Oracle® Identity Governance

Configuring the SAP S/4 HANA Cloud Application

Release 12.2.1.3.0
F50308-02
January 2023

ORACLE

Oracle Identity Governance Configuring the SAP S/4 HANA Cloud Application, Release 12.2.1.3.0

F50308-02

Primary Author: Oracle Corporation

Contents

List of Figures

List of Tables

Preface

This guide describes the connector that is used to onboard the DocuSign application 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 12.2.1.4.0, visit the following Oracle Help Center page:

Oracle Identity Governance 12.2.1.4.0

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

Conventions

The following text conventions are used in this document:

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

What’s New in This Guide?

Resolved Issues in Release 12.2.1.3.0A

The following table lists the issues resolved in release 12.2.1.3.0A:

Bug Number	Issue	Resolution
34612487	ADD BUSINESS ROLES TO OIG USING LOOKUP RECON	This issue has been resolved.

1

About the SAP S/4 HANA Connector

The SAP S/4HANA connector integrates Oracle Identity Governance with the SAP S/4HANA target system.

The following topics provide a high-level overview of the SAP S/4HANA connector:

1.1 Introduction to the 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 S/4HANA Cloud connector lets you create and onboard SAP S/4HANA Cloud applications 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.

> **Note:**
>
> In this Guide, the term SAP S/4HANA Cloud is also referred to as the **target system**.

1.2 Certified Components

These are the software components and their versions required for installing and using the SAP S/4HANA Cloud connector.

Table 1-1 Certified Components

Component	Requirement for AOB Application
Oracle Identity Governance	You can use any one of the following releases: • Oracle Identity Governance 12*c* PS3 (12.2.1.3.0) • Oracle Identity Governance 12*c* PS4 (12.2.1.4.0)
Oracle Identity Governance JDK	JDK 1.8 and later
Target systems	SAP S/4HANA CLOUD 2208
Connector Server	11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 and later

1.3 Usage Recommendation

If you are using Oracle Identity Governance 12*c* (12.2.1.3.0) or a later version, 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.

New customers are recommended to use the S4HANA-12.2.1.3.0A version as the Roles Lookup Reconciliation feature is implemented.

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

- SAP S/4HANA On-Premise: The traditional upgraded release of SAP ERP 6.0, to which the customers are mostly migrating, has SAP GUI-based access to the system with access to Fiori launchpad as well. It is a fully customer-controlled environment with respect to administration/support/maintenance. **Recommendation** - use Oracle Identity Governance - SAP User Management Connector. For more information about it, see About the SAP User Management Connector.
- SAP S/4HANA Cloud Private Edition: Everything is similar to SAP S/4HANA On-Premise, but the entire system control/administration/maintenance is with SAP. It is offered under the “Rise with SAP” program only as a Service with SAP GUI access given to the end/business users, who have access to Fiori Launchpad as well. **Recommendation** - use Oracle Identity Governance - SAP User

Management Connector. For more information about it, see About the SAP User Management Connector.

- SAP S/4HANA Cloud Public Edition/Essential Edition: Core SaaS offering for S/4HANA, where the instance is provisioned, which has browser-based access only to the end/business users; No SAP GUI access is valid/exposed for this cloud instance. **Recommendation** - use Oracle Identity Governance - SAP S/4 HANA Cloud Connector. For more information about it, see Introduction to the Connector.

1.4 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

1.5 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	Yes
Disable user	Yes
Delete user	Yes
Business Role Management	
Add and Remove Roles to Users	Yes

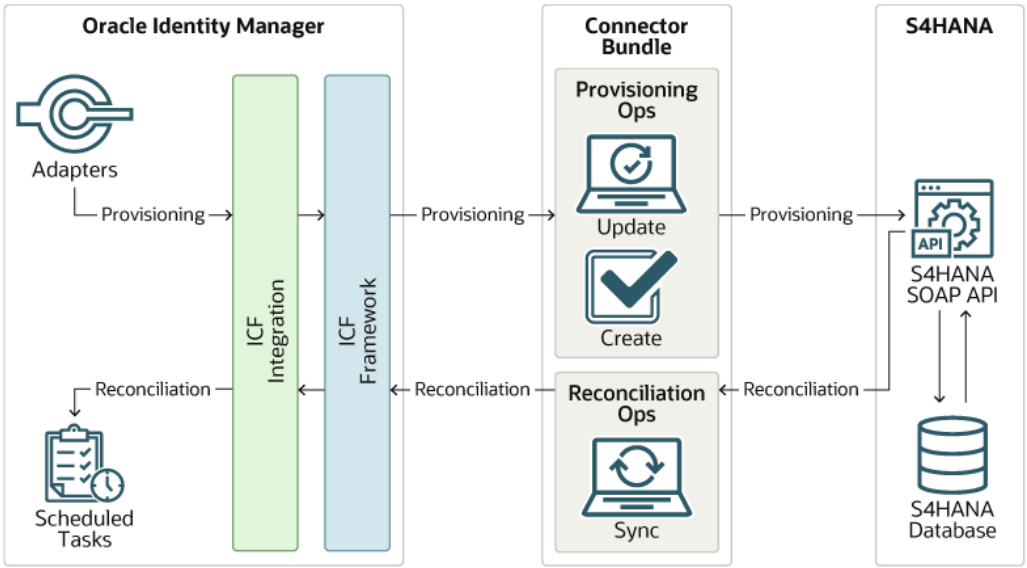
1.6 Connector Architecture

The SAP S/4HANA Cloud connector is implemented by using the Identity Connector Framework (ICF).

The ICF is a component that is required in order to use Identity Connector. ICF provides basic reconciliation and provisioning operations that are common to all Oracle Identity Governance connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as, buffering, time outs, and filtering. ICF is distributed together with Oracle Identity Governance. Therefore, you do not need to configure or modify ICF.

