Oracle® Identity Governance

Configuring the Azure Active Directory Application

12c (12.2.1.3.0)
F30762-06
November 2021

Oracle Identity Governance Configuring the Azure Active Directory Application, 12c (12.2.1.3.0)

F30762-06

Primary Author: Maya Chakrapani

Contributors: Raghunath Edhara

Contents

Preface

What's New in This Guide?

1 About the Connector

2 Creating an Application by Using the Connector

3 Configuring the Connector

4 Performing Postconfiguration Tasks for the Connector

5 Using the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to onboard the Azure Active Directory 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 12.2.1.3.0, visit the following Oracle Help Center page:

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

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

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

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.

What’s New in This Guide?

These are the updates made to the software and documentation for release 12.2.1.3.0.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is a software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

From this release onward, the connector bundle includes application onboarding templates required for performing connector operations on the Azure Active Directory target. This helps in quicker onboarding of the applications for Azure Active Directory into Oracle Identity Governance by using an intuitive UI.

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following documentation-specific updates have been made in revision "03" of this guide:

- Added the 'granularLicenses' parameter to Advanced Settings Parameters
- Updated the 'relURIs' parameter in Advanced Settings Parameters
- Added details for Direct and Inherited Licenses to Use Cases Supported by the Connector

The following documentation-specific update has been made in revision "01" of this guide:

This is the first release of this connector. Therefore, there are no documentation-specific updates in this release.

1 About 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 Azure Active Directory connector lets you create and onboard Azure AD (Azure Active Directory) 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 Azure AD connector:

- Connector Offerings Compared to Office 365
- Certified Components
- Usage Recommendation
- Certified Languages
- Supported Connector Operations
- Connector Architecture
- Use Cases Supported by the Connector
- Connector Features

1.1 Connector Offerings Compared to Office 365

Azure AD connector provides additional benefits over the Office 365 connector. Here are a few top reasons to opt-in for Azure AD, instead of the Office 365 connector.

- Azure AD connector users can leverage latest Microsoft graph API using the Azure AD connector.
- Azure AD connector offers Out Of the Box feature that helps distinguish between security and Office 365 groups.
- Azure AD connector provides improved reconciliation performance over the Office 365 connector.

1.2 Certified Components

These are the software components and their versions required for installing and using the Azure AD 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 release 12*c* PS4 (12.2.1.4.0) • Oracle Identity Governance 12*c* PS3 (12.2.1.3.0) and apply 12.2.1.3.180413(p27861122_122130_Generic.zip) Patch.
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later
Target systems	Azure AD
Connector Server	11.1.2.1.0 or 12.2.1.3 and later
Connector Server JDK	JDK 1.8 and later
Target API version	Azure Active Directory (AD) Microsoft graph API v1.0 and Authentication API version v2.0

1.3 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.

1.4 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
Reset Password	Yes
Role Grant Management	
Assign and Revoke Roles	Yes
License Grant Management	
Grant and Revoke Licences	Yes
Security Group Management	
Add, Update, and Remove Groups	Yes
Office Group Management	
Add, Update, and Remove Groups	Yes
MS Teams Management	
Create groups to the user	Yes
Delete groups from the user	Yes
Reconcile groups to the user	Yes
Teams Group Assignment	
Add Teams Group to the user	Yes
Remove Teams Group from the user	Yes

> **Note:**
>
> The MS Teams support is applicable from 12.2.1.3.0B.

> **Note:**
>
> All the connector artifacts required for managing groups as an object (for example groups attribute mappings, reconciliation rules, jobs, and so on) are not visible in the Applications UI in Identity Self Service. However, all the required information is available in the predefined application templates of the connector installation package. For more information about the artifacts related to groups, see Connector Objects Used for Groups Management.

