Oracle® Identity Governance

Configuring the SAP User Management Engine Application

12c (12.2.1.3.0)
F12376-03
July 2020

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

F12376-03

Primary Author: Alankrita Prakash

Contributing Authors: Gowri.G.R

Contributors: Syam Kumar Battu, Jagadeesh Kumar, Niranjana Murthy

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

What's New in This Guide?

1 About the SAP User Management Engine Connector

5 Using the SAP User Management Engine Connector

6 Extending the Functionality of the SAP User Management Engine Connector

List of Figures

List of Tables

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 Governance 12.2.1.3.0, visit the following Oracle Help Center page:

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

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

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

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

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

For information about Oracle Identity Manager Connectors 11.1.1 documentation, visit the following Oracle Help Center page:

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

Conventions

The following text conventions are used in this document:

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

What's New in This Guide?

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

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

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

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

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following documentation-specific update has been made in revision "03" of this guide:

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

The following documentation-specific updates have been made in revision "02" of this guide:

- In this revision, the document is updated for editorial corrections.
- 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 12*c* (12.2.1.4.0).
- Usage Recommendation has been modified to include support for Oracle Identity Governance 12*c* (12.2.1.4.0).
- Table 3-20 has been added.
- Table 3-1 and Table 3-2 of Basic Configuration Parameters have been modified and added respectively.

1 About the SAP User Management Engine Connector

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

The SAP User Management Engine connector (SAP UME and SAP AC UME connectors) lets you onboard SAP applications in Oracle Identity Governance.

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

Note:

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

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

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

The following topics provide a high-level overview of the connector:

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

1.1 Certified Components

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

Table 1-1   Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* Release BP02 (12.2.1.3.2)	You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* Release BP02 (12.2.1.3.2) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) and any later BP in this release track

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Target systems	The target system can be one of the following: • 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 **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. If you install an SAP application, such as SAP Business Warehouse (BW) or SAP Supplier Relationship Management (SRM), in Advanced Business Application Programming (ABAP) stack, then you must configure SAP Enterprise Portal against SAP user Management Engine (UME) of the application. See the respective target system documentation for information about this configuration. If you install an SAP application, such as SAP Process Integration (PI), in dual stack (ABAP and Java), then the connector can connect to SAP UME of the application. However, the limitations of the	The target system can be one of the following: • 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 **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. If you install an SAP application, such as SAP Business Warehouse (BW) or SAP Supplier Relationship Management (SRM), in Advanced Business Application Programming (ABAP) stack, then you must configure SAP Enterprise Portal against SAP User Management Engine (UME) of the application. See the respective target system documentation for information about this configuration. If you install an SAP application, such as SAP Process Integration (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.

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
	ABAP data source are applicable.	
Connector Server	11.1.2.1.0	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	JDK 1.6 update 24 or later and JDK 1.7 or later, or JRockit 1.6 or later

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
SAP Governance, Risk and Compliance Access Control (GRC AC)	If you want to configure and use the Access Risk Analysis or Access Request Management feature of this target system, then install the following: • SAP GRC AC 10 on SAP NetWeaver AS ABAP 7.02 Support Pack 7 Install the GRCFND_A SP 10 component. • SAP GRC AC 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 03 patch 2 (on deploying GRCAC1073003P	If you want to configure and use the Access Risk Analysis or Access Request Management feature of this target system, then install the following: • SAP GRC AC 10 on SAP NetWeaver AS ABAP 7.02 Support Pack 7 Install the GRCFND_A SP 10 component. • SAP GRC AC 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 03 patch 2 (on deploying GRCAC1073003P_2-20009496.SCA)

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
	_2-20009496.SCA)	

1.2 Usage Recommendation

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

> **Note:**
>
> In Oracle Identity Governance, you can install and configure both SAP User Management and SAP User Management Engine connectors.
>
> You can configure the connectors with SAP GRC target system to use either Access Risk Analysis or Access Request Management feature.

- If you are using Oracle Identity Governance releases 12*c* BP02 (12.2.1.3.2) or 12.2.1.4.0, then use the latest 12.2.1.*x* version of this connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service.
- If you are using Oracle Identity Manager release 11.1. 2.*x*, as listed in the “Requirement for CI-Based Connector" column of Table 1-1, then use the 11.1.*x* version of the SAP User Management Engine connector. If you want to use the 12.2.1.*x* version of this connector with Oracle Identity Manager release 11.1. 2.*x*, then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0.

1.3 Certified Languages

These are the languages that the connector supports.

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

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

1.4 Supported Connector Operations

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

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

Operation	Supported for SAP UME?	Supported for SAP AC UME?
User Management		
Create a user account	Yes	Yes
Modify a user account	Yes	Yes
Delete a user account	Yes	Yes
Enable a user account	Yes	Yes
Disable a user account	Yes	Yes
Lock a user account	Yes	Yes
Unlock a user account	Yes	Yes
Assign a role to a user account	Yes	Yes
Assign multiple roles to a user account	Yes	Yes

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

Operation	Supported for SAP UME?	Supported for SAP AC UME?
Remove role for a user account	Yes	Yes
Remove multiple roles from a user account	Yes	Yes
Assign a group to a user account	Yes	No
Assign multiple groups from a user account	Yes	No
Remove a group for user account	Yes	No
Remove multiple groups from a user account	Yes	No
Entitlements		
Add Role	Yes	Yes
Add Multiple Roles	Yes	Yes
Remove Role	Yes	Yes
Remove Multiple Roles	Yes	Yes

1.5 Connector Architecture

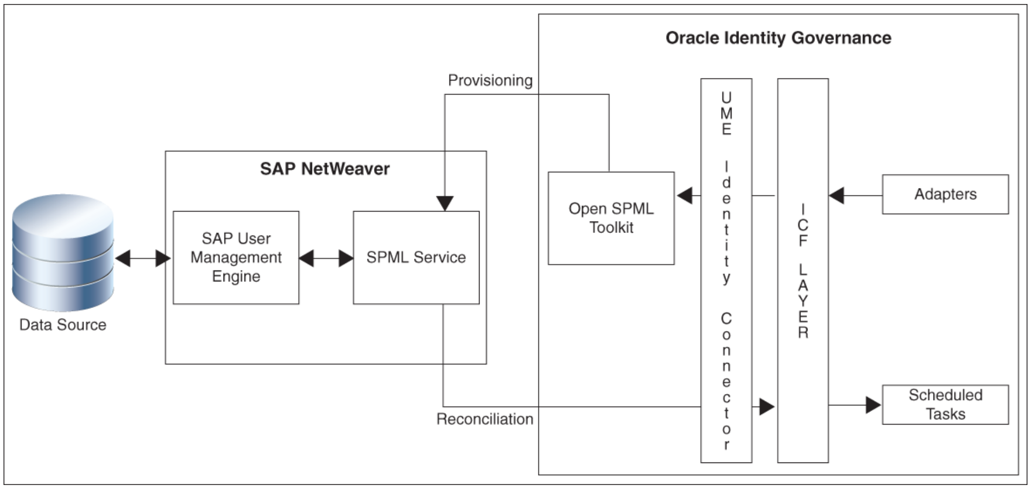
The SAP UME connector is implemented by using the Identity Connector Framework (ICF).

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

The connector reconciles any account data added or modified through provisioning operations performed directly on the data source into Oracle Identity Governance through SAP User Management Engine.

Figure 1-1 shows the connector integrating SAP User Management Engine with Oracle Identity Governance.

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 (Application Server) Java data source, 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 creating an application, you configure SAP User Management Engine as a target resource of Oracle Identity Governance.

Oracle Identity Governance sends provisioning requests which are routed through the SPML service to the application or system that uses the data source linked with SAP User Management Engines. You can view the user data changes resulting from the provisioning requests through the SAP User Management Engine UI.

You can configure the connector 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 Governance. When you allocate (or provision) an SAP User Management Engine resource to an OIG User, the operation results in the creation of an account on SAP UME for that user. In the Oracle Identity Governance context, the term **provisioning** is also used to mean updates made to the target system account through Oracle Identity Governance.

  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 Governance.

- 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 Governance.

Each record fetched from the target system is compared with SAP User Management Engine resources that are already provisioned to OIG 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 Governance. If no match is found, then the user ID of the record is compared with the user ID of each OIG 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 OIG User.

1.6 Supported Deployment Configurations

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

You can use the connector to act as an interface with the Access Risk Analysis and Access Request Management modules of SAP GRC in addition to enabling direct integration with the target system. The target system (SAP NetWeaver Java Application Server) and these two modules of SAP GRC together provide various deployment configurations. The following sections provide information about the supported deployment configurations of the connector:

- 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 an Application Configuration
- Considerations to Be Addressed When You Enable Access Request Management

1.6.1 User Management with Access Request Management

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

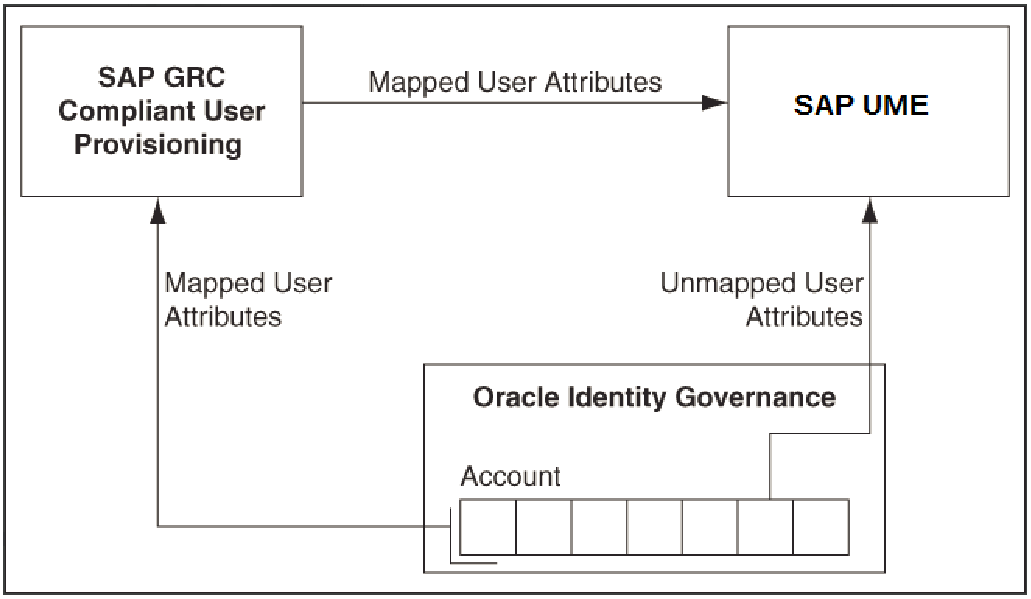
> **Note:**
>
> In this guide, the phrase **configuring Access Request Management** has been used to mean configuring the integration between Oracle Identity Governance and SAP GRC Access Request Management.

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 GRC Access Request Management. Scheduled tasks on Oracle Identity Governance fetch data from the target system to Oracle Identity Governance.

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

Figure 1-2   Connector Integrating SAP GRC Access Request Management with Oracle Identity Governance and the Target System



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

1. The provisioning operation is initiated through direct provisioning, request-based provisioning, or an access policy change.
2. An 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 GRC Access Request Management.
    - For a Create 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 GRC Access Request Management.

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

    - 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 GRC Access Request Management logs.

The process form holds fields for both basic user management and Access Request Management. However, for a Create User operation, only the Access Request Management fields (attributes) on the process form are used.

> **Note:**
>
> SAP GRC Access Request Management does not process passwords. Therefore, during Create User provisioning operations, the system ignores any value that you enter in the password field.
>
> 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 GRC Access Request Management *and* attributes that are directly updated on the target system.

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

- If an error occurs during communication between Access Request Management and the target system, then the request remains in the Open state. A message stating that the operation has failed is recorded in the audit log associated with the request. An error message is displayed on the console.

