Oracle® Identity Governance

Configuring the SAP User Management Application

12c (12.2.1.3.0)
F12375-13
January 2023

ORACLE

Oracle Identity Governance Configuring the SAP User Management Application, 12c (12.2.1.3.0)

F12375-13

Primary Author: Oracle Corporation

Contents

4 Performing Postconfiguration Tasks for the SAP User Management Connector

5 Using the SAP User Management Connector

6 Extending the Functionality of the SAP User Management 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 Governance 12.2.1.3.0, visit the following Oracle Help Center page:

http://docs.oracle.com/middleware/12213/oig/index.html

For information about installing and using Oracle Identity Manager 11.1.2.3, visit the following Oracle Help Center page:

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

For information about Oracle Identity Governance Connectors 12.2.1.3.0 documentation, visit the following Oracle Help Center page:

http://docs.oracle.com/middleware/oig-connectors-12213/index.html

For information about Oracle Identity Manager Connectors 11.1.1 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.
`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 This Guide?

These are the updates made to the software and documentation for release 12.2.1.3.0 of Configuring the SAP User Management Application.

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

From this release onward, the connector bundle includes application onboarding templates required for performing connector operations on the SAP User Management and SAP Access Control User Management targets. This helps in quicker onboarding of the applications for these targets into Oracle Identity Governance by using an intuitive UI.

Support for Target System Version

From this release onward, the connector supports SAP NetWeaver 7.5 with the following details as a target system:

- 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
  - SAP Enhancement Package 4for SAP SRM 7.0
- SAP S/4 HANA 1610 with component S4CORE Release 101 SP 0000

Support for SAP Governance, Risk and Compliance Access Control (GRC AC)

- SAP GRC 10.1 on SAP NetWeaver 7.5 with SAPBASIS 7.5 with component GRCFND_A V1100 SP 19 NetWeaver 7.5 (ECC6EHP8) 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 OIG
- 2399698: For WebService grac_risk_analysis_wout_no_ws, ReportFormat is mandatory field from SP17

- SAP GRC AC 10.1 on SAP NetWeaver 7.5 with SAP BASIS 7.5 with component GRCFND_A V1100 SP 12 NetWeaver 7.5 (ECC6EHP8) with plugin GRCPINW V1100_731 SP 14.

> **Note:**
>
> 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

Issues Resolved in 12.2.1.3.0

The following are issues resolved in 12.2.1.3.0:

Bug Number	Issue	Resolution
25200576	The SAP AC UM Request Status scheduled job failed to update the status in the process form because of an API-level change in ICF layer.	This issue has been resolvd by using a comptaible API.
26128086	Reconciliation mapping for the fax extension and communication type target system attributes were missing in the process definition task.	This issue has been resolved by including reconciliation mappings in the SAPUM-ConnectorConfig.xml file.

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following document-specific update has been made in revision "09" of the guide:

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

The following document-specific update has been made in revision "08" of the guide:

Information about Oracle Identity Governance cluster has been added to Advanced Settings Parameters and Enabling Logging.

The following document-specific update has been made in revision "07" of the guide:

The "Target systems" row of Certified Components has been updated to include SAP BPC 11.1 with component BPC4HANA Release 200 SP 0001.

The following document-specific updates have been made in revision "06" of the guide:

Information about Oracle Identity Manager versions prior to 11*g* Release 2 PS3 (11.1.2.3.0) has been removed from the guide.

The following document-specific updates have been made in revision "05" of the guide:

- The "Target systems" and "SAP Governance, Risk and Compliance Access Control (GRC AC)" rows of Certified Components have been updated.
- Usage Recommendation has been updated to include support for SAP NetWeaver 7.51.
- Image in Assigning Roles to a User Account in a SAP GRC System for Connector Operations has been modified.

The following document-specific updates have been made in revision "04" of the guide:

- Assigning Roles to a User Account in a SAP GRC System for Connector Operations has been updated.
- Creating a Target System User Account for the SAP HR Target has been updated.
- Frequently Asked Questions for the SAP User Management Connector has been updated to include information about the SoD Check Tracking ID field.

The following document-specific update has been made in revision "03" of the guide:

- Configuring Password Changes for Newly Created Accounts and Configuring Password Changes for Newly Created Accounts has been modified.

The following document-specific updates have been made in revision "02" of the guide:

- In this revision, the document is updated for editorial corrections.
- The following updates have been made to Certified Components:
  - 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
- The following steps have been modified:
  - Step 1 of Installing the Security Package

  - Step 2 of Creating a Target System User Account for the SAP UM (SAP ERP or SAP CUA) Target
  - Step 3.b of Configuring SNC
  - Step 4 of Downloading and Installing the SAP JCo
- A "Note" regarding entitlements has been added to SoD Validation of Entitlement Requests.
- Usage Recommendation has been modified to include support for Oracle Identity Governance 12*c* (12.2.1.4.0).

1

About the SAP User Management Connector

Oracle Identity Governance is a centralized identity management solution that provides self service, compliance, provisioning and password management services for applications residing on-premise or on the Cloud. Oracle Identity Governance connectors are used to integrate Oracle identity Governance with the external identity-aware applications.

The SAP User Management connector (SAP UM connector) lets you onboard applications in Oracle Identity Governance.

The SAP UM connector can be integrated with two flavors of SAP target systems (SAP Netweaver ABAP Application Server and SAP GRC Access Request Management).

The SAP UM connector is used for provisioning and reconciling accounts from SAP NetWeaver ABAP Application Server. This connector also supports SoD validation feature with the help of SAP GRC Access Risk Analysis (ARA) module. The SAP AC UM Connector can be configured with SAP GRC Access Request Managent (ARM) module for user provisioning through web services.

> **Note:**
>
> In this guide, the connector that is deployed using the **Applications** option on the **Manage** tab of Identity Self Service is referred to as an **AOB application**. The connector that is deployed using the **Manage Connector** option in Oracle Identity System Administration is referred to as a **CI-based connector** (Connector Installer-based connector).

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Oracle Identity Self Service. This capability lets business users to onboard applications with minimum details and effort. The connector installation package includes a collection of predefined templates (XML files) that contain all the information required for provisioning and reconciling data from a given application or target system. These templates also include basic connectivity and configuration details specific to your target system. The connector uses information from these predefined templates allowing you to onboard your applications quickly and easily using only a single and simplified UI.

Application onboarding is the process of registering or associating an application with Oracle Identity Governance and making that application available for provisioning and reconciliation of user information.

This following topics provide a high-level overview of the SAP UM connector:

- Certified Components
- Usage Recommendation
- Certified Languages
- Supported Connector Operations

- Connector Architecture
- Supported Deployment Configurations
- Supported Connector Features Matrix
- Connector Features

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

1.1 Certified Components

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

Table 1-1 Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based connector
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* Release BP02 (12.2.1.3.2)	You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* Release BP02 (12.2.1.3.2) • 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 for AOB Application	Requirement for CI-Based connector
Target systems	The target system can be any one of the following: • 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 ERP 6.0 SAP Enhancement Package 4 for SAP CRM 7.0 SAP Enhancement Package 4 for SAP SRM 7.0 SAP Enhancement Package 4 for SAP SCM 7.0 SAP BW/4 HANA 1.0 with component DW4CORE Release 100 SP 0003 • 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	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:

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based connector
	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 • SAP ABAP Platform 2021 SAP S/4HANA 2021 with component S4CORE Release 106 SP 0000	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 ERP 6.0 SAP Enhancement Package 4 for SAP CRM 7.0 SAP Enhancement Package 4 for SAP SRM 7.0 SAP Enhancement Package 4 for SAP SCM 7.0 SAP BW/4 HANA 1.0 with component DW4CORE Release 100 SP 0003 • 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

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based connector
		SAP S/4HANA 2020 with component S4CORE Release 105 SP 0000 • SAP ABAP Platform 2021 SAP S/4HANA 2021 with component S4CORE Release 106 SP 0000
Connector Server	11.1.2.1.0 or 12.2.1.3.0	11.1.2.1.0 or 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	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.	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 for AOB Application	Requirement for CI-Based connector
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 12 for SAP S/4 HANA 2021 with SAP_BASIS 756 with plugin GRCPINW V1200_750 SP 16 • 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	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 12 for SAP S/4 HANA 2021 with SAP_BASIS 756 with plugin GRCPINW V1200_750 SP 16 • 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,

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based connector
	• 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	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.

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based connector
	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 **Note**: If you are using any other SAP application, then you must install the RTA component which is compatible with that SAP application.	

Note:

In general:

- SAP applications installed on the ABAP stack are supported.
- Applications installed on the JAVA stack are *not* supported.
- Some SAP application can be installed on the ABAP+JAVA stack. While installing such an application, you specify ABAP or JAVA as the data source. The connector supports SAP applications that use the ABAP data source.

1.2 Usage Recommendation

These are the recommendations for the SAP UM connector versions that you can deploy and use depending on the Oracle Identity Governance or Oracle Identity Manager version that you are using.

> **Note:**
>
> In Oracle Identity Manager, you can install and configure both SAP UM and SAP UM 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.

- 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 7.51 SPS 00 with SAP S/4HANA 1610 and SAP BusinessObjects AC 10.1 or a later version, then use the latest 12.2.1.*x* version of this connector.

  Deploy the connector using the **Applications** option from the **Manage** tab of Oracle Identity Self Service console.

- If you are using Oracle Identity Manager release 11.1.2.*x*, as listed in the “Requirement for CI-Based Connector” column of Table 1-1, then use the 11.1.*x* version of the SAP User Management connector. If you want to use the 12.2.1.*x* version of this connector with Oracle Identity Manager release 11.1.2.*x*, then you can install and use the it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0. If you are using the latest 12.2.1.*x* version of the SAP UM connector in the CI-based mode, then see *Oracle Identity Manager Connector Guide for SAP User Management*, Release 11.1.1 for complete details on connector deployment, usage, and customization.

Based on various flavors of SAP S/4 HANA, Oracle recommends the following usage:

- SAP S/4HANA On-Premise: The traditional upgraded release of SAP ERP 6.0, to which the customers are mostly migrating, has SAP GUI-based access to the system with access to Fiori launchpad as well. It is a fully customer-controlled environment with respect to administration/support/maintenance. **Recommendation** - use Oracle Identity Governance - SAP User Management Connector. For more information about it, see About the SAP User Management Connector.
- SAP S/4HANA Cloud Private Edition: Everything is similar to SAP S/4HANA On-Premise, but the entire system control/administration/maintenance is with SAP. It is offered under the “Rise with SAP” program only as a Service with SAP GUI access given to the end/business users, who have access to Fiori Launchpad as well. **Recommendation** - use Oracle Identity Governance - SAP User Management Connector. For more information about it, see About the SAP User Management Connector.
- SAP S/4HANA Cloud Public Edition/Essential Edition: Core SaaS offering for S/4HANA, where the instance is provisioned, which has browser-based access only to the end/business users; No SAP GUI access is valid/exposed for this cloud instance. **Recommendation** - use Oracle Identity Governance - SAP S/4 HANA Cloud Connector. For more information about it, see Introduction to the Connector.

1.3 Certified Languages

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- French (Canadian)
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.4 Supported Connector Operations

These are the list of operations that the connector supports for your target system.

Table 1-2 Connector Operations Supported by the SAP UM and SAP AC UM Connectors

Operation	Supported for SAP UM?	Supported for SAP AC UM?
User Management		
Create a user account	Yes	Yes
Update a user account	Yes	Yes
Delete a user account	Yes	Yes
Enable a user account	Yes	Yes
Disable a user account	Yes	Yes
Lock a user account	Yes	Yes
Unlock a user account	Yes	Yes
Reset password	Yes	No
Assign a role to a user account	Yes	Yes
Assign multiple roles to a user account	Yes	Yes
Remove a role from a user account	Yes	Yes
Remove multiple roles from a user account	Yes	Yes
Assign a profile to a user account	Yes	Yes
Assign multiple profiles to a user account	Yes	Yes
Remove a profile from a user account	Yes	Yes
Remove multiple profiles from a user account	Yes	Yes
Assign a group to a user account	Yes	No
Assign multiple Groups to a user account	Yes	No
Remove a group to a user account	Yes	No
Remove multiple groups from a user account	Yes	No
Assign a parameter to a user account	Yes	No
Assign multiple parameters to a user account	Yes	No
Remove a parameter to a user account	Yes	No
Remove multiple parameters from a user account	Yes	No
Entitlements		
Add Role	Yes	Yes
Add Multiple Roles	Yes	Yes

Table 1-2 (Cont.) Connector Operations Supported by the SAP UM and SAP AC UM Connectors

Operation	Supported for SAP UM?	Supported for SAP AC UM?
Remove Role	Yes	Yes
Remove Multiple Roles	Yes	Yes
Add Profile	Yes	Yes
Add Multiple Profiles	Yes	Yes
Remove Profile	Yes	Yes
Remove Multiple Profiles	Yes	Yes

1.5 Connector Architecture

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 Governance as the front end for sending account creation or modification provisioning requests to either SAP ERP or SAP CUA. While creating an application, you can opt for enabling either direct provisioning or request-based provisioning in Oracle Identity Governance. In direct provisioning, only Oracle Identity Governanc 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 Governance.

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

Figure 1-1 shows the connector integrating SAP ERP with Oracle Identity Governance.

Figure 1-1 Connector Integrating SAP ERP with Oracle Identity Governance

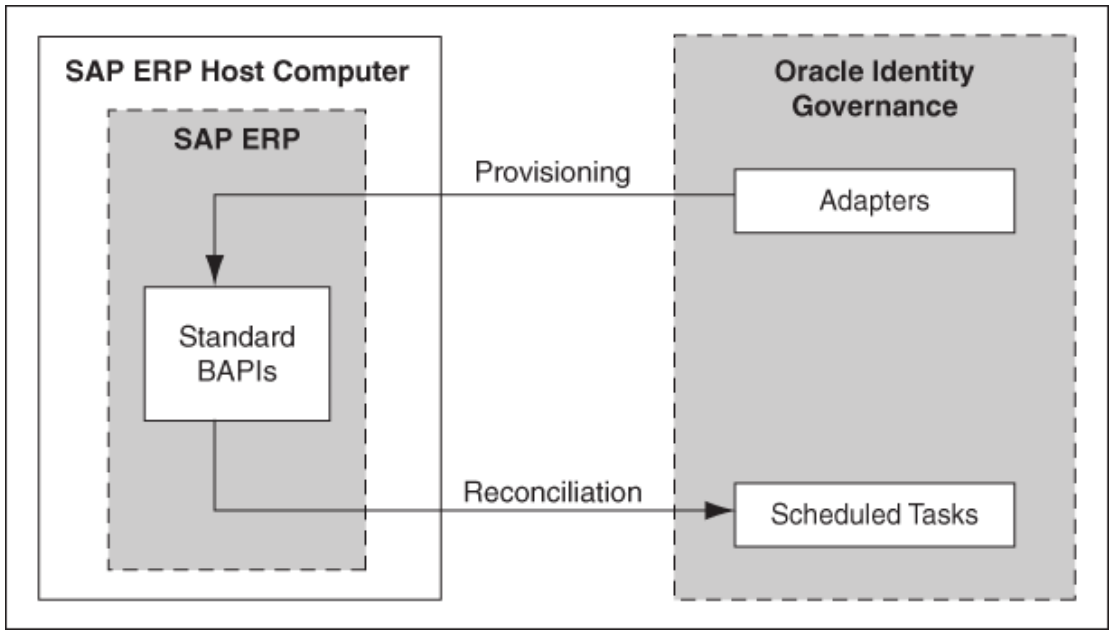
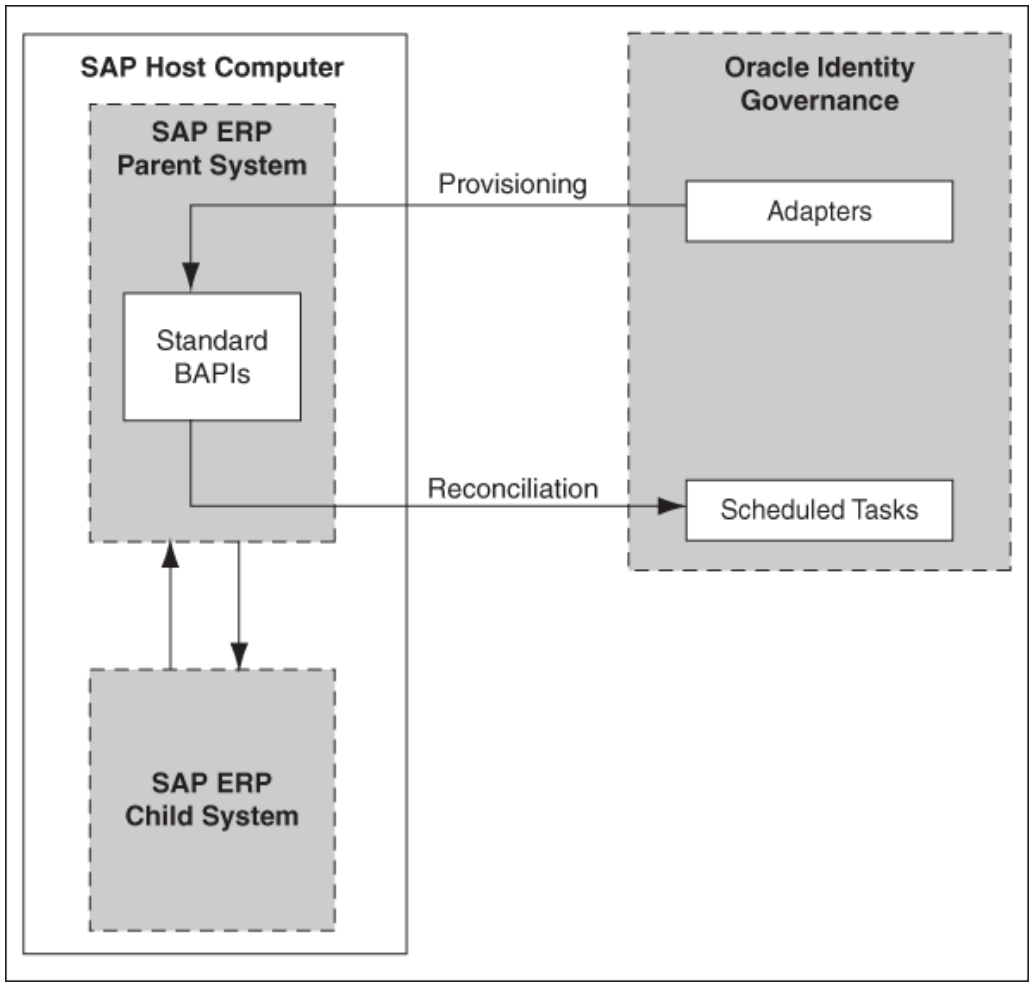


Figure 1-2 shows the connector integrating SAP CUA with Oracle Identity Governance.

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



As shown in these figures, either SAP ERP or SAP CUA is configured as a target resource of Oracle Identity Governance. Through provisioning operations performed on Oracle Identity Governance, 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 Governance 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 Governance and the SAP ERP 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 Governance.

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 Governance.

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 Governance. 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.

1.6 Supported Deployment Configurations

These are the list of supported deployment configurations of the connector.

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

- 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

1.6.1 Basic User Management

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

Figure 1-1 and Figure 1-2show 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 Governance.

