Oracle® Identity Governance

Configuring the Zoom Connector Application

12c (12.2.1.3.0)

F50309-01

Oracle Identity Governance Configuring the Zoom Connector Application, 12c (12.2.1.3.0)

F50309-01

Contributing Authors: (contributing author) Maya Chakrapani

Contributors: (contributor) Syam Battu, (contributor) Raghunath Edhara

Contents

Preface

This guide describes the connector that is used to onboard the Zoom 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.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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, 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 Zoom Connector lets you create and onboard Zoom 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.

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

- Certified Components
- Usage Recommendation
- Certified Languages
- Supported Connector Operations
- Connector Architecture
- Use Cases Supported by the Connector
- Connector Features

1.1 Certified Components

These are the software components and their versions required for installing and using the Zoom 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: • Oracle Identity Governance 12*c*(12.2.1.4.0) or later • Oracle Identity Governance 12*c* PS3 (12.2.1.3.0) **Note**: Ensure that you download and apply the patch 27861122 from My Oracle Support for 12 *c* PS3 (12.2.1.3.0).
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later
Target systems	Zoom
Connector Server	11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 and later
Target API version	Zoom v2

1.2 Usage Recommendation

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

1.3 Certified Languages

These are the languages that the connector supports.

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

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

1.4 Supported Connector Operations

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

Table 1-2 Supported Connector Operations

Operation	Supported
User Management	
Create user	Yes
Update user	Yes
Enable user	Yes
Disable user	Yes
Delete user	Yes
Reset Password	Yes
Role Grant Management	
Assign and Revoke Roles	Yes
Group Grant Management	
Assign and Revoke Group	Yes

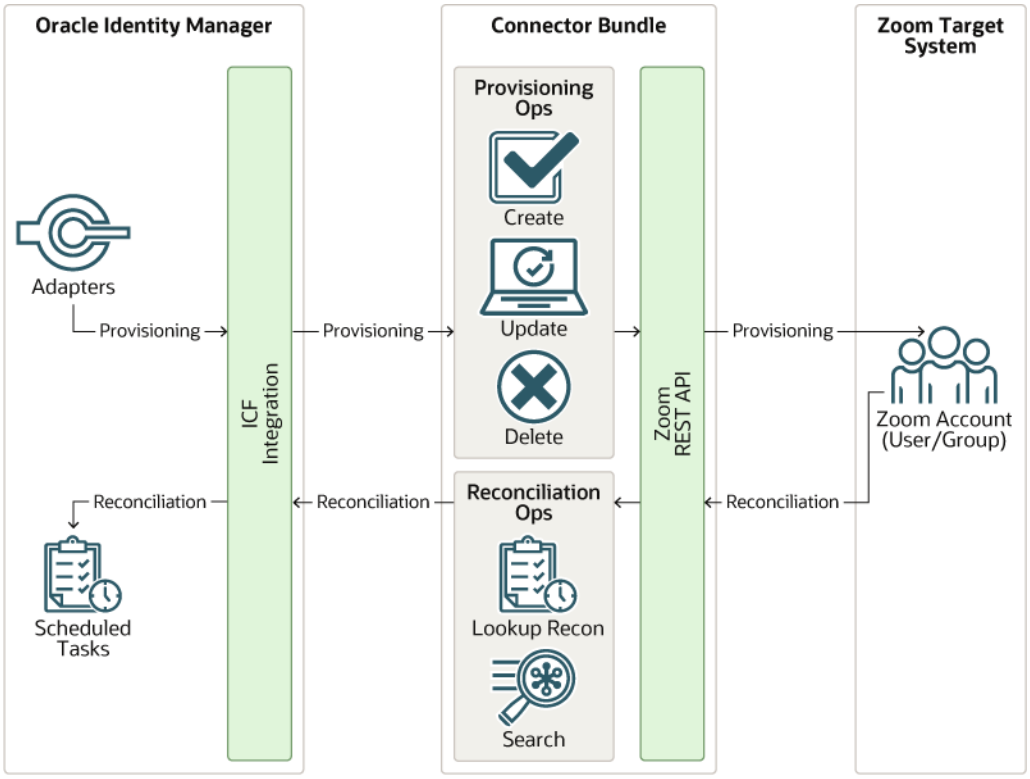
1.5 Connector Architecture

The Zoom 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 Zoom.

Figure 1-1 Zoom Connector Architecture



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 inturn invokes create operation on the Zoom Identity Connector Bundle and then the bundle calls the target system API (Zoom 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 Zoom Identity Connector Bundle and then the bundle calls Zoom 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 Zoom resources that are already provisioned to OIM Users. If a match is found, then the update made to the Zoom record from the target system is copied to the Zoom 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 Zoom resource to the OIM User.

The Zoom Identity Connector Bundle communicates with the Zoom API using the HTTPS protocol. The Zoom API provides programmatic access to Zoom through REST API endpoints. Apps can use the REST 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

The Zoom is used to integrate Oracle Identity Governance with Zoom to ensure that all Zoom accounts are created, updated, and deactivated on an integrated cycle with the rest of the identity-aware applications in your enterprise. The Zoom supports management of identities for Cloud Identity, Synchronized Identity, and Federated Identity models of Zoom. In a typical IT scenario, an organization using Oracle Identity Governance wants to manage accounts, groups, roles across Zoom Cloud Service. The following are some of the most common scenarios in which this connector can be used:

- **Zoom User Management**:
  An organization using Zoom wants to integrate with Oracle Identity Governance to manage identities. The organization wants to manage its user identities by creating them in the target system using Oracle Identity Governance. The organization also wants to synchronize user identity changes performed directly in the target system with Oracle Identity Governance. In such a scenario, a quick and an easy way is to install the Zoom and configure it with your target system by providing connection information.

