

Oracle® Identity Manager

Connector Guide for SAP User Management Engine



11.1.1
E40586-12
July 2020

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2020, Oracle and/or its affiliates.

Primary Author: Alankrita Prakash

Contributing Authors: Gowri.G.R

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	xii
Documentation Accessibility	xii
Related Documents	xii
Documentation Updates	xii
Conventions	xiii

What's New in This Guide?

Software Updates	xiv
Documentation-Specific Updates	xvii

1 About the Connector

1.1	Certified Components	1-1
1.2	Usage Recommendation	1-3
1.3	Certified Languages	1-3
1.4	Connector Architecture and Supported Deployment Configurations	1-4
1.4.1	User Management with Access Request Management	1-6
1.4.2	Audit Trail Details in Connector Logs	1-9
1.4.3	User Management with SoD	1-10
1.4.4	User Management with Both SoD and Access Request Management	1-11
1.4.5	Guidelines on Using a Deployment Configuration	1-12
1.4.5.1	User Management Engine with SoD and Access Request Management	1-12
1.4.5.2	Summary of Account Management Process when SAP BusinessObjects AC Access Risk Analysis and SAP BusinessObjects AC Access Request Management are Enabled	1-13
1.4.5.3	User Management with Access Request Management	1-13
1.4.5.4	Summary of Account Request Management when SAP BusinessObjects AC Access Request Management is Configured and Enabled in your SAP Operating Environment	1-13
1.4.6	Considerations to Be Addressed When You Enable Access Request Management	1-14

1.5	Features of the Connector	1-14
1.5.1	Routing of Provisioning Requests Through SAP BusinessObjects AC Access Request Management	1-15
1.5.2	SoD Validation of Entitlement Requests	1-15
1.5.3	Full Reconciliation	1-16
1.5.4	Limited (Filtered) Reconciliation	1-16
1.5.5	Enabling and Disabling Accounts	1-16
1.5.6	Support for Multiple Data Sources	1-17
1.5.7	Support for Remote Role Assignment in Federated Portal Network	1-17
1.5.8	Transformation and Validation of Account Data	1-17
1.5.9	Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations	1-17
1.5.10	Support for Bulk Update of Attributes	1-17
1.6	Lookup Definitions Used During Connector Operations	1-18
1.6.1	Lookup Definitions Synchronized with the Target System	1-18
1.6.2	Preconfigured Lookup Definitions	1-19
1.6.2.1	Lookup.SAPUME.Configuration	1-20
1.6.2.2	Lookup.SAPUME.UM.Configuration	1-21
1.6.2.3	Lookup.SAPUME.UM.ProvAttrMap	1-22
1.6.2.4	Lookup.SAPUME.UM.ReconAttrMap	1-22
1.6.2.5	Lookup.SAPUME.UM.ReconValidation	1-22
1.6.2.6	Lookup.SAPUME.UM.ReconTransformation	1-22
1.6.2.7	Lookup.SAPUME.UM.ProvValidation	1-23
1.6.2.8	Lookup.SAPUME.UM.SecurityPolicy	1-23
1.6.2.9	Lookup.SAPUME.UM.RoleChildformMappings	1-23
1.6.2.10	Lookup.SAPUME.UM.RoleDatasource	1-23
1.6.2.11	Lookup.SAPUME.UM.GroupDatasource	1-23
1.6.2.12	Lookup.SAPUME.UM.TimeZone	1-23
1.6.2.13	Lookup.SAPUME.UM.Lock	1-24
1.6.2.14	Lookup.SAPUME.UM.Locale	1-24
1.6.2.15	Lookup.SAPUME.UM.Country	1-24
1.6.2.16	Lookup.SAPUME.UM.Group	1-24
1.6.2.17	Lookup.SAPUME.UM.Role	1-24
1.6.2.18	Lookup Definitions for Exclusion Lists	1-24
1.6.3	Preconfigured Lookup Definitions for SAP BusinessObjects AC 10	1-25
1.6.3.1	Lookup.SAPAC10UME.Configuration	1-25
1.6.3.2	Lookup.SAPAC10UME.UM.Configuration	1-27
1.6.3.3	Lookup.SAPAC10UME.UM.ProvAttrMap	1-28
1.6.3.4	Lookup.SAPAC10UME.UM.ReconAttrMap	1-30
1.6.3.5	Lookup.SAPAC10UME.UM.ProvValidation	1-31
1.6.3.6	Lookup.SAPAC10UME.UM.ReconTransformation	1-31
1.6.3.7	Lookup.SAPAC10UME.UM.ReconValidation	1-31

1.6.3.8	Lookup.Lookup.SAPAC10UME.ItemProvAction	1-32
1.6.3.9	Lookup.SAPAC10UME.RequestType	1-32
1.7	Connector Objects Used During Reconciliation	1-32
1.7.1	User Attributes for Reconciliation	1-32
1.7.2	Reconciliation Rules	1-33
1.7.2.1	Reconciliation Rule	1-34
1.7.2.2	Viewing Reconciliation Rules in the Design Console	1-34
1.7.3	Reconciliation Action Rules	1-35
1.7.3.1	Reconciliation Action Rules for Reconciliation	1-36
1.7.3.2	Viewing Reconciliation Action Rules in the Design Console	1-36
1.8	Connector Objects Used During Provisioning	1-37
1.8.1	User Provisioning Functions	1-37
1.8.2	User Attributes for Provisioning	1-38
1.9	Roadmap for Deploying and Using the Connector	1-39

2 Deploying the Connector

2.1	Preinstallation	2-1
2.1.1	Creating a Target System User Account for Connector Operations	2-1
2.1.2	Installing and Configuring the Connector Server	2-2
2.1.3	Running the Connector Server	2-4
2.2	Installation	2-5
2.2.1	Installing the Connector in Oracle Identity Manager	2-5
2.2.2	Deploying the Connector Bundle in a Connector Server	2-7
2.3	Postinstallation	2-8
2.3.1	Configuring Oracle Identity Manager 11.1.2 or Later	2-9
2.3.1.1	Creating and Activating a Sandbox	2-9
2.3.1.2	Creating a New UI Form	2-9
2.3.1.3	Creating an Application Instance	2-9
2.3.1.4	Publishing a Sandbox	2-10
2.3.1.5	Harvesting Entitlements and Sync Catalog	2-10
2.3.1.6	Updating an Existing Application Instance with a New Form	2-10
2.3.2	Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later	2-11
2.3.3	Configuring Password Changes for Newly Created Accounts	2-12
2.3.4	Changing to the Required Input Locale	2-13
2.3.5	Clearing Content Related to Connector Resource Bundles from the Server Cache	2-13
2.3.6	Managing Logging	2-14
2.3.6.1	Understanding Log Levels	2-14
2.3.6.2	Enabling Logging	2-15
2.3.7	Setting Up the Lookup.SAPUME.UM.RoleDataSource Lookup Definition	2-17

2.3.7.1	Adding Role Data Source Names to the Lookup.SAPUME.UM.RoleDataSource lookup definition in Oracle Identity Manager Release 11.1.1.x	2-18
2.3.7.2	Adding Role Data Source Names to the Lookup.SAPUME.UM.RoleDataSource lookup definition in Oracle Identity Manager Release 11.1.2.x	2-18
2.3.8	Setting Up the Lookup.SAPUME.UM.GroupDataSource Lookup Definition	2-19
2.3.8.1	Adding Group Data Source Names to the Lookup.SAPUME.UM.GroupDataSource lookup definition in Oracle Identity Manager Release 11.1.1.x	2-20
2.3.8.2	Adding Group Data Source Names to the Lookup.SAPUME.UM.GroupDataSource lookup definition in Oracle Identity Manager Release 11.1.1.x	2-20
2.3.9	Setting Up the Lookup Definitions for Exclusion Lists	2-20
2.3.10	Configuring Oracle Identity Manager for Request-Based Provisioning	2-22
2.3.10.1	Importing Request Datasets Using Deployment Manager	2-23
2.3.10.2	Enabling the Auto Save Form Feature	2-23
2.3.10.3	Running the PurgeCache Utility	2-23
2.3.11	Configuring SSL to Secure Communication Between the Target System and Oracle Identity Manager	2-24
2.3.12	Configuring the IT Resource for the Target System	2-25
2.3.13	Configuring the IT Resource for the Connector Server	2-28
2.3.14	Configuring the Access Request Management Feature of the Connector	2-35
2.3.14.1	Specifying Values for the GRC UME-ITRes IT Resource	2-36
2.3.14.2	Configuring Request Types and Workflows on SAP BusinessObjects AC Access Request Management	2-37
2.3.15	Configuring SoD (Segregation of Duties)	2-37
2.3.15.1	Configuring SAP GRC to Act As the SoD Engine	2-38
2.3.15.2	Specifying Values for the GRC UME-ITRes IT Resource	2-38
2.3.15.3	Specifying a Value for the TopologyName IT Resource Parameter	2-38
2.3.15.4	Disabling and Enabling SoD	2-39
2.3.16	Downloading WSDL files from SAP BusinessObjects AC	2-40
2.3.17	Localizing Field Labels in UI Forms	2-41
2.3.18	Synchronizing the SAPUME Process Form and SAP AC UME Process Form with Target System Field Lengths	2-43
2.4	Upgrading the Connector	2-43
2.4.1	Prerequisites for Upgrading the Connector	2-43
2.4.2	Upgrading the Connector	2-44
2.4.3	Performing the Postupgrade Steps	2-44
2.4.3.1	Performing the Postupgrade Steps for Releases 9.x, 11.1.1.5.0, and 11.1.1.6.0 of the SAP User Management Engine Connector	2-45

2.4.3.2	Perform the Postupgrade Steps for Release 11.1.1.8.0 or later of the SAP User Management Engine Connector	2-45
---------	---	------

3 Using the Connector

3.1	Performing Full Reconciliation	3-1
3.2	Scheduled Job for Lookup Field Synchronization	3-1
3.3	Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization	3-3
3.4	Configuring Reconciliation	3-5
3.4.1	Full Reconciliation	3-5
3.4.2	Limited Reconciliation	3-5
3.4.3	Reconciliation Scheduled Jobs	3-6
3.4.3.1	SAP UME Target User Reconciliation and SAP AC UME Target User Reconciliation	3-7
3.4.3.2	SAP UME Target User Delete Reconciliation and SAP AC UME Target User Delete Reconciliation	3-7
3.4.3.3	SAP AC Request Status	3-8
3.5	Configuring Scheduled Jobs	3-9
3.6	Guidelines on Performing Provisioning	3-10
3.6.1	Guidelines While Performing Provisioning Operations in any of the supported deployment configurations	3-10
3.6.2	Guidelines While Performing Provisioning Operations After Configuring the Access Request Management Feature of the Connector	3-12
3.7	Configuring Provisioning in Oracle Identity Manager Release 11.1.1.x	3-13
3.7.1	Overview of the Provisioning Process in an SoD-Enabled Environment	3-14
3.7.2	Direct Provisioning	3-14
3.7.3	Direct Provisioning in an SoD-Enabled Environment	3-15
3.7.3.1	Prerequisites	3-16
3.7.3.2	Performing Direct Provisioning	3-16
3.7.4	Request-Based Provisioning	3-18
3.7.4.1	Creating of Request-Based Provisioning by the End User	3-18
3.7.4.2	Approving Request-Based Provisioning	3-19
3.7.5	Request-Based Provisioning in an SoD-Enabled Environment	3-20
3.7.5.1	Creating of Request-Based Provisioning by End-Users	3-20
3.7.5.2	Approving Request-Based Provisioning	3-21
3.7.6	Switching Between Request-Based Provisioning and Direct Provisioning	3-22
3.7.6.1	Switching from Request-Based Provisioning to Direct Provisioning	3-23
3.7.6.2	Switching from Direct Provisioning to Request-Based Provisioning	3-23
3.8	Configuring Provisioning in Oracle Identity Manager Release 11.1.2.x	3-24
3.9	Uninstalling the Connector	3-26

4 Extending the Functionality of the Connector

4.1	Determining the Names of Target System Attributes	4-1
4.2	Adding New Attributes for Reconciliation	4-2
4.2.1	Creating a New Version of the Process Form	4-2
4.2.2	Adding the New Attribute to the List of Reconciliation Field in the Resource Object	4-3
4.2.3	Creating a Reconciliation Field Mapping for the New Attribute	4-4
4.2.4	Creating an Entry for the Attribute in the Lookup Definition for Reconciliation	4-5
4.2.5	Defining the Connector	4-5
4.2.6	Creating a New UI Form to make the New Attribute Visible	4-6
4.3	Adding New Attributes for Provisioning	4-6
4.3.1	Creating a New Version of the Process Form	4-6
4.3.2	Creating an Entry for the Attribute in the Lookup Definition for Provisioning	4-8
4.3.3	Updating the Request Dataset	4-9
4.3.4	Running the PurgeCache Utility to Clear Content Related to Request Datasets	4-10
4.3.5	Importing the Modified Request Datasets Using the Deployment Manager	4-10
4.3.6	Updating the New Attribute for Provisioning a User	4-10
4.3.7	Defining the Connector	4-11
4.3.8	Creating a New UI Form to the Make the New Attribute Visible	4-11
4.4	Adding New Standard SAP BusinessObjects AC Access Request Management Attributes for Provisioning	4-11
4.4.1	Creating a New Version of the Process Form	4-12
4.4.2	Creating an Entry for the Attribute in the Lookup Definition	4-13
4.4.3	Creating a Process Task to Update the Attribute During Provisioning Operations	4-13
4.4.4	Creating a New UI Form and attaching it to the Application Instance to make the New Attribute Visible	4-15
4.5	Removing SAP BusinessObjects AC Access Request Management Attributes from Process Form	4-15
4.5.1	SAP BusinessObjects AC Access Request Management Attributes	4-16
4.6	Configuring Validation of Data During Reconciliation and Provisioning	4-17
4.7	Configuring Transformation of Data During User Reconciliation	4-19
4.8	Modifying Field Lengths on the Process Form	4-20
4.9	Configuring the Connector for Multiple Installations of the Target System	4-21
4.10	Defining the Connector	4-21

5 Known Issues, Limitations, and FAQs

5.1	Known Issues	5-1
-----	--------------	-----

5.2	Connector Limitations Related to Features of the Target System	5-2
5.2.1	Limitations for AS ABAP Data Source for the Connector	5-2
5.2.2	Limitations for Groups That Represent AS ABAP Roles	5-3
5.2.3	Limitations for Role Management with the Connector	5-3
5.3	Frequently Asked Questions (FAQs)	5-4

A Files and Directories in the Installation Package

B Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Index

List of Figures

1-1	Architecture of the Connector	1-5
1-2	Connector Integrating SAP BusinessObjects AC Access Request Management with Oracle Identity Manager and the Target System	1-7
1-3	Data Flow During the SoD Validation Process	1-10
1-4	Reconciliation Rule	1-35
1-5	Reconciliation Action Rules	1-37
2-1	Step 1: Provide IT Resource Information	2-29
2-2	Step 2: Specify IT Resource Parameter Values	2-30
2-3	Step 3: Set Access Permission to IT Resource	2-32
2-4	Step 4: Verify IT Resource Details	2-33
2-5	Step 5: IT Resource Connection Result	2-34
2-6	Step 6: IT Resource Created	2-35

List of Tables

1-1	Certified Components	1-2
1-2	Entries in the Lookup.SAPUME.Configuration Lookup Definition	1-20
1-3	Entries in the Lookup.SAPUME.UM.Configuration	1-21
1-4	Entries in the Lookup.SAPAC10UME.Configuration Lookup Definition	1-26
1-5	Entries in the Lookup.SAPAC10UME.UM.Configuration Lookup Definition	1-28
1-6	Entries in the Lookup.SAPAC10UME.UM.ProvAttrMap Lookup Definition	1-29
1-7	Entries in the Lookup.SAPAC10UME.ReconAttrMap Lookup Definition	1-30
1-8	Entries in the Lookup.SAPUME.UM.ReconAttrMap Lookup Definition	1-32
1-9	Action Rules for Reconciliation	1-36
1-10	User Provisioning Functions Supported by the SAP UME Connector	1-38
1-11	User Provisioning Functions Supported by the SAP AC UME Connector	1-38
1-12	Entries in the Lookup.SAPUME.UM.ProvAttrMap Lookup Definition	1-38
2-1	Log Levels and ODL Message Type:Level Combinations	2-15
2-2	Certificate Store Locations	2-24
2-3	Parameters of the SAP UME IT Resource	2-26
2-4	Parameters of the SAP AC UME IT Resource	2-27
2-5	Parameters of the IT Resource for the Connector Server	2-30
2-6	Parameters of the GRC UME-ITRes IT Resource	2-36
3-1	Attributes of the Scheduled Jobs for Lookup Field Synchronization	3-2
3-2	Attributes of the Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization	3-3
3-3	Attributes of the SAP UME Target User Reconciliation and SAP AC UME Target User Reconciliation Scheduled Jobs	3-7
3-4	Attributes of the SAP UME Target User Delete Reconciliation and SAP AC UME Target User Delete Reconciliation Scheduled Jobs	3-8
3-5	Attributes of the SAP AC Request Status Scheduled Job	3-8
A-1	Files and Directories in the Installation Package	A-1
B-1	Scheduled Tasks for Lookup Field Synchronization and Reconciliation	B-1

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that displays on the screen, or text that you enter.

What's New in This Guide?

This chapter provides an overview of the updates made to the software and documentation for the SAP User Management Engine connector in release 11.1.1.9.0.

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

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

Software Updates

The following sections discuss software updates:

- [Software Updates in Release 11.1.1.9.0](#)
- [Software Updates in Release 11.1.1.8.0](#)
- [Software Updates in Release 11.1.1.7.0](#)
- [Software Updates in Release 11.1.1.6.0](#)
- [Software Updates in Release 11.1.1.5.0](#)

Software Updates in Release 11.1.1.9.0

There are no software updates in release 11.1.1.9.0.

Software Updates in Release 11.1.1.8.0

The following are issues resolved in release 11.1.1.8.0:

Bug Number	Issue Description	Resolution
16506263	The task responses are displayed only in English even when the connector is configured for any other native language.	This issue has been resolved.

Bug Number	Issue Description	Resolution
13090423	<p>If a User has two roles in the target system and you perform a reconciliation operation, both the roles reflect on Oracle Identity Manager.</p> <p>If you unassign the two roles from the User in the target system and perform a reconciliation operation, then both the roles are not removed from the child form.</p>	This issue has been resolved.
12951484	If you try to stop a scheduled job when it is running in the Administrative and User Console, then the status of the scheduled job is displayed as INTERRUPT instead of STOPPED.	This issue has been resolved.
17748918	The default value of UD_SAPUME_IS_LOCK has been changed to NO instead of BLANK.	This issue has been resolved.
17401453	During User Reconciliation in SAP User Management Engine, two resource objects are created for a particular account in Oracle Identity Manager if the account id is in lowercase.	This issue has been resolved.
17288932	The "Error in processing WSDL document" issue occurs as there are no logs available within the SAP web dispatcher for the OIM "Create User" task.	<p>This issue has been resolved.</p> <p>In this release, the connector supports new connector configuration entries in the Lookup.SAPUME.AC53.Configuration lookup definition, which can also be used to configure SSL (Secure Socket Layer) for SAP GRC 5.3.</p>

Software Updates in Release 11.1.1.7.0

The following is the software update in release 11.1.1.7.0:

Support for SAP BusinessObjects Access Control Versions 5.3 and 10

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

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

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

Software Updates in Release 11.1.1.6.0

There are no software updates in release 11.1.1.6.0.

Software Updates in Release 11.1.1.5.0

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

- [Support for Identity Connector Framework](#)
- [Support for Deployment Using Connector Server](#)
- [Support for Multiple Data Sources](#)
- [Support for Remote Role Assignment in Federated Portal Network](#)
- [Support for Dependent Lookup Fields](#)
- [Transformation and Validation of Account Data](#)
- [Reconciliation of Deleted User Records](#)

Support for Identity Connector Framework

The Oracle Identity Manager Connector for SAP User Management Engine is an ICF-based connector.

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager and Oracle Waveset connectors require. The ICF also uses classpath isolation, which allows the SAP User Management Engine connector to co-exist with legacy versions of the connector.

See [Connector Architecture and Supported Deployment Configurations](#) for more information.

Support for Deployment Using Connector Server

In the earlier releases, the Enterprise Portal connector could be deployed in the machine on which Oracle Identity Manager was running. This release onward, you can deploy the SAP User Management Engine connector either locally in Oracle Identity Manager or remotely in the Connector Server.

See [Deploying the Connector Bundle in a Connector Server](#) for more information.

Support for Multiple Data Sources

The SAP User Management Engine connector can be configured and used for provisioning and reconciling user-related data to and from multiple data sources such as Lightweight Directory Access Protocol (LDAP) directories, system database of the SAP NetWeaver Application Server Java, and user management of an Application Server ABAP. In other words, this connector can be configured for performing user

management operations from user management engines irrespective of the data source configuration.

Support for Remote Role Assignment in Federated Portal Network

Federated Portal Network (FPN) allows organizations with multiple portals, SAP and non-SAP, to share content between independent portals. In FPN, the producers hold and run the applications. The consumer manages the redirect to producer portals. In FPN configuration, the content can be shared throughout the network using Remote Role Assignment content usage mode. It enables the consumer to assign roles offered by a producer. Connector can be configured to support Remote Role Assignment in FPN configuration.

Support for Dependent Lookup Fields

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

From this release onward, entries in lookup definitions are linked to the target system installation from which they are copied.

See [Lookup Definitions Synchronized with the Target System](#) for more information.

Transformation and Validation of Account Data

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

- [Configuring Transformation of Data During User Reconciliation](#)
- [Configuring Validation of Data During Reconciliation and Provisioning](#)

Reconciliation of Deleted User Records

You can configure the connector for reconciliation of deleted user records. If a record is deleted on the target system, then the corresponding SAP UME resource is revoked from the OIM User.

See [Reconciliation Scheduled Jobs](#) for more information about the scheduled job used for reconciling deleted user records.

Documentation-Specific Updates

The following sections discuss the documentation-specific updates:

- [Documentation-Specific Updates in Release 11.1.1.9.0](#)
- [Documentation-Specific Updates in Release 11.1.1.8.0](#)
- [Documentation-Specific Updates in Release 11.1.1.7.0](#)
- [Documentation-Specific Updates in Release 11.1.1.6.0](#)

- [Documentation-Specific Updates in Release 11.1.1.5.0](#)

Documentation-Specific Updates in Release 11.1.1.9.0

The following is a documentation-specific update in revision "12" of this guide:

The "Oracle Identity Governance or Oracle Identity Manager" row of [Table 1-1](#) has been updated.

The following are documentation-specific updates in revision "11" of this guide:

- A "Note" regarding entitlements has been added to [SoD Validation of Entitlement Requests](#).
- The "Oracle Identity Governance or Oracle Identity Manager" row of [Table 1-1](#) has been updated to include support for Oracle Identity Governance 12c (12.2.1.4.0).
- [Usage Recommendation](#) has been modified to include support for Oracle Identity Governance 12c (12.2.1.4.0).
- The description for the wsdFilePath code key has been modified in [Table 1-2](#) and [Table 1-4](#).

The following are documentation-specific updates in revision "10" of this guide:

- The following rows of [Table 1-1](#) have been modified:
 - The "Oracle Identity Governance" row has been updated to support 12c Release BP02 (12.2.1.3.2)
 - The "Target systems" row has been updated to include support for SAP NetWeaver 7.5
 - The "SAP Governance, Risk and Compliance Access Control (GRC AC)" row has been modified to include support for SAP NetWeaver AS ABAP 7.01 Support Pack 10 with EP RTA component GRPIEP SP 03 patch 10
- [Usage Recommendation](#) has been modified to include which version of SAP User Management Engine must be used if you are using 12c Release BP02 and NetWeaver 7.5 SPS 00 or later.
- [Known Issues](#) has been updated on the following issues and their respective workarounds:
- [Frequently Asked Questions \(FAQs\)](#) has been updated to include a question on whether the SAP UME AC connector provision attributes are mapped directly to SAP ECC system without GRC during a create user provisioning operation.
- [Frequently Asked Questions \(FAQs\)](#) has been updated on why SOD violation does not work in GRC 10.1 with 7.5 NW on Oracle Identity Manager 11.1.x.

The following documentation-specific update has been made in revision "9" of this guide:

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

The following are documentation-specific updates in revision "8" of this guide:

- OIM interface names have been corrected throughout the guide.
- [Preinstallation](#) has been restructured.

- Information pertaining to procedures performed on the target system has been replaced with a high-level summary in the following sections:
 - [Creating a Target System User Account for Connector Operations](#)
 - [Setting Up the Lookup.SAPUME.UM.RoleDataSource Lookup Definition](#)
 - [Setting Up the Lookup.SAPUME.UM.GroupDataSource Lookup Definition](#)
 - [Configuring Request Types and Workflows on SAP BusinessObjects AC Access Request Management](#)
 - [Downloading WSDL files from SAP BusinessObjects AC](#)

The following are documentation-specific updates in revision "7" of the guide:

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

Documentation-Specific Updates in Release 11.1.1.8.0

The following are documentation-specific updates in revision "6" of release 11.1.1.8.0:

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

The following is a documentation-specific update in revision "5" of release 11.1.1.8.0:

A "Note" has been added at the beginning of [Extending the Functionality of the Connector](#).

The following are documentation-specific updates in revision "4" of release 11.1.1.8.0:

- The "Connector Server" row has been added to [Table 1-1](#).
- In [Table 1-6](#), the following rows have been modified:
 - AC Request Id[WRITEBACK]
 - UniqueID
- [Synchronizing the SAPUME Process Form and SAP AC UME Process Form with Target System Field Lengths](#) has been added.
- [Performing the Postupgrade Steps](#) has been added.
- The connector version has been modified from "11.1.1.7.0" to "11.1.1.8.0" in Step 5.a of [Upgrading the Connector](#) .
- A note has been added to Step 3.d of Section 2.1.2.1, "Creating a Target System User Account for Connector Operations."

Documentation-Specific Updates in Release 11.1.1.7.0

The following is a documentation-specific update in revision "3" of release 11.1.1.7.0:

Step 3 of Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" has been modified.

The following are documentation-specific updates in revision "2" of release 11.1.1.7.0:

- The "Oracle Identity Manager" row in [Table 1-1](#) has been modified.
- A note has been added in the "xml/SAPUME-Datasets.xml" row of [Table A-1](#).
- The following sections have been added:
 - [Configuring Oracle Identity Manager 11.1.2 or Later](#)
 - [Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later](#)
 - [Localizing Field Labels in UI Forms](#)
- Instructions specific to Oracle Identity Manager release 11.1.2.x have been added in the following sections:
 - [Installing the Connector in Oracle Identity Manager](#)
 - [Configuring the IT Resource for the Target System](#)
 - [Configuring the IT Resource for the Connector Server](#)
 - [Configuring Scheduled Jobs](#)

Documentation-Specific Updates in Release 11.1.1.6.0

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 11.1.1.5.0

There are no documentation-specific updates in this release.

