lookup.SAPABAP.UM.ProvAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: Lookup.SAPABAP.UM.ProvAttrMap

	Code Key	Decode
1	Accounting Number	ACCNT;LOGONDATA;ACCNT;LOGONDATAX
2	Alias	USERALIAS;ALIAS;BAPIALIAS;ALIASX
3	Building	BUILDING_P;ADDRESS;BUILDING_P;ADDRESSX
4	Communication Type[Lookup]	COMM_TYPE;ADDRESS;COMM_TYPE;ADDRESSX
5	Company[Lookup]	COMPANY;COMPANY;COMPANY;COMPANYX
6	Contractual User Type[Lookup]	LIC_TYPE;UCLASS;UCLASS;UCLASSX
7	Cost Center	KOSTL;DEFAULTS;KOSTL;DEFAULTSX
8	Date Format[Lookup]	DATFM;DEFAULTS;DATFM;DEFAULTSX
9	Decimal Notation[Lookup]	DCPFM;DEFAULTS;DCPFM;DEFAULTSX
10	Department	DEPARTMENT;ADDRESS;DEPARTMENT;ADDRESSX
11	E Mail	E_MAIL;ADDRESS;E_MAIL;ADDRESSX
12	Fax Extension	FAX_EXTENS;ADDRESS;FAX_EXTENS;ADDRESSX
13	Fax Number	FAX_NUMBER;ADDRESS;FAX_NUMBER;ADDRESSX
14	First Name	FIRSTNAME;ADDRESS;FIRSTNAME;ADDRESSX
15	Floor	FLOOR_P;ADDRESS;FLOOR_P;ADDRESSX
16	Function	FUNCTION;ADDRESS;FUNCTION;ADDRESSX
17	Group Name[Lookup]	CLASS;LOGONDATA;CLASS;LOGONDATAX
18	Language Communication[Lookup]	LANGU_P;ADDRESS;LANGU_P;ADDRESSX
19	Last Name	LASTNAME;ADDRESS;LASTNAME;ADDRESSX
20	Logon Language[Lookup]	LANGU;DEFAULTS;LANGU;DEFAULTSX
21	Password	__PASSWORD__
22	Personnel Number	PERNR
23	Room Number	ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX
24	Start Menu	START_MENU;DEFAULTS;START_MENU;DEFAULTSX
25	Telephone Extension	TEL1_EXT;ADDRESS;TEL1_EXT;ADDRESSX
26	Telephone Number	TEL1_NUMBR;ADDRESS;TEL1_NUMBR;ADDRESSX

4.3.3 Creating a Task to Update the Attribute During Provisioning Operations

If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of the attribute during provisioning operations, add a process task for updating the attribute:

See Also:

Configuring Requests in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about these steps

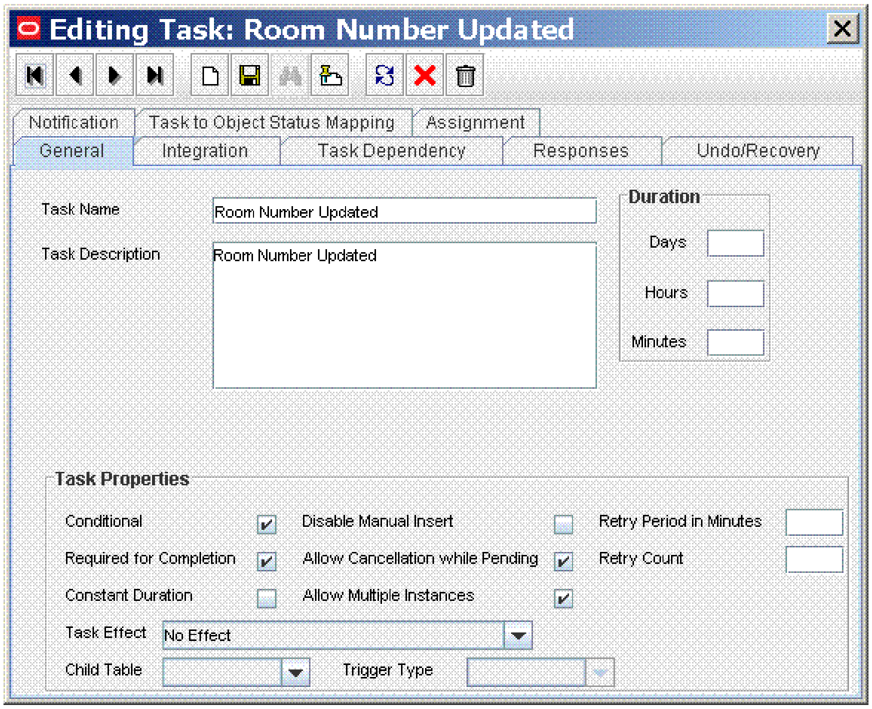
1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open the **SAP UM Process Form** process definition.
3. Click **Add**.
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

   Conditional

   Required for Completion

   Allow Cancellation while Pending

   Allow Multiple Instances
5. Click the Save icon. The following screenshot shows the new task added to the process definition:



Editing Task: Room Number Updated

Task Name: Room Number Updated

Task Description: Room Number Updated

Duration

Days:

Hours:

Minutes:

Task Properties

Conditional ☑ Disable Manual Insert □ Retry Period in Minutes:

Required for Completion ☑ Allow Cancellation while Pending ☑ Retry Count:

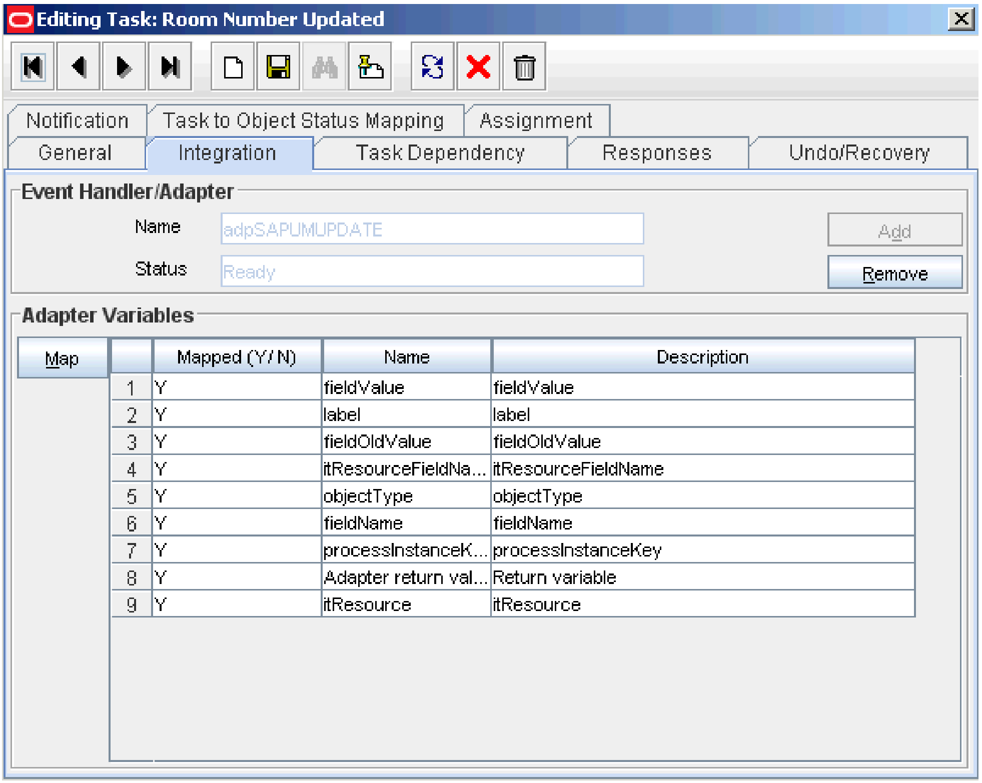
Constant Duration □ Allow Multiple Instances ☑

Task Effect: No Effect

Child Table: Trigger Type:

6. On the Integration tab of the Creating New Task dialog box, click **Add**.
7. In the Handler Selection dialog box, select **Adapter**, click **adpSAPUMUPDATE**, and then click the Save icon.

   The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Event Handler/Adapter

Name: adpSAPUMUPDATE

Status: Ready

Adapter Variables

	Mapped (Y/N)	Name	Description
1	Y	fieldValue	fieldValue
2	Y	label	label
3	Y	fieldOldValue	fieldOldValue
4	Y	itResourceFieldNa...	itResourceFieldName
5	Y	objectType	objectType
6	Y	fieldName	fieldName
7	Y	processInstanceK...	processInstanceKey
8	Y	Adapter return val...	Return variable
9	Y	itResource	itResource

8. 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.

9. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Name	Map To	Qualifier
fieldValue	Process Data	Room Number
fieldName	Literal	String For example: UD_SAP_ROOMNUMBER
itResourceFieldName	Literal	String For example: UD_SAP_ITRESOURCE
objectType	Literal	String For example: User
processInstanceKey	Process Data	Process Instance
fieldOldValue	Process Data	Room Number **Note:** Select the Old Value check box.
label	Literal	String For example: Room Number

Variable Name	Map To	Qualifier
itResource	Literal	String For example: SAP UM ITResource

10. Click the Save icon in the Editing Task dialog box, and then close the dialog box.
11. Click the Save icon to save changes to the process definition.

4.3.4 Updating the Request Dataset

If you are using Oracle Identity Manager release prior to 11.1.2, update the request dataset.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

1. In a text editor, open the request dataset XML file, SAPUM-Datasets.xml, which is in the xml directory of the installation media for editing.
2. Add the AttributeReference element and specify values for the mandatory attributes of this element.

> **See Also:**
>
> For more information about creating and updating request datasets, see the Configuring Requests chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for 11*g* Release 1(11.1.1.5)