  To create a new user in the target system, fill in and submit the OIM process form to trigger the provisioning operation. The connector executes the CreateOp operation against your target system and the user is created on successful execution of the operation. Similarly, operations like delete and update can be performed.

  To search or retrieve the user identities, you must run a scheduled task from Oracle Identity Governance. The connector will run the corresponding SearchOp against the user identities in the target system and fetch all the changes to Oracle Identity Governance
- **Zoom Group Management**:

An organization has a number of Zoom Groups allowing its users to set up new groups, manage memberships, and delete groups. The organization now wants to know the list of groups that have not been recently accessed or who have inactive members. In such a scenario, you can use the Zoom to highlight the usage trend for groups. By using the Zoom, you can leverage the reporting capabilities of Oracle Identity Governance to track any operations (such as create, update, delete) performed on groups.

- **Zoom Admin Role Management**:
  In large organizations, it may be necessary for an administrator to designate other employees to act as administrators to serve different functions. For example, you can set admin roles for your IT staff that can act as support agents to other employees, partners, customers and vendors. With the Zoom, you can assign or revoke an Zoom admin role to users as an entitlement, thus facilitating you to leverage the delegated administration capability of Zoom.

1.7 Connector Features

The features of the connector include support for connector server, full reconciliation, limited reconciliation, and reconciliation of deleted account data.

Table 1-3 provides the list of features supported by the AOB application.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application
Full reconciliation	Yes
Limited reconciliation	Yes
Delete reconciliation	Yes
Use connector server	Yes
Transformation and validation of account data	Yes
Perform connector operations in multiple domains	Yes
Support for paging	Yes
Test connection	Yes
Reset password	Yes
Zoom Group assignment	Yes
Zoom Role assignment	Yes

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

- Full Reconciliation
- Limited Reconciliation
- Support for the Connector Server
- Transformation and Validation of Account Data

1.7.1 Full Reconciliation

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

After the first full reconciliation run, you can configure your connector if the target system contains an attribute that holds the time-stamp at which an object is created or modified.

1.7.2 Limited 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.

1.7.3 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 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

1.7.4 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 Validation and Transformation of Provisioning and Reconciliation Attributes in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

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 Zoom Cloud 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.

- Registering the Client Application
- Downloading the Connector Installation Package

2.1.1 Registering the Client Application

Registering a client application (Zoom connector) with the target system is the first step that is performed before creating an application instance so that the connector can access Zoom REST APIs. It also involves generating the API key and API secret for authenticating to the target system and setting the permissions and scopes for the client application. Pre-provisioning involves performing the following tasks on the target system

1. Register your client application with Zoom Marketplace to provide secure sign in and authorization for your services. To do so:
   a. Sign in to Zoom marketplace.
   b. Select **Develop** from the top right.
   c. Choose **Build App** from the drop-down.
   d. Create the App from Server to Server OAuth by providing the **App Name**.
2. In the **App Credentials**, the details of **Client ID**, **Client Secret** and **Account ID** values for your client application is available.

   > **Note:**
   >
   > Make a note of these values as it is needed for connector Basic Configuration parameters.

3. Select **Scope** and click **Add Scope** to add permissions needed for client application to access the target system.
   Under **User**, **Group**, and **Role** tabs, perform the following:

a. Assign the Read, and Write scope that the client application requires on Zoom.

b. Assign the following delegated scope that the client application requires on Zoom:

- user:write:admin
- group:write:admin
- role:write:admin

4. Activate your Application.

2.1.2 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.