1

About the Connector

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

Note:

At some places in this guide, SAP User Management Engine has been referred to as the **target system**.

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

This chapter contains the following sections:

- [Certified Components](#)
- [Usage Recommendation](#)
- [Certified Languages](#)
- [Connector Architecture and Supported Deployment Configurations](#)
- [Features of the Connector](#)
- [Lookup Definitions Used During Connector Operations](#)
- [Connector Objects Used During Reconciliation](#)
- [Connector Objects Used During Provisioning](#)
- [Roadmap for Deploying and Using the Connector](#)

1.1 Certified Components

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

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

Table 1-1 Certified Components

Component	Requirement
Oracle Identity Governance or Oracle Identity Manager	<p>You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:</p> <ul style="list-style-type: none"> • Oracle Identity Governance 12c (12.2.1.4.0) • Oracle Identity Governance 12c Release BP02 (12.2.1.3.2) • Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) and any later BP in this release track • Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0) and any later BP in this release track • Oracle Identity Manager 11g Release 2 PS1 (11.1.2.1.0) and any later BP in this release track • Oracle Identity Manager 11g Release 2 BP05 (11.1.2.0.5) with patch 16627415 and any later BP in this release track • Oracle Identity Manager 11g Release 1 PS2 BP01 (11.1.1.7.1) and any later BP in this release track • Oracle Identity Manager 11g Release 1 PS1 BP07 (11.1.1.5.7) with patch 16627402 and any later BP in this release track
Target systems	<p>The target system can be one of the following:</p> <ul style="list-style-type: none"> • SAP User Management Engine running on SAP NetWeaver '04 SPS 14 or later • SAP User Management Engine running on SAP NetWeaver 7.0 SPS 05 or later • SAP User Management Engine running on SAP NetWeaver 7.4 SPS 08 or later • SAP User Management Engine running on SAP NetWeaver 7.5 SPS 00 or later <p>Note: If you install an SAP application in Java stack, such as SAP Enterprise Portal, then the connector can connect to SAP User Management Engine (UME) of the application.</p> <p>If you install an SAP application, such as SAP BW or SAP SRM, in ABAP stack, then you must configure SAP Enterprise Portal against SAP UME of the application. See the respective target system documentation for information about this configuration.</p> <p>If you install an SAP application, such as SAP PI, in dual stack (ABAP and Java), then the connector can connect to SAP UME of the application. However, the limitations of the ABAP data source are applicable.</p>
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 update 24 or later and JDK 1.7 or later, or JRockit 1.6 or later
SAP Governance, Risk and Compliance Access Control (GRC AC)	<p>If you want to configure and use the Access Risk Analysis or Access Request Management feature of this target system, then install the following:</p> <ul style="list-style-type: none"> • SAP BusinessObjects Access Control 10 on SAP NetWeaver AS ABAP 7.02 Support Pack 7 Install the GRCFND_A SP 10 component. • SAP BusinessObjects Access Control 10.1 on SAP NetWeaver AS ABAP 7.40 Support Pack 8 Install the GRCFND_A SP 10 component. • To use the connector with Java, ABAP, or LDAP data source, use SAP NetWeaver AS ABAP 7.01 Support Pack 10 with EP RTA component GRCPIEP SP 10 patch 2 (on deploying GRCAC1010_4-20007574.SCA) • To use the connector with Java, ABAP, or LDAP data source, use SAP NetWeaver AS ABAP 7.01 Support Pack 10 with EP RTA component GRCPIEP SP 10 patch 2 (on deploying GRCAC1010_4-20007574.SCA)
OpenSPML Toolkit	OpenSPML Toolkit version 0.6 (included with the connector bundle).

1.2 Usage Recommendation

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

 **Note:**

In Oracle Identity Manager, you can install and configure both SAP User Management and SAP User Management Engine connectors.

You can configure the connectors with SAP GRC AC target system to use either Access Risk Analysis or Access Request Management feature.

- If you are using an Oracle Identity Manager release 9.1.0.2 or later and earlier than Oracle Identity Manager 11g Release 1 PS1 BP07 (11.1.1.5.7), then you must use the 9.1.0 version of this connector.
- If you are using Oracle Identity Manager 11g Release 1 PS1 BP07 (11.1.1.5.7) and any later BP in this release track (such as Oracle Identity Manager 11g Release 1 PS1 BP08 (11.1.1.5.8) or later, or Oracle Identity Manager 11g Release 2 BP05 (11.1.2.0.5)), or Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.x version of this connector.
- If you are using Oracle Identity Governance releases 12c BP02 (12.2.1.3.2) or 12.2.1.4.0, then use the latest SAP User Management Engine 11.1.1.9.2 (one-off p28550151_111190_Generic.zip) version of this connector. However, if you are using SAP NetWeaver 7.5 SPS 00 or later and SAP GRC AC 10.1, then you must use the SAP User Management Engine 11.1.1.9.2 (one-off p28550151_111190_Generic.zip) version of this connector.

1.3 Certified Languages

These are the languages that the connector supports.

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

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

1.4 Connector Architecture and Supported Deployment Configurations

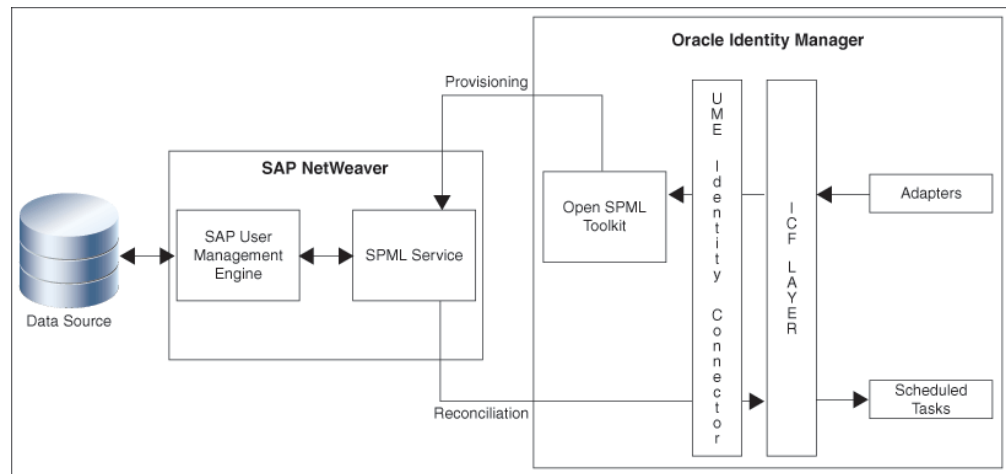
The SAP UME connector is implemented by using the Identity Connector Framework (ICF).

The connector sets up Oracle Identity Manager as the front end for sending account creation or modification requests to applications that use the data source linked with SAP User Management Engine.

Account data added or modified through provisioning operations performed directly on the data source can be reconciled into Oracle Identity Manager through SAP User Management Engine.

[Figure 1-1](#) shows the connector integrating SAP User Management Engine with Oracle Identity Manager.

Figure 1-1 Architecture of the Connector



As shown in the figure, SAP User Management Engine is configured as the management tool for user data stored on a data source, which is either the ABAP module, AS Java database, or an LDAP-based solution. User data changes made through the SAP User Management Engine UI are reflected on applications that use the data source or on the UI of the LDAP-based solution.

By deploying the connector, you configure SAP User Management Engine as a target resource of Oracle Identity Manager.

Provisioning requests sent from Oracle Identity Manager are routed through the SPML service to the application or system that uses the data source linked with SAP User Management Engine. User data changes resulting from the provisioning requests can be viewed through the SAP User Management Engine UI. Reconciliation is performed directly from SAP User Management Engine.

This connector can be configured to run in the account management mode. Account management is also known as target resource management. In the account management mode, the target system is used as a target resource. This mode of the connector enables the following operations:

- **Provisioning**
Provisioning involves creating or updating users on the target system through Oracle Identity Manager. When you allocate (or provision) an SAP User Management Engine resource to an OIM User, the operation results in the creation of an account on SAP UME for that user. In the Oracle Identity Manager context, the term **provisioning** is also used to mean updates made to the target system account through Oracle Identity Manager.

During provisioning, adapters carry provisioning data submitted through the process form to the target system. The SPML service in the SAP User Management Engine accepts provisioning data from the adapters, performs the necessary provisioning operation, and then returns the response to adapters in Oracle Identity Manager.
- **Reconciliation**
The scheduled task provided by the connector acts as the SPML client to send SPML requests to the SPML service in this application server.

During reconciliation, a scheduled task establishes a connection with the SPML service. Reconciliation criteria are sent through SPML requests to this SPML service. The SPML service processes the requests and returns SPML responses containing user records that match the reconciliation criteria. The scheduled task brings these records to Oracle Identity Manager.

Each record fetched from the target system is compared with SAP User Management Engine resources that are already provisioned to OIM Users. If a match is found, then the update made to the record is copied to the SAP User Management Engine resource in Oracle Identity Manager. If no match is found, then the user ID of the record is compared with the user ID of each OIM User. If a match is found, then data in the target system record is used to provision an SAP User Management Engine resource to the OIM User.

Besides enabling direct integration with the target system, the connector can also be used to act as an interface with the Access Risk Analysis and Access Request Management modules of SAP BusinessObjects AC. The target system (SAP R/3 or SAP CUA) and these two modules of SAP BusinessObjects AC together provide various deployment configurations. The following sections provide information about the supported deployment configurations of the connector:

- [User Management with Access Request Management](#)
- [Audit Trail Details in Connector Logs](#)
- [User Management with SoD](#)
- [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](#)

1.4.1 User Management with Access Request Management

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



Note:

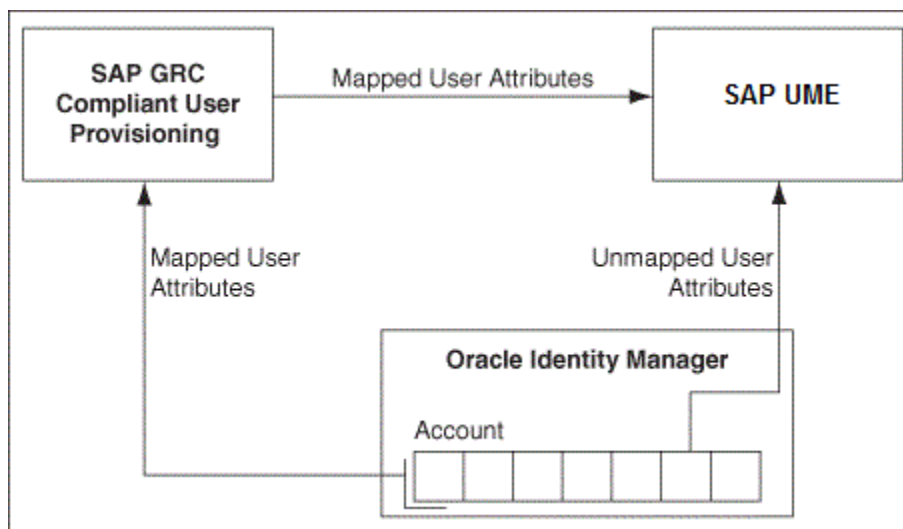
In this guide, the phrase **configuring Access Request Management** has been used to mean configuring the integration between Oracle Identity Manager and SAP BusinessObjects AC Access Request Management.

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

Reconciliation does not involve SAP BusinessObjects AC Access Request Management. Scheduled tasks on Oracle Identity Manager fetch data from the target system to Oracle Identity Manager.

Figure 1-2 shows data flow in this mode of the connector.

Figure 1-2 Connector Integrating SAP BusinessObjects AC Access Request Management with Oracle Identity Manager and the Target System



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

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

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

- GRAC_USER_ACCESS_WS: This Web service is used to submit requests.
- GRAC_REQUEST_STATUS_WS: This Web service is used to fetch request statuses.
- GRAC_AUDIT_LOGS_WS: This Web service is used to check if there are error messages in the SAP BusinessObjects AC Access Request Management logs.

The process form holds fields for both basic user management and Access Request Management. However, for a Create User operation, only the Access Request Management fields (attributes) on the process form are used. Mappings for these fields are stored in the Lookup.SAPAC10UME.UM.ProvAttrMap lookup definitions. If you specify values for any attribute that is not present in these lookup definitions, then the connector ignores those attributes during the Create User operation.

 **Note:**

SAP BusinessObjects AC Access Request Management does not process passwords. Therefore, any value entered in the Password field is ignored during Create User provisioning operations.

See [Guidelines on Performing Provisioning](#) for information about setting passwords when you configure Access Request Management.

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

 **Note:**

In a Modify User operation, you can specify values for attributes that are mapped with SAP BusinessObjects AC Access Request Management *and* attributes that are directly updated on the target system.

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

- If Access Request Management rejects the provisioning request, then the status of the request is set to Failed. Then, a message is recorded in the Oracle Identity Manager logs.
- If an error occurs during communication between Access Request Management and the target system, then the request remains in the Open state. A message stating that the operation has failed is recorded in the audit log associated with the request. An error message is displayed on the console.

1.4.2 Audit Trail Details in Connector Logs

You can capture the audit trail details in the connector logs after configuring the Access Request Management.

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

- **Create User**

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

- **Request Status Schedule Job**

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

- **Modify User**

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

1.4.3 User Management with SoD

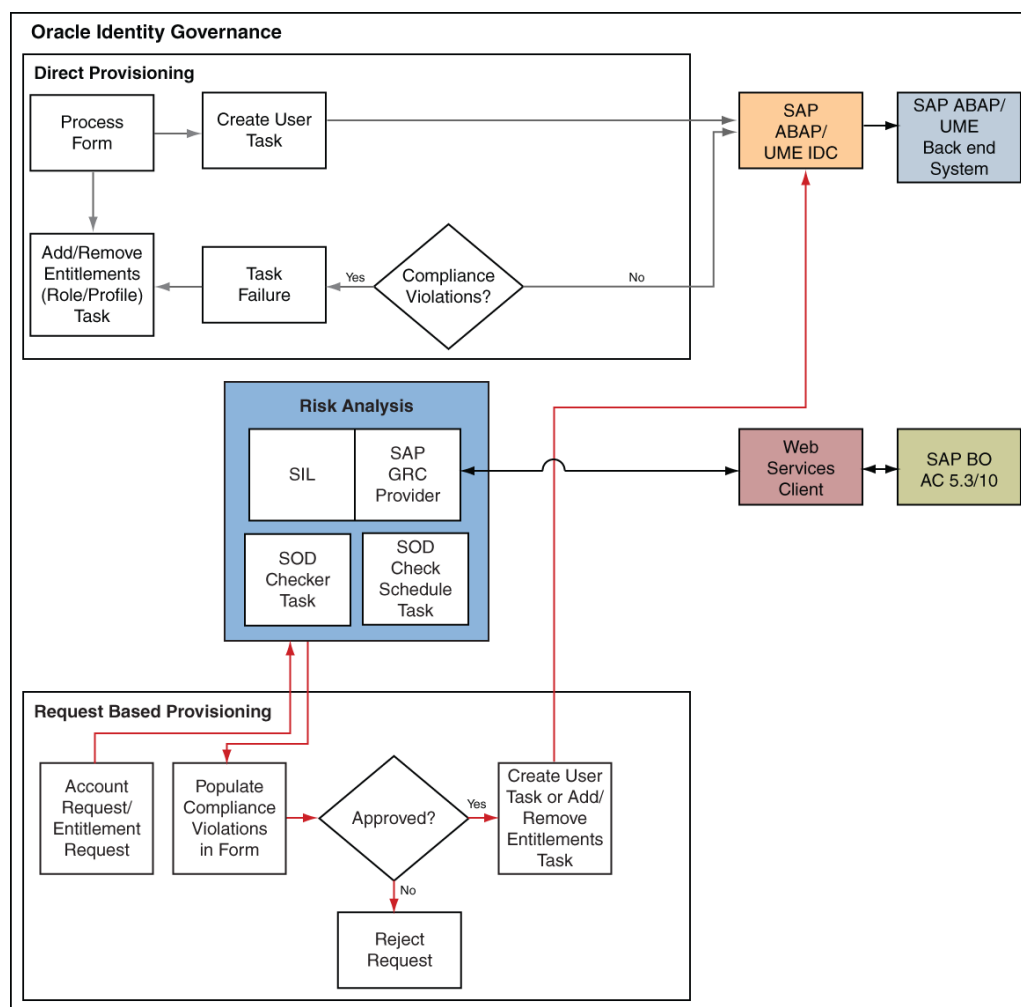
If the Access Risk Analysis module of SAP GRC is configured to implement segregation of duties (SoD) in your SAP operating environment, the connector can be used as the interface between Oracle Identity Governance and the SoD module. You can configure the connector to first process the provisioning requests sent from Oracle Identity Governance through SoD validation 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:

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.

1.4.4 User Management with Both SoD and Access Request Management

If both SAP GRC Access Risk Analysis and Access Request Management are configured in your SAP operating environment, then 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 discretely configured (that is, not linked) modules in your operating environment.

Note:

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

Summary of Account Management Process when SAP GRC Access Risk Analysis and SAP GRC Access Request Management are Enabled:

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.

1.4.5 Guidelines on Using a Deployment Configuration

These are the guidelines that you must apply while using a deployment configuration.

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

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

The following sections describe guidelines on the supported deployment configurations:

Note:

There are no special guidelines for the Basic User Management configuration and the User Management Engine with SoD configuration.

- [User Management Engine with SoD and Access Request Management](#)
- [Summary of Account Management Process when SAP BusinessObjects AC Access Risk Analysis and SAP BusinessObjects AC Access Request Management are Enabled](#)
- [User Management with Access Request Management](#)
- [Summary of Account Request Management when SAP BusinessObjects AC Access Request Management is Configured and Enabled in your SAP Operating Environment](#)

1.4.5.1 User Management Engine with SoD and Access Request Management

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

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

If a role or profile is provisioned on Oracle Identity Manager but rejected on SAP BusinessObjects AC Access Request Management, then the role or profile is revoked from Oracle Identity Manager at the end of the next user reconciliation

run. Therefore, you can have approval workflows defined for role provisioning requests on SAP BusinessObjects AC Access Request Management.

1.4.5.2 Summary of Account Management Process when SAP BusinessObjects AC Access Risk Analysis and SAP BusinessObjects AC Access Request Management are Enabled

Summary of the account management process:

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

1.4.5.3 User Management with Access Request Management

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

 **Note:**

SAP BusinessObjects AC Access Risk Analysis is either configured as a linked module of SAP BusinessObjects AC Access Request Management or it is not used at all.

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

The scenario described earlier in this section explains this guideline.

- Configure the Access Request Management feature of the connector.
- Do *not* configure the SoD feature of the connector.

1.4.5.4 Summary of Account Request Management when SAP BusinessObjects AC Access Request Management is Configured and Enabled in your SAP Operating Environment

Summary of the account management process:

1. Data from a provisioning operation on Oracle Identity Manager is sent to SAP BusinessObjects AC Access Request Management.

2. The workflow defined in SAP BusinessObjects AC Access Request Management sends the request to the SAP BusinessObjects AC Access Risk Analysis module for SoD validation.
3. After the SoD validation checks are cleared, the provisioning request is implemented on the target system.
4. Scheduled tasks run from Oracle Identity Manager reconcile the outcome of the operation from the target system into Oracle Identity Manager.

1.4.6 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 Manager in response to some provisioning operations. For example, if you assign multiple roles to a user in a particular provisioning operation, then one request is created and sent to Access Request Management for each role.
- For a particular account, Oracle Identity Manager keeps track of the latest request only. This means, for example, if more than one attribute of an account has been modified in separate provisioning operations, then Oracle Identity Manager keeps track of data related to the last operation only.
- A Modify User operation can involve changes to multiple process form fields or child form fields. For each field that is modified, one request is created and sent to SAP BusinessObjects AC Access Request Management. Only information about the last request sent to Access Request Management is stored in Oracle Identity Manager.
- Only parent or child form requests can be submitted in a single operation. You cannot submit both parent and child form requests at the same time.

1.5 Features of the Connector

The features of the connector include SoD validation of entitlement requests, full reconciliation, limited reconciliation and some additional features like support for multiple data sources, support for remoted role assignment in federated portal network and so on.

The following are features of the connector:

- [Routing of Provisioning Requests Through SAP BusinessObjects AC Access Request Management](#)
- [SoD Validation of Entitlement Requests](#)
- [Full Reconciliation](#)
- [Limited \(Filtered\) Reconciliation](#)
- [Enabling and Disabling Accounts](#)
- [Support for Multiple Data Sources](#)
- [Support for Remote Role Assignment in Federated Portal Network](#)
- [Transformation and Validation of Account Data](#)

- [Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations](#)
- [Support for Bulk Update of Attributes](#)

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

You can configure the connector to work with SAP BusinessObjects AC Access Request Management. See [User Management with Access Request Management](#) for detailed information about this feature.

1.5.2 SoD Validation of Entitlement Requests

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

- The SoD Invocation Library (SIL) is bundled with Oracle Identity Manager. The SIL acts as a pluggable integration interface with any SoD engine.
- The connector can be configured to work with SAP BusinessObjects AC as the SoD engine. To enable this, changes have been made in the approval and provisioning workflows of the connector.

Note:

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

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

- The SoD engine processes role 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.

1.5.3 Full Reconciliation



Note:

The SPML UME API does not return records for which the Last Modified Date value is greater than a specified date. Therefore, the connector cannot support incremental reconciliation. This point is also mentioned in [Connector Limitations Related to Features of the Target System](#).

In full reconciliation, all records are fetched from the target system to Oracle Identity Manager. During reconciliation, an SPML request is sent to the target system to fetch user accounts with user IDs that start with valid characters allowed in SAP. See the `logonNameInitialSubstring` entry in the [Table 2-3](#) for a list of all valid characters.

During full reconciliation, a single reconciliation event is generated for each target system account.

1.5.4 Limited (Filtered) Reconciliation

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

See [Limited Reconciliation](#) for more information.

1.5.5 Enabling and Disabling Accounts

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



Note:

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

1.5.6 Support for Multiple Data Sources

The SAP User Management Engine connector can be configured and used for provisioning and reconciling user-related data to and from multiple data sources such as Lightweight Directory Access Protocol (LDAP) directories, system database of the SAP NetWeaver Application Server Java, and user management of an Application Server ABAP. In other words, this connector can be configured for performing user management operations from user management engines irrespective of the data source configuration.

1.5.7 Support for Remote Role Assignment in Federated Portal Network

Federate Portal Network (FPN) allows organizations with multiple portals, SAP and non-SAP, to share content between independent portals. In FPN, the producers hold and run the applications. The consumer manages the redirect to producer portals. In FPN configuration, the content can be shared throughout the network using Remote Role Assignment content usage mode. It enables the consumer to assign roles offered by a producer. The SAP User Management Engine connector can be used to support Remote Role Assignment in FPN configuration.

1.5.8 Transformation and Validation of Account Data

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

- [Configuring Validation of Data During Reconciliation and Provisioning](#)
- [Configuring Transformation of Data During User Reconciliation](#)

1.5.9 Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations

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

[Lookup Definitions for Exclusion Lists](#) describes the lookup definitions where you specify the user IDs to be excluded during reconciliation and provisioning operations.

[Setting Up the Lookup Definitions for Exclusion Lists](#) describes the procedure to add entries in these lookup definitions.

1.5.10 Support for Bulk Update of Attributes

The connector supports the bulk update of attributes. That is, the connector allows you to update multiple attributes in one operation. With earlier connectors, you could update only one attribute at a time. However, if you specify an invalid value for any of the attributes, none of the attributes are updated. The entire update operation

is unsuccessful, and an error is returned. You must then correct any errors in the attribute values and repeat the bulk update operation.

1.6 Lookup Definitions Used During Connector Operations

Lookup definitions used during reconciliation and provisioning are preconfigured. Preconfigured lookup definitions are automatically created in Oracle Identity Manager after you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

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

- [Lookup Definitions Synchronized with the Target System](#)
- [Preconfigured Lookup Definitions](#)
- [Preconfigured Lookup Definitions for SAP BusinessObjects AC 10](#)

1.6.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Role lookup field to select a role from the list of roles defined on the target system. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are automatically created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.



Note:

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

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

- Lookup.SAPUME.UM.Group
- Lookup.SAPUME.UM.Role

The SAP UME Group Lookup Reconciliation or SAP UME Role Lookup Reconciliation scheduled jobs are used to synchronize values of these lookup definitions with the target system. [Scheduled Job for Lookup Field Synchronization](#) provides more information about these scheduled jobs.

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

- Code Key format: *IT_RESOURCE_KEY-LOOKUP_FIELD_ID*

In this format:

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

- *LOOKUP_FIELD_ID* is the target system code assigned to the lookup field entry, which is in the following format:

OBJ_CLASS_NAME.DATASOURCE_NAME.AUTO_GEN_VALUE

In this format:

OBJ_CLASS_NAME is the name of the object class. For groups, the object class name is GRUP. Similarly, the object class name for roles is ROLE.

DATASOURCE_NAME is name of the data source on the target system from which values are being fetched.

AUTO_GEN_VALUE is the auto generated value.

Sample value: 1~ROLE.UME_ROLE_PERSISTENCE.un:SAP_SLD_CONFIGURATOR

- Decode format: *IT_RESOURCE_NAME~LOOKUP_FIELD_ENTRY*

In this format:

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

Sample value: SAPUME IT Resource~Configurator role

While performing a provisioning operation on the Oracle Identity Self Service, 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. Because the IT resource key is part of each entry created in each lookup definition, only lookup field entries that are specific to the IT resource you select during a provisioning operation are displayed.

1.6.2 Preconfigured Lookup Definitions

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

- [Lookup.SAPUME.Configuration](#)
- [Lookup.SAPUME.UM.Configuration](#)
- [Lookup.SAPUME.UM.ProvAttrMap](#)
- [Lookup.SAPUME.UM.ReconAttrMap](#)
- [Lookup.SAPUME.UM.ReconValidation](#)
- [Lookup.SAPUME.UM.ReconTransformation](#)
- [Lookup.SAPUME.UM.ProvValidation](#)
- [Lookup.SAPUME.UM.SecurityPolicy](#)
- [Lookup.SAPUME.UM.RoleChildformMappings](#)
- [Lookup.SAPUME.UM.RoleDatasource](#)

- [Lookup.SAPUME.UM.GroupDatasource](#)
- [Lookup.SAPUME.UM.TimeZone](#)
- [Lookup.SAPUME.UM.Lock](#)
- [Lookup.SAPUME.UM.Locale](#)
- [Lookup.SAPUME.UM.Country](#)
- [Lookup.SAPUME.UM.Group](#)
- [Lookup.SAPUME.UM.Role](#)
- [Lookup Definitions for Exclusion Lists](#)

1.6.2.1 Lookup.SAPUME.Configuration

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

[Table 1-2](#) lists the default entries in this lookup definition.