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:

```
<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.
- 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.

3. Save and close the XML file.

4.3.5 Running the PurgeCache Utility

If you are using Oracle Identity Manager release prior to 11.1.2, run the PurgeCache utility to clear content related to request datasets from the server cache.

See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.

4.3.6 Importing the Request Dataset Definitions

If you are using Oracle Identity Manager release prior to 11.1.2, import into MDS, the request dataset definitions in XML format.

See Importing Request Datasets Using Deployment Manager for detailed information about the procedure.

4.3.7 Creating a New UI Form to make the New Attribute Visible

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

4.4 Adding New Standard SAP BusinessObjects AC Access Request Management Attributes for Provisioning

You can map additional single-valued attributes between Oracle Identity Manager and SAP BusinessObjects AC Access Request Management.

By default, the attributes listed in Table 1-8 are mapped for sending requests from Oracle Identity Manager to SAP BusinessObjects AC Access Request Management. If required, you can map additional single-valued attributes.

> **Note:**
>
> Perform the procedure described in this section only if you want to map additional standard Access Request Management attributes for requests sent from Oracle Identity Manager to Access Request Management.

To add a new SAP BusinessObjects AC Access Request Management attribute for provisioning, perform the following procedures:

4.4.1 Creating a New Version of the Process Form

If the attribute does not already exist on the process form, then add it on the process form as follows:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools,** and double-click **Form Designer.**
3. Search for and open the **UD_SAP_UMAC** process form.
4. Click Create **New Version,** and then click **Add.**
5. Enter the details of the attribute.

   For example, if you are adding the Telephone field, enter `UD_SAP_UMAC_TELEPHONE` in the **Name** field, and then enter the rest of the details of this field.

   The following screenshot shows this page:

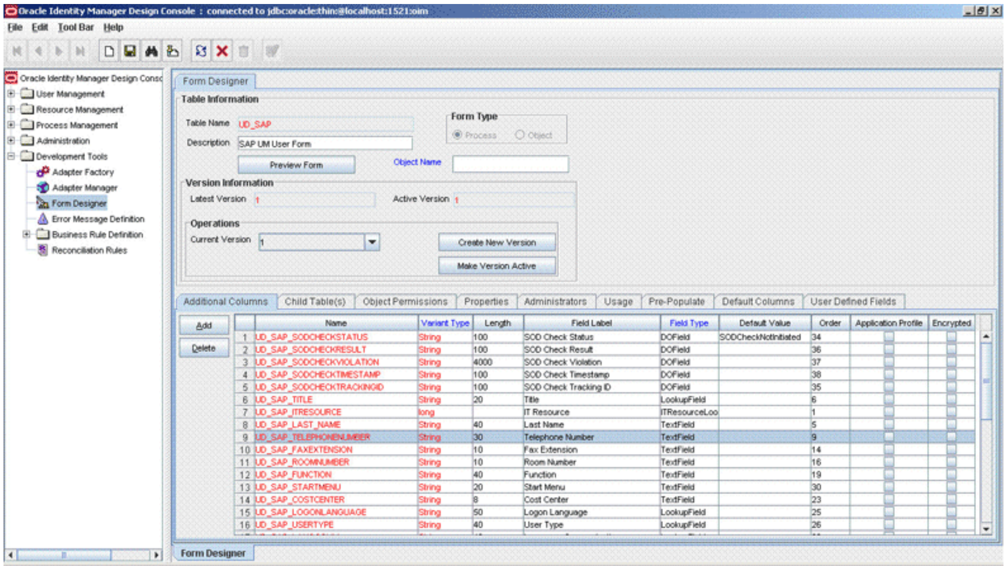


Table Information

Table Name: UD_SAP

Description: SAP UM User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 1

Active Version: 1

Operations

Current Version: 1

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encrypted
1	UD_SAP_SODCHECKSTATUS	String	100	SOD Check Status	DOField	SODCheckNotInitiated	34	□	□
2	UD_SAP_SODCHECKRESULT	String	100	SOD Check Result	DOField		36	□	□
3	UD_SAP_SODCHECKVIOLATION	String	4000	SOD Check Violation	DOField		37	□	□
4	UD_SAP_SODCHECKTIMESTAMP	String	100	SOD Check Timestamp	DOField		38	□	□
5	UD_SAP_SODCHECKTRACKINGID	String	100	SOD Check Tracking ID	DOField		35	□	□
6	UD_SAP_TITLE	String	20	Title	LookupField		6	□	□
7	UD_SAP_ITRESOURCE	long		IT Resource	ITResourceLoo		1	□	□
8	UD_SAP_LAST_NAME	String	40	Last Name	TextField		5	□	□
9	UD_SAP_TELEPHONENUMBER	String	30	Telephone Number	TextField		9	□	□
10	UD_SAP_FAXEXTENSION	String	10	Fax Extension	TextField		14	□	□
11	UD_SAP_ROOMNUMBER	String	10	Room Number	TextField		16	□	□
12	UD_SAP_FUNCTION	String	40	Function	TextField		19	□	□
13	UD_SAP_STARTMENU	String	20	Start Menu	TextField		30	□	□
14	UD_SAP_COSTCENTER	String	8	Cost Center	TextField		23	□	□
15	UD_SAP_LOGONLANGUAGE	String	50	Logon Language	LookupField		25	□	□
16	UD_SAP_USERTYPE	String	40	User Type	LookupField		26	□	□

6. Click the Save icon, and then click **Make Version Active**.

4.4.2 Creating an Entry for the Attribute in the Lookup Definition

Create an entry for the attribute in the Lookup.SAPAC10ABAP.UM.ProvAttrMap lookup definition according to the configured GRC system as follows:

1. Expand **Administration.**
2. Double-click **Lookup Definition.**
3. Search for and open the **Lookup.SAPAC10ABAP.UM.ProvAttrMap** lookup definition.
4. Click **Add** and then enter the Code Key and Decode values for the attribute.

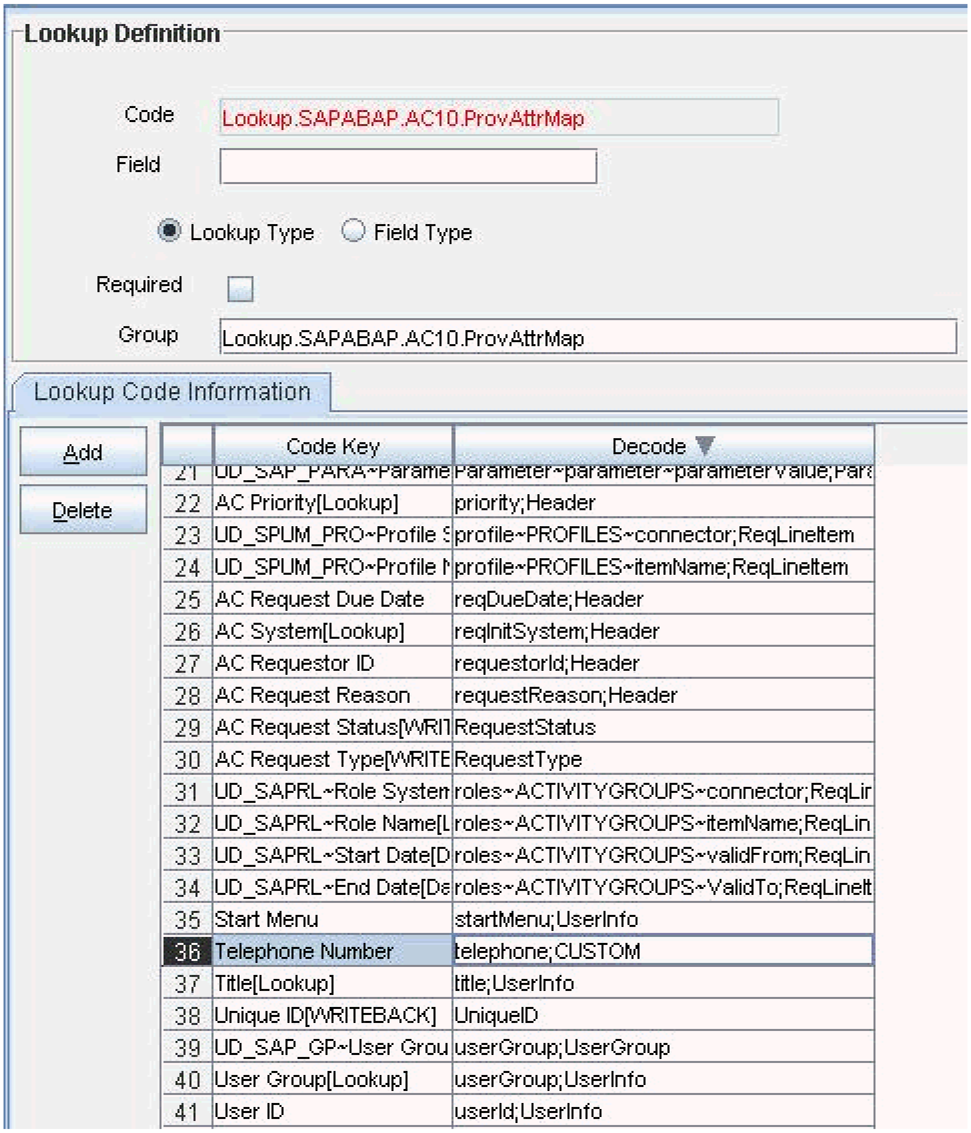
   The Code Key value must be the name of the field on the process form. The Decode value is in the following format:

   FIELD_NAME;CUSTOM

   In this format:

   - *FIELD_NAME* is the name of the attribute.
   - *CUSTOM* is used to specify that the attribute is a custom attribute on SAP BusinessObjects AC Access Request Management.