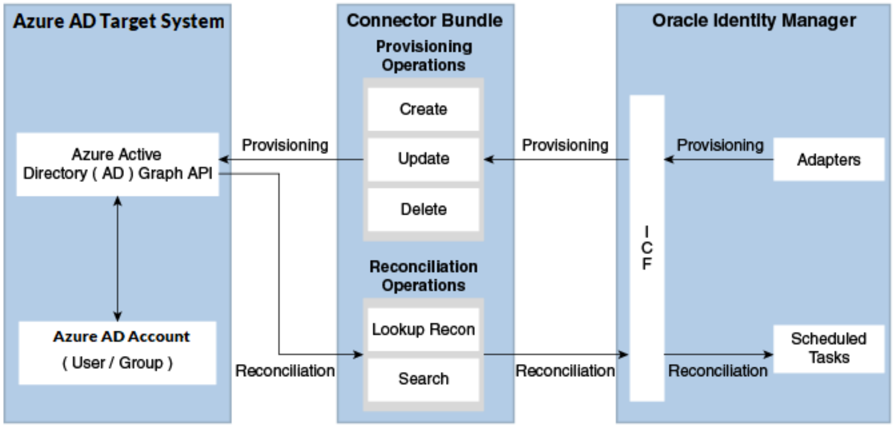
1.6 Connector Architecture

The Azure AD 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 Azure AD connector.

Figure 1-1 Connector Architecture



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

- Identity reconciliation

  Identity reconciliation is also known as authoritative or trusted source reconciliation. In this mode, the Azure AD application is used as the trusted source and users are directly created and modified on Oracle Identity Governance. During reconciliation, a scheduled task invokes an ICF operation. ICF inturn invokes a search operation on the Azure AD Identity Connector Bundle and then the bundle calls Azure AD 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 user record fetched from the target system is compared with existing OIM Users. If a match is found between the target system record and the OIM User, then the OIM User attributes are updated with changes made to the target system record. If no match is found, then the target system record is used to create an OIM User.

- 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 Azure AD Identity Connector Bundle and then the bundle calls the target system API (Microsoft Azure Active Directory (AD) Graph 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 inturn invokes a search operation on the Azure AD Identity Connector Bundle and then the bundle calls Azure AD 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 Azure AD resources that are already provisioned to OIM Users. If a match is found, then the update made to the Azure AD record from the target system is copied to the Azure AD resource in Oracle Identity Governance. If no match is found, then the userPrincipalName 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 Azure AD resource to the OIM User.

The Azure AD Identity Connector Bundle communicates with the Microsoft Graph API using the HTTPS protocol. The Microsoft Graph API provides programmatic access to Azure Active Directory through REST API endpoints. Apps can use the Microsoft Graph 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

1.7 Use Cases Supported by the Connector

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

The following are some of the most common scenarios in which this connector can be used:

- **Azure AD User Management**

An organization using Azure AD 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 Azure AD connector 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.

- **Azure AD Group Management**

  An organization has a number of Azure AD Security 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 Azure AD connector to highlight the usage trend for groups. By using the Azure AD connector, you can leverage the reporting capabilities of Oracle Identity Governance to track any operations (such as create, update, delete) performed on groups and changes made in their memberships .

- **Azure AD 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 Azure AD connector, you can assign or revoke an Azure AD admin role to users as an entitlement, thus facilitating you to leverage the delegated administration capability of Azure AD.

- **Azure AD User License Management**

  Another scenario is one in which an organization is using Azure AD for business and manages user licenses as per the changing needs of the organization by assigning or unassigning licenses for users. What is needed is an effective way to keep track of all the licenses and user rights both in cloud and on-premise servers. In such a scenario, you can use the Azure AD connector to effectively track all user licenses. You can keep track of these license assignment changes by leveraging Oracle Identity Governance capability of auditing and reporting.

  There are two types of Licensing available to make your large-scale license management easier.

  1. **Direct License**
     Assigns product licenses to a group of users and verifys that they are licensed correctly in Azure Active Directory, for example, Office 365 Enterprise E3 licenses.

  2. **Inherited License**
     Microsoft has made group-based license management available through the Azure portal. The customer can enable/disable the individual service plans available for a single product. Service plans are known as Inherited licenses, for example, Office 365 Enterprise E3 licenses have available service plans such as, Teams, PowerBI, Yammer, and SharePoint.