Figure 1-1 shows the architecture of the SAP S/4HANA Cloud connector.

Figure 1-1 Connector Architecture



The connector is configured to run in the Account management mode. 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 inturn invokes create operation on the SAP S/4HANA Cloud Identity Connector Bundle and then the bundle calls the S/4HANA Cloud Webservice for provisioning operations. The webservice 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 inturn invokes a search operation on the SAP S/4HANA Cloud Identity Connector Bundle and then the bundle calls the S/4HANA Cloud Webservice for the reconciliation operation. The Webservice 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 S/4HANA Cloud resources that are already provisioned to OIM Users. If a match is found, then the update made to the SAP S/4HANA Cloud record from the target system is copied to the SAP S/4HANA Cloud resource in Oracle Identity Governance. If no match is found, then the UserName 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 S/4HANA Cloud resource to the OIM User.

See Also:

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

1.7 Supported Connector Features Matrix

Provides the list of features supported by the AOB application.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application
Full reconciliation	Yes
Limited (Filtered) Reconciliation	Yes
Provide secure communication to the target system through SSL	Yes
Use connector server	Yes
Clone applications or create new application instances	Yes

Table 1-3 (Cont.) Supported Connector Features Matrix

Feature	AOB Application
Transformation and validation of account data	Yes
Support for pagination	Yes
Test connection	Yes

1.8 Features of the Connector

The features of the connector include full and incremental reconciliation, limited reconciliation, transformation and validation of account data and so on.

- Support for Full Reconciliation
- Support for Limited (Filtered) Reconciliation
- Support for the Connector Server
- Transformation and Validation of Account Data
- Support for Cloning Applications and Creating Instance Applications
- Secure Communication to the Target System
- Configuring Action Scripts
- Support for Enabling and Disabling Accounts

1.8.1 Support for Full Reconciliation

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

You can switch to full reconciliation at any time after you deploy the connector. For more information on performing full reconciliation runs, see Performing Full Reconciliation.

1.8.2 Support for Limited (Filtered) Reconciliation

You can reconcile records from the target system based on a specified filter criterion.

You can set a reconciliation filter as the value of the Filter Query attribute of the user reconciliation scheduled job. This filter specifies the subset of newly added and modified target system records that must be reconciled. The Filter Query attribute helps you to assign filters to the web services based on which you will get a filtered response from the target system.

For more information on performing limited reconciliation, see Performing Limited Reconciliation.

1.8.3 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*.

1.8.4 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 Transformation and Validation of Account Data in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.8.5 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 Instance Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.8.6 Secure Communication to the Target System

To provide secure communication to the target system, SSL is required. You can configure SSL between Oracle Identity Governance and the Connector Server and between the Connector Server and the target system.

If you do not configure SSL, passwords can be transmitted over the network in clear text. For example, this problem can occur when you are creating a user or modifying a user's password.

For more information, see Configuring SSL.

1.8.7 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*.

1.8.8 Support for Enabling and Disabling Accounts

The attributes **Valid From** and **Valid Through** are the user attributes on the target system. For a particular user in SAP S/4HANA Cloud, if the **Valid Through** date is less than the current date, then the account is in the Disabled state, else , 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.

2

Creating an Application by Using the Connector

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

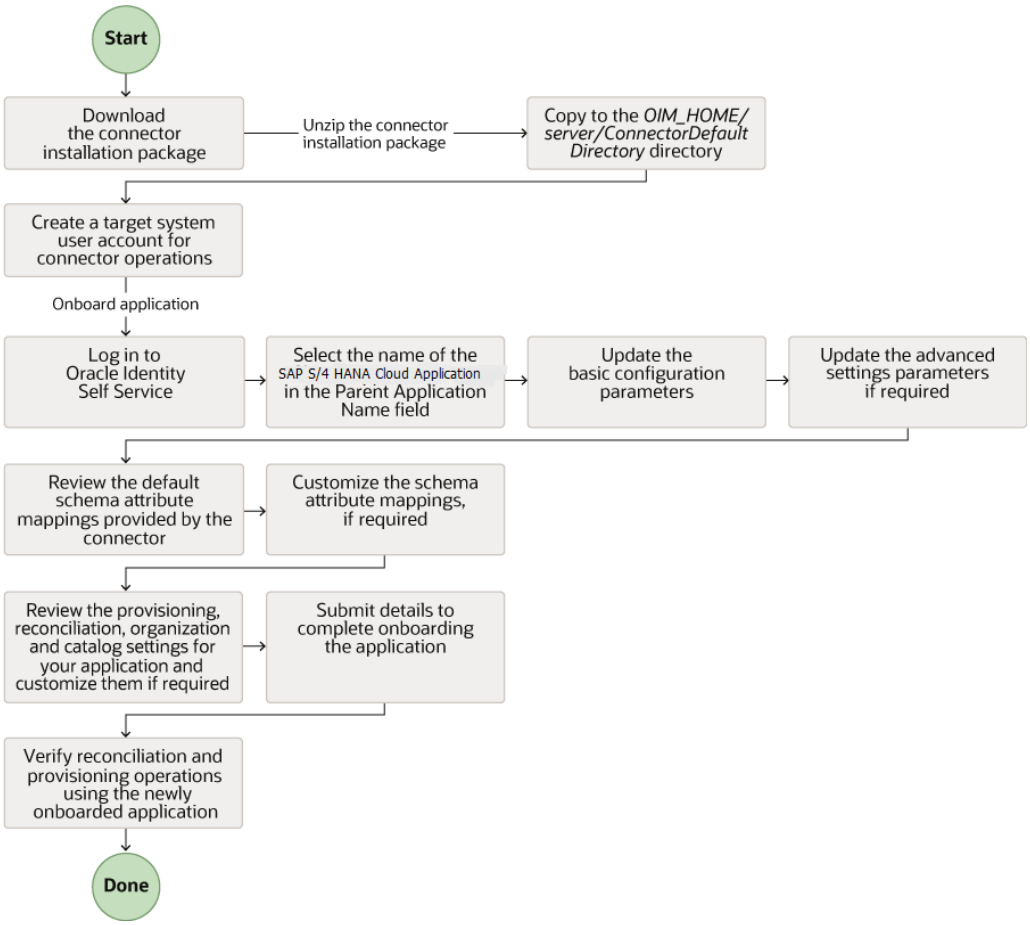
Topics

2.1 Process Flow for Creating an Application By Using the Connector

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

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

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



2.2 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.