     The following screenshot shows this page:



Lookup Definition

Code: Lookup.SAPABAP.AC10.ProvAttrMap

Field:

● Lookup Type ○ Field Type

Required ☐

Group: Lookup.SAPABAP.AC10.ProvAttrMap

Lookup Code Information

	Code Key	Decode
21	UD_SAP_PARA~Parame	Parameter~parameter~parameterValue;Para
22	AC Priority[Lookup]	priority;Header
23	UD_SPUM_PRO~Profile S	profile~PROFILES~connector;ReqLineItem
24	UD_SPUM_PRO~Profile N	profile~PROFILES~itemName;ReqLineItem
25	AC Request Due Date	reqDueDate;Header
26	AC System[Lookup]	reqInitSystem;Header
27	AC Requestor ID	requestorId;Header
28	AC Request Reason	requestReason;Header
29	AC Request Status[WRIT	RequestStatus
30	AC Request Type[WRITE	RequestType
31	UD_SAPRL~Role System	roles~ACTIVITYGROUPS~connector;ReqLin
32	UD_SAPRL~Role Name[L	roles~ACTIVITYGROUPS~itemName;ReqLin
33	UD_SAPRL~Start Date[D	roles~ACTIVITYGROUPS~validFrom;ReqLin
34	UD_SAPRL~End Date[Da	roles~ACTIVITYGROUPS~ValidTo;ReqLineIt
35	Start Menu	startMenu;UserInfo
36	Telephone Number	telephone;CUSTOM
37	Title[Lookup]	title;UserInfo
38	Unique ID[WRITEBACK]	UniqueID
39	UD_SAP_GP~User Grou	userGroup;UserGroup
40	User Group[Lookup]	userGroup;UserInfo
41	User ID	userId;UserInfo

4.4.3 Creating a Task to Update the Attribute During Provisioning Operations

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 BusinessObjects AC Access Request Management 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:**
>
> Creating Provisioning Metadata in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about creating a process form

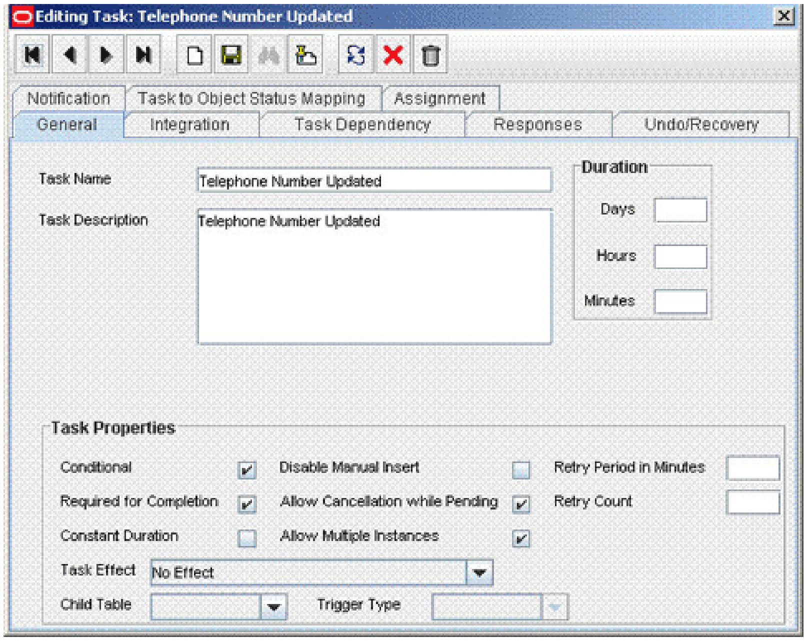
1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open the **SAP AC UM ProcessForm** process definition.
3. Click **Add**.
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

   Conditional

   Required for Completion

   Allow Cancellation while Pending

   Allow Multiple Instances
5. Click the Save icon. The following screenshot shows the new task added to the process definition:



Task Name: Telephone Number Updated

Task Description: Telephone Number Updated

Duration: Days, Hours, Minutes

Task Properties

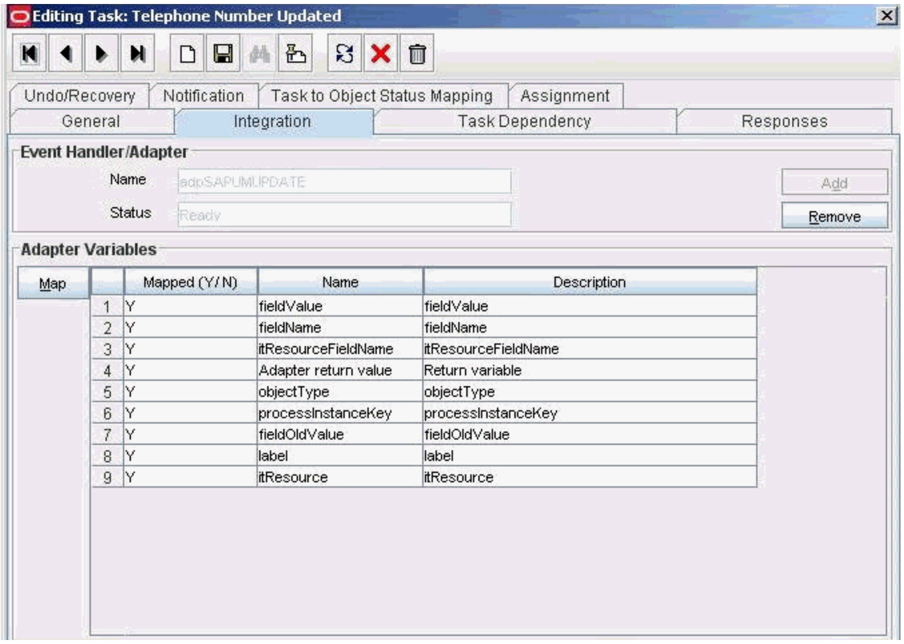
Conditional	☑	Disable Manual Insert	□	Retry Period in Minutes	
Required for Completion	☑	Allow Cancellation while Pending	☑	Retry Count	
Constant Duration	□	Allow Multiple Instances	☑		

Task Effect: No Effect

Child Table:

6. On the Integration tab of the Creating New Task dialog box, click **Add**.
7. In the Handler Selection dialog box, select **Adapter**, click **adpSAPACUMUPDATEUSER,** and then click the Save icon.

   The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:



Name: adpSAPUMUPDATE

Status: Ready

	Mapped (Y/N)	Name	Description
1	Y	fieldValue	fieldValue
2	Y	fieldName	fieldName
3	Y	itResourceFieldName	itResourceFieldName
4	Y	Adapter return value	Return variable
5	Y	objectType	objectType
6	Y	processInstanceKey	processInstanceKey
7	Y	fieldOldValue	fieldOldValue
8	Y	label	label
9	Y	itResource	itResource

8. 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.

9. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Name	Map To	Qualifier
fieldValue	ProcessData	Telephone Number
fieldName	Literal	String For example: UD_SAP_UMAC_TELEPHONENUMBER
itResourceFieldName	Literal	String For example: UD_SAP_ITRESOURCE
objectType	Literal	String For example: User
processInstanceKey	Process Data	Process Instance
fieldOldValue	Process Data	Telephone Number **Note:** Select the Old Value check box.
itResource	Literal	String For example: GRC-ITRes

10. Click the Save icon in the Editing Task dialog box, and then close the dialog box.
11. Click the Save icon to save changes to the process definition.

4.4.4 Updating the Request Dataset

If you are using Oracle Identity Manager release prior to 11.1.2, update the request dataset.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

1. In a text editor, open the request dataset XML file, SAPUM-Datasets.xml, which is in the xml directory of the installation media for editing.
2. Add the AttributeReference element and specify values for the mandatory attributes of this element.

> **See Also:**
>
> For more information about creating and updating request datasets, refer to the Configuring Requests chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for Release 11*g* Release 1 (11.1.1.5) .

For example, while performing Step 2 of this procedure, if you added Telephone Number as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "TELEPHONENUMBER"