1.6.2 User Management with SoD

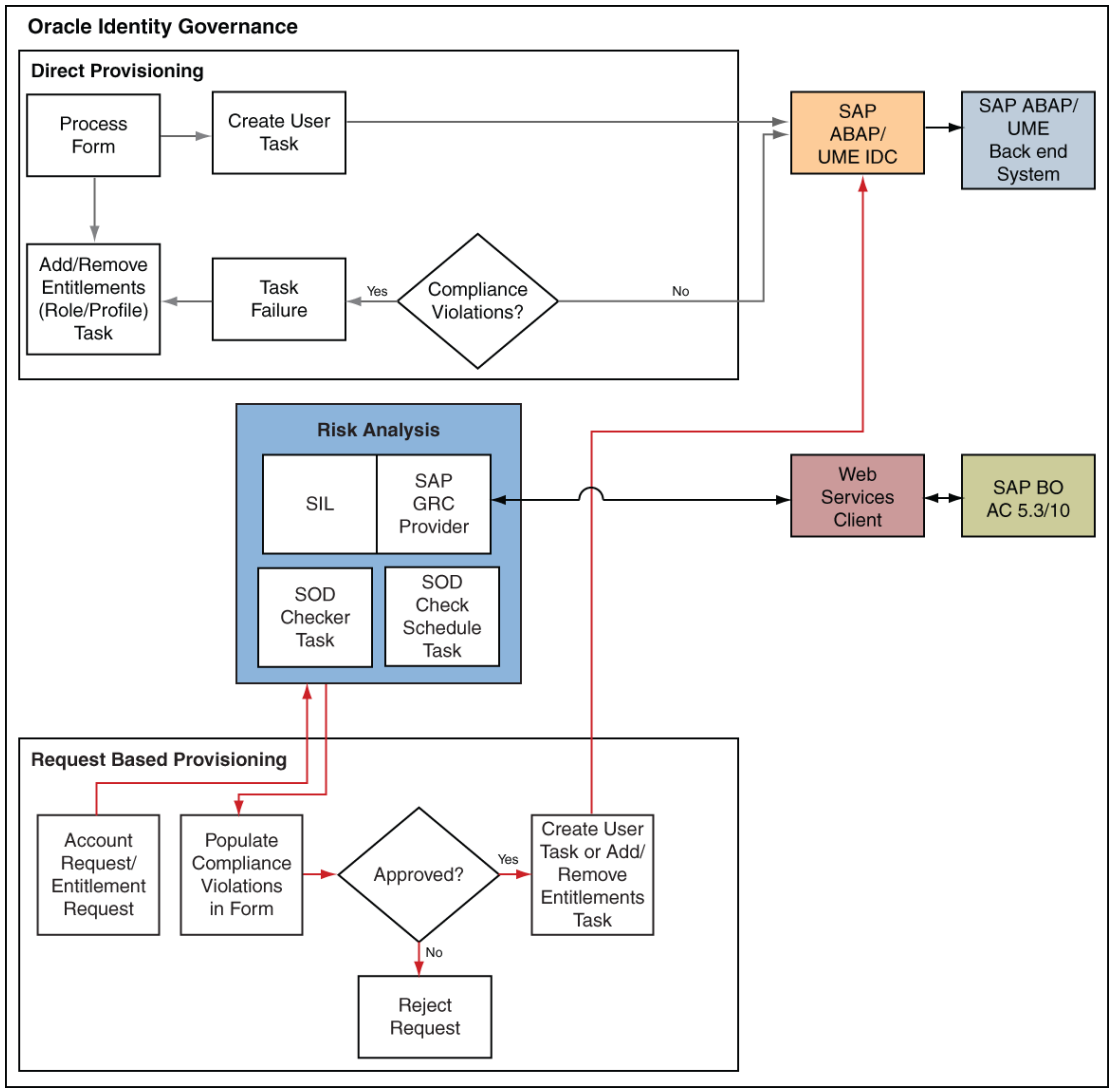
You might have the Access Risk Analysis module of SAP GRC configured to implement segregation of duties (SoD) in your SAP operating environment. In this scenario, the connector can be used as the interface between Oracle Identity Governance and the SoD module. You can configure the connector so that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

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

In this guide, the phrase **configuring SoD** is used to mean configuring the integration between Oracle Identity Governance and SAP GRC 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 Developer's Guide for Oracle Identity Manager* 11g Release 2 (11.1.2.2) 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 Governance sends this request to the SoD engine (SAP GRC 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 Governance.
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 Governance 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 Governance.

Summary of the account management process:

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

1.6.3 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}
```

1.6.4 User Management with Access Request Management

Access Request Management is a module in the SAP GRC 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.

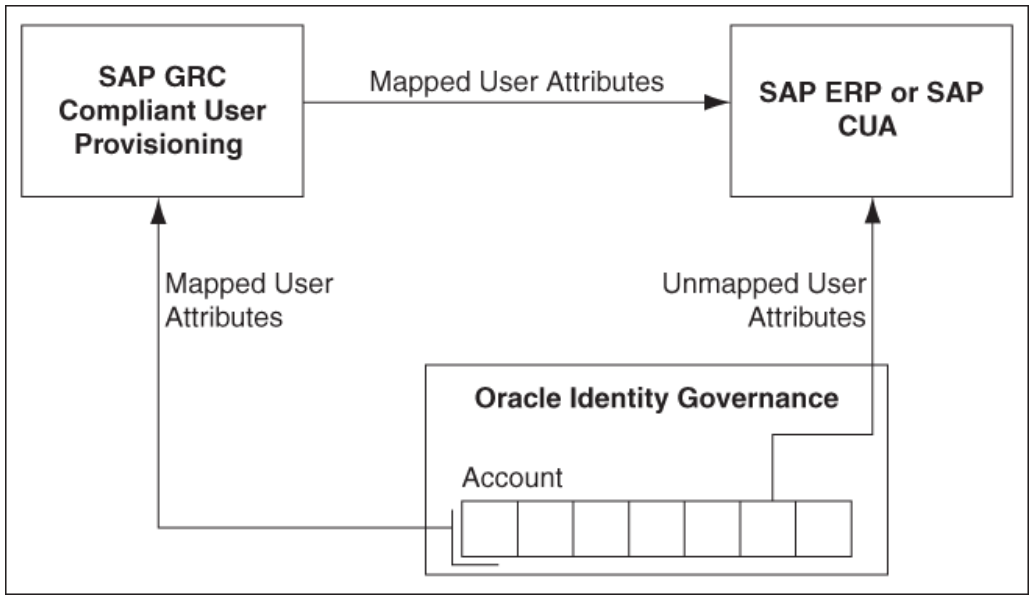
> **Note:**
>
> In this guide, (for the SAP UM AC Connector that uses the SAPUM-AC-Connector-CI.xml file) the phrase **configuring Access Request Management** has been used to mean configuring the integration between Oracle Identity Governance and SAP GRC Access Request Management.
>
> This connector 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 GRC Access Request Management. Scheduled tasks on Oracle Identity Governance fetch data from the target system to Oracle Identity Governance.

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

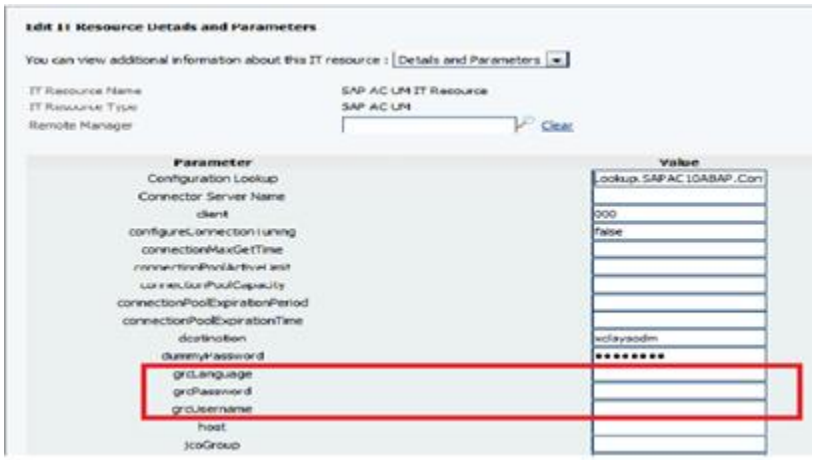
Figure 1-4 Connector Integrating SAP GRC Access Request Management with Oracle Identity Governance and the Target System



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



2. The connector sends requests and receives responses through the following Web services of SAP GRC:
   - SAPGRC_AC_IDM_SUBMITREQUEST: This Web service is used to submit requests.
   - SAPGRC_AC_IDM_REQUESTSTATUS: This Web service is used to fetch request statuses.

- SAPGRC_AC_IDM_AUDITTRAIL: This Web service is used to check if there are error messages in the SAP GRC 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 GRC 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 GRC Access Request Management.

3. When the request is created on SAP GRC Access Request Management, data sent back by Access Request Management is stored in the following read-only fields in Oracle Identity Governance:
   - AC Request ID: This field holds the request ID that is generated on SAP GRC 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 GRC 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 GRC 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 GRC 10. Then, a message is recorded in the Oracle Identity Governance logs.
   - If Access Request Management rejects the provisioning request, then the status of the request is set to Failed in case of SAP GRC 10. Then, a message is recorded in the Oracle Identity Governance 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 GRC Access Request Management.

2. The workflow defined in SAP GRC Access Request Management sends the request to the SAP GRC 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.

1.6.5 User Management with Both SoD and Access Request Management

You might have both SAP GRC 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 GRC Access Request Management is configured to send provisioning requests to GRC Access Risk Analysis for SoD validation, then you must not configure the SoD feature of the connector.

1.6.6 Guidelines on Using a Deployment Configuration

These are the guidelines that you must apply while using any of the supported deployment configurations.

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

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

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

1.6.6.1 User Management with SoD and Access Request Management

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

- Configure both SoD and Access Request Management features of the connector.
- On SAP GRC 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 Governance but rejected on SAP GRC Access Request Management, then the role or profile is revoked from Oracle Identity Governance at the end of the next user reconciliation run. Therefore, you can have approval workflows defined for role and profile provisioning requests on SAP GRC Access Request Management.

1.6.6.2 User Management with Access Request Management

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

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

- On SAP GRC 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.

1.6.7 Considerations to Be Addressed When You Enable Access Request Management

These are the considerations you must keep in mind when you enable the Access Request Management feature of the connector.

- Multiple requests are generated from Oracle Identity Governance 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 Governance 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 Governance keeps track of data related to the last operation only.
- A Modify User operation can involve changes to multiple process form fields or child form fields. For each field that is modified, one request is created and sent to SAP GRC Access Request Management. Only information about the last request sent to Access Request Management is stored in Oracle Identity Governance.
- 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 ERP 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 GRC 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.

1.6.8 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 Governance 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 Governance and the Target System for more information.

  If you are using SAP GRC as the target system, then you must enable SSL between Oracle Identity Governance and SAP GRC. See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for the instructions.
- Password management

For accounts created through Oracle Identity Governance, 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 Governance is set as the new password on the target system.

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

1.7 Supported Connector Features Matrix

Provides the list of features supported by the AOB application and CI-based connector.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application	CI-Based Application
Support for SAP GRC Version 10	Yes	Yes
Support for Connector Server	Yes	Yes
Support for Standard and Custom Single-Valued Attributes for Reconciliation and Provisioning	Yes	Yes
SoD Validation of Entitlement Requests	Yes	Yes
Routing of Provisioning Requests Through SAP GRC Access Request Management	Yes	Yes
Full and Incremental Reconciliation	Yes	Yes
Limited (Filtered) Reconciliation	Yes	Yes
Batched Reconciliation	Yes	Yes
Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts	Yes	Yes
SNC Communication Between the Target System and Oracle Identity Governance	Yes	Yes
Configuring Password Changes for Newly Created Accounts	Yes	Yes
Specifying a SAP JCo Trace Level	Yes	Yes
Connection Pooling	Yes	Yes
Specifying the Use of a Logon Group on the Target System for Connector Operations	Yes	Yes
Transformation and Validation of Account Data	Yes	Yes
Support for Resource Exclusion Lists	Yes	Yes
Support for Both Unicode and Non-Unicode Modes	Yes	Yes

1.8 Connector Features

The features of the connector include support for connector server, full reconciliation, incremental reconciliation, limited reconciliation, reconciliation of updates to account data, and so on.

The following are the features of the connector:

- Support for SAP Governance, Risk, and Compliance Version 10 or Later
- Support for the Connector Server
- Support for Standard and Custom Single-Valued Attributes for Reconciliation and Provisioning
- SoD Validation of Entitlement Requests
- Routing of Provisioning Requests Through SAP GRC Access Request Management
- Full and Incremental Reconciliation
- Limited (Filtered) Reconciliation
- Batched Reconciliation
- Enabled and Disabled Accounts
- Linking of SAP HRMS and SAP ERP or SAP CUA Accounts
- SNC Communication Between the Target System and Oracle Identity Governance
- 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

1.8.1 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.

1.8.2 Support for the Connector Server

Connector Server is one of the features provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles.

A Java connector server is useful when you do not wish to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements.

For information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server, see Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

1.8.3 SoD Validation of Entitlement Requests

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

The connector supports the SoD feature in Oracle Identity Governance and the following updates have been made in this feature:

- The SoD Invocation Library (SIL) is bundled with Oracle Identity Governance. The SIL acts as a pluggable integration interface with any SoD engine.
- The SAP User Management connector can be configured to work with SAP GRC as the SoD engine. To enable this, changes have been made in the approval and provisioning workflows of the connector.
- The SoD engine processes role and profile entitlement requests that are sent through the connector. This preventive simulation approach helps identify and correct potentially conflicting assignment of entitlements to a user, before the requested entitlements are granted to users.

See Also:

Configuring SoD (Segregation of Duties) in this guide.

Note:

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

1.8.4 Support for Standard and Custom Single-Valued Attributes for Reconciliation and Provisioning

The connector provides a default set of attribute mappings for provisioning and reconciliation between Oracle Identity Governance and the target system. If required, you can add new user or group attributes for provisioning and reconciliation.

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 SAP User Management Connector for more information.

1.8.5 Routing of Provisioning Requests Through SAP GRC Access Request Management

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

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

1.8.6 Full and Incremental Reconciliation

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

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 Performing Full and Incremental Reconciliation for more information.

1.8.7 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 Performing Limited Reconciliation for more information.

1.8.8 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 Performing Batched Reconciliation for more information.

1.8.9 Enabled and Disabled 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 Governance 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.

1.8.10 Linking of SAP HRMS and SAP ERP or SAP CUA Accounts

An SAP HRMS account created for an individual can be linked with the SAP ERP 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 ERP or SAP CUA account.

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

- validatePERNR
- overwriteLink

See Linking of SAP HRMS and SAP ERP or SAP CUA Accounts for more information.

1.8.11 SNC Communication Between the Target System and Oracle Identity Governance

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

See Configuring SNC to Secure Communication Between Oracle Identity Governance and the Target System for more information.

1.8.12 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 Governance, password management can be configured by using the **changePasswordAtNextLogon** parameter of the Configuration Lookup. If you are using the AOB implementation, see the **Advanced Configuration** 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 IT Resource. If you are using the AOB implementation, see 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.

1.8.13 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.

1.8.14 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target system. Oracle Identity Governance 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 set of basic configuration parameters that you provide while creating an application. For example, if you have three applications for three installations of the target system, then three connection pools are created, one for each target system installation. For more information about the parameters that you can configure for connection pooling, see Table 3-3.

1.8.15 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.

1.8.16 Transformation and Validation of Account Data

You can configure transformation and validation of account data that is brought into or sent from Oracle Identity Governance during reconciliation and provisioning operations by writing Groovy scripts while creating your application.

For more information, see Validation and Transformation of Provisioning and Reconciliation Attributes in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.8.17 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.

1.8.18 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.

2

Creating an Application By Using the SAP User Management Connector

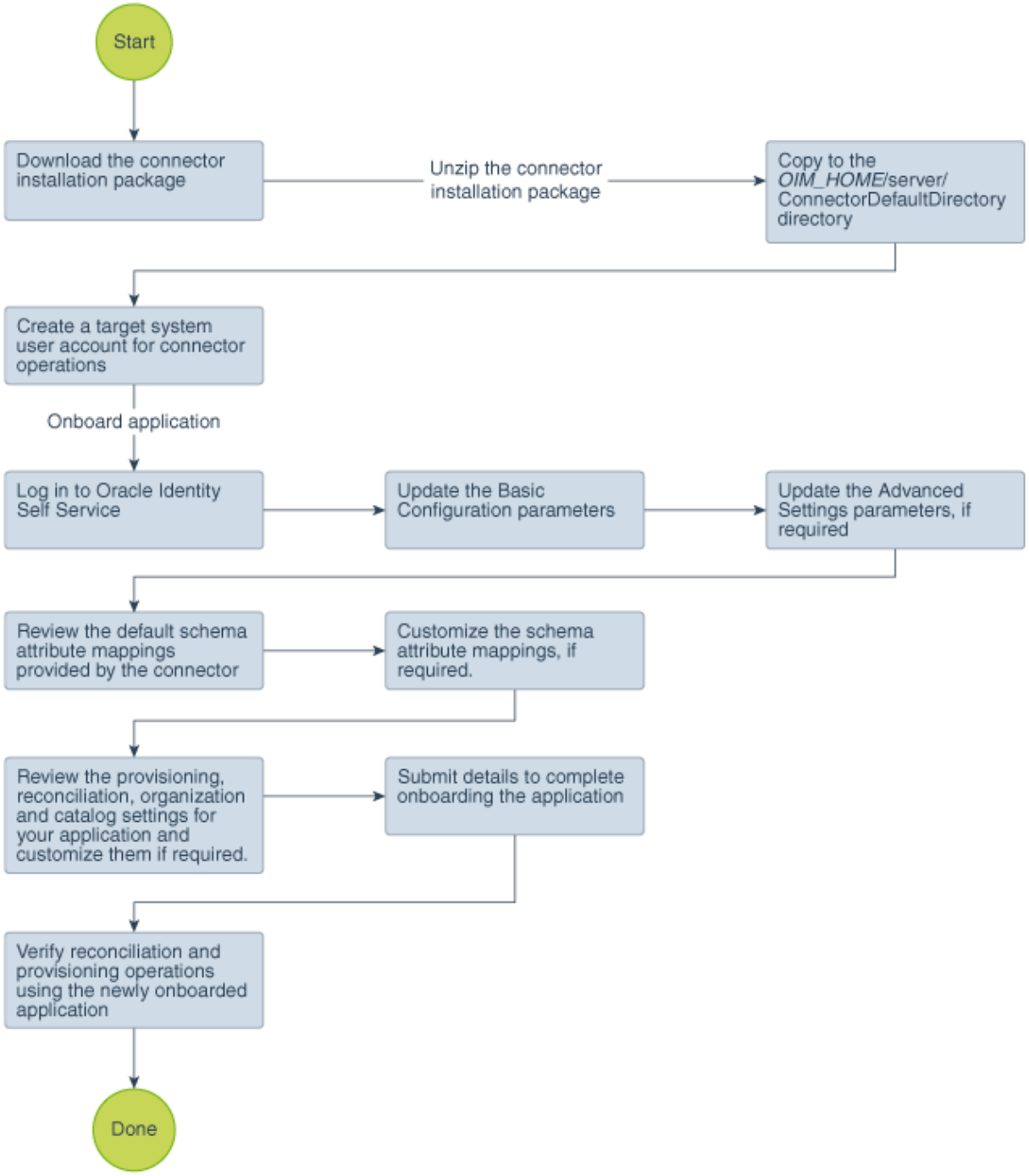
Learn about onboarding applications using the connector and the prerequisites for doing so.

2.1 Process Flow for Creating an Application By Using the Connector

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Identity Self Service.

Figure 2-1 is a flowchart depicting high-level steps for creating an application in Oracle Identity Governance by using the connector installation package.

Figure 2-1 Overall Flow of the Process for Creating an Application By Using the Connector



2.2 Prerequisites for Creating an Application by Using the Connector

Learn about the tasks that you must complete before you create the application.

- Downloading the Connector Installation Package
- Downloading and Installing the SAP JCo
- Creating a Target System User Account for Connector Operations
- Assigning Roles to a User Account in a SAP GRC System for Connector Operations

2.2.1 Downloading the Connector Installation Package

You can obtain the installation package for your connector on the Oracle Technology Network (OTN) website.

To download the connector installation package:

1. Navigate to the OTN website at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html.
2. Click **OTN License Agreement** and read the license agreement.
3. Select the **Accept License Agreement** option.

   You must accept the license agreement before you can download the installation package.
4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER*.
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

2.2.2 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 and save the SAP JCo release file from the SAP website.
2. Extract the contents of the file that you download.
3. Copy the **sapjco3.jar** file into the *OIG_HOME*/server/ThirdParty directory. Then, add its path to the *DOMAIN_HOME*\bin\startWebLogic file as follows:

   > **Note:**
   >
   > In an OIG cluster, copy the sapjco3.jar file to each node of the cluster and set the CLASSPATH.

   - 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\idm\server\ThirdParty\sapjco3.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:

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

     For example, `CLASSPATH=/home/oracle/12cPS3/Middleware/idm/server/ThirdParty/sapjco3.jar:"${SAVE_CLASSPATH}"`

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

4. Copy the RFC files into the required directory on the Oracle Identity Governance 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.

5. On a Microsoft Windows platform, ensure that the msvcr80.dll and msvcp80.dll files are in the c:\WINDOWS\system32 directory. If required, both files can be downloaded from various sources on the Internet.
6. Restart the server for the changes in the environment variable to take effect.

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

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

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

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

2.2.3 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

2.2.3.1 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: *

2.2.3.2 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.

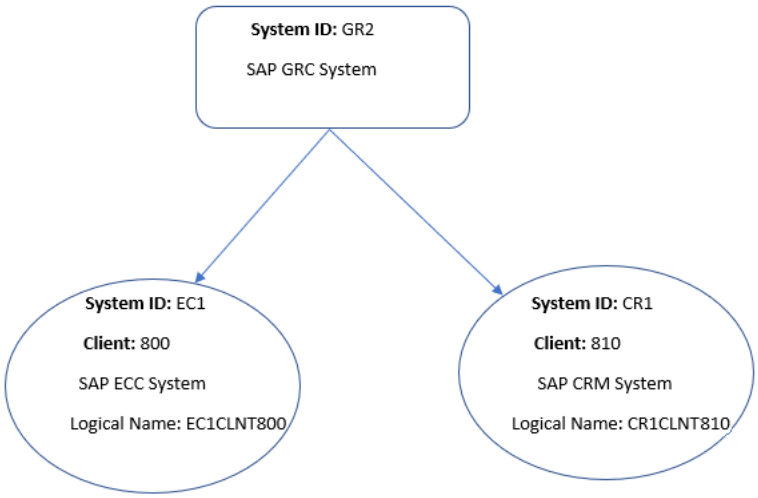
2.2.4 Assigning Roles to a User Account in a SAP GRC System for Connector Operations

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

> **Note:**
>
> The naming convention of the connector name created in SAP GRC 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 GRC, 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 2-2 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 GRC system, then assign the following minimum set of roles to a user account in SAP GRC:

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: *

2.3 Creating an Application By Using the Connector

You can onboard an application into Oracle Identity Governance from the connector package by creating a Target application. To do so, you must log in to Identity Self Service and then choose the **Applications** box on the **Manage** tab.

The following is the high-level procedure to create an application by using the connector:

> **Note:**
>
> For detailed information on each of the steps in this procedure, see Creating Applications of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1. Create an application in Identity Self Service. The high-level steps are as follows:
   a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.
   b. Ensure that the **Connector Package** option is selected when creating an application.
   c. Update the basic configuration parameters to include connectivity-related information.
   d. If required, update the advanced setting parameters to update configuration entries related to connector operations.

e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.

f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.

g. Review the details of the application and click **Finish** to submit the application details.

   The application is created in Oracle Identity Governance.

h. When you are prompted whether you want to create a default request form, click **Yes** or **No**.

   If you click **Yes**, then the default form is automatically created and is attached with the newly created application. The default form is created with the same name as the application. The default form cannot be modified later. Therefore, if you want to customize it, click **No** to manually create a new form and attach it with your application.

2. Verify reconciliation and provisioning operations on the newly created application.

See Also:

- Configuring the SAP User Management Connector for details on basic configuration and advanced settings parameters, default user account attribute mappings, default correlation rules, and reconciliation jobs that are predefined for this connector
- Configuring Oracle Identity Governance for details on creating a new form and associating it with your application, if you chose not to create the default form

3
Configuring the SAP User Management Connector

While creating a target application, you must configure connection-related parameters that the connector uses to connect Oracle Identity Governance with your target system and perform connector operations. In addition, you can view and edit attribute mappings between the process form fields in Oracle Identity Governance and target system columns, predefined correlation rules, situations and responses, and reconciliation jobs.

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to the target applications.

The following tables list basic configuration parameters of the SAP UM and SAP AC UM connectors.

Table 3-1 Parameters in the Basic Configuration Section for the SAP UM Connector and the SAP UM Connector with SoD

Parameters	Mandatory?	Description
Connector Server Name	No	If you created an IT resource of the type `Connector Server`, then enter its name.
TopologyName	No	Name of the topology of the target system host computer.
client	Yes	SAP client setting Default value: `000`
configureConnectionTuning	No	Allows the connection properties to be customized when the SAP Destination is configured. Default value: `false`
connectionMaxGetTime	No	Maximum time to wait for a connection (specified in milliseconds). Default value: `None`
connectionPoolActiveLimit	No	Maximum number of active connections that can be created for a destination simultaneously. Default value: `None`

Table 3-1 (Cont.) Parameters in the Basic Configuration Section for the SAP UM Connector and the SAP UM Connector with SoD

Parameters	Mandatory?	Description
connectionPoolCapacity	No	Maximum number of idle connections that can be kept open by the destination. Default value: `None`
connectionPoolExpirationPeriod	No	Enter an integer value which specifies the number of milliseconds after which the connections that have been released have expired. See Table 3-3 for more information. Default value: `None`
connnectionPoolExpirationTime	No	Enter an integer value which specifies the number of milliseconds after which the connections that have been freed can be closed. See Table 3-3 for more information. Default value: `None`
destination	Yes	Enter a unique value that the SAPJCo library uses to interact with the SAP system. Sample value: `dest or dest123` (any random value)
dummyPassword	No	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.
host	Yes	Enter the host name of the target system.
jcoGroup	No	Group of SAP application servers. It is one of the parameters used for enabling the use of a logon group.
jcoSAPRouter	No	SAP router string to be used for a system protected by a firewall Default value: `None`
jcoTrace	No	Absolute path to the directory where the trace files will be created Default value: `0`
jcoTraceDir	No	Level of SAP JCO tracing to enable. Enter `0` or any positive integer up to and including 10 Default value: `None`
language	Yes	Enter the two-letter code for the language set on the target system. Default value: `EN`
loadBalance	No	Enter `TRUE` to enable the use of Logon Group. Default value: `false`

Table 3-1 (Cont.) Parameters in the Basic Configuration Section for the SAP UM Connector and the SAP UM Connector with SoD

Parameters	Mandatory?	Description
