Oracle® Identity Governance

Configuring SAP Fieldglass Connector

12c (12.2.1.3.0)

F96084-02

Oracle Identity Governance Configuring SAP Fieldglass Connector, 12c (12.2.1.3.0)

F96084-02

Primary Author: Maya Chakrapani

Contributing Authors: Brinda M, Syam Bhattu

Contents

1 Introduction to the Connector

2 Creating an Application By Using the Connector

3 Configuring the SAP Fieldglass Connector

4 Performing Postconfiguration Tasks for the Connector

List of Figures

List of Tables

1 Introduction to the Connector

Oracle Identity Governance is a centralized identity management solution that provides self service, compliance and provisioning services for applications residing on the Cloud. Oracle Identity Governance connectors are used to integrate Oracle identity Governance with the external identity-aware applications. The SAP Fieldglass Connector lets you onboard applications, pertaining to the SAP Fieldglass target system, in Oracle Identity Governance.

> **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**.

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 sections provide a high-level overview of the connector:

1. Certified Components
2. Certified Languages
3. Usage Recommendation
4. Supported Connector Operations
5. Connector Architecture
6. Use Cases Supported by the Connector
7. Connector Features

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
Oracle Identity Governance or Oracle Identity Manager	You can use any one of the following releases: 1. Oracle Identity Governance release 12c PS4 (12.2.1.4.0) or later. 2. Oracle Identity Governance release 12c PS3 (12.2.1.3.0) or later.
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later
Target systems	SAP Fieldglass
Connector Server	11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 and later
Target API version	V1

1.2 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

1.3 Usage Recommendation

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

- If you are using Oracle Identity Governance 12c (12.2.1.3.0), 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. **Use Cases Supported by the Connector**

1.4 Supported Connector Operations

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

If you are using Oracle Identity Governance 12c (12.2.1.3.0), 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. Supported Connector Operations These are the list of operations that the connector supports for your target system.

Table 1-2 Supported Connector Operations

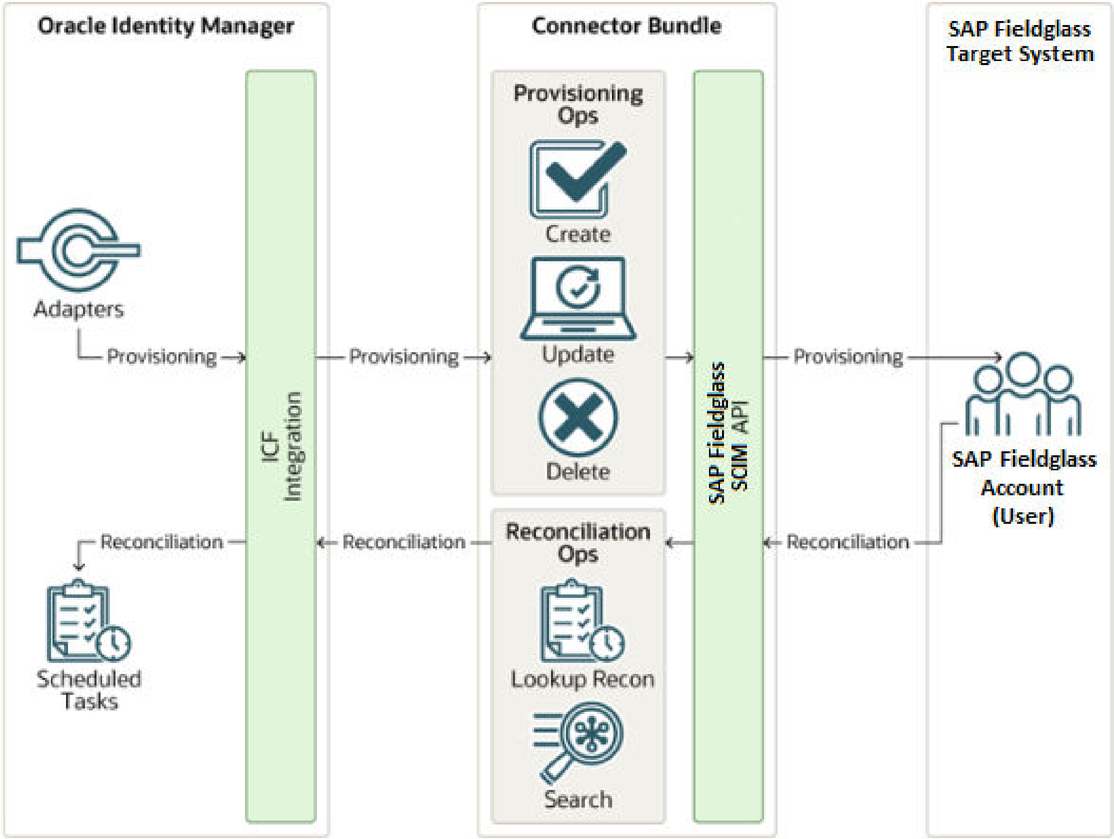
Operation	Supported?
User Management	
Create user	Yes
Update user	Yes
Enable user	No
Disable user	No
Delete user	Yes
Reset Password	No
Group Assignment	
Assign and Revoke Groups	Yes

1.5 Connector Architecture

The SAP Fieldglass Connector enables management of accounts on the target system through Oracle Identity Governance.

The following figure shows architecture of the SAP Fieldglass Connector.