attr-ref = "Telephone Number"
type = "String"
widget = "text"
length = "30"
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_TELEPHONENUMBER is the value in the Name column of the process form, then you must specify `TELEPHONENUMBER` 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 2.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 2.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 2.
- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 2.
- For the available-in-bulk attribute, specify `true` if the data value is available for bulk modification. Otherwise specify `false`.

While performing Step 2, if you added more than one attribute on the process form, then repeat this step for each attribute added.

3. Save and close the XML file.

4.4.5 Running the PurgeCache Utility

If you are using Oracle Identity Manager release prior to 11.1.2, run the PurgeCache utility to clear content related to request datasets from the server cache.

See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.

4.4.6 Importing the Request Datasets into MDS

If you are using Oracle Identity Manager release prior to 11.1.2, import into MDS, the request dataset definitions in XML format.

See Importing Request Datasets Using Deployment Manager for detailed information about the procedure.

4.4.7 Creating a New UI Form to make the New Attribute Visible

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

4.5 Removing SAP BusinessObjects AC Access Request Management Attributes from Process Form

You can remove SAP BusinessObjects AC Access Request Management attributes if the connector is not configured for SAP BusinessObjects AC.

The form attributes used for Access Request Management are prefixed with AC. These attributes are available in the process form. If the connector is not configured for SAP BusinessObjects AC, then the AC-specific attributes can be removed manually.

See SAP BusinessObjects AC Access Request Management Attributes for a consolidated list of SAP BusinessObjects AC attributes.

To remove the AC attributes from the process form:

1. From Oracle Identity Manager Design Console, expand **Development Tools.**
2. Double-click **Form Designer.**
3. Search for and open the **UD_SAP_UMAC** process form.
4. Click **Create New Version.**
5. In the Label field, enter the version name. For example, `version#1`.
6. Click the Save icon.
7. Select the current version created in Step 5 from the Current Version list.
8. Select the AC field to be removed.
9. Click **Delete** to remove the selected attribute row from the form.
10. Similarly, repeat Steps 8 and 9 until you remove all the AC attributes.
11. Click the Save icon.
12. Click **Make Version Active.**
13. If you are using Oracle Identity Manager release 11.1.1, after you remove an attribute on the process form, you must update the XML file containing the request dataset definitions. To update a request dataset:

    a. Locate and open the SAPUM-Datasets.xml file, which is located in the xml directory of the installation media.

    b. Search for and find the AC field tags. You can either comment or delete the entire set of AC field tags in the XML file.

    c. Save and close the XML file.

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

    See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.

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

    See Importing Request Datasets Using Deployment Manager for detailed information about the procedure.

4.5.1 SAP BusinessObjects AC Access Request Management Attributes

The form attributes used for Access Request Management are prefixed with AC. These attributes are available in the process form.

The following is the list of AC attributes:

- AC Manager
- AC Manager email
- AC Priority
- AC System
- AC Requestor ID
- AC Requestor email
- AC Request Reason
- AC Manager First Name
- AC Manager Last Name
- AC Manager Telephone
- AC Request Due Date
- AC Functional Area
- AC Business Process
- AC Requestor First Name
- AC Requestor Last Name
- AC Requestor Telephone
- AC Request Reason
- AC Request Status
- AC Request Type
- AC Company

4.6 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.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class with a fully qualified domain name (FQDN), such as `org.identityconnectors.sapum.extension.SAPUMValidator`.

This validation class must implement the validate method. The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