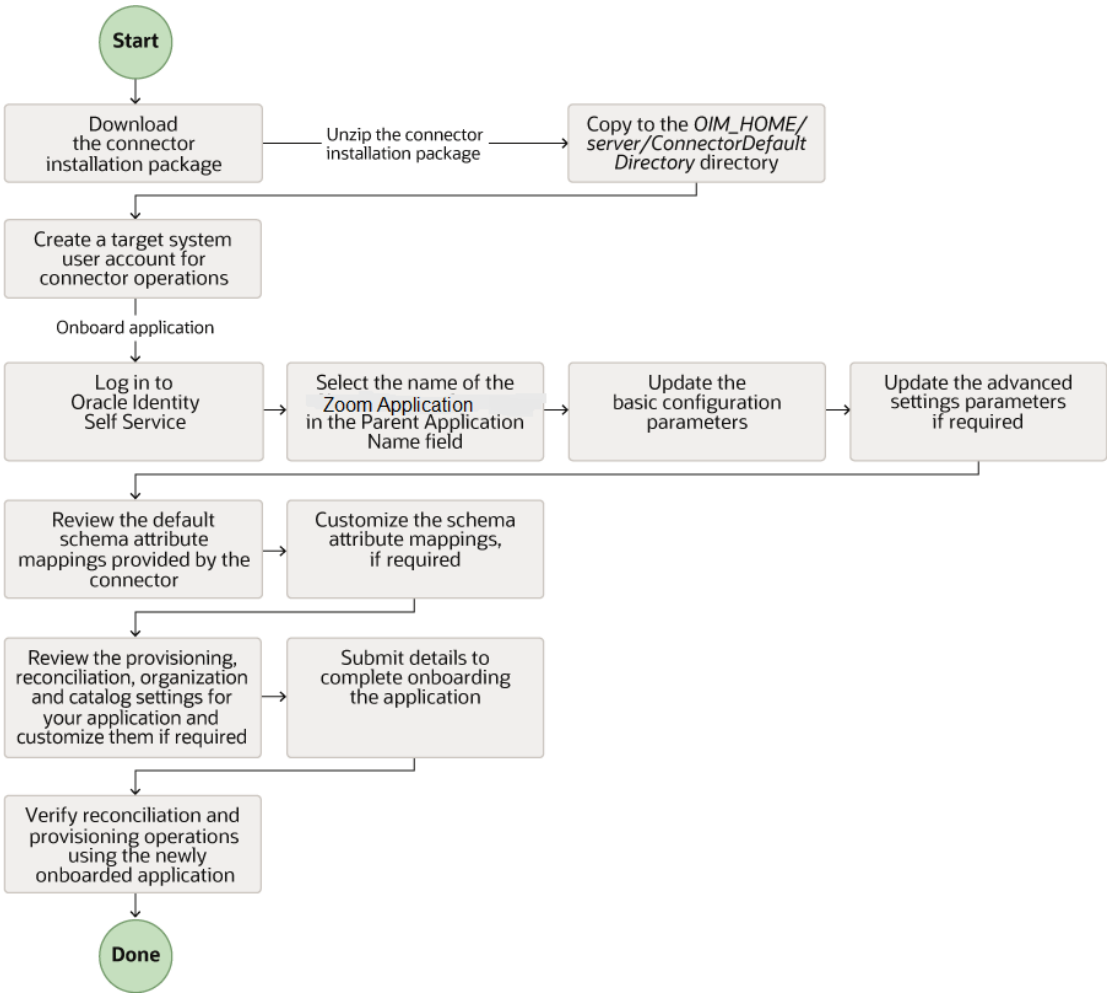
   You must accept the license agreement before you can download the installation package.
4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle 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.

2.2 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.

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



2.3 Creating an Application By Using the Zoom 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.

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 Connector of 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 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 a Zoom application.

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

Table 3-1 Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
authenticationType	Yes	Enter the type of authentication used by your Zoom target system. For this connector, the target system supports `OAuth credentials`. This is a mandatory attribute while creating an application. Do *not* modify the value of the parameter. **Default value**: client_credentials
authenticationServerUrl	Yes	End point URL of the server which authenticates the application. Default Value: https://zoom.us/oauth/token?grant_type=account_credentials&account_id=YourAccountIDFromApplication

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

Parameter	Mandatory ?	Description
clientId	Yes	Enter the API key (a unique string) issued by the authorization server to your `OAuth application` during the registration process. You will obtain the API key while performing the procedure described in Configuring the Newly Added Application.
clientSecret	Yes	Enter the API secret key used to authenticate the identity of your `OAuth application`. You will obtain the API secret key while performing the procedure described in Configuring the Newly Added Application.
Connector Server Name	No	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.
Host	Yes	Enter the host name of the machine hosting your Zoom target system. This is a mandatory attribute while creating an application. **Sample value**: api.zoom.us
uriPlaceHolder	Yes	Enter the key-value pair for replacing place holders in the relURIs. The URI place holder consists of values which are repeated in every relative URL. Values must be comma separated. For example, Tenant ID and API version values are a part of every request URL. Therefore, we replace it with a key-value pair. **Sample value**: api_version;v2
port	No	Enter the port number at which the target system is listening. **Sample value**: 443
proxyHost	No	Enter the name of the proxy host used to connect to an external target.
proxyPassword	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.
proxyPort	No	Enter the proxy port number.

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

Parameter	Mandatory ?	Description
sslEnabled	No	If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false. **Default 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

Bundle Name	This entry holds the name of the connector bundle. **Default value**: `org.identityconnectors.genericrest`
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.genericrest.GenericRESTConnector`

Table 3-2 (Cont.) Advanced Settings Parameters

relURIs	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. This is a mandatory attribute while creating an application. **Default value**: "__ACCOUNT__.CREATEOP=/$(api_version)$/users","__ACCOUNT__.UPDATEOP=/$(api_version)$/users/$(__UID__)$","__ACCOUNT__.DELETEOP=/$(api_version)$/users/$(__UID__)$?action=delete","__ACCOUNT__.__PASSWORD__.UPDATEOP=/$(api_version)$/users/$(__UID__)$/password","__ACCOUNT__.SEARCHOP=/$(api_version)$/users?$(FilterSuffix)$&page_size=$(PAGE_SIZE)$&next_page_token=$(PAGE_TOKEN)$","__GROUP__.SEARCHOP=/$(api_version)$/groups","__ACCOUNT__.group_ids.SEARCHOP=/$(api_version)$/users/$(__UID__)$","__ACCOUNT__.group_ids.UPDATEOP=/$(api_version)$/groups/$(group_ids)$/members","__ACCOUNT__.group_ids.DELETEOP=/$(api_version)$/groups/$(group_ids)$/members/$(__UID__)$","__ROLE__.SEARCHOP=/$(api_version)$/roles","__ACCOUNT__.role_id.UPDATEOP=/$(api_version)$/roles/$(role_id)$/members","__ACCOUNT__.role_id.DELETEOP=/$(api_version)$/roles/$(role_id)$/members/$(__UID__)$","__ACCOUNT__.__ENABLE__.UPDATEOP=/$(api_version)$/users/$(__UID__)$/status","__ACCOUNT__.__NAME__.UPDATEOP=/$(api_version)$/users/$(__UID__)$/email"