2.3 Copying Third-Party Jar Libraries

You can either use third-party jars from the `S4HANA-12.2.1.3.0 /lib` folder shipped with the connector package or download any latest, stable, and secure version. Please follow the below procedure to include third-party jars:

Copy the third-party library jars for the S4HANA Apps connector to the computer hosting Oracle Identity Governance.

1. Create a directory named S4HANA-12.2.1.3.0 for the S4HANA Apps connector in the following directory:

   OIM_HOME/server/ConnectorDefaultDirectory/targetsystems-lib/

   From the installation media copy SAP S/4HANA Cloud third-party libraries <S4HANA-12.2.1.3.0\lib> to the above created new directory.

   The files in this directory are not shared with any other connectors, which avoids version conflicts among shared libraries.

2. If you are using Connector Server, from the installation media copy SAP S/4HANA Cloud third-party libraries `<S4HANA-12.2.1.3.0\lib>` to the `CONNECTOR_SERVER_HOME/lib` directory

Table 2-1 Third-party jars

Jar Name	Type
commons-codec-1.15.jar	These files are 3rd and 4th party dependent JARs for S4HANA Target.
commons-logging-1.2-1b97e70.jar	
httpclient5-5.1.3.jar	
httpcore5-5.1.3.jar	
jackson-annotations-2.13.3.jar	
jackson-core-2.13.3.jar	
jackson-databind-2.13.3.jar	
slf4j-api-2.0.0.jar	

2.4 Creating an Application By Using the SAP S/4HANA Cloud 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.

> **Note:**
>
> For detailed information on the steps in this procedure, see Creating a Target Application 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 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

2.5 Creating a Target System User Account for the SAP S/4HANA Cloud Target

The following topics describe the procedures to create a target system user account for the SAP S/4HANA Cloud target:

- Create a Communication User

- Create a Communication System
- Create a Communication Arrangement

2.5.1 Create a Communication User

1. Log in to **SAP S/4HANA Cloud** application with administrator credentials.
2. Under **Communication Management**, click **Maintain Communication Users**.
3. Click **New** to create a new communication user.
   The **Create Communication User** page appears.
4. Enter User Name, Description, and password.
5. Click **Propose Password** to get a system-generated password.

> **Note:**
>
> Keep a note of the User Name and password for your communication user.

6. Click **Create**.

2.5.2 Create a Communication System

Perform the following steps to create a communication system and assign a communication user to the communication system.

1. Log in to the **SAP S/4HANA Cloud** application with administrator credentials.
2. Under **Communication Management**, click **Communication Systems**.
3. Click **New** to create a new communication system.
4. Enter System ID and System Name, then click **Create**.
5. Under **Technical Data**, enter the Host Name of your SAP S/4HANA Cloud tenant in the following format: `<tenant ID>.s4hana.ondemand.com`
6. Click **User for Inbound Communication** tab, then click the add (+) icon.
7. Assign the communication user you create and select the authentication method as **User ID** and **Password**.
8. Click **Save**.

2.5.3 Create a Communication Arrangement

1. Log in to **SAP S/4HANA Cloud** application with administrator credentials.
2. Under **Communication Management**, click **Communication Arrangements**.
3. Click **New** to create a new communication arrangement.
4. Select communication scenario SAP_COM_0193, enter an arrangement name, and click **Create**.
5. Select **Communication Arrangement** in the list.
   The inbound communication user is automatically assigned.

6. Under **Inbound Services**, the endpoint URLs to call the SOAP service is found in the following format:
   - https://<S4HANA tenant ID>-api.s4hana.ondemand.com/sap/bc/srt/scs_ext/sap/managebusinessuserin
   - https://<S4HANA tenant ID>-api.s4hana.ondemand.com/sap/bc/srt/scs_ext/sap/querybusinessuserin
   - https://<S4HANA tenant ID>-api.s4hana.ondemand.com/sap/bc/srt/scs_ext/sap/querybusinessusermetadatain
7. Click **Save**.
   WSDLs can be downloaded from this arrangement once saved.

The same SAP S/4HANA user can be used as a communication user in Oracle Identity Governance to perform all the connector operations.

2.6 Create System Account for SAP Identity Authentication Service (IAS)

This account is used to connect to SAP IAS to verify user existence. The User ID must exist here to provision it to S4/HANA Cloud and manage users credential. For more information refer to, **Add System as Administrator** under **SAP Cloud Identity Services - Identity Authentication** in SAP Help Portal.

To add a person as a new tenant administrator, proceed as follows:

1. Access the tenant's administration console for Identity Authentication by using the console's URL.
2. Choose the **Administrators** tile.

> **Note:**
>
> The URL has the following pattern:
> `https://<tenant ID>.accounts.ondemand.com/admin`
>
> *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID. For more information about your tenants refer to **Viewing Assigned Tenants and Administrators** under **SAP Cloud Identity Services - Identity Authentication** in SAP Help Portal.
>
> If you have a configured custom domain, the URL pattern is: `<your custom domain>/admin`.

This operation opens a list of all administrators in alphabetical order.

> **Note:**
>
> The list also includes the SAP BTP system, which by default has authorizations to set up the trust with Identity Authentication.