Summary of Account Request Management when SAP GRC Access Request Management is Configured and Enabled in your SAP Operating Environment:

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

1.6.2 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}
```

1.6.3 User Management with SoD

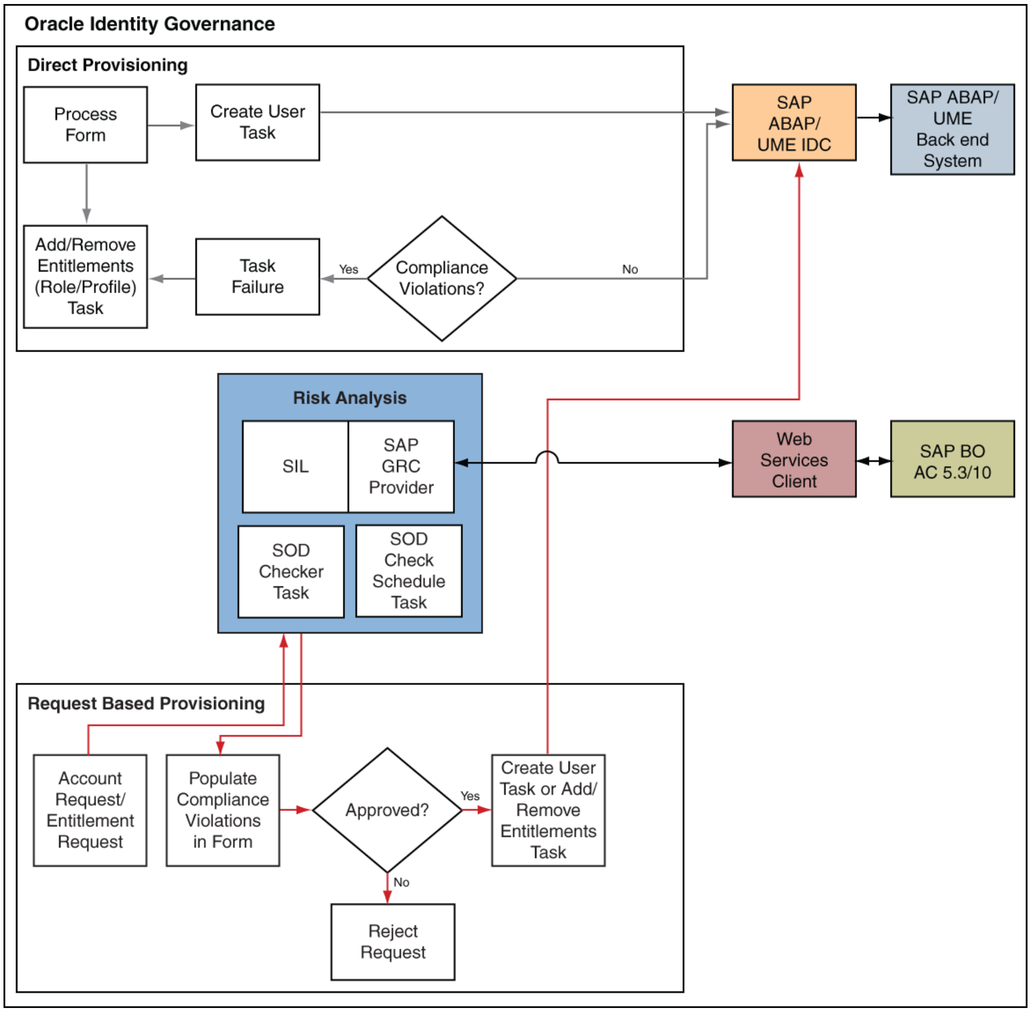
If the Access Risk Analysis module of SAP GRC is configured to implement segregation of duties (SoD) in your SAP operating environment, the connector can be used as the interface between Oracle Identity Governance and the SoD module. You can configure the connector to first process the provisioning requests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


Oracle Identity Governance
Direct Provisioning
Process Form
Create User Task
Add/Remove Entitlements (Role/Profile) Task
Task Failure
Yes
Compliance Violations?
No
SAP ABAP/ UME IDC
SAP ABAP/ UME Back end System
Risk Analysis
SIL
SAP GRC Provider
SOD Checker Task
SOD Check Schedule Task
Web Services Client
SAP BO AC 5.3/10
Request Based Provisioning
Account Request/ Entitlement Request
Populate Compliance Violations in Form
Approved?
Yes
Create User Task or Add/ Remove Entitlements Task
No
Reject Request

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.

1.6.4 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.

1.6.5 Guidelines on Using an Application Configuration

These are the guidelines that you must apply while using an application configuration.

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

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

The following sections describe guidelines on the supported application 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
- User Management with Access Request Management

1.6.5.1 User Management Engine with SoD and Access Request Management

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

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

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

1.6.5.2 User Management with Access Request Management

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

> **Note:**
>
> SAP GRC Access Risk Analysis is either configured as a linked module of SAP GRC Access Request Management or it is not used at all.

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

  The scenario described earlier in this section explains this guideline.
- Configure the Access Request Management feature of the connector.
- Do *not* configure the SoD feature of the connector.

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

1.7 Supported Connector Features Matrix

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

Table 1-3 Supported Connector Features Matrix

Feature	AOB Connector	CI-Based Connector
Full reconciliation	Yes	Yes
Limited (filtered) reconciliation	Yes	Yes
Provision requests through SAP GRC access request management	Yes	Yes
SoD validation of entitlement requests	Yes	Yes
Enable and disable accounts	Yes	Yes
Provision and reconcile user-related data to and from multiple data sources	Yes	Yes
Remove role assignment in Federated Portal Network (FPN) configuration	Yes	Yes
Configure transformation and validation of account data	Yes	Yes
Specify accounts to be excluded from all reconciliation and provisioning operations	Yes	Yes
Test Connection	Yes	No

1.8 Connector Features

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 remote role assignment in federated portal network (FDN) and so on.

The following are the features of the connector:

- Full Reconciliation
- Limited (Filtered) Reconciliation
- Routing of Provisioning Requests Through SAP GRC Access Request Management
- SoD Validation of Entitlement Requests
- Enabled and Disabled Accounts
- Support for Multiple Data Sources
- Support for Remote Role Assignment in Federated Portal Network
- Support for the Connector Server
- Transformation and Validation of Account Data
- Support for Resource Exclusion Lists

1.8.1 Full Reconciliation

In full reconciliation, all records are fetched from the target system to Oracle Identity Governance.

> **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 Limitations Related to Target System Features and Specific Connectors.

In full reconciliation, all records are fetched from the target system to Oracle Identity Governance. 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 3-2 for a list of all valid characters.

During full reconciliation, a single reconciliation event is generated for each target system account. For more information, see Performing Full Reconciliation.

1.8.2 Limited (Filtered) Reconciliation

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

You can set a reconciliation filter as the value of the Filter Suffix attribute of the user reconciliation scheduled job. The Filter Suffix attribute helps you to assign filters to the API based on which you get a filtered response from the target system.

See Performing Limited Reconciliation for more information.

1.8.3 Routing of Provisioning Requests Through SAP GRC Access Request Management

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

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

1.8.4 SoD Validation of Entitlement Requests

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

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

- The SoD Invocation Library (SIL) is bundled with Oracle Identity Governance. The SIL acts as a pluggable integration interface with any SoD engine.
- Configure the connector to work with SAP GRC as the SoD engine.

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

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

See Configuring SoD (Segregation of Duties) for more information about configuring SoD.

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

1.8.5 Enabled and Disabled Accounts

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

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

1.8.6 Support for Multiple Data Sources

You can configure the SAP User Management Engine connector 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.

1.8.7 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.

1.8.8 Support for the Connector Server

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

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

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

1.8.9 Transformation and Validation of Account Data

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

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

1.8.10 Support for Resource Exclusion Lists

You can specify a list of accounts that must be excluded from reconciliation and provisioning operations.

Accounts whose user IDs you specify in the exclusion list are not affected by reconciliation and provisioning operations.

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

2

Creating an Application By Using the SAP User Management Engine Connector

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

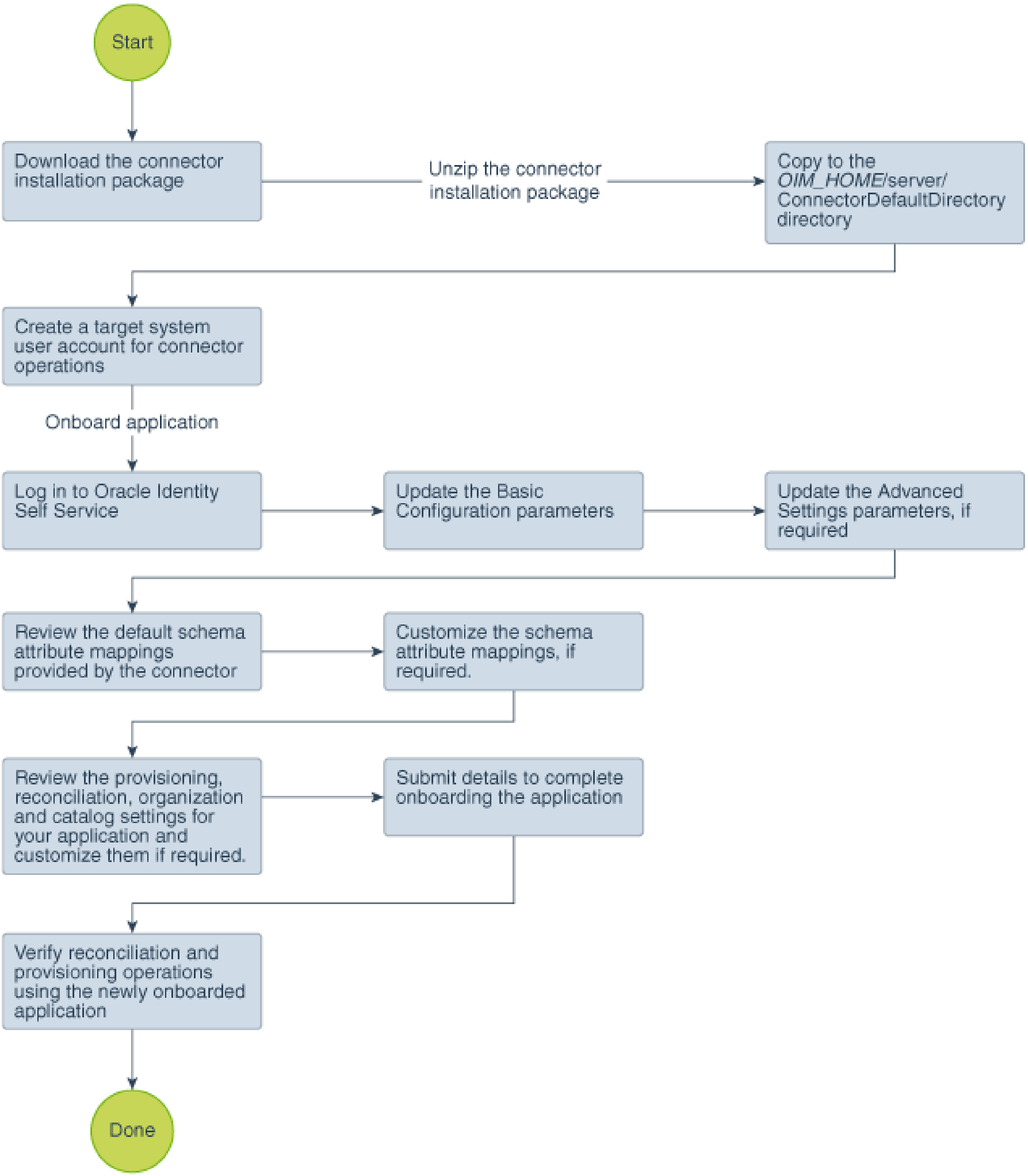
- Process Flow for Creating an Application By Using the Connector
- Prerequisites for Creating an Application By Using the Connector
- Creating an Application By Using the Connector

2.1 Process Flow for Creating an Application By Using the Connector

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

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

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


Start
Download the connector installation package
Unzip the connector installation package
Copy to the *OIM_HOME*/server/ ConnectorDefaultDirectory directory
Create a target system user account for connector operations
Onboard application
Log in to Oracle Identity Self Service
Update the Basic Configuration parameters
Update the Advanced Settings parameters, if required
Review the default schema attribute mappings provided by the connector
Customize the schema attribute mappings, if required.
Review the provisioning, reconciliation, organization and catalog settings for your application and customize them if required.
Submit details to complete onboarding the application
Verify reconciliation and provisioning operations using the newly onboarded application
Done

2.2 Prerequisites for Creating an Application By Using the Connector

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

- Downloading the Connector Installation Package
- Creating a Target System User Account for Connector Operations
- Creating an Application By Using the Connector

2.2.1 Downloading the Connector Installation Package

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

To download the connector installation package:

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

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

2.2.2 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.

2.3 Creating an Application By Using the Connector

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

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

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

1. Create an application in Identity Self Service. The high-level steps are as follows:

a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.

b. Ensure that the **Connector Package** option is selected when creating an application.

c. Update the basic configuration parameters to include connectivity-related information.

d. If required, update the advanced setting parameters to update configuration entries related to connector operations.

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

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

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

   The application is created in Oracle Identity Governance.

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

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

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

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

3

Configuring the SAP User Management Engine Connector

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

- Basic Configuration Parameters
- Advanced Setting Parameters
- Attribute Mappings
- Correlation Rules
- Reconciliation Jobs

3.1 Basic Configuration Parameters

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

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

Parameters	Mandatory?	Description
Connector Server Name	No	If you created an IT resource of the type "Connector Server," then enter its name. **Note:** Enter a value for this parameter only if you have deployed the SAP UME connector in the Connector Server.
changePwdFlag	Yes	For accounts created through Oracle Identity Governance, password management can be configured by using the changePwdFlag and dummyPassword parameters of the basic configuration parameters. Default value: `no` See Configuring Password Changes for Newly Created Accounts for more information about this parameter.
dummyPassword	Yes	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.