Figure 1-1 Architecture of the SAP Fieldglass Connector



The connector is configured to run in one of the following modes:

- **Account management**
  Account management is also known as target resource management. In this mode, the target system is used as a target resource and the connector enables the following operations:
  – **Provisioning**
    Provisioning involves creating, updating, or deleting users on the target system through Oracle Identity Governance. During provisioning, the Adapters invoke ICF operation, ICF in turn invokes create operation on the SAP Fieldglass Identity Connector Bundle and then the bundle calls the target system API (SAP Fieldglass API) for provisioning operations. The API on the target system accepts provisioning data from the bundle, carries out the required operation on the target system, and returns the response from the target system back to the bundle, which passes it to the adapters.
  – **Target resource reconciliation**
    During reconciliation, a scheduled task invokes an ICF operation. ICF in turn invokes a search operation on the SAP Fieldglass Identity Connector Bundle and then the bundle calls SAP Fieldglass API for Reconciliation operation. The API extracts user records that match the reconciliation criteria and hands them over through the bundle and ICF back to the scheduled task, which brings the records to Oracle Identity Governance.

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

The SAP Fieldglass Identity Connector Bundle communicates with the SAP Fieldglass API using the HTTPS protocol. The SAP Fieldglass API provides programmatic access to SAP Fieldglass through SCIM API endpoints. Apps can use the SCIM API to perform create, read, update, and delete (CRUD) operations on directory data and directory objects, such as users, groups.

> **See Also:**
>
> Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications* for Oracle Identity Governance for more information about ICF.

1.6 Use Cases Supported by the Connector

SAP Fieldglass can be integrated with Oracle Identity Governance to ensure synchronized lifecycle management of privileged accounts within your enterprise, aligning with other identity-aware applications. SAP Fieldglass offers identity management for various models, including Cloud Identity, Synchronized Identity, and Federated Identity, making it a valuable choice for organizations seeking consistent management of accounts, groups. The following is the most common scenarios in which this connector can be used:

- **SAP Fieldglass User Management:**

An organization using SAP Fieldglass aims to integrate it with Oracle Identity Governance for efficient identity management. This integration enables user identity creation within the target system via Oracle Identity Governance. It also facilitates the synchronization of user identity changes made directly in the target system with Oracle Identity Governance.

To achieve this, you need to configure the SAP Fieldglass connector application with your target system, providing the necessary connection details. When you wish to create a new user in the target system, you can complete and submit the OIM process form to initiate the provisioning operation. The connector will execute the CreateOp operation in the target system, resulting in the user's creation upon successful execution. Updates can be performed in a similar manner.

For searching and retrieving user identities, a scheduled task from Oracle Identity Governance must be run. The connector will execute the corresponding SearchOp operation within the target system, capturing all changes and syncing them with Oracle Identity Governance.

1.7 Connector Features

The features of the connector include support for connector server, connector operations in multiple domains, full reconciliation, limited reconciliation and others.

For searching and retrieving user identities, a scheduled task from Oracle Identity Governance must be run. The connector will execute the corresponding SearchOp operation within the target system, capturing all changes and syncing them with Oracle Identity Governance.

The following table provides the list of features supported by the AOB application connector.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application
User Provisioning	Yes
Full reconciliation	Yes
Limited (Filtered)reconciliation	Yes
Use connector server	Yes
Transformation and validation of account data	Yes
Perform connector operations in multiple domains	Yes
Support for pagination	Yes
Test connection	Yes
Clone applications or create new application instances	Yes
Provide secure communication to the target system through SSL	Yes

The following topics provide more information on the features of the AOB application:

1. User Provisioning
2. Full Reconciliation
3. Limited (Filtered)Reconciliation
4. Support for the Connector Server
5. Transformation and Validation of Account Data
6. Support for Cloning Applications and Creating Instance Applications
7. Secure Communication to the Target System

1.7.1 User Provisioning

User provisioning involves creating or modifying the account data on the target system through Oracle Identity Governance.

> **Note:**
>
> For more information, see Performing Provisioning Operations.

1.7.2 Full Reconciliation

You can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Governance.

For more information, see Performing Full Reconciliation.

1.7.3 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.

For more information, see Performing Limited Reconciliation.

1.7.4 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 want 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 if the bundle works faster when deployed on the same host as the native managed resource.

See Also:

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

1.7.5 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*.

1.7.6 Support for Cloning Applications and Creating Instance Applications

You can configure this connector for multiple installations of the target system by cloning applications or by creating instance applications.

When you clone an application, all the configurations of the base application are copied into the cloned application. When you create an instance application, it shares all configurations as the base application.

For more information about these configurations, see Cloning Applications and Creating an Instance Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.7.7 Secure Communication to the Target System

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

For more information, see Configuring SSL.

2

Creating an Application By Using the Connector

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

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

2.1 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

2.1.1 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:

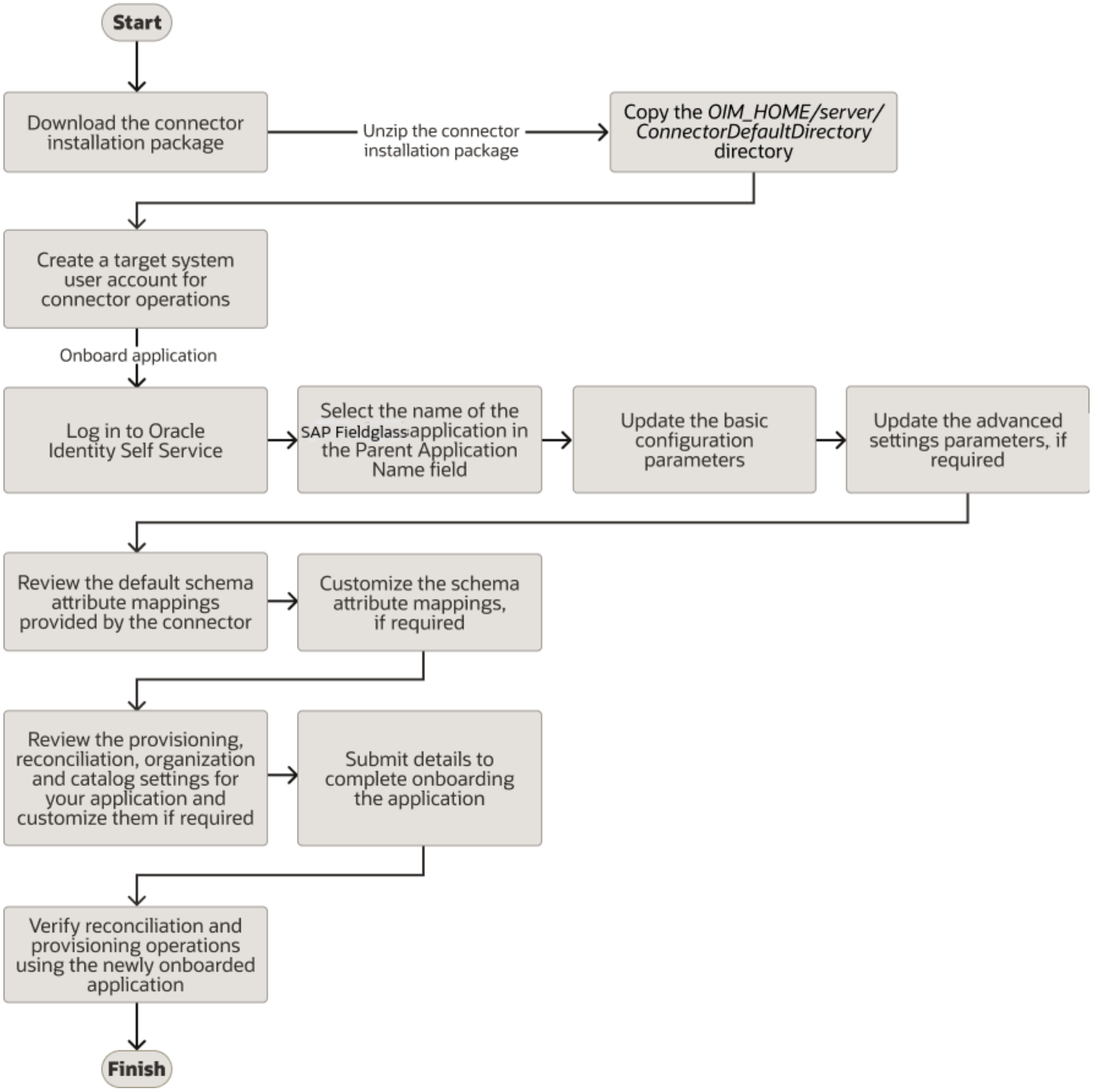
1. Navigate to the OTN website at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html .
2. Click **OTN License Agreement** and read the license agreement.
3. Select the **Accept License Agreement** option.
   You must accept the license agreement before you can download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

The following figure shows the 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 the *OIM_HOME/server/ConnectorDefaultDirectory* directory
Create a target system user account for connector operations
Onboard application
Log in to Oracle Identity Self Service
Select the name of the SAP Fieldglass application in the Parent Application Name field
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
Finish

2.3 Creating an Application by Using the SAP Fieldglass Connector

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

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

> **Note:**
>
> For detailed information regarding each step 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.

> **Note:**
>
> - Configuring the SAP Fieldglass 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 Fieldglass 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 attributes, predefined correlation rules, situations and responses, and reconciliation jobs.

- Basic Configuration Parameters
- Advanced Settings 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 SAP Fieldglass Connector.

> ✎ **Note:**
>
> Unless specified, do not modify entries in the below table.

Table 3-1 Basic Configuration Parameters for SAP Fieldglass Connector

Parameter	Mandatory?	Description
grantType	Yes	Enter the type of authentication used by your target system. For this connector, target uses OAuth2.0 client credentials. This is a mandatory attribute while creating an application. Do *not* modify the value of the parameter. **Default value**: client_credentials
host	Yes	Enter the host name of the machine hosting your target system. This is a mandatory attribute while creating an application. **Sample value**: partner.fgvms.com
authenticationServerUrl	Yes	Enter the URL of the authentication server that validates the client ID and client secret for your target system. **Sample value**: https://<host>/api/oauth2/v2.0/token?grant_type=client_credentials
clientId	Yes	Enter the Username received from SAP Fieldglass instance owner. **Sample Value**: JohnSmith
clientSecret	Yes	Enter the Password received from SAP Fieldglass instance owner. **Sample Value**: password