> **Note:**
>
> If Direct License is added to a user without any service plans there is a default license attached to that user. The user cannot add/remove the default license. If a user wants to remove all the Inherited Licenses, they should mandatorily remove the Direct License.

- **MS Teams Group Support**
  Microsoft Teams is a proprietary business communication platform developed by Microsoft, as part of the Microsoft 365 family of products. By using the MS Team, users can share files, organize meetings from their calendar, and sync with other Office apps like MS OneNote, MS OneDrive, and Skype for Business. This improves collaboration and communication while simultaneously aiding the adoption of Office 365.

1.8 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
Support for authoritative source reconciliation	Yes
Support for authoritative source 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
MS Teams management	Yes

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

Feature	AOB Application
Teams Group assignment	Yes

> **Note:**
>
> MS Teams support is applicable from 12.2.1.3.0

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

Feature	AOB Application
	B .

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

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

1.8.1 Full Reconciliation and Incremental 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 for incremental reconciliation if the target system contains an attribute that holds the timestamp at which an object is created or modified.

In the Azure AD connector, the incremental reconciliation option is not enabled by default. The connector supports incremental reconciliation only if the target system contains an attribute that holds the timestamp at which an object is created or modified.

> **Note:**
>
> The connector supports incremental reconciliation if the target system contains an attribute that holds the timestamp at which an object is created or modified.

You can perform a full reconciliation run at any time. See Performing Full Reconciliation and Incremental Reconciliation for more information about performing full and incremental reconciliation.

1.8.2 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 .

1.8.3 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 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

1.8.4 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 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

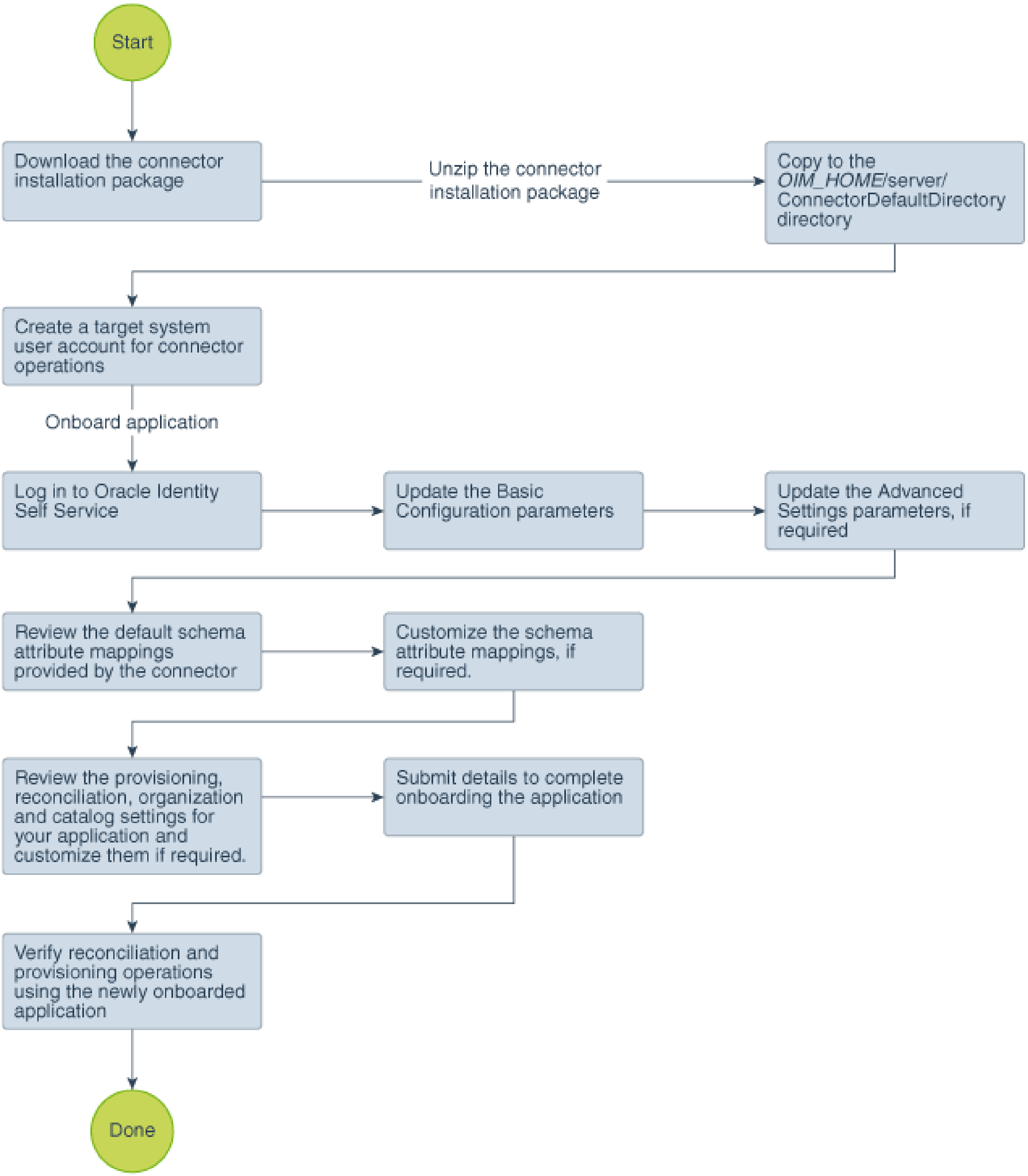
Learn about onboarding applications using the connector and the prerequisites for doing so.