enableDate	Yes	Enter the date in the YYYY-MM-DD format to enable a user with end date as default value. Default value: `2500-12-31`
logSPMLRequst	No	Enter `yes` to specify that the SPML requests being sent to the target system be written to the log file. Otherwise, enter `no`.

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

Parameters	Mandatory?	Description
logonNameInitialSubstring	Yes	Enter the set of characters to support full reconciliation for the English language. For other languages, enter all characters of that language. Sample value: `abcdefghijklmnopqrstuvwxyz1234567890`
pwdHandlingSupport	Yes	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 to `no`. Otherwise, set the value of this parameter to `yes`. Default value: `yes`
TopologyName	No	Name of the topology of the target system host computer.
umePassword	Yes	Enter the password of the target system user account that you create for connector operations. See Creating a Target System User Account for Connector Operations for more information.
umeUrl	Yes	• If you configure SSL to secure communication between the target system and Oracle Identity Governance, 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 Governance, then enter the URL for the SPML service in the following format: `http://HOSTNAME:PORT/spml/spmlservice` Sample value: `http://myhost:50000/spml/spmlservice`
umeUserId	Yes	Enter the user ID of the target system user account that you create for connector operations. See Creating a Target System User Account for Connector Operations for more information.

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

Parameters	Mandatory?	Description
Connector Server Name	No	If you created an IT resource of the type "Connector Server," then enter its name. **Note:** Enter a value for this parameter only if you have deployed the SAP UME connector in the Connector Server.
changePwdFlag	Yes	For accounts created through Oracle Identity Governance, password management can be configured by using the changePwdFlag and dummyPassword parameters of the basic configuration parameters. Default value: `no` See Configuring Password Changes for Newly Created Accounts for more information about this parameter.

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

Parameters	Mandatory?	Description
dummyPassword	Yes	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.
enableDate	Yes	Enter the date in the YYYY-MM-DD format to enable a user with end date as default value. Default value: `2500-12-31`
logSPMLRequst	No	Enter `yes` to specify that the SPML requests being sent to the target system be written to the log file. Otherwise, enter `no`.
logonNameInitialSubstring	Yes	Enter the set of characters to support full reconciliation for the English language. For other languages, enter all characters of that language. Sample value: `abcdefghijklmnopqrstuvwxyz1234567890`
pwdHandlingSupport	Yes	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 to `no`. Otherwise, set the value of this parameter to `yes`. Default value: `yes`
TopologyName	No	Name of the topology of the target system host computer.
umePassword	Yes	Enter the password of the target system user account that you create for connector operations. See Creating a Target System User Account for Connector Operations for more information.
umeUrl	Yes	• If you configure SSL to secure communication between the target system and Oracle Identity Governance, 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 Governance, then enter the URL for the SPML service in the following format: `http://HOSTNAME:PORT/spml/spmlservice` Sample value: `http://myhost:50000/spml/spmlservice`
umeUserId	Yes	Enter the user ID of the target system user account that you create for connector operations. See Creating a Target System User Account for Connector Operations for more information.
grcLanguage	Yes	This parameter defines the language in which we are sending requests to SAP GRC system. Value: `en` **Note:** This parameter is applicable only to the SAP AC UME connector.

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

Parameters	Mandatory?	Description
grcPassword	Yes	This parameter holds the password for accessing the SAP GRC system. **Note:** This parameter is applicable only to the SAP AC UME connector.
grcUsername	Yes	This parameter holds the user name for accessing the SAP GRC system. **Note:** This parameter is applicable only to the SAP AC UME connector.

3.2 Advanced Setting Parameters

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

Table 3-3 Advanced Setting Parameters for the SAP UME Connector with SoD

Parameter	Mandatory?	Description
Bundle Name	No	This parameter holds the name of the connector bundle package. Default Value: `org.identityconnectors.sapume`
Bundle Version	No	This parameter holds the version of the connector bundle class. Do *not* modify this parameter. Default Value: `12.3.0`
Connector Name	No	This parameter holds the name of the connector class. Do *not* modify this parameter. Default Value: `org.identityconnectors.sapume.SAPUMEConnector`
ConnectorImpl Type	No	Enter the value `SAPUME` to enable SOD for SAP UME roles.
Group attribute name	No	This parameter holds the name of the role duty type used in SIL. Default Value: `GROUPNAME`
Group form names	Yes	This value is used to get the group child form names in SIL Layer. Do *not* modify this value. Default Value: `UD_UME_GROUP`
Role attribute name	No	Name of the role duty type used in SIL. Default Value: `ROLENAME`
Role form names	Yes	This value is used to get the role child form names from the SIL Layer. Do *not* modify this value. Default Value: `UD_UME_ROLE`
RoleAttributeLabel	No	Label name of the role ID field in the child form. Default Value: `Role`

Table 3-3 (Cont.) Advanced Setting Parameters for the SAP UME Connector with SoD

Parameter	Mandatory?	Description
entitlementRiskAnalysisAccessURL	No	This parameter holds the WSDL URL for the Entitlement Risk Analysis web service. Default Value: `None` **Note:** This parameter is applicable only to the SAP UME with SoD
wsdlFilePath	No	Enter the absolute path of the directory containing the following file: GRAC_RISK_ANALYSIS_WOUT_NO_WS.WS D
entitlementRiskAnalysisWS	Yes	Web service client class to perform risk analysis without request number. Default Value: `oracle.iam.grc.sod.scomp.impl.grcsap.util.webservice.sap.ac10.RiskAnalysisWithoutNo` **Note:** This parameter is applicable only to the SAP UME with SoD
SODSystemKey	Yes	Name of the RFC destination/Connector used for connecting GRC with portal. Default Value: `None` **Note:** This parameter is applicable only to the SAP UME with SoD

Table 3-4 Advanced Setting Parameters for the SAP AC UME Connector

Parameter	Mandatory?	Description
appLookupAccessURL	No	WSDL URL for Application Lookup web service. Default Value: `None`
appLookupWS	No	Web service client class to get all applications configured in SAP GRC. Default Value: `oracle.iam.ws.sap.ac10.SelectApplication`
assignRoleReqType	No	This entry holds the name of the request type that is used for assign role request in SAP GRC. The format of the decode value is as follows: Default Value: `002~Change Account~002~006`
auditLogsAccessURL	No	WSDL URL for Audit Logs web service. Default Value: `None`
auditLogsWS	No	Web service client class to get audit logs. Default Value: `oracle.iam.ws.sap.ac10.AuditLogs`

Table 3-4 (Cont.) Advanced Setting Parameters for the SAP AC UME Connector

Parameter	Mandatory?	Description
Bundle Name	No	Name of the connector bundle package. Default Value: `org.identityconnectors.sapacume`
Bundle Version	No	This parameter holds the version of the connector bundle class. Do *not* modify this parameter. Default Value: `12.3.0`
Connector Name	No	This parameter holds the name of the connector class. Do *not* modify this parameter. Default Value: `org.identityconnectors.sapacume.SAPACUMEConnector`
ConnectorImplType	No	Enter the value `SAPUME` to enable SAP UME roles in SOD. Default Value: `SAPUME`
createUserReqType	No	Name of the request type that the connector must use for the create user request in SAP GRC. Default Value: `001~New Account~001`
deleteUserReqType	No	Name of the request type that the connector must use for the delete user request in SAP GRC. Default Value: `003~Delete Account~003`
ignoreOpenStatus	No	Specify whether the connector must send the new request for a particular user even if the last request for the user is in the Open status. Default Value: `No`
lockUserReqType	No	This parameter holds the name of the request type to use to lock user request in SAP GRC. Default Value: `004~Lock Account~004`

Table 3-4 (Cont.) Advanced Setting Parameters for the SAP AC UME Connector

Parameter	Mandatory?	Description
logAuditTrial	No	Specify whether the connector must log complete audit trails whenever status request web service is invoked. Default Value: `No`
modifyUserReqType	No	This parameter holds the name of the request type to use for modify user request in SAP GRC. Default Value: `002~Change Account~002`
otherLookupAccessURL	No	URL for other lookup web service areas such as Business Process, Funcational Area. Default Value: `none`
otherLookupWS	No	Web service client class to get other lookup field details such as Business Process, Function Area, and so on. Default Value: `oracle.iam.ws.sap.ac10.SearchLookup`
provActionAttrName	No	Name of the attribute in the target system that contains the details required for performing provisioning operations to a specific backend system. Default Value: `provAction;ReqLineItem`
provItemActionAttrName	No	Name of the attribute in the target system that contains the details required for performing provisioning roles. Default Value: `provItemAction;ReqLineItem`
removeRoleReqType	No	Name of the request type to use for remove user request in SAP GRC. Default Value: `002~Change Account~002~009`
requestStatusAccessURL	No	WSDL URL for Status Request web service. Default Value: `None`

Table 3-4 (Cont.) Advanced Setting Parameters for the SAP AC UME Connector

Parameter	Mandatory?	Description
requestStatusValue	No	The value that get updated in the AC Request Status field on the process form. Default Value: `OK`
requestStatusWS	No	Web service client class to get status of provisioning request. Default Value: `oracle.iam.ws.sap.ac10.RequestStatus`
requestTypeAttrName	No	Name of the request type parameter used to differentiate request flows from the SAPUMCREATE adapter. Default Value: `Reqtype;Header`
riskLevel	No	In SAP GRC, each business risk is assigned a criticality level. You can control the risk analysis data returned by SAP GRC by specifying a risk level. Default Value: `High`
Role form names	No	This value is used to get the role child form names in SIL Layer. Do *not* modify this value. Default Value: `UD_UME_ROLE`
roleLookupAccessURL	No	WSDL URL for Role Lookup web services. Default Value: `None`
roleLookupWS	No	Web service client class to get all roles. Default Value: `oracle.iam.ws.sap.ac10.SearchRoles`