3. Press the **+Add** button on the left-hand panel to add a new administrator to the list.
4. Choose **Add User**.
5. Make the appropriate entries in the Email, First Name, and Last Name fields for the user you want to add as an administrator.
   The E-mail must be unique for the tenant.

   The First Name, and Last Name fields are pre-filled automatically for users who already exist in system.

> **Note:**
>
> Once the administrator is created, the First Name, Last Name, and Email fields are not editable from the administrator section. If you want to change the information you must go to the User Management section. For more information refer to **List and Edit User Details** under **SAP Cloud Identity Services - Identity Authentication** in SAP Help Portal.

6. Assign the required administrator roles for the user. To be a tenant administrator, a user must be assigned at least one of the following roles.

Table 2-2 Administrator Roles

Authorization	Description
Manage Applications	This role gives the tenant administrator permission to configure the applications via the administration console.
Manage Corporate Identity Providers	This role gives the tenant administrator permission to configure the identity providers via the administration console.
Manage Users	This role gives the tenant administrator permission to manage, import, and export users via the administration console.
Read Users	This role gives the tenant administrator permission to retrieve user data and import users via the administration console and the SCIM REST API of Identity Authentication.
Manage Groups	This role gives the tenant administrator permission to create, edit, and delete user groups via the administration console.
Manage Tenant Configuration	This role gives the tenant administrator permission to manage tenant configuration and authorization assignment to users. Tenant administrators with that role can add additional roles to themselves or to other administrators.

> **Note:**
>
> By default, all administrator roles are assigned.

7. Configure the method for authentication when the system is used.
   - Set Password

> **Note:**
>
> You must set password for basic authentication when Identity Authentication is used. The client ID is in the universally unique identifier (UUID) format and will be automatically generated. For example, 1ab7c243-5de5-4530-8g14-1234h26373ab. The password must meet the following conditions:
>
> – Minimum length of 8 characters.
>
> – Characters from at least three of the following groups:
>
> * Lower-case Latin characters (a-z)
> * Upper-case Latin characters (A-Z)
> * Base 10 digits (0-9)
> * Non-alphabetic characters (!@#$...)
>
> – Must not include space and the %, +, \, !, #, $, &, ‘, (,), *, ,, ;, <, >, ^, `, {, |, and } characters.
>
> – The password is locked for 60 min after 5 failed attempts with wrong value.

8. Save your changes.

2.7 Application Post Configuration

Post the configuration of application, it is a must to add business roles to OIG.

> **Note:**
>
> This step is not appliable if you are using S4HANA-12.2.1.3.0A or a later version.

To add business role in target export, follow the below steps:

1. Login to S/4 HANA cloud tenant.
2. Search for **Maintain Business Roles**.
3. Select **Business Role ID**.
4. Click **Download Business Roles**.

In OIG, add data for `Lookup.S4HANA.Roles`. Do the following:

1. Login to OIG Identity System Administration console as sysadmin.
2. Navigate to **System Configuration>Lookups**
3. Search for **Lookup.S4HANA.Roles**.
4. Click **Actions**.
5. Select **Edit**.
6. Add entries as shown in the following example.

Table 2-3 Example Data Table

Code	Decode/Meaning
5~BR_GRANT_RESPONSIBLE	S4HANA1~Grant Responsible
5~BR_GRANT_SPECIALIST	S4HANA1~Grant Specialist

Note:

- The code `<IT Resource Key>~<Business Role ID>`Decode/Meaning: `<Application Name>~<Business Role Description>`.
- IT Resource Key is provided using `svr table`,and `svr_key column data`.
- The above steps are applicable for all S4HANA OIG Applications. You must also run the entitlement list for scheduled job.

3
Configuring the Connector

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

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to an SAP S/4HANA application.

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

Table 3-1 Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
username	Yes	Enter the user name of the target system that you create for performing connector operations. **Sample value**: `johndoe`
password	Yes	Enter the password of your API user name. **Sample Value**:`qWErty12@3`

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description

baseUrl	Yes	Enter the base URL of S4/HANA Webservice/ API.
		Sample Value
		`http(s)://<tenant>.s4hana.ondemand.com/sap`
		Note:
		The below sample value is applicable if you are using S4HANA-12.2.1.3.0A or a later version.
		Sample Value
		`http(s)://s4hana.ondemand.com/sap`

Connector Server Name	No	By default, this field is blank. If you are using this connector with the Java Connector Server, then provide the name of Connector Server IT Resource here.

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
clientID	Yes	Enter SAP IAS' service account ClientID. **Sample Value** `7de7371f-029c-42aa-b142-2cbf`
clientSecret	Yes	Enter the ClientID for SAP IAS password. **Sample Value**: `qWErty12@3`
host	Yes	Enter the hostname of the target system. **Default Value:**`https://<S4/HANA Host or DNS>`

Note:

This attribute is applicable from S4HANA-12.2.1.3.0A or a later version.

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
IASUserUrl	Yes	Enter SAP IAS User search URL. **Sample Value:**`https://<SAP IAS Host IP or DNS>/service/scim/Users?filter=userName eq "%s"`

Note:

The `%s` should be in quotes.

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
lookupUrl	Yes	This entry specifies the S4/HANA Cloud Webservice endpoint to list the roles. **Default Value:**`/sap/opu/odata/sap/APS_IAM_SIAG_BROLE_SRV/Aps_Iam_Siag_Br_Dll` **Note:** This attribute is applicable from S4HANA-12.2.1.3.0A or a later version.
skipIASUserVerification	Yes	Set it to true if you don't want to verify user existence in SAP IAS else false.
proxyHost	No	Enter the proxy host or IP if you are using proxy server to access internet. **Sample value**`www.example.com`
proxyPassword	No	Enter the proxy password if you are using proxy server to access internet.
proxyPort	No	Enter the proxy port. **Sample Value**:`8080`

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
proxyUsername	No	If you are using proxy server to access internet.