Table 3-2 (Cont.) Advanced Settings Parameters

nameAttributes	This entry holds the name attribute for all the objects that are handled by this connector. For example, for the __ACCOUNT__ object class that it used for User accounts, the name attribute is userPrincipalName. **Default value** `"__ACCOUNT__.email","__GROUP__.name", "__ROLE__.name"`
uidAttributes	This entry holds the uid attribute for all the objects that are handled by this connector. For example, for User accounts, the uid attribute is objectId. In other words, the value __ACCOUNT__objectId in decode implies that the __UID__attribute (that is, GUID) of the connector for _ACCOUNT__object class is mapped to objectId which is the corresponding uid attribute for user accounts in the target system. **Default value:** `"__ACCOUNT__.id","__GROUP__.id","__ROLE__.id"`
opTypes	This entry specifies the HTTP operation type for each object class supported by the connector. Values are comma separated and are in the following format: *OBJ_CLASS.OP=HTTP_OP* In this format, *OBJ_CLASS* is the connector object class, OP is the connector operation (for example, CreateOp, UpdateOp, SearchOp), and HTTP_OP is the HTTP operation (GET, PUT, or POST). **Default value**: `"__ACCOUNT__.CREATEOP=POST","__ACCOUNT__.UPDATEOP=PATCH","__ACCOUNT__.SEARCHOP=GET","__ACCOUNT__.TESTOP=GET","__ACCOUNT__.group_ids.UPDATEOP=POST","__ACCOUNT__.role_id.UPDATEOP=POST","__ACCOUNT__.__PASSWORD__.UPDATEOP=PUT","__ACCOUNT__.__ENABLE__.UPDATEOP=PUT","__ACCOUNT__.__NAME__.UPDATEOP=PUT"`
pageSize	The number of resources/users that appears on a page for a search operation. **Default value**: 30

Table 3-2 (Cont.) Advanced Settings Parameters

pageTokenAttribute	The attribute in response payload that denotes the next page token. **Default value**: `next_page_token`
jsonResourcesTag	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload. **Default value**: `"__ACCOUNT__=users","__GROUP__=groups","__ROLE__=roles"`
httpHeaderContentType	This entry holds the content type expected by the target system in the header. **Default value**: `application/json`
httpHeaderAccept	This entry holds the accept type expected from the target system in the header. **Default value**: `application/json`
provisionDisableValue	This value is used to deactivate the user by provisioning. **Default value**: `deactivate`
provisionEnableValue	This value is used to activate the user by provisioning. **Default value**: `activate`
statusDisableValue	This value is used to deactivate the user during reconciliation. **Default value**: `inactive`

Table 3-2 (Cont.) Advanced Settings Parameters

statusEnableValue	This value is used to activate the user during reconciliation. **Default value**: `active`
specialAttributeTargetFormat	This entry lists the format in which an attribute is present in the target system endpoint. For example, the alias attribute will be present as aliases.alias in the target system endpoint. Values are comma separated and are presented in the following format: *OBJ_CLASS.ATTR_NAME=TARGET_FORMAT* **Default value:** `"__ACCOUNT__.group_ids=group_ids","__ACCOUNT__.role_id=value"`
specialAttributeHandling	This entry lists the special attributes whose values should be sent to the target system one by one ("SINGLE"). Values are comma separated and are in the following format: *OBJ_CLASS.ATTR_NAME.PROV_OP*=SINGLE For example, the __ACCOUNT__.manager.UPDATEOP=SINGLE value in decode implies that during an update provisioning operation, the manager attribute of the __ACCOUNT__ object class must be sent to the target system one-by-one. **Default value:** `"__ACCOUNT__.group_ids.CREATEOP=SINGLE","__ACCOUNT__.group_ids.UPDATEOP=SINGLE","__ACCOUNT__.role_id.CREATEOP=SINGLE","__ACCOUNT__.role_id.UPDATEOP=SINGLE"`