2.1 Process Flow for Creating an Application By Using the Connector

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

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

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


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

2.2 Prerequisites for Creating an Application By Using the Connector

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

2.2.1 Registering the Client Application

Registering a client application (that is, the Azure AD connector) with the target system is a step that is performed before creating an application instance so that the connector can access Azure AD Graph APIs. It also involves generating the client ID and client secret for authenticating to the target system and setting the permissions for the client application.

Preprovisioning involves performing the following tasks on the target system:

1. Register your client application with Microsoft Azure Active Directory to provide secure sign in and authorization for your services. You can register your client application by creating an application in the Microsoft Azure Management Portal.
2. Generate the client ID and client secret values for your client application. Note down these values as they are required while configuring IT resource parameters.
3. Specify the permissions that the client application requires to access the target system. To do so:
   a. Assign the **Read and write domains** and **Read and write directory data** application permissions that the client application requires on Windows Azure Active Directory.
   b. Assign the following delegated permissions that the client application requires on Windows Azure Active Directory:
      - Read and write directory data
      - Read and write all groups
      - Read all groups
      - Access the directory as the signed-in user
      - Read directory data
      - Read all user’s full profiles
      - Read all user’s basic profiles
      - Sign in and read user profile

   c. Add the client application to "Company Administrator" and “User Account Administrator” in the Azure AD administrative roles. Visit the following Microsoft support URL for detailed information: https://support.microsoft.com/en-in/kb/3004133

      This provides the necessary permissions for the client application to perform the Change Password and Delete user and group membership operations.

2.2.2 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 Creating an Application By Using the 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 on each of the steps in this procedure, see Creating Applications of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

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

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

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

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

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

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

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

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

      The application is created in Oracle Identity Governance.

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

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

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

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

3
Configuring the Connector

While creating a target or an authoritative 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.

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

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to an Azure AD application. These parameters are common for both target applications and authoritative applications.