masterSystem	Yes	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	No	Maximum number of retries for BAPI execution. Default value: `5`
msHost	No	Enter the host name of the message server. Default value: `None`
msServ	No	SAP message server port to be used instead of the default sapms Default value: `None`
password	Yes	When using normal authentication, password of the User account.
r3Name	No	Enter the host name of the SAP ERP or SAP CUA system
retryWaitTime	No	Enter a value in milliseconds within which the connection to the target system is retried after a connection failure. Default value: `500`
sncLib	No	Enter the full path and name of the crypto library on the target system host computer. This is required only if SNC is enabled. • For Windows: `c://usr//sap/sapcrypto.dll` • For Linux: `sncLib: //home/oracle/sec/sapcrypto.so`
sncName	No	Enter a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Governance. Sample value: `p:CN=TST,OU=SAP, O=ORA,c=IN`
sncPartnerName	No	Enter the domain name of the target system host computer. Enter a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Governance. Sample value: `p:CN=I47,OU=SAP, O=ORA, c=IN`

Table 3-1 (Cont.) Parameters in the Basic Configuration Section for the SAP UM Connector and the SAP UM Connector with SoD

Parameters	Mandatory?	Description
sncProtectionLevel	No	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 **Note:** Enter a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Governance. Default value: `3`
sncX509Cert	No	The X509 certificate that does not contain the BEGIN CERTIFICATE or END CERTIFICATE strings when using SNC
systemNumber	Yes	SAP system number Default value: `00`
useSNC	No	Enter `true`, if you want to configure secure communication between Oracle Identity Governance and the target system. Otherwise, enter `false`. Default value: `false`
user	Yes	Enter a user name that has permissions to create accounts in target.

Table 3-2 Parameters in the Basic Configuration Section for the SAP AC UM Connector

Parameters	Mandatory?	Description
Connector Server Name	No	If you created an IT resource of the type `Connector Server`, then enter its name.
TopologyName	No	Name of the topology of the target system host computer.
client	Yes	SAP client setting Default value: `000`
configureConnectionTuning	No	Allows the connection properties to be customized when the SAP Destination is configured. Default value: `false`
connectionMaxGetTime	No	Maximum time to wait for a connection (specified in milliseconds). Default value: `None`
connectionPoolActiveLimit	No	Maximum number of active connections that can be created for a destination simultaneously. Default value: `None`

Table 3-2 (Cont.) Parameters in the Basic Configuration Section for the SAP AC UM Connector

Parameters	Mandatory?	Description
connectionPoolCapacity	No	Maximum number of idle connections that can be kept open by the destination. Default value: `None`
connectionPoolExpirationPeriod	No	Enter an integer value which specifies the number of milliseconds after which the connections that have been released have expired. See Table 3-3 for more information. Default value: `None`
connnectionPoolExpirationTime	No	Enter an integer value which specifies the number of milliseconds after which the connections that have been freed can be closed. See Table 3-3 for more information. Default value: `None`
destination	Yes	Enter a unique value that the SAPJCo library uses to interact with the SAP system. Sample value: `dest or dest123` (any random value)
dummyPassword	No	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.
host	Yes	Enter the host name of the target system.
jcoGroup	No	Group of SAP application servers. It is one of the parameters used for enabling the use of a logon group.
jcoSAPRouter	No	SAP router string to be used for a system protected by a firewall Default value: `None`
jcoTrace	No	Absolute path to the directory where the trace files will be created Default value: `0`
jcoTraceDir	No	Level of SAP JCO tracing to enable. Enter `0` or any positive integer up to and including 10 Default value: `None`
language	Yes	Enter the two-letter code for the language set on the target system. Default value: `EN`
loadBalance	No	Enter `TRUE` to enable the use of Logon Group. Default value: `false`

Table 3-2 (Cont.) Parameters in the Basic Configuration Section for the SAP AC UM Connector

Parameters	Mandatory?	Description
masterSystem	Yes	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	No	Maximum number of retries for BAPI execution. Default value: `5`
msHost	No	Enter the host name of the message server. Default value: `None`
msServ	No	SAP message server port to be used instead of the default sapms Default value: `None`
password	Yes	When using normal authentication, password of the User account.
r3Name	No	Enter the host name of the SAP ERP or SAP CUA system
retryWaitTime	No	Enter a value in milliseconds within which the connection to the target system is retried after a connection failure. Default value: `500`
sncLib	No	Enter the full path and name of the crypto library on the target system host computer. This is required only if SNC is enabled. • For Windows: `c://usr//sap/sapcrypto.dll` • For Linux: `sncLib: //home/oracle/sec/sapcrypto.so`
sncName	No	Enter a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Governance. Sample value: `p:CN=TST,OU=SAP, O=ORA,c=IN`
sncPartnerName	No	Enter the domain name of the target system host computer. Enter a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Governance. Sample value: `p:CN=I47,OU=SAP, O=ORA, c=IN`

Table 3-2 (Cont.) Parameters in the Basic Configuration Section for the SAP AC UM Connector

Parameters	Mandatory?	Description
sncProtectionLevel	No	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 **Note:** Enter a value for this parameter only if you enable SNC communication between the target system and Oracle Identity Governance. Default value: `3`
sncX509Cert	No	The X509 certificate that does not contain the BEGIN CERTIFICATE or END CERTIFICATE strings when using SNC
systemNumber	Yes	SAP system number Default value: `00`
useSNC	No	Enter `true`, if you want to configure secure communication between Oracle Identity Governance and the target system. Otherwise, enter `false`. Default value: `false`
user	Yes	Enter a user name that has permissions to create accounts in target.
grcLanguage	yes	Enter the two-letter code for the language set on the GRC system. Sample value: `EN` **Note:** This is applicable only to the SAP AC UM connector.
grcPassword	Yes	Enter the password of the GRC System. **Note:** This is applicable only to the SAP AC UM connector.
grcUsername	Yes	Enter the user name of the GRC System. **Note:** This is applicable only to the SAP AC UM connector.

3.2 Advanced Settings Parameters

These are the configuration-related entries that the connector uses during reconciliation and provisioning operations.

The following table lists the advanced settings parameters for the SAP UM connector.

Table 3-3 Advanced Settings Parameters for the SAP UM Connector and the SAP UM Connector with SoD

Parameter	Mandatory?	Description
aliasUser	No	Enter the logon on user alias depending on the target system. Default value: `none`
batchSize	No	Enter the number of records in each batch that must be fetched from the target system during a reconciliation run. Default value: `100`
Bundle Name	No	Name of the connector bundle package. Default value: `org.identityconnectors.sap`
Bundle Version	No	Version of the connector bundle class. Default value: `12.3.0`
changePasswordAtNext Logon	No	For accounts created through Oracle Identity Governance, password management can be configured by using the changePasswordAtNextLogon entry. Enter `yes` if you want to configure the password.
codePage	No	This entry holds the initial code page in SAP notation. Default value: `none`
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	No	Name of the connector class. Default value: `org.identityconnectors.sap.SAPConnector`
cuaChildInitialPassword ChangeFuncModule	No	Name of the Remote Enabled function module that changes the initial password for a user on all CUA child systems. This parameter 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* this entry. Default value: `ZXLCBAPI_ZXLCUSR_PW_CHANGE`

Table 3-3 (Cont.) Advanced Settings Parameters for the SAP UM Connector and the SAP UM Connector with SoD

Parameter	Mandatory?	Description
cuaChildPasswordChangeFuncModue	No	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. Default value: `ZXLCBAPI_ZXLCUSR_PASSWORDCHNGE`
disableLockStatus	No	Enter a lock status of a user in SAP system. Default value: `64`
enableCUA	No	Enter `yes` if the target system is SAP CUA. Otherwise, enter `no`.
gatewayHost	No	This entry holds the name or IP address of the gateway host. Default value: `None`
gatewayService	No	This entry holds the name of the gateway service. Default value: `None`
getSSO2	No	Get or do not get a SSO ticket after logon. The value of this entry can be `1` or `0`.
groups	No	This field is an embedded object that is defined in the attribute mapping. In the default entry, GROUPS is a table name and USERGROUP is a field name on the target system. Default value: `GROUPS~USERGROUP`
ICheck	No	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	No	Specifies the SAP Cookie Version 2 that must be used as a logon ticket.
parameters	No	This field is an embedded object that is defined in the attribute mapping. In the default entry, PARAMETER1 is a table name, and PARID and PARVA are the field names on the target system. Default value: `PARAMETER1~PARID;PARVA`
overwriteLink	No	Enter `Yes` as the value if you want existing links in SAP to be overwritten by the ones set up through provisioning operations.
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`

Table 3-3 (Cont.) Advanced Settings Parameters for the SAP UM Connector and the SAP UM Connector with SoD

Parameter	Mandatory?	Description
profiles	No	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. Default value: `PROFILES~SUBSYSTEM;PROFILE`
ProfileAttributeLabel	No	This field holds the label name of the profile name field in the child form. Sample value: `Profile Name`
Profile attribute name	No	This field holds a list of field names for the Profile duty type. The values of this list are separated by a semicolon (;). Sample value: `PROFILE_NAME`
Profile form names	No	This field holds a list of all profile child form names used during direct and request-based provisioning. Sample value: `PROFILE`
reconcilefuturedatedroles	No	Enter `yes` if you want to reconcile future-dated roles. Otherwise, enter `no`.
reconcilepastdatedroles	No	Enter `yes` if you want to reconcile past-dated roles. Otherwise, enter `no`.
repositoryDestination	No	Specifies the destination to be used as repository. Default value: `None`
repositoryPassword	No	Specifies the password for a repository user. This entry is mandatory if a repository user is used Default value: `None`
repositorySNCMode	No	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 parameter to `0`
repositoryUser	No	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. Default value: `None`
RoleAttributeLabel	No	This entry holds the label name of the role name field in the child form. Sample value: `Role Name`
Role attribute name	No	This field holds a list of field names for the Role duty type. The values of this list are separated by a semicolon (;). Sample value: `ROLE_NAME`

Table 3-3 (Cont.) Advanced Settings Parameters for the SAP UM Connector and the SAP UM Connector with SoD

Parameter	Mandatory?	Description
Role form names	No	This field holds a list of all role child form names used during direct and request-based provisioning. Sample value: `USERROLE`
sapSystemTimeZone	No	This entry holds the SAP target system time zone. Default value: `PST`
singleRoles	No	Enter `yes` if you want to fetch single roles from target. Otherwise enter `no`.
tpHost	No	This entry holds the host name of the external server program. Default value: `None`
tpName	No	This entry holds the program ID of the tp server program Default value: `None`
type	No	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`
validatePERNR	No	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`.
wsdlFilePath	No	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.
roles	No	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. Default value: `ACTIVITYGROUPS~SUBSYSTEM;AGR_NAME;TO_DAT;FROM_DAT;ORG_FLAG`

Table 3-3 (Cont.) Advanced Settings Parameters for the SAP UM Connector and the SAP UM Connector with SoD

Parameter	Mandatory?	Description
Pool Max Idle	No	Maximum number of idle objects in a pool. Default value: `10`
Pool Max Size	No	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	No	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	No	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `150000`
Pool Min Idle	No	Minimum number of idle objects in a pool. Default value: `1`
entitlementRiskAnalysis AccessURl	No	This entry holds the URL for Entitlement Risk Analysis web service. **Note:** This parameter is applicable only for SAP UM with SoD.
entitlementRiskAnalysis WS	No	Web service client class to do the risk analysis in SAP BusinessobjectAC. Default value: `oracle.iam.grc.sod.scomp.impl.grcsap.util.webservice.sap.ac10.RiskAnalysisWithoutNo` **Note:** This parameter is applicable only for SAP UM with SoD.
ReportFormat	No	**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.

The following table lists the advanced settings parameters for the SAP AC UM connector.

Table 3-4 Advanced Settings Parameters for the SAP AC UM Connector

Parameter	Mandatory?	Description
aliasUSer	No	Enter the logon on user alias depending on the target system. Default value: `None`
appLookupAccessURL	No	URL for Application Lookup web service. Default value: `None`

Table 3-4 (Cont.) Advanced Settings Parameters for the SAP AC UM Connector

Parameter	Mandatory?	Description
appLookupWS	No	Web service client class to get all applications configured in SAP GRC. Default value: `oracle.iam.ws.sap.ac10.SelectApplication`
assignRoleReqType	No	This entry holds the name of the request type that is used for assign role request in SAP GRC. 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. Default value: `002~Change Account~002~006`
auditLogsAccessURL	No	URL for Audit Logs web service. Default value: `None`
auditLogsWS	No	Web service client class to get audit logs. Default value: `oracle.iam.ws.sap.ac10.AuditLogs`
batchSize	No	Enter the number of records in each batch that must be fetched from the target system during a reconciliation run. Default value: `100`
Bundle Name	No	Name of the connector bundle package. Default value: `org.identityconnectors.sapacum`
Bundle Version	No	Version of the connector bundle class. Default value: `12.3.0`
changePasswordAtNextLogon	No	For accounts created through Oracle Identity Governance, password management can be configured by using the changePasswordAtNextLogon entry. Enter `yes` if you want to configure the password.
codePage	No	This entry holds the initial code page in SAP notation. Default value: `none`
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."

Table 3-4 (Cont.) Advanced Settings Parameters for the SAP AC UM Connector

Parameter	Mandatory?	Description
Connector Name	No	Name of the connector class. Default value: `org.identityconnectors.sap.SAPConnector`
createUserReqType	No	Name of the request type that the connector must use for the create user request in SAP GRC. 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. Default value: `001~New Account~001`
UserReqType	No	Name of the request type to use for modifying user request in SAP GRC. Default value: `002~Change Account~002`
cuaChildInitialPasswordChangeFuncModule	No	Name of the Remote Enabled function module that changes the initial password for a user on all CUA child systems. This parameter 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* this entry. Default value: `ZXLCBAPI_ZXLCUSR_PW_CHANGE`
cuaChildPasswordChangeFuncModue	No	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. Default value: `ZXLCBAPI_ZXLCUSR_PASSWORDCHNGE`
deleteUserReqType	No	Name of the request type that the connector must use for the delete user request in SAPGRC. Default value: `003~Delete user~003`
disableLockStatus	No	Enter a lock status of a user in SAP system. Default value: `64`
enableCUA	No	Enter `yes` if the target system is SAP CUA. Otherwise, enter `no`.

Table 3-4 (Cont.) Advanced Settings Parameters for the SAP AC UM Connector

Parameter	Mandatory?	Description
gatewayHost	No	This entry holds the name or IP address of the gateway host. Default value: `None`
gatewayService	No	This entry holds the name of the gateway service. Default value: `None`
getSSO2	No	Get or do not get a SSO ticket after logon. The value of this entry can be `1` or `0`.
ignoreOpenStatus	No	Specify whether new requests can be sent for a particular user, even if the last request for the user is in the Open status. Default value: `Yes`
ICheck	No	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	No	Name of the request type to use for lock user request in SAP GRC. Default value: `004~Lock user~004`
logAuditTrial	No	Specify whether complete audit trial needs to be logged whenever status request web service is invoked. Default value: `Yes`
mySAPSSO2	No	Specifies the SAP Cookie Version 2 that must be used as a logon ticket. Default value: `none`
otherLookupAccessURL	No	URL for Other Lookup web service areas such as Business Process, Functional Area, and so on. Default value: `none`
otherLookupWS	No	Web service client class to get other lookup fields such as Business Process, Functional Area, and so on. Default value: `oracle.iam.ws.sap.ac10.SearchLookup`
overwriteLink	No	Enter `Yes` as the value if you want existing links in SAP to be overwritten by the ones set up through provisioning operations.
provActionAttrName	No	Name of the attribute in the target system that contains the details required for performing provisioning operations to a specific backend system. Default value: `provAction;ReqLineItem` **Note:** Do *not* this value.

Table 3-4 (Cont.) Advanced Settings Parameters for the SAP AC UM Connector

Parameter	Mandatory?	Description
provItemActionAttrName	No	Name of the attribute in the target system that contains the details required for performing provisioning roles. Default value: `provItemAction;ReqLineItem` **Note:** Do *not* this value.
reconcilefuturedatedroles	No	Enter `yes` if you want to reconcile future-dated roles. Otherwise, enter `no`.
reconcilepastdatedroles	No	Enter `yes` if you want to reconcile past-dated roles. Otherwise, enter `no`.
removeRoleReqType	No	Name of the request type to use for remove user request in SAP GRC. Default value: `002~Change Account~002~009`
repositoryDestination	No	Specifies the destination to be used as repository. Default value: `None`
repositoryPassword	No	Specifies the password for a repository user. This entry is mandatory if a repository user is used Default value: `None`
repositorySNCMode	No	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 parameter to `0`
repositoryUser	No	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. Default value: `None`
requestStatusAccessURL	No	URL for Status Request web service. Default value: `None`
requeststatusvalue	No	The value that gets updated in the AC Request Status field on the process form. Default value: `OK`
requestStatusWS	No	Web service client class to get status of provisioning request. Default value: `oracle.iam.ws.sap.ac10.RequestStatus`
requestTypeAttrName	No	Name of the request type attribute used to differentiate request flows from the SAPUMCREATE adapter. Default value: `Reqtype;Header`

Table 3-4 (Cont.) Advanced Settings Parameters for the SAP AC UM Connector

Parameter	Mandatory?	Description
riskLevel	No	In SAP GRC, each business risk is assigned a criticality level. You can control the risk analysis data returned by SAP GRC by specifying a risk level. Default value: `3`
roleLookupAccessURL	No	URL for Role Lookup web service. Default value: `None`
roleLookupWS	No	Web service client class to get all roles. Default value: `oracle.iam.ws.sap.ac10.SearchRoles`
sapSystemTimeZone	No	This entry holds the SAP target system time zone. Default value: `PST`
singleRoles	No	Enter `yes` if you want to fetch single roles from target. Otherwise enter `no`.
tpHost	No	This entry holds the host name of the external server program. Default value: `None`
tpName	No	This entry holds the program ID of the tp server program Default value: `None`
type	No	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	No	Name of the request type to use for unlock user request in SAP GRC. Default value: `005~unlock user~005`
userAccessAccessURL	No	URL for User Access web service. Default value: `None`
userAccessWS	No	Web service client class to get status of user access. Default value: `oracle.iam.ws.sap.ac10.UserAccess`

Table 3-4 (Cont.) Advanced Settings Parameters for the SAP AC UM Connector

Parameter	Mandatory?	Description
wsdlFilePath	No	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.
parameters	No	This field is an embedded object that is defined in the attribute mapping. In the default entry, PARAMETER1 is a table name, and PARID and PARVA are the field names on the target system. Default value: `PARAMETER1~PARID;PARVA`
profiles	No	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. Default value: `PROFILES~SUBSYSTEM;PROFILE`
roles	No	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. Default value: `ACTIVITYGROUPS~SUBSYSTEM;AGR_NAME;TO_DAT;FROM_DAT;ORG_FLAG`
groups	No	This field is an embedded object that is defined in the attribute mapping. In the default entry, GROUPS is a table name and USERGROUP is a field name on the target system. Default value: `GROUPS~USERGROUP`

3.3 Attribute Mappings

The attribute mappings on the Schema page vary depending on whether you are using the SAP UM or SAP AC UM connector.

- Attribute Mappings for the SAP UM Connector