Table 3-2 (Cont.) Advanced Settings Parameters

customPayload	This entry lists the payloads for all operations that are not in the standard format. **Default value:** `"__ACCOUNT__.CREATEOP={\"action\": \"$(createType)$\",\"user_info\": { \"email\": \"$(__NAME__)$ \",\"type\": \"$(type)$ \",\"first_name\": \"$(first_name)$ \",\"last_name\": \"$(last_name)$ \",\"password\": \"$(__PASSWORD__)$ \"}}","__ACCOUNT__.group_ids.UPDATEOP={\"members\": [{ \"id\": \"$ (__UID__)$ \"}]}","__ACCOUNT__.role_id.UPDATEOP={\"members\": [{\"id\": \"$ (__UID__)$ \"}]}","__ACCOUNT__.__ENABLE__.UPDATEOP={\"action\": \"$(__ENABLE__)$ \"}","__ACCOUNT__.__NAME__.UPDATEOP={\"email\": \"$(__NAME__)$\"}"`
statusAttributes	This entry lists the name of the target system attribute that holds the status of an account. For example, for the __ACCOUNT__ object class that it used for User accounts, the status attribute is “status”. **Default value:** `"__ACCOUNT__.status"`
passwordAttribute	This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute of the connector in OIM. **Default value:** `password`
childFieldsWithSingleEndpoint	This entry specifiesspecial attributes data coming in from a single end point response **Default value:** `"__GROUP__","__ROLE__"`

3.3 Attribute Mappings

The following topic provides the attribute mappings details.

- Attribute Mappings for the Target Application

3.3.1 Attribute Mappings for the Target Application

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.

Table 3-3 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Zoom 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 Zoom Target Application

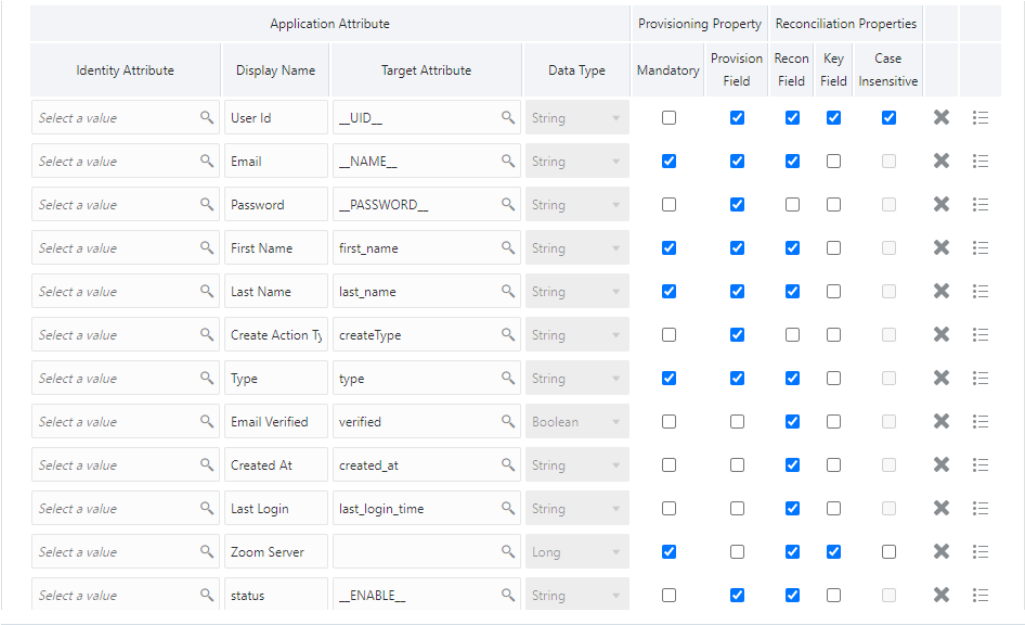
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User Id	__UID__	String	No	Yes	Yes	Yes	Yes
Email	__NAME__	String	Yes	Yes	Yes	No	Not applicable
Password	__PASSWORD__	String	No	Yes	No	No	Not applicable
First Name	first_name	String	Yes	Yes	Yes	No	Not applicable
Last Name	last_name	String	Yes	Yes	Yes	No	Not applicable
Create Action Type	createType	String	No	Yes	No	No	Not applicable
Type	type	String	Yes	Yes	Yes	No	Not applicable
Email Verified	verified	Boolean	No	No	Yes	No	Not applicable
Created At	created_at	String	No	No	Yes	No	Not applicable
Last Login	last_login_time	String	No	No	Yes	No	Not applicable
Zoom Server		Long	Yes	No	Yes	Yes	No
Status	__ENABLE__	String	No	Yes	Yes	No	Not applicable

Note:

The value **Create Action Type** must be selected during user provisioning as it is not a target attribute, we are just passing values through this attribute in payload.

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

Figure 3-1 Default Attribute Mappings for Zoom User Account



Zoom Role Entitlement

lists the roles forms attribute mappings between the process form fields in Oracle Identity Governance and Zoom 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.

> **Note:**
>
> Role is a single valued attribute, and default Role is member. You cannot add or delete users to member/owner roles.

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.

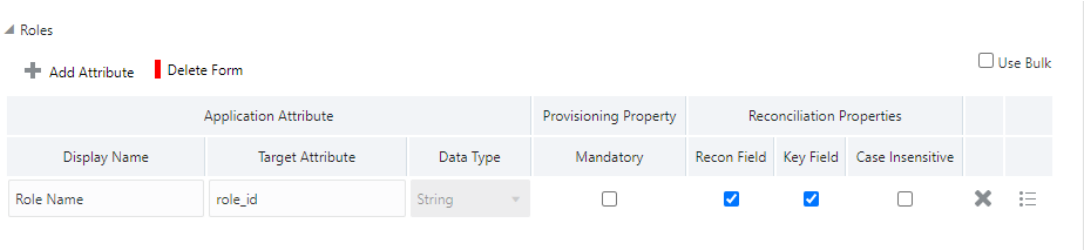
Default Attribute Mappings for Roles

Table 3-4 Default Attribute Mappings for Roles

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

Figure 3-2 shows the default Roles Entitlement mapping.