unlockUserReqType	No	Name of the request type to use for unlock user request in SAP GRC. Default Value: `005~unlock user~005`
userAccessAccessURL	No	WSDL URL for User Access web service. Default Value: `None`
userAccessWS	No	Web service client class to get status of user access. Default Value: `oracle.iam.ws.sap.ac10.UserAccess`

Table 3-4 (Cont.) Advanced Setting Parameters for the SAP AC UME Connector

Parameter	Mandatory?	Description
wsdlFilePath	No	File path where the WSDL files are available in local machine. Default Value: `None` **Note:** If you are using a Connector Server, copy the WSDL File on the system running the Connector Server. Location of the WSDL files is available in the local machine that is running the Connector Server.

3.3 Attribute Mappings

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

- Attribute Mappings for the SAP UME Connector
- Attribute Mapping for the SAP AC UME Connector

3.3.1 Attribute Mappings for the SAP UME Connector

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

SAP UME User Account Attributes

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

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

Table 3-5 Default Attribute Mappings for the SAP UME User Account

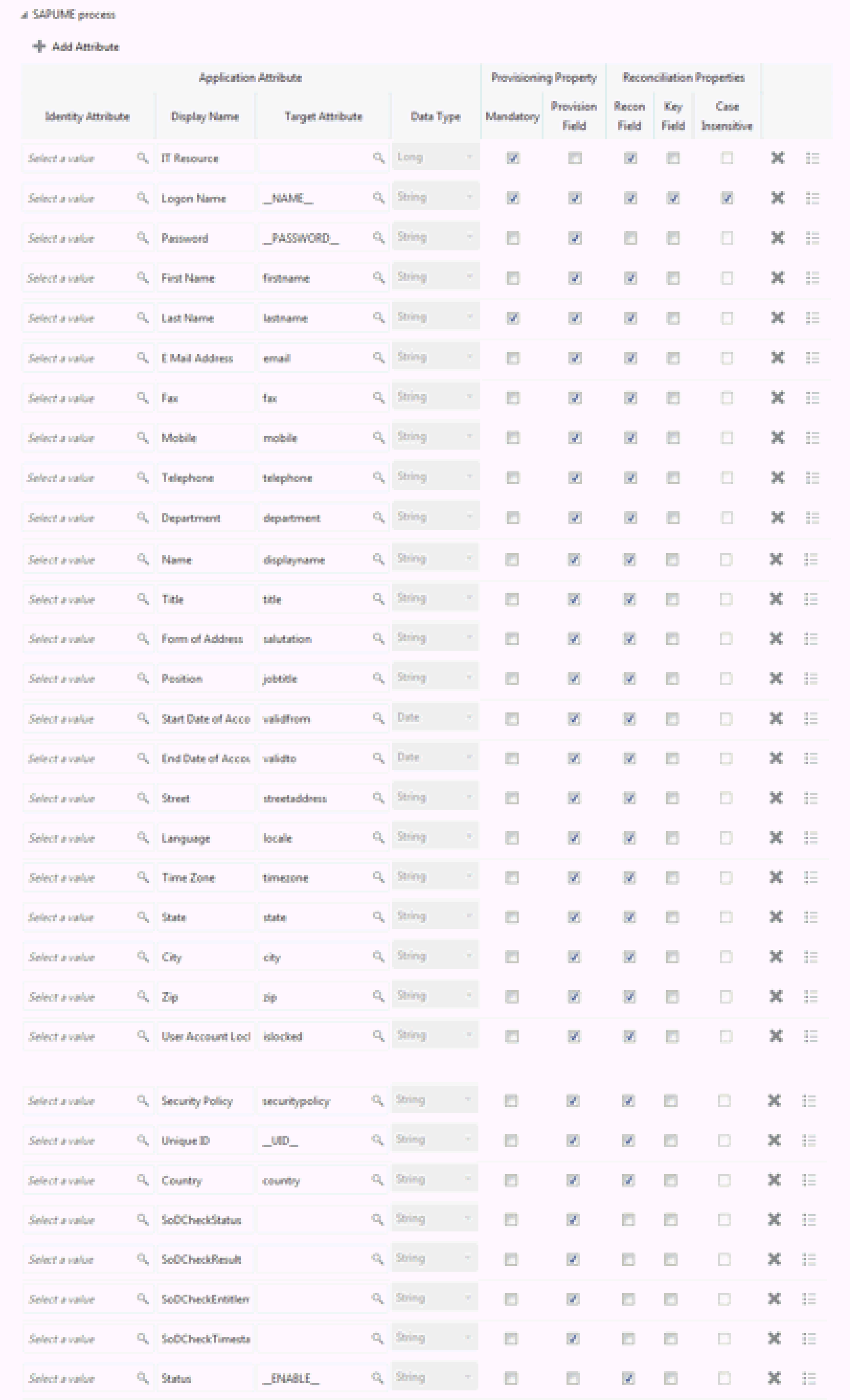
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Logon Name	_NAME_	String	Yes	Yes	Yes	Yes	Yes
Password	_PASSWORD_	String	No	Yes	No	No	No
First Name	firstname	String	No	Yes	Yes	No	No
Last Name	lastname	String	Yes	Yes	Yes	No	No
E Mail Address	email	String	No	Yes	Yes	No	No
Fax	fax	String	No	Yes	Yes	No	No
Mobile	mobile	String	No	Yes	Yes	No	No
Telephone	telephone	String	No	Yes	Yes	No	No
Department	department	String	No	Yes	Yes	No	No
Name	displayname	String	No	Yes	Yes	No	No
Title	title	String	No	Yes	Yes	No	No
Form of Address	salutation	String	No	Yes	Yes	No	No
Postion	jobtitle	String	No	Yes	Yes	No	No
Start Date of Account Validity (date)	validfrom	String	No	Yes	Yes	No	No
End Date of Account Validity (date)	validto	String	No	Yes	Yes	No	No
Street	streetaddress	String	No	Yes	Yes	No	No
Language	locale	String	No	Yes	Yes	No	No
Timezone	timezone	String	No	Yes	Yes	No	No
State	state	String	No	Yes	Yes	No	No
City	city	String	No	Yes	Yes	No	No
Zip	zip	String	No	Yes	Yes	No	No
User Account Locked	islocked	String	No	Yes	Yes	No	No

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

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Security Policy	securitypolicy	String	No	Yes	Yes	No	No
Unique ID	_UID_	String	No	Yes	Yes	No	No
Country	country	String	No	Yes	Yes	No	No
SoDCheck Status		String	No	Yes	Yes	No	No
SoDCheck Result		String	No	Yes	Yes	No	No
SoDCheck Entitlement		String	No	Yes	Yes	No	No
SoDCheck Timestamp		String	No	Yes	Yes	No	No
Status	_Enable_	String	No	Yes	Yes	No	No

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

Figure 3-1   Default Attribute Mappings for the SAP UME User Account



SAPUME process

Add Attribute

Application Attribute				Provisioning Property		Reconciliation Properties				
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive		
Select a value	IT Resource		Long	☑	□	☑	□	□	✖	☰
Select a value	Logon Name	__NAME__	String	☑	☑	☑	☑	☑	✖	☰
Select a value	Password	__PASSWORD__	String	□	☑	□	□	□	✖	☰
Select a value	First Name	firstname	String	□	☑	☑	□	□	✖	☰
Select a value	Last Name	lastname	String	☑	☑	☑	□	□	✖	☰
Select a value	E Mail Address	email	String	□	☑	☑	□	□	✖	☰
Select a value	Fax	fax	String	□	☑	☑	□	□	✖	☰
Select a value	Mobile	mobile	String	□	☑	☑	□	□	✖	☰
Select a value	Telephone	telephone	String	□	☑	☑	□	□	✖	☰
Select a value	Department	department	String	□	☑	☑	□	□	✖	☰
Select a value	Name	displayname	String	□	☑	☑	□	□	✖	☰
Select a value	Title	title	String	□	☑	☑	□	□	✖	☰
Select a value	Form of Address	salutation	String	□	☑	☑	□	□	✖	☰
Select a value	Position	jobtitle	String	□	☑	☑	□	□	✖	☰
Select a value	Start Date of Acco	validfrom	Date	□	☑	☑	□	□	✖	☰
Select a value	End Date of Accou	validto	Date	□	☑	☑	□	□	✖	☰
Select a value	Street	streetaddress	String	□	☑	☑	□	□	✖	☰
Select a value	Language	locale	String	□	☑	☑	□	□	✖	☰
Select a value	Time Zone	timezone	String	□	☑	☑	□	□	✖	☰
Select a value	State	state	String	□	☑	☑	□	□	✖	☰
Select a value	City	city	String	□	☑	☑	□	□	✖	☰
Select a value	Zip	zip	String	□	☑	☑	□	□	✖	☰
Select a value	User Account Locl	islocked	String	□	☑	☑	□	□	✖	☰
Select a value	Security Policy	securitypolicy	String	□	☑	☑	□	□	✖	☰
Select a value	Unique ID	__UID__	String	□	☑	☑	□	□	✖	☰
Select a value	Country	country	String	□	☑	☑	□	□	✖	☰
Select a value	SoDCheckStatus		String	□	☑	□	□	□	✖	☰
Select a value	SoDCheckResult		String	□	☑	□	□	□	✖	☰
Select a value	SoDCheckEntitlen		String	□	☑	□	□	□	✖	☰
Select a value	SoDCheckTimesta		String	□	☑	□	□	□	✖	☰
Select a value	Status	__ENABLE__	String	□	□	☑	□	□	✖	☰

Group Entitlement Attributes

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

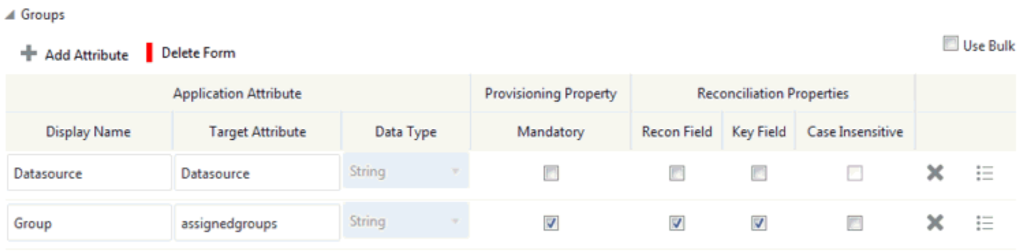
If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-6 Default Attribute Mappings for Group Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Datasource	Datasource	String	No	No	No	No
Group	assignedgroups	String	Yes	Yes	Yes	No

Figure 3-2 shows the group entitlement mappings.

Figure 3-2 Default Attribute Mappings for Group Entitlement



Groups

Add Attribute Delete Form □ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Datasource	Datasource	String	□	□	□	□	✕	☰
Group	assignedgroups	String	☑	☑	☑	□	✕	☰

Role Entitlement Attributes

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

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

Table 3-7 Default Attribute Mappings for a Role Entitlement

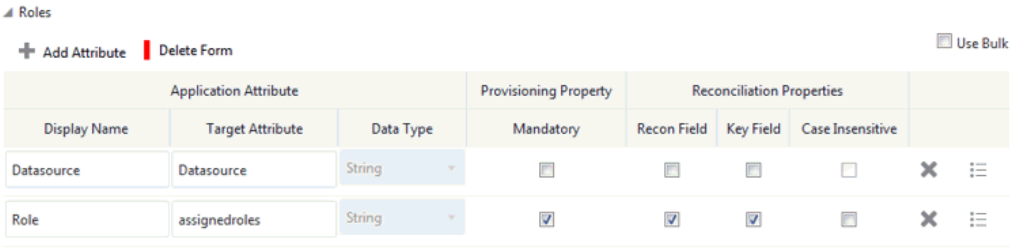
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Datasource	Datasource	String	No	No	No	No

Table 3-7 (Cont.) Default Attribute Mappings for a Role Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
role	assignedroles	String	Yes	Yes	Yes	No

Figure 3-3 shows the default role entitlement mapping.

Figure 3-3 Default Attribute Mappings for a Role Entitlement



Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Datasource	Datasource	String	□	□	□	□	✖	☰
Role	assignedroles	String	☑	☑	☑	□	✖	☰

3.3.2 Attribute Mapping for the SAP AC UME Connector

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

SAP AC UME User Account Attributes

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

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

Table 3-8 Default Attribute Mappings for the SAP AC UME User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
logon Name	UserId;UserInfo	String	Yes	Yes	Yes	Yes	Yes

Table 3-8 (Cont.) Default Attribute Mappings for the SAP AC UME User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Password	_PASSWORD_	String	No	No	No	No	No
First Name	fname;UserInfo	String	No	No	Yes	No	No
Last Name	lname;UserInfo	String	No	No	Yes	No	No
E Mail Address	email;Userinfo	String	No	No	Yes	No	No
Fax	fax;UserInfo	String	No	No	Yes	No	No
Mobile	personnelno;UserInfo	String	No	No	Yes	No	No
Telephone	telnumber;UserInfo	String	No	No	Yes	No	No
Department	department;UserInfo	String	No	No	Yes	No	No
Name	displayname	String	No	No	Yes	No	No
Form of Address	personnelarea;UserInfo	String	No	No	Yes	No	No
Position	empposition;UserInfo	String	No	No	Yes	No	No
Start Date of Account Validity (date)	validFrom;UserInfo	Date	No	No	Yes	No	No
End Date of Account Validity (date)	validTo;UserInfo	Date	No	No	Yes	No	No
Street	streetaddress	String	No	No	Yes	No	No
Language	logonLang;Userinfo	String	No	No	Yes	No	No
Time Zone	timezone	String	No	No	Yes	No	No
State	state	String	No	No	Yes	No	No
City	city	String	No	No	Yes	No	No
Zip	zip	String	No	No	Yes	No	No
User Account Locked	userLocak;None	String	No	No	Yes	No	No

Table 3-8 (Cont.) Default Attribute Mappings for the SAP AC UME User Account

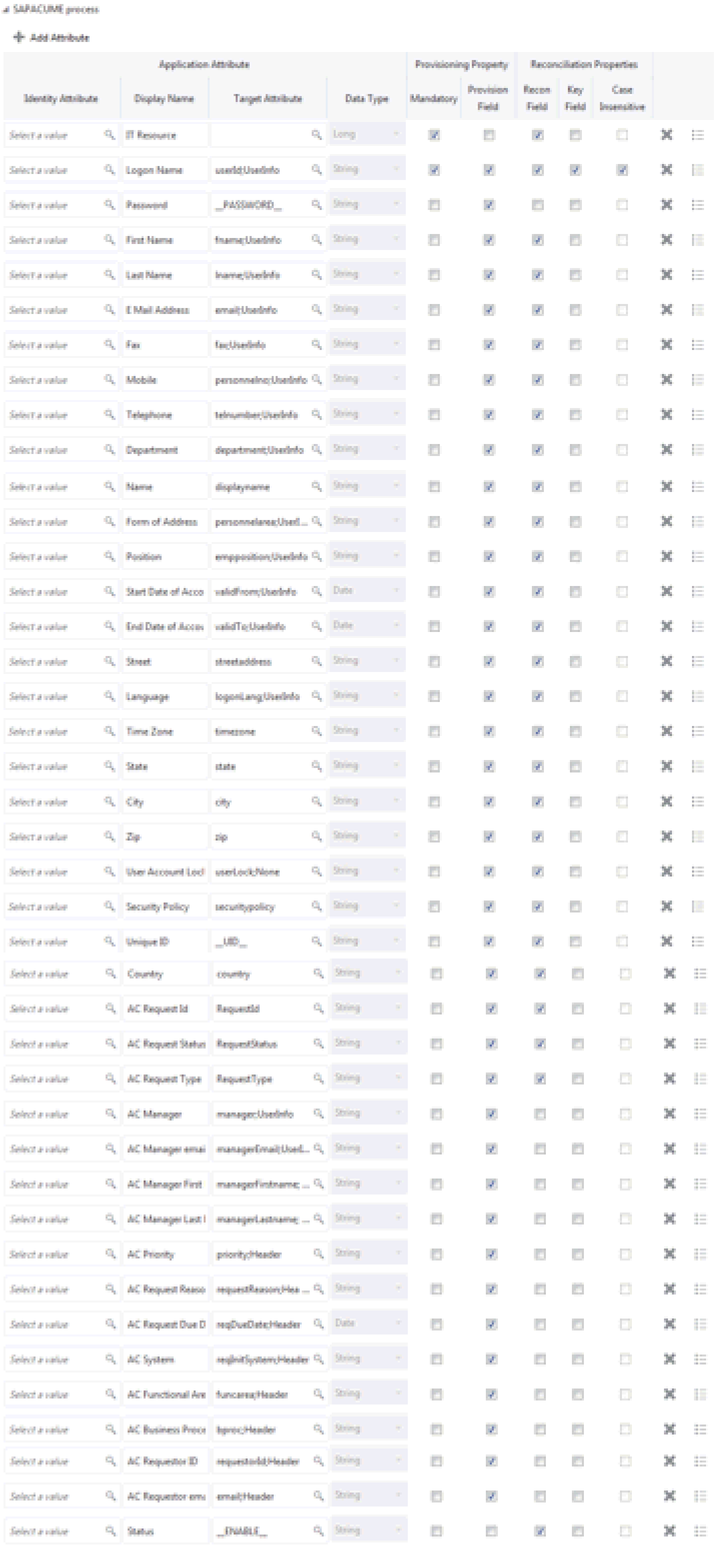
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Security Policy	securitypolicy	String	No	No	Yes	No	No
Unique ID	_UID_	String	No	No	Yes	No	No
Country	country	String	No	No	Yes	No	No
AC Request Id	RequestId	String	No	No	Yes	No	No
AC Request Status	RequestStatus	String	No	No	Yes	No	No
AC Request Type	RequestType	String	No	No	Yes	No	No
AC Manager	manager;UserInfo	String	No	No	No	No	No
AC Manager email	manager;UserInfo	String	No	No	No	No	No
AC Manager First Name	managerFirstname;Userinfo	String	No	No	No	No	No
AC Manager Last Name	managerLastname;Userinfo	String	No	No	No	No	No
AC Priority	priority;Header	String	No	No	No	No	No
AC Request Reason	requestreason;Header	String	No	No	No	No	No
AC Request Due Date (Date)	reqDueDate;Header	Date	No	No	No	No	No
AC System	reqInitSystem;Header	String	No	No	No	No	No
AC Functional Area (Lookup)	funcarea;Header	String	No	No	No	No	No
AC Business Process (Lookup)	bproc;Header	String	No	No	No	No	No

Table 3-8 (Cont.) Default Attribute Mappings for the SAP AC UME User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
AC Requestor ID	requestorId:Header	String	No	No	No	No	No
AC Requestor email	email;Header	String	No	No	No	No	No
Status	_ENABLE_	String	No	No	Yes	No	No

Figure 3-4 shows the default User account attribute mappings.

Figure 3-4 Default Attribute Mappings for an SAP AC UME Account



SAPACUME process

Add Attribute

	Application Attribute			Provisioning Property		Reconciliation Properties				
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive		
Select a value	IT Resource		Long	☑	☐	☑	☐	☐	✖	☰
Select a value	Logon Name	userId;UserInfo	String	☑	☑	☑	☑	☑	✖	☰
Select a value	Password	__PASSWORD__	String	☐	☑	☐	☐	☐	✖	☰
Select a value	First Name	fname;UserInfo	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Last Name	lname;UserInfo	String	☐	☑	☑	☐	☐	✖	☰
Select a value	E Mail Address	email;UserInfo	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Fax	fax;UserInfo	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Mobile	personnelno;UserInfo	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Telephone	telnumber;UserInfo	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Department	department;UserInfo	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Name	displayname	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Form of Address	personnelarea;UserI...	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Position	empposition;UserInfo	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Start Date of Acco	validFrom;UserInfo	Date	☐	☑	☑	☐	☐	✖	☰
Select a value	End Date of Accou	validTo;UserInfo	Date	☐	☑	☑	☐	☐	✖	☰
Select a value	Street	streetaddress	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Language	logonLang;UserInfo	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Time Zone	timezone	String	☐	☑	☑	☐	☐	✖	☰
Select a value	State	state	String	☐	☑	☑	☐	☐	✖	☰
Select a value	City	city	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Zip	zip	String	☐	☑	☑	☐	☐	✖	☰
Select a value	User Account Locl	userLock;None	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Security Policy	securitypolicy	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Unique ID	__UID__	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Country	country	String	☐	☑	☑	☐	☐	✖	☰