Table 3-1 (Cont.) Basic Configuration Parameters for SAP Fieldglass Connector

Parameter	Mandatory?	Description
baseURI	Yes	This is a mandatory attribute while creating an application. Do *not* modify the value of the parameter. **Default value**: /api/v1
acceptType	Yes	This is a mandatory attribute while creating an application. Do *not* modify the value of the parameter. **Default value**: application/scim+json
contentType	Yes	This entry holds the type of the body of the request .This is a mandatory attribute while creating an application. Do *not* modify the value of the parameter. **Default value**: application/scim+json
Connector Server Name	No	If you are using the SAP Fieldglass Connector together with a Java Connector Server, then enter the name of Connector Server IT resource.
proxyHost	No	Enter the name of the proxy host used to connect to an external target. **Sample value**: www.example.com
Proxy Password	No	Enter the password of the proxy user ID of the target system user account that Oracle Identity Governance uses to connect to the target system.
Proxy Port	No	Enter the proxy port number. **Sample value**: 1105
Proxy Username	No	Proxy user name of the target system user account that Oracle Identity Manager uses to connect to the target system.
sslEnabled	No	If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false. **Sample value:**true

3.2 Advanced Settings Parameters

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

> **Note:**
>
> - Unless specified, do not modify entries in the below table.
> - All parameters in the below table are mandatory.

Table 3-2 Advanced Settings Parameters

Parameter	Mandatory?	Description
Connector Name	Yes	This parameter holds the name of the connector class. **Default value:** org.identityconnectors.genericscim.GenericSCIMConnector
Bundle Name	Yes	This parameter holds the name of the connector bundle package. **Default value:** org.identityconnectors.genericscim
Bundle Version	Yes	This parameter hods the version of the connector bundle class. **Default value:** 12.3.0
defaultBatchSize	No	This entry holds the value of the number of records that can be retrieved from the target system in one go. **Default value:** 200
relURLs	No	This entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes. **Default value:** "__ACCOUNT__.TESTOP=/Users?count=1","__ACCOUNT__.DELETEOP=/Users","__ACCOUNT__.SEARCHOP=/Users","__GROUP__.SEARCHOP=/Groups"
checkAliveUri	No	This entry holds URL for test connection functionality **Default value:** /Users?count=1
schemaBuildingOption	No	This value indicates that there is no URL for schema definition. **Default value:** static
schemaCorePath	No	Enter the path of User Schema file. **Sample value:** <MW_HOME>/idm/server/ConnectorDefaultDirectory/SAPFieldGlass-12.2.1.3.0/schemafiles/User_Schema_Core.json
schemaEnterprisePath	No	Enter the path of Enterprise Schema file. **Sample value:** <MW_HOME>/idm/server/ConnectorDefaultDirectory/SAPFieldGlass-12.2.1.3.0/schemafiles/User_Schema_Enterprise.json
schemaGroupPath	No	Enter the path of Group Schema file. **Sample value:** <MW_HOME>/idm/server/ConnectorDefaultDirectory/SAPFieldGlass-12.2.1.3.0/schemafiles/Group_Schema_Core.json
extensionSchemaTags	No	This entry holds extension schema tags. **Default value:** "urn:ietf:params:scim:schemas:extension:Fieldglass:2.0:User","urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
customPayload	No	This entry holds the payloads for all operations that are not in the standard format. **Default value:** "__ACCOUNT__.groups.AddOp={\"Operations\":[{\"op\":\"add\",\"path\":\"members\",\"value\":[{\"value\":\"$(__ACCOUNT__.__UID__)$\"}]}],\"schemas\":[\"urn:ietf:params:scim:api:messages:2.0:PatchOp\"]}","__ACCOUNT__.groups.RemoveOp={\"Operations\":[{\"op\":\"remove\",\"path\":\"members\",\"value\":[{\"value\":\"$(__ACCOUNT__.__UID__)$\"}]}],\"schemas\":[\"urn:ietf:params:scim:api:messages:2.0:PatchOp\"]}"
nameAttributes	Yes	This is the __NAME__ attribute mapping of Oracle Identity Governance to the relevant attribute on target system. **Default value:** "Users=userName","Groups=displayName"
uidAttributes	Yes	This is the __UID__ attribute mapping of Oracle Identity Governance to the GUID attribute on target system. **Default value:** "Users=id","Groups=id"
attrToOClassMapping	No	This is Attribute names to Other Object Class mapping. **Default value:** "__ACCOUNT__.groups=Groups"
jsonResourcesTag	No	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload. **Default value:** Resources
scimVersion	Yes	This entry specifies the SCIM version. **Default value:** 1
statusAttributes	No	This entry lists the name of the target system attribute that holds the status of an account. **Default value:** "Users=active"
passwordAttributes	No	This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute of the connector in OIM. **Default value:** "Users=password"

3.3 Attribute Mappings

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

Following table lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP Fieldglass Connector 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.