```
package com.validationexample;

import java.util.HashMap;

public class MyValidator {
    public boolean validate(HashMap hmUserDetails, HashMap
hmEntitlementDetails, String sField) throws ConnectorException {

        /* 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(sField);
        for (int i = 0; i < sFirstName.length(); i++) {
            if (sFirstName.charAt(i) == '#') {
                valid = false;
                break;
            }
        }
        return valid;

    }
}
```

2. Log in to the Design Console.

3. Search for and open one of the lookup definitions listed in Lookup Definitions for Validation of Data.

   For example, if you are using the SAP AC UM connector, then search for and open the **Lookup.SAPAC10ABAP.UM.ProvValidation** lookup definition.

   > **Note:**
   >
   > If you cannot find these lookup definitions, create new lookup definitions.

4. In the **Code Key** column, enter the resource object field name that you want to validate. For example, `Username`.

5. In the **Decode** column, enter the class name. For example, `org.identityconnectors.sapum.extension.SAPUMValidator`.

6. Save the changes to the lookup definition.

7. Search for and open the configuration lookup definition for the target system you use.

   For example, if you are using the SAP AC UM connector, then search for and open the **Lookup.SAPAC10ABAP.UM.ProvValidation** lookup definition.

8. In the **Code Key** column, enter one of the following entries:

   - To configure validation of data for reconciliation:

     `Recon Validation Lookup`

   - To configure validation of data for provisioning:

     `Provisioning Validation Lookup`

9. In the **Decode** column, enter the name of the lookup you updated or created in step 3.

   For example, if you are using the SAP AC UM connector, then search for and open the **Lookup.SAPAC10ABAP.UM.ProvValidation** lookup definition.

10. Save the changes to the lookup definition.

11. Create a JAR with the class and upload it to the Oracle Identity Manager database as follows:

    Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 7 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. Select 1 as the value of the JAR type.

    > **See Also:**
    >
    > Upload JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Upload JARs utility

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

13. Perform reconciliation or provisioning to verify validation for the field, for example, Username.

4.7 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 with a fully qualified domain name (FQDN), such as `org.identityconnectors.sapum.extension.SAPUMTransfomation`.

   This transformation class must implement the transform method. The following sample transformation class modifies the Username attribute by using values fetched from the __NAME__ attribute of the target system:

   ```
   package com.transformationexample;

   import java.util.HashMap;


   public class MyTransformer {
       public Object transform(HashMap hmUserDetails, HashMap
   hmEntitlementDetails, String sField) throws ConnectorException {
           /*
           * 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 sUserName = (String) hmUserDetails.get("__NAME__");
           return sUserName + "@example.com";

       }
   }
   ```

2. Log in to the Design Console.

3. Search for and open one of the lookup definitions (or create a new lookup) listed in Lookup.SAPABAP.UM.ReconTransformation.

   For example, if you are using the SAP AC UM connector, then search for and open the **Lookup.SAPAC10ABAP.UM.ReconTransformation** lookup definition.

   Note:

   If you cannot find these lookup definitions, create new lookup definitions.

4. In the **Code Key** column, enter the resource object field name you want to transform. For example, `Username`.

5. In the **Decode** column, enter the class name. For example, `org.identityconnectors.sapum.extension.SAPUMTransfomation`.
6. Save the changes to the lookup definition.
7. Search for and open the **Lookup.SAPABAP.UM.Configuration** lookup definition. If you are using the SAP AC UM connector then open the **Lookup.SAPAC10ABAP.UM.ReconTransformation** lookup definition.
8. In the **Code Key** column, enter `Recon Transformation Lookup`.
9. In the **Decode** column, enter the name of the lookup you updated or created in step 3.

   For example, if you are using the SAP AC UM connector then enter `Lookup.SAPAC10ABAP.UM.ReconTransformation`.
10. Save the changes to the lookup definition.
11. Create a JAR with the class and upload it to the Oracle Identity Manager database as follows:

    Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 7 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. Select 1 as the value of the JAR type.

    > **See Also:**
    >
    > Upload JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Upload JARs utility
12. Run the PurgeCache utility to clear content related to request datasets from the server cache.
13. Perform reconciliation to verify transformation of the field, for example, SimpleDisplayName.

4.8 Configuring Resource Exclusion Lists

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

In one of the lookup definitions for exclusion lists, enter the user IDs of target system accounts for which you do not want to perform provisioning and reconciliation operations. See Lookup Definitions for Exclusion Lists for information about the lookup definitions and the format of the entries in these lookups.

To add entries in the lookup for exclusions during provisioning or reconciliation operations:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the **Lookup.SAPACABAP.UM.ProvExclusionList** or **Lookup.SAPACABAP.UM.ReconExclusionList** lookup definition.
3. Click **Add.**
4. In the Code Key and Decode columns, enter the first user ID to exclude.

   > **Note:**
   >
   > The Code Key represents the resource object field name on which the exclusion list is applied during provisioning operations.

5. Repeat Steps 3 and 4 for the remaining user IDs to exclude.

   For example, if you do not want to provision users with user IDs User001, User002, and User088 then you must populate the lookup definition with the following values:

Code Key	Decode
userName	User001
userName	User002
userName	User088

   You can also perform pattern matching to exclude user accounts. You can specify regular expressions supported by the representation in the `java.util.regex.Pattern` class.

   > **See Also:**
   >
   > For information about the supported patterns, visit `http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html`

For example, if you do not want to provision users matching any of the user IDs User001, User002, and User088, then you must populate the lookup definition with the following values:

Code Key	Decode
userName[PATTERN]	User001|User002|User088

If you do not want to provision users whose user IDs start with 00012, then you must populate the lookup definition with the following values:

Code Key	Decode
userName[PATTERN]	00012*

6. Click the save icon.

4.9 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. If you are using the SAP AC UM connector, open the **UD_SAP_UMAC** 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**.
10. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to activate this modified field length. See Creating a New UI Form and Updating an Existing Application Instance with a New Form for detailed procedures.

4.10 About 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.SAPABAP.Configuration. If you create a copy of an object, then you must specify the name of the copy in associated connector objects. Table 4-1 lists associations between connector objects whose copies can be created and the other objects that reference these objects. When you create a copy of a connector object, use this information to change the associations of that object with other objects.

Note:

On a particular Oracle Identity Manager installation, if you create a copy of a connector object, then you must set a unique name for it.

Table 4-1 Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
IT resource	SAP UM ITResource	Scheduled tasks	Create a copy of the IT resource. See Configuring the IT Resource for more information.

Table 4-1 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Resource object	SAP UM Resource Object	Scheduled tasks	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 Scheduled Jobs for Lookup Field Synchronization and Reconciliation Scheduled Jobs for the SAP UM Connector for more information.
Process definition	SAP UM Process Form	NA	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.
Attribute Mapping Lookup Definition	Lookup.SAPABAP.UM.ProvAttrMap Lookup.SAPABAP.UM.ReconAttrMap	NA	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: Connector Objects Used During Target Resource Reconciliation Connector Objects Used During Provisioning
Process form	UD_SAP	NA	Create a copy of a process form 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.
Configuration lookup definition	Lookup.SAPABAP.Configuration	SAP UM ITResource (IT resource)	Create copies of this lookup definition only if you want to use a different set of configuration values for the various installations of the target system. See Section 2.3.3, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager" for more information.
Lookup mappings lookup definitions	See Lookup Definitions Synchronized with the Target System for the list of lookups.	Scheduled tasks	Create copies of these lookup definition only if you want to use a different set of lookup mappings for the various installations of the target system.

When you configure reconciliation:

To reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the scheduled task attribute that holds the IT resource name. For example, you enter the name of the IT resource as the value of the IT resource attribute of the SAP UM User Recon scheduled task.

When you perform provisioning operations:

When you use Oracle Identity System Administration to perform provisioning, you can specify the IT resource corresponding to the target system installation to which you want to provision the user.

5

Known Issues and FAQs

This chapter is divided into the following sections:

- Known Issues
- Frequently Asked Questions (FAQs)

5.1 Known Issues

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

- **Bug 14152765**

  If the size of the violation details obtained from SAP BusinessObjects AC target system is more than 4000 characters, then you must update the Length of the SODCheckViolation field as per the expected size of the violation data.

- **Bug 14391414**

  The ICF-based SAP User Management connector and the legacy SAP ER connector do not work together with Oracle Identity Manager because ICF uses a different class loader for each connector bundle. When both the connectors are installed, the connector bundle that creates the first connection will work. When the second bundle tries to create a connection, it will try to register the data provider that is already registered by first bundle. Then, it throws an error, "DestinationDataProvider already registered".

  As a work around, to use both the SAP User Management connector and the legacy SAP ER connector, deploy the SAP UM connector in a connector server and deploy the SAP ER connector in Oracle Identity Manager.

- **Bug 19683143**

  Before upgrading the connector, the lookup default decode values of Lookup.SAPAC10ABAP.Configuration and Lookup.SAPABAP.Configuration are upgraded with target configuration values.

  Once the connector is upgraded, it generates duplicate entries with decode default values.

  As a work around, manually delete each instance of the duplicate entries with decode default values.

- **Bug 23559285**

  In Access Request Management (AC) flow, if you trigger a revoke account in OIG and reject the revoke request for the same account in GRC, then the account is still active in the SAP ECC system (backend ABAP system) and you cannot modify the account details in OIG.

  There is no workaround for this issue.

- **Enh 11835752**

If application server is not restarted whenever any JAR is updated or modified, then it throws the following error:

```
java.lang.UnsatisfiedLinkError: Native Library
      /usr/local/jco/libsapjco3.sojava.lang.UnsatisfiedLinkError:
Native  Library
      /usr/local/jco/libsapjco3.dll
```

It is a limitation from SAP JCO. Whenever any JAR is updated or 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 is to restart the application server if any JAR is updated or modified in the Oracle Identity Governance server.

5.2 Frequently Asked Questions (FAQs)

You can refer the following FAQs as guidelines and to troubleshoot connector issues:

1. What is the cause of "Class Definition not found" error while running lookup schedulers or provisioning a user for the first time after installing and configuring the connector successfully?

   Answer: The class path of SapJCo.jar may not be detected. Mention its path in the startWebLogic.cmd file located in *DOMAIN_HOME/*bin. For more information, refer to Step 4 of Downloading and Installing the SAP JCo.

2. Can I simultaneously use the SAP ER and the SAP UM connectors in the same Oracle Identity Manager environment?

   Answer: Yes, but it is possible only if you have one connector configured as connector server and the other connector installed directly in the same Oracle Identity Manager. Refer to Bug 14391414 in Known Issues for more information.

3. I have decided to use the SAP UM connector directly without configuring the Access Request Management feature. The default process form has AC fields in it. How do I remove these AC fields from the form?

   Answer: See Removing SAP BusinessObjects AC Access Request Management Attributes from Process Form for the procedure.

4. I have changed the system property for SOD as XL.SoDCheckRequired = TRUE. Is it now possible to use two SAP connectors in the same OIM environment having one connector configured for SOD analysis and the other connector configured without SOD analysis?

   Answer: No, the system property is common in OIM. Hence, the property applies to all the connectors installed in that OIM.

5. I have configured the connector for Access Request Management and would like to see the Audit trail details. Where can I get these details?

   Answer: To get the Audit trail details, you need to enable the logs specific to AC for the connector. The Audit trail details can be viewed in the log file along with the connector logs.

   Here are a few formatted samples of the Audit trial:

   - **Create User**

Audit Trial: {Result=[Createdate:20130409,

Priority: HIGH,

Requestedby:, johndoe (JOHNDOE),

Requestnumber: 9000001341,

Status: Decision pending,

Submittedby:, johndoe (JOHNDOE),

auditlogData:{,ID:000C290FC2851ED2A899DA29DAA1B1E2,

Description:,

Display String: Request 9000001341 of type **New Account** Submitted by johndoe (JOHNDOE) for JK1APRIL9 JK1APRIL9 (JK1APRIL9) with Priority HIGH}],

Status=0_Data Populated successfully}

- **Request Status**

  Audit Trial: {Result=[Createdate:20130409,

  Priority:HIGH,

  Requestedby:,johndoe (JOHNDOE),

  Requestnumber: 9000001341,

  Status: Approved,

  Submittedby:, johndoe (JOHNDOE),

  auditlogData:{,ID:000C290FC2851ED2A899DA29DAA1B1E2,

  Description:,

  Display String: Request 9000001341 of type **New Account** Submitted by johndoe (JOHNDOE) for JK1APRIL9 JK1APRIL9 (JK1APRIL9) with Priority HIGH,

  ID: 000C290FC2851ED2A899DAF9961C91E2,Description:,Display String:Request is pending for approval at path GRAC_DEFAULT_PATH stage GRAC_MANAGER,

  ID: 000C290FC2851ED2A89A1400B60631E2,

  Description:,

  Display String: Approved by JOHNDOE at Path GRAC_DEFAULT_PATH and Stage GRAC_MANAGER,

  ID: 000C290FC2851ED2A89A150972D091E2,

  Description:,

  Display String: Auto provisioning activity at end of request at Path GRAC_DEFAULT_PATH and Stage GRAC_MANAGER,

  ID: 000C290FC2851ED2A89A150972D111E2,

  Description:,

  Display String: Approval path processing is finished, end of path reached,

  ID: 000C290FC2851ED2A89A150972D151E2,

  Description:,

Display String: Request is closed}],

Status=0_Data Populated successfully}

- **Modify Request (First Name)**

  Audit Trial: {Result=[Createdate:20130409,

  Priority: HIGH,

  Requestedby:, johndoe (JOHNDOE),

  Requestnumber: 9000001342,

  Status: Decision pending,

  Submittedby:,johndoe (JOHNDOE),

  auditlogData:{,

  ID: 000C290FC2851ED2A89A3ED3B1D7B1E2,

  Description:,

  Display String: Request 9000001342 of type **Change Account** Submitted by johndoe (JOHNDOE) for JK1FirstName JK1APRIL9 (JK1APRIL9) with Priority HIGH}],

  Status=0_Data Populated successfully}

6. What is the purpose of SAP Roles and SAP Profiles resource objects available with the connector?

   Answer: These resource objects must be used only with Oracle Identity Manager 11*g* Release 1 (11.1.1). They are used in Oracle Identity Manager release 11.1.1 to serve the same purpose as entitlements do in Oracle Identity Manager 11*g* Release 2 (11.1.2). They are not required in Oracle Identity Manager release 11.1.2.

7. During a Create User provisioning operation, does the SAP UM AC connector provision attributes that are mapped directly to SAP ECC system without GRC?

   Answer: No, for account creation request in GRC, the request is created only with the GRC attributes. Attributes mapped directly to SAP ECC system are not part of the create operation. Once the request is approved and the account is provisioned to the SAP ECC system (backend ABAP system), these attributes (mapped directly to SAP) can be provisioned as part of the update operation.

8. Why am I not able to add groups when using SAP UM connector for access control?

   Answer: This a desired behavior and not a bug. Groups need to be managed on the backend server only.