Select a value	AC Request Id	RequestId	String	☐	☑	☑	☐	☐	✖	☰
Select a value	AC Request Status	RequestStatus	String	☐	☑	☑	☐	☐	✖	☰
Select a value	AC Request Type	RequestType	String	☐	☑	☑	☐	☐	✖	☰
Select a value	AC Manager	manager;UserInfo	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Manager emai	managerEmail;UserI...	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Manager First	managerFirstname; ...	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Manager Last I	managerLastname; ...	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Priority	priority;Header	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Request Reaso	requestReason;Hea ...	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Request Due D	reqDueDate;Header	Date	☐	☑	☐	☐	☐	✖	☰
Select a value	AC System	reqInitSystem;Header	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Functional Are	funcarea;Header	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Business Proce	bproc;Header	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Requestor ID	requestorId;Header	String	☐	☑	☐	☐	☐	✖	☰
Select a value	AC Requestor emi	email;Header	String	☐	☑	☐	☐	☐	✖	☰
Select a value	Status	__ENABLE__	String	☐	☐	☑	☐	☐	✖	☰

Group Entitlement Attributes

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

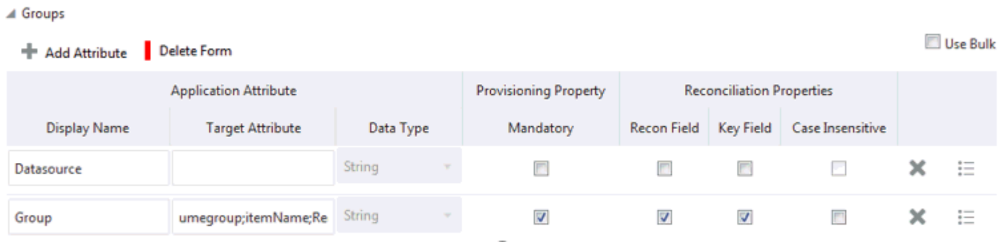
If required, you can edit these attribute mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-9 Default Attribute Mappings for a Group Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Datasource		String	No	No	No	No
Group	umegroup;itemnameReqLineItem	String	Yes	Yes	Yes	No

Figure 3-5 shows the default group entitlement mapping.

Figure 3-5 Default Attribute Mapping for a Group Entitlement



Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Datasource		String	□	□	□	□	✕	☰
Group	umegroup;itemName;Re	String	☑	☑	☑	□	✕	☰

Role Entitlement Attributes

Table 3-10 lists the role-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP AC UME attributes. The table lists whether a given role is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

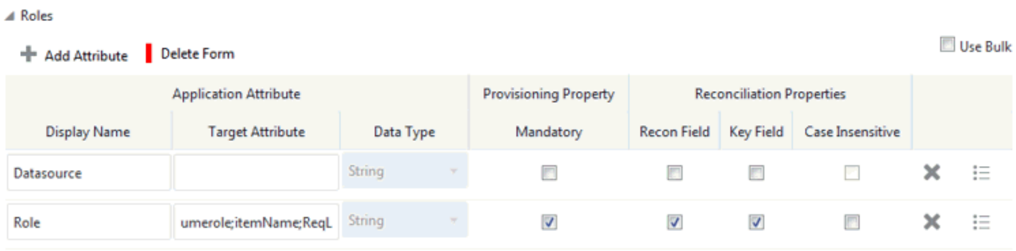
If required, you can edit these attribute mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-10 Default Attribute Mappings for a Role Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive ?
Datasource		String	No	No	No	No
role	umerole;itemnameReqLineItem	String	Yes	Yes	Yes	No

Figure 3-6 shows the default role entitlement mapping.

Figure 3-6 Default Attribute Mappings for a Role Entitlement



◢ Roles

➕ Add Attribute | Delete Form

□ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties		
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive
Datasource		String	□	□	□	□
Role	umerole;itemName;ReqL	String	☑	☑	☑	□

3.4 Correlation Rules

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

- Rules, Situations, and Responses for the SAP UME Connector
- Rules, Situations, and Responses for the SAP AC UME Connector

3.4.1 Rules, Situations, and Responses for the SAP UME Connector

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

Predefined Identity Correlation Rules

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

Table 3-11 lists the default simple correlation rule for the SAP UME connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-11 Predefined Identity Correlation Rule for the SAP UME Connector

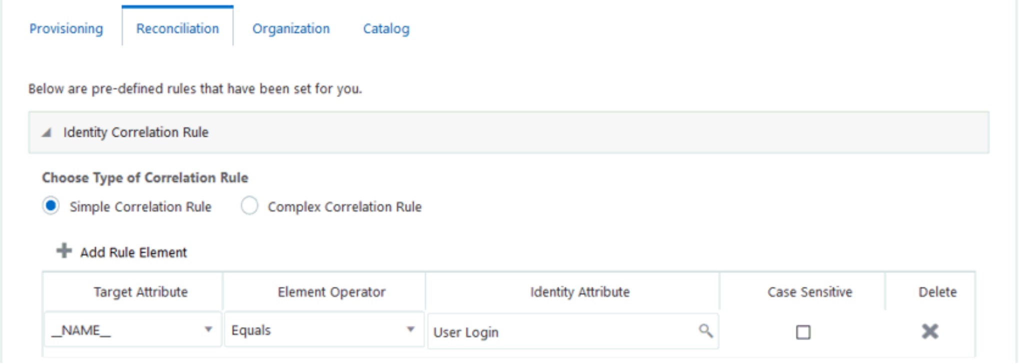
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

In this identity rule:

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

Figure 3-7 shows the simple correlation rule for the SAP UME Connector.

Figure 3-7 Simple Correlation Rule for the SAP UME Connector



Below are pre-defined rules that have been set for you.

Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
NAME	Equals	User Login	□	✖

Predefined Situations and Responses

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

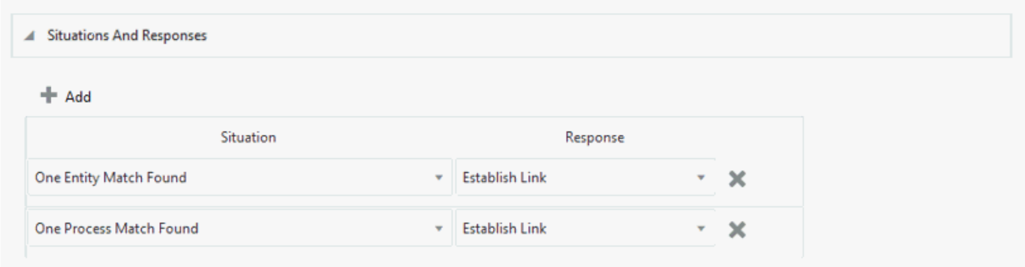
Table 3-12 lists the default situations and responses for the SAP UME connector.
If required, you can edit these default situations and responses or add new ones.
For more information about adding or editing situations and responses, see Updating Situations and Responses of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-12 Predefined Situations and Responses for the SAP UME Connector

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

Figure 3-8 shows the situations and responses that the connector provides by default.

Figure 3-8 Predefined Situations and Responses for the SAP UME Connector



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

3.4.2 Rules, Situations, and Responses for the SAP AC UME Connector

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

Predefined Identity Correlation Rules

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

Table 3-13 lists the default simple correlation rule for the SAP AC UME connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-13 Predefined Identity Correlation Rule for the SAP AC UME Connector

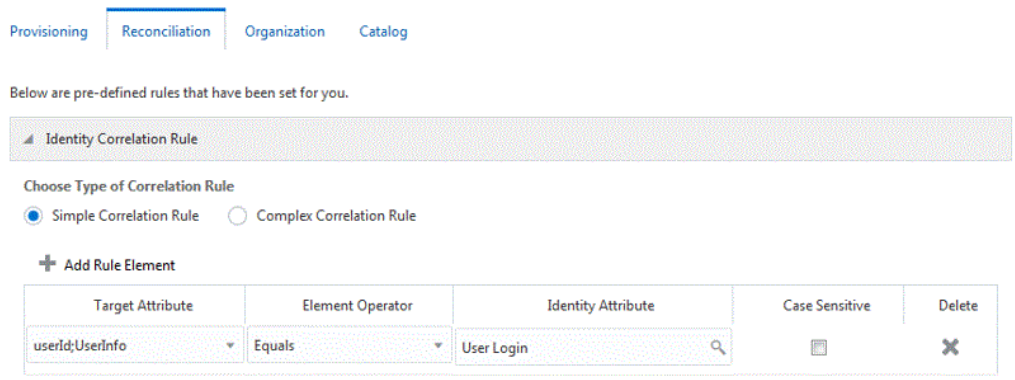
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
userId;UserInfo	Equals	User Login	No

In this identity rule:

- userId;UserInfo is a single-valued attribute on the target system that identifies the user ID of the user account.
- User Login is the field on the OIG User form.

Figure 3-9 shows the simple correlation rule for the SAP AC UME Connector.

Figure 3-9 Simple Correlation Rule for the SAP AC UME Connector



Below are pre-defined rules that have been set for you.

Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

Add Rule Element

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
userId;UserInfo	Equals	User Login	□	✖

Predefined Situations and Responses

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

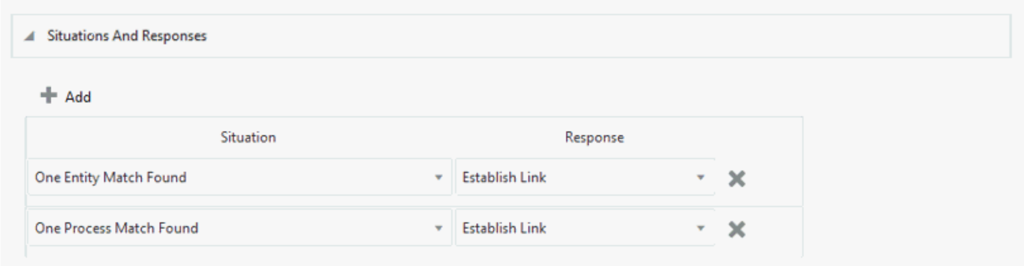
lists the default situations and responses for the SAP AC UME connector. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses of *Oracle Fusion Middleware Performing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

Table 3-14 Predefined Situations and Responses for the SAP AC UME Connector

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

Figure 3-10 shows the situations and responses that the connector provides by default.

Figure 3-10 Predefined Situations and Responses for the SAP AC UME Connector


Situations And Responses

Add

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

3.5 Reconciliation Jobs

These are the reconciliation jobs that the connector creates after you create your application.

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

3.5.1 Reconciliation Jobs for the SAP UME Connector

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

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

> **Note:**
>
> All of the jobs are prefixed with an application name when you create an application. For example, For SAPUMEAPP SAP UME Group Lookup Reconciliation where SAPUMEAPP is the application name.

Full User Reconciliation Job

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

Table 3-15 Parameters of the SAP UME Target User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Sample value: `SAPUMEAPP`
Filter	Enter the expression for filtering records that the scheduled job must reconcile. Sample value: `equalTo('__UID__','SEPT12USER1')` Default value: `None` For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.
Object Type	Enter the type of object you want to reconcile. Default value: `User`

User Delete Reconciliation Job

The SAP UME Target User Delete Reconciliation job is used to reconcile data about deleted user accounts from a target application.

Table 3-16 Parameters of the SAP UME Target User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value. Sample value: `SAPUMEAPP`
Object Type	Enter the type of object you want to reconcile. Sample Value: `User`

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- SAP UME Group Lookup Reconciliation: This reconciliation job is used to synchronize group lookup fields in Oracle Identity Governance with group-related data in the target system.
- SAP UME Role Lookup Reconciliation: This reconciliation job is used to synchronize role lookup fields in Oracle Identity Governance with role-related data in the target system.

The parameters for both the reconciliation jobs are the same.

Table 3-17 Parameters of the Reconciliation Jobs for Entitlements of the SAP UME Connector

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value. Default value: `SAPUMEAPP`
Lookup Name	This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched. Depending on the reconciliation job you are using, the default values are as follows: • For SAPUMEAPP SAP UME Group Lookup Reconciliation: `Lookup.SAPUME.UM.Group` • For SAPUMEAPP SAP UME Role Lookup Reconciliation: `Lookup.SAPUME.UM.Role`

Table 3-17 (Cont.) Parameters of the Reconciliation Jobs for Entitlements of the SAP UME Connector

Parameter	Description
Object Type	Enter the type of object whose values must be synchronized. Depending on the scheduled job you are using, the default values are as follows: • For SAPUMEAPP SAP UME Group Lookup Reconciliation: `GROUP` • For SAPUMEAPP SAP UME Role Lookup Reconciliation: `Role`
Code Key Attribute	Enter the name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job you are using, the default values of Code Key Attribute is as follows: • For SAPUMEAPP SAP UME Group Lookup Reconciliation: `id` • For SAPUMEAPP SAP UME Role Lookup Reconciliation: `id`
Decode Attribute	Enter the name of the connector or target system attribute that is used to populate the Decode Attribute column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job you are using, the default values of Decode Attribute is as follows: • For SAPUMEAPP SAP UME Group Lookup Reconciliation: `description` • For SAPUMEAPP SAP UME Role Lookup Reconciliation: `description`

3.5.2 Reconciliation Jobs for the SAP AC UME Connector

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

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

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

Full User Reconciliation Job

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

Table 3-18 Parameters of the SAP AC UME Target User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Sample value: `SAPACUMEAPP`
Filter	Enter the expression for filtering records that the scheduled job must reconcile. For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.
Object Type	Type of object you want to reconcile. Default value: `User`

User Delete Reconciliation Job

The SAP AC UME Target User Delete Reconciliation job is used to reconcile data about deleted user accounts from a target application.

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

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value. Sample value: `SAPACUMEAPP`
Object Type	Type of object you want to reconcile. Default value: `User`