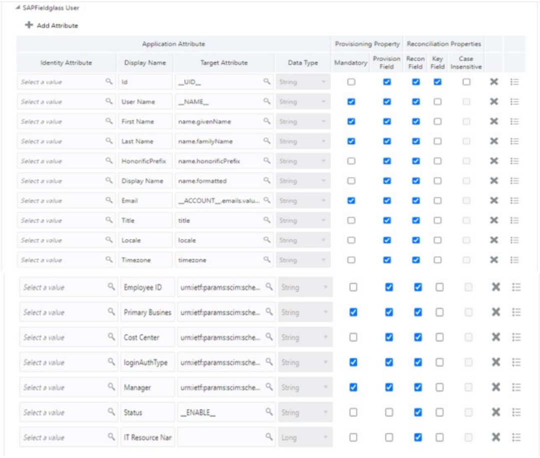
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attribute Mappings for SAP Fieldglass User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Id	__UID__	String	No	Yes	Yes	Yes	No
User Name	__NAME__	String	Yes	Yes	Yes	No	Not applicable
First Name	name.givenName	String	Yes	Yes	Yes	No	Not applicable
Last Name	name.familyName	String	Yes	Yes	Yes	No	Not applicable
HonorificPrefix	name.honorificPrefix	String	No	Yes	Yes	No	Not applicable
Display Name	name.formatted	String	No	Yes	Yes	No	Not applicable
Email	__ACCOUNT__.emails.value,type:Work	String	Yes	Yes	Yes	No	Not applicable
Title	title	String	No	Yes	Yes	No	Not applicable
Locale	locale	String	No	Yes	Yes	No	Not applicable
Timezone	timezone	String	No	Yes	Yes	No	Not applicable
Employee ID	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User;employeeNumber	String	No	Yes	Yes	No	Not applicable
Primary Business Unit	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User;division	String	Yes	Yes	Yes	No	Not applicable
Cost Center	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User;costCenter	String	No	Yes	Yes	No	Not applicable
loginAuthType	urn:ietf:params:scim:schemas:extension:Fieldglass:2.0:User;loginAuthType	String	Yes	Yes	Yes	No	Not applicable
Manager	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User;manager.value	String	Yes	Yes	Yes	No	Not applicable
Status	__ENABLE__	String	No	No	Yes	No	Not applicable
IT Resource Name		Long	No	No	Yes	No	Not applicable

Following figure shows the default User account attribute mappings.

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



SAPFieldglass User

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	Id	__UID__	String	□	☑	☑	☑	□	✕	☰
Select a value	User Name	__NAME__	String	☑	☑	☑	□	□	✕	☰
Select a value	First Name	name.givenName	String	☑	☑	☑	□	□	✕	☰
Select a value	Last Name	name.familyName	String	☑	☑	☑	□	□	✕	☰
Select a value	HonorificPrefix	name.honorificPrefix	String	□	☑	☑	□	□	✕	☰
Select a value	Display Name	name.formatted	String	□	☑	☑	□	□	✕	☰
Select a value	Email	__ACCOUNT__.emails.valu...	String	☑	☑	☑	□	□	✕	☰
Select a value	Title	title	String	□	☑	☑	□	□	✕	☰
Select a value	Locale	locale	String	□	☑	☑	□	□	✕	☰
Select a value	Timezone	timezone	String	□	☑	☑	□	□	✕	☰
Select a value	Employee ID	urn:ietf:params:scim:sche...	String	□	☑	☑	□	□	✕	☰
Select a value	Primary Busines	urn:ietf:params:scim:sche...	String	☑	☑	☑	□	□	✕	☰
Select a value	Cost Center	urn:ietf:params:scim:sche...	String	□	☑	☑	□	□	✕	☰
Select a value	loginAuthType	urn:ietf:params:scim:sche...	String	☑	☑	☑	□	□	✕	☰
Select a value	Manager	urn:ietf:params:scim:sche...	String	☑	☑	☑	□	□	✕	☰
Select a value	Status	__ENABLE__	String	□	□	☑	□	□	✕	☰
Select a value	IT Resource Nar		Long	□	□	☑	□	□	✕	☰

SAP Fieldglass Groups Entitlement

Following table lists the attribute mappings for groups between the process form fields in Oracle Identity Governance and SAP Fieldglass Connector 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.

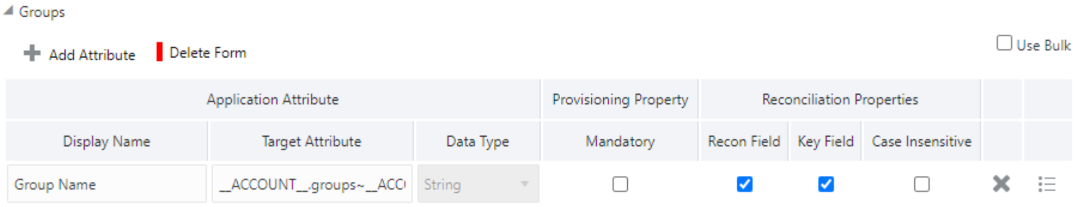
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4 Default Attribute Mappings for SAP Fieldglass Groups

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Group Name	__ACCOUNT__.groups~__ACCOUNT__.groups~value	String	No	Yes	Yes	No

Following figure shows the default Groups child attribute mapping.

Figure 3-2 Default Attribute Mappings for the Groups



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		
Group Name	__ACCOUNT__.groups~__ACC(	String	□	☑	☑	□	✕	☰

3.4 Correlation Rules

When you create a Target application, 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 Fieldglass 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.

Following table lists the default simple correlation rule for SAP Fieldglass Connector application. If required, you can edit the default correlation rule or add new rules. You can create simple correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rules in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5 Predefined Identity Correlation Rule for an SAP Fieldglass Connector