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

Code Key	Decode	Description
Bundle Name	org.identityconnectors.sapume	This entry holds the name of the connector bundle package. Do not modify this entry.
Bundle Version	1.0.111100	This entry holds the version of the connector bundle class. Do not modify this entry.
Connector Name	org.identityconnectors.sapume.SAPUMEConnector	This entry holds the name of the connector class. Do not modify this entry.
entitlementRiskAnalysisAccessURL	None	This entry holds the WSDL URL for the Entitlement Risk Analysis web service.
entitlementRiskAnalysisWS	oracle.iam.grc.sod.scomp.impl.grcsap.util.webservice.sap.ac10.RiskAnalysisWithoutNo	Web service client to perform risk analysis without request number
Group attribute name	GROUPNAME	Name of the role duty type used in SIL
Group form names	UD_UME_GRP	List of all group child form names used during direct and request-based provisioning
RoleAttributeLabel	Role	Label name of the role ID field in the child form
Role attribute name	ROLENAME	Name of the role duty type used in SIL
Role form names	UD_UMERC_P;UD_UME_ROLE	List of all role child form names used during direct and request-based provisioning
SOD Configuration lookup	Lookup.SAPUME.Configuration	This entry holds the name of the lookup definition that contains SoD configuration properties.
SODSystemKey	None	Specify the name of the computer hosting the SAP UME connector from the Lookup.SAPUME.ReqInitSystem lookup definition.
User Configuration Lookup	Lookup.SAPUME.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do not modify this entry.

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

Code Key	Decode	Description
wsdIFilePath	<wsdl file directory>	Enter the absolute path of the directory containing the following file on your local machine: GRAC_RISK_ANALYSIS_WOUT_NO_WS.WSDL Note: If you are using a Connector Server, the WSDL File must be copied on the system running the Connector Server. The location of WSDL files are available on the local machine that is running the Connector Server.

1.6.2.2 Lookup.SAPUME.UM.Configuration

As discussed earlier, the Lookup.SAPUME.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations.

[Table 1-3](#) lists the default entries in this lookup definition.

Table 1-3 Entries in the Lookup.SAPUME.UM.Configuration

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

Table 1-3 (Cont.) Entries in the Lookup.SAPUME.UM.Configuration

Code Key	Decode	Description
Provisioning Exclusion List	Lookup.SAPUME.UM.ProvExclusionList	This entry is optional. You can enable exclusions during provisioning operations by adding this entry. This entry holds the name of the lookup definition that is used to specify exclusions during provisioning. See Lookup Definitions for Exclusion Lists for more information about adding entries in this lookup definition.
Recon Exclusion List	Lookup.SAPUME.UM.ReconExclusionList	This entry is optional. You can enable exclusions during reconciliation operations by adding this entry. This entry holds the name of the lookup definition that is used to specify exclusions during reconciliation. See Lookup Definitions for Exclusion Lists for more information about adding entries in this lookup definition.

1.6.2.3 Lookup.SAPUME.UM.ProvAttrMap

The Lookup.SAPUME.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during provisioning. This lookup definition is preconfigured. [Table 1-12](#) lists the default entries.

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

1.6.2.4 Lookup.SAPUME.UM.ReconAttrMap

The Lookup.SAPUME.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definitions is used during reconciliation. This lookup definition is preconfigured. [Table 1-8](#) lists the default entries.

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

1.6.2.5 Lookup.SAPUME.UM.ReconValidation

The Lookup.SAPUME.UM.ReconValidation lookup definition is used to configure validation of attribute values that are fetched from the target system during reconciliation. See [Configuring Validation of Data During Reconciliation and Provisioning](#) for more information about adding entries in this lookup definition.

1.6.2.6 Lookup.SAPUME.UM.ReconTransformation

The Lookup.SAPUME.UM.ReconnTransformation lookup definition is used to configure transformation of attribute values that are fetched from the target system

during user reconciliation. See [Configuring Transformation of Data During User Reconciliation](#) for more information about adding entries in this lookup definition.

1.6.2.7 Lookup.SAPUME.UM.ProvValidation

The Lookup.SAPUME.UM.ProvValidation lookup definition is used to configure validation of attribute values entered on the process form during provisioning operations. See [Configuring Validation of Data During Reconciliation and Provisioning](#) for more information about adding entries in this lookup definition.

1.6.2.8 Lookup.SAPUME.UM.SecurityPolicy

The Lookup.SAPUME.UM.SecurityPolicy lookup definition holds information about security policies that you can select for a user account that you create through Oracle Identity Manager. This lookup definition is preconfigured. You cannot add or modify entries in this lookup definition.

1.6.2.9 Lookup.SAPUME.UM.RoleChildformMappings

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

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

This lookup definition contains the following entries:

Code Key	Decode
UD_UMERC_P_DATASOURCE	UD_UME_ROLE_DATASOURCE
UD_UMERC_P_ROLENAME	UD_UME_ROLE_ROLENAME

1.6.2.10 Lookup.SAPUME.UM.RoleDatasource

The Lookup.SAPUME.UM.RoleDatasource lookup definition holds data source names of the role object class that you can select for a user account that you create through Oracle Identity Manager. See [Setting Up the Lookup.SAPUME.UM.RoleDataSource Lookup Definition](#) for more information.

1.6.2.11 Lookup.SAPUME.UM.GroupDatasource

The Lookup.SAPUME.UM.GroupDatasource lookup definition holds data source names of the group object class that you can select for a user account that you create through Oracle Identity Manager. See [Setting Up the Lookup.SAPUME.UM.GroupDataSource Lookup Definition](#) for more information.

1.6.2.12 Lookup.SAPUME.UM.TimeZone

The Lookup.SAPUME.UM.TimeZone lookup definition contains information about time zones that you can select for a user account that you create through Oracle Identity

Manager. This lookup definition is preconfigured. You cannot add or modify entries in this lookup definition.

1.6.2.13 Lookup.SAPUME.UM.Lock

The Lookup.SAPUME.UM.Lock lookup definition contains information about statuses (lock or unlock) that you can select for a user account that you create through Oracle Identity Manager. This lookup definition is preconfigured. You cannot add or modify entries in this lookup definition.

1.6.2.14 Lookup.SAPUME.UM.Locale

The Lookup.SAPUME.UM.Locale lookup definition contains information about locales that you can select for a user account that you create through Oracle Identity Manager.

1.6.2.15 Lookup.SAPUME.UM.Country

The Lookup.SAPUME.UM.Country lookup definition contains information about countries that you can select for a user account that you create through Oracle Identity Manager.

1.6.2.16 Lookup.SAPUME.UM.Group

The Lookup.SAPUME.UM.Group lookup contains information about the Groups. SAPUME Group Lookup Reconciliation scheduled job is used to synchronize values with the target system for this lookup.

1.6.2.17 Lookup.SAPUME.UM.Role

The Lookup.SAPUME.UM.Role lookup contains information about the Roles. SAPUME Role Lookup Reconciliation scheduled job is used to synchronize values with the target system for this lookup.

1.6.2.18 Lookup Definitions for Exclusion Lists

The Lookup.SAPUME.UM.ProvExclusionList and Lookup.SAPUME.UM.ReconExclusionList lookup definitions hold user IDs of target system accounts for which you do not want to perform provisioning and reconciliation operations, respectively.



Note:

The Lookup.SAPUME.UM.ProvExclusionList and Lookup.SAPUME.UM.ReconExclusionList lookup definitions are optional and do not exist by default.

You must add these lookups to the Lookup.SAPUME.UM.Configuration lookup definition to enable exclusions during provisioning and reconciliation operations. See [Lookup.SAPUME.UM.Configuration](#) for more information.

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

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

[Setting Up the Lookup Definitions for Exclusion Lists](#) describes the procedure to add entries in these lookup definitions.

1.6.3 Preconfigured Lookup Definitions for SAP BusinessObjects AC 10

This section discusses the lookup definitions for SAP BusinessObjects AC 10 that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

The lookup definitions are as follows:

- [Lookup.SAPAC10UME.Configuration](#)
- [Lookup.SAPAC10UME.UM.Configuration](#)
- [Lookup.SAPAC10UME.UM.ProvAttrMap](#)
- [Lookup.SAPAC10UME.UM.ReconAttrMap](#)
- [Lookup.SAPAC10UME.UM.ProvValidation](#)
- [Lookup.SAPAC10UME.UM.ReconTransformation](#)
- [Lookup.SAPAC10UME.UM.ReconValidation](#)
- [Lookup.Lookup.SAPAC10UME.ItemProvAction](#)
- [Lookup.SAPAC10UME.RequestType](#)

1.6.3.1 Lookup.SAPAC10UME.Configuration

The `Lookup.SAPAC10UME.Configuration` lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

[Table 1-4](#) lists the default entries in this lookup definition.

Table 1-4 Entries in the Lookup.SAPAC10UME.Configuration Lookup Definition

Code Key	Decode	Description
appLookupAccessURL	None	WSDL URL for Application Lookup web service
appLookupWS	oracle.iam.ws.sap.ac10.SelectApplication	Web service client to get all applications configured in SAP BusinessObjects AC
assignRoleReqType	002~Change Account~002~006	Name of the request type to be used for assign role request in SAP BusinessObjects AC
auditLogsAccessURL	None	WSDL URL for Audit Logs web service
auditLogsWS	oracle.iam.ws.sap.ac10.AuditLogs	Web service client to get audit logs
Bundle Name	org.identityconnectors.sapacume	Name of the connector bundle package
Bundle Version	1.0.111100	Version of the connector bundle class
Connector Name	org.identityconnectors.sapacume.SAPACUMConnector	Name of the connector class
ConnectorImplType	SAPUME	Enter this value to enable SAP UME roles in SOD
createUserReqType	001~New Account~001	Name of the request type to use for create user request in SAP BusinessObjects AC
deleteUserReqType	003~Delete Account~003	Name of the request type to use for delete user request in SAP BusinessObjects AC
ignoreOpenStatus	Yes	Specify whether new requests can be sent for a particular user, even if the last request for the user is in the Open status
lockUserReqType	004~Lock Account~004	Name of the request type to use for lock user request in SAP BusinessObjects AC
logAuditTrial	Yes	Specify whether complete audit trial needs to be logged whenever status request web service is invoked
modifyUserReqType	002~Change Account~002	Name of the request type to use for modify user request in SAP BusinessObjects AC
otherLookupAccessURL	None	WSDL URL for Other Lookup web service
otherLookupWS	oracle.iam.ws.sap.ac10.SearchLookup	Web service client to get other lookup field details
provActionAttrName	provAction;ReqLineItem	Name of the Provision Action target system attribute
provItemActionAttrName	provItemAction;ReqLineItem	Name of the Provision Item Action target system attribute
removeRoleReqType	002~Change Account~002~009	Name of the request type to use for remove user request in SAP BusinessObjects AC
requestStatusAccessURL	None	WSDL URL for Status Request web service

Table 1-4 (Cont.) Entries in the Lookup.SAPAC10UME.Configuration Lookup Definition

Code Key	Decode	Description
requestStatusValue	OK	This entry is used by the SAP UME AC Request Status schedule job to update status in the process form.
requestStatusWS	oracle.iam.ws.sap.ac10.RequestStatus	Web service client to get status of provisioning request
requestTypeAttrName	Reqtype;Header	Name of the request type attribute used to differentiate request flows from the SAPUMCREATE adapter
RiskLevel	High	In SAP BusinessObjects AC, each business risk is assigned a criticality level. You can control the risk analysis data returned by SAP BusinessObjects by specifying a risk level.
roleLookupAccessURL	None	WSDL URL for Role Lookup web service
roleLookupWS	oracle.iam.ws.sap.ac10.SearchRoles	Web service client to get all roles
Status Configuration	Lookup.SAPACUME.Status.Configuration	Status Configuration.
unlockUserReqType	005~unlock user~005	Name of the request type to use for unlock user request in SAP BusinessObjects AC
userAccessAccessURL	None	WSDL URL for User Access web service
userAccessWS	oracle.iam.ws.sap.ac10.UserAccess	Web service client to get status of user access
User Configuration Lookup	Lookup.SAPAC10UME.UM.Configuration	Name of the lookup definition that contains user-specific configuration properties
wsdlFilePath	WSDL file directory	Enter the absolute path of the directory containing the following files on your local machine: <ul style="list-style-type: none"> • GRAC_AUDIT_LOGS_WS • GRAC_LOOKUP_WS • GRAC_REQUEST_STATUS_WS • GRAC_SELECT_APPL_WS • GRAC_USER_ACCESS_WS Note: If you are using a Connector Server, the WSDL File must be copied on the system running the Connector Server. The location of WSDL files are available on the local machine that is running the Connector Server.

1.6.3.2 Lookup.SAPAC10UME.UM.Configuration

The Lookup.SAPAC10UME.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a target resource.

Table 1-5 lists the default entries in this lookup definition.

Table 1-5 Entries in the Lookup.SAPAC10UME.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.SAPAC10UME.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.SAPAC10UME.UM.ProvAttrMap for more information about this lookup definition.
Provisioning Validation Lookup	Lookup.SAPAC10UME.UM.ProvValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.
Recon Attribute Map	Lookup.SAPAC10UME.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.SAPAC10UME.UM.ReconAttrMap for more information about this lookup definition.
Recon Transformation Lookup	Lookup.SAPAC10UME.UM.ReconTransformation	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user Reconciliation. See Configuring Transformation of Data During User Reconciliation for more information about adding entries in this lookup definition.
Recon Validation Lookup	Lookup.SAPAC10UME.UM.ReconValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the Target system during reconciliation. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

1.6.3.3 Lookup.SAPAC10UME.UM.ProvAttrMap

The Lookup.SAPAC10UME.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during provisioning. This lookup definition is preconfigured. Table 1-6 lists the default entries.

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

Table 1-6 Entries in the Lookup.SAPAC10UME.UM.ProvAttrMap Lookup Definition

Code Key	Decode
AC Business Process[Lookup]	bproc;Header
Accounting Number	accno;UserInfo
AC Functional Area[Lookup]	funcarea;Header
AC Manager	manager;UserInfo
AC Manager email	managerEmail;UserInfo
AC Manager First Name	managerFirstname;UserInfo
AC Manager Last Name	managerLastname;UserInfo
AC Priority[Lookup]	priority;Header
AC Request Due Date[Date]	reqDueDate;Header
AC Request Id[WRITEBACK]	RequestId
AC Requestor email	email;Header
AC Requestor ID	requestorId;Header
AC Request Reason	requestReason;Header
AC Request Status[WRITEBACK]	RequestStatus
AC Request Type[WRITEBACK]	RequestType
AC System[Lookup]	reqInitSystem;Header
City	city
Country	country
Department	department;UserInfo
E-Mail Address	email;UserInfo
End Date of Account Validity[Date]	validTo;UserInfo
Fax	fax;UserInfo
First Name	fname;UserInfo
Form of Address	personnelarea;UserInfo
Language	logonLang;UserInfo
Last Name	lname;UserInfo
Logon Name	userId;UserInfo
Mobile	personnelno;UserInfo
Name	displayname
Password	__PASSWORD__
Position	emposition;UserInfo
Security Policy	securitypolicy

Table 1-6 (Cont.) Entries in the Lookup.SAPAC10UME.UM.ProvAttrMap Lookup Definition

Code Key	Decode
Start Date of Account Validity[Date]	validFrom;UserInfo
State	state
Street	streetaddress
Telephone	telnumber;UserInfo
Time Zone	timezone
Title	title;UserInfo
UD_ACUMEGRP~Group[Lookup]	itemName;ReqLineItem
UD_ACUMEROL~Role[Lookup]	itemName;ReqLineItem
UniqueID	__UID__
User Account Locked	userLock;None
Zip	zip

1.6.3.4 Lookup.SAPAC10UME.UM.ReconAttrMap

The Lookup.SAPAC10UME.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured. [Table 1-7](#) lists the default entries.

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

Table 1-7 Entries in the Lookup.SAPAC10UME.ReconAttrMap Lookup Definition

Code Key	Decode
City	city
Country	country
Department	department
E-Mail Address	email
End Date of Account Validity[Date]	validto
Fax	fax
First Name	firstname
Form of Address	salutation
Groups~Group[Lookup]	assignedgroups
Language	locale

Table 1-7 (Cont.) Entries in the Lookup.SAPAC10UME.ReconAttrMap Lookup Definition

Code Key	Decode
Last Name	lastname
Logon Name	logonname
Mobile	mobile
Name	displayname
Position	jobtitle
Roles~Role[Lookup]	assignedroles
Security Policy	securitypolicy
Start Date of Account Validity[Date]	validfrom
State	state
Status	__ENABLE__
Street	streetaddress
Telephone	telephone
Time Zone	timezone
Title	title
UniqueID	id
User Account Locked	islocked
Zip	zip

1.6.3.5 Lookup.SAPAC10UME.UM.ProvValidation

The Lookup.SAPAC10UME.UM.ProvValidation lookup definition is used to configure validation of attribute values entered on the process form during provisioning operations. See [Configuring Validation of Data During Reconciliation and Provisioning](#) for more information.

1.6.3.6 Lookup.SAPAC10UME.UM.ReconTransformation

The Lookup.SAPAC10UME.UM.ReconTransformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See [Configuring Transformation of Data During User Reconciliation](#) for more information about adding entries in this lookup definition

1.6.3.7 Lookup.SAPAC10UME.UM.ReconValidation

The Lookup.SAPAC10UME.UM.ReconValidationlookup definition is used to configure validation of attribute values that are fetched from the target system during reconciliation. See [Configuring Validation of Data During Reconciliation and Provisioning](#) for more information about adding entries in this lookup definition

1.6.3.8 Lookup.Lookup.SAPAC10UME.ItemProvAction

The Lookup.SAPAC10UME.ItemProvAction is used to obtain the request type from the GRC system using the web service, when scheduler job get executed then, ItemProvAction lookup is populated.

1.6.3.9 Lookup.SAPAC10UME.RequestType

The Lookup.SAPAC10UME.ItemProvAction is used to obtain request type from the GRC system using the web service, when scheduler job get executed then ItemProvAction lookup is populated.

1.7 Connector Objects Used During Reconciliation

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

The SAP UME User Recon scheduled task is used to initiate a reconciliation run. This scheduled task is discussed in [Reconciliation Scheduled Jobs](#).



See Also:

Managing Reconciliation of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for conceptual information about reconciliation

This section discusses the following topics:

- [User Attributes for Reconciliation](#)
- [Reconciliation Rules](#)
- [Reconciliation Action Rules](#)

1.7.1 User Attributes for Reconciliation

The Lookup.SAPUME.UM.ReconAttrMap lookup definition maps resource object fields and target system attributes. This lookup definition is used for performing target resource user reconciliation runs.

[Table 1-8](#) lists entries in this lookup definition.

Table 1-8 Entries in the Lookup.SAPUME.UM.ReconAttrMap Lookup Definition

Resource Object Field (Code Key)	Target System Attribute (Decode)
City	city
Country	country
Department	department

Table 1-8 (Cont.) Entries in the Lookup.SAPUME.UM.ReconAttrMap Lookup Definition

Resource Object Field (Code Key)	Target System Attribute (Decode)
E-Mail Address	email
End Date of Account Validity[Date]	validto
Fax	fax
First Name	firstname
Form of Address	salutation
Groups~Group[Lookup]	assignedgroups
Language	locale
Last Name	lastname
Logon Name	logonname
Mobile	mobile
Name	displayname
Position	jobtitle
Roles~Role[Lookup]	assignedroles
Security Policy	securitypolicy
Start Date of Account Validity[Date]	validfrom
State	state
Status	__ENABLE__
Street	streetaddress
Telephone	telephone
Time Zone	timezone
Title	title
Unique Id	id
User Account Locked	islocked
Zip	zip

1.7.2 Reconciliation Rules

Reconciliation rules are automatically created when you generate the SAP UME connector.

See Also:

Reconciliation Engine of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for generic information about reconciliation matching and action rules

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

- [Reconciliation Rule](#)
- [Viewing Reconciliation Rules in the Design Console](#)

1.7.2.1 Reconciliation Rule

The following is the process-matching rule:

Rule name: SAPUME Recon Rule

Rule element: User Login Equals Logon Name



Note:

Perform the following procedure only after the connector is deployed. If you are using SAP BusinessObjects AC system, see the following rule:

- **Rule name:** SAP AC UME Recon Rule
- **Rule element:** User Login Equals Logon Name

In this rule element:

- User Login is the User ID field of the OIM User form.
- Logon Name is the logonname of the SAP account.

1.7.2.2 Viewing Reconciliation Rules in the Design Console

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



Note:

Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for and open the **SAPUME Recon Rule** rule.



Note:

If you are using SAP BusinessObjects AC system. Search for and open the SAP AC UME Recon Rule rule.

Figure 1-4 shows this reconciliation rule.

Figure 1-4 Reconciliation Rule

Reconciliation Rule Builder

Name: SAPUME Recon Rule

Object: SAPUME Resource Object

Description: SAP UME Recon Rule

Operator: AND OR

Valid Active

For User For Organization

Rule Elements

Rule Definition

Add Rule

Add Rule Element

Delete

Legend

Rule: SAPUME Recon Rule

- User Login Equals Logon Name

1.7.3 Reconciliation Action Rules

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

 **Note:**

No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See

- [Setting a Reconciliation Action Rule \(Developing Identity Connectors using Java\)](#)
- [Setting a Reconciliation Action Rule \(Developing Identity Connectors using .net\)](#)

in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about setting a reconciliation action rule.

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

- [Reconciliation Action Rules for Reconciliation](#)
- [Viewing Reconciliation Action Rules in the Design Console](#)

1.7.3.1 Reconciliation Action Rules for Reconciliation

[Table 1-9](#) lists the action rules for reconciliation.

Table 1-9 Action Rules for Reconciliation

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

1.7.3.2 Viewing Reconciliation Action Rules in the Design Console

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. If you want to view the reconciliation action rules for reconciliation, then search for and open the **SAPUME Resource Object** resource object.

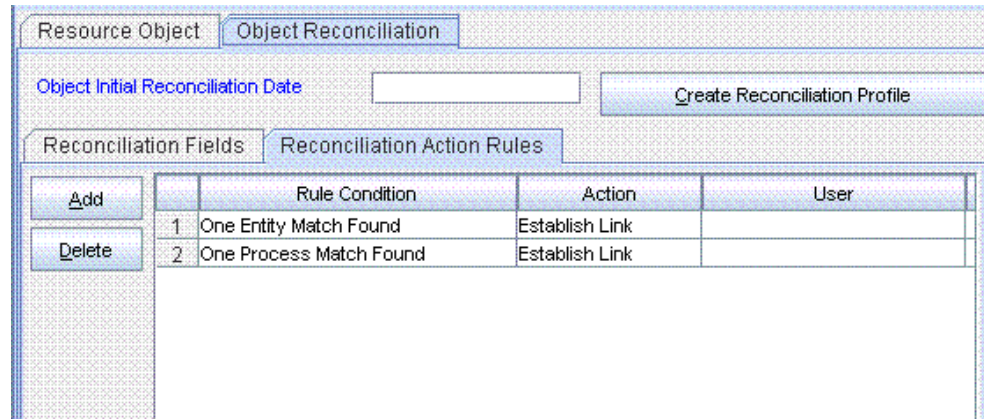
 **Note:**

If you are using SAP BusinessObjects AC system.

If you want to view the reconciliation action rules for reconciliation, then search for and open the **SAP AC UME Resource Object** resource object.

4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. [Figure 1-5](#) shows the reconciliation action rules for reconciliation.

Figure 1-5 Reconciliation Action Rules



1.8 Connector Objects Used During Provisioning

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

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

See Also:

Managing Provisioning Tasks of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for conceptual information about provisioning

This section discusses the following topics:

- [User Provisioning Functions](#)
- [User Attributes for Provisioning](#)

1.8.1 User Provisioning Functions

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

[Table 1-10](#) and [Table 1-12](#) list the user provisioning functions supported by the SAP UME and SAP AC UME connectors, and the adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.

Table 1-10 User Provisioning Functions Supported by the SAP UME Connector

Function	Adapter
Create a user account	adpSAPUMECREATE
Modify a user account	adpSAPUMEUPDATE
Delete a user account	adpSAPUMEDELETE
Enable a user account	adpSAPUMEENABLE
Disable a user account	adpSAPUMEDISABLE
Add multivalued attribute	adpSAPUMEADDCHILD
Prepopulates the SAPUME Form	adpPREPOPULATESAPUMEFORM
Remove multivalued attribute	adpSAPUMEREMOVECHILD
SAPUME request ENTITLEMENT	adpSAPUMEREQUESTENTITLEMENT
Updates the SAPUME	adpSAPUMEUPDATE
Child SAPUME update	adpSAPUMEUPDATECHILD
Initiates the SODCheck	InitiateSODCheck

Table 1-11 User Provisioning Functions Supported by the SAP AC UME Connector

Function	Adapter
Create a user account	adpSAPACUMCREATEUSER
Modify a user account	adpSAPACUMEUPDATE
Delete a user account	adpSAPACUMEDELETE
Enable a user account	adpSAPACUMEENABLE
Disable a user account	adpSAPACUMEDISABLE
Add multivalued attribute	adpSAPACUMEADDCHILD
Remove multivalued attribute	adpSAPACUMEREMOVECHILD
Prepopulates the SAPACUME	adpPREPOPULATESAPACUME

1.8.2 User Attributes for Provisioning

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

The Lookup.SAPUME.UM.ProvAttrMap lookup definition maps process form fields with target system attributes. This lookup definition is used for performing provisioning operations.

[Table 1-12](#) lists the default entries in this lookup definition.

Table 1-12 Entries in the Lookup.SAPUME.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Attribute
Single-Valued Fields	

Table 1-12 (Cont.) Entries in the Lookup.SAPUME.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Attribute
City	city
Country	country
Department	department
E-Mail Address	email
End Date of Account Validity[Date]	validto
Fax	fax
First Name	firstname
Language	locale
Last Name	lastname
Logon Name	__NAME__
Mobile	mobile
Name	displayname
Password	__PASSWORD__
Position	jobtitle
Security Policy	securitypolicy
Start Date of Account Validity[Date]	validfrom
State	state
Street	streetaddress
Telephone	telephone
Time Zone	timezone
Title	title
Unique ID	__UID__
User Account Locked	islocked
Zip	zip
Multivalued Fields	
UD_UME_GRP~Group[Lookup]	assignedgroups
UD_UME_ROLE~Role[Lookup]	assignedroles

1.9 Roadmap for Deploying and Using the Connector

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

- [Deploying the Connector](#) describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- [Using the Connector](#) describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- [Extending the Functionality of the Connector](#) describes procedures that you can perform if you want to extend the functionality of the connector.

- [Known Issues, Limitations, and FAQs](#) lists known issues, limitations, and FAQs associated with this release of the connector.
- [Files and Directories in the Installation Package](#) provides information about files and directories on the installation media.
- [Scheduled Jobs for Lookup Field Synchronization and Reconciliation](#) provides information about scheduled jobs for lookup field synchronization and reconciliation.