SAP AC UME User Delete Recon	You can use the SAP AC UME Target User Delete Reconciliation scheduled job 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 AC UME resource is revoked for the corresponding OIG User. Default value: `Application Name`

SAP AC UME Request Status Job

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

Table 3-20 Parameters of the SAP AC UME Request Status Reconciliation Job

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

Note:

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

Reconciliation Jobs for Entitlements

The following jobs are available for lookup field synchonizations. You can configure these scheduled jobs for lookup field synchronization and reconciliation:

- 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 Request Type Lookup Reconciliation
- SAP AC UME Role Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-21 Parameters of the Reconciliation Jobs for Entitlements of the SAP AC UME Connector

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Sample Value: SAPACUMEAPP
Code Key Attribute `	Enter the name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job you are using, the default values are as follows: • For SAP AC UME BusinessProcess Lookup Reconciliation: LCODE • For SAP AC UME FunctionalArea Lookup Reconciliation: LCODE • For SAP AC UME Group Lookup Reconciliation: uniquename • For SAP AC UME ItemProvAction Lookup Reconciliation: LCODE • For SAP AC UME Priority Lookup Reconciliation: LCODE • For SAP AC UME ReqInitSystem Lookup Reconciliation: REQSYSCODE • For SAP AC UME Request Type Lookup Reconciliation: LCODE • For SAP AC UME Role Lookup Reconciliation: uniquename
Decode Attribute	Enter the name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job you are using, the default values are as follows: • For SAP AC UME BusinessProcess Lookup Reconciliation: LDECODE • For SAP AC UME FunctionalArea Lookup Reconciliation: LDECODE • For SAP AC UME Group Lookup Reconciliation: description • For SAP AC UME ItemProvAction Lookup Reconciliation: LDECODE • For SAP AC UME Priority Lookup Reconciliation: LDECODE • For SAP AC UME ReqInitSystem Lookup Reconciliation: REQSYSDECODE • For SAP AC UME Request Type Lookup Reconciliation: LDECODE • For SAP AC UME Role Lookup Reconciliation: description

Table 3-21 (Cont.) Parameters of the Reconciliation Jobs for Entitlements of the SAP AC UME Connector

Parameter	Description
Lookup Name	This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched. Depending on the reconciliation job you are using, the default values are as follows: • For SAP AC UME BusinessProcess Lookup Reconciliation: `Lookup.SAPACUME.Bproc` • For SAP AC UME FunctionalArea Lookup Reconciliation: `Lookup.SAPACUME.Funcarea` • For SAP AC UME Group Lookup Reconciliation: `Lookup.SAPACUME.Group` • For SAP AC UME ItemProvAction Lookup Reconciliation: `Lookup.SAPAC10UME.ItemProvAction` • For SAP AC UME Priority Lookup Reconciliation: `Lookup.SAPACUME.Priority` • For SAP AC UME ReqInitSystem Lookup Reconciliation: `Lookup.SAPACUME.ReqInitSystem` • For SAP AC UME Request Type Lookup Reconciliation: `Lookup.SAPAC10UME.RequestType` • For SAP AC UME Role Lookup Reconciliation: `Lookup.SAPACUME.Role`
Object Class	Enter the class of object whose values must be synchronized. Depending on the scheduled job you are using, the default values are as follows: • For SAP AC UME BusinessProcess Lookup Reconciliation: `BusProc` • For SAP AC UME FunctionalArea Lookup Reconciliation: `FunctionArea` • For SAP AC UME Group Lookup Reconciliation: `_GROUP_` • For SAP AC UME ItemProvAction Lookup Reconciliation: `ItemProvActionType` • For SAP AC UME Priority Lookup Reconciliation: `PriorityType` • For SAP AC UME ReqInitSystem Lookup Reconciliation: `SYSTEM` • For SAP AC UME Request Type Lookup Reconciliation: `RequestType` • For SAP AC UME Role Lookup Reconciliation: `_ROLE_`

Table 3-21 (Cont.) Parameters of the Reconciliation Jobs for Entitlements of the SAP AC UME Connector

Parameter	Description
Object Type	Enter the type of object whose values must be synchronized. Depending on the scheduled job you are using, the default values are as follows: • For SAP AC UME BusinessProcess Lookup Reconciliation: `BusProc` • For SAP AC UME FunctionalArea Lookup Reconciliation: `FunctionArea` • For SAP AC UME Group Lookup Reconciliation: `Group` • For SAP AC UME ItemProvAction Lookup Reconciliation: `ItemProvActionType` • For SAP AC UME Priority Lookup Reconciliation: `Priority Type` • For SAP AC UME ReqInitSystem Lookup Reconciliation: `SYSTEM` • For SAP AC UME Request Type Lookup Reconciliation: `RequestType` • For SAP AC UME Role Lookup Reconciliation: `Role`

4 Performing Postconfiguration Tasks for the SAP User Management Engine Connector

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

- Configuring Oracle Identity Governance
- Harvesting Entitlements and Sync Catalog
- Configuring Password Changes for Newly Created Accounts
- Managing Logging
- Configuring SSL to Secure Communication Between the Target System and Oracle Identity Governance
- 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 GRC
- Localizing Field Labels in UI Forms
- Synchronizing the SAPUME Process Form and SAP AC UME Process Form with Target System Field Lengths

4.1 Configuring Oracle Identity Governance

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

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

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

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

4.1.2 Creating a New UI Form

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

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

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

4.1.3 Publishing a Sandbox

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

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

4.1.4 Creating an Application Instance

Create an application instance as follows

1. In the left pane of the Identity System Administration, under Configuration, click **Application Instances.** The Application Instances page appears.
2. From the Actions menu, select **Create.** Alternatively, click **Create** on the toolbar. The Create Application Instance page appears.
3. Specify values for the following fields:
   - **Name:** The name of the application instance.
   - **Display Name:** The display name of the application instance.
   - **Description:** A description of the application instance.

- **Resource Object:** The resource object name. Click the search icon next to this field to search for and select SAP UME Resource Object.
- **IT Resource Instance:** The IT resource instance name. Click the search icon next to this field to search for and select SAP UME.ITResource.
- **Form:** Select the form name (Creating a New UI Form).

4. Click **Save**.

   The application instance is created.

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

4.1.5 Updating an Existing Application Instance with a New Form

For any changes that you do in the schema of your application in Identity Self Service, you must create a new UI form and update the changes in an application instance.

To update an existing application instance with a new form:

1. Create and activate a sandbox.
2. Create a new UI form for the resource.
3. Open the existing application instance.
4. In the Form field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox.

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

4.2 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

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

See Also:

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

4.3 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 Governance, password management can be configured by using the changePwdFlag and dummyPassword parameters of the Advanced Settings section.

You can apply one of the following approaches:

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

  To achieve this, set the changePwdFlag parameter of Basic Configuration section 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 Governance is set as the new password on the target system. The user is not prompted to change the password at first logon.

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

  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`.

4.4 Managing Logging

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

4.4.1 Understanding Log Levels

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

ODL is the principle logging service used by Oracle Identity Governance and is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.
- SEVERE

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

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

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

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

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

These message types are mapped to ODL message type and level combinations as shown in Table 4-1.

Table 4-1 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

Table 4-1 (Cont.) Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
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 Governance.

4.4.2 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. Understanding Log Levels 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 Governance, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

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

   For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

   For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

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

4. Restart the application server.

4.5 Configuring SSL to Secure Communication Between the Target System and Oracle Identity Governance

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

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

1. Generate the certificate on the target system.

   See the target system documentation for detailed instructions.

2. To import the certificate on Oracle Identity Governance:

   a. Copy the target system certificate to the Oracle Identity Governance 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 4-2 shows the location of the certificate store of the supported application server.

   The following is a sample command:

   ```
   keytool -import -alias ibm1-cert140 -
   file C:\syaug24\Middleware\ibm1-cert.cer -keystore
   C:\syaug24\Middleware\jrockit_160_24_D1.1.2-4\jre\lib\security\cacerts -
   storepass changeit
   ```

Table 4-2 Certificate Store Locations

Application Server	Certificate Store Location
Oracle WebLogic Server	• If you are using Oracle jrockit_R27.3.1-jdk, then copy the certificate into the following directory: *JROCKIT_HOME*/jre/lib/security/cacerts • If you are using the default Oracle WebLogic Server JDK, then copy the certificate into the following directory: *WEBLOGIC_HOME*/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
```