Figure 3-2 Default Attribute Mappings for Zoom Roles



Zoom Groups Entitlement

lists the group forms attribute mappings between the process form fields in Oracle Identity Governance and Zoom 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.

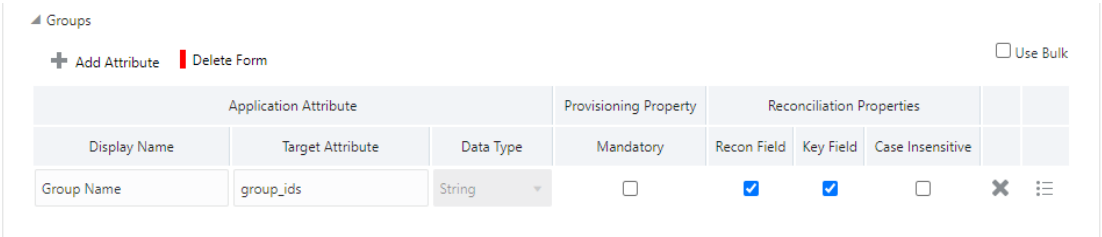
Table 3-5 Default Attribute Mappings for Groups

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

Zoom Groups Entitlement

Figure 3-3 shows the default Groups entitlement mapping.

Figure 3-3 Zoom Groups Entitlement



3.4 Correlation Rules

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

- Correlation Rules for the Target Application

3.4.1 Correlation Rules for the 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 Zoom 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 3-6 lists the default simple correlation rule for a Zoom connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rules in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-6 Predefined Identity Correlation Rule for a Zoom Connector

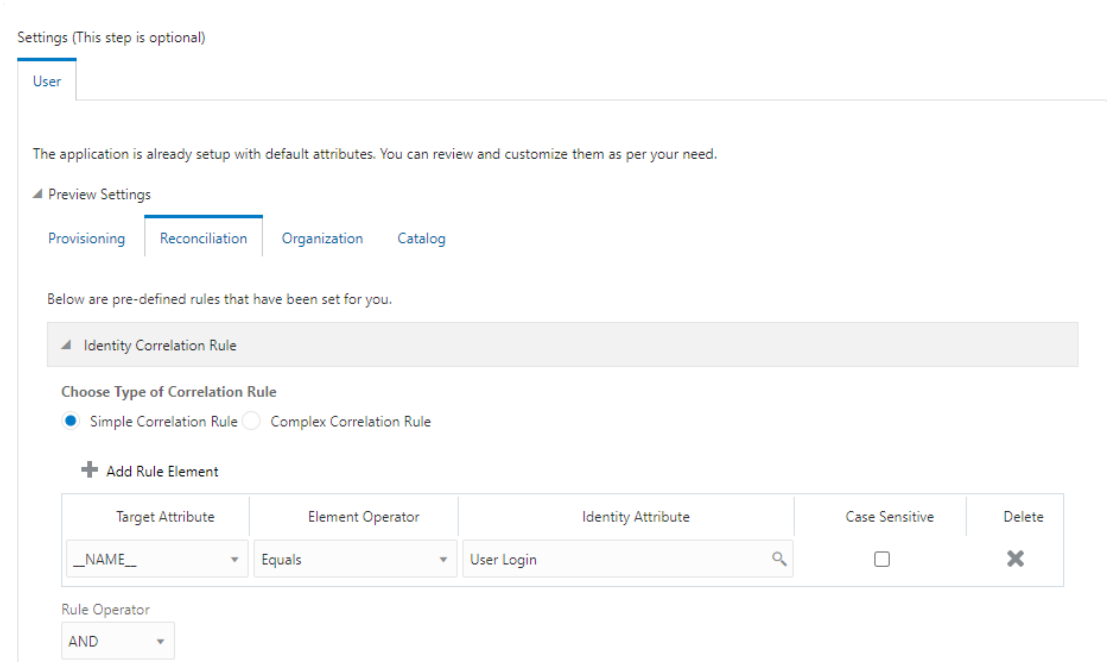
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

In this identity rule:

- :__NAME__ is a single-valued attribute on the target system that identifies the user account.
- User Login is the field on the OIG User form.Figure 3-1 shows the simple correlation rule for Zoom target application.

Simple Correlation Rule for Zoom Target Application

Figure 3-4 Simple Correlation Rule for Zoom Target Application



Predefined Situations and Responses

The Zoom 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.