2

Deploying the Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, and postinstallation.

The following topics provide details on these stages:

- [Preinstallation](#)
- [Installation](#)
- [Postinstallation](#)
- [Upgrading the Connector](#)

2.1 Preinstallation

Preinstallation involves creating a target system user account for connector operations.

Preinstallation information is divided across the following sections:

- [Creating a Target System User Account for Connector Operations](#)
- [Installing and Configuring the Connector Server](#)
- [Running the Connector Server](#)

2.1.1 Creating a Target System User Account for Connector Operations

The connector uses a target system account to connect to and perform operations on the target system.

To create this target system account:

1. Create a technical user account in the target system and assign it a role with the **Spml_Read_Action** and **Spml_Write_Action** actions.
2. If the target system is configured with JAVA data source by default, then assign the following roles:
 - NWA_SUPERADMIN
 - MY_SPML_FULL_ACCESS_ROLE

 **Note:**

If target system Netweaver 7.3 is configured with JAVA data source by default and if JAVA Data source is used for Admin User, then assign the following roles:

- Administrator
- Super Administration
- MY_SPML_FULL_ACCESS_ROLE

3. If the target system is configured with ABAP data source, then assign the SAP_J2EE_ADMIN group.
4. If this connector is configured with the ABAP data source and CUA is enabled in the backend ABAP application, then assign a system to the user account created earlier.
5. If you want to perform connector operations such as Access Request Management and Access Risk Analysis through an SAP Business Objects Access Control system, then assign the following minimum set of roles to a user account in SAP Business Objects Access Control:

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

For detailed information on each of these preinstallation tasks, refer to the SAP documentation.

2.1.2 Installing and Configuring the Connector Server

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

Connector servers are available in two implementations:

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

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

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

 **Note:**

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

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

 **Note:**

In this guide, `CONNECTOR_SERVER_HOME` represents this directory.

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

Property	Description
<code>connectorserver.port</code>	Port on which the Java Connector Server listens for requests. Default is: 8759.
<code>connectorserver.bundleDir</code>	Directory where the connector bundles are deployed. Default is: <code>bundles</code> .
<code>connectorserver.libDir</code>	Directory in which to place dependent libraries. Default is: <code>lib</code> .
<code>connectorserver.usessl</code>	If set to <code>true</code> , the Java Connector Server uses SSL for secure communication. Default is: <code>false</code> . If you specify <code>true</code> , use the following options on the command line when you start the Java Connector Server: <ul style="list-style-type: none"> • <code>-Djavax.net.ssl.keyStore</code> • <code>-Djavax.net.ssl.keyStoreType</code> (<i>optional</i>) • <code>-Djavax.net.ssl.keyStorePassword</code>
<code>connectorserver.ifaddress</code>	Bind address. To set this property, uncomment it in the file (if necessary). The bind address can be useful if there are more NICs installed on the computer.
<code>connectorserver.key</code>	Java Connector Server key.

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

 **Note:**

For more information, see [Running the Connector Server](#).

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

 **Note:**

Oracle Identity Manager has no built-in support for connector servers, so you cannot test your configuration.

2.1.3 Running the Connector Server

When you run the Connector Installer, it automatically copies the connector files to directories in Oracle Identity Manager, imports connector XML files, and compiles adapters used for provisioning.

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

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in [Installing and Configuring the Connector Server](#).
2. Change to the `CONNECTOR_SERVER_HOME\bin` directory and find the ConnectorServer.bat script.

The ConnectorServer.bat supports the following options:

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

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

2.2 Installation

You can run the connector code either locally in Oracle Identity Manager or remotely in a Connector Server.

Depending on where you want to run the connector code (bundle), the connector provides the following installation options:

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

2.2.1 Installing the Connector in Oracle Identity Manager

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

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

 **Note:**

In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

OIM_HOME/server/ConnectorDefaultDirectory

2. If you are using Oracle Identity Manager release 11.1.1.x, then perform the following steps:
 - a. Log in to the Administrative and User Console.
 - b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector**.
3. If you are using Oracle Identity Manager release 11.1.2.x, then perform the following steps:
 - a. Log in to Oracle Identity System Administration.
 - b. In the left pane, under System Management, click **Manage Connector**.
4. In the Manage Connector page, click **Install**.
5. From the Connector List list, select **SAP UME Connector RELEASE_NUMBER**.

 **Note:**

If you are using SAP BusinessObjects AC system, from the Connector List list, select **SAPACUME Connector RELEASE_NUMBER**.

This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

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

- a. In the **Alternative Directory** field, enter the full path and name of that directory.
- b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
- c. From the Connector List list, select **SAP UME Connector RELEASE_NUMBER**.

 **Note:**

If you are using SAP BusinessObjects AC system, from the Connector List list, select **SAPACUME Connector RELEASE_NUMBER**.

6. Click **Load**.
7. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

- a. Configuration of connector libraries
- b. Import of the connector XML files (by using the Deployment Manager)
- c. Compilation of adapters

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

- Retry the installation by clicking **Retry**.
 - Cancel the installation and begin again from Step 1.
8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:
 - a. Ensuring that the prerequisites for using the connector are addressed

 **Note:**

At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See [Clearing Content Related to Connector Resource Bundles from the Server Cache](#) for information about running the PurgeCache utility.

There are no prerequisites for some predefined connectors.

b. Configuring the IT resource for the connector

Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

c. Configuring the scheduled tasks that are created when you installed the connector

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in [Table A-1](#).

2.2.2 Deploying the Connector Bundle in a Connector Server

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

To deploy the connector bundle remotely in a Connector Server, you must first deploy the connector in Oracle Identity Manager, as described in [Installing the Connector in Oracle Identity Manager](#).

 **Note:**

- You can download the Connector Server from the Oracle Technology Network web page.
- See [Configuring the IT Resource for the Connector Server](#) for related information.
- See *Using an Identity Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about installing, configuring, and running the Connector Server.

To install the connector into the Connector Server:

1. Stop the Connector Server.

 **Note:**

You can download the necessary Java Connector Server from the Oracle Technology Network web page.

2. Copy the SAP UME connector bundle into the `CONNECTOR_SERVER_HOME/bundles` directory.
3. Start the Connector Server. See [Running the Connector Server](#) for information about starting the Connector Server.

 **Note:**

If you are using a Connector Server, the WSDL File must be copied on the system running the Connector Server. Location of the WSDL files is available in the local machine that is running the Connector Server.

You can download the necessary Java Connector Server from the Oracle Technology Network web page.

2.3 Postinstallation

Postinstallation for the connector involves configuring Oracle Identity Manager, enabling logging to track information about all connector events, and configuring SSL. It also involves performing some optional configurations such as enabling the reset password option, configuring password changes for newly created accounts, setting up lookup definitions for exclusion lists and so on.

Postinstallation steps are divided across the following sections:

- [Configuring Oracle Identity Manager 11.1.2 or Later](#)
- [Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later](#)
- [Configuring Password Changes for Newly Created Accounts](#)
- [Changing to the Required Input Locale](#)
- [Clearing Content Related to Connector Resource Bundles from the Server Cache](#)
- [Managing Logging](#)
- [Setting Up the Lookup.SAPUME.UM.RoleDataSource Lookup Definition](#)
- [Setting Up the Lookup.SAPUME.UM.GroupDataSource Lookup Definition](#)
- [Setting Up the Lookup Definitions for Exclusion Lists](#)
- [Configuring Oracle Identity Manager for Request-Based Provisioning](#)
- [Configuring SSL to Secure Communication Between the Target System and Oracle Identity Manager](#)
- [Configuring the IT Resource for the Target System](#)
- [Configuring the IT Resource for the Connector Server](#)

- [Configuring the Access Request Management Feature of the Connector](#)
- [Configuring SoD \(Segregation of Duties\)](#)
- [Downloading WSDL files from SAP BusinessObjects AC](#)
- [Localizing Field Labels in UI Forms](#)
- [Synchronizing the SAPUME Process Form and SAP AC UME Process Form with Target System Field Lengths](#)

2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later

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

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

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

2.3.1.1 Creating and Activating a Sandbox

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

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

2.3.1.2 Creating a New UI Form

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

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

2.3.1.3 Creating an Application Instance

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

1. In the System Administration page, under Configuration in the left pane, click **Application Instances**.
2. Under Search Results, click **Create**.
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save**.
4. In the Form drop-down list, select the newly created form and click **Apply**.
5. Publish the application instance for a particular organization.

2.3.1.4 Publishing a Sandbox

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

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

2.3.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

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

2.3.1.6 Updating an Existing Application Instance with a New Form

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

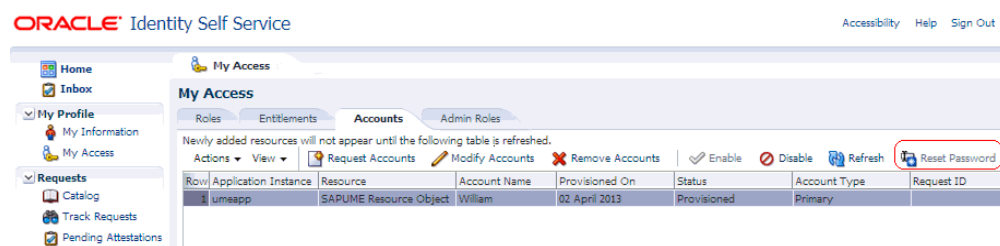
1. Create a sandbox and activate it as described in [Creating and Activating a Sandbox](#).
2. Create a new UI form for the resource as described in [Creating a New UI Form](#).
3. Open the existing application instance.

4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in [Publishing a Sandbox](#).

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

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

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



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

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **Form Designer**.
3. Enter `UD_SAPUME` in the Table Name field and click the **Query for records** button.

Note:

If you are using SAP BusinessObjects AC system, then enter the table name as `UD_SAPACUME`.

4. Click **Create New Version**.
5. In the Create a New Version dialog box, specify the version name in the Label field, save the changes, and then close the dialog box.
6. From the **Current Version** list, select the newly created version.
7. Click the **Properties** tab.
8. Select the password field, and click **Add Property**.
9. From the Property Name list, select **AccountPassword**.
10. In the Property Value field, enter `true`.
11. Click **Save**.

The password field is tagged with the `AccountPassword = true` property as shown in the following screenshot:

The screenshot displays the 'Form Designer' interface. At the top, the 'Table Information' section includes fields for 'Table Name' (UD_SAPUME) and 'Description' (SAPUME PROCESS FORM), along with a 'Form Type' dropdown set to 'Process' and a 'Preview Form' button. Below this is the 'Version Information' section with 'Latest Version' and 'Active Version' both set to '11'. The 'Operations' section features a 'Current Version' dropdown set to '11' and buttons for 'Create New Version' and 'Make Version Active'. The bottom section shows tabs for 'Properties', 'Administrators', 'Usage', 'Pre-Populate', 'Default Columns', and 'User Defin...'. Under the 'Properties' tab, there are sub-tabs for 'Additional Columns' and 'Child Table(s)'. A tree view on the right lists properties for various fields: 'AccountName = true', 'Password (PasswordField)' (expanded to show 'AccountPassword = true'), 'First Name (TextField)', 'Last Name (TextField)' (expanded to show 'Required = true'), 'E-Mail Address (TextField)', 'Fax (TextField)', 'Mobile (TextField)', 'Telephone (TextField)', and 'Department (TextField)'. On the left, there are buttons for 'Add Property' and 'Delete Property'.

12. Click **Make Version Active**.
13. Update the application instance with the new form as described in [Updating an Existing Application Instance with a New Form](#).

2.3.3 Configuring Password Changes for Newly Created Accounts

When you log in to SAP by using a newly created account, you are prompted to change your password at first logon. For accounts created through Oracle Identity Manager, password management can be configured by using the `changePwdFlag` and `dummyPassword` parameters of the IT resource.

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 `changePwdFlag` parameter of the IT resource to `no`. With this setting, the password entered on the process form for a new user account is used to set the password for the new account on the target system. When the user logs in to the target system, the user is prompted to change the password.

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

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

 **Note:**

Security policies of a few target systems allow a user to change the password only once per day. In such a scenario, the target system allows the user to only reset the password and not to change it. The password update task throws an error message, such as `Could not update user NEW_PASSWORD_INVALID`.

If the password feature is disabled for users on the target system, then set the `changePwdFlag` parameter to `no`.

2.3.4 Changing to the Required Input Locale

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

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

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

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

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

1. In a command window, switch to the `OIM_HOME/server/bin` directory.

 **Note:**

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

```
OIM_HOME/server/bin/SCRIPT_FILE_NAME
```

2. Enter the following command:

 **Note:**

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

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

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

On Microsoft Windows: `PurgeCache.bat All`

On UNIX: `PurgeCache.sh All`

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

```
t3://OIM_HOST_NAME:OIM_PORT_NUMBER
```

In this format:

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

2.3.6 Managing Logging

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

The following topics provide detailed information about logging:

- [Understanding Log Levels](#)
- [Enabling Logging](#)

2.3.6.1 Understanding Log Levels

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

- `SEVERE.intValue()+100`

This level enables logging of information about fatal errors.

- `SEVERE`

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

- `WARNING`

This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

These message types are mapped to ODL message type and level combinations as shown in [Table 2-1](#).

Table 2-1 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_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

2.3.6.2 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.SAPUME" 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 2-1](#) 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.SAPUME" 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 Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

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

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

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

4. Restart the application server.

2.3.7 Setting Up the Lookup.SAPUME.UM.RoleDataSource Lookup Definition

The Lookup.SAPUME.UM.RoleDataSource lookup definition is used to hold data source names of the role object class. By default, this lookup definition contains entry for the UME_ROLE_PERSISTENCE role data source, which is common to all SAP configurations. If there are role data sources specific to your environment, then you must update the Lookup.SAPUME.UM.RoleDataSource lookup definition for these data sources.

Note:

If you are using SAP BusinessObjects AC system, then you must update the Lookup.SAPACUME.RoleDatasource.

You must log into SAP User Management Engine as the administrator to view and determine the list of role data sources in your environment.

The name of the role data source is available as part of the Unique ID field. The value of the Unique ID field is in the following format:

```
ROLE.DATA_SOURCE_NAME.AUTO_GENERATED_VALUE
```

The following is a simple value of the Unique ID field:

```
ROLE.PCD_ROLE_PERSISTENCE.YJ1ku1NfcgCd1ZoMDG78ocBzkA=
```

In this value, PCD_ROLE_PERSISTENCE is the name of the role data source.

After you determine the names of all role data sources available in your environment, add each data source name by creating an entry in the `Lookup.SAPUME.UM.RoleDataSource` lookup definition as described in the following procedures:

- [Adding Role Data Source Names to the Lookup.SAPUME.UM.RoleDataSource lookup definition in Oracle Identity Manager Release 11.1.1.x](#)
- [Adding Role Data Source Names to the Lookup.SAPUME.UM.RoleDataSource lookup definition in Oracle Identity Manager Release 11.1.2.x](#)

2.3.7.1 Adding Role Data Source Names to the Lookup.SAPUME.UM.RoleDataSource lookup definition in Oracle Identity Manager Release 11.1.1.x

For Oracle Identity Manager release 11.1.1.x:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAPUME.UM.RoleDataSource** lookup definition.
3. Click **Add**.
4. In the **Code** and **Decode** columns, enter the name of the role data source.
5. Repeat Steps 3 and 4 to create entries for all data source names determined in this section.
6. Click the Save icon.

2.3.7.2 Adding Role Data Source Names to the Lookup.SAPUME.UM.RoleDataSource lookup definition in Oracle Identity Manager Release 11.1.2.x

For Oracle Identity Manager release 11.1.2.x:

1. Log in to Oracle Identity System Administration.
In the left pane, under System Configuration, click **Lookups**.
2. Search for and open the **Lookup.SAPUME.UM.RoleDataSource** lookup definition.
3. Click **Add**.
4. In the **Code** and **Decode** columns, enter the name of the role data source.
5. Repeat Steps 3 and 4 to create entries for all data source names determined in this section.
6. Click the Save icon.

2.3.8 Setting Up the Lookup.SAPUME.UM.GroupDataSource Lookup Definition

The Lookup.SAPUME.UM.GroupDataSource lookup definition is used to hold data source names of the group object class. By default, this lookup definition contains entry for the PRIVATE_DATASOURCE group data source, which is common to all SAP configurations. If there are group data sources specific to your environment, then you must update the Lookup.SAPUME.UM.GroupDataSource lookup definition for these data sources.

Note:

- If you are using SAP BusinessObjects AC system, then you must update the Lookup.SAPACUME.GroupDatasource lookup definition
- SAP User Management Engine does not allow adding a group from the built-in groups adapter data source. Therefore, this data source must not be added in this lookup definition. If SAP User Management Engine is configured with SAP ABAP-based system as data source, such as R3_ROLE_DS, then check whether User Management Engine allows adding a group that assigns ABAP roles to a user. You can check if this is allowed from the Identity Management page of SAP User Management Engine. If adding the group is allowed, then add the data source, R3_ROLE_DS, to the Lookup.SAPUME.UM.GroupDataSource lookup definition

You must log into SAP User Management Engine as the administrator to view and determine the list of group data sources in your environment.

The name of the group data source is available as part of the Unique ID field.

The value of the Unique ID field is in the following format:

GRUP.DATA_SOURCE_NAME.AUTO_GENERATED_VALUE

The following is a sample value of the Unique ID field:

```
GRUP.PRIVATE_DATASOURCE.un:Guests
```

In this value, PRIVATE_DATASOURCE is the name of the group data source.

After you determine the names of all group data sources available in your environment, add each data source name by creating an entry in the Lookup.SAPUME.UM.GroupDataSource lookup definition as described in the following procedures:

- [Adding Group Data Source Names to the Lookup.SAPUME.UM.GroupDataSource lookup definition in Oracle Identity Manager Release 11.1.1.x](#)
- [Adding Group Data Source Names to the Lookup.SAPUME.UM.GroupDataSource lookup definition in Oracle Identity Manager Release 11.1.1.x](#)

2.3.8.1 Adding Group Data Source Names to the Lookup.SAPUME.UM.GroupDataSource lookup definition in Oracle Identity Manager Release 11.1.1.x

For Oracle Identity Manager release 11.1.1.x:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAPUME.UM.GroupDataSource** lookup definition.
3. Click **Add**.
4. In the **Code** and **Decode** columns, enter the name of the group data source.
5. Repeat Steps 3 and 4 to create entries for all data source names determined in this section.
6. Click the Save icon.

2.3.8.2 Adding Group Data Source Names to the Lookup.SAPUME.UM.GroupDataSource lookup definition in Oracle Identity Manager Release 11.1.1.x

For Oracle Identity Manager release 11.1.2.x:

1. Log in to Oracle Identity System Administration.
In the left pane, under System Configuration, click **Lookups**.
2. Search for and open the **Lookup.SAPUME.UM.GroupDatasource** lookup definition.
3. Click **Add**.
4. In the **Code** and **Decode** columns, enter the name of the role data source.
5. Repeat Steps 3 and 4 to create entries for all data source names determined in this section.
6. Click the Save icon.

2.3.9 Setting Up the Lookup Definitions for Exclusion Lists

In the Lookup.SAPUME.UM.ProvExclusionList and Lookup.SAPUME.UM.ReconExclusionList lookup definitions, enter the user IDs of target system accounts for which you do not want to perform provisioning and reconciliation operations, respectively. See [Lookup Definitions for Exclusion Lists](#) for information about the format of the entries in these lookups.

 **Note:**

The `Lookup.SAPUME.UM.ProvExclusionList` and `Lookup.SAPUME.UM.ReconExclusionList` lookup definitions are optional and do not exist by default.

You must add these lookups to the `Lookup.SAPUME.UM.Configuration` lookup definition to enable exclusions during provisioning and reconciliation operations. See [Lookup.SAPUME.UM.Configuration](#) for more information.

To add entries in the lookup for exclusions during provisioning operations:

 **Note:**

To specify user IDs to be excluded during reconciliation operations, add entries in the `Lookup.SAPUME.UM.ReconExclusionList` lookup.

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAPUME.UM.ProvExclusionList** lookup definition.
3. Click **Add**.
4. In the Code Key and Decode columns, enter the first user ID to exclude.

 **Note:**

The Code Key represents the resource object field name on which the exclusion list is applied during provisioning operations.

5. Repeat Steps 3 and 4 for the remaining user IDs to exclude.

For example, if you do not want to provision users with user IDs `User001`, `User002`, and `User088` then you must populate the lookup definition with the following values:

Code Key	Decode
Logon Name	User001
Logon Name	User002
Logon Name	User088

You can also perform pattern matching to exclude user accounts. You can specify regular expressions supported by the representation in the `java.util.regex.Pattern` class.

 **See Also:**

For information about the supported patterns, visit <http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html>

For example, if you do not want to provision users matching any of the user IDs User001, User002, and User088, then you must populate the lookup definition with the following values:

Code Key	Decode
Logon Name[PATTERN]	User001 User002 User088

If you do not want to provision users whose user IDs start with 00012, then you must populate the lookup definition with the following values:

Code Key	Decode
Logon Name[PATTERN]	00012*

6. Click the save icon.

2.3.10 Configuring Oracle Identity Manager for Request-Based Provisioning

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

 **Note:**

Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1.x.

The direct provisioning feature of the connector is automatically disabled when you enable request-based provisioning. Therefore, do not enable request-based provisioning if you want to use the direct provisioning.

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

- [Importing Request Datasets Using Deployment Manager](#)
- [Enabling the Auto Save Form Feature](#)
- [Running the PurgeCache Utility](#)

2.3.10.1 Importing Request Datasets Using Deployment Manager

The request datasets (predefined or generated) can be imported by using the Deployment Manager (DM). The predefined request datasets are stored in the xml/SAPUME-Datasets.xml file on the installation media.

To import a request dataset definition by using the Deployment Manager:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.
4. Locate and open the SAPUME-Datasets.xml file, which is located in the xml directory of the installation media.

Details of this XML file are shown on the File Preview page.

5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the XML file and then click **OK**.

The request datasets are imported into MDS.

2.3.10.2 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management**, and then double-click **Process Definition**.
3. Search for and open the **SAPUME process** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.3.10.3 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See [Clearing Content Related to Connector Resource Bundles from the Server Cache](#) for instructions.

The procedure to configure request-based provisioning ends with this step.

2.3.11 Configuring SSL to Secure Communication Between the Target System and Oracle Identity Manager

You configure SSL to secure data communication between Oracle Identity Manager and the target system.

To configure SSL between the target system and Oracle Identity Manager:

1. Generate the certificate on the target system.
See the target system documentation for detailed instructions.
2. To import the certificate on Oracle Identity Manager:
 - a. Copy the target system certificate to the Oracle Identity Manager host computer.
 - b. In a command window, change to the directory where you copy the certificate file and then enter a command similar to the following:

```
keytool -import -alias ALIAS -file CER_FILE -keystore MY_CACERTS -storepass PASSWORD
```

In this command:

ALIAS is the alias for the certificate (for example, the server name).

CER_FILE is the full path and name of the certificate (.cer) file.

[Table 2-2](#) shows the location of the certificate store of the supported application server.

The following is a sample command:

```
keytool -import -alias ibml-cert140 -file C:\syaug24\Middleware\ibml-cert.cer -keystore C:\syaug24\Middleware\jrockit_160_24_D1.1.2-4\jre\lib\security\cacerts -storepass changeit
```

Table 2-2 Certificate Store Locations

Application Server	Certificate Store Location
Oracle WebLogic Server	<ul style="list-style-type: none"> • If you are using Oracle jrockit_R27.3.1-jdk, then copy the certificate into the following directory: <i>JROCKIT_HOME</i>/jre/lib/security/cacerts • If you are using the default Oracle WebLogic Server JDK, then copy the certificate into the following directory: <i>WEBLOGIC_HOME</i>/java/jre/lib/security/cacerts

- c. To confirm whether or not the certificate has been imported successfully, enter a command similar to the following:

```
keytool -list -alias ALIAS -keystore MY_CACERTS -storepass PASSWORD
```

For example:

```
keytool -list -alias MyAlias -keystore C:\mydir\java\jre\lib\security\cacerts -storepass changeit
```

2.3.12 Configuring the IT Resource for the Target System

An IT resource contains connection information about the target system. Oracle Identity Manager uses this information during reconciliation and provisioning.

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

 **Note:**

If you are using SAP BusinessObjects AC system, then the SAP AC UME IT resource is automatically created when you run the Connector Installer.

 **Note:**

If you are using SAP BusinessObjects AC system, then the SAP AC UME IT resource is automatically created when you run the Connector Installer.

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

To specify values for the parameters of the IT resource:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
 - For Oracle Identity Manager release 11.1.1.x:
Log in to the Administrative and User Console.
 - For Oracle Identity Manager release 11.1.2.x:
Log in to Oracle Identity System Administration.
2. If you are using Oracle Identity Manager release 11.1.1.x, then:
 - a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
 - b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.x, then, in the left pane under Configuration, click **IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `SAPUME IT Resource` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.

7. Specify values for the parameters of the IT resource. [Table 2-3](#) describes the parameters of the SAP UME IT resource and [Table 2-4](#) describes the parameters of the SAP AC UME IT resource.