- Attribute Mappings for the SAP AC UM Connector

3.3.1 Attribute Mappings for the SAP UM Connector

The Schema page for a target application displays the default schema (provided by the connector) that maps Oracle Identity Governance attributes to target system attributes. The SAP UM connector uses these mappings during reconciliation and provisioning operations.

SAP UM User Account Attributes

Table 3-5 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and the SAP UM attributes. The table also lists whether a specific attribute is used during provisioning or reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

The mapping for the SoD fields in the target attribute is empty because they do not exist in the target system but in the GRC system. When SOD is enabled in OIG, adding any violation or nonviolation entitlement triggers a response from the GRC system and the following SoD fields are updated with their respective values:

- SoDCheckStatus
- SodCheckResult
- SoDCheckEntitlement
- SodCheckTimestamp

Table 3-5 Default Attribute Mappings for SAP UM User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User ID	_NAME_	String	Yes	Yes	Yes	Yes	Yes
Password	_PASSWORD_	String	No	Yes	No	No	No
First Name	FIRSTNAME;ADDRESS;FIRSTNAME;ADDRESSX	String	No	Yes	Yes	No	No

Table 3-5 (Cont.) Default Attribute Mappings for SAP UM User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Last Name	LASTNAME;ADDRESS;LASTNAME;ADDRESSX	String	yes	Yes	Yes	No	No
Title	TITLE_P;ADDRESS;TITLE_P;ADDRESSX	String	No	Yes	Yes	No	No
Alias	USERALIAS;ALIAS;BAPIALIAS;ALIASX	String	No	Yes	Yes	No	No
E Mail	E_MAIL;ADDRESS;E_MAIL;ADDRESSX	String	No	Yes	Yes	No	No
Telephone Number	TEL1_NUMBR;ADDRESS;TEL1_NUMBR;ADDRESSX	String	No	Yes	Yes	No	No
Telephone Extension	TEL1_EXT;ADDRESS;TEL1_EXT;ADDRESSX	String	No	Yes	Yes	No	No
Valid From	GLTGV;LOGONDATA;GLTGV;LOGONDATAX	Date	No	Yes	Yes	No	No
Valid Through	GLTGB;LOGONDATA;GLTGB;LOGONDATAX	String	No	Yes	Yes	No	No
Fax Number	FAX_NUMBER;ADDRESS;FAX_NUMBER;ADDRESSX	Date	No	Yes	Yes	No	No
Fax Extension	FAX_EXTENS;ADDRESS;FAX_EXTENS;ADDRESSX	String	No	Yes	Yes	No	No

Table 3-5 (Cont.) Default Attribute Mappings for SAP UM User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Building	BUILDING_P;ADDRESS;BUILDING_P;ADDRESSX	String	No	Yes	Yes	No	No
Room Number	ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX	String	No	Yes	Yes	No	No
Floor	FLOOR_P;ADDRESS;FLOOR_P;ADDRESSX	String	No	Yes	Yes	No	No
Function	FUNCTION;ADDRESS;FUNCTION;ADDRESSX	String	No	Yes	Yes	No	No
Group Name	CLASS;LOGONDATA;CLASS;LOGONDATAX	String	No	Yes	Yes	No	No
Department	DEPARTMENT;ADDRESS;DEPARTMENT;ADDRESSX	String	No	Yes	Yes	No	No
Accounting Number	ACCNT;LOGONDATA;ACCNT;LOGONDATAX	String	No	Yes	Yes	No	No
Cost Center	KOSTL;DEFAULTS;KOSTL;DEFAULTSX	String	No	No	Yes	No	No
User Lock	__LOCK_OUT__	String	No	Yes	Yes	No	No
Logon language	LANGU;DEFAULTS;LANGU;DEFAULTSX	String	No	Yes	Yes	No	No
User Type	USTYP;LOGONDATA;USTYP;LOGONDATAX	String	No	Yes	Yes	No	No

Table 3-5 (Cont.) Default Attribute Mappings for SAP UM User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Date Format	DATFM;DEFAULTS;DATFM;DEFAULTSX	String	No	Yes	Yes	No	No
Decimal Notation	DCPFM;DEFAULTS;DCPFM;DEFAULTSX	String	No	Yes	Yes	No	No
Time Zone	TZONE;LOGONDATA;TZONE;LOGONDATAX	String	No	Yes	Yes	No	No
Start Menu	START_MENU;DEFAULTS;START_MENU;DEFAULTSX	String	No	Yes	Yes	No	No
Company	COMPANY;COMPANY;COMPANY;COMPANYX	String	No	Yes	Yes	No	No
Contractual User	LIC_TYPE;UCLASS;UCLASS;UCLASSX	String	No	Yes	Yes	No	No
Communication Type	COMM_TYPE;ADDRESS;COMM_TYPE;ADDRESSX	String	No	Yes	Yes	No	No
Language Comm	LANGU_P;ADDRESS;LANGU_P;ADDRESSX	String	No	Yes	Yes	No	No
unique ID	_UID_	String	No	Yes	Yes	No	No
Personnel Number	PERNR	String	No	Yes	No	No	No
SoDCheck Status	NA	String	No	No	No	No	No
SodCheck Result	NA	String	No	No	No	No	No
SoDCheck Entitlement	NA	String	No	No	No	No	No
SodCheck Timestamp	NA	String	No	No	No	No	No

Table 3-5 (Cont.) Default Attribute Mappings for SAP UM User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Status	_ENABLE_	String	No	No	Yes	No	No

Figure 3-1 shows the default User account attribute mappings.

Figure 3-1 Default Attribute Mappings for SAP UM User Account

Group Attributes

Table 3-6 lists the group-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP UM attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

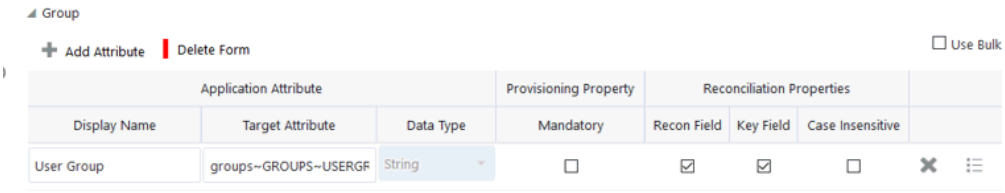
If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-6 Default Attribute Mappings for Groups

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
User Group	groups~GROUPS~USERGROUP	String	No	Yes	Yes	No

Figure 3-2 shows default attribute mappings for groups.

Figure 3-2 Default Attribute Mappings for Groups



Parameter Attributes

Table 3-7 lists the parameter-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP UM attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

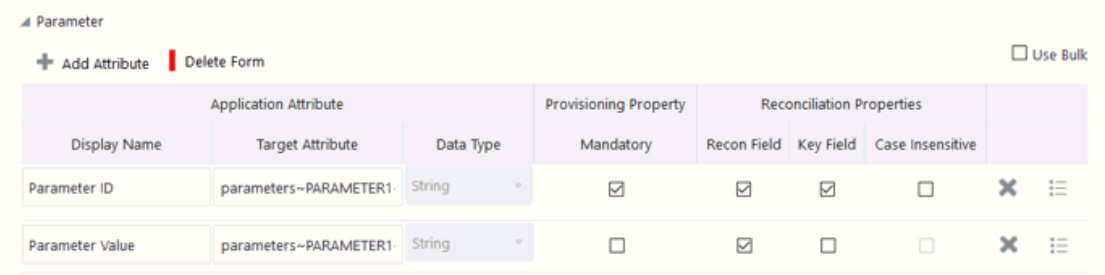
If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-7 Default Attribute Mappings for Parameters

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Parameter Id	parameters~PARAMETER1~PARID	String	Yes	Yes	Yes	No
Parameter Value	parameters~PARAMETER1~PARVA	String	No	Yes	No	No

Figure 3-3 shows default attribute mappings for parameters.

Figure 3-3 Default Attribute Mappings for Parameters



Role Entitlement Attributes

Table 3-8 lists the role-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP UM attributes. The table lists whether a given role is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-8 Default Attribute Mappings for Role Entitlement

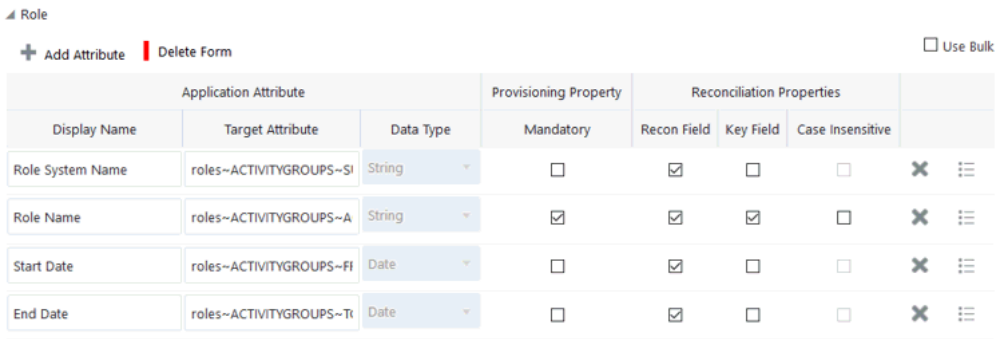
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Role System Name	roles~ACTIVITYGROUPS~SUBSYSTEM	String	No	Yes	No	No
Role Name	roles~ACTIVITYGROUPS~AGR_NAME	String	Yes	Yes	Yes	No

Table 3-8 (Cont.) Default Attribute Mappings for Role Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Start Date	roles~ACTIVITYGROUPS~FROM_DAT	String	No	Yes	No	No
End Date	roles~ACTIVITYGROUPS~TO_DAT	String	No	Yes	No	No

Figure 3-4 shows the role entitlement mappings.

Figure 3-4 Default Attribute Mappings for Role Entitlement



Profile Entitlement Attributes

Table 3-9 lists the profile-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP UM attributes. The table lists whether a given profile is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-9 Default Attribute Mappings for Profile Entitlement

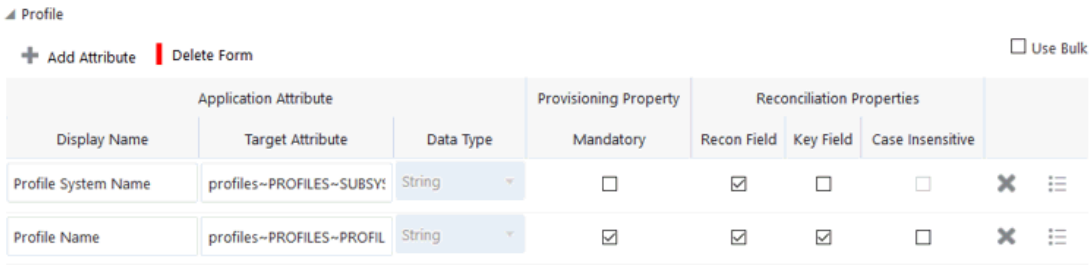
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Profile System Name	profiles~PROFILES~SUBSYSTEM	String	No	Yes	No	No

Table 3-9 (Cont.) Default Attribute Mappings for Profile Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Profile Name	profiles~PROFILES~PROFILE	String	Yes	Yes	Yes	No

Figure 3-5 shows the profile entitlement mappings.

Figure 3-5 Default Attribute Mappings for Profile Entitlement



3.3.2 Attribute Mappings for the SAP AC UM Connector

The Schema page for an SAP AC UM target application displays the default schema (provided by the connector) that maps Oracle Identity Governance attributes to target system attributes. The connector uses these mappings during reconciliation and provisioning operations.

SAP AC UM User Account Attributes

Table 3-5 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP AC UM attributes. The table also lists whether a specific attribute is used during provisioning or reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-10 Default Attribute Mappings for the SAP AC UM User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User ID	_NAME_	String	Yes	Yes	Yes	Yes	Yes
Password	_PASSWORD_	String	No	Yes	No	No	No

Table 3-10 (Cont.) Default Attribute Mappings for the SAP AC UM User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
First Name	fname;UserInfo	String	No	Yes	Yes	No	No
Last Name	lname;UserInfo	String	No	Yes	Yes	No	No
Title	title;UserInfo	String	No	Yes	Yes	No	No
Alias	alias;UserInfo	String	No	Yes	Yes	No	No
E Mail	email;UserInfo	String	No	Yes	Yes	No	No
Telephone Number	telnumber;UserInfo	String	No	Yes	Yes	No	No
Telephone Extension	TEL1_EXT;ADDRESS;TEL1_EXT;ADDRESSX	String	No	Yes	Yes	No	No
Valid From	validFrom;UserInfo	Date	No	Yes	Yes	No	No
Valid Through	validTo;UserInfo	String	No	Yes	Yes	No	No
Fax Number	fax;UserInfo	Date	No	Yes	Yes	No	No
Fax Extension	FAX_EXTENS;ADDRESS;FAX_EXTENS;ADDRESSX	String	No	Yes	Yes	No	No
Building	BUILDING_P;ADDRESS	String	No	Yes	Yes	No	No
Room Number	ROOM_NO_P;ADDRESS	String	No	Yes	Yes	No	No
Floor	FLOOR_P;ADDRESS;FLOOR_P;ADDRESSX	String	No	Yes	Yes	No	No
Function	FUNCTION;ADDRESS	String	No	Yes	Yes	No	No
Group Name	CLASS;LOGONDATA	String	No	Yes	Yes	No	No
Department	DEPARTMENT;ADDRESS	String	No	Yes	Yes	No	No
Accounting Number	accno;UserInfo	String	No	Yes	Yes	No	No

Table 3-10 (Cont.) Default Attribute Mappings for the SAP AC UM User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Cost Center	costcenter; UserInfo	String	No	Yes	Yes	No	No
User Lock	userLock;None	String	No	Yes	Yes	No	No
Logon Language	logonlang; UserInfo	String	No	Yes	Yes	No	No
user Type	userType;UserInfo	String	No	Yes	Yes	No	No
Date Format	dateFormat;UserInfo	String	No	Yes	Yes	No	No
Decimal Notation	decNotation;UserInfo	String	No	Yes	Yes	No	No
Time Zone	TZONE;LOGONDATA	String	No	Yes	Yes	No	No
Start menu	startmenu; UserInfo	String	No	Yes	Yes	No	No
Company	COMPANY; COMPANY	String	No	Yes	Yes	No	No
Contractual User Type (Lookup)	LIC_TYPE; UCLASS|UCLASSSYS	String	No	Yes	Yes	No	No
Communication Type (Lookup)	COMM_TYPE;ADDRESS	String	No	Yes	Yes	No	No
Language Communication (Lookup)	LANGU_P; ADDRESS	String	No	Yes	Yes	No	No
Unique ID	_UID_	String	No	Yes	Yes	No	No
Personnel Number	PERNR	String	No	Yes	No	No	No
AC Request Id	RequestId	String	No	Yes	No	No	No
AC Request Status	RequestStatus	String	No	Yes	No	No	No
AC Request Type	RequestType	String	No	Yes	No	No	No
AC Manager	manager;UserInfo	String	No	Yes	No	No	No
AC Manager email	managerEmail;UserInfo	String	No	Yes	No	No	No

Table 3-10 (Cont.) Default Attribute Mappings for the SAP AC UM User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
AC Manager First Name	managerFirstname;UserInfo	String	No	Yes	No	No	No
AC Manager Last Name	managerLastname;UserInfo	String	No	Yes	No	No	No
AC Priority	priority;Header	String	No	Yes	No	No	No
AC Request Reason	requestReason;Header	String	No	Yes	No	No	No
AC Request Due Date(Date)	reqDueDate;Header	String	No	Yes	No	No	No
AC Functional Area (Lookup)	funcarea;Header	String	No	Yes	No	No	No
AC Business Process (Lookup)	bproc;Header	String	No	Yes	No	No	No
AC Requestor ID	requestorId;Header	String	No	Yes	No	No	No
AC Requestor email	email;Header	String	No	Yes	No	No	No

Figure 3-6 shows the default User account attribute mappings.

Figure 3-6 Default Attribute Mappings for SAP AC UM User Account

Group Attributes

Table 3-6 lists the group-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP AC UM attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

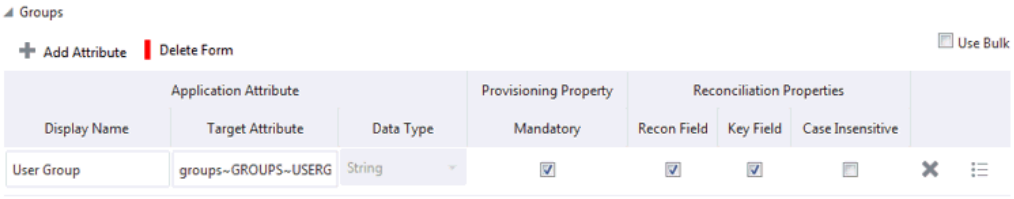
If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-11 Default Attribute Mapping for Groups

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
User Group	groups~GROUPS~USERGROUP	String	Yes	Yes	Yes	No

Figure 3-7 shows the group entitlement mappings.

Figure 3-7 Default Attribute Mapping for Groups



Parameter Entitlements

Table 3-7 lists the parameter-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP AC UM attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

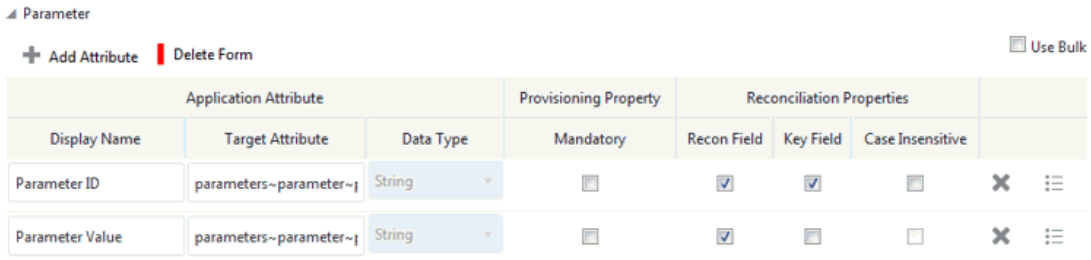
If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-12 Default Attribute Mappings for Parameters

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Parameter Id	parameters~PARAMETER1~PARID	String	No	Yes	Yes	No
Parameter Value	parameters~PARAMETER1~PARVA	String	No	Yes	No	No

Figure 3-8 shows the role entitlement mappings.

Figure 3-8 Default Attribute Mappings for Parameters



Profile Attributes

Table 3-9 lists the profile-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP AC UM attributes. The table lists whether a given profile is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

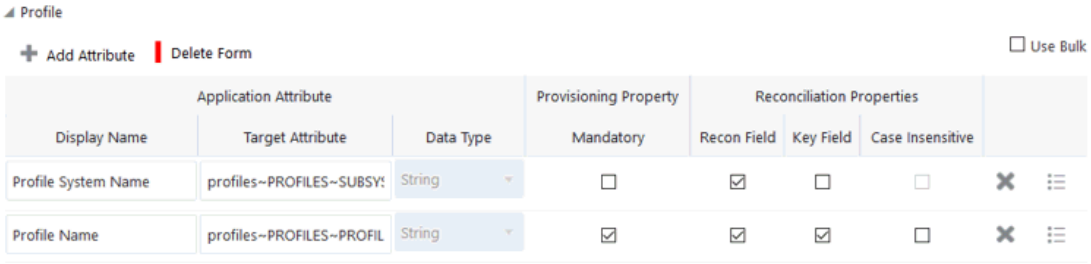
If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-13 Default Attribute Mappings for Profiles

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Profile System Name	profiles~PROFILES~SUBSYSTEM	String	No	Yes	No	No
Profile Name	profiles~PROFILES~PROFILE	String	Yes	Yes	Yes	No

Figure 3-9 shows the profile entitlement mappings.

Figure 3-9 Default Attribute Mappings for Profiles



Role Attributes

Table 3-8 lists the role-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP AC UM attributes. The table lists whether a given role is

mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

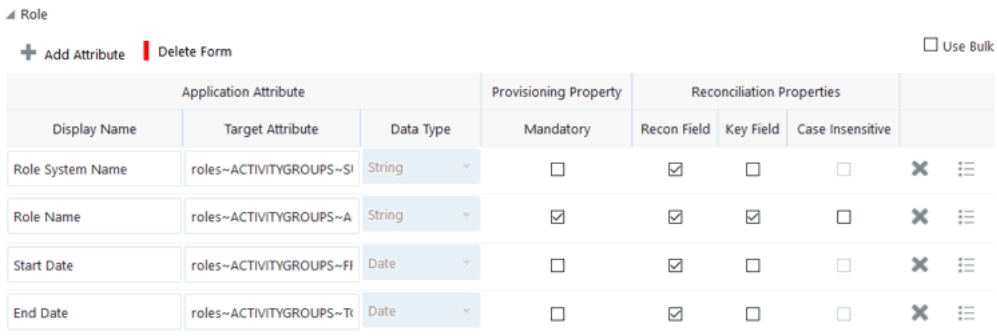
If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-14 Default Attribute Mappings for Roles

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Role System Name	roles~ACTIVITYGROUPS~SUBSYSTEM	String	No	Yes	No	No
Role Name	roles~ACTIVITYGROUPS~AGR_NAME	String	Yes	Yes	Yes	No
Start Date	roles~ACTIVITYGROUPS~FROM_DAT	Date	No	Yes	No	No
End Date	roles~ACTIVITYGROUPS~TO_DAT	Date	No	Yes	No	No

Figure 3-10 shows the role entitlement mappings.

Figure 3-10 Default Attribute Mappings for Roles



3.4 Rules, Situations, and Responses for the Connector

Learn about the predefined rules, responses and situations for target and authoritative applications. The connector use these rules and responses for performing reconciliation.

Predefined Identity Correlation Rules

By default, the SAP UM and SAP AC UM connectors provide a simple correlation rule when you create a Target application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the target system repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

Table 3-15 lists the default simple correlation rule for the SAP UM and SAP AC UM connectors. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-15 Predefined Identity Correlation Rule for the SAP UM and SAP AC UM Connectors

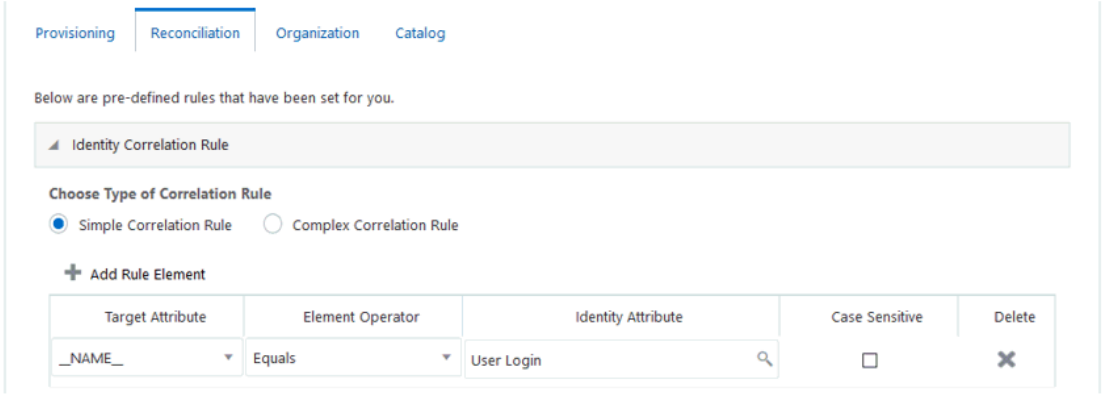
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

In this identity rule:

- __NAME__ is a single-valued attribute on the target system that identifies the user account.
- User Login is the field on the OIG User form.

Figure 3-11 shows the simple correlation rule for the SAP UM and SAP AC UM Connectors.

Figure 3-11 Simple Correlation Rule for the SAP UM and SAP AC UM Connectors



Predefined Situations and Responses

The SAP UM and SAP AC UM connectors provide a default set of situations and responses when you create a Target application. These situations and responses specify the action that Oracle Identity Governance must take based on the result of a reconciliation event.

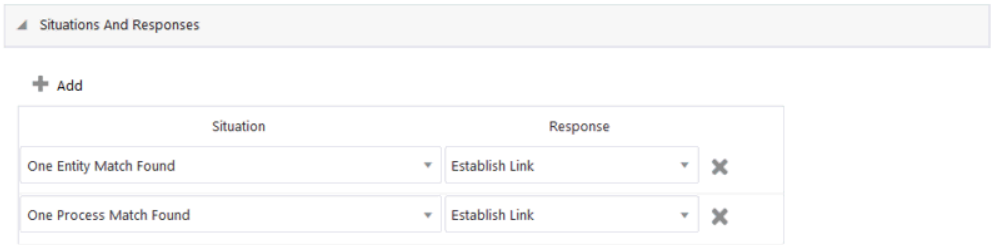
Table 3-16 lists the default situations and responses for the SAP UM and SAP AC UM connectors. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-16 Predefined Situations and Responses for the SAP UM and SAP AC UM Connectors

Situation	Response
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Figure 3-12 shows the situations and responses that the connector provides by default.

Figure 3-12 Predefined Situations and Responses for the SAP UM and SAP AC UM Connectors



3.5 Reconciliation Jobs

These are the reconciliation jobs that are automatically created in Oracle Identity Governance after you create the application for your target system.

- Reconciliation Jobs for the SAP UM Connector
- Reconciliation Jobs for the SAP AC UM Connector

3.5.1 Reconciliation Jobs for the SAP UM Connector

These are the reconciliation jobs that are automatically created in Oracle Identity Governance after you create the application for your target system.

You can either use these predefined jobs or edit them to meet your requirements. Alternatively, you can create custom reconciliation jobs. For information about editing

these predefined jobs or creating new ones, see Updating Reconciliation Jobs in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

> **Note:**
>
> All of the jobs are prefixed with an application name when you create an application. For example, SAPUM SAPUM UM CommType Lookup Reconciliation where the first SAPUM is the application name.

Full User Reconciliation Job

The SAP UM Target User Reconciliation job is used to fetch all user records from the target system.

Table 3-17 Parameters of the SAP UM Target User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Filter	Enter the expression for filtering records that the scheduled job must reconcile. Sample value: `equalTo('__UID__','SEPT12USER1')` Default value: `None` For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Developing and Customizing Applications for Oracle Identity Governance*.
Incremental Recon Attribute	Time stamp at which the last reconciliation run started Default value: `Last Updated` **Note:** Do *not* enter a value for this attribute. The reconciliation engine automatically enters a value for this attribute.
Object Type	Type of object you want to reconcile. Default value: `User`
Latest Token	This attribute holds the time stamp (in *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. **Note:** The reconciliation engine automatically enters a value in this attribute. Sample value: `20120417123006`
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: `SAP UM User Recon`

Incremental User Reconciliation Job

The SAP UM Target Incremental User Reconciliation job is used to fetch the records that are added or modified after the last reconciliation run.

Table 3-18 Parameters of the SAP UM Target Incremental User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Sync Token	Enter the expression for filtering records that the scheduled job must reconcile. Sample value: `equalTo('__UID__','SEPT12USER1')` For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Developing and Customizing Applications for Oracle Identity Governance*.
Object Type	Type of object you want to reconcile. Default value: `User`
Scheduled Task Name	Name of the scheduled task used for reconciliation. **Note:** For the scheduled job included with this connector, you must not change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute.

Delete User Reconciliation Job

The SAP UM Target User Delete Reconciliation job is used to reconcile user data when for target application.

Table 3-19 Parameters of the SAP UM Target User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Object Type	Type of object you want to reconcile. Default value: `User`
Disable User	Enter `yes` if you want the connector to disable accounts (in Oracle Identity Governance) corresponding to accounts deleted on the target system. Enter `no` if you want the connector to revoke accounts in Oracle Identity Governance. Default value: `User`

Table 3-19 (Cont.) Parameters of the SAP UM Target User Delete Reconciliation Job

Parameter	Description
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: `no`
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.

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 connector:

- SAPUM UM CommType Lookup Reconciliation
- SAPUM UM Company Lookup Reconciliation
- SAPUM UM ContractUserType Lookup Reconciliation
- SAPUM UM DateFormat Lookup Reconciliation
- SAPUM UM DecimalNot Lookup Reconciliation
- SAPUM UM LangComm Lookup Reconciliation
- SAPUM UM Parameter Lookup Reconciliation
- SAPUM UM Profile Lookup Reconciliation
- SAPUM UM Role Lookup Reconciliation
- SAPUM UM Systems Lookup Reconciliation
- SAPUM UM TimeZoneLookup Reconciliation
- SAPUM UM Title Lookup Reconciliation
- SAPUM UM UserGroup Lookup Reconciliation
- SAPUM UM UserType Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-20 Parameters of SAP UM Reconciliation Jobs

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Lookup Name	This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched. Depending on the reconciliation job you are using, the default values are as follows: • For SAPUM UM CommType Lookup Reconciliation: `Lookup.SAPABAP.CommType` • For SAPUM UM Company Lookup Reconciliation: `Lookup.SAPABAP.Company` • For SAPUM UM ContractUserType Lookup Reconciliation: `Lookup.SAPABAP.ContractualUserType` • For SAPUM UM DateFormat Lookup Reconciliation: `Lookup.SAPABAP.DateFormat` • For SAPUM UM DecimalNot Lookup Reconciliation: `Lookup.SAPABAP.DecimalNotation` • For SAPUM UM LangComm Lookup Reconciliation: `Lookup.SAPABAP.LangComm` • For SAPUM UM Parameter Lookup Reconciliation: `Lookup.SAPABAP.Parameter` • For SAPUM UM Profile Lookup Reconciliation: `Lookup.SAPABAP.Profile` • For SAPUM UM Role Lookup Reconciliation: `Lookup.SAPABAP.Role` • For SAPUM UM Systems Lookup Reconciliation: `Lookup.SAPABAP:Systems` • For SAPUM UM TimeZoneLookup Reconciliation: `Lookup.SAPABAP.TimeZone` • For SAPUM UM Title Lookup Reconciliation: `Lookup.SAPABAP.Title` • For SAPUM UM UserGroup Lookup Reconciliation: `Lookup.SAPABAP.UserGroup` • For SAPUM UM UserType Lookup Reconciliation: `Lookup.SAPABAP.userType`

Table 3-20 (Cont.) Parameters of SAP UM Reconciliation Jobs

Parameter	Description
Object Type	Enter the type of object whose values must be synchronized. Depending on the scheduled job you are using, the default values are as follows: • For SAPUM UM CommType Lookup Reconciliation: `commtype` • For SAPUM UM Company Lookup Reconciliation: `company` • For SAPUM UM ContractUserType Lookup Reconciliation: `contractualusertype` • For SAPUM UM DateFormat Lookup Reconciliation: `dateformat` • For SAPUM UM DecimalNot Lookup Reconciliation: `decimalnotation` • For SAPUM UM LangComm Lookup Reconciliation: `languagecommunication` • For SAPUM UM Parameter Lookup Reconciliation: `parameters` • For SAPUM UM Profiles Lookup Reconciliation: `profiles` • For SAPUM UM Role Lookup Reconciliation: `activitygroups` • For SAPUM UM Systems Lookup Reconciliation: `cuasystems` • For SAPUM UM TimeZone Lookup Reconciliation: `timezones` • For SAPUM UM Title Lookup Reconciliation: `title` • For SAPUM UM UserGroup Lookup Reconciliation: `GROUP` • For SAPUM UM UserType Lookup Reconciliation: `usertype`