4.6 Configuring the IT Resource for the Connector Server

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

After you create the application for your target system, you must create an IT resource for the Connector Server as described in Creating IT Resources of *Oracle Fusion Middleware Administering Oracle Identity Governance*. While creating the IT resource, ensure to select **Connector Server** from the **IT Resource Type** list. In addition, specify values for the parameters of IT resource for the Connector Server listed in Table 4-3. For more information about searching for IT resources and updating its parameters, see Managing IT Resources in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

Table 4-3 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 Governance times out. Sample value: `300`
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter `false.` Default value: `false` **Note:** 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.

4.7 Configuring the Access Request Management Feature of the Connector

You can configure Oracle Identity Governance as the medium for sending provisioning requests to SAP GRC Access Request Management. A request from Oracle Identity Governance is sent to Access Request Management, which forwards the provisioning data contained within the request to the target system (SAP NetWeaver Java Application Server). 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 an Application Configuration.

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

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

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

4.8 Configuring SoD (Segregation of Duties)

SoD is a process that ensures that 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 Basic Configuration 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.

4.8.1 Specifying Values for the GRC UME-ITRes IT Resource

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

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

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

Table 4-4 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`
username	Enter the user name of an account created on Access Request Management system. This account is used to call Access Request Management system APIs that are used during request validation. Sample value: `jdoe`

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

4.8.2 Configuring SAP GRC to Act As the SoD Engine

To configure 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 11*g* Release 1 (11.1.2).

4.8.3 Specifying a Value for the TopologyName Basic Configuration Parameter

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

- Oracle Identity Governance installation
- SAP GRC installation
- SAP ERP installation

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 Basic Configuration Parameters for information about specifying values for Basic Configuration Parameters.

4.8.4 Disabling and Enabling SoD

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

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

4.8.4.1 Disabling SoD on Oracle Identity Governance

To disable SoD:

1. For Oracle Identity Governance release 12.2.1.3.0, log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **System Configuration.**
3. In the Search System Configuration box, enter `XL.SoDCheckRequired` and then click **Search.**

   A list that matches your search criteria is displayed in the search results table.
4. Click the **XL.SoDCheckRequired** property name.

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

4.8.4.2 Enabling SoD on Oracle Identity Governance

To enable SoD:

1. For Oracle Identity Governance release 12.2.1.3.0, log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **System Configuration.**
3. In the Search System Configuration box, enter `XL.SoDCheckRequired` and then click **Search.**

   A list that matches your search criteria is displayed in the search results table.
4. Click the **XL.SoDCheckRequired** property name.

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

4.9 Downloading WSDL files from SAP GRC

You need to download the WSDL files from SAP GRC before configuring the web services in SAP GRC. 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 OIG:

WSDL	Description
GRAC_AUDIT_LOGS_WS	Audit log web service
GRAC_LOOKUP_WS	Look Up Service
GRAC_REQUEST_STATUS_WS	Request status web service
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.

4.10 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 (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer.
5. Extract the contents of the archive, and open the *SAVED_LOCATION*\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf file in a text editor:

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

6. Edit the BizEditorBundle.xlf file in the following manner:

   a. Search for the following text:

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

   b. Replace with the following text:

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

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

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

   c. Search for the application instance code. This procedure shows a sample edit for SAP User Management 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 Governance* for more information about exporting and importing metadata files

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

4.11 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.

5
Using the SAP User Management Engine Connector

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

- Configuring Reconciliation
- Configuring Reconciliation Jobs
- Configuring Provisioning
- Uninstalling the Connector

5.1 Configuring Reconciliation

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

Reconciliation involves duplicating in Oracle Identity Governance the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Performing Full Reconciliation
- Performing Limited Reconciliation

5.1.1 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Governance. After you create the application, you must first perform full reconciliation.

To perform a full reconciliation run, remove (delete) any value currently assigned to the Filter parameter of the SAP UME Target User Reconciliation job.