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	Description
Bundle Name	This entry holds the name of the connector bundle. **Default value**: `org.identityconnectors.s4hana`
Bundle Version	This entry holds the version of the connector bundle. **Default value**: `12.3.0`
Connector Name	This entry holds the name of the connector class. **Default value**: `org.identityconnectors.s4hana.S4HANAConnector`
createUrl	This entry specifies the S4/HANA Cloud Webservice endpoint to create user. **Default value**: `Null`
updateUrl	This entry specifies the S4/HANA Cloud Webservice endpoint to update user **Default value**: `/managebusinessuserin`
reconUrl	This entry specifies the S4/HANA Cloud Webservice endpoint to list user(s) **Default value**: `/querybusinessuserin`

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Description
targetDateFormat	This entry specifies the date format supported by target for field like Validity period i.e. Start and End Date **Default value**: `yyyy-MM-dd`
updateNotSupportedForAttribute	This entry specifies comma separated list of target attributes that can't be updated as target doesn't support it **Default value**: `FirstName,LastName,PersonFullName,MiddleName,EmailAddress,GenderCode,CompanyCode,PersonWorkAgreementType,Username,PersonExternalID`

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.

Default Attributes for SAP S/4HANA Cloud Target Application

Table 3-3 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP S/4HANA Cloud target application 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 Application Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

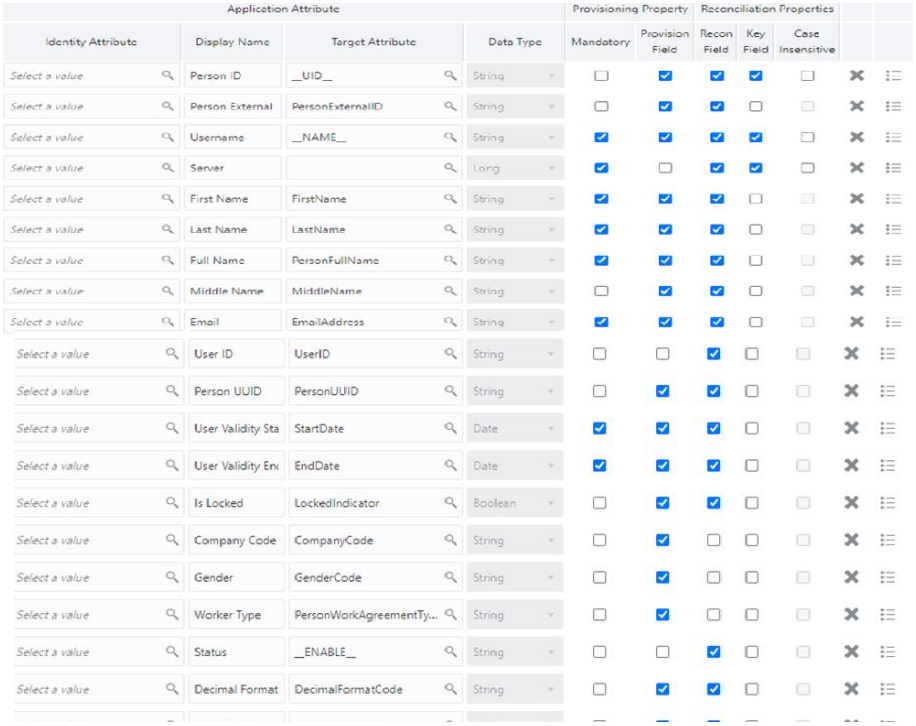
Table 3-3 Default Attributes for SAP S/4HANA Cloud Target Application

Display Name	Target Attribute	Data Type	Length	Mandatory Provisioning Property?	Provision Field?	Recon Field	Key Field?	Case Insensitive?
Person ID	__UID__	String	10	No	Yes	Yes	Yes	Not applicable
Person External ID	PersonExternalID	String	20	No	Yes	Yes	No	Not applicable
Username	__NAME__	String	40	Yes	Yes	Yes	Yes	Not applicable
Server		Long		Yes		Yes	Yes	Not applicable

Table 3-3 (Cont.) Default Attributes for SAP S/4HANA Cloud Target Application

Display Name	Target Attribute	Data Type	Length	Mandatory Provisioning Property?	Provision Field?	Recon Field	Key Field?	Case Insensitive?
First Name	FirstName	String	80	Yes	Yes	Yes	No	Not applicable
Last Name	LastName	String	80	Yes	Yes	Yes	No	Not applicable
Full Name	PersonFullName	String	80	Yes	Yes	Yes	No	Not applicable
Middle Name	MiddleName	String	80	No	Yes	Yes	No	Not applicable
Email	EmailAddress	String	241	Yes	Yes	Yes	No	Not applicable
User ID	UserID	String	12	No	No	Yes	No	Not applicable
Person UUID	PersonUUID	String	36	No	Yes	Yes	No	Not applicable
User Validity Start Date	StartDate	Date		Yes	Yes	Yes	No	Not applicable
User Validity End Date	EndDate	Date		Yes	Yes	Yes	No	Not applicable
Is Locked	LockedIndicator	Boolean		No	Yes	Yes	No	Not applicable
Company Code	CompanyCode	String	250	No	Yes	No	No	Not applicable
Gender	GenderCode	String	250	No	Yes	No	No	Not applicable
Worker Type	PersonWorkAgreementType	String	250	No	Yes	No	No	Not applicable
Status	__ENABLE__	String		No	No	Yes	No	Not applicable
Decimal Format	DecimalFormatCode	String	250	No	Yes	Yes	No	Not applicable
Date Format	DateFormatCode	String	250	No	Yes	Yes	No	Not applicable
Time Format	TimeFormatCode	String	250	No	Yes	Yes	No	Not applicable
Time Zone	TimeZoneCode	String	250	No	Yes	Yes	No	Not applicable

Figure 3-1 Default Attribute Mappings for SAP S/4HANA Cloud User Account



Role Attribute

Table 3-4 lists the inline Role attribute mappings between the process form fields in Oracle Identity Governance and SAP S/4HANA Cloud target application 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.