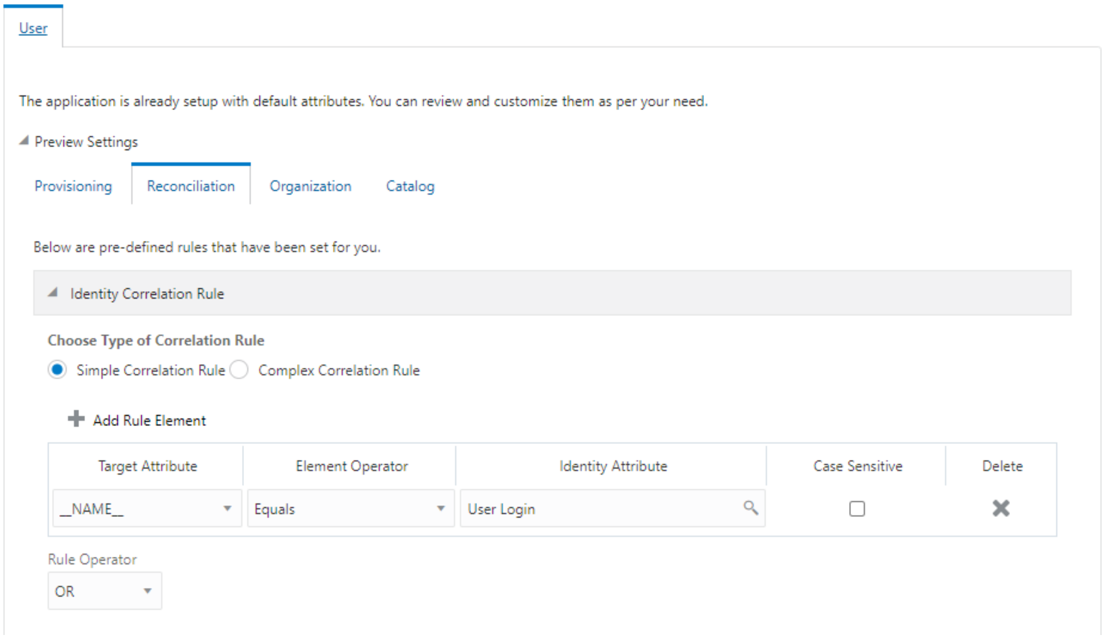
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

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.

Following figure shows the Simple Correlation Rule for SAP Fieldglass Target Application

Figure 3-3 Simple Correlation Rule for SAP Fieldglass Target Application



The application is already setup with default attributes. You can review and customize them as per your need.

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

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

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

Rule Operator: OR

Predefined Situations and Responses

The SAP Fieldglass 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.

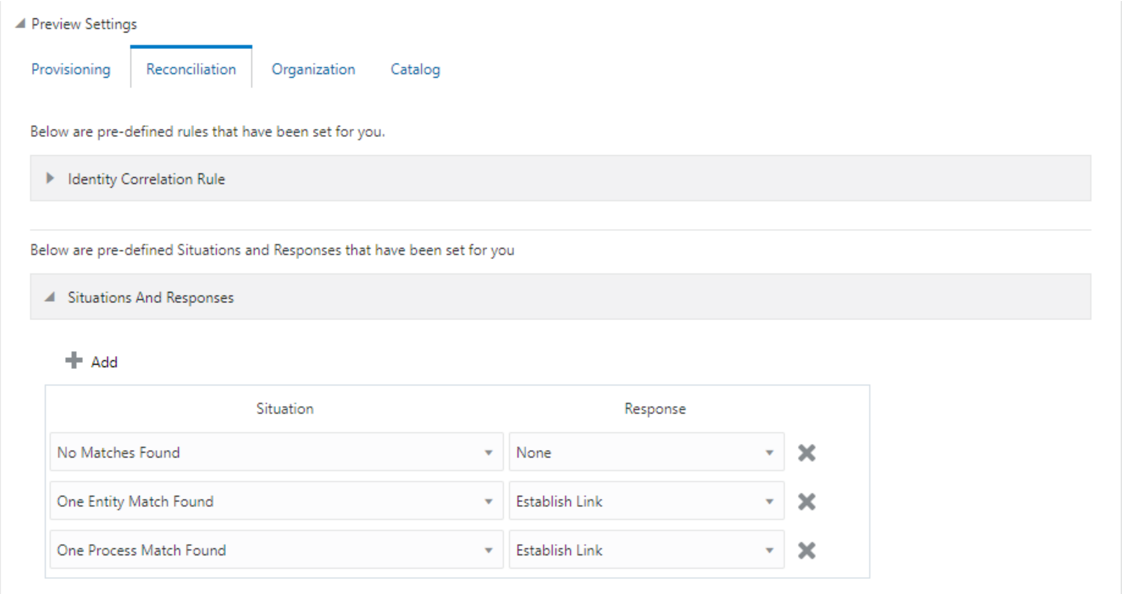
Following table lists the default situations and responses for the SAP Fieldglass Connector application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-6 Predefined Situations and Responses for SAP Fieldglass Connector

Situation	Response
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Following figure shows the situations and responses that the connector provides by default.

Figure 3-4 Predefined Situations and Responses for SAP Fieldglass Connector



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

Below are pre-defined Situations and Responses that have been set for you

Situation	Response
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

3.5 Reconciliation Jobs

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

User Reconciliation Jobs

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.

The following reconciliation jobs are available for reconciling user data:

- **SAP Fieldglass Full User Reconciliation**: Use this reconciliation job to reconcile user data from a target application.
- **SAP Fieldglass Limited User Reconciliation**: Use this reconciliation job to reconcile records from the target system based on a specified filter criterion.

Following table describes the parameters of the SAP Fieldglass Full User Reconciliation job.