 **Note:**

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

Table 2-3 Parameters of the SAP UME IT Resource

Parameter	Description
Configuration Lookup	This parameter holds the name of the lookup definition containing configuration information. Value: <code>Lookup.SAPUME.Configuration</code>
ConnectorServerName	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 <i>only</i> if you have deployed the SAP User Management Engine connector in the Connector Server.
changePwdFlag	See Configuring Password Changes for Newly Created Accounts for information about the value to be specified for this parameter. Default value: <code>no</code>
dummyPassword	Enter the dummy password that you want the connector to use during a Create User provisioning operation. The connector first sets the password as this value and then changes it to the password specified on the process form. See Configuring Password Changes for Newly Created Accounts for more information about this parameter.
enableDate	Enter the date that must be set (in the YYYY-MM-DD format) if a user must be enabled. Sample value: <code>9999-12-31</code>
logonNameInitialSubstring	Enter a set of characters to support full reconciliation for the English language. For other languages, enter all characters of that language. Sample value: <code>abcdefghijklmnopqrstuvwxy1234567890</code>
logSPMLRequest	Enter <code>yes</code> to specify that the SPML requests being sent to the target system be written to the log file. Otherwise, enter <code>no</code> .
pwdHandlingSupport	If SAP User Management Engine is configured with an LDAP-based data source in writable mode, then SSL configuration between SAP User Management Engine and the LDAP-based data source is mandatory for password management. In such a scenario, if SSL is not configured between SAP User Management Engine and the LDAP-based data source and password need not be maintained from SAP User Management Engine, then set the value of this parameter <code>no</code> . Otherwise, set the value of this parameter to <code>yes</code> . Default value: <code>yes</code>
TopologyName	Enter the name of the topology of the computer hosting the target system
umePassword	Enter the password of the target system user account that you create for connector operations

Table 2-3 (Cont.) Parameters of the SAP UME IT Resource

Parameter	Description
umeUrl	<ul style="list-style-type: none"> If you perform the procedure described in Configuring SSL to Secure Communication Between the Target System and Oracle Identity Manager, then enter the URL for the SPML service in the following format: https://HOSTNAME:SSL_PORT/spml/spmlservice If you do not configure SSL between the target system and Oracle Identity Manager, then enter the URL for the SPML service in the following format: http://HOSTNAME:PORT/spml/spmlservice <p>Sample value: http://myhost:50000/spml/spmlservice</p>
umeUserId	Enter the user ID of the target system user account that you create for connector operations

Table 2-4 Parameters of the SAP AC UME IT Resource

Parameter	Description
changePwdFlag	See Configuring Password Changes for Newly Created Accounts for information about the value to be specified for this parameter. Default value: no
Configuration Lookup	This parameter holds the name of the lookup definition containing configuration information. Value: Lookup.SAPAC10UME.Configuration
ConnectorServerName	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 <i>only</i> if you have deployed the SAP User Management Engine connector in the Connector Server.
dummyPassword	Enter the dummy password that you want the connector to use during a Create User provisioning operation. The connector first sets the password as this value and then changes it to the password specified on the process form. See Configuring Password Changes for Newly Created Accounts for more information about this parameter.
enableDate	Enter the date that must be set (in the YYYY-MM-DD format) if a user must be enabled. Sample value: 9999-12-31
grcLanguage	This parameter defines the language of grc. Value: en
grcPassword	This parameter is used to authenticate the user access.
grcUsername	This parameter holds the GrcUsername for accessing the grc system.
logonNameInitialSubstring	Enter a set of characters to support full reconciliation for the English language. For other languages, enter all characters of that language. Sample value: abcdefghijklmnopqrstuvwxyz1234567890
logSPMLRequest	Enter <i>yes</i> to specify that the SPML requests being sent to the target system be written to the log file. Otherwise, enter <i>no</i> .

Table 2-4 (Cont.) Parameters of the SAP AC UME IT Resource

Parameter	Description
pwdHandlingSupport	If SAP User Management Engine is configured with an LDAP-based data source in writable mode, then SSL configuration between SAP User Management Engine and the LDAP-based data source is mandatory for password management. In such a scenario, if SSL is not configured between SAP User Management Engine and the LDAP-based data source and password need not be maintained from SAP User Management Engine, then set the value of this parameter <code>no</code> . Otherwise, set the value of this parameter to <code>yes</code> . Default value: <code>yes</code>
umePassword	Enter the password of the target system user account that you create for connector operations
umeUrl	<ul style="list-style-type: none"> If you perform the procedure described in Configuring SSL to Secure Communication Between the Target System and Oracle Identity Manager, then enter the URL for the SPML service in the following format: <code>https://HOSTNAME:SSL_PORT/spml/spmlservice</code> If you do not configure SSL between the target system and Oracle Identity Manager, then enter the URL for the SPML service in the following format: <code>http://HOSTNAME:PORT/spml/spmlservice</code> Sample value: <code>http://myhost:50000/spml/spmlservice</code>
umeUserId	Enter the user ID of the target system user account that you create for connector operations

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

2.3.13 Configuring the IT Resource for the Connector Server

An IT resource contains connection information about the target system. Oracle Identity Manager uses this information during reconciliation and provisioning.

Perform the procedure described in this section only if you have installed the connector bundle in a Connector Server, as described in [Deploying the Connector Bundle in a Connector Server](#). You must create a separate IT resource for the Connector Server.

To create the IT resource for the Connector Server:

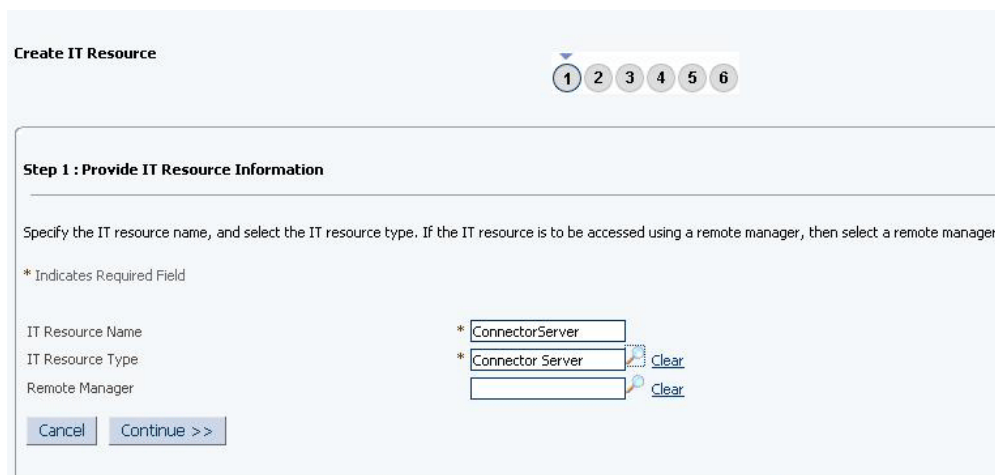
- Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
 - For Oracle Identity Manager release 11.1.1.x:
Log in to the Administrative and User Console.
 - For Oracle Identity Manager release 11.1.2.x:
Log in to Oracle Identity System Administration.
- If you are using Oracle Identity Manager release 11.1.1.x, then:
 - On the Welcome page, click **Advanced** in the upper-right corner of the page.
 - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Create IT Resource**.
- If you are using Oracle Identity Manager release 11.1.2.x, then:
 - In the left pane under Configuration, click **IT Resource**.

 **Note:**

If you are using Oracle Identity Manager release 11.1.2.3.x or later, then in the left pane, under Provisioning Configuration, click **IT Resource**.

- b. In the Manage IT Resource page, click **Create IT Resource**.
4. **Note:** On the Step 1: Provide IT Resource Information page, perform the following steps:
 - **IT Resource Name:** Enter a name for the IT resource.
 - **IT Resource Type:** Select **Connector Server** from the IT Resource Type list.
 - **Remote Manager:** Do not enter a value in this field.
5. Click **Continue**. [Figure 2-1](#) shows the IT resource values added on the Create IT Resource page.

Figure 2-1 Step 1: Provide IT Resource Information



Create IT Resource

1 2 3 4 5 6

Step 1 : Provide IT Resource Information

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

* Indicates Required Field

IT Resource Name * ConnectorServer

IT Resource Type * Connector Server Clear

Remote Manager Clear

Cancel Continue >>

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

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

Create IT Resource

1 2 3 4 5 6

Step 2 : Specify IT Resource Parameter Values

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

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

Cancel << Back Continue >>

Table 2-5 provides information about the parameters of the IT resource.

Table 2-5 Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: RManager
Key	Enter the key for the Java connector server.
Port	Enter the number of the port at which the connector server is listening. Default value: 8759
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: 300
UseSSL	Enter <code>true</code> to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter <code>false</code> . Default value: <code>false</code> Note: If you configure the connector to communicate with the Connector Server using SSL, including setting the <code>connectorserver.usssl</code> property to <code>true</code> and importing the target system certificate into the Connector Server JDK keystore, an attempt to access the target system or run the Connector Server returns an error.

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

 **Note:**

This step is optional.

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

- a. Click **Assign Group**.
 - b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.
 - c. Click **Assign**.
8. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

 **Note:**

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

- a. Click **Update Permissions**.
 - b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.
 - c. Click **Update**.
9. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

 **Note:**

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

- a. Select the **Unassign** check box for the group that you want to unassign.
 - b. Click **Unassign**.
10. Click **Continue**. [Figure 2-3](#) shows the Step 3: Set Access Permission to IT Resource page.

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

Create IT Resource 1 2 3 4 5 6

Step 3 : Set Access Permission to IT Resource

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

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

Administrative Role	Display Name	Read Access	Write Access	Delete Access	Unassign
SYSTEM ADMINISTRATORS	SYSTEM ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>
IDENTITY USER ADMINISTRATORS	IDENTITY USER ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>
ROLE ADMINISTRATORS	ROLE ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>
REQUEST ADMINISTRATORS	REQUEST ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>
RECONCILIATION ADMINISTRATORS	RECONCILIATION ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>
ATTESTATION EVENT ADMINISTRATORS	ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>
APPROVAL POLICY ADMINISTRATORS	APPROVAL POLICY ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>
ATTESTATION CONFIGURATION ADMINISTRATORS	ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>
USER CONFIGURATION ADMINISTRATORS	USER CONFIGURATION ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>
RESOURCE ADMINISTRATORS	RESOURCE ADMINISTRATORS	✓	✓	✓	<input type="checkbox"/>

[Unassign](#)

First | Previous | Next | Last

[Assign Role](#) [Update Permissions](#)

[Cancel](#) [<< Back](#) [Continue >>](#)

11. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.
12. To proceed with the creation of the IT resource, click **Continue**. Figure 2-4 shows Step 4: Verify IT Resource Details page.

Figure 2-4 Step 4: Verify IT Resource Details

Create IT Resource 1 2 3 4 5 6

Step 4 : Verify IT Resource Details

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

IT Resource Name ConnectorServer
IT Resource Type Connector Server

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

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

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

13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:
- Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
 - Click **Cancel** to stop the procedure, and then begin from the first step onward.

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

Figure 2-5 Step 5: IT Resource Connection Result

Create IT Resource

1 2 3 4 5 6

Step 5 : IT Resource Connection Result

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

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

Cancel << Back Continue >>

14. Click **Finish**. [Figure 2-6](#) shows the IT Resource Created Page.

Figure 2-6 Step 6: IT Resource Created

Create IT Resource

1 2 3 4 5 6

Step 6 : IT Resource Created

You have created **ConnectorServer**.

IT Resource Name ConnectorServer
IT Resource Type Connector Server

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

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

Finish

2.3.14 Configuring the Access Request Management Feature of the Connector

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

Note:

Before you configure the Access Request Management feature, it is recommended that you read the guidelines described in [Guidelines on Using a Deployment Configuration](#).

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

- [Specifying Values for the GRC UME-ITRes IT Resource](#)

- [Configuring Request Types and Workflows on SAP BusinessObjects AC Access Request Management](#)

2.3.14.1 Specifying Values for the GRC UME-ITRes IT Resource

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

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
 - For Oracle Identity Manager release 11.1.1.x:
Log in to the Administrative and User Console.
 - For Oracle Identity Manager release 11.1.2.x:
Log in to Identity System Administration.
2. If you are using Oracle Identity Manager release 11.1.1.x, then:
 - a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
 - b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.x, then, in the left pane under Configuration, click **IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter GRC UME-ITRes and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource.

[Table 2-6](#) lists the parameters of the GRC UME-ITRes IT resource.

Table 2-6 Parameters of the GRC UME-ITRes IT Resource

Parameter	Description
Configuration Lookup	Enter the name of the configuration lookup definition. Value for Lookup Lookup.SAPUME.Configuration
Connector Server Name	Name of the IT resource of the type "Connector Server."
language	Enter the two-letter code for the language set on the target system. Sample value: EN
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 2-6 (Cont.) Parameters of the GRC UME-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

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

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

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

1. Create a request type in SAP BusinessObjects AC Access Request Management.
In SAP BusinessObjects AC Access Request Management, a request type defines the action that is performed when a request is processed. Oracle Identity Manager is a requester. It works with request types defined in SAP BusinessObjects AC Access Request Management. The Lookup.SAPUME.AC10.Configuration lookup definition maps request types to provisioning operations submitted through Oracle Identity Manager.
2. Create an access request workflow using the MSMP (Multi Step Multi process) Workflow engine.

2.3.15 Configuring SoD (Segregation of Duties)

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

This section discusses the following procedures:

- [Specifying Values for the GRC UME-ITRes IT Resource](#)
- [Configuring SAP GRC to Act As the SoD Engine](#)
- [Specifying a Value for the TopologyName IT Resource Parameter](#)
- [Disabling and Enabling SoD](#)

 **Note:**

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

2.3.15.1 Configuring SAP GRC to Act As the SoD Engine

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

2.3.15.2 Specifying Values for the GRC UME-ITRes IT Resource

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

To set values for the parameters of this IT resource, see [Specifying Values for the GRC UME-ITRes IT Resource](#).

2.3.15.3 Specifying a Value for the TopologyName IT Resource Parameter

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

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

By default, the GRC-ITRes IT resource is registered. However, you must manually register the GRC UME-ITRes IT resource and enter the new topology name as the value of the TopologyName IT resource parameter.

To register the GRC UME-ITRes IT resource:

1. Run the following command and add instance names for SAP and GRC.

On Microsoft Windows: `OIM_HOME\server\bin>registration.bat`

On a UNIX-based computer: `OIM_HOME/server/bin/./registration.sh`

After running this command, enter options as shown in the following sample output:

```
Do you want to proceed with registration? (y/n) y
Register System Instance for type OIM?(y/n) n
Register System Instance for type EBS?(y/n) n
Register System Instance for type PSFT?(y/n) n
```

```

Register System Instance for type OAACG?(y/n) n
Register System Instance for type SAP?(y/n) y
Provide instance name sap1
Register System Instance for type GRC?(y/n) y
Provide instance name grc1
GRC ITResource Instance Name: GRC UME-ITRes
Register System Instance for type OIM SDS?(y/n) n
Register System Instance for type OIA?(y/n) n

```

2. Run the following command and find the registration IDs for the above instance names:

```
OIM_HOME\server\bin>registration printRegistrationIDs
```

3. Import the metadata/iam-features-sil/db/SILConfig.xml file from MDS and add the <Topology> element with IDs found in Step 2.

Here is a sample element:

```

<Topology>
  <name>sodgrcume</name>
  <IdmId>1</IdmId>
  <SodId>24</SodId>
  <SDSID>23</SDSID>
</Topology>

```

4. Export the metadata/iam-features-sil/db/SILConfig.xml file to MDS and restart the server.

See [Configuring the IT Resource for the Target System](#) for information about specifying values for parameters of the IT resource.

2.3.15.4 Disabling and Enabling SoD

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

- [Disabling SoD on Oracle Identity Manager](#)
- [Enabling SoD on Oracle Identity Manager](#)

2.3.15.4.1 Disabling SoD on Oracle Identity Manager

To disable SoD:

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

3. In the Search System Configuration box, enter `XL.SoDCheckRequired` and then click **Search**.
A list that matches your search criteria is displayed in the search results table.
4. Click the **XL.SoDCheckRequired** property name.
System properties for SoD are displayed on the right pane.
5. In the Value box, enter `FALSE` to disable SoD.
6. Click **Save**.
7. Restart Oracle Identity Manager.

2.3.15.4.2 Enabling SoD on Oracle Identity Manager

To enable SoD:

1. If you are using Oracle Identity Manager release 11.1.1.x, then perform the following steps:
 - a. Log in to the Administrative and User Console.
 - b. On the Welcome page, click **Advanced** in the upper-right corner of the page.
 - c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management tab, click **System Configuration**.
2. If you are using Oracle Identity Manager release 11.1.2.x, then perform the following steps:
 - a. Log in to Identity System Administration.
 - b. In the left pane, under System Management, click **System Configuration**.
3. In the Search System Configuration box, enter `XL.SoDCheckRequired` and then click **Search**.
A list that matches your search criteria is displayed in the search results table.
4. Click the **XL.SoDCheckRequired** property name.
System properties for SoD are displayed on the right pane.
5. In the Value box, enter `TRUE` to enable SoD.
6. Click **Save**.
7. Restart Oracle Identity Manager.

2.3.16 Downloading WSDL files from SAP BusinessObjects AC

You need to download the WSDL files from SAP BusinessObjects AC before configuring the web services in SAP BusinessObjects AC. WSDL is required for connector to connect SAP web services.

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

WSDL	Description
GRAC_AUDIT_LOGS_WS	Audit log web service

WSDL	Description
GRAC_LOOKUP_WS	Look Up Service
GRAC_REQUEST_STATUS_WS	Request status web service
GRAC_RISK_ANALYSIS_WOUT_NO_WS	Risk analysis without request number
GRAC_SELECT_APPL_WS	Select Application web service
GRAC_USER_ACCESS_WS	User Access Request Service
GRAC_SEARCH_ROLES_WS	Search role web service

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

2.3.17 Localizing Field Labels in UI Forms

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

Note:

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

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

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear**.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open one of the following files in a text editor:
 - For Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):
SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
 - For releases prior to Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):
SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:
 - a. Search for the following text:

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

- b. Replace with the following text:

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

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

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

- c. Search for the application instance code. This procedure shows a sample edit for SAP User Management Engine 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_SAPUME_DEPARTMENT__c_description']]">
<source>Department</source>
</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.SAPUMEFORM.entity.SAPUMEF
ORMEO.UD_SAPUME_DEPARTMENT__c_LABEL">
<source>Department</source>
</target>
</trans-unit>
```

- d. Open the resource file from the connector package, for example SAPUME_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_SAPUME_DEPARTMENT=\u90E8\u9580.

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_SAPUME_DEPARTMENT__c_description']]">
<source>Department</source>
<target>\u90E8\u9580</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.SAPUMEFORM.entity.SAPUMEF
ORMEO.UD_SAPUME_DEPARTMENT__c_LABEL">
<source>Department</source>
<target>\u90E8\u9580</target>
</trans-unit>
```

- f. Repeat Steps 6.a through 6.d for all attributes of the process form.
- g. Save the file as BizEditorBundle_LANG_CODE.xlf. In this file name, replace LANG_CODE with the code of the language to which you are localizing.

Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

 **See Also:**

Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*, for more information about exporting and importing metadata files

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

2.3.18 Synchronizing the SAPUME Process Form and SAP AC UME Process Form with Target System Field Lengths

Ensure that the field length of attribute values in the target system must be the same as the field length of values in the SAPUME process form and SAP AC UME Process Form fields.

2.4 Upgrading the Connector

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

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

- [Prerequisites for Upgrading the Connector](#),
- [Upgrading the Connector](#),
- [Performing the Postupgrade Steps](#),

 **Note:**

- Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
- As a best practice, first perform the upgrade procedure in a test environment.

2.4.1 Prerequisites for Upgrading the Connector

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

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

- Run the Oracle Identity Manager Delete JARs utility to delete the old connector bundle to the Oracle Identity Manager database.

 **See Also:**

Delete JAR Utility of *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Delete JARs utility

2.4.2 Upgrading the Connector

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

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

 **See Also:**

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

2.4.3 Performing the Postupgrade Steps

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

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

 **See Also:**

Upload JAR Utility of *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Upload JARs utility

2. Re-configure the IT resource of the connector.
3. Upgrading the connector will generate duplicate entries in Lookups, you must manually delete these duplicate entries. Perform the Postupgrade procedure documented in *Managing Connector Lifecycle of Oracle Fusion Middleware Administering Oracle Identity Manager*.
4. Perform the postupgrade steps. Depending on the version of the connector that you are using, perform one of the procedures described in the following sections:

- [Performing the Postupgrade Steps for Releases 9.x, 11.1.1.5.0, and 11.1.1.6.0 of the SAP User Management Engine Connector](#)
- [Perform the Postupgrade Steps for Release 11.1.1.8.0 or later of the SAP User Management Engine Connector](#)

2.4.3.1 Performing the Postupgrade Steps for Releases 9.x, 11.1.1.5.0, and 11.1.1.6.0 of the SAP User Management Engine Connector

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

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

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

```
ResourceObject;SAPUME Resource Object
FormName;UD_SAPEP
FromVersion;V_9.0.4.12
ToVersion;v_11.1.1.8.0
Parent;UD_SAPEP_IS_LOCK;false
```

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

```
ResourceObject;SAPUME Resource Object
FormName;UD_SAPUME
FromVersion;V_11.1.1.5.0
ToVersion;v_11.1.1.8.0
Parent;UD_SAPUME_IS_LOCK;false
```

2.4.3.2 Perform the Postupgrade Steps for Release 11.1.1.8.0 or later of the SAP User Management Engine Connector

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

- [Postupgrade Steps While Upgrading the Basic User Management Engine configuration from Release 11.1.1.8.0 to Release 11.1.1.9.0](#)
- [Postupgrade Steps While Upgrading the SoD validation of SAP BusinessObjects AC Access Risk Analysis from Release 11.1.1.8.0 to Release 11.1.1.9.0](#)
- [Postupgrade Steps While Upgrading the SAP BusinessObjects AC Access Request Management from Release 11.1.1.8.0 to Release 11.1.1.9.0](#)

2.4.3.2.1 Postupgrade Steps While Upgrading the Basic User Management Engine configuration from Release 11.1.1.8.0 to Release 11.1.1.9.0

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

If you are using the connector release 11.1.1.8.0, include the following entries:

```
ResourceObject;SAPUME Resource Object
FormName;UD_SAPUME
```

```
FromVersion;V_11.1.1.8.0  
ToVersion;v_11.1.1.9.0
```

 **Note:**

While upgrading the connector, the following information will display. You must manually delete the following adapters and Event handlers:

- The "sapume ac remove child" and "sapume ac add child" Adapters.
- The "adpSAPUMEACREMOVECHIL" and "adpSAPUMEACADDCHILD" event handlers.

2.4.3.2.2 Postupgrade Steps While Upgrading the SoD validation of SAP BusinessObjects AC Access Risk Analysis from Release 11.1.1.8.0 to Release 11.1.1.9.0

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

1. Re-configure the GRC UME-ITRes IT resource.
2. You must manually update the decode values of the following entries in the "Lookup.SAPUME.Configuration" lookup definition:
 - SODSystemKey
 - wsdlFilePath
 - entitlementRiskAnalysisAccessURL
3. Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation. To do so, in a text editor, open the fvc.properties file located in the OIM_DC_HOME directory. If you are using the connector release 11.1.1.8.0, include the following entries:

```
ResourceObject;SAPUME Resource Object  
FormName;UD_SAPUME  
FromVersion;V_11.1.1.8.0  
ToVersion;v_11.1.1.9.0
```

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

 **Note:**

While upgrading the connector, the following information will display. You must manually delete the following adapters and Event handlers:

- The "sapume ac remove child" and "sapume ac add child" Adapters.
- The "adpSAPUMEACREMOVECHIL" and "adpSAPUMEACADDCHILD" event handlers.

2.4.3.2.3 Postupgrade Steps While Upgrading the SAP BusinessObjects AC Access Request Management from Release 11.1.1.8.0 to Release 11.1.1.9.0

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

1. Re-configure the SAPUME IT Resource IT resource with GRC credentials.
2. You must manually update the decode values for the following entries in the "Lookup.SAPAC10UME.Configuration" lookup definition:
 - roleLookupAccessURL
 - otherLookupAccessURL
 - auditLogsAccessURL
 - appLookupAccessURL
 - wsdlFilePath
 - userAccessAccessURL
 - requestStatusAccessURL
 - **Note:** Upgrading the connector will generate duplicate entries in Lookups, you must manually delete these duplicate entries.
 - Perform the postupgrade procedure documented in the Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Manager*.
3. Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation. To do so:

In a text editor, open the fvc.properties file located in the OIM_DC_HOME directory. If you are using the connector release 11.1.1.8.0, include the following entries:

```
ResourceObject;SAP AC UME Resource Object
FormName;UD_SAPUME
FromVersion;v_11.1.1.8.0
ToVersion;v_11.1.1.9.0
```

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

For Microsoft Windows:

OIM_DC_HOME/fvcutil.bat

For UNIX:

OIM_DC_HOME/fvcutil.sh

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

 **See Also:**

Using the Form Version Control Utility of *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the FVC utility

4. Run the PostUpgradeScript_SAPUME.sql script as follows:
 - a. Connect to the Oracle Identity Manager database by using the OIM DB User credentials.
 - b. Run the PostUpgradeScript_SAPUME.sql. This script is located in the Upgrade directory on the installation media.

 **Note:**

Change the task name of the bulk adapter after upgrade. Example: Replace UD_SAPACUME Updated with UD_SAPUME Updated.

5. Create a new version of the process form.

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

 - a. Log in to Oracle Identity System Administration.
 - b. Create and activate a sandbox. See [Creating and Activating a Sandbox](#) for more information.
 - c. Create a new UI form to view the upgraded fields. See [Creating a New UI Form](#) for more information about creating a UI form.
 - d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in the preceding step), and then save the application instance.
 - e. Publish the sandbox. See [Publishing a Sandbox](#) for more information.
6. Run all the following scheduled jobs that are used for SAP BusinessObjects AC lookup field synchronization:

 **Note:**

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

- SAP AC UME Role Lookup Reconciliation
- SAP AC UME Group Lookup Reconciliation
- SAP AC UME BusinessProcess Lookup Reconciliation

- SAP AC UME FunctionalArea Lookup Reconciliation
 - SAP AC UME ItemProvAction Lookup Reconciliation
 - SAP AC UME Priority Lookup Reconciliation
 - SAP AC UME ReqInitSystem Lookup Reconciliation
 - SAP AC UME RequestType Lookup Reconciliation
7. Perform full reconciliation.
This operation updates the Unique Id resource object field and the lock status of the users. The lock status will be updated as per the value specified in the fvc.properties file in Step 5a.
See [Full Reconciliation](#) for more information about this step.
 8. After upgrading the connector, you can perform delete reconciliation.
See [Reconciliation Scheduled Jobs](#) for more information about delete reconciliation.
 9. If you are using Connector Server, Deploy the Connector Bundle in a Connector Server. See [Deploying the Connector Bundle in a Connector Server](#) for more information.

3

Using the Connector

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

 **Note:**

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

- [Performing Full Reconciliation](#)
- [Scheduled Job for Lookup Field Synchronization](#)
- [Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization](#)
- [Configuring Reconciliation](#)
- [Configuring Scheduled Jobs](#)
- [Guidelines on Performing Provisioning](#)
- [Configuring Provisioning in Oracle Identity Manager Release 11.1.1.x](#)
- [Configuring Provisioning in Oracle Identity Manager Release 11.1.2.x](#)
- [Uninstalling the Connector](#)

3.1 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

To perform a full reconciliation run, remove (delete) any value currently assigned to the Filter attribute of the SAP UME User Recon scheduled task. See [Configuring Scheduled Jobs](#) for information about this scheduled task.

3.2 Scheduled Job for Lookup Field Synchronization

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

The following scheduled jobs are used for lookup field synchronization:

- SAP UME Group Lookup Reconciliation
- SAP UME Role Lookup Reconciliation

You must specify values for the attributes of these scheduled jobs. [Table 3-1](#) describes the attributes of these scheduled jobs. The procedure to configure scheduled tasks is described later in the guide.