5.1.2 Performing 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 parameter that allows you to use any of the SAP UME resource parameters 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')
```

5.2 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

1. Log in to Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the parameters of the scheduled task:
   - **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

In addition to modifying the job details, you can enable or disable a job.

5. On the **Job Details** tab, in the Parameters region, specify values for the attributes of the scheduled task.

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

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

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

5.3 Configuring Provisioning

You can configure the provisioning operation for the SAP UME and SAP AC UME connectors.

This section provides information on the following topics:

- Guidelines on Performing Provisioning
- Performing Provisioning Operations

5.3.1 Guidelines on Performing Provisioning

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

> **See Also:**
>
> Guidelines on Using an Application Configuration

This section provides more information about the following guidelines:

- Guidelines for Performing Provisioning Operations in Supported Deployment Configurations
- Guidelines for Performing Provisioning Operations After Configuring Access Request Management

5.3.1.1 Guidelines for Performing Provisioning Operations in 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 Governance.
- If you disable a user account in Oracle Identity Governance, the connector updates the value of the Valid Through parameter 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 parameter with today's date and lock the user.

  Ensure that the dates on Oracle Identity Governance 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 Governance, then an error is encountered. Therefore, the length of the Logon Name field must be limited to 15 characters in Oracle Identity Governance.
- 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 parameter 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 OIG User is in the Disabled state immediately after the account is created.

  However, on the target system, if you set the Valid Through parameter 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 parameter on Oracle Identity Governance and the target system do not match.
  - On the target system, the user can log in all through the current day. The user cannot log in from the next day onward.

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

and Customizing Applications for Oracle Identity Governance for information about configuring process tasks.

- When you perform the Lock User or Unlock User provisioning operation, remember that the connector makes the required change on the target system without checking whether the account is currently in the Locked or Unlocked state. This is because the target system does not provide a method to check the current state of the account.
- The target system does not accept non-English letters in the E-mail Address field. Therefore, during provisioning operations, you must enter only English language letters in the E-mail Address field on the process form.
- When you assign a role to a user through provisioning, you set values for the following parameters:
  - Datasource
  - Role

5.3.1.2 Guidelines for Performing Provisioning Operations After Configuring Access Request Management

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 parameters on SAP GRC Access Request Management:
  - AC Manager
  - AC Manager email
  - AC Priority
  - AC System
  - AC Requestor ID
  - AC Requestor email
  - AC Request Reason

> **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.

The following fields may be mandatory or optional based on the configuration in SAP GRC 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
- SAP GRC Access Request Management does not process passwords. Therefore, during Create User provisioning operations, the system ignores any value entered in the Password field. After a Create User operation is performed, the user for whom the account is created on the target system must apply one of the following approaches to set the password:
  - To use the Oracle Identity Governance password as the target system password, change the password through Oracle Identity Governance.
  - Directly log in to the target system, and change the password.
- You perform an Enable User operation by setting the Valid From field to a future date. Similarly, you perform a Disable User operation by setting the Valid Through field to the current date. Both operations are treated as Modify User operations.
- When you delete a user (account) on Oracle Identity System Administration (process form), a Delete User request is created.
- When you select the Lock User check box on the process from, a Lock User request is created.
- When you deselect the Lock User check box on the process from, an Unlock User request is created.
- The Enable User and Disable User operations are implemented through the Valid From and Valid Through fields on the process form.
- In a Modify User operation, you can specify values for parameters that are mapped with SAP GRC Access Request Management and parameters that are directly updated on the target system. A request is created in SAP GRC Access Request Management only for parameters whose mappings are present in these lookup definitions. If you specify values for parameters that are not present in these lookup definitions, then the connector sends them to directly the target system.

5.3.2 Performing Provisioning Operations

You create a new user in Identity Self Service by using the Create User page. You provision or request for accounts on the Accounts tab of the User Details page.

To perform provisioning operations in Oracle Identity Governance:

1. Log in to Identity Self Service.
2. Create a user as follows:

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

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

5.4 Uninstalling the Connector

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

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

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

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

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

6 Extending the Functionality of the SAP User Management Engine Connector

You can extend the functionality of the connector to address your specific business requirements.
This chapter provides information on the following optional procedures:

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

6.1 Configuring the Connector for Multiple Installations of the Target System

You can configure the connector for multiple installations of the target system.

You must create copies of configurations of your base application to configure it for multiple installations of the target system.

The following example illustrates this requirement:

The London, New York, and Toronto offices of Example Multinational Inc. have their own installations of the target system, including independent schema for each. The company has recently installed Oracle Identity Governance, and they want to configure it to link all the installations of the target system.

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

6.2 Configuring Transformation and Validation of Data

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

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Governance.

Similarly, you can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

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

6.3 Configuring Resource Exclusion Lists

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

See Validation and Transformation of Provisioning and Reconciliation Attributes of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for more information about configuring resource exclusion lists.

6.4 Configuring Action Scripts

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

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

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

7

Upgrading the SAP User Management Engine Connector

You can upgrade the SAP UME 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.

If you have already deployed 11.1.1.9.0 version of this connector, then you can upgrade the connector to version 12.2.1.3.0.

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

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

> **Note:**
>
> - Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Governance database. Refer to the database documentation for information about creating a backup.
> - As a best practice, first perform the upgrade procedure in a test environment.
> - Direct upgrade to release 11.1.1.9.0 or later from release 9.*x* of the connector is not supported. You must first upgrade to release 11.1.1.8.0 from release 9.*x* and then upgrade to release 11.1.1.9.0 or later.

7.1 Preupgrade Steps

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

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

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

3. Run the Oracle Identity Governance Delete JARs utility to delete the old connector bundle from the Oracle Identity Manager database.
4. Run the connector preupgrade utility.

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

7.2 Upgrade Steps

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

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

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.

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

- Production Environment

  Perform the upgrade procedure by using the silent mode.

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

7.3 Postupgrade Steps

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

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

Perform the following procedure:

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

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

   For Basic User Management and SoD validation of SAP GRC Access Risk Analysis:

   - Upload bundle/org.identityconnectors.sapume-12.3.0.jar as an ICFBundle
   - Upload lib/sapume-oim-integration.jar as a JavaTask

   For SAP GRC Access Request Management,

   - Upload bundle/org.identityconnectors.sapacume-12.3.0.jar as an ICFBundle
   - Upload lib/sapac-oim-integration.jar as a ScheduleTask

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

2. If the connector is deployed on a Connector Server, then:

   a. Stop the Connector Server.

   b. Replace the existing connector bundle and lib JARs located in the *CONNECTOR_SERVER_HOME*/bundles and *CONNECTOR_SERVER_HOME*/lib directories respectively with the new connector bundles (bundle/org.identityconnectors.sapacume-12.3.0.jar and bundle/org.identityconnectors.sapume-12.3.0.jar) and lib JARs (lib/sapac-oim-integration.jarlib/sapume-oim-integration.jar) from the connector installation media.

   c. Start the Connector Server.

3. Reconfigure the IT resource of the connector if the IT resource details are updated.
4. Replicate all changes as in the previous version of the connector process form in a new UI form as follows:
   a. Log in to Oracle Identity System Administration.
   b. Create and activate a sandbox.
   c. Create a new UI form to view the upgraded fields.
   d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource from the form field, select the form (created in Step 4 c) and then save the application instance.
   e. Publish the sandbox and perform full reconciliation.
5. Delete the duplicated lookup entries that are generated while upgrading the connector.

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

   - For Basic User Management Engine and SoD validation of SAP GRC Access Risk Analysis:
     – Lookup.SAPUME.Configuration
     – Lookup.SAPUME.UM.ProvAttrMap
     – Lookup.SAPUME.UM.ReconAttrMap
   - For SAP GRC Access Request Management:
     – Lookup.SAPAC10UME.Configuration
     – Lookup.SAPAC10UME.UM.ProvAttrMap
     – Lookup.SAPAC10UME.UM.ReconAttrMap

   Perform the postupgrade procedure documented in Managing Connector Lifecycle of *Oracle Fusion Middlware Administering Oracle Identity Governance*.
6. Run the Form Upgrade Job to manage data changes on a form after an upgrade operation.
7. Perform full reconciliation or delete reconciliation.

See Also:

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

8

Known Issues and Limitations of the SAP User Management Engine Connector

These are the known issues and limitations associated with the SAP UME connector.

This chapter is divided into the following sections:

- Known Issues
- Limitations Related to Target System Features and Specific Connectors

8.1 Known Issues

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

- Connector Issues
- Oracle Identity Governance Issues

8.1.1 Connector Issues

These are the known issues and workarounds associated with the connector.

- Error During SoD Check
- Code Key Values Displayed Instead of Decode Values
- Accessing the Target Server or Running the Connector Server returns an Error
- Postupgrade Issue
- Lookup Data of Timezone, Country, and Locale is not Dynamic

8.1.1.1 Error During SoD Check

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

Workaround: If the size of the violation details obtained from SAP GRC target system is more than 4000 characters, then you must update the Length of the SODCheckViolation field as per the expected size of the violation data.

8.1.1.2 Code Key Values Displayed Instead of Decode Values

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 in the edit and view form.

Workaround: There is no workaround for this issue.

8.1.1.3 Accessing the Target Server or Running the Connector Server returns an Error

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.

Workaround: There is no workaround for this issue.

8.1.1.4 Postupgrade Issue

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

- Lookup.SAPUME.Configuration
- Lookup.SAPUME.UM.ProvAttrMap
- Lookup.SAPUME.UM.ReconAttrMap
- Lookup.SAPAC10UME.Configuration
- Lookup. SAPAC10UME.UM.ProvAttrMap
- Lookup.SAPAC10UME.UM.ReconAttrMap

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

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

Code	Decode
Bundle Version	12.3.0
SOD Configuration lookup	Lookup.SAPUME.Configuration
User Configuration Lookup	Lookup.SAPUME.UM.Configuration
Connector Name	org.identityconnectors.sapume.SAPUMEConnector
Bundle Name	org.identityconnectors.sapume
Role attribute name	ROLENAME
RoleAttributeLabel	Role
SODSystemKey	GRCACEP
Role form names	UD_UMERC_P;UD_UME_ROLE
entitlementRiskAnalysisWS	oracle.iam.grc.sod.scomp.impl.grcsap.util.webservice.sap.ac10.RiskAnalysisWithoutNoentitlementRiskAnalysisAccessURL
wsdlFilePath	None
Group form names	UD_UME_GRP
Group attribute name	GROUPNAME
ConnectorImplType	SAPUME

The following table lists the entries in the Lookup.SAPUME.UM.ProvAttrMap lookup definition.

Table 8-2   Entries in the Lookup.SAPUME.UM.ProvAttrMap Lookup Definition

Code	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
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
UD_UME_GRP~Group[Lookup]	assignedgroups
UD_UME_ROLE~Role[Lookup]	assignedroles
Unique ID	__UID__
User Account Locked	islocked
Zip	zip

The following table lists the entries in the Lookup.SAPUME.UM.ReconAttrMap lookup definition.

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

Code	Decode
City	city
Country	country
Department	department

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

Code	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

The following table lists the entries in the Lookup.SAPAC10UME.Configuration lookup definition.

Table 8-4   Entries in the Lookup.SAPAC10UME.Configuration Lookup Definition

Code	Decode
appLookupAccessURL	None
appLookupWS	oracle.iam.ws.sap.ac10.SelectApplication
assignRoleReqType	002~Change Account~002~006
auditLogsAccessURL	None
auditLogsWS	oracle.iam.ws.sap.ac10.AuditLogs
Bundle Name	org.identityconnectors.sapacume

Table 8-4   (Cont.) Entries in the Lookup.SAPAC10UME.Configuration Lookup Definition

Code	Decode
Bundle Version	12.3.0
ConnectorImplType	SAPUME
Connector Name	org.identityconnectors.sapacume.SAPACUME Connector
createUserReqType	001~New Account~001
deleteUserReqType	003~Delete Account~003
ignoreOpenStatus	Yes
lockUserReqType	004~Lock Account~004
logAuditTrial	Yes
modifyUserReqType	002~Change Account~002
otherLookupAccessURL	None
otherLookupWS	oracle.iam.ws.sap.ac10.SearchLookup
provActionAttrName	provAction;ReqLineItem
provItemActionAttrName	provItemAction;ReqLineItem
removeRoleReqType	002~Change Account~002~009
requestStatusAccessURL	None
requestStatusValue	OK
requestStatusWS	oracle.iam.ws.sap.ac10.RequestStatus
requestTypeAttrName	Reqtype;Header
riskLevel	High
roleLookupAccessURL	None
roleLookupWS	oracle.iam.ws.sap.ac10.SearchRoles
Status Configuration Lookup	Lookup.SAPACUME.Status.Configuration
unlockUserReqType	005~unlock user~005
userAccessWS	oracle.iam.ws.sap.ac10.UserAccess
User Configuration Lookup	Lookup.SAPAC10UME.UM.Configuration
wsdlFilePath	None

The following table lists the entries in the Lookup.SAPAC10UME.UM.ProvAttrMap lookup definition.

Table 8-5   Entries in the Lookup.SAPAC10UME.UM.ProvAttrMap Lookup Definition

Code	Decode
AC Business Process[Lookup]	bproc;Header
Accounting Number	accno;UserInfo
AC Functional Area[Lookup]	funcarea;Header
AC Manager	manager;UserInfo

Table 8-5 (Cont.) Entries in the Lookup.SAPAC10UME.UM.ProvAttrMap Lookup Definition

Code	Decode
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	empposition;UserInfo
Security Policy	securitypolicy
Start Date of Account Validity[Date]	validFrom;UserInfo
State	state
Street	streetaddress
Telephone	telnumber;UserInfo
Time Zone	timezone
UD_ACUMEGRP~Group[Lookup]	umegroup;itemName;ReqLineItem
UD_ACUMEROL~Role[Lookup]	umerole;itemName;ReqLineItem
Unique ID	__UID__
User Account Locked	userLock;None

Table 8-5 (Cont.) Entries in the Lookup.SAPAC10UME.UM.ProvAttrMap Lookup Definition

Code	Decode
Zip	zip

The following table lists the entries in the Lookup.SAPAC10UME.UM.ReconAttrMap lookup definition.

Table 8-6 Entries in the Lookup.SAPAC10UME.UM.ReconAttrMap Lookup Definition

Code	Decode
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
Groups~Group[Lookup]	assignedgroups
Language	logonLang;UserInfo
Last Name	lname;UserInfo
Logon Name	userId;UserInfo
Mobile	personnelno;UserInfo
Name	displayname
Position	empposition;UserInfo
Roles~Role[Lookup]	assignedroles
Security Policy	securitypolicy
Start Date of Account Validity[Date]	validFrom;UserInfo
State	state
Status	__ENABLE__
Street	streetaddress
Telephone	telnumber;UserInfo
Time Zone	timezone
Unique Id	__UID__
User Account Locked	userLock;None
Zip	zip

Workaround: Delete each instance of the duplicate entries with decode default values.

8.1.1.5 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.

Workaround: If there is any mismatch in data between target and lookup, customer needs to modify the lookups manually in the OIM design console.

8.1.2 Oracle Identity Governance Issues

These are the issues and workarounds associated with Oracle Identity Governance.

- Revoke Account Task Rejected and Unable to Update OIG Account
- Date 9999 Issue While Provisioning a User in the Enterprise Portal

8.1.2.1 Revoke Account Task Rejected and Unable to Update OIG Account

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 OIG.

Workaround: There is no workaround for this issue.

8.1.2.2 Date 9999 Issue While Provisioning a User in the Enterprise Portal

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: Apply the following SNOTEs on top of GRCFND_A SP 10:

- SNOTE 2653244
- SNOTE 2203867

8.2 Limitations Related to Target System Features and Specific Connectors

These are limitations related to target system features and specific connectors.

- 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:

8.2.1 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.

8.2.2 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.

8.2.3 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.

9 Frequently Asked Questions of the SAP User Management Engine Connector

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

1. I have installed only the SAP UME connector in my Oracle Identity Governance (OIG) environment. I want to use it with SAP GRC. 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 changed the system property for SOD as XL.SoDCheckRequired = TRUE. Is it now possible to use two SAP connectors in the same OIG environment having one connector configured for SOD analysis and the other connector configured without SOD analysis?

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

4. I have configured the 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.AC*xx.*Configuration where *xx* denotes 10 for SAP GRC 10 release. You need to mention the correct system value.

5. 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 Trial: {Result=[Createdate:20130409,

Priority: HIGH,

Requestedby:, johndoe (JOHNDOE),

Requestnumber: 9000001342,

Status: Decision pending,

Submittedby:,johndoe (JOHNDOE),

auditlogData:{,

ID: 000C290FC2851ED2A89A3ED3B1D7B1E2,

Description:,

Display String: Request 9000001342 of type **Change Account** Submitted by johndoe (JOHNDOE) for JK1FirstName JK1APRIL9 (JK1APRIL9) with Priority HIGH}],

Status=0_Data Populated successfully}

6. 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 Target User Reconciliation job before performing any provisioning operations.

7. 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. In the Configtool GUI, change the value of the `use.spml.http_header_check_active` parameter to `false` if it had been set to `true`.

8. 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.

A

Files and Directories in the SAP User Management Engine Connector Installation Package

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

Table A-1 Files and Directories in the Connector Installation Package

File in the Installation Media Directory	Description
bundle/ org.identityconnectors.sapume-12.3.0.jar	These JAR files contain the connector bundle.
bundle/ org.identityconnectors.sapacume-12.3.0.jar	These JAR files contain GRC system connector bundle.
configuration/ SAPUMEConnector-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the SAP UME Connector Installer during connector installation.
configuration/ SAPACUMEConnector-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the SAP AC UME Connector Installer during connector installation.
lib/sapume-oim-integration.jar	This JAR file is required to request entitlements for roles and profiles through request-based provisioning using request dataset. **Note:** This file will not be used if you are using Oracle Identity Manager release 11.1.2.x or later.
lib/sapac-oim-integration.jar	This JAR file includes a custom scheduled job to update request status from SAP GRC. **Note:** This file will not be used if you are using Oracle Identity Manager release 11.1.2.x or later.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied to Oracle Identity Governance database. **Note:** A resource bundle is a file containing localized versions of the text strings that include GUI element labels and messages.
xml/SAPUME-Datasets.xml	This XML file contains attributes of the following resource objects for request-based provisioning:SAP UME Resource Object (to provision and modify resources)SAP UME Roles (to provision role entitlements)SAP UME Profiles (to provision profile entitlements) **Note:** This file is applicable only for a CI-based connector. You must not import this dataset if you are using Oracle Identity Governance release 11.1.2.x or later.

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

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