Table 3-7 Parameters of the SAP Fieldglass Full User Reconciliation Job

Parameter	Description
Application name	Name of the AOB application with which the reconciliation job is associated. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* change the default value.
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. Filter suffix: **Sample value:** equalTo('__NAME__',John') For more information about creating filters, see Performing Limited Reconciliation.
Object Type	This parameter holds the name of the object type for the reconciliation run. **Default value**: User Do *not* change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Do *not* modify the value of this parameter.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- SAPFieldglass Manager Lookup Reconciliation
- SAPFieldglass Group Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-8 Parameters of the Reconciliation Jobs for Entitlements

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

Table 3-8 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Object Type	Enter the type of object whose values must be synchronized. Depending on the reconciliation job that you are using, the default values are as follows: • For SAPFieldglass Manager Lookup Reconciliation: User • For SAPFieldglass Group Lookup Reconciliation: __GROUP__ **Note:** Do not change the value of this attribute.
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the reconciliation job that you are using, the default values are as follows: • For SAPFieldglass Manager Lookup Reconciliation: __UID__ • For SAPFieldglass Group Lookup Reconciliation: __UID__ **Note:** Do not change the value of this attribute.
Decode Attribute	Name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the reconciliation job that you are using, the default values are as follows: • For SAPFieldglass Manager Lookup Reconciliation: __NAME__ • For SAPFieldglass Group Lookup Reconciliation: __NAME__ **Note:** Do not change the value of this attribute.

4

Performing Postconfiguration Tasks for the 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
- Managing Logging for the Connector
- Configuring the IT Resource for the Connector Server
- Localizing Field Labels in UI Forms
- Configuring SSL

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.

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

- Creating and Activating a Sandbox
- Creating a New UI Form
- Publishing a Sandbox
- 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 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

You can populate Entitlement schema from child process form table, and harvest roles, application instances, and entitlements into catalog. You can also load catalog metadata.

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Reconciliation Jobs.

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:

Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for a description of the Entitlement List and Catalog Synchronization Job scheduled jobs.

4.3 Managing Logging for the Connector

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

The following topics provide detailed information about logging:

- Understanding Logging on the Connector Server
- Enabling Logging for the Connector Server
- Understanding Log Levels
- Enabling Logging

4.3.1 Understanding Logging on the Connector Server

When you enable logging, the connector server stores in a log file information about events that occur during the course of provisioning and reconciliation operations for different statuses. By default, the connector server logs are set at INFO level and you can change this level to any one of these.

- Error

This level enables logging of information about errors that might allow connector server 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 operation.

- FINE, FINER, FINEST

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

4.3.2 Enabling Logging for the Connector Server

Edit the logging properties file located in the CONNECTOR_SERVER_HOME/Conf directory to enable logging.

1. Open the logging.properties file in a text editor.
2. Navigate to the *CONNECTOR_SERVER_HOME*/Conf directory.
3. Edit the following entry by replacing INFO with the required level of logging:.level=INFO

example:

.level=FINEST

ORG.IDENTITYCONNECTORS.GENERICSCIM.level=FINEST

4. Save and close the file.
5. Restart the connector server.

4.3.3 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 following table.

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
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

4.3.4 Enabling Logging

Perform this procedure to enable logging in Oracle WebLogic Server.

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='SAPFieldGlass-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.GENERICSCIM" level="[LOG_LEVEL]"
useParentHandlers="false"> <handler name="SAPFieldGlass-handler"/>
<handler name="console-handler"/> </logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 4-1 lists the supported message type and level combinations. Similarly, replace [FILE_NAME] with the full path and name of the log file in which you want log messages to be recorded. The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]:**

```
<log_handler name= ‘SAPFieldGlass-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\server
s\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.GENERICSCIM"
level="NOTIFICATION:1" useParentHandlers="false"> <handler
name="SAPFieldGlass-handler"/> <handler name="console-handler"/> </
logger>
```

2. 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.
3. Save and close the file.
4. Set the following environment variable to redirect the server logs to a file:
   a. For Microsoft Windows: set WLS_REDIRECT_LOG= ***FILENAME***

b. 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.

5. Restart the application server.

4.4 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 below table. 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 4-2 Parameters of the IT Resource for the SAP Fieldglass Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. **Sample value**: HostName
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. **Sample value:** 8763
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Governance times out. If the value is zero or if no value is specified, the timeout is unlimited. **Sample value:** 0 (recommended value)
UseSSL	Enter true to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter false. **Default value:** false **Note**: It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see Configuring the Java Connector Server with SSL for OIG in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.5 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. Resource bundles are available in the connector installation media.

To localize field labels that is added to the UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**

4. On the MDS Configuration page, click **Export** and save the archive (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer**.**
5. Extract the contents of the archive, and open the following file in a text editor:

   ```
   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
   ```

   > **Note:**
   >
   > You will not be able to view the BizEditorBundle.xlf file 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 Fieldglass Application instance. The original code is:

      ```
       <trans-unit Id=”$
      {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBund
      le']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO
      .UD_SAPFieldGlassAPP_DISPLAY_NAME__c_description']}"> <source>Display
      Name</source> <target/> </trans-unit> <trans-unit
      id="sessiondef.oracle.iam.ui.runtime.form.model.SAPField
      GlassApp.entity.SAPFieldGlassApp.UD_SAPFieldGlassAPP_DISPLAY_NAME__c_LAB
      EL"> <source>Display Name</source> <target/> </trans-unit>
      ```

   d. Open the resource file from the connector package, for example SAP Field Glass_ja.properties, and get the value of the attribute from the file, for example,

      ```
      global.udf.UD_SAPFieldGlass_USR_DISPLAY_NAME =\u8868\u793A\u540D
      ```

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBund
le']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO
.UD_ SAPFieldGlassAPP_DISPLAY_NAME__c_description']}">
<source>Display Name</source> <target>\u8868\u793A\u540D </target>
</trans-unit>
<trans-
unitid="sessiondef.oracle.iam.ui.runtime.form.model.SAPFieldGlassApp.ent
ity.SAPFieldGlassAPPEO.UD_SAPFieldGlassAPP_DISPLAY_NAME__c_LABEL">
<source>Display Name</source> <target>\u8868\u793A\u540D</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.