Table 3-20 (Cont.) Parameters of SAP UM Reconciliation Jobs

Parameter	Description
Code Key Attribute	Enter the 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 SAPUM UM CommType Lookup Reconciliation: `COMMTYPE` • For SAPUM UM Company Lookup Reconciliation: `COMPANY` • For SAPUM UM ContractUserType Lookup Reconciliation: `USERTYP` • For SAPUM UM DateFormat Lookup Reconciliation: `_LOW` • For SAPUM UM DecimalNot Lookup Reconciliation: `_LOW` • For SAPUM UM LangComm Lookup Reconciliation: `SPRAS` • For SAPUM UM Parameter Lookup Reconciliation: `PARAMID` • For SAPUM UM Profiles Lookup Reconciliation: `SUBSYSTEM` • For SAPUM UM Role Lookup Reconciliation: `SUBSYSTEM` • For SAPUM UM Systems Lookup Reconciliation: `RCVSYSTEM` • For SAPUM UM TimeZone Lookup Reconciliation: `TZONE` • For SAPUM UM Title Lookup Reconciliation: `TITLE_MEDI` • For SAPUM UM UserGroup Lookup Reconciliation: `USERGROUP` • For SAPUM UM UserType Lookup Reconciliation: `_LOW`

Table 3-20 (Cont.) Parameters of SAP UM Reconciliation Jobs

Parameter	Description
Decode Attribute	Enter the 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 SAPUM UM CommType Lookup Reconciliation: `COMMTYPE` • For SAPUM UM Company Lookup Reconciliation: `COMPANY` • For SAPUM UM ContractUserType Lookup Reconciliation: `UTYPTEXT` • For SAPUM UM DateFormat Lookup Reconciliation: `_TEXT` • For SAPUM UM DecimalNot Lookup Reconciliation: `_TEXT` • For SAPUM UM LangComm Lookup Reconciliation: `SPTXT` • For SAPUM UM Parameter Lookup Reconciliation: `PARTEXT` • For SAPUM UM Profiles Lookup Reconciliation: `USRSYSPRF` • For SAPUM UM Role Lookup Reconciliation: `USRSYSACT` • For SAPUM UM Systems Lookup Reconciliation: `RCVSYSTEM` • For SAPUM UM TimeZone Lookup Reconciliation: `DESCRIPT` • For SAPUM UM Title Lookup Reconciliation: `TITLE_MEDI` • For SAPUM UM UserGroup Lookup Reconciliation: `TEXT` • For SAPUM UM UserType Lookup Reconciliation: `_TEXT`

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.

3.5.2 Reconciliation Jobs for the SAP AC UM Connector

These are the reconciliation jobs that are automatically created in Oracle Identity Governance after you create the application for your target system.

You can either use these predefined jobs or edit them to meet your requirements. Alternatively, you can create custom reconciliation jobs. For information about editing these predefined jobs or creating new ones, see Updating Reconciliation Jobs in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

> **Note:**
>
> All of the jobs are prefixed with an application name when you create an application. For example, SAPACUMAPP SAP AC UM BusinessProcess Lookup Reconciliation where SAPACUMAPP is the application name.

Full User Reconciliation Job

The SAP AC UM Target User Reconciliation job is used to fetch all user records from the target system.

Table 3-21 Parameters of the SAP AC UM Target User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Filter	Enter the expression for filtering records that the scheduled job must reconcile. Sample value: `equalTo('__UID__','SEPT12USER1')` Default value: `None` For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Developing and Customizing Applications for Oracle Identity Governance*.
Object Type	Type of object you want to reconcile. Default value: `User`

Table 3-21 (Cont.) Parameters of the SAP AC UM Target User Reconciliation Job

Parameter	Description
Latest Token	This attribute holds the time stamp (in *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. **Note:** The reconciliation engine automatically enters a value in this attribute. Sample value: `20120417123006`
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: `SAP UM User Recon`
Incremental Recon Attribute	Time stamp at which the last reconciliation run started Default value: `Last Updated` **Note:** Do *not* enter a value for this attribute. The reconciliation engine automatically enters a value for this attribute.

Delete User Reconciliation Job

The SAP AC UM Target User Delete Reconciliation job is used to reconcile user data when for target application.

Table 3-22 Parameters of the SAP AC UM Target User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Object Type	Type of object you want to reconcile. Default value: `User`
Disable User	Enter `yes` if you want the connector to disable accounts (in Oracle Identity Governance) corresponding to accounts deleted on the target system. Enter `no` if you want the connector to revoke accounts in Oracle Identity Governance. Default value: `no`
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: `SAPACUMAPP SAP AC UM User Delete Recon`
Sync Token	Default value is blank. Last modified timestamp of the user account

SAP AC UM Request Status Job

SAP AC UM Request Status Reconciliation job is used to reconcile request status from SAP BusinessObjects AC target system.

Table 3-23 Parameters of the SAP AC UM Request Status Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Object Type	Type of object you want to reconcile. Default value: `Status`
Custom Lookup Name	Name of the lookup definition. Default value: `Lookup.SAPACABAP.Status.ReconAttrMap`
Resource Object Name	Name of the resource object against which reconciliation runs must be performed. Default value: `SAP AC UM Resource Object`
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Default value: `SAP AC UM IT Resource`
Scheduled Task Name	Name of the scheduled task. Default value: `SAP AC UM Request Status`

Note:

To run the SAP AC UM Request Status reconciliation job, you must update Application Name and IT Resource Name parameters based on the name created while configuring the connector.
For example, if the name of the connector is SAPACUM, then ensure to update the Application name as `SAPACUM` and the IT Resource Name as `SAPACUM`.

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 targetsystem by the scheduled jobs for lookup field synchronization, for the SAP AC UM connector:

- 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 Functional Area Lookup Reconciliation
- SAP AC UM ItemProvAction Lookup Reconciliation
- SAP AC UM LangComm Lookup Reconciliation
- SAP AC UM Parameter Lookup Reconciliation
- SAP AC UM DecimalNot 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 TimeZoneLookup Reconciliation
- SAP AC UM Title Lookup Reconciliation
- SAP AC UM UserGroup Lookup Reconciliation
- SAP AC UM UserType Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-24 Parameters of the SAP AC UM Reconciliation Jobs

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.

Table 3-24 (Cont.) Parameters of the SAP AC UM Reconciliation Jobs

Parameter	Description
Code Key Attribute	Enter the 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 AC UM BusinessProcess Lookup Reconciliation: `LCODE` • For SAP AC UM CommType Lookup Reconciliation: `COMM_TYPE` • For SAP AC UM Company Lookup Reconciliation: `COMPANY` • For SAP AC UM ContractUserType Lookup Reconciliation: `USERTYP` • For SAP AC UM DateFormat Lookup Reconciliation: `_LOW` • For SAP AC UM Functional Area Lookup Reconciliation: `LCODE` • For SAP AC UM ItemProvAction Lookup Reconciliation: `LCODE` • For SAP AC UM LangComm Lookup Reconciliation: `SPRAS` • For SAP AC UM Parameter Lookup Reconciliation: `PARAMID` • For SAP AC UM DecimalNot Lookup Reconciliation: `_LOW` • For SAP AC UM Priority Lookup Reconciliation: `LCODE` • For SAP AC UM Profile Lookup Reconciliation: `SUBSYSTEM` • For SAP AC UM ReqInitSystem Lookup Reconciliation: `REQSYSCODE` • For SAP AC UM RequestType Lookup Reconciliation: `LCODE` • For SAP AC UM Role Lookup Reconciliation: `SUBSYSTEM` • For SAP AC UM Systems Lookup Reconciliation: `RCVSYSTEM` • For SAP AC UM TimeZoneLookup Reconciliation: `TZONE` • For SAP AC UM Title Lookup Reconciliation: `TITLE_MEDI` • For SAP AC UM UserGroup Lookup Reconciliation: `USERGROUP` • For SAP AC UM UserType Lookup Reconciliation: `_LOW`

Table 3-24 (Cont.) Parameters of the SAP AC UM Reconciliation Jobs

Parameter	Description
Decode Attribute	Enter the 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 AC UM BusinessProcess Lookup Reconciliation: `LDECODE` • For SAP AC UM CommType Lookup Reconciliation: `COMM_TYPE` • For SAP AC UM Company Lookup Reconciliation: `COMPANY` • For SAP AC UM ContractUserType Lookup Reconciliation: `UTYPTEXT` • For SAP AC UM DateFormat Lookup Reconciliation: `_TEXT` • For SAP AC UM Functional Area Lookup Reconciliation: `LDECODE` • For SAP AC UM ItemProvAction Lookup Reconciliation: `LDECODE` • For SAP AC UM LangComm Lookup Reconciliation: `SPTXT` • For SAP AC UM Parameter Lookup Reconciliation: `PARTEXT` • For SAP AC UM DecimalNot Lookup Reconciliation: `_TEXT` • For SAP AC UM Priority Lookup Reconciliation: `LDECODE` • For SAP AC UM Profile Lookup Reconciliation: `USRSYSPRF` • For SAP AC UM ReqInitSystem Lookup Reconciliation: `REQSYSDECODE` • For SAP AC UM RequestType Lookup Reconciliation: `LDECODE` • For SAP AC UM Role Lookup Reconciliation: `USRSYSACT` • For SAP AC UM Systems Lookup Reconciliation: `RCVSYSTEM` • For SAP AC UM TimeZoneLookup Reconciliation: `DESCRIPT` • For SAP AC UM Title Lookup Reconciliation: `TITLE_MEDI` • For SAP AC UM UserGroup Lookup Reconciliation: `TEXT` • For SAP AC UM UserType Lookup Reconciliation: `_TEXT`

Table 3-24 (Cont.) Parameters of the SAP AC UM Reconciliation Jobs

Parameter	Description
Lookup Name	This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched. Depending on the reconciliation job you are using, the default values are as follows: • For SAP AC UM BusinessProcess Lookup Reconciliation: `Lookup.SAPACABAP.Bproc` • For SAP AC UM CommType Lookup Reconciliation: `Lookup.SAPACABAP.CommType` • For SAP AC UM Company Lookup Reconciliation: `Lookup.SAPACABAP.Company` • For SAP AC UM ContractUserType Lookup Reconciliation: `Lookup.SAPACABAP.ContractualUserType` • For SAP AC UM DateFormat Lookup Reconciliation: `Lookup.SAPACABAP.DateFormat` • For SAP AC UM Functional Area Lookup Reconciliation: `Lookup.SAPACABAP.Funcarea` • For SAP AC UM ItemProvAction Lookup Reconciliation: `Lookup.SAPACABAP.ItemProvAction` • For SAP AC UM LangComm Lookup Reconciliation: `Lookup.SAPACABAP.LangComm` • For SAP AC UM Parameter Lookup Reconciliation: `Lookup.SAPACABAP.Parameter` • For SAP AC UM DecimalNot Lookup Reconciliation: `Lookup.SAPACABAP.DecimalNotation` • For SAP AC UM Priority Lookup Reconciliation: `Lookup.SAPACABAP.Priority` • For SAP AC UM Profile Lookup Reconciliation: `Lookup.SAPACABAP.Profile` • For SAP AC UM ReqInitSystem Lookup Reconciliation: `Lookup.SAPACABAP.ReqInitSystem` • For SAP AC UM RequestType Lookup Reconciliation: `Lookup.SAPACABAP.RequestType` • For SAP AC UM Role Lookup Reconciliation: `Lookup.SAPACABAP.Roles` • For SAP AC UM Systems Lookup Reconciliation: `Lookup.SAPACABAP.System` • For SAP AC UM TimeZoneLookup Reconciliation: `Lookup.SAPACABAP.TimeZone` • For SAP AC UM Title Lookup Reconciliation: `Lookup.SAPACABAP.UserTitle` • For SAP AC UM UserGroup Lookup Reconciliation: `Lookup.SAPACABAP.UserGroups` • For SAP AC UM UserType Lookup Reconciliation: `Lookup.SAPACABAP.UserType`

Table 3-24 (Cont.) Parameters of the SAP AC UM Reconciliation Jobs

Parameter	Description
Object Class	Enter the class of object whose values must be synchronized. Depending on the scheduled job you are using, the default values are as follows: • For SAP AC UM BusinessProcess Lookup Reconciliation: `BusProc` • For SAP AC UM CommType Lookup Reconciliation: `commtype` • For SAP AC UM Company Lookup Reconciliation: `company` • For SAP AC UM ContractUserType Lookup Reconciliation: `contractualusertype` • For SAP AC UM DateFormat Lookup Reconciliation: `dateformat` • For SAP AC UM Functional Area Lookup Reconciliation: `FunctionArea` • For SAP AC UM ItemProvAction Lookup Reconciliation: `ItemProvActionType` • For SAP AC UM LangComm Lookup Reconciliation: `languagecommunication` • For SAP AC UM Parameter Lookup Reconciliation: `parameters` • For SAP AC UM DecimalNot Lookup Reconciliation: `decimalnotation` • For SAP AC UM Priority Lookup Reconciliation: `PriorityType` • For SAP AC UM Profile Lookup Reconciliation: `profiles` • For SAP AC UM ReqInitSystem Lookup Reconciliation: `SYSTEM` • For SAP AC UM RequestType Lookup Reconciliation: `RequstType` • For SAP AC UM Role Lookup Reconciliation: `activityGroups` • For SAP AC UM Systems Lookup Reconciliation: `cuaSystems` • For SAP AC UM TimeZoneLookup Reconciliation: `timeZones` • For SAP AC UM Title Lookup Reconciliation: `title` • For SAP AC UM UserGroup Lookup Reconciliation: `GROUP` • For SAP AC UM UserType Lookup Reconciliation: `usertype`

Table 3-24 (Cont.) Parameters of the SAP AC UM Reconciliation Jobs

Parameter	Description
Object Type	Enter the type of object whose values must be synchronized. Depending on the scheduled job you are using, the default values are as follows: • For SAP AC UM BusinessProcess Lookup Reconciliation: `BusProc` • For SAP AC UM CommType Lookup Reconciliation: `commtype` • For SAP AC UM Company Lookup Reconciliation: `company` • For SAP AC UM ContractUserType Lookup Reconciliation: `contractualusertype` • For SAP AC UM DateFormat Lookup Reconciliation: `dateformat` • For SAP AC UM Functional Area Lookup Reconciliation: `FunctionArea` • For SAP AC UM ItemProvAction Lookup Reconciliation: `ItemProvActionType` • For SAP AC UM LangComm Lookup Reconciliation: `languagecommunication` • For SAP AC UM Parameter Lookup Reconciliation: `parameters` • For SAP AC UM DecimalNot Lookup Reconciliation: `decimalnotation` • For SAP AC UM Priority Lookup Reconciliation: `PriorityType` • For SAP AC UM Profile Lookup Reconciliation: `profiles` • For SAP AC UM ReqInitSystem Lookup Reconciliation: `SYSTEM` • For SAP AC UM RequestType Lookup Reconciliation: `RequstType` • For SAP AC UM Role Lookup Reconciliation: `activityGroups` • For SAP AC UM Systems Lookup Reconciliation: `cuaSystems` • For SAP AC UM TimeZoneLookup Reconciliation: `timeZones` • For SAP AC UM Title Lookup Reconciliation: `title` • For SAP AC UM UserGroup Lookup Reconciliation: `GROUP` • For SAP AC UM UserType Lookup Reconciliation: `usertype`

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.

4

Performing Postconfiguration Tasks for the SAP User Management Connector

These are the tasks that you can perform after creating an application in Oracle Identity Governance.

- Configuring Ports on the Target System
- Configuring the Target System to Enable Propagation of User Password Changes
- Configuring Oracle Identity Governance
- Harvesting Entitlements and Sync Catalog
- Setting Up the Advanced Configuration Values in Oracle Identity Governance
- Managing Logging for the SAP UM Connector
- Configuring SoD (Segregation of Duties)
- Configuring the Access Request Management Feature of the Connector
- Configuring SNC to Secure Communication Between Oracle Identity Governance and the Target System
- Configuring the IT Resource for the Connector Server
- Downloading WSDL files from SAP GRC
- Localizing Field Labels in UI Forms
- Synchronizing the SAPUM Process Form Field Length Needs with the Target Field Length

4.1 Configuring Ports on the Target System

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

To enable communication between the target system and Oracle Identity Governance, you must ensure that the ports listed in Table 4-1 are open.

Table 4-1 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 Governance to these ports.

4.2 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

4.2.1 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

4.2.2 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.

4.2.3 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
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 both parent and child SAP system.

> **Note:**
>
> After importing the transport request, ensure the user details maintained while configuring CUA has the following authorizations in the child system. User details can be verified from the partner profile configured in WE20 for CUA.

For Authorization Object S_RFC:

- ACTVT: 16
- RFC_NAME:ZXLCRFC_ZXLCUSR_PW_CHANG
- RFC_TYPE: FUNC

4.3 Configuring Oracle Identity Governance

During application creation, if you did not choose to create a default form, then you must create a UI form for the application that you created by using the connector.

> **Note:**
>
> Perform the procedures described in this section only if you did not choose to create the default form during creating the application.

The following topics describe the procedures to configure Oracle Identity Governance:

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

4.3.1 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 Creating a Sandbox and Activating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.3.2 Creating a New UI Form

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

See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

While creating the UI form, ensure that you select the resource object corresponding to the newly created application that you want to associate the form with. In addition, select the **Generate Entitlement Forms** check box.

4.3.3 Publishing a Sandbox

Before publishing a sandbox, perform this 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 application instance form for your resource appears with correct fields.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.3.4 Creating an Application Instance

Create an application instance as follows.

1. In the left pane of the Identity System Administration, under Configuration, click **Application Instances.** The Application Instances page appears.
2. From the Actions menu, select **Create.** Alternatively, click **Create** on the toolbar. The Create Application Instance page appears.
3. Specify values for the following fields:
   - **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 ITResource.
   - **Form:** Select the form name (Creating a New UI Form).
4. Click **Save**.

   The application instance is created.
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See Managing Organizations Associated With Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Governance* for detailed instructions.

4.3.5 Updating an Existing Application Instance with a New Form

For any changes that you do in the schema of your application in Identity Self Service, 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 and activate a sandbox.
2. Create a new UI form for the resource.
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.

See Also:

- Creating a Sandbox and Activating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*
- Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*
- Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*

4.4 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

See Also:

- Reconciliation Jobs for a list of jobs for entitlements (lookup field synchronization)
- Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for information about the Entitlement List and Catalog Synchronization Job scheduled jobs

4.5 Setting Up the Advanced Configuration Values in Oracle Identity Governance

The Advanced Configuration settings are entered in Oracle Identity Governance when you create an application.

The following sections provide information on the entries in Advanced Configuration:

- Linking of SAP HRMS and SAP ERP or SAP CUA Accounts
- Configuring Password Changes for Newly Created Accounts

4.5.1 Linking of SAP HRMS and SAP ERP or SAP CUA Accounts

An SAP HRMS account created for a particular user can be linked with the SAP ERP 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 ERP or SAP CUA account.

You can duplicate this link in Oracle Identity Governance 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

4.5.1.1 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.

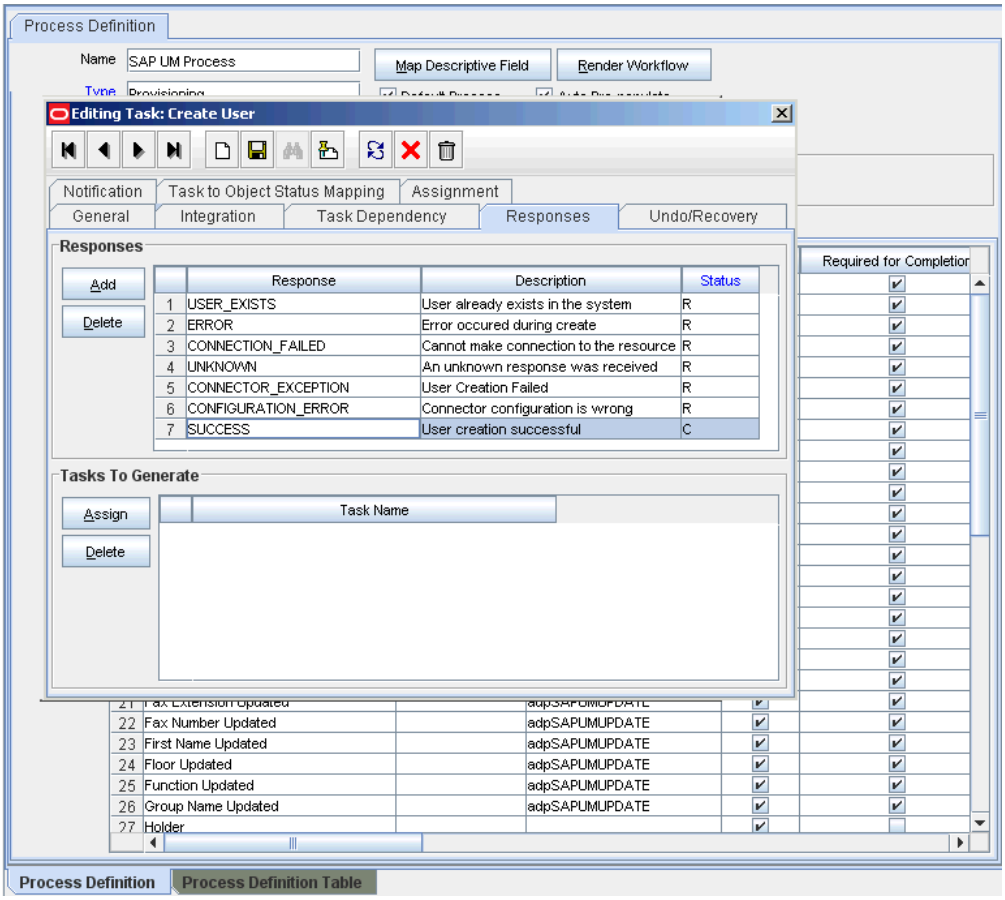
- If the value of overwriteLink advanced settings parameter is `no`, then the connector posts the User ID value of the SAP R/3 or SAP CUA account into the 0001 subtype in the Communication (0105) infotype of the SAP HRMS account only if that subtype does not hold a value.

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.

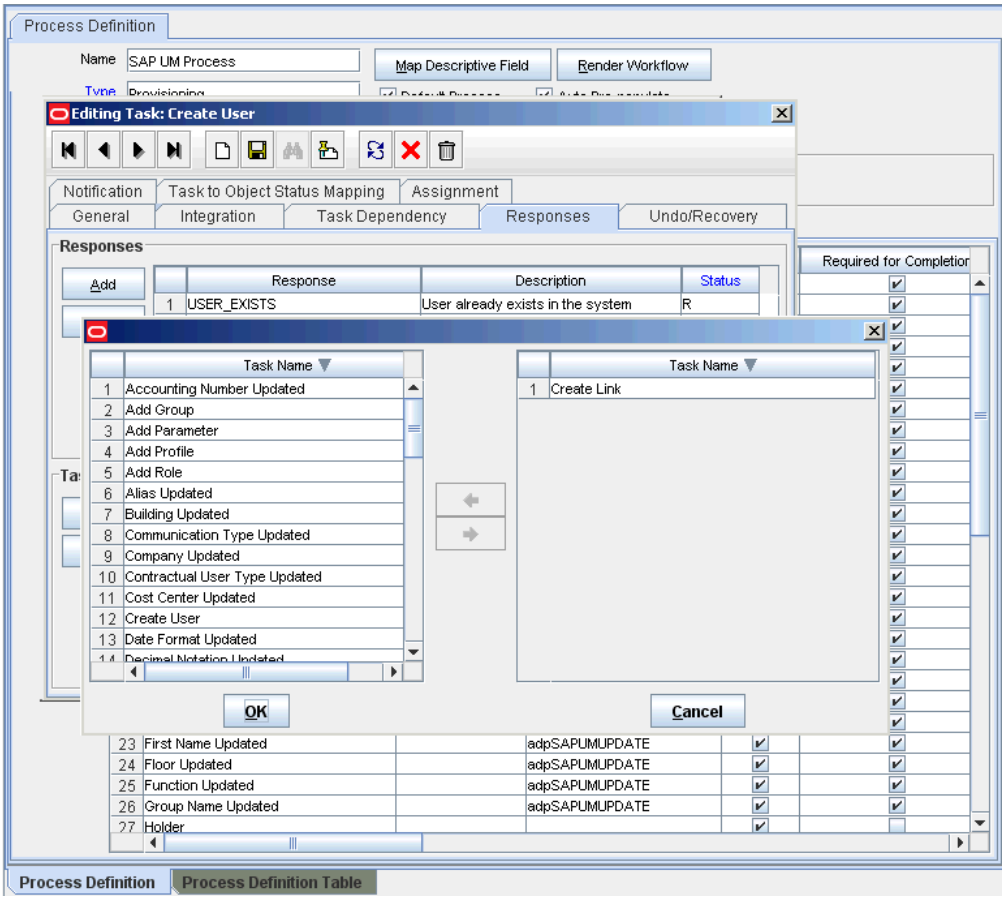
4.5.1.2 Enabling Linking of SAP HRMS and SAP R/3 or SAP CUA Accounts

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

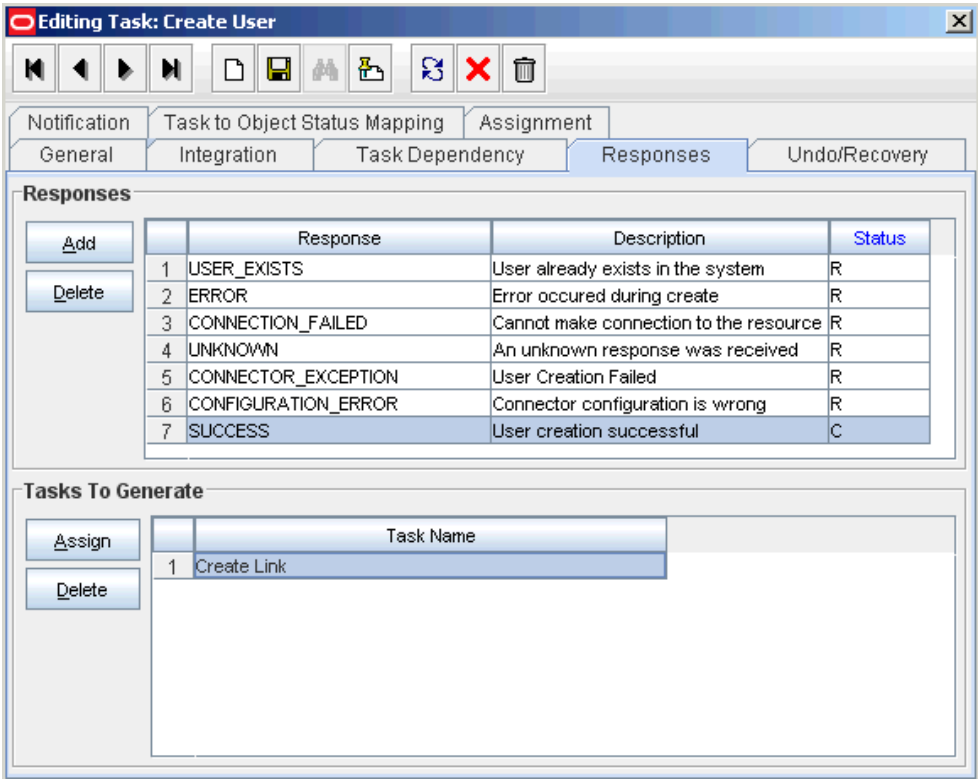
1. In the Design Console, expand **Process Management** and then double-click **Process Definition.**
2. Search for and open the **SAP UM Process** form.
3. Double-click the **Create User** task to open the Editing Task:Create User dialog box.
4. In the Responses tab, select the **SUCCESS** response,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



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



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



8. Save the changes and close the dialog box.

4.5.2 Configuring Password Changes for Newly Created Accounts

For information about configuring password changes for newly created accounts, see Configuring Password Changes for Newly Created Accounts.

4.6 Managing Logging for the SAP UM Connector

Oracle Identity Governance 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

4.6.1 Understanding Log Levels

When you enable logging, Oracle Identity Governance automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations.

ODL is the principle logging service used by Oracle Identity Governance and 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 Governance 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 4-2.

Table 4-2 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
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 Governance.

4.6.2 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 GRC, then add the following block:

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

If you are using Application onboarding, then add the following block:

```
<logger name='oracle.iam.application' 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 4-2 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 GRC, then add the following block:

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

```
     <handler name="console-handler"/>
</logger>
```

If you are using Application Onboarding, then add the following block:

```
<logger name='oracle.iam.application' level="NOTIFICATION:1"
useParentHandlers='false'>
     <handler name='sap-handler'/>
     <handler name='console-handler'/>
</logger>
</logger>
```

With these sample values, when you use Oracle Identity Governance, 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.

4.7 Configuring the Access Request Management Feature of the Connector

Access Request Management is a module in the SAP GRC 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 Governance can be configured as the medium for sending provisioning requests to SAP GRC Access Request Management. A request from Oracle Identity Governance is sent to Access Request Management, which forwards the provisioning data contained within the request to the target system (SAP ERP 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

See Configuring Request Types and Workflows on SAP GRC Access Request Management for more information about configuring the Access Request Management feature.

4.7.1 Configuring Request Types and Workflows on SAP GRC Access Request Management

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

1. Create a request type in SAP GRC Access Request Management.

   A request type In SAP GRC Access Request Management defines the action that is performed when a request is processed. Oracle Identity Governance is a requester. It works with request types defined in SAP GRC Access Request Management. The application advanced configuration maps request types to provisioning operations submitted through Oracle Identity Governance.
2. Create an access request workflow using the MSMP (Multi Step Multi process) Workflow Engine.

4.8 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 provides information on the following procedures:

- Specifying Values for the GRC-ITRes IT Resource
- Configuring SAP GRC to Act As the SoD Engine
- Verifying Entries Created in the Lookup.SAPABAP.System Lookup Definition
- Specifying a Value for the TopologyName of Basic Configuration 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.

4.8.1 Specifying Values for the GRC-ITRes IT Resource

The GRC-ITRes IT resource holds information that is used during communication with SAP GRC Access Request Management. To set values for the parameters of this IT resource:

1. For Oracle Identity Governance 12.2.1.3.0, log in to Oracle Identity System Administration.
2. In the left pane under Configuration, click **IT Resource.**
3. In the IT Resource Name field on the Manage IT Resource page, enter `GRC-ITRes` and then click **Search**.
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource.

   Table 4-3 lists the parameters of the GRC-ITRes IT resource.

Table 4-3 Parameters of the GRC-ITRes IT Resource

Parameter	Description
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`

Table 4-3 (Cont.) Parameters of the GRC-ITRes IT Resource

Parameter	Description
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`

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

4.8.2 Configuring SAP GRC to Act As the SoD Engine

To configure SAP GRC 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).

4.8.3 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.

4.8.4 Specifying a Value for the TopologyName of Basic Configuration 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 Governance installation
- SAP GRC 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 Basic Configuration Parameters for information about specifying values for parameters of Basic Configuration.

4.8.5 Disabling and Enabling SoD

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

- Disabling SoD on Oracle Identity Governance
- Enabling SoD on Oracle Identity Governance

4.8.5.1 Disabling SoD on Oracle Identity Governance

To disable SoD:

1. For Oracle Identity Governance release 12.2.1.3.0, log in to Oracle Identity System Administration.
2. 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 Governance.

4.8.5.2 Enabling SoD on Oracle Identity Governance

To enable SoD:

1. For Oracle Identity Governance release 12.2.1.3.0, log in to Oracle Identity System Administration.
2. 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 Governance.

4.9 Configuring SNC to Secure Communication Between Oracle Identity Governance and the Target System

Oracle Identity Governance 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 Governance and the SAP system.

This section provides information on the following topics:

- Prerequisites for Configuring the Connector to Use SNC

- Installing the Security Package
- Configuring SNC

4.9.1 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.

4.9.2 Installing the Security Package

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

1. Download SAP Cryptolib for encrypted communication with Oracle Identity Governance.

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

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

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

> **See Also:**
>
> 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

4.9.3 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 Governance certificate by entering the following command:

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

   b. Import the Oracle Identity Governance 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 Governance 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:
   - SAP lib
   - SAP mode
   - SAP myname
   - SAP partnername
   - SAP qop

4.10 Configuring the IT Resource for the Connector Server

If you have used the Connector Server, then you must configure values for the parameters of the Connector Server IT resource.

After you create the application for your target system, you must create an IT resource for the Connector Server as described in Creating IT Resources of *Oracle Fusion Middleware Administering Oracle Identity Governance*. While creating the IT resource, ensure to select **Connector Server** from the **IT Resource Type** list. In addition,

specify values for the parameters of IT resource for the Connector Server listed in Table 4-4. For more information about searching for IT resources and updating its parameters, see Managing IT Resources in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

Table 4-4 Parameters of the IT Resource for the SAP UM 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 Governance times out. If the value is zero or if no value is specified, the timeout is unlimited. Recommended value: `0`
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Governance 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, see Configuring SSL for Java Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.11 Downloading WSDL files from SAP GRC

In SAP GRC 10 or later, you need to download the WSDL files from SAP GRC 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 OIG:

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.

4.12 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.

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 (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer.
5. Extract the contents of the archive, and open one of the following files in a text editor:

   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf

   > **Note:**
   >
   > You will not be able to view the BizEditorBundle.xlf unless you complete creating the application for your target system or perform any customization such as creating a UDF.

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_T
ITLE__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.BaseRuntimeResourceBundle']
['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_T
ITLE__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 Governance.

4.13 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.

5

Using the SAP User Management Connector

You can use the SAP UM connector for performing reconciliation and provisioning operations after configuring the application to meet your requirements.
This chapter is divided into the following sections:

5.1 Guidelines on Configuring Reconciliation

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

- 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 Governance 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.

5.2 Configuring Reconciliation

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

Reconciliation involves duplicating in Oracle Identity Governance the creation of and modifications to user accounts on the target system.

This section provides information on the following topics related to configuring reconciliation:

5.2.1 Performing Full and Incremental Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Governance. After you create the application, you must first perform full reconciliation.
At the end of the reconciliation run, the connector automatically sets the `Latest Token` parameter of the job for user record reconciliation to the time stamp at which the run ended. From the next run onward, the connector considers only records created or modified after this time stamp for reconciliation. This is incremental reconciliation.

You can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Governance. 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 .

5.2.2 Performing Batched Reconciliation

You can perform batched reconciliation to reconcile a specific number of records from the target system into Oracle Identity Governance.

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, you must specify a value for the batchSize parameter of the Advanced Settings section. Use this attribute to specify the number of records that must be included in each batch. By default, this value is empty.

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 parameter.

5.2.3 Performing Limited Reconciliation

You can perform limited reconciliation by creating filters for the reconciliation module, and reconcile records from the target system based on a specified filter criterion.