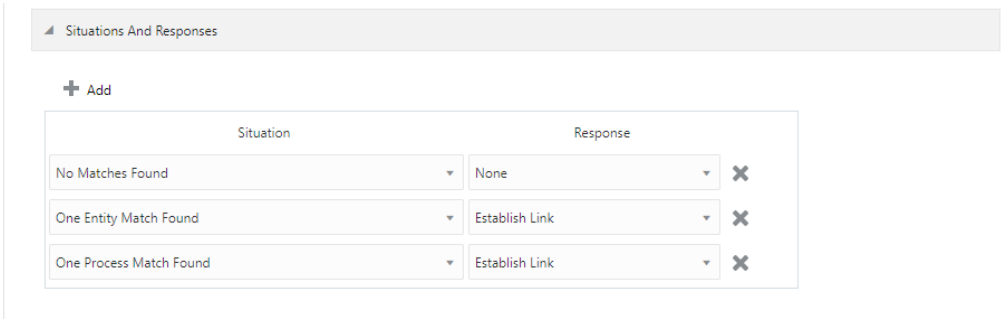
Table 3-7 lists the default situations and responses for a Zoom Target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and ResponsesUpdating Situations and Responses in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance

Table 3-7 Predefined Situations and Responses for a Zoom Target Application

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

Figure 3-5 shows the situations and responses for a Zoom that the connector provides by default.

Figure 3-5 Predefined Situations and Responses for a Zoom Target Application



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:

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

Table 3-8 describes the parameters of the Zoom Full User Reconciliation job.

Table 3-8 Parameters of the Zoom 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.

Table 3-8 (Cont.) Parameters of the Zoom Full User Reconciliation Job

Parameter	Description
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. Filter suffix for single user: 1. /UserID 2. /Email Filter suffix for reconning set of users 1. Status = all (gets active and inactive users) 2. Status = active (gets all active users) 3. Status = inactive (gets all inactive users) 4. role_id = role id of users (gets users based on role id) 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.

Target Delete User Reconciliation Job

The Zoom User Target Delete Recon job is used to reconcile data about deleted users from Zoom target application. During a reconciliation run, for each deleted user account on the target system, the Zoom resource is revoked for the corresponding OIM User.

Table 3-9 Parameters of the Zoom User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
Object Type	This parameter holds the type of object you want to reconcile. **Default value**: User **Note**: If you configure the connector to provision users to a custom class (for example, InetOrgPerson) then enter the value of the object class here.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- Zoom Group Lookup Reconciliation
- Zoom Role Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-10 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__ Do *not* modify this value.
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 Zoom Group Lookup Reconciliation: Lookup.Zoom.Groups • For Zoom Role Lookup Reconciliation: Lookup.Zoom.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 Zoom Group Lookup Reconciliation: __GROUP__ • For Zoom Role Lookup Reconciliation: __ROLE__ **Note**: 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 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 Resources of *Oracle Fusion Middleware Administering Oracle Identity Governance.*While creating the IT resource, ensure to select Connector Server from the IT Resource Type list. In addition, specify values for the parameters of IT resource for the Connector Server listed in Table 4-2. 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 Zoom 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 Zoom 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_PRINCIPAL_NAME__c_description']}"><source>User Principal
      Name</source><target/></trans-unit><trans-unit
```

```
id="sessiondef.oracle.iam.ui.runtime.form.model.RSAForm.entity.Zo
omFormEO.UD_USER_PRINCIPAL_NAME
      __c_LABEL"><source>First Name</source><target/> </trans-
unit>
```

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