9. Which version of the SAP BusinessObjects Access does the connector support?

   Answer: As listed in Table 1-1, the connector supports SAP BusinessObjects Access versions 10, 10.1, and 12.

   While configuring the connector, if you are using SAP BusinessObjects Access version 10.1 or 12, you need not modify the lookup definition name.

10. Is the SoD Check Tracking ID field no longer populated with a value during the SoD check?

Answer: From Oracle Identity Manager 11.1.2.*x*, the **SoD Check Tracking ID** field no longer populates a value during the SoD check. You can ignore this field as it displays a null value and does not result in functionality loss.

6

Troubleshooting the Connector

This chapter provides solutions to problems you might encounter after you deploy or while using the SAP User Management connector.

The following table provides solutions to common SNC errors:

Table 6-1   Common SNC Errors

Problem Description	Solution
Trying to connect to SAP through SNC. **Returned Error Message:** SAP Connection JCO Exception **Returned Error Code** SNC required or this connection	Ensure that the values for the following IT resource parameters are correctly specified as shown in the following example: • sncName: `p:CN=TST,OU=SAP, O=ORA,c=IN` • snc_PartnerName: `p:CN=I47, OU=SAP, O=ORA, C=IN` • sncLib: The following are examples of sncLib paths for Windows and Linux: – For Windows: `sncLib: C://usr//sap//sapcrypto.dll` – For Linux: `sncLib: //home/oracle/sec/sapcrypto.so` • useSNC: `True`
When you try to provision account or lookup field synchronization in SNC mode **Returned Error Message:** No suitable SAP user found for X.509-client certificate **Returned Error Code:** JCO_ERROR_LOGON_FAILURE	Set up a mapping between the Distinguished Name provided by an X.509 Certificate and an ABAP User in the VUSREXTID view in the SM30 transaction. Choose external ID type as DN.
When you try to provision account or lookup field synchronization in SNC mode **Returned Error Message:** SNC name of partner system not in the ACL system **Returned Error Code:** `JCO_ERROR_LOGON_FAILURE`	Maintain SNC names of the system from which RFC and CPIC connections are to be accepted in the VSNCSYSACL view for External type ACL entry.
When you try to provision account or lookup recon in SNC mode **Returned Error Message:** Reconcillation via TRFC fails when SNC is enabled **Returned Error Code:** `JCO_ERROR_LOGON_FAILURE`	Program ID must have SNC enabled in transaction SM59.

A

Files and Directories in the SAP UM Connector Package

These are the components of the connector installation media that comprise the SAP UM connector.

The contents of the connector installation package are described in Table A-1.

Table A-1 Files and Directories in the Installation Media

File in the Installation Package	Description
bundle/ org.identityconnectors.sap-1.0.11170 bundle/ org.identityconnectors.sapacum-1.0.11170	These JAR files contain the connector bundle. Use org.identityconnectors.sapacum-1.0.11170.jar file if you are using SAP BusinessObjects AC system.
configuration/ SAPUMConnector-CI.xml configuration/ SAPACUMConnector-CI.xml	This XML file contains configuration information that is used during the connector installation process. Use the SAPACUMConnector-CI.xml file if you are using SAP BusinessObjects AC system.
lib/sap-oim-integration.jar	This JAR file is required to request entitlements for roles and profiles through request-based provisioning using request dataset.
lib/sapac-oim-integration.jar	This JAR file includes a custom scheduled job to update request status from SAP BusinessObjects AC.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied to Oracle Identity Manager database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages.
Files in the sar directory	The SAR file contains custom BAPI/RFC that is used to propagate the password to SAP CUA child systems.
xml/SAPUM-Datasets.xml	This XML file contains attributes of the following resource objects for request-based provisioning: • SAP UM Resource Object (to provision and modify resources) • SAP UM Roles (to provision role entitlements) • SAP UM Profiles (to provision profile entitlements) **Note:** This dataset should *not* be imported if you are using Oracle Identity Manager release 11.1.2.*x* or later.
xml/SAPUM-ConnectorConfig.xml xml/SAPACUM-ConnectorConfig.xml	This XML file contains definitions of connector objects. Use the SAPACUM-ConnectorConfig.xml file if you are using SAP BusinessObjects AC system.
upgrade/PostUpgradeScript	This file contains the scripts that are run after performing an upgrade of the connector.

B

Standard BAPIs Used During Connector Operations

Standard BAPIs used during connector operations can be categorized as follows:

- Standard BAPIs Used on SAP CUA
- Custom BAPIs Used on SAP CUA

B.1 Standard BAPIs Used on SAP CUA

The following standard BAPIs are 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
- BAPI_USER_LOCPROFILES_ASSIGN: Changes User-Profile assignments in CUA Central system
- BAPI_USER_LOCACTGROUPS_ASSIGN: Changes User-Role assignments in CUA Central system

B.2 Custom BAPIs Used on SAP CUA

The following custom BAPIs are used during connector operations on SAP CUA:

- ZXLCBAPI_ZXLCUSR_PASSWORDCHNGE: Changes the productive password for a user on a CUA child system.
- ZXLCBAPI_ZXLCUSR_PW_CHANGE: Changes the initial password for a user on all CUA child systems.

> **Note:**
>
> Refer to Importing the Request for importing the request in CUA lanscape.

Import the following TRs in given sequence in the parent as well as child system to get the mentioned BAPIs:

- EC1K900023

- G10K900013

Index