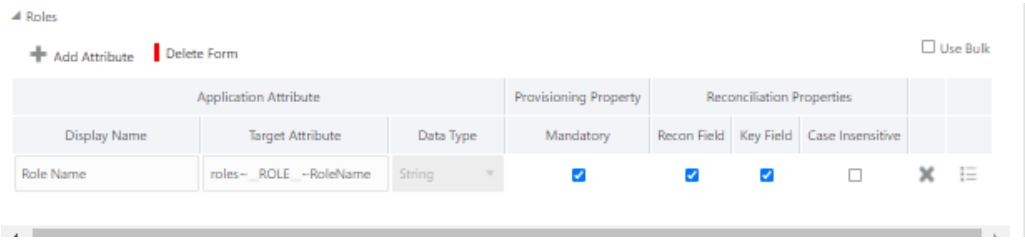
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.*

Table 3-4 Default Attribute Mappings for Role

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?	Advanced Settings
Role Name	roles~__ROLE__~RoleName	String	Yes	Yes	Yes	No	Length:250

Figure 3-2 shows the default attribute Role mapping.

Figure 3-2 Default Attribute Mappings for Role



3.4 Correlation Rules, Situations, and Responses for a Target Application

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 S/4HANA Cloud 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 3-5 lists the default simple correlation rule for SAP S/4HANA Cloud connector. 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, Updating Identity Correlation in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5 Predefined Identity Correlation Rule for SAP S/4HANA Cloud Target Application

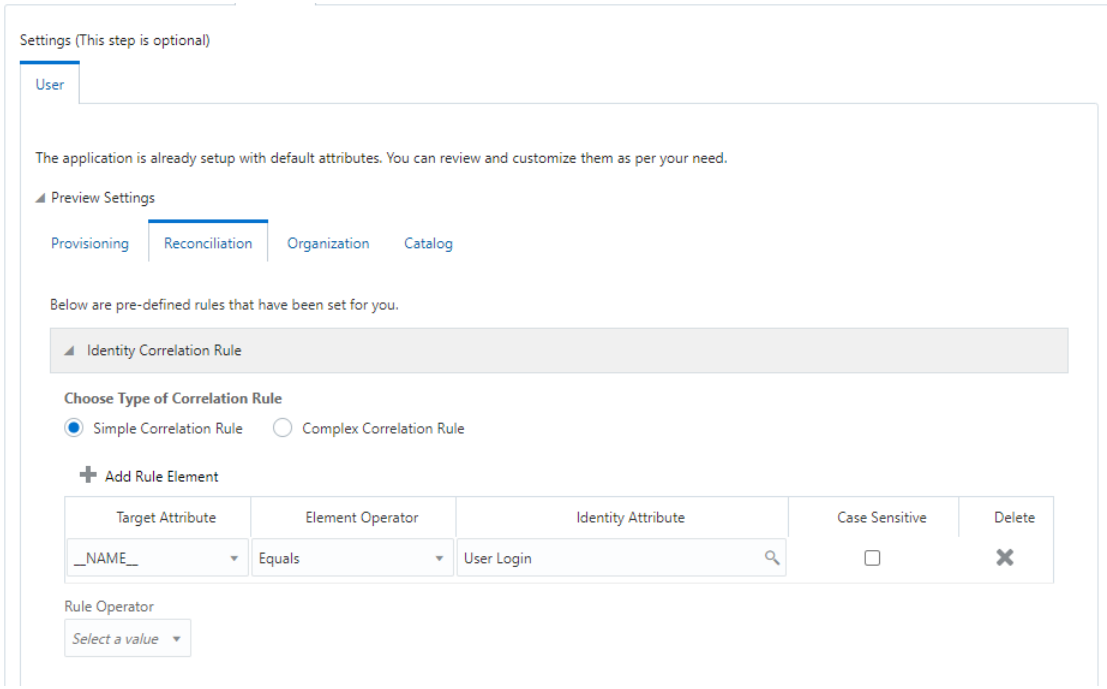
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?	Rule Operator
__NAME__	Equals	User Login	No	

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 3-3 shows the simple correlation rule for SAP S/4HANA Cloud target application.

Figure 3-3 Simple Correlation Rule for SAP S/4HANA Cloud Target Application



Predefined Situations and Responses

The SAP S/4HANA Cloud 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 3-6 lists the default situations and responses for a SAP S/4HANA Cloud Target 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 a SAP S/4HANA Cloud Target Application

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 SAP S/4HANA Cloud Resource User Reconciliation job is used to reconcile user data from a target application.

Table 3-7 shows the parameters of the S4HANA user reconciliation job.

Table 3-7 Parameters of the S4HANA User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Scheduled Task Name	This parameter holds the name of the scheduled job. **Note:** For the scheduled job included with this connector, you must not change the value of this parameter. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter. Default value: *APP_NAME* S4HANA Target Resource User Reconciliation
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. See Performing Limited Reconciliation for more information about this attribute.
Object Type	This attribute holds the name of the object type for the reconciliation run. **Default value**: `User` Do not change the default value.

Reconciliation Jobs for Entitlements

> **Note:**
>
> This Lookup Recon is applicable from S4HANA-12.2.1.3.0A or a later version.

The following jobs are available for reconciling entitlements:

- Roles Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-8 describes the parameters of the Reconciliation jobs for entitlements.