> **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 target system. For this connector, the target system OAuth2.0 client credentials. This is a mandatory attribute while creating an application. Do *not* modify the value of the parameter. **Default value**: `client_credentials`
host	Yes	Enter the host name of the machine hosting your target system. This is a mandatory attribute while creating an application. **Sample value**: `graph.microsoft.com`

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

Parameter	Mandatory ?	Description
authenticationServerUrl	Yes	Enter the URL of the authentication server that validates the client ID and client secret for your target system. **Sample value**: `https://login.microsoftonline.com/idmconnector.onmicrosoft.com/oauth2/v2.0/token`
clientId	Yes	Enter the client identifier (a unique string) issued by the authorization server to your client application during the registration process. You obtained the client ID while performing the procedure described in Configuring the Newly Added Application.
clientSecret	Yes	Enter the secret key used to authenticate the identity of your client application. You obtained the secret key while performing the procedure described in Configuring the Newly Added Application.
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;v1.0"`
port	No	Enter the port number at which the target system is listening. **Sample value**: `443`
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`

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

Parameter	Mandatory ?	Description
Scope	Yes	Enter the scope of your client application. **Default value:** `https://graph.microsoft.com/.default`
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.
proxyUser	No	Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system. **Sample value:** `80`

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
granularLicenses	This parameter enables the support for granular licenses. **Default value**: False **Note:** granularLicenses parameter is supported from 12.2.1.3.0A

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Description
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__.SEARCHOP=/$(api_version)$/users?$(Filter Suffix)$&$select=assignedLicenses,userType,displayName,givenName,userPrincipalName,id,city,usageLocation,accountEnabled,mailNickname,surname,country&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__=/$(api_version)$/users/$(__UID__)$?$select=assignedLicenses,displayName,givenName,userPrincipalName,id,city,usageLocation,accountEnabled,mailNickname,country,surname,userType","__ACCOUNT__.manager.SEARCHOP=/$(api_version)$/users/$(__UID__)$/manager","__ACCOUNT__.manager=/$(api_version)$/users/$(__UID__)$/manager/$ref","__ACCOUNT__.__GROUP__.SEARCHOP=/$(api_version)$/users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__.__GROUP__.DELETEOP=/$(api_version)$/groups/$(__GROUP__.id)$/members/$(__UID__)$/$ref","__ACCOUNT__.__GROUP__=/$(api_version)$/groups/$(__GROUP__.id)$/members/$ref","__GROUP__.CREATEOP=/$(api_version)$/groups","__GROUP__.UPDATEOP=/$(api_version)$/groups/$(__UID__)$","__GROUP__.SEARCHOP=/$(api_version)$/groups?&$filter=securityEnabled+eq+true&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__OFFICEGROUP__.SEARCHOP=/$(api_version)$/groups?&$filter=securityEnabled+eq+false&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__GROUP__=/$(api_version)$/groups/$`

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Description
	`(__UID__)$","__GROUP__.member=/$(api_version)$/groups/$(__UID__)$/members/$ref?","__ROLE__.SEARCHOP=/$(api_version)$/directoryRoles?/$(Filter Suffix)$","__ACCOUNT__.__ROLE__=/$(api_version)$/directoryRoles/$(__ROLE__.id)$/members/$ref","__ACCOUNT__.__ROLE__.DELETEOP=/$(api_version)$/directoryRoles/$(__ROLE__.id)$/members/$(__UID__)$/$ref","__ROLE__.member=/$(api_version)$/directoryRoles/$(__UID__)$/members/$ref","__ACCOUNT__.__ROLE__.SEARCHOP=/$(api_version)$/users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","assignedLicenses.SEARCHOP=/$(api_version)$/subscribedSkus?/$(Filter Suffix)$","__ACCOUNT__.assignedLicenses.ADDATTRIBUTE=/$(api_version)$/users/$(__UID__)$/assignLicense","__ACCOUNT__.assignedLicenses.REMOVEATTRIBUTE=/$(api_version)$/users/$(__UID__)$/assignLicense","__ACCOUNT__.__OFFICEGROUP__=/$(api_version)$/groups/$(__OFFICEGROUP__.id)$/members/$ref","__ACCOUNT__.__OFFICEGROUP__.DELETEOP=/$(api_version)$/groups/$(__OFFICEGROUP__.id)$/members/$(__UID__)$/$ref","__ACCOUNT__.__OFFICEGROUP__.SEARCHOP=/$(api_version)$/users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$"` **Note:** granularLicenses parameter is supported from 12.2.1.3.0A If you are enabling the granular license replace the relURIs provided below.