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

Attribute	Description
Code Key Attribute	<p>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).</p> <p>Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> For SAP UME Group Lookup Reconciliation: id For SAP UME Role Lookup Reconciliation: id <p>Note: You must not change the value of this attribute.</p>
Decode Attribute	<p>Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute).</p> <p>Depending on the scheduled job that you are using, the default values are as follows:</p> <ul style="list-style-type: none"> For SAP UME Group Lookup Reconciliation: description For SAP UME Role Lookup Reconciliation: description
Filter	<p>Enter a filter condition using the or operator, represented by vertical bar (), to filter out the data sources from which group or role details must be fetched.</p> <p>Sample value of this attribute for group lookup synchronization: <code>equalTo('datasource', 'R3_ROLE_DS') equalTo('datasource', 'PRIVATE_DATASOURCE') equalTo('datasource', 'SUPER_GROUPS_DATASOURCE')</code></p> <p>Sample value of this attribute for role lookup synchronization: <code>equalTo('datasource', 'PCD_ROLE_PERSISTENCE') equalTo('datasource', 'UME_ROLE_PERSISTENCE')</code></p> <p>Note: Specifying a value for this attribute is mandatory for Group and Role reconciliation schedule jobs.</p>
IT Resource Name	<p>Enter the name of the IT resource for the target system installation from which you want to reconcile user records.</p> <p>Default value: SAPUME IT Resource</p>
Lookup Name	<p>This attribute holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched.</p> <p>Default value of this attribute for group lookup synchronization: Lookup.SAPUME.UM.Group</p> <p>Default value of this attribute for role lookup synchronization: Lookup.SAPUME.UM.Role</p>
Object Class	<p>Enter the name of the object class from which value must be fetched.</p> <p>Default value of this attribute for group synchronization: <code>__GROUP__</code></p> <p>Default value of this attribute for role synchronization: <code>__ROLE__</code></p> <p>Note: You must not change the value of the attribute.</p>
Object Type	<p>Enter the type of object whose values must be synchronized.</p> <p>Default value of this attribute for group synchronization: Group</p> <p>Default value of this attribute for role synchronization: Role</p> <p>Note: You must not change the value of this attribute.</p>

3.3 Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization

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

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

- SAP AC UME BusinessProcess Lookup Reconciliation
- SAP AC UME FunctionalArea Lookup Reconciliation
- SAP AC UME Group Lookup Reconciliation
- SAP AC UME ItemProvAction Lookup Reconciliation
- SAP AC UME Priority Lookup Reconciliation
- SAP AC UME ReqInitSystem Lookup Reconciliation
- SAP AC UME RequestType Lookup Reconciliation
- SAP AC UME Request Status
- SAP AC UME Role Lookup Reconciliation
- SAP AC UME Target User Delete Reconciliation
- SAP AC UME Target User Reconciliation

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

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

Attribute	Description
Code Key Attribute	<p>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).</p> <p>Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> • SAP AC UME BusinessProcess Lookup Reconciliation: LCODE • SAP AC UME FunctionalArea Lookup Reconciliation: LCODE • SAP AC UME Group Lookup Reconciliation: id • SAP AC UME ItemProvAction Lookup Reconciliation: LCODE • SAP AC UME Priority Lookup Reconciliation: LCODE • SAP AC UME ReqInitSystem Lookup Reconciliation: REQSYS_CODE • SAP AC UME RequestType Lookup Reconciliation: LCODE • SAP AC UME Role Lookup Reconciliation: id <p>Note: You must not change the value of this attribute.</p>

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

Attribute	Description
Decode Attribute	<p>Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute).</p> <p>Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> • SAP AC UME BusinessProcess Lookup Reconciliation: LDECODE • SAP AC UME FunctionalArea Lookup Reconciliation: LDECODE • SAP AC UME Group Lookup Reconciliation: description • SAP AC UME ItemProvAction Lookup Reconciliation: LDECODE • SAP AC UME Priority Lookup Reconciliation: LDECODE • SAP AC UME ReqInitSystem Lookup Reconciliation: REQSYSDECODE • SAP AC UME RequestType Lookup Reconciliation: LDECODE • SAP AC UME Role Lookup Reconciliation: description
IT Resource Name	<p>Name of the IT resource for the target system installation from which you want to reconcile records.</p> <p>Default value: SAP AC UME IT Resource</p>
Lookup Name	<p>Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system.</p> <p>Note: If the lookup name that you specify as the value of this attribute is not present in Oracle Identity Manager, then this lookup definition is created while the scheduled job is run.</p> <p>Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> • SAP AC UME BusinessProcess Lookup Reconciliation: Lookup.SAPACUME.Bproc • SAP AC UME FunctionalArea Lookup Reconciliation: Lookup.SAPACUME.Funcarea • SAP AC UME Group Lookup Reconciliation: Lookup.SAPACUME.Group • SAP AC UME ItemProvAction Lookup Reconciliation: Lookup.SAPAC10UME.ItemProvAction • SAP AC UME Priority Lookup Reconciliation: Lookup.SAPACUME.Priority • SAP AC UME ReqInitSystem Lookup Reconciliation: Lookup.SAPACUME.RegInitSystem • SAP AC UME RequestType Lookup Reconciliation: Lookup.SAPAC10UME.RequestType • SAP AC UME Role Lookup Reconciliation: Lookup.SAPACUME.Role
Object Class	<p>Enter the name of the class of the object you want to reconcile.</p> <p>Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> • SAP AC UME BusinessProcess Lookup Reconciliation: BusProc • SAP AC UME FunctionalArea Lookup Reconciliation: FunctionArea • SAP AC UME Group Lookup Reconciliation: __GROUP__ • SAP AC UME ItemProvAction Lookup Reconciliation: ItemProvActionType • SAP AC UME Priority Lookup Reconciliation: PriorityType • SAP AC UME ReqInitSystem Lookup Reconciliation: SYSTEM • SAP AC UME RequestType Lookup Reconciliation: RequestType • SAP AC UME Role Lookup Reconciliation: __ROLE__

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

Attribute	Description
Object Type	<p>Enter the name of the type of object you want to reconcile.</p> <p>Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> • SAP AC UME BusinessProcess Lookup Reconciliation: BusProc • SAP AC UME FunctionalArea Lookup Reconciliation: FunctionArea • SAP AC UME Group Lookup Reconciliation: Group • SAP AC UME ItemProvAction Lookup Reconciliation: ItemProvActionType • SAP AC UME Priority Lookup Reconciliation: PriorityType • SAP AC UME ReqInitSystem Lookup Reconciliation: SYSTEM • SAP AC UME RequestType Lookup Reconciliation: RequestType • SAP AC UME Role Lookup Reconciliation: Role

3.4 Configuring Reconciliation

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

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

- [Full Reconciliation](#)
- [Limited Reconciliation](#)
- [Reconciliation Scheduled Jobs](#)

3.4.1 Full Reconciliation

In full reconciliation, all existing target system records are fetched into Oracle Identity Manager for reconciliation.

See [Performing Full Reconciliation](#) for instructions.

3.4.2 Limited Reconciliation

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

The connector provides a Filter attribute that allows you to use any of the SAP UME 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 those in which the account name starts with "a" letter, you could use the following expression:

```
startsWith('__NAME__', 'a')
```

For a more advanced search, where you want to filter only those account names that end with 'z', you could use the following filter:

```
startsWith('__NAME__', 'a') & endsWith('__NAME__', 'z')
```

While deploying the connector, follow the instructions in [Configuring Scheduled Jobs](#) to specify attribute values.

3.4.3 Reconciliation Scheduled Jobs

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

Depending on whether you want to reconcile data about users or deleted users from the target system, you must specify values for the attributes of one of the following scheduled jobs:

- **SAP UME Target User Reconciliation**
You use the SAP UME Target User Reconciliation scheduled job to reconcile user data from the SAP UME target system.
- **SAP UME Target User Delete Reconciliation**
You use the SAP UME Target User Delete Reconciliation scheduled to reconcile data about deleted users from the target system. During a reconciliation run, for each deleted user account on the target system, the SAP User Management Engine resource is revoked for the corresponding OIM User.
- **SAP AC UME Target User Reconciliation**
You use the SAP AC UME Target User Reconciliation scheduled job to reconcile user data from the SAP AC UME target system.
- **SAP AC UME Target User Delete Reconciliation**

You use the SAP AC UME Target User Delete Reconciliation scheduled to reconcile data about deleted users from the target system. During a reconciliation run, for each deleted user account on the target system, the SAP User Management Engine resource is revoked for the corresponding OIM User.

This section discusses the attributes of the following scheduled jobs:

- [SAP UME Target User Reconciliation and SAP AC UME Target User Reconciliation](#)
- [SAP UME Target User Delete Reconciliation and SAP AC UME Target User Delete Reconciliation](#)
- [SAP AC Request Status](#)

3.4.3.1 SAP UME Target User Reconciliation and SAP AC UME Target User Reconciliation

You use the SAP UME Target User Reconciliation and SAP AC UME Reconciliation scheduled job to reconcile user records from SAP BusinessObjects AC target system. [Table 3-3](#) describes the attributes of the SAP UME Target User Reconciliation and SAP AC UME Target User Reconciliation scheduled jobs.

Table 3-3 Attributes of the SAP UME Target User Reconciliation and SAP AC UME Target User Reconciliation Scheduled Jobs

Attribute	Description
Filter	Expression for filtering records. Sample value: <code>equalTo('logonname', 'SEPT12USER1')</code>
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Depending on the scheduled job you are using, the default values are as follows: <ul style="list-style-type: none"> • For SAP UME Target User Reconciliation SAPUME IT Resource • For SAP AC UME Target User Reconciliation SAP AC UME IT Resource
Object Type	Enter the type of object you want to reconcile. Default value: <code>User</code>
Resource Object Name	Name of the resource object that is used for reconciliation. Depending on the scheduled job you are using, the default values are as follows: <ul style="list-style-type: none"> • For SAP UME Target User Reconciliation SAPUME Resource Object • For SAP AC UME Target User Reconciliation SAP AC UME Resource Object

3.4.3.2 SAP UME Target User Delete Reconciliation and SAP AC UME Target User Delete Reconciliation

You use the SAP UME Target User Delete Reconciliation and SAP AC UME Target User Delete Reconciliation scheduled job to reconcile deleted user records from SAP BusinessObjects AC target system. [Table 3-4](#) describes the attributes of the SAP UME

Target User Delete Reconciliation and SAP AC UME Target User Delete Reconciliation scheduled jobs.

Table 3-4 Attributes of the SAP UME Target User Delete Reconciliation and SAP AC UME Target User Delete Reconciliation Scheduled Jobs

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Depending on the scheduled job you are using, the default values are as follows: <ul style="list-style-type: none"> For SAP UME Target User Delete Reconciliation SAPUME IT Resource For SAP AC UME Target User Delete Reconciliation SAP AC UME IT Resource
Object Type	Enter the type of object you want to reconcile. Default value: User
Resource Object Name	Name of the resource object that is used for reconciliation. Depending on the scheduled job you are using, the default values are as follows: <ul style="list-style-type: none"> For SAP UME Target User Delete Reconciliation SAPUME Resource Object For SAP AC UME Target User Delete Reconciliation SAP AC UME Resource Object

3.4.3.3 SAP AC Request Status

You use the SAP AC Request Status scheduled job to reconcile request status from SAP BusinessObjects AC target system. [Table 3-5](#) describes the attributes of this scheduled job.

Table 3-5 Attributes of the SAP AC Request Status Scheduled Job

Attribute	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data Default value: SAP AC UME IT Resource
Object Type	Type of object you want to reconcile Default value: STATUS
Resource Object Name	Name of the resource object against which reconciliation runs must be performed Default value: SAP AC UME Resource Object
Scheduled Task Name	Name of the scheduled task Default value: SAP AC UME Request Status

3.5 Configuring Scheduled Jobs

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

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

[Table B-1](#) lists the scheduled jobs that you must configure.

To configure a scheduled job:

1. If you are using Oracle Identity Manager release 11.1.1.x, then perform the following steps:
 - a. Log in to the Administrative and User Console.
 - b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
2. If you are using Oracle Identity Manager release 11.1.2.x, then perform the following steps:
 - a. Log in to Identity System Administration.
 - b. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
 - a. If you are using Oracle Identity Manager release 11.1.1.x, then on the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
 - b. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
 - c. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the following parameters:
 - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
 - **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

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 job.

 **Note:**

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
- Attributes of the scheduled job are discussed in [Reconciliation Scheduled Jobs](#).

6. Click **Apply** to save the changes.

 **Note:**

You can use the Scheduler Status page in Identity System Administration to either start, stop, or reinitialize the scheduler.

3.6 Guidelines on Performing Provisioning

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

 **See Also:**

[Guidelines on Using a Deployment Configuration](#)

This section provides more information about the following guidelines:

- [Guidelines While Performing Provisioning Operations in any of the supported deployment configurations](#)
- [Guidelines While Performing Provisioning Operations After Configuring the Access Request Management Feature of the Connector](#)

3.6.1 Guidelines While Performing Provisioning Operations in any of the supported deployment configurations

The following are guidelines that you must apply while performing provisioning operations in any of the supported deployment operations:

- If an ABAP data source is configured in SAP User Management Engine, then ABAP roles are shown as groups in SAP User Management Engine. However, SAP User Management Engine does not allow assigning such groups to user accounts in some configurations.

To assign groups that represent the AS ABAP role, create a new AS Java role in the User Administration tool of SAP User Management Engine. Then, assign

the group that represents the AS ABAP role to the newly created AS Java role in Oracle Identity Manager.

- If you disable a user account in Oracle Identity Manager, the connector updates the value of the Valid Through attribute with yesterday's date. If the user has logged in to the target system today, or if the password of the user was changed today, then SAP User Management Engine updates the Valid Through attribute with today's date and lock the user.

Ensure that the dates on Oracle Identity Manager and the SAP User Management Engine target system are in sync.

- The length of the Logon Name field varies in the target system based on the data source configuration. If a target system allows 15 characters, and if you enter more than 15 characters for the Logon Name field in Oracle Identity Manager, then an error is encountered. Therefore, the length of the Logon Name field must be limited to 15 characters in Oracle Identity Manager.
- Through provisioning, if you want to create and disable an account at the same time, then you can set the value of the Valid Through attribute to a date in the past. For example, while creating an account on 31-Jul, you can set the Valid Through date to 30-Jul. With this value, the resource provisioned to the OIM User is in the Disabled state immediately after the account is created.

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

- The value of the Valid Through attribute on Oracle Identity Manager and the target system do not match.
- On the target system, the user can log in all through the current day. The user cannot log in from the next day onward.

You can lock the user on the target system so that the user is not able to log in the day the account is created.

- Remember that if password or system assignment fails during a Create User provisioning operation, then the user is not created.
- When you try to provision a multivalued attribute, such as a role or group, if the attribute has already been set for the user on the target system, then the status of the process task is set to Completed in Oracle Identity Manager. If required, you can configure the task so that it shows the status Rejected in this situation. See *Modifying Process Tasks in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* 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.
- When you assign a role to a user through provisioning, you set values for the following attributes:

- Datasource
- Role

3.6.2 Guidelines While Performing Provisioning Operations After Configuring the Access Request Management Feature of the Connector

The following are 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 attributes on SAP BusinessObjects AC 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 the 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 BusinessObjects Access Control 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 BusinessObjects 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 Manager password as the target system password, change the password through Oracle Identity Manager.
 - Directly log in to the target system, and change the password.
- You perform an Enable User operation by setting the Valid From field to a future date. Similarly, you perform a Disable User operation by setting the Valid Through field to the current date. Both operations are treated as Modify User operations.
- When you delete a user (account) on Oracle Identity System Administration (process form), a Delete User request is created.
- When you select the Lock User check box on the process form, a Lock User request is created.
- When you deselect the Lock User check box on the process form, an Unlock User request is created.
- The Enable User and Disable User operations are implemented through the Valid From and Valid Through fields on the process form.
- In a Modify User operation, you can specify values for attributes that are mapped with SAP BusinessObjects AC Access Request Management and attributes that are directly updated on the target system. A request is created SAP BusinessObjects AC Access Request Management only for attributes whose mappings are present in these lookup definitions. If you specify values for attributes that are not present in these lookup definitions, then the connector sends them to directly the target system.

3.7 Configuring Provisioning in Oracle Identity Manager Release 11.1.1.x

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager release 11.1.1.x, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in [Switching Between Request-Based Provisioning and Direct Provisioning](#).

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes



See Also:

Manually Completing a Task in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for information about the types of provisioning

This section discusses the following topics:

- [Overview of the Provisioning Process in an SoD-Enabled Environment](#)
- [Direct Provisioning](#)
- [Direct Provisioning in an SoD-Enabled Environment](#)
- [Request-Based Provisioning](#)
- [Request-Based Provisioning in an SoD-Enabled Environment](#)
- [Switching Between Request-Based Provisioning and Direct Provisioning](#)

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

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

1. The provisioning operation triggers the appropriate adapter.
2. SAP BusinessObjects SoD Invocation Library (SIL) Provider passes the entitlement data to the Web service of SAP BusinessObjects AC.
3. After SAP BusinessObjects AC runs the SoD validation process on the entitlement data, the response from the process is returned to Oracle Identity Manager.
4. The status of the process task that received the response depends on the response itself. If the entitlement data clears the SoD validation process, then the adapter carries provisioning data to the corresponding SPML request on the target system and the status of the process task changes to Completed. This translates into the entitlement being granted to the user. If the SoD validation process returns the failure response, then status of the process task changes to Canceled.

3.7.2 Direct Provisioning

In direct provisioning, only Oracle Identity Manager administrators can create and manage target system resources.

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
 - a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
 - b. On the Create User page, enter values for the OIM User fields, and then click **Save**.

3. If you want to provision a target system account to an existing OIM User, then:
 - a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
 - b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. On the user details page, click the **Resources** tab.
5. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.
6. On the Step 1: Select a Resource page, select **SAPUME Resource Object** from the list and then click **Continue**.



Note:

If you are using SAP BusinessObjects AC system, then select **SAP AC UME Resource Object** from the list and then click **Continue**.

7. On the Step 2: Verify Resource Selection page, click **Continue**.
8. On the Step 5: Provide Process Data for SAPUME Process Form page, enter the details of the account that you want to create on the target system and then click **Continue**.
If you are using SAP BusinessObject AC system, you enter the details of the account on the Provide Process Data for SAP AC UME Process Form page.
9. If required, on the Step 5: Provide Process Data for SAPUME Group Form page, search for and select a group for the user on the target system and then click **Continue**.
If you are using SAP BusinessObjects AC system, then search for a select a group on the Provide Process Data for SAP AC UME Group Form.
10. If required, on the Step 5: Provide Process Data for SAPUME Role Form page, search for and select a role for the user on the target system and then click **Continue**.
If you are using SAP BusinessObjects AC system, then search for a select a role on the Provide Process Data for SAP AC UME Role Form.
11. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
12. The "Provisioning has been initiated" message is displayed. Close the window displaying this message.
13. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.7.3 Direct Provisioning in an SoD-Enabled Environment

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

- [Prerequisites](#)
- [Performing Direct Provisioning](#)

3.7.3.1 Prerequisites

 **Note:**

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

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

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

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

 **Note:**

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

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the **SAPUME process** process definition.
 - c. Deselect the Auto Save Form check box.
 - d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
 - a. Expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the **SAPUME Resource Object** resource object.
 - c. Deselect the **Self Request Allowed** check box.
 - d. Click the Save icon.

3.7.3.2 Performing Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
 - a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.

- b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM User, then:
 - a. On the Welcome to Identity Administration page, search for the OIM User by selecting Users from the drop-down list on the left pane.
 - b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. On the user details page, click the **Resources** tab.
5. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.
6. On the Step 1: Select a Resource page, select **SAPUME Resource Object** from the list and then click **Continue**.
7. On the Step 2: Verify Resource Selection page, click **Continue**.
8. On the Step 5: Provide Process Data page for process data, enter the details of the account that you want to create on the target system and then click **Continue**.
9. On the Step 5: Provide Process Data page for profile data, search for and select profiles for the user on the target system and then click **Continue**.
10. On the Step 5: Provide Process Data page for role data, search for and select roles for the user on the target system and then click **Continue**.
11. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
12. The "Provisioning has been initiated" message is displayed. Close the window displaying this message.
13. On the Resource tab of the user details page, click **Refresh** to view the newly provisioned resource.
14. To view the Resource Provisioning Details page, which shows the details of the process tasks that were run:

On the Resources tab of the user details page, from the Action menu, select **Resource History**.
15. The SOD Check Status field is updated with SOD Check Completed status.
16. As the administrator assigning a resource to a user, you can either end the process when a violation is detected or modify the assignment data and then resend it. To modify the assignment data, on the Resource tab of the user details page, select the row containing the resource, and then click **Open**.
17. In the Edit Form window that is displayed, you can modify the role and profile data that you had selected earlier.



Note:

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

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

Logon Name	<input type="text"/>	Street	<input type="text"/>
Password	<input type="password"/>	Language	<input type="text"/>
First Name	<input type="text"/>	Time Zone	<input type="text"/>
Last Name	<input type="text"/>	State	<input type="text"/>
E-Mail Address	<input type="text"/>	City	<input type="text"/>
Fax	<input type="text"/>	Zip	<input type="text"/>
Mobile	<input type="text"/>	User Account Locked	<input type="checkbox"/> No
Telephone	<input type="text"/>	Security Policy	<input type="text"/>
Department	<input type="text"/>	Unique ID	USER.PRIVATE_DATASOURCE.un:t
Name	<input type="text"/>	Country	<input type="text"/>
Title	<input type="text"/>	SoDCheckStatus	SODCheckCompleted
Form of Address	<input type="text"/>	SoDCheckResult	Passed
Position	<input type="text"/>	SoDCheckEntitlementViolation	
Start Date of Account Validity	<input type="text"/>	SoDCheckTimestamp	2015-10-16 04:53:28
End Date of Account Validity	12/31/2500		

18. After invoking the risk analysis web service, the results of the SoD validation process are brought to Oracle Identity Manager. If you open the process form, the results will be displayed as shown in the screenshot in Step 17.

3.7.4 Request-Based Provisioning

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.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

 **Note:**

The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- [Creating of Request-Based Provisioning by the End User](#)
- [Approving Request-Based Provisioning](#)

3.7.4.1 Creating of Request-Based Provisioning by the End User

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

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.
The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **SAPUME Resource Object**, move it to the Selected Resources list, and then click **Next**.

If you are using SAP BusinessObjects AC system, select SAP AC UME Resource Object
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 successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.7.4.2 Approving Request-Based Provisioning

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

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.

5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

A message confirming that the task was approved is displayed.

3.7.5 Request-Based Provisioning in an SoD-Enabled Environment

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.



See Also:

[Configuring SoD \(Segregation of Duties\)](#)

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 topics provide more information about request-based provisioning:

- [Creating of Request-Based Provisioning by End-Users](#)
- [Approving Request-Based Provisioning](#)

3.7.5.1 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 on Oracle Identity Manager release 11.1.1.x:



See Also:

Registering to Oracle Identity Manager of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.

2. On the Welcome page, click **Advanced** on the top right corner of the page.
3. On the Welcome to Identity Manager Advanced Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.
The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and then click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specified is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.
If you want to create a provisioning request for more than one user, then from the Available Users list, select the users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **SAPUME 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
 - JustificationOn the resulting page, a message confirming that your request has been sent is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. On the Resource tab of the Request Details page, click the View Details link in the row containing the resource for which the request was created. The Resource Details page is displayed in a new window.
One of the fields on this page is the SODCheckStatus field. The value in this field can be SoD Check Not Initiated or SoDCheckCompleted. When the request is placed, the SODCheckStatus field contains the SoDCheckCompleted status.
15. To view details of the approval, on the Request Details page, click the **Approval Tasks** tab.
On this page, the status of the SODChecker task is pending.

3.7.5.2 Approving Request-Based Provisioning

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

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

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 on Oracle Identity Manager release 11.1.1.x:

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

A message confirming that the task has been approved is displayed and the request status is changed to **Obtaining Operation Approval**.

6. Select the row containing the request which is approved, and then click **Approve Task**.

A message confirming that the task has been approved is displayed and the request status is changed to **Request Completed**.

7. Click the **Administration** tab and search for the user(s) for whom the request is completed.
8. Select the user.

The user detail information is displayed in the right pane.

9. Click the **Resources** tab to view the resource being provisioned.
10. Select the resource being provisioned, and then click **Open** to view the resource details.
11. On the Resources tab of the User Details page, from the **Action** menu, select **Resource History** to view the resource provisioning tasks.

3.7.6 Switching Between Request-Based Provisioning and Direct Provisioning

Note:

Perform this procedure only if you are using Oracle Identity Manager release 11.1.1.x. It is assumed that you have performed the procedure described in [Configuring Oracle Identity Manager for Request-Based Provisioning](#).

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager. Direct provisioning cannot be used if you enable request-based provisioning.

The following sections discuss the steps to be performed to switch between request-based provisioning and direct provisioning:

- [Switching from Request-Based Provisioning to Direct Provisioning](#)
- [Switching from Direct Provisioning to Request-Based Provisioning](#)

3.7.6.1 Switching from Request-Based Provisioning to Direct Provisioning

You can switch from request-based provisioning to direct provisioning using the following steps.

To switch from request-based provisioning to direct provisioning, do the following:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the **SAPUME process** process definition.

 **Note:**

If you are using SAP BusinessObjects AC system, then search for and open the **SAP AC UME process** process definition.

- c. Deselect the **Auto Save Form** check box.
 - d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
 - a. Expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the **SAPUME Resource Object** resource object.

 **Note:**

If you are using SAP BusinessObjects AC system, then search for and open the **SAP AC UME process** process definition.

- c. Deselect the **Self Request Allowed** check box.
- d. Click the Save icon.

3.7.6.2 Switching from Direct Provisioning to Request-Based Provisioning

You can switch from direct provisioning to request-based provisioning using the following steps.

To switch from direct provisioning to request-based provisioning, do the following:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the **SAPUME process** process definition.
 - c. Select the **Auto Save Form** check box.
 - d. Click the Save icon.
3. If you want to enable end users to raise requests for themselves, then:
 - a. Expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the **SAPUME Resource Object** resource object.

 **Note:**

If you are using SAP BusinessObjects AC system, then search for and open the **SAP AC UME Resource Object** resource object.

- c. Select the **Self Request Allowed** check box.
- d. Click the Save icon.

3.8 Configuring Provisioning in Oracle Identity Manager Release 11.1.2.x

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

To configure provisioning operations in Oracle Identity Manager release 11.1.2.x:

 **Note:**

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

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see *Managing Sandboxes in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
3. Create an application instance. To do so:
 - a. In the left pane, under Configuration, click **Application Instances**. The Application Instances page is displayed.
 - b. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Application Instance page is displayed.

- c. Specify values for the following fields:

Name: The name of the application instance.

Name: The 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 **SAPUME Resource Object**. If you are using SAP BusinessObjects AC system, then select **SAP AC UME Resource Object**.

IT Resource Instance: The IT resource instance name. Click the search icon next to this field to search for and select **SAPUME IT Resource**. If you are using SAP BusinessObject AC system, then select **SAP AC UME IT Resource**.