Table 3-8 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Current AOB application name with which the reconciliation job is associated. Do *not* modify this value.
Code Key Attribute	Name of the connector attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). **Default value**: `__UID__`
Decode Attribute	Name of the connector attribute that is used to populate the **Decode** column of the lookup definition (specified as the value of the Lookup Name attribute). **Default value**: `Name`
Lookup Name	Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system. Depending on the Reconciliation job that you are using, the default values are as follows: • For S4HANA Role Lookup Reconciliation: Lookup.S4HANA.Roles If you create a copy of any of these lookup definitions, then enter the name of that new lookup definition as the value of the Lookup Name attribute.
Object Type	Enter the type of object you want to reconcile. Depending on the Reconciliation job that you are using, the default values are as follows: • For S4HANA Role Lookup Reconciliation: __ROLE__ Do *not* change the value of this parameter.

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 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 Log Levels
- Enabling Logging

4.3.1 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
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.

4.3.2 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='S4HANA-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> Copy<logger name="
        ORG.IDENTITYCONNECTORS.S4HANA" level="[LOG_LEVEL]"
          useParentHandlers="false">   <handler
          name="S4HANA-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= 'S4HANA -handler'

level='NOTIFICATION:1'class='oracle.core.ojdl.logging.ODLHandlerFactor
y'>
             <property name='logreader:' value='off'/>      <property
name='path'

value='F:\MyMachine\middleware\user_projects\domains\base_domain1\serv
ers\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.S4HANA" level="NOTIFICATION:1"
          useParentHandlers="false">   <handler name="S4HANA-
handler"/>
             <handler
          name="console-handler"/>
    </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.

4.4 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 Resource of *Oracle Fusion Middleware Administering Oracle Identity Governance*. While creating the IT resource, ensure to use to select **Connector Server** from the **IT Resource Type** list.

Table 4-2 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: `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 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 S4HANA Application instance. The original code is:

```
 <trans-unit
          id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.user
EO.UD_USER_NAME__c_description']}"><source>Username</
source><target/></trans-unit><trans-unitid="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.user
EO.UD_S4HANAApp_USER_NAME__c_description']}"><source>UserName</
source><target/></trans-unit><trans-
```

```
unitid="sessiondef.oracle.iam.ui.runtime.form.model.S4HANAApp.ent
ity.S4HANAAppEO.UD_S4HANAApp_USER_NAME__c_LABEL"><source>UserName
</source><target/></trans-unit>Open the resource file from the
connector package, for       example
            S4HANA_ja.properties, and get the value of the
attribute from the       file, for

example,Copyglobal.udf.UD_S4HANA_USER_NAME=\u30E6\u30FC\u30B6\u30
FC\u540DReplace the original code shown in Step 6.c with the
          following:Copy<trans-unit
          id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_USER_NAME__c_description']}"><source>Username</
source><trans-unitid="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_S4HANAApp_USER_NAME__c_description']}"><source>UserNam
e</source>
          <target>\u30E6\u30FC\u30B6\u30FC\u540D</target></trans-
unit><trans-
unitid="sessiondef.oracle.iam.ui.runtime.form.model.S4HANAApp.ent
ity.S4HANAAppEO.UD_S4HANAApp_USER_NAME__c_LABEL"><source>User

    Name</source> <target>\u30E6\u30FC\u30B6\u30FC\u540D</
target> </trans-unit>
```

d. Open the resource file from the connector package, for example S4HANA_ja.properties, and get the value of the attribute from the file, for example,

```
global.udf.UD_S4HANA_USER_NAME=\u30E6\u30FC\u30B6\u30FC\u540D
```

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

```
<trans-unit
          id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_USER_NAME__c_description']}"><source>Username</
source><trans-unitid="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_S4HANAApp_USER_NAME__c_description']}"><source>UserNam
e</source>
          <target>\u30E6\u30FC\u30B6\u30FC\u540D</target></trans-
unit><trans-
unitid="sessiondef.oracle.iam.ui.runtime.form.model.S4HANAApp.ent
```

```
ity.S4HANAAppEO.UD_S4HANAApp_USER_NAME__c_LABEL"><source>UserName</
source> <target>\u30E6\u30FC\u30B6\u30FC\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.

> **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.

4.6 Configuring SSL

Configure SSL to secure data communication between Oracle Identity Governance and the Zoom 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 S/4HANA Cloud and SAP IAS.

   To obtain these certificates use one of the following methods: (Recommended method a and b):

   a. Using openssl utility: Most of Unix OS have this utility installed by default. If you don't have it, get it installed or follow other method(s) available.

   b. Run following command to obtain certificates. Replace host IP/ DNS, port and certificate name and rerun this command until all the required certificates are obtained.

   ```
   Syntax: echo | openssl s_client -connect <host IP/ DNS>:<port number>
   -showcerts >> [path where you want to save your cert]/<file name (use
   crt, cert, pem, der etc . extension based on your keystore)>example:
   echo | openssl s_client -connect oracle.com:443 -showcerts >>
   oracle.cert
   ```

   c. Ask your Certificate Management Team to download and share the certs

Follow the below steps while using the browser:

- a. Login to your SAP IAS instance.
  b. Click **Lock Icon > Secure Connection/Connection is secure**.

> **Note:**
>
> – Depending on the browser type the next steps will change. The following steps are applicable for Firefox browser.
>
> – Use the **Download Application Certificate** for all types of browser and not the Root CA or issuer.

  c. Select **More information > Security > View certificate.**
  d. Scroll to the option **Miscellaneous** and download certificate.

2. Copy the public key certificate of SAP S/4HANA Cloud and SAP IAS 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
- ERT_FILE_NAME is the full path and name of the certificate to be added to store KEYSTORE_NAME is the name of the keystore.
- CPASSWORD is the password of the keystore.

The following are sample values for this command:

```
keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file
<fully qualified S4/HANA Cloud certificate name -storepass
DemoTrustKeyStorePassPhrase -alias s4hana_cloud
```