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. The connector provides a Filter parameter that allows you to use any of the SAP 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')
```

For detailed information about ICF Filters, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

5.3 Configuring Reconciliation Jobs

Configure reconciliation jobs to perform reconciliation runs that check for new information on your target system periodically and replicates the data in Oracle Identity Governance.

You can apply this procedure to configure the reconciliation jobs for users and entitlements.

To configure a reconciliation job:

1. Log in to Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
   a. 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.
   b. 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 task:
   - **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. See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

   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.

> **Note:**
>
> Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.

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.

5.4 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

5.4.1 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.

5.4.2 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).

5.5 Performing Provisioning Operations

You create a new user in 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 perform provisioning operations in Oracle Identity Governance:

1. Log in to Identity Self Service.
2. Create a user as follows:
   a. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
   b. From the Actions menu, select **Create**. Alternatively, you can click **Create** on the toolbar. The Create User page is displayed with input fields for user profile attributes.
   c. Enter details of the user in the Create User page.
3. On the Account tab, click **Request Accounts**.
4. In the Catalog page, search for and add to cart the application instance for the connector that you configured earlier, and then click **Checkout**.
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.

> **See Also:**
>
> Creating a User in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for details about the fields on the Create User page

5.6 Performing Provisioning Operations in an SoD-Enabled Environment

Provisioning a resource for an OIM User involves using Oracle Identity Governance 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 provides information on the following topics:

- Overview of the Provisioning Process in an SoD-Enabled Environment
- Guidelines on Performing Provisioning Operations in an SoD-Enabled Environment
- Request-Based Provisioning in an SoD-Enabled Environment

5.6.1 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 GRC SoD Invocation Library (SIL) Provider passes the entitlement data to the Web service of SAP GRC.
3. After SAP GRC runs the SoD validation process on the entitlement data, the response from the process is returned to Oracle Identity Governance.
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.

5.6.2 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.

5.6.3 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 Governance.

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:

- Creating of Request-Based Provisioning by End-Users
- Approving Request-Based Provisioning

See Configuring SoD (Segregation of Duties) for related information.

5.6.3.1 Creating 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 Governance 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.

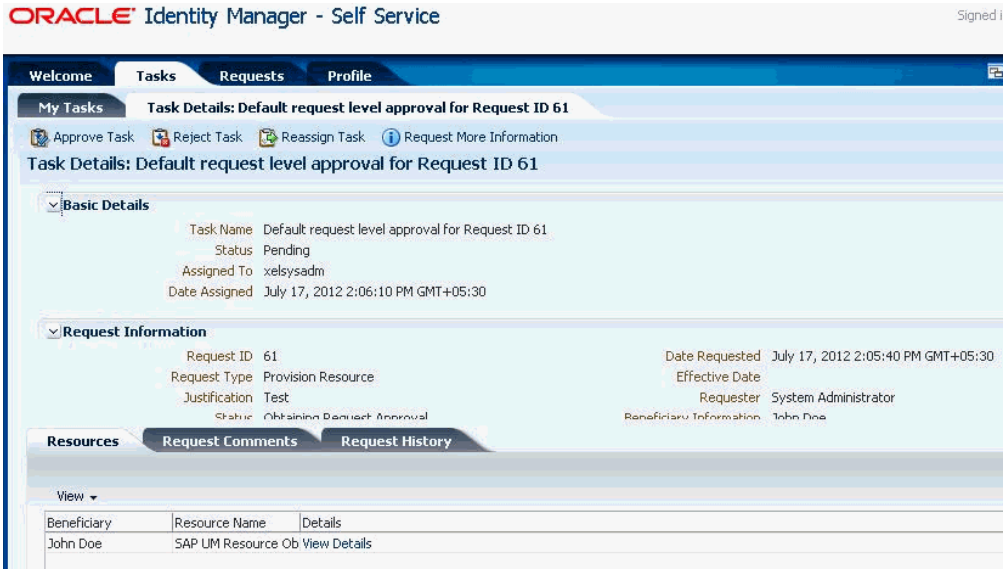
    One of the fields on this page is the SODCheckStatus field. The value in this field can be SoD Check Not Initiated or SoDCheckCompleted. When the request is placed, the SODCheckStatus field contains the SoDCheckCompleted status.
15. To view details of the approval, on the Request Details page, click the **Approval Tasks** tab.

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

5.6.3.2 Approving Request-Based Provisioning

This section provides information on the role of the approver in a request-based provisioning operation.

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



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

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

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 Governance 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.

5.7 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 ERP and SAP CUA Target Systems for Reconciliation
- Switching Between the SAP ERP and SAP CUA Target Systems for Provisioning

5.7.1 Switching Between the SAP ERP and SAP CUA Target Systems for Reconciliation

To switch between SAP ERP 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 ERP, then set the value to `no`.

   See Setting Up the Advanced Configuration Values in Oracle Identity Governance 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.

5.7.2 Switching Between the SAP ERP and SAP CUA Target Systems for Provisioning

To switch between SAP ERP 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 ERP, 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.
3. Start the provisioning operation on Oracle Identity System Administration by selecting the required IT resource.

5.8 Switching From an SAP ERP or SAP CUA Target Systems to an SAP GRC Target System and Vice Versa

You can switch from an SAP ERP or SAP CUA target system to an SAP GRC target system and viceversa.

If you want to switch from an SAP ERP or SAP CUA target system to a SAP GRC 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 Governance in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* 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**.
4. Import the request datasets for the target system to which you want to switch.
5. Run the PurgeCache utility to clear the cache for the content category **Metadata**.

5.9 Uninstalling the Connector

Uninstalling the SAP UM connector deletes all the account-related data associated with its resource objects.

If you want to uninstall the connector for any reason, then run the Uninstall Connector utility. Before you run this utility, ensure that you set values for `ObjectType` and `ObjectValues` properties in the ConnectorUninstall.properties file. For example, if you want to delete resource objects, scheduled tasks, and scheduled jobs associated with the connector, then enter `"ResourceObject", "ScheduleTask", "ScheduleJob"` as the value of the `ObjectType` property and a semicolon-separated list of object values corresponding to your connector as the value of the `ObjectValues` property.

For example: `SAP UM User; SAP UM Group`

> **Note:**
>
> If you set values for the `ConnectorName` and `Release` properties along with the `ObjectType` and `ObjectValue` properties, then the deletion of objects listed in the `ObjectValues` property is performed by the utility and the Connector information is skipped.

For more information, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

6

Extending the Functionality of the SAP User Management Connector

You can extend the functionality of the connector to address your specific business requirements.
This following topics are discussed in this section:

- Determining the Names of Target System Attributes
- Configuring the Connector for Multiple Installations of the Target System
- Configuring Transformation and Validation of Data
- Configuring Resource Exclusion Lists
- Configuring Action Scripts

6.1 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:

Application Attribute			Provisioning Property		Reconciliation Property		
Display Name	**Target Attribute**	**Data Type**	**Mandatory ?**	**Provisioning Field**	**Reconciliation Field**	**Key Field**	**Case Insensitive**
Nick Name	NICKNAME;ADDRESS;NICKNAME;ADDRESSX	String	No	Yes	Yes	No	No
user ID	_NAME_	String	Yes	Yes	Yes	Yes	No
Password	_PASSWORD_	String	No	Yes	No	No	No

The format of single-valued target system attributes is as follows:

FIELD_NAME;STRUCTURE_NAME

In this format:

- *FIELD_NAME* is the name of the field
- *STRUCTURE_NAME* is the name of the structure

The format of multivalued target system 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*.

> **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 provided in the custom BAPI.

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 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 attribute and structure names are case-sensitive.

6.2 Configuring the Connector for Multiple Installations of the Target System

You must create copies of configurations of your base application to configure it 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, including independent schema for each. The company has recently installed Oracle Identity Governance, and they want to configure it to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must clone your application which copies all configurations of the base application into the cloned application. For more information about cloning applications, see Cloning Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.3 Configuring Transformation and Validation of Data

Configure transformation and validation of user account data by writing Groovy script logic while creating your application.

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 Governance.

Similarly, 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 transformation or validation of user account data, you must write Groovy scripts while creating your application. For more information about writing Groovy script-based validation and transformation logic, see Validation and Transformation of Provisioning and Reconciliation Attributes of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.4 Configuring Resource Exclusion Lists

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

See Resource Exclusion Lists of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.5 Configuring Action Scripts

You can configure **Action Scripts** by writing your own Groovy scripts while creating your application.

These scripts can be configured to run before or after the create, update, or delete an account provisioning operations. For example, you can configure a script to run before every user creation operation.

For information on adding or editing action scripts, see Updating the Provisioning Configuration in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

7

Upgrading the SAP User Management Connector

If you have already deployed the 11.1.1.7.0 version of this connector, then you can upgrade the connector to version 12.2.1.3.0 by uploading the new connector JAR files to the Oracle Identity Manager database.

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

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.

The following sections discuss the procedure to upgrade the connector:

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

See Also:

Upgrading Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information on these steps

7.1 Preupgrade Steps

Preupgrade steps involve performing a reconciliation run, defining the source, running the Delete JARs utility and connector preupgrade utility.

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.
- If required, create the connector XML file for a clone of the source connector.
- Disable all scheduled tasks.
- Run the Oracle Identity Manager Delete JARs utility to delete the old connector bundle to the Oracle Identity Manager database.
- Run the connector preupgrade utility.

> **See Also:**
>
> – Delete JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for detailed information about the Delete JARs utility
>
> – Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about the preupgrade utility

7.2 Upgrade Steps

This is a summary of the procedure to upgrade the connector for both staging and production environments.

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.

> **Note:**
>
> Do not upgrade IT resource type definition. In order to retain the default setting, you must map the IT resource definition to "None".

- Production Environment

  Perform the upgrade procedure by using the silent mode.

See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the wizard and silent modes.

7.3 Postupgrade Steps

Postupgrade steps involve uploading new connector JAR files, configuring the upgraded IT resource of the source connector, deploying and reconfiguring the Connector Server, and deleting duplicate entries for lookup definitions.

> **Note:**
>
> If you have not retained the customizations, you must reapply them after you upgrade the connector.

Perform the following procedure:

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

   > **Note:**
   >
   > You can download the JARs from Oracle Technology Network Website (OTN) website. See Downloading the Connector Installation Package for more information.

   - For Basic User Management and SoD validation of SAP GRC Access Risk Analysis:
     - Upload bundle/org.identityconnectors.sap-12.3.0.jar as an ICFBundle
     - Upload lib/sap-oim-integration.jar as a JavaTask
   - For SAP GRC Access Request Management:
     - Upload bundle/org.identityconnectors.sapacum-12.3.0.jar as an ICFBundle
     - Upload lib/sapac-oim-integration.jar as a ScheduleTask

   > **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 if the IT resource details are updated.
4. Replicate all changes as in the previous version of the connector process form in a new UI form as follows:
   a. Log in to Oracle Identity System Administration.
   b. Create and activate a sandbox.
   c. Create a new UI form to view the upgraded fields.
   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 Step 4 c), and then save the application instance.
   e. Publish the sandbox and perform full reconciliation.
5. Delete the duplicated lookup entries that are generated while upgrading the connector.

   The following are the list of lookup definitions. See Postupgrade Issue for the detailed list of entries of these lookups:

   - Lookup.SAPABAP.Configuration
   - Lookup.SAPABAP.UM.ProvAttrMap
   - Lookup.SAPABAP.UM.ReconAttrMap
   - Lookup.SAPAC10ABAP.Configuration
   - Lookup.SAPAC10ABAP.UM.ProvAttrMap
   - Lookup.SAPAC10ABAP.UM.ReconAttrMap

   Perform the postupgrade procedure in Managing Connector Lifecycle of *Oracle Fusion Middlware Administering Oracle Identity Governance*.
6. Perform full reconciliation or delete reconciliation.

See Also:

- Configuring Oracle Identity Governance for information about creating, activating, and publishing a sandbox and creating a new UI form
- Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for information about deploying the Connector Server

8

Known Issues for the SAP User Management Connector

These are the known issues and workarounds associated with this release of the connector.

8.1 Connector Issues

These are the issues and workarounds associated with the connector.

8.1.1 Error During SoD Check

During SoD check, when the data that is returned from SAP GRC webservices crosses 4000 characters, only the first 4000 characters are displayed.

Workaround: If the size of the violation details obtained from SAP GRC 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.

8.1.2 SAP UM 12c Connector and SAP ER 9.*x* connector Do Not Work

The ICF-based SAP User Management connector and the legacy SAP ER connector do not work together with Oracle Identity Governance 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 works. When the second bundle tries to create a connection, it tries to register the data provider that is already registered by first bundle. Then, it throws an error, "DestinationDataProvider already registered".

Workaround: 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 Governance.

8.1.3 Postupgrade Issue

Before upgrading the connector, the following lookup default decode values are upgraded with target configuration values:

- Lookup.SAPABAP.Configuration
- Lookup.SAPABAP.UM.ProvAttrMap
- Lookup.SAPABAP.UM.ReconAttrMap

- Lookup.SAPAC10ABAP.Configuration
- Lookup.SAPAC10ABAP.UM.ProvAttrMap
- Lookup.SAPAC10ABAP.UM.ReconAttrMap

After the connector is upgraded, it generates duplicate entries with decode default values as shown in the following tables:

Table 8-1 Entries in the Lookup.SAPABAP.Configuration Lookup Definition

Code Key	Decode
CodeKey	Decode
aliasUser	none
batchSize	100
Bundle Name	org.identityconnectors.sap
Bundle Version	12.3.0
changePasswordAtNextLogon	no
codePage	none
compositeRoles	no
Connector Name	org.identityconnectors.sap.SAPConnector
cuaChildInitialPasswordChangeFuncModule	ZXLCBAPI_ZXLCUSR_PW_CHANGE
cuaChildPasswordChangeFuncModule	ZXLCBAPI_ZXLCUSR_PASSWORDCHNGE
disableLockStatus	64
enableCUA	no
entitlementRiskAnalysisAccessURL	
entitlementRiskAnalysisWS	oracle.iam.grc.sod.scomp.impl.grcsap.util.webservice.sap.ac10.RiskAnalysisWithoutNo
gatewayHost	none
gatewayService	none
getSSO2	none
groups	GROUPS~USERGROUP
lCheck	none
mySAPSSO2	none
overwriteLink	no
parameters	PARAMETER1~PARID;PARVA
passwordPropagateToChildSystem	no
ProfileAttributeLabel	Profile Name
Profile attribute name	USERPROFILE
Profile form names	UD_SPUMPC_P;UD_SPUM_PRO
profiles	PROFILES~SUBSYSTEM;PROFILE
reconcilefuturedatedroles	yes
reconcilepastdatedroles	yes
repositoryDestination	none
repositoryPassword	none

Table 8-1 (Cont.) Entries in the Lookup.SAPABAP.Configuration Lookup Definition

Code Key	Decode
repositorySNCMode	none
repositoryUser	none
riskLevel	3
RoleAttributeLabel	Role Name
Role attribute name	USERROLE
Role form names	UD_SPUMRC_P;UD_SAPRL
roles	ACTIVITYGROUPS~SUBSYSTEM;AGR_NAME;TO_DAT;FROM_DAT;ORG_FLAG
sapSystemTimeZone	IST
singleRoles	yes
SOD Configuration lookup	Lookup.SAPABAP.Configuration
tpHost	none
tpName	none
type	none
User Configuration Lookup	Lookup.SAPABAP.UM.Configuration
validatePERNR	no
wsdlFilePath	none

The following table lists the code and decode key of the Lookup.SAPABAP.UM.ProvAttrMap lookup.

Table 8-2 Entries in the Lookup.SAPABAP.UM.ProvAttrMap

Code Key	Decode Key
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
Date Format[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

Table 8-2 (Cont.) Entries in the Lookup.SAPABAP.UM.ProvAttrMap

Code Key	Decode Key
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	__LOCK_OUT__
User Type[Lookup]	USTYP;LOGONDATA;USTYP;LOGONDATAX
Valid From[Date]	GLTGV;LOGONDATA;GLTGV;LOGONDATAX
Valid Through[Date]	GLTGB;LOGONDATA;GLTGB;LOGONDATAX

The following table lists the code and decode key of the Lookup.SAPABAP.UM.ReconAttrMap lookup.

Table 8-3 Entries in the Lookup.SAPABAP.UM.ReconAttrMap Lookup Definition

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

Table 8-3 (Cont.) Entries in the Lookup.SAPABAP.UM.ReconAttrMap Lookup Definition

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

The following table lists the code and decode keys in the Lookup.SAPAC10ABAP.Configuration.

Table 8-4 Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode Key
aliasUser	none
appLookupAccessURL	none
appLookupWS	oracle.iam.ws.sap.ac10.SelectApplication
assignRoleReqType	002~Change Account~002~006
auditLogsAccessURL	none
auditLogsWS	oracle.iam.ws.sap.ac10.AuditLogs
batchSize	100
Bundle Name	org.identityconnectors.sapacum
Bundle Version	12.3.0
changePasswordAtNextLogon	no
codePage	none
compositeRoles	no
Connector Name	org.identityconnectors.sapacum.SAPACUMConnector
createUserReqType	001~New Account~001
cuaChildInitialPasswordChangeFuncModule	ZXLCBAPI_ZXLCUSR_PW_CHANGE
cuaChildPasswordChangeFuncModule	ZXLCBAPI_ZXLCUSR_PASSWORDCHNGE
deleteUserReqType	003~Delete Account~003
disableLockStatus	64
enableCUA	no
gatewayHost	none
gatewayService	none
getSSO2	none
groups	GROUPS~USERGROUP
ignoreOpenStatus	Yes
lCheck	none
lockUserReqType	004~Lock Account~004

Table 8-4 (Cont.) Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode Key
logAuditTrial	Yes
modifyUserReqType	002~Change Account~002
mySAPSSO2	none
otherLookupAccessURL	none
otherLookupWS	oracle.iam.ws.sap.ac10.SearchLookup
overwriteLink	no
parameters	PARAMETER1~PARID;PARTXT
passwordPropagateToChildSystem	no
profiles	PROFILES~SUBSYSTEM;PROFILE
provActionAttrName	provAction;ReqLineItem
provItemActionAttrName	provItemAction;ReqLineItem
reconcilefuturedatedroles	yes
reconcilepastdatedroles	yes
removeRoleReqType	002~Change Account~002~009
repositoryDestination	none
repositoryPassword	none
repositorySNCMode	none
repositoryUser	none
requestStatusAccessURL	none
requestStatusValue	OK
requestStatusWS	oracle.iam.ws.sap.ac10.RequestStatus
requestTypeAttrName	Reqtype;Header
riskLevel	High
roleLookupAccessURL	none
roleLookupWS	oracle.iam.ws.sap.ac10.SearchRoles
roles	ACTIVITYGROUPS~SUBSYSTEM;AGR_NAME;TO_DAT;FROM_DAT;ORG_FLAG
sapSystemTimeZone	PST
singleRoles	yes
Status Configuration Lookup	Lookup.SAPACABAP.Status.Configuration
tpHost	none
tpName	none
type	none
unlockUserReqType	005~unlock user~005
userAccessAccessURL	none
userAccessWS	oracle.iam.ws.sap.ac10.UserAccess
User Configuration Lookup	Lookup.SAPAC10ABAP.UM.Configuration

Table 8-4 (Cont.) Entries in the Lookup.SAPAC10ABAP.Configuration Lookup Definition

Code Key	Decode Key
validatePERNR	no
wsdlFilePath	none

The following table lists the code and decode keys in the Lookup.SAPAC10ABAP.UM.ProvAttrMap lookup.

Table 8-5 Entries in the Lookup.SAPAC10ABAP.UM.ProvAttrMap Lookup Definition

Code Key	Decode Key
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
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

Table 8-5 (Cont.) Entries in the Lookup.SAPAC10ABAP.UM.ProvAttrMap Lookup Definition

Code Key	Decode Key
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]	parameters~PARAMETER1~parameter;Parameter
UD_UMAC_PRM~Parameter Value	parameters~PARAMETER1~parameterValue;Parameter
UD_UMAC_PRO~Profile Name[Lookup]	profiles~PROFILES~itemName;ReqLineItem
UD_UMAC_PRO~Profile System Name[Lookup]	profiles~PROFILES~connector;ReqLineItem
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
Unique ID	__UID__
User Group[Lookup]	userGroup;UserInfo
User ID	__NAME__
User Lock	userLock;None

Table 8-5 (Cont.) Entries in the Lookup.SAPAC10ABAP.UM.ProvAttrMap Lookup Definition

Code Key	Decode Key
User Type	userType;UserInfo
Valid From[Date]	validFrom;UserInfo
Valid Through[Date]	validTo;UserInfo

The following table lists the code and decode keys in the Lookup.SAPAC10ABAP.UM.ReconAttrMap lookup,

Table 8-6 Entries in the Lookup.SAPAC10ABAP.UM.ReconAttrMap Lookup Definition

Code Key	Decode Key
Accounting Number	accno;UserInfo
Alias	alias;UserInfo
Building	BUILDING_P;ADDRESS;BUILDING_P;ADDRESSX
Communication Type[Lookup]	commMethod;UserInfo
Company[Lookup]	COMPANY;COMPANY;COMPANY;COMPANYX
Contractual User Type[Lookup]	LIC_TYPE;UCLASS;UCLASS;UCLASSX
Cost Center	costcenter;UserInfo
Date Format[Lookup]	dateFormat;UserInfo
Decimal Notation[Lookup]	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~User Group[Lookup]	groups~GROUPS~USERGROUP
Group Name[Lookup]	CLASS;LOGONDATA;CLASS;LOGONDATAX
Language Communication[Lookup]	LANGU_P;ADDRESS;LANGU_P;ADDRESSX
Last Name	lname;UserInfo
Logon Language[Lookup]	logonLang;UserInfo
Parameter~Parameter ID[Lookup]	parameters~PARAMETER1~parameter;Parameter
Parameter~Parameter Value	parameters~PARAMETER1~parameterValue;Parameter

Table 8-6 (Cont.) Entries in the Lookup.SAPAC10ABAP.UM.ReconAttrMap Lookup Definition

Code Key	Decode Key
Profile~Profile Name[Lookup]	profiles~PROFILES~itemName;ReqLineItem
Profile~Profile System Name[Lookup]	profiles~PROFILES~connector;ReqLineItem
Role~End Date[Date]	roles~ACTIVITYGROUPS~ValidTo;ReqLineItem
Role~Role Name[Lookup]	roles~ACTIVITYGROUPS~itemName;ReqLineItem
Role~Role System Name[Lookup]	roles~ACTIVITYGROUPS~connector;ReqLineItem
Role~Start Date[Date]	roles~ACTIVITYGROUPS~validFrom;ReqLineItem
Room Number	ROOM_NO_P;ADDRESS;ROOM_NO_P;ADDRESSX
Start Menu	startMenu;UserInfo
Status	__ENABLE__
Telephone Extension	TEL1_EXT;ADDRESS;TEL1_EXT;ADDRESSX
Telephone Number	telnumber;UserInfo
Time Zone[Lookup]	TZONE;LOGONDATA;TZONE;LOGONDATAX
Title[Lookup]	title;UserInfo
Unique ID	__UID__
User ID	__NAME__
User Lock	userLock;None
User Type[Lookup]	userType;UserInfo
Valid From[Date]	validFrom;UserInfo
Valid Through[Date]	validTo;UserInfo

Workaround: Delete each instance of the duplicate entries.

8.2 Oracle Identity Governance Issues

These are issues and workarounds associated with Oracle Identity Governance.

- Revoke Account Task Rejected and Unable to Update OIG Account
- Application Server Error Whenever a JAR File is Updated or Modified

8.2.1 Revoke Account Task Rejected and Unable to Update OIG Account

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.

Workaround: There is no workaround for this issue.

8.2.2 Application Server Error Whenever a JAR File is Updated or Modified

Whenever a JAR file 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 the following error:

```
java.lang.UnsatisfiedLinkError: Native Library /usr/local/jco/
libsapjco3.sojava.lang.UnsatisfiedLinkError: Native
Library /usr/local/jco/libsapjco3.dll
```

Workaround: Restart the application server if any JAR is updated or modified in the Oracle Identity Governance server.

9

Frequently Asked Questions for the SAP User Management Connector

This chapter provides information on the frequently asked questions about the SAP UM connector.

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 Governance 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 Governance. Refer to SAP UM 12c Connector and SAP ER 9.*x* connector Do Not Work for more information.

3. I have changed the system property for SOD as XL.SoDCheckRequired = TRUE. Is it now possible to use two SAP connectors in the same OIG environment having one connector configured for SOD analysis and the other connector configured without SOD analysis?

   Answer: No, the system property is common in OIG. Hence, the property applies to all the connectors installed in that OIG.

4. 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}

5. 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.

6. 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 and not on the GRC server, therefore SAP will not fix this. This is a limitation with the SAP target system.

7. Which version of the SAP BusinessObjects Access does the connector support?

   Answer: As listed in Certified Components, 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.

8. Where should I copy the third party libraries (sapjco3.jar) if I am using the connector server?

   Answer: Copy SAP User Management third party libraries (sapjco3.jar) into the *CONNECTOR_SERVER_HOME*\lib directory.

9. 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.

10

Troubleshooting the SAP User Management 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 10-1 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 connect to SAP through SNC **Returned Error Message:** SAP Connection JCO Exception **Returned Error Code** `SNC required or this connection`	Ensure that values for the following basic configuration parameters are correctly specified: • SAPsnc_myname: `p:CN=win2003, OU=SAP, O=ORA, C=IN` • SAPsnc_qop: `3` • SAPsnc_partnername: `p:CN=I47, OU=SAP, O=ORA, C=IN` The following are examples of sncLib paths for Windows and Linux: • For Windows: `SAPsnc_lib: C://usr//sap//sapcrypto.dll` • For Linux: `SAPsnc_lib: //home/oracle/sec/sapcrypto.so`
When you try to provision account or lookup recon 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 a X.509 Certificate and an ABAP User in view VUSREXTID in transaction SM30. Choose external ID type as DN.
When you try to provision account or lookup recon 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 view VSNCSYSACL for External type ACL entry.

Table 10-1 (Cont.) Common SNC Errors

Problem Description	Solution
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_SYSTEM_FAILURE`	Program ID must have SNC enabled in transaction SM59.

A

Files and Directories in the SAP User Management Connector Package

These are the components of the connector installation media that comprise the SAP UM connector.

Table A-1 Files and Directories in the Installation Media

File in the Installation Package	Description
bundle/ org.identityconnectors.sap-12.3.0.jar	These JAR files contain the connector bundle.
bundle/ org.identityconnectors.sapacum-12.3.0.jar	These JAR files contain GRC system connector bundle.
configuration/ SAPUMConnector-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the SAP UM Connector Installer during connector installation.
configuration/ SAPACUMConnector-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the SAP AC UM Connector Installer during connector installation.
lib/sap-oim-integration.jar	This JAR file is required to request entitlements for roles and profiles through request-based provisioning using request datasets.
lib/sapac-oim-integration.jar	This JAR file includes a custom scheduled job to update request status from SAP GRC.
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 Governance 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-ConnectorConfig.xml	This XML file contains definitions for the following connector components: Note: These files are applicable only for a CI-based connector. • Resource objects • IT resource types • IT resource instance • Process forms • Process tasks and adapters • Process definition • Lookup definitions • Reconciliation rules • Scheduled tasks **Note:** These files are applicable only for a CI-based connector.

Table A-1 (Cont.) Files and Directories in the Installation Media

File in the Installation Package	Description
xml/SAPACUM-ConnectorConfig.xml	This XML file contains GRC system definitions for the following connector components: • Resource objects • IT resource types • IT resource instance • Process forms • Process tasks and adapters • Process definition • Lookup definitions • Reconciliation rules • Scheduled tasks **Note:** These files are applicable only for a CI-based connector.
xml/SAPUM-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system . It also includes basic and advanced configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/SAPUM-pre-config.xml	This XML file contains definitions for lookup and GRC IT Resource required for lock/unlock user and SoD configuration.
xml/SAPACUM-target-template.xml	This file contains definitions for the Access Control connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes basic and advanced configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/SAPACUM-pre-config.xml	This XML file contains definitions for lookup, schedule task, and schedule job for updating user status in Access Control configuration.
upgrade/PostUpgradeScript.sql	This file contains the scripts that are run after performing an upgrade of the connector.

B

BAPIs Used During Connector Operations

These are the standard and custom BAPIs used during connector operations 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.

Import the following TRs in given sequence in the parent as well as child system to get the mentioned BAPIs:

- EC1K900023
- G10K900013

Index