Form: Select the form name, for example, **SAPUME** (or **SAPACUME** for SAP BusinessObjects AC system). To do so, click **Create** against the Form list, specify the form name, and then create it. On the Create Application Instance page, click the Refresh icon next to the Form field. From this list, select the form name that you created.

 **Note:**

If you are using SAP BusinessObjects AC system, then:

- **Resource Object:** SAP AC UME Resource Object
- **IT Resource Instance:** SAP AC UME IT Resource
- **Form:** UD_SAPACUME

4. Publish the sandbox.
5. Run lookup field synchronization. See [Scheduled Job for Lookup Field Synchronization](#) and [Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization](#) for more information.
6. Search for and run the Entitlement List scheduled job to populate the ENT_LIST table. See [Configuring Scheduled Jobs](#) for more information about configuring and running scheduled jobs.
7. Publish the application instance (created in Step 3) to an organization. To do so:
 - a. On the Organizations tab of the Application Instance page, click **Assign**.
 - b. In the Select Organizations dialog box, select the organization to which you want to publish the application instance.
 - c. Select the **Apply to entitlements** checkbox.
 - d. Click **OK**.
8. Search for and run the Catalog Synchronization Job scheduled job. See [Configuring Scheduled Jobs](#) for more information about configuring and running scheduled jobs.
9. Log in to Oracle Identity System Administration.

10. Create a user. See *Managing Users in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
11. On the Account tab, click **Request Accounts**.
12. In the Catalog page, search for and add to cart the application instance created in Step 3, and then click **Checkout**.
13. Specify value for fields in the application form and then click **Ready to Submit**.
14. Click **Submit**.
15. If you want to provision entitlements, then:
 - a. On the Entitlements tab, click **Request Entitlements**.
 - b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout**.
 - c. Click **Submit**.

3.9 Uninstalling the Connector

If you want to uninstall the connector for any reason, see *Uninstalling Connectors in Oracle Fusion Middleware Administering Oracle Identity Manager*.

4

Extending the Functionality of the Connector

You can extend the functionality of the connector to address your specific business requirements.

This chapter discusses the following optional procedures:

Note:

From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See *Managing Lookups of Oracle Fusion Middleware Administering Oracle Identity Manager* guide for information about managing lookups by using the Form Designer in Oracle Identity Manager System Administration.

- [Determining the Names of Target System Attributes](#)
- [Adding New Attributes for Reconciliation](#)
- [Adding New Attributes for Provisioning](#)
- [Adding New Standard SAP BusinessObjects AC Access Request Management Attributes for Provisioning](#)
- [Removing SAP BusinessObjects AC Access Request Management Attributes from Process Form](#)
- [Configuring Validation of Data During Reconciliation and Provisioning](#)
- [Configuring Transformation of Data During User Reconciliation](#)
- [Modifying Field Lengths on the Process Form](#)
- [Configuring the Connector for Multiple Installations of the Target System](#)
- [Defining the Connector](#)

4.1 Determining the Names of Target System Attributes

This section describes the procedure to determine the names of standard single-valued target system attributes that you want to add for reconciliation or provisioning. The names that you determine are used to determine values for the Decode column of the lookup definitions such as Lookup.SAPUME.UM.ReconAttrMap and Lookup.SAPUME.UM.ProvAttrMap that hold attribute mappings.

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

1. Open the schema.xml file provided with AS Java.

2. In the section containing the object class definition for `sapuser`, the `memberAttributes` element defines the list of attributes available.

4.2 Adding New Attributes for Reconciliation

You can map new attributes between Oracle Identity manager and the target system for reconciliation.

Note:

This section describes an optional procedure. Perform this procedure only if you want to add new attributes for target resource reconciliation.

You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the attributes listed in [User Attributes for Reconciliation](#) are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation.

To add a new attribute for target resource reconciliation, perform the procedures listed in the following sections:

- [Creating a New Version of the Process Form](#)
- [Adding the New Attribute to the List of Reconciliation Field in the Resource Object](#)
- [Creating a Reconciliation Field Mapping for the New Attribute](#)[Creating an Entry for the Attribute in the Lookup Definition for Reconciliation](#)
- [Creating an Entry for the Attribute in the Lookup Definition for Reconciliation](#)
- [Defining the Connector](#)
- [Creating a New UI Form to make the New Attribute Visible](#)

4.2.1 Creating a New Version of the Process Form

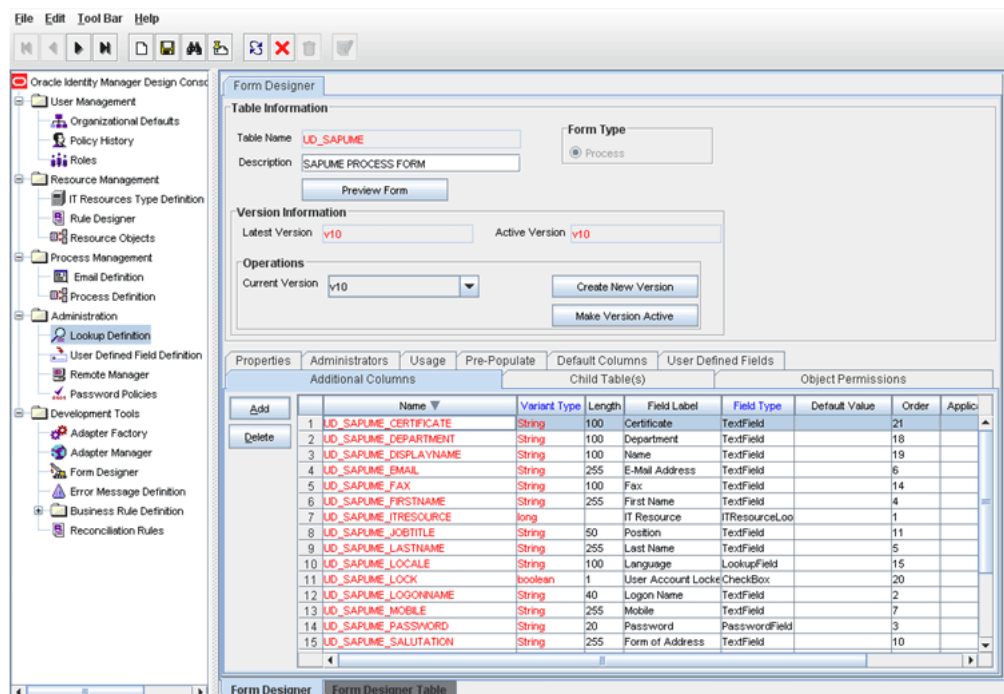
To add a new attribute for target resource reconciliation:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Form Designer**.
4. Search for and open the **SAPUME process** process form.
5. Click **Create New Version**.
6. In the **Label** field, enter the version name. For example, `version#1`.
7. Click the Save icon.
8. Select the current version created in Step e from the **Current Version** list.
9. Click **Add** to create a new attribute, and provide the values for that attribute.

For example, if you are adding the `Certificate` attribute, then enter the following values in the **Additional Columns** tab:

Field	Value
Name	Certificate
Variant Type	String
Length	100
Field Label	certificate
Order	20

The following screenshot shows this form:



10. Click the Save icon.
11. Click **Make Version Active**.

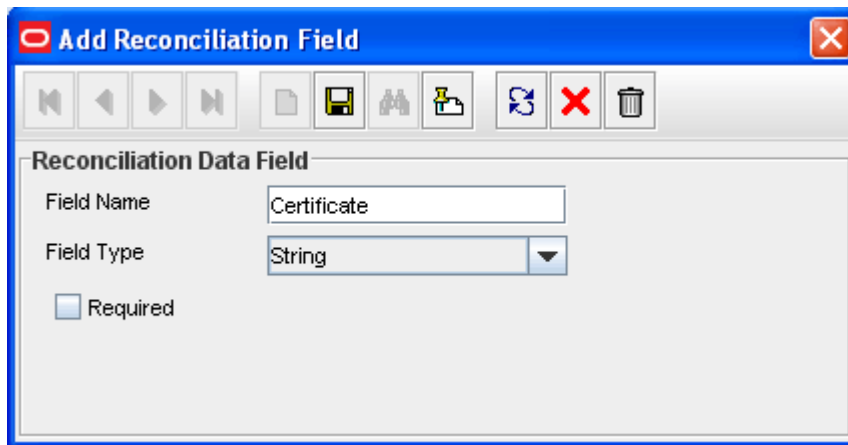
4.2.2 Adding the New Attribute to the List of Reconciliation Field in the Resource Object

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

1. Expand **Resource Management**.
2. Double-click **Resource Objects**.
3. Search for and open the **SAPUME Resource Object** resource object.
4. On the **Object Reconciliation** tab, click **Add Field**, and then enter the following values:

Field Name: `Certificate`

Field Type: String



5. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.
6. Click the Save icon.

4.2.3 Creating a Reconciliation Field Mapping for the New Attribute

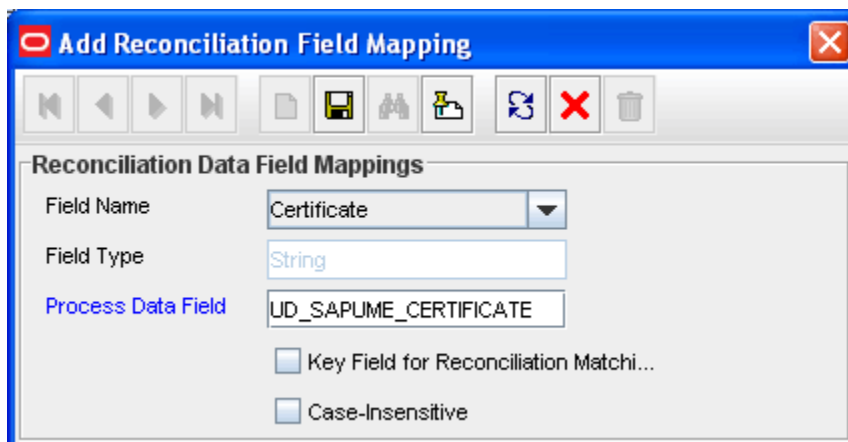
Create a reconciliation field mapping for the new attribute in the process definition form as follows:

1. Expand **Process Management**.
2. Double-click **Process Definition**.
3. Search for and open the **SAPUME process** process definition.
4. On the **Reconciliation Field Mappings** tab, click **Add Field Map**, and then select the following values:

Field Name: Certificate

Field Type: String

Process Data Field:



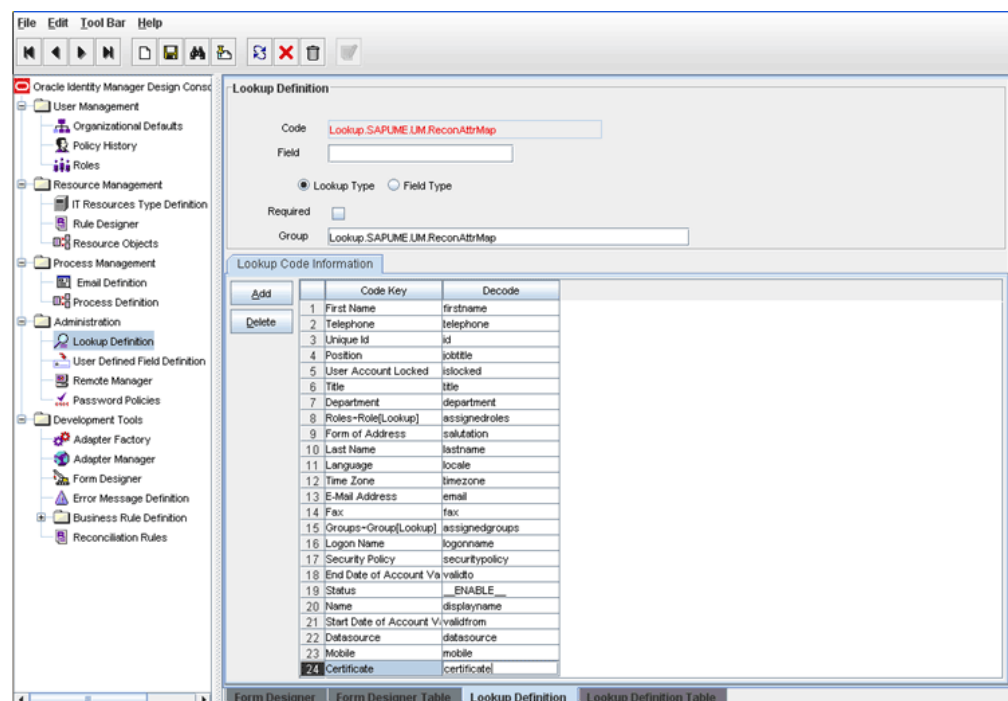
5. Click the Save icon.

4.2.4 Creating an Entry for the Attribute in the Lookup Definition for Reconciliation

If you are using Oracle Identity Manager release prior to 11.1.2, create an entry for the attribute in the lookup definition for reconciliation as follows:

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open the **Lookup.SAPUME.UM.ReconAttrMap** lookup definition.
4. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the resource object field. The Decode value is the name of the attribute in the target system.

For example, enter `Certificate` in the **Code Key** field and then enter `certificate` in the **Decode** field.



5. Click the Save icon.

4.2.5 Defining the Connector

If you are using Oracle Identity Manager release prior to 11.1.2, define the connector. If you are planning to perform any of the other procedures described in this chapter, perform those procedures and then define the connector. See [Defining the Connector](#) for more information.

4.2.6 Creating a New UI Form to make the New Attribute Visible

If you are using Oracle Identity Manager release 11.1.2.x or later, create a new UI form and attach it to the application instance to make this new attribute visible. See [Creating a New UI Form](#) and [Updating an Existing Application Instance with a New Form](#) for the procedures.

4.3 Adding New Attributes for Provisioning

You can map additional attributes for provisioning between Oracle Identity Manager and the target system.

 **Note:**

This section describes an optional procedure. Perform this procedure only if you want to add new attributes for provisioning.

By default, the attributes listed in [User Attributes for Provisioning](#) are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a new attribute for provisioning, perform the procedures listed in the following sections:

 **Note:**

You need not perform steps that you have already performed as part of the procedure described in [Adding New Attributes for Reconciliation](#).

- [Creating a New Version of the Process Form.](#)
- [Creating an Entry for the Attribute in the Lookup Definition for Provisioning.](#)
- [Updating the Request Dataset.](#)
- [Running the PurgeCache Utility to Clear Content Related to Request Datasets.](#)
- [Importing the Modified Request Datasets Using the Deployment Manager.](#)
- [Updating the New Attribute for Provisioning a User .](#)
- [Defining the Connector.](#)
- [Creating a New UI Form to the Make the New Attribute Visible.](#)

4.3.1 Creating a New Version of the Process Form

To create a new version of a process form:

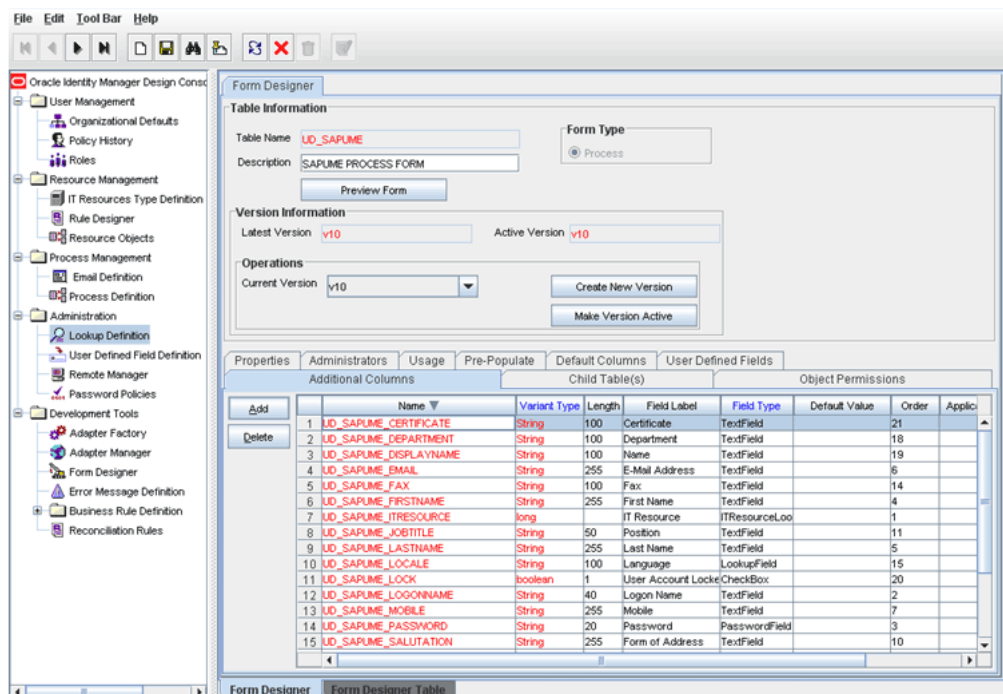
If you have added the attribute on the process form by performing [Creating a New Version of the Process Form](#) then you need not add the attribute again. If you have not added the attribute, then:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Form Designer**.
4. Search for and open the **UD_SAPUME** process form.
5. Click **Create New Version**.
6. In the **Label** field, enter the version name. For example, `version#1`.
7. Click the Save icon.
8. Select the current version created in Step e from the **Current Version** list.
9. Click **Add** to create a new attribute, and provide the values for that attribute.

For example, if you are adding the certificate attribute, then enter the following values in the **Additional Columns** tab:

Field	Value
Name	certificate
Variant Type	String
Length	100
Field Label	Certificate
Order	20

The following screenshot shows this form:



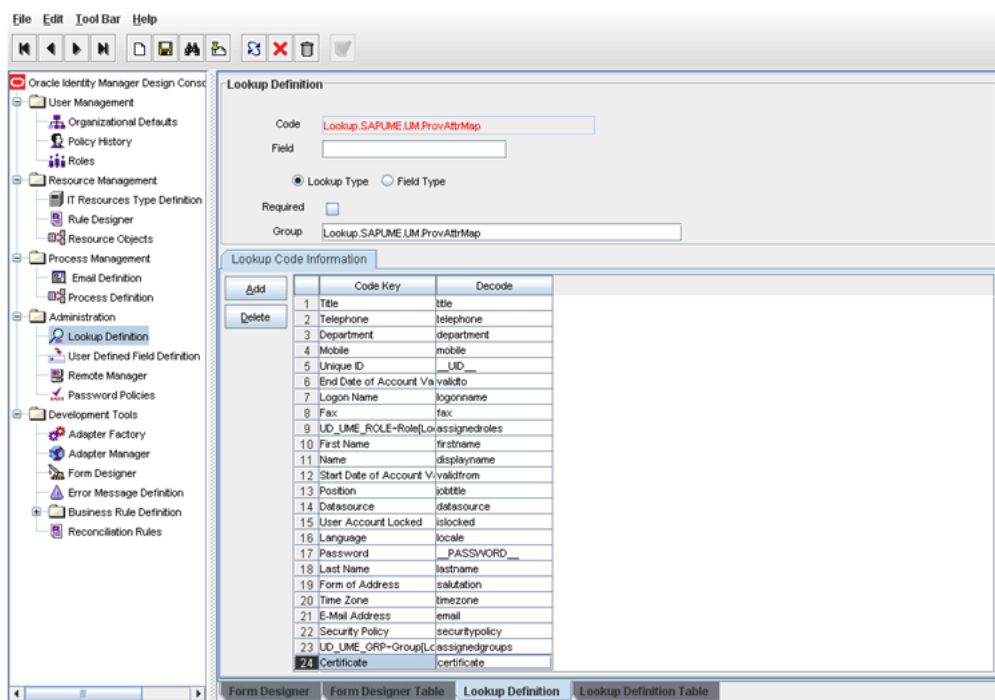
10. Click the Save icon.
11. Click **Make Vcersion Active**.

4.3.2 Creating an Entry for the Attribute in the Lookup Definition for Provisioning

Create an entry for the attribute in the lookup definition for provisioning as follows:

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open the **Lookup.SAPUME.UM.ProvAttrMap** lookup definition.
4. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the value specified in the Field Label column in the process form. The Decode value is the name of the attribute in the target system.

For example, enter `Certificate` in the **Code Key** field and then enter `certificate` in the **Decode** field.



5. Click the Save icon.

 **Note:**

Perform the following procedures only if you want to perform request-based provisioning.

- [Updating the Request Dataset](#)
- [Running the PurgeCache Utility to Clear Content Related to Request Datasets](#)
- [Importing the Modified Request Datasets Using the Deployment Manager](#)

4.3.3 Updating the Request Dataset

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

1. In a text editor, open the `SAPUME-Datasets.xml` file located in the `xml` directory of the installation media.
2. Add the `AttributeReference` element and specify values for the mandatory attributes of this element.

For example, while performing Step 2 of this procedure, if you added `certificate` as an attribute on the process form, then enter the following line:

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

In this `AttributeReference` element:

- For the `name` attribute, enter the value in the `Name` column of the process form without the `tablename` prefix.
For example, if `UD_SAPUME_CERTIFICATE` is the value in the `Name` column of the process form, then you must specify `Certificate` as the value of the `name` attribute in the `AttributeReference` element.
- For the `attr-ref` attribute, enter the value that you entered in the `Field Label` column of the process form while performing Step 2.
- For the `type` attribute, enter the value that you entered in the `Variant Type` column of the process form while performing Step 2.
- For the `widget` attribute, enter the value that you entered in the `Field Type` column of the process form, while performing Step 2.
- For the `length` attribute, enter the value that you entered in the `Length` column of the process form while performing Step 2.
- For the `available-in-bulk` attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing Step 2, if you added more than one attribute on the process form, then repeat this step for each attribute added.

3. Save and close the XML file.

4.3.4 Running the PurgeCache Utility to Clear Content Related to Request Datasets

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

See *Purging Cache in Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.

4.3.5 Importing the Modified Request Datasets Using the Deployment Manager

Import this modified request datasets in XML format using the deployment manager.

See [Importing Request Datasets Using Deployment Manager](#) for detailed information about the procedure.

4.3.6 Updating the New Attribute for Provisioning a User

To enable the update of a new attribute for provisioning a user:

1. Expand **Process Management**.
2. Double-click **Process Definition** and open the **SAPUME process** process definition.
3. In the process definition, add a new task for updating the field as follows:
 - Click **Add** and enter the task name, for example, `CellPhone Updated`, and the task description.
 - In the Task Properties section, select the following fields:
 - Conditional
 - Required for Completion
 - Allow Cancellation while Pending
 - Allow Multiple Instances
 - Click the Save icon.
4. On the Integration tab, click **Add**, and then click **Adapter**.
5. Select the **sapume update** adapter, click **Save**, and then click **OK** in the message that is displayed.
6. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify the data given in the following table:

Variable Name	Data Type	Map To	Qualifier	Literal Value
Adapter return value	Object	Response code	NA	NA

Variable Name	Data Type	Map To	Qualifier	Literal Value
objectType	String	Literal	String	User
itResourceFieldName	String	Literal	String	UD_SAPUME_RESOURCETYPE
IProcessInstKey	Long	Process data	Iprocessinstance	NA

- On the Responses tab, click **Add** to add the following response codes:

Code Name	Description	Status
ERROR	Error occurred during Certificate update	R
CONNECTOR_EXCEPTION	Certificate update Failed	R
INVALID_CREDENTIAL	Unauthorized user Login	R
UNKNOWN	UNKNOWN	R
CONNECTION_FAILED	Cannot make connection to the resource	R
UNKNOWN_UID	User does not exist in the target	R
SUCCESS	Certificate update Successful	C

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

4.3.7 Defining the Connector

Define the connector. If you are planning to perform any of the other procedures described in this chapter, perform those procedures and then define the connector. See [Defining the Connector](#) for more information.

4.3.8 Creating a New UI Form to the Make the New Attribute Visible

If you are using Oracle Identity Manager release 11.1.2.x or later, create a new UI form and attach it to the application instance to make this new attribute visible. See [Creating a New UI Form](#) and [Updating an Existing Application Instance with a New Form](#) for the procedures.

4.4 Adding New Standard SAP BusinessObjects AC Access Request Management Attributes for Provisioning

You can map additional single-valued attributes between Oracle Identity Manager and SAP BusinessObjects AC Access Request Management.

By default, the attributes listed in [Table 1-6](#) and [Table 1-10](#) are mapped for sending requests from Oracle Identity Manager to SAP BusinessObjects AC Access Request Management. If required, you can map additional single-valued attributes.

Note:

Perform the procedure described in this section only if you want to map additional standard Access Request Management attributes for requests sent from Oracle Identity Manager to Access Request Management.

To add a new SAP BusinessObjects AC Access Request Management attribute for provisioning, perform the procedures in the following sections:

- [Creating a New Version of the Process Form](#)
- [Creating an Entry for the Attribute in the Lookup Definition](#)
- [Creating a Process Task to Update the Attribute During Provisioning Operations](#)
- [Creating a New UI Form and attaching it to the Application Instance to make the New Attribute Visible](#)

4.4.1 Creating a New Version of the Process Form

If the attribute does not already exist on the process form, then add it on the process form as follows:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_SAPACUME** process form.
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the attribute.

For example, if you are adding the Telephone field, enter `UD_SAPACUME_TELEPHONE` in the Name field, and then enter the rest of the details of this field.

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

The screenshot shows the Oracle Identity Manager Design Console interface. The main window is titled 'Form Designer' and displays the 'UD_SAPACUME' process form. The 'Table Information' section shows the table name 'UD_SAPACUME' and the form type 'Process'. The 'Version Information' section shows the latest version as 'version 17' and the active version as 'version 18'. The 'Operations' section shows the current version as 'version 18' and buttons for 'Create New Version' and 'Make Version Active'. Below this, a table lists the fields in the process form:

Additional Columns	Child Table(s)	Object Permissions	Properties	Administrators	Usage	Pre-Populate	Default Columns	User Defined Fields
Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encrypted
1 UD_SAPACUME_TELEPHONE	String	100	TELEPHONE	TextField		47		
2 UD_SAPACUME_RESOURCETYPE	long		IT Resource	ITResource		1		
3 UD_SAPACUME_USERID	String	40	Login Name	TextField		2		
4 UD_SAPACUME_PASSWORD	String	20	Password	PasswordField		3		
5 UD_SAPACUME_FIRSTNAME	String	255	First Name	TextField		4		
6 UD_SAPACUME_LASTNAME	String	255	Last Name	TextField		5		
7 UD_SAPACUME_EMAIL	String	255	E-Mail Address	TextField		6		
8 UD_SAPACUME_FAX	String	100	Fax	TextField		7		
9 UD_SAPACUME_MOBILE	String	255	Mobile	TextField		8		
10 UD_SAPACUME_TELEPHONE	String	255	Telephone	TextField		9		
11 UD_SAPACUME_DEPARTMENT	String	100	Department	TextField		10		
12 UD_SAPACUME_DISPLAYNAME	String	100	Name	TextField		11		
13 UD_SAPACUME_TITLE	String	20	Title	TextField		12		
14 UD_SAPACUME_CALIFICATION	String	255	Form of Address	TextField		13		
15 UD_SAPACUME_ORGTITLE	String	50	Position	TextField		14		
16 UD_SAPACUME_VALID_FROM	Date		Start Date of Account	DateFieldDtg		15		
17 UD_SAPACUME_VALID_TO	Date		End Date of Account	DateFieldDtg	13/1/2000	16		

4.4.2 Creating an Entry for the Attribute in the Lookup Definition

Create an entry for the attribute in the Lookup.SAPAC10UME.UM.ProvAttrMap lookup definition as follows:

1. Expand Administration.
2. Double-click Lookup Definition.
3. Search for and open the Lookup.SAPAC10UME.UM.ProvAttrMap lookup definition.
4. Click Add and then enter the Code Key and Decode values for the attribute.