```
global.udf.UD_GA_USR_USER_PRINCIPAL_NAME
    =\u30A2\u30AB\u30A6\u30F3\u30C8\u540D
```

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBu ndle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.use rEO.UD_GA_USR_ USER_PRINCIPAL_NAME
__c_description']}"><source>Account Name</source>
<target>u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target></trans-
unit> <trans-
unitid="sessiondef.oracle.iam.ui.runtime.form.model.Zoom.entity
sEO.UD_GA_USR_ACCOUNT_NAME__c_LABEL"><source>Account Name</
source> <target>\u30A2\u30AB\u30A6\u30F3\u30C8\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 Zoom.
2. Copy the public key certificate of Zoom 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.

   ```
   keytool -import -alias serverwl -trustcacerts -file supportcert.pem -
   keystore client_store.jks -storepass weblogic1
   ```

   - ```
     keytool -import -keystore <JAVA_HOME>/jre/lib/security/cacerts -file
     <Cert_Location>/BaltimoreCyberTrustRoot.crt -storepass changeit -alias
     BaltimoreCyberTrustRoot_1
     keytool -import -keystore <JAVA_HOME>/jre/lib/security/cacerts -file
     <Cert_Location>/MicrosoftITTLSCA1.crt -storepass changeit -alias
     MicrosoftITTLSCA1_1
     ```
   - ```
     keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file
     <Cert_Location>/BaltimoreCyberTrustRoot.crt -storepass
     DemoTrustKeyStorePassPhrase -alias BaltimoreCyberTrustRoot_1
     keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file
     <Cert_Location>/MicrosoftITTLSCA1.crt -storepass
     DemoTrustKeyStorePassPhrase -alias MicrosoftITTLSCA1_1
     ```

   > **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.

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:

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 one of the reconciliation jobs listed in the Reconciliation Jobs section.

> **Note:**
>
> Zoom connector only supports recon of active and inactive users. Connector does not support recon of pending 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 criteria.

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.

You can perform limited reconciliation by creating filters for the reconciliation module. An example `Filter Suffix` value that is valid in the API version V2 is as follows:

Filter Suffix for single user:

1. /UserID
2. /Email

Filter suffix for reconning set of users

1. Status = all (gets active and inactive users)
2. Status = active (gets all active users)
3. Status = inactive (gets all inactive users)
4. role_id = role id of users (gets users based on role id)

> **Note:**
>
> - While running full user recon without any filter it only brings in active users by default it doesn't recon inactive and pending users.
> - While running full user recon with filter "status=all" and "status=inactive" it doesn't bring the "Last Login" time and date of the users.

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.

5.2 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

1. Log in to Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the parameters of the scheduled task:
   - **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

- **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

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

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

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

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

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

5.3 Configuring Provisioning

You can configure the provisioning operation for the Zoom connector.

This section provides information on the following topics:

- Guidelines on Performing Provisioning Operations
- Performing Provisioning Operations

5.3.1 Guidelines on Performing Provisioning Operations

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

Provisioning Prerequisites:

These parameters are required for user provisioning. These values must be added to the design console in the Lookup definition as `createType` and `Type` must be passed as static Lookup and values must be mapped as provided in the following steps:.

1. Add Code Key and Decode Key for `Lookup.Zoom.createType Lookup` as provided in the following design console under LookupDefinition.

Table 5-1 Code Key and Decode Key

Code Key	Decode Key
create	create
autoCreate	autoCreate
custCreate	custCreate
ssoCreate	ssoCreate

2. Add Code Key and Decode Key for Lookup.Zoom.type as below in design console under LookupDefinition.

Table 5-2 Code Key and Decode Key

Code Key	Decode Key
1	Basic
2	Licensed
3	On-prem
99	None

Provisioning attributes required to create user account

To create User provisioning operation, follow the following values as required:

- First Name: The user's first name.
- Last Name: The user's last name.
- Email: The user's email ID. (You must have managed domain registered with Zoom to update email.)
- Type: The user's license type. The Default type is Basic.
- Password: The password of the user, which is applicable only when autoCreate option is selected.

> **Note:**
>
> - Permission requirements that are required to provision the user type with On-Prem from zoom support.
> - Passwords can only be updated for Zoom accounts that were created using a work email. Passwords cannot be changed for accounts that were created using custCreate, SSO, Sign in With Google and Sign In With Facebook options
> - Target does not allow to create the user with the email id which has already been used in Zoom cloud.
> - Create action type is not a target attribute so we cannot update it, incase if you update it also nothing is updated in target and does not throw any error.
> - Permission requirements that are required to provision the user type with On-Prem from zoom support.
> - Target does not allow to create the user with the email id which has already been used in zoom cloud.

Attributes required to be updated in the parent form

- First Name: The user's first name.
- Last Name: The user's last name.

- Email: The user's email ID. (You must have managed domain registered with Zoom to update email.)
- Type: The user's license type. The Default type is Basic.
- Password: The password of the user.

> **Note:**
>
> - Only users provisioned with SSO can set the user type to None.
> - Permission requirements that are required to provision the user type with On-Prem from zoom support.
> - Passwords can be updated for Zoom accounts that were created using a work email. Passwords cannot be changed for accounts that were created using custCreate, SSO, Sign in With Google and Sign In With Facebook options.
> - Target does not allow to create the user with the email id which has already been used in Zoom cloud.
> - Create action type is not a target attribute so we cannot update it, if you update it also nothing is updated in target and does not throw any error.

Delete/Revoke a User

By default, you can delete all types of users, but to delete a pending user, update the rel URL action to disassociate. Default rel URL for delete "`__ACCOUNT__.DELETEOP=/$(api_version)$/users/$(__UID__)$?action=delete`" Update the rel URL to delete pending user. "`__ACCOUNT__.DELETEOP=/$(api_version)$/users/$(__UID__)$?action=disassociate`"

> **Note:**
>
> If the pending users must be deleted from OIM and pending users list in Target, you must update the rel URL as above. Also, you must identify the pending user and select and delete the User from OIM so that users can be revoked in OIM and deleted in Target from pending user's list.

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**.

5.4 Uninstalling the Connector

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

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

For example: `Zoom User; Zoom Group`

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

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

6
Extending the Functionality of the 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*.

6.3 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.

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 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 following are the known issues and limitations associated with the Zoom connector.

Known Issues:

1. In Zoom Target, the accounts created with action type **Create** are sent an invitation email, such users will be in pending status until invite is accepted within the valid period. However, this pending user will be in Provisioned Status in OIG.
   Workaround:

   You must run the **Delete User Recon** job to sync and revoke the accounts in OIG for accounts in Pending status in the Zoom target.
2. If you run the **Delete User Recon** job without approving the *Activation Account* email within the time period, then OIG accounts will be revoked. If you approve the activation email, the user status is updated to Active in Zoom target.
   Workaround:

   Ensure to run the User Recon/Full Recon job, in such situations in OIG, which results in creation of a new account with status as provisioned.
3. If you initiate revoke accounts in OIG, which are in Pending status in the Zoom target, this will result in an error message in logs.
   Workaround:

   You need to update the relURL action as disassociate. For more information see the details on Guidelines on Performing Provisioning Operations.

8

Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the Zoom connector.

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

File in the Installation Package	Description
/bundle/org.identityconnectors.genericrest-12.3.0	This JAR is the ICF connector bundle.
configuration/Zoom-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.
xml/Zoom-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.

Glossary

Index