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Description
	`"__ACCOUNT__.CREATEOP=/$(api_version)$/users","__ACCOUNT__.UPDATEOP=/$(api_version)$/users/$(__UID__)$","__ACCOUNT__.SEARCHOP=/$(api_version)$/users?$(Filter Suffix)$&$select=assignedLicenses,userType,displayName,givenName,userPrincipalName,id,city,usageLocation,accountEnabled,mailNickname,surname,country&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__=/$(api_version)$/users/$(__UID__)$?$select=assignedLicenses,displayName,givenName,userPrincipalName,id,city,usageLocation,accountEnabled,mailNickname,country,surname,userType","__ACCOUNT__.manager.SEARCHOP=/$(api_version)$/users/$(__UID__)$/manager","__ACCOUNT__.manager=/$(api_version)$/users/$(__UID__)$/manager/$ref","__ACCOUNT__.__GROUP__.SEARCHOP=/$(api_version)$/users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__.__GROUP__.DELETEOP=/$(api_version)$/groups/$(__GROUP__.id)$/members/$(__UID__)$/$ref","__ACCOUNT__.__GROUP__=/$(api_version)$/groups/$(__GROUP__.id)$/members/$ref","__GROUP__.CREATEOP=/$(api_version)$/groups","__GROUP__.UPDATEOP=/$(api_version)$/groups/$(__UID__)$","__GROUP__.SEARCHOP=/$(api_version)$/groups?&$filter=securityEnabled%20eq%20true&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__OFFICEGROUP__.SEARCHOP=/$(api_version)$/groups?&$filter=securityEnabled%20eq%20false&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__GROUP__=/$(api_version)$/groups/$(__UID__)$","__GROUP__.member=/$(api_version)$/groups/$(__UID__)$/members/$ref?","__ROLE__.SEARCHOP=/$(api_version)$/directoryRoles?/$(Filter`

Table 3-2   (Cont.) Advanced Settings Parameters

Parameter	Description
	Suffix)$","__ACCOUNT__.__ROLE__=/$(api_version)$/directoryRoles/$(__ROLE__.id)$/members/$ref","__ACCOUNT__.__ROLE__.DELETEOP=/$(api_version)$/directoryRoles/$(__ROLE__.id)$/members/$(__UID__)$/$ref","__ROLE__.member=/$(api_version)$/directoryRoles/$(__UID__)$/members/$ref","__ACCOUNT__.__ROLE__.SEARCHOP=/$(api_version)$/users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","assignedLicenses.SEARCHOP=/$(api_version)$/subscribedSkus?/$(Filter Suffix)$","__ACCOUNT__.assignedLicenses.ADDATTRIBUTE=/$(api_version)$/users/$(__UID__)$/assignLicense","__ACCOUNT__.assignedLicenses.REMOVEATTRIBUTE=/$(api_version)$/users/$(__UID__)$/assignLicense","__ACCOUNT__.__OFFICEGROUP__=/$(api_version)$/groups/$(__OFFICEGROUP__.id)$/members/$ref","__ACCOUNT__.__OFFICEGROUP__.DELETEOP=/$(api_version)$/groups/$(__OFFICEGROUP__.id)$/members/$(__UID__)$/$ref","__ACCOUNT__.__OFFICEGROUP__.SEARCHOP=/$(api_version)$/users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__.assignedLicenses.SEARCHOP=/$(api_version)$/users/$(__UID__)$/licenseDetails?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$" **Note:** If you are disabling the granular license kindly use the default RelURIs

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Description
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__.userPrincipalName,"__GROUP__.displayName","__ROLE__.displayName","assignedLicenses.skuPartNumber","__OFFICEGROUP__.displayName"`
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","assignedLicenses.skuId","__OFFICEGROUP__.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__.UPDATEOP=POST","__ACCOUNT__.manager.