The Code Key value must be the name of the field on the process form. The Decode value is in the following format:

FIELD_NAME;*CUSTOM*

In this format:

- *FIELD_NAME* is the name of the attribute.
- *CUSTOM* is used to specify that the attribute is a custom attribute on SAP BusinessObjects AC Access Request Management.

4.4.3 Creating a Process Task to Update the Attribute During Provisioning Operations

Create a process task to enable update of the attribute during provisioning operations if the following conditions are true:

- The task does not already exist.
- This attribute exists on both SAP BusinessObjects AC Access Request Management and the target system.

Note:

If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of the attribute during provisioning operations, add a process task for updating the attribute:

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open the **SAP AC UME process** definition.
3. Click **Add**.
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
 - Conditional

- Required for Completion
 - Required for Completion
 - Allow Cancellation while Pending
 - Allow Multiple Instances
5. Click the Save icon.
 6. On the Integration tab of the Creating New Task dialog box, click **Add**.
 7. In the Handler Selection dialog box, select **Adapter**, click **adpSAPACUMEUPDATE**, and then click the Save icon.

The list of adapter variables is displayed on the Integration tab.

8. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the Save icon.

9. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Name	Map To	Qualifier
fieldValue	ProcessData	Telephone Number
fieldName	Literal	String For example: UD_SAPACUME_TELEPHONENUMBER
itResourceFieldName	Literal	String For example: UD_SAPACUME_RESOURCETYPE
objectType	Literal	String For example: User
IProcessInstanceKey	Process Data	Process Instance
fieldOldValue	Process Data	Telephone Number Note: Select the Old Value check box.
Adapter Return Variable	Response Code	N/A

10. Click the Save icon in the Editing Task dialog box, and then close the dialog box.
11. Click the Save icon to save changes to the process definition.

4.4.4 Creating a New UI Form and attaching it to the Application Instance to make the New Attribute Visible

If you are using Oracle Identity Manager release 11.1.2.x or later, create a new UI form and attach it to the application instance to make this new attribute visible. See [Creating a New UI Form](#) and [Updating an Existing Application Instance with a New Form](#) for the procedures.

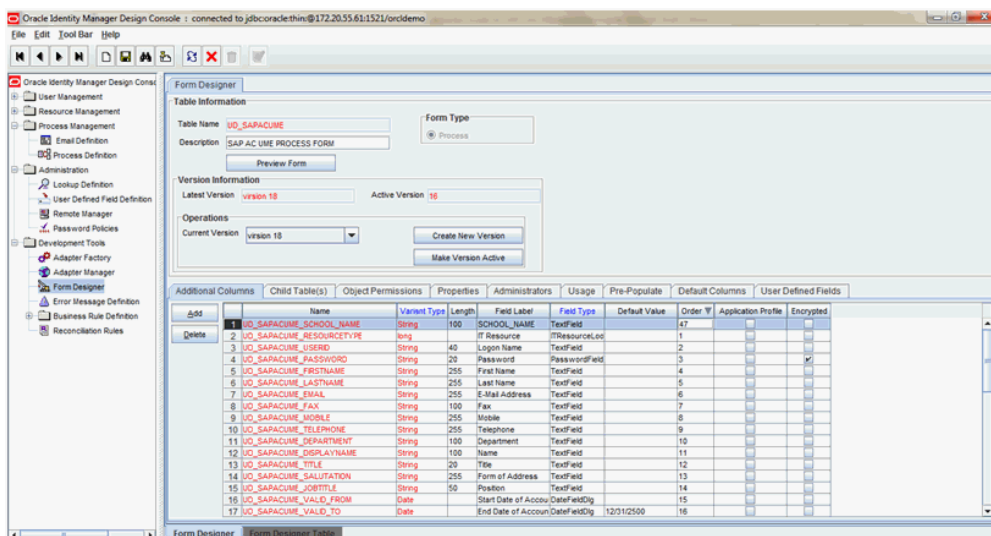
4.5 Removing SAP BusinessObjects AC Access Request Management Attributes from Process Form

You can remove SAP BusinessObjects AC Access Request Management attributes if the connector is not configured for SAP BusinessObjects AC.

The form attributes used for Access Request Management are prefixed with AC. These attributes are available in the process form. If the connector is not configured for SAP BusinessObjects AC, then the AC-specific attributes can be removed manually. See [SAP BusinessObjects AC Access Request Management Attributes](#) for list of attributes.

To remove the AC attributes from the process form:

1. From Oracle Identity Manager Design Console, expand **Development Tools**.
2. Double-click **Form Designer**.
3. Search for and open the **UD_SAPACUME** process form.
4. Click **Create New Version**.
5. In the Label field, enter the version name. For example, `version#1`.
6. Click the Save icon.
7. Select the current version created in Step 5 from the Current Version list.
8. Select the AC field to be removed.
9. Click **Delete** to remove the selected attribute row from the form.
10. Similarly, repeat Steps 8 and 9 until you remove all the AC attributes.
11. Click the Save icon. The following screenshot shows to remove the AC attributes from the process form:



12. Click **Make Version Active**.

13. If you are using Oracle Identity Manager release 11.1.1, after you remove an attribute on the process form, you must update the XML file containing the request dataset definitions. To update a request dataset:

- a. Locate and open the SAPUME-Datasets.xml file, which is located in the xml directory of the installation media.
- b. Search for and find the AC field tags. You can either comment or delete the entire set of AC field tags in the XML file.
- c. Save and close the XML file.
- d. Run the PurgeCache utility to clear content related to request datasets from the server cache.
- e. Import into MDS the request dataset definitions in XML format.

See [Importing Request Datasets Using Deployment Manager](#) for detailed information about the procedure.

4.5.1 SAP BusinessObjects AC Access Request Management Attributes

The form attributes used for Access Request Management are prefixed with AC. These attributes are available in the process form.

The following is the list of AC attributes:

- AC Manager
- AC Manager email
- AC Priority
- AC System
- AC Requestor ID
- AC Requestor email
- AC Request Reason

- AC Manager First Name
- AC Manager Last Name
- AC Manager Telephone
- AC Request Due Date
- AC Functional Area
- AC Business Process
- AC Requestor First Name
- AC Requestor Last Name
- AC Requestor Telephone
- AC Company

4.6 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

Note:

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

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

This validation class must implement the validate method.

The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

```
package com.validationexample;

import java.util.HashMap;

public class MyValidator {
    public boolean validate(HashMap hmUserDetails, HashMap
hmEntitlementDetails, String sField) throws ConnectorException {

        /* You must write code to validate attributes. Parent
        * data values can be fetched by using
hmUserDetails.get(field)
        * For child data values, loop through the
        * ArrayList/Vector fetched by
hmEntitlementDetails.get("Child Table")
        * Depending on the outcome of the validation operation,
```



```

        * the code must return true or false.
        */
    /*
    * In this sample code, the value "false" is returned if the field
    * contains the number sign (#). Otherwise, the value "true" is
    * returned.
    */
    boolean valid = true;
    String sFirstName = (String) hmUserDetails.get(sField);
    for (int i = 0; i < sFirstName.length(); i++) {
        if (sFirstName.charAt(i) == '#') {
            valid = false;
            break;
        }
    }
    return valid;
}
}
}

```

2. If you created the Java class for validating a process form field for reconciliation, then:
 - a. Log in to the Design Console.
 - b. Search for and open the **Lookup.SAPUME.UM.ReconValidation** or create another custom name) lookup definition.

 **Note:**

If you cannot find the **Lookup.SAPUME.UM.ReconValidation** lookup definition, create a new lookup definition.

- c. In the **Code Key** column, enter the resource object field name that you want to validate.
 - d. In the **Decode** column, enter the class name. For example, `com.VALIDATIONEXAMPLE.MYVALIDATOR`.
 - e. Save the changes to the lookup definition.
 - f. Search for and open the **Lookup.SAPUME.Configuration** lookup definition.
 - g. In the **Code Key** column, enter `Recon Validation Lookup`.
 - h. In the **Decode** column, enter the name of the lookup you created in step 2.b.
 - i. Save the changes to the lookup definition.
3. If you created the Java class for validating a process form field for provisioning, then:
 - a. Log in to the Design Console.
 - b. Search for and open the **Lookup.SAPUME.UM.ProvValidation** or create another custom name) lookup definition.

 **Note:**

If you cannot find the `Lookup.SAPUME.UM.ProvValidation` lookup definition, create a new lookup definition.

- c. In the **Code Key** column, enter the process form field name that you want to validate.
- d. In the **Decode** column, enter the class name. For example, `com.VALIDATIONEXAMPLE.MYVALIDATOR`.
- e. Save the changes to the lookup definition.
- f. Search for and open the **Lookup.SAPUME.Configuration** lookup definition.
- g. In the **Code Key** column, enter `Provisioning Validation Lookup`.
- h. In the **Decode** column, enter `Lookup.SAPUME.UM.ProvValidation` or enter the name of the lookup you created in step 3.b.
- i. Save the changes to the lookup definition.

4.7 Configuring Transformation of Data During User Reconciliation

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

 **Note:**

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

To configure transformation of single-valued user data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class.

This transformation class must implement the transform method.

The following sample transformation class creates a value for the Full Name attribute by using values fetched from the First Name and Last Name attributes of the target system:

```
package com.transformationexample;

import java.util.HashMap;

public class MyTransformer {
    public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails, String sField) throws ConnectorException {
        /*
         * You must write code to transform the attributes.
         * Parent data attribute values can be fetched by
```

```

        * using hmUserDetails.get("Field Name").
        * To fetch child data values, loop through the
        * ArrayList/Vector fetched by
hmEntitlementDetails.get("Child      Table")
        * Return the transformed attribute.
        */
String sFirstName = (String) hmUserDetails.get("First Name");
String sLastName = (String) hmUserDetails.get("Last Name");
return sFirstName + "." + sLastName;

    }
}

```

2. Log in to the Design Console.
3. Search for and open the **Lookup.SAPUME.UM.ReconTransformation** (or create another custom name) lookup definition.

 **Note:**

If you cannot find the Lookup.SAPUME.UM.ReconTransformation lookup definition, create a new lookup definition.

4. In the **Code Key** column, enter the resource object field name you want to transform.
5. In the **Decode** column, enter the class name. For example, com.TRANSFORMATIONEXAMPLE.MYTRANSFORMER.
6. Save the changes to the lookup definition.
7. Search for and open the **Lookup.SAPUME.Configuration** lookup definition.
8. In the **Code Key** column, enter Recon Transformation Lookup.
9. In the **Decode** column, enter Lookup.SAPUME.UM.ReconTransformation or enter the name of the lookup you created in step 3.
10. Save the changes to the lookup definition.

4.8 Modifying Field Lengths on the Process Form

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

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

1. Log in to the Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_UME** process form.



Note:

If you are using SAP BusinessObjects AC system, then search for and open the **UD_SAPACUME** process form.

4. Click **Create New Version**.
5. Enter a label for the new version, click the Save icon, and then close the dialog box.
6. From the **Current Version** list, select the version that you create.
7. Modify the length of the required field.
8. Click the Save icon.
9. Click **Make Version Active**.

4.9 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector for multiple installations of the target system.

The following example illustrates this requirement:

The London and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you can create copies of connector objects, such as the IT resource and resource object.

The decision to create a copy of a connector object might be based on a requirement. For example, an IT resource can hold connection information for one target system installation. Therefore, it is mandatory to create a copy of the IT resource for each target system installation.

With some other connector objects, you do not need to create copies at all. For example, a single attribute-mapping lookup definition can be used for all installations of the target system.

If you want to create copies of all the objects that constitute the connector, then see Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4.10 Defining the Connector

By using the Identity System Administration, you can define a customized or reconfigured connector. Defining a connector is equivalent to registering the connector with Oracle Identity Manager.

A connector is automatically defined when you install it using the Install Connectors feature or when you upgrade it using the Upgrade Connectors feature. You must manually define a connector if:

- You import the connector by using the Deployment Manager.
- You customize or reconfigure the connector.
- You upgrade Oracle Identity Manager.

The following events take place when you define a connector:

- A record representing the connector is created in the Oracle Identity Manager database. If this record already exists, then it is updated:
- The status of the newly defined connector is set to Active. In addition, the status of a previously installed release of the same connector automatically is set to Inactive.

See Defining Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the procedure to define connectors.

5

Known Issues, Limitations, and FAQs

These are the known issues and limitations associated with the SAP UME connector.

This chapter is divided into the following sections:

- [Known Issues](#)
- [Connector Limitations Related to Features of the Target System](#)
- [Frequently Asked Questions \(FAQs\)](#)

5.1 Known Issues

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

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

- **Bug 14152765**

If the size of the violation details obtained from SAP BusinessObjects AC target system is more than 4000 characters, then you must update the Length of the SODCheckViolation field as per the expected size of the violation data.

- **Bug 13248559**

After performing user reconciliation on the user form in the Administrative and User Console, the code key values are displayed instead of the decode values.

- **Bug 13343976**

If you configure the connector to communicate with the Connector Server using SSL, including setting the `connectorserver.usessl` property to true and importing the target system certificate into the Connector Server JDK keystore, an attempt to access the target system or run the Connector Server returns an error.

There is no workaround for this issue. Do not use SSL to communicate with the Connector Server.

- **Bug 28217796**

While creating a user in the enterprise portal through a GRC access request with valid date on the system set at 31/12/9999, the following error message is encountered:

```
Exception while creating user:  
BAPI_USER_CREATE1@GR1CLNT001:TYPE=E, ID=S5, NUMBER=003,
```

Workaround is to apply the following SNOTEs on top of GRCFND_A SP 10:

- SNOTE 2653244
- SNOTE 2203867
- **Bug 23342634**

Lookup Data of Timezone, Country, and Locale is not Dynamic.

During provisioning and reconciliation, the look up data of timezone, country, and locale can be inconsistent with the target system because the lookup values were generated during the earlier versions of Netweaver.

If there is any mismatch in data between target and lookup, the workaround is for the customer to modify the lookup definitions manually in the Oracle Identity Manager Design console

- **Bug 23559285**

In the 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 NetWeaver Java Application server (backend Java Stack) and you cannot modify the account details in Oracle Identity Manager.

There is no workaround for this issue.

5.2 Connector Limitations Related to Features of the Target System

The following are connector limitations related to features of the target system:

- The SPML UME API does not return records for which the Last Modified Date value is greater than a specified date. Therefore, the connector cannot support incremental reconciliation.
- Configurable batched reconciliation is not supported. The connector performs batched reconciliation implicitly when it first fetches user records with logonname that begin with valid characters allowed in the target system.

In addition, the following sections describe specific connector limitations:

- [Limitations for AS ABAP Data Source for the Connector](#)
- [Limitations for Groups That Represent AS ABAP Roles](#)
- [Limitations for Role Management with the Connector](#)

5.2.1 Limitations for AS ABAP Data Source for the Connector

These are the limitations associated with AS ABAP Data source for the connector.

- Limitation when searching for users
The search considers only actions performed using the AS Java tools. Therefore, the connector cannot search using the last modified timestamp.
- List of SAP User Management Engine (UME) user attributes
The list of user attributes that can be read from or written to the SAP UME with an AS ABAP data source is fixed and cannot be extended. However, a backend AS ABAP system can have additional attributes, but these attributes are not supported from the SAP UME.
- Delay in the display of AS ABAP roles in the SAP UME
If you create a new AS ABAP role or change the description of an existing AS ABAP role, these changes might not be visible in the SAP UME for up to 30 minutes. The SAP UME reads this data from the AS ABAP data source every 30

minutes. To force the SAP UME to read the data from the AS ABAP data source, you must restart the AS Java. Therefore, performing a reconciliation operation might lose roles that have been created recently.

- Limitation in a Central User Administration (CUA) environment

The SAP UME can view only the roles that are present in the central system. Roles in child systems are not visible to the SAP UME. Therefore, you can view and maintain role assignments from the connector only to the central system.

- The SAP UME does not support maintaining the Form of Address and TimeZone attributes in an AS ABAP data source.

5.2.2 Limitations for Groups That Represent AS ABAP Roles

The SAP UME groups that represent AS ABAP roles on the target system have the following limitations for the connector:

- You can assign ABAP users only to the SAP UME groups that represent ABAP roles.
- The SAP UME cannot show a user-group assignment when the current date is outside the validity period of the corresponding user-role assignment in the AS ABAP data source.
- If you try to assign a SAP UME group to a user when the user is already assigned to the corresponding ABAP role, but the current date is outside the validity period, you will receive an error message.
- If a role assignment to a user in ABAP is by means of a collective role or organizational management, you cannot unassign the user from the corresponding SAP UME group.
- If a role assignment to a user in ABAP is by means of an indirect assignment through a reference user (visible in transaction SU01), you cannot unassign the user from the corresponding SAP UME group.
- If a role assignment to a user in ABAP is by means of direct and indirect assignment simultaneously, you cannot unassign the user from the corresponding SAP UME group.

For example, a user administrator named ADMIN has assigned the user named USER1 to the roles Z_DIRECT and Z_COLLECT. Z_COLLECT is a collective role including the role Z_DIRECT. When ADMIN uses identity management of the AS Java, ADMIN cannot unassign USER1 from the SAP UME group Z_DIRECT because this ABAP role is also assigned indirectly by the ABAP role Z_COLLECT.

- New groups created with the SAP UME are stored in a local database.

5.2.3 Limitations for Role Management with the Connector

The connector supports the assignment of the following types of roles to users:

- Roles that define what is displayed in SAP Enterprise Portal
 - Portal roles
 - These roles are applicable to SAP Enterprise Portal. The connector supports the assignment of these roles to users.
- Roles that define what authorizations a user has in the backend system

- UME authorization roles
These roles support programmatic authorization checks. The connector supports the assignment of these roles to users.
- J2EE Security role
These roles support declarative authorization checks. The connector does not support the assignment of these roles to users. These roles need to be managed from the Visual Administrator tool of the J2EE Engine.
- ABAP authorization role
These roles are applicable when the SAP UME is configured with an ABAP data source. These roles will be displayed as groups in the SAP UME. The SAP UME instance needs to be checked whether it is supported or not. The connector will support the assignment of these roles if the SAP UME instance supports it.

5.3 Frequently Asked Questions (FAQs)

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

You can refer the following FAQs as guidelines and to troubleshoot connector issues:

1. I have installed only the SAP UME connector in my Oracle Identity Governance (OIG) environment. I want to use it with SAP BusinessObjects AC. Is it mandatory to follow the SIL Registration steps to use it with GRC?

Answer: Not mandatory if you are not using the sodgrc topology name for any other connector. The sodgrc topology name is already registered by default and it is mapped to GRC-ITRes IT Resource. So, you must create the IT resource with instance name GRC-ITRes of type GRC-UME if it does not exist already. Specify the GRC details in this instance and use this IT Resource for GRC. To use GRC-ITRes instance, mention sodgrc as the topology name in SAPUME IT Resource.

2. Can I simultaneously use the SAP ER and the SAP UME connectors in the same OIG environment?

Answer: Yes.

3. I have decided to use the SAP UME connector directly without configuring the Access Request Management feature. The default process form has AC fields on it. How do I remove these AC fields from the form?

Answer: See [Removing SAP BusinessObjects AC Access Request Management Attributes from Process Form](#) for the procedure.

4. I have changed the system property for SOD as XL.SoDCheckRequired = TRUE. Is it now possible to use two SAP connectors in the same 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.

5. Suppose I have installed the SAP ER connector and I want to upgrade it to the SAP UME connector. What are the changes that need to be done after upgrading it?

Answer: You need to change the child table name mapping in Add Role, Remove Role, Add Group, and Remove Group tasks in the process definition according to the existing child table names. Similarly, replace all the new child form names with the existing form names in the below mentioned lookup definitions:

- Lookup.SAPUME.UM.ProvAttrMap
- Lookup.SAPUME.AC10.Configuration
- Lookup.SAPUME.AC10.ProvAttrMap

6. I have configured the SAP UME connector for SOD analysis. I have multiple GRC systems but have configured this connector to only one system. I have added a set of violated roles but my SOD analysis result shows as Passed without violations. Have I missed any configuration in order to get correct analysis?

Answer: It may be a configuration mistake. Verify the Sod System Key decode value in Lookup.SAPUME.ACxx.Configuration where xx denotes 10 for SAP BusinessObjects AC 10 release. You need to mention the correct system value.

7. I have configured the SAP UME 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 Trail: {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}

8. What is the purpose of SAP UME Roles resource object available with the connector?

Answer: These resource objects must be used only with Oracle Identity Manager 11g Release 1 (11.1.1). They are used in Oracle Identity Manager release 11.1.1 to serve the same purpose as entitlements do in Oracle Identity Manager 11g

Release 2 (11.1.2). They are not required in Oracle Identity Manager release 11.1.2.

9. After changing the mapped adapter for Delete User Task, the responses within the task are not available in the Responses Tab because of which the task fails or the description of executed task is blank. Should the responses be added manually?

Answer: Yes, only if the responses are not available, you need to add the responses manually after changing the adapter. Add the following responses:

Response	Description	Status
INVALID_CREDENTIAL	Unauthorized user login	R
CONNECTION_FAILED	Cannot make connection to the resource	R
UNKNOWN_UID	User does not exist in the target	R
UNKNOWN	Unknown	R
CONNECTOR_EXCEPTION	User deletion failed	R
ERROR	Error occurred during delete user	R
SUCCESS	User deletion successful	C

10. I had configured the SAP UME connector for Access Request Management and have users provisioned through GRC. Now, I have reverted back the connector to the default type without Access Request Management feature. When I try to update an existing user, the task fails. Do I need to run any schedule job before performing any operations on the existing users provisioned through Access Request Management?

Answer: Yes, run a full reconciliation once using the SAP UME User Reconciliation schedule job before performing any provisioning operations.

11. I have installed the SAP UME connector in my Oracle Identity Governance environment. I see the following exception while provisioning the user. How do I work around this issue?

Exception :

```
org.identityconnectors.framework.common.exceptions.ConnectorException:
The HTTP request is not valid.
```

Answer: Perform the following procedure as a workaround for this issue:

- a. Login to the Operation system level of the SAP NW7.4 UME and navigate to the following path:

```
D:\usr\sap\<SID>\SYS\PROFILE\
```

- b. Edit the DEFAULT.PFL as follows:

```
#icm/HTTP/mod_0 = PREFIX=/,FILE=${DIR_GLOBAL}/security/data/
icm_filter_rules.txt
```

- c. Run configtool.sh from the directory present within the profile directory as shown in the following path:

```
cd /usr/sap/<SID>/j2ee/configtool
```

```
./configtool.sh
```

- d. Now the Configtool GUI will open and change the value of the `use.spml.http_header_check_active` parameter to `false` if it had been set to `true`.
12. During a Create User provisioning operation, does the SAP UME 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.

13. I am using Oracle Identity Manager 11.1.x and SOD violation is not working in GRC10.1 with NW7.5. Why is it so?

Answer: You must mandatorily apply bug 23582379 one-off fix or BP.

A

Files and Directories in the Installation Package

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

[Table A-1](#) describes the files and directories in the installation package.

Table A-1 Files and Directories in the Installation Package

File in the Installation Media Directory	Description
org.identityconnectors.sapume-1.0.111100.jar org.identityconnectors.sapacume-1.0.111100.jar	These JAR files contain the connector bundle. Use org.identityconnectors.sapacume-1.0.111100.jar file if you are using SAP BusinessObjects AC system.
configuration/SAPUMConnector-CI.xml configuration/SAPACUMConnector-CI.xml	This XML file contains configuration information that is used during connector installation. Use the SAPACUMConnector-CI.xml file if you are using SAP BusinessObjects AC system.
lib/sapume-oim-integration.jar	This JAR file is required to request entitlements for roles and groups through request-based provisioning using request dataset.
lib/sapac-oim-integration.jar	This JAR file includes a custom scheduled job to update request status from SAP BusinessObjects AC.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. Note: A resource bundle is a file containing localized versions of the text strings that include GUI element labels and messages.
xml/SAPUME-ConnectorConfig.xml xml/SAPACUME-ConnectorConfig.xml	This XML file contains definitions of connector objects. Use the SAPACUME-ConnectorConfig.xml file if you are using SAP BusinessObjects AC system.
xml/SAPUME-Datasets.xml	This XML file contains the dataset related definitions for the create and modify user provisioning operations. This file is used if you want to enable request-based provisioning by using the deployment manager. Note: This dataset should <i>not</i> be imported if you are using Oracle Identity Manager release 11.1.2.x or later.
upgrade/PostUpgradeScript	This file contains the scripts that are run after performing an upgrade of the connector.

B

Scheduled Jobs for Lookup Field Synchronization and Reconciliation

[Table B-1](#) lists the scheduled jobs that you must configure.

Table B-1 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
SAP UME Group Lookup Reconciliation	This scheduled job is used for lookup field synchronization of groups. Scheduled Job for Lookup Field Synchronization describes this scheduled job.
SAP UME Role Lookup Reconciliation	This scheduled job is used for lookup field synchronization of roles. Scheduled Job for Lookup Field Synchronization describes this scheduled job.
SAPUME Target User Reconciliation	This scheduled job is used for user record reconciliation. Reconciliation Scheduled Jobs describes this scheduled job.
SAPUME Target User Delete Reconciliation	This scheduled job is used for reconciliation of deleted user records. Reconciliation Scheduled Jobs describes this scheduled job.
SAP AC UME Group Lookup Reconciliation	This scheduled job is used for lookup field synchronization of groups if you are using SAP BusinessObjects AC system. Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization describes this scheduled job.
SAP AC UME Role Lookup Reconciliation	This scheduled job is used for lookup field synchronization of roles if you are using SAP BusinessObject AC system. Scheduled Jobs for SAP BusinessObjects AC Lookup Field Synchronization describes this scheduled job.
SAP AC UME Target User Reconciliation	This scheduled job is used for user record reconciliation if you are using SAP BusinessObject AC system. Reconciliation Scheduled Jobs describes this scheduled job.
SAP AC UME Target User Delete Reconciliation	This scheduled job is used for reconciliation of deleted user records if you are using SAP BusinessObject AC system. Reconciliation Scheduled Jobs describes this scheduled job.