```
keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file
<fully qualified SAP IAS certificate name> -storepass
DemoTrustKeyStorePassPhrase -alias SAP_IAS
```

> **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 it to meet your requirements.

Topics

This chapter discusses the following topics:

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 provides information on the following topics related to configuring 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, ensure that no value is specified for the Filter attribute.

5.1.2 Performing Batched Reconciliation

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

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

You can configure batched reconciliation to avoid such problems.

To configure batched reconciliation, you must specify a value for the batch-size parameter of the Basic Settings section. Use this attribute to specify the number of records that must be

included in each batch. By default, this value is 10 and SAP recommends to use value between 10-100.

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

5.1.3 Performing Limited Reconciliation

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

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. The connector provides a Filter parameter that allows you to use any of the SAP resource attributes to filter the target system records.

The following are the list of supported filters:

1. BusinessPartnerRoleCodeInterval
2. FirstNameInterval
3. EmailAddressInterval
4. LastNameInterval
5. PersonExternalIDInterval
6. PersonIDInterval
7. UserIDInterval
8. UserNameInterval

The syntax for this parameter is as follows:

Filter Account using Username

For example, EQ("UserNameInterval","NEHA")

Here any user with Username NEHA is reconciled.

Remaining Attributes filter parameters:

EQ("FirstNameInterval","NEHA")

EQ("LastNameInterval","Chandra")

EQ("BusinessPartnerRoleCodeInterval","BUP003")

EQ("EmailAddressInterval","nikhil@mail.com")

EQ("PersonExternalIDInterval","EE1912903_NIKHIL")

Other than EQUAL filter will support below Operation

Table 5-1 SAP S/4HANA Cloud connector

Operation	Syntax	Example
EQUAL	EQ(“<filterName>”,<value>)	EQ("BusinessPartnerRoleCodeInterval","BUP003")
BETWEEN	BT(“<filtername>”,”<from value>”,”<to value>”)	BT("BusinessPartnerRoleCodeInterval","BUP003","BUP003")
GREATER EQUAL	GE(“<filtername>”,”<from value>”,”[to value]”)	GE("BusinessPartnerRoleCodeInterval","BUP003")
GREATER THAN	GT(“<filtername>”,”<from value>”,”[to value]”)	GT("BusinessPartnerRoleCodeInterval","BUP003")
LESS EQUAL	LE(“<filtername>”,”<from value>”,”[to value]”)	LE("BusinessPartnerRoleCodeInterval","BUP003")
LESS THAN	LT(“<filtername>”,”<from value>”,”[to value]”)	LT("BusinessPartnerRoleCodeInterval","BUP003")

Note:

SAP S/4HANA Cloud connector does not support any other filters.
<> - indicates value is required

[ ] – indicates optional

BusinessPartnerRoleCodeInterval filter only supports BUP003 (Employee)

For more details on S4/HANA Cloud filters, to **Business User - Read** under **APIs for Setting Up Your SAP S/4HANA Cloud**" in SAP Help Portal.

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 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:
   - **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 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 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.

Below are examples to uninstall ResourceObjects and ScheduleJobs respectively:

- `ObjectType=ResourceObject`

  `ObjectValues=<Application Name>`

- `ObjectType= ScheduleJob`

  `ObjectValues= <Application Name>Workday Target User Reconciliation`

> **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 a Connector in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

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:

- Adding New Attributes for Reconciliation
- Adding New Attributes for Provisioning
- Configuring Transformation and Validation of Data
- Configuring Action Scripts

6.1 Adding New Attributes for Reconciliation

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

The default attribute mappings for reconciliation are listed in Attribute Mappings.

6.2 Adding New Attributes for Provisioning

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

The default attribute mappings for provisioning are listed in Attribute Mappings.

> **Note:**
>
> Note: If the added attribute cannot be updated, ensure to add the attribute to `updateNotSupportedForAttribute` in the Advanced Settings Parameters.

6.3 Configuring Transformation and Validation of Data

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

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

Similarly, you can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First

Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

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

6.4 Configuring 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

Known Issues and Workarounds

This chapter provides solutions to the commonly encountered issues associated with the S4HANA connector:

- The delete operation is not supported by S4HANA APIs. So, revoking the S4HANA account results in locking user account and shrinking validity period in target.
- Reconciling revoked account in OIM will result in creating new account in Disabled state. Due to above reason.
- Lock indicator (Lock) field can’t be set while creating user. Even though you set it it’ll not reflect in target.
- On User Enable, Start and End date will be set to today’s date and 31-12-9999 respectively. Same will not reflect in Account details until reconciled.
- On User Disable, End date will be set to today’s date. Same will not reflect in Account details until reconciled.
- Locking user account or user validity in past date will restrict user to login to S4HANA Cloud,
- Accounts created thru reconciliation will not populate fields like Gender, Worker Type, Company name, or attributes which are not part of S4HANA Cloud Web Service response.
- In target, Start and End Date will only be updated on Employee page while user creation and not thereafter.
- In target, End date will be set as ’31-12-9999’ even if value is provided during user creation. It’s a target limitation. To sync it with OIM user attribute, update on user is created

A

Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the SAP S/4HANA Cloud connector.

Table A-1 Files and Directories in the SAP S/4HANA Cloud Connector Installation Package

File in the Installation Package	Description
/bundle/org.identityconnectors.s4hana-12.3.0.jar	This JAR is the ICF connector bundle.
configuration/S4HANA-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the Connector Installer during connector installation.
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.
xml/S4HANA-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/S4HANA-pre-config.xml	This XML file contains definitions for lookup and pre-defined lookup values.
/lib/commons-codec-1.15.jar /lib/commons-logging-1.2-1b97e70.jar /lib/httpclient5-5.1.3.jar /lib/httpcore5-5.1.3.jar /lib/jackson-annotations-2.13.0.jar /lib/jackson-core-2.13.3.jar /lib/jackson-databind-2.13.3.jar /lib/slf4j-api-2.0.0.jar	These files are 3rd and 4th party dependent JARs for S4HANA Target

Glossary

Index