> **Note:**
>
> 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.

4.6 Configuring SSL

Configure SSL to secure data communication between Oracle Identity Governance and the SAP Fieldglass target system.

> **Note:**
>
> If you are using this connector along with a Connector Server, then there is no need to configure SSL. You can skip this section.

To configure SSL:

1. Obtain the SSL public key certificate of SAP Fieldglass.
2. Copy the public key certificate of SAP Fieldglass to the computer hosting Oracle Identity Governance.
3. Run the following keytool command to import the public key certificate into the identity key store in Oracle Identity Governance:
   ```
   keytool -import -alias ALIAS -trustcacerts -file CERT_FILE_NAME -keystore
   KEYSTORE_NAME -storepass PASSWORD
   ```

In this command:

- *ALIAS* is the public key certificate alias.
- *CERT_FILE_NAME* is the full path and name of the certificate store (the default is cacerts).
- *KEYSTORE_NAME* is the name of the keystore.
- *PASSWORD* is the password of the keystore.

The following are sample values for this command:

```
keytool -import -keystore <JAVA_HOME>/jre/lib/security/cacerts -file
<Cert_Location>/SAPFieldGlass.crt -storepass changeit -alias FieldGlass _1
```

```
keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file
<Cert_Location>/SAPFieldGlass.crt -storepass DemoTrustKeyStorePassPhrase -alias
FieldGlass_2
```

Note:

- Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool arguments.
- Ensure that the system date for Oracle Identity Governance is in sync with the validity date of the SSL certificate to avoid any errors during SSL communication.

5 Using the Connector

You can use the connector for performing reconciliation and provisioning operations after configuring your application to meet your requirements.

- Configuring Reconciliation
- Configuring Reconciliation Jobs
- Configuring Provisioning

5.1 Configuring Reconciliation

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

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 suffix parameters and run job for reconciling users.

5.1.2 Performing Limited Reconciliation

Limited or filtered reconciliation is the process of limiting the number of records being reconciled based on a set filter criterion.

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

This connector provides a Filter Suffix attribute (a scheduled task attribute) that allows you to use any of the attributes of the target system to filter target system records. You specify a value for the Filter Suffix attribute while configuring the user reconciliation scheduled job.

Due to the limited functionality support of SAP Fieldglass target system with respect to filtering query for string data type fields, the connector only supports *equalTo* filter. Below is the example for the filters:

Filter Suffix Value: equalTo('__NAME__','<User Name>')

Example: equalTo('__NAME__','John')

In this example, all records whose User Name is 'John' are reconciled.

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**.
   Note:

   If you are using OIG 12cPS4 with 2022OCTBP or later version, log in to Identity Console, click **Manage**, under **System Configuration**, 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:
   a. **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.

   b. **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 Fieldglass connector.

This section discusses the following topics related to configuring reconciliation:

5.3.1 Guidelines on Performing Provisioning Operations

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

Provisioning attributes required to create user account.

To create User provisioning operation, following values are required:

- User name: The user's Username.
- First Name: The user’s First name.
- Last Name: The user’s Last name.
- Email: Email ID of the user.
- Primary Business Unit: Domain to which user belongs to.
- loginaAuthType: Type of authentication that the user uses to login.
- Manager: The user’s manager.

Note: Only ‘password’ value is supported for loginAuthType.

Attributes required to be updated in the parent form.

- User name: The user's Username
- First Name: The user’s First name.
- Last Name: The user’s Lastname.
- HonorificPrefix: Prefix used to address the user.s
- Email: Email ID of the user.
- Display name: The user's Display name.
- Title: Title of the user.
- Locale: The user’s language.
- Timezone: The user’s time zone.
- EmployeeID: The user’s Employee ID.
- Primary Business Unit: Domain to which the user belongs to.
- Cost Center: Cost Center to which the user belongs.
- Manager: The user’s manager.

5.3.2 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance, perform the following steps:

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, 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**.

6 Extending the Functionality of the Connector

You can extend the functionality of the connector to address your specific business requirements.

This section discusses the following topics:

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

6.1 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 Managing Application Onboarding of Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

6.2 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 operation. 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*.

6.3 Configuring the Connector for Multiple Installations of the Target System

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

The following example illustrates this requirement:

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

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

7

Frequently Asked Questions for the SAP Fieldglass Connector

Question

Why am I not able to assign "Worker" Group to the User?

Answer

Worker is a restricted Role in SAP Fieldglass Target. It cannot be assigned from SAP Fieldglass target as well as from OIM even though it is Group Lookup value.

8

Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the SAP Fieldglass connector.

Table 8-1 Files and Directories in the SAP Fieldglass Connector Installation Package

File in the Installation Package	Description
/bundle/ org.identityconnectors.genericscim-12.3.0.jar	This JAR is the ICF connector bundle.
configuration/SAPFieldGlass-CI.xml	This XML file contains configuration information.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to Oracle Identity database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
JSON files in the Schemafiles directory	These directory contains the JSON files for User schema, Enterprise schema and Group schema
xml/SAPFieldGlass-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/SAPFieldGlass-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User objects such as Groups. Also, it contains definitions of Lookups and schedule tasks.

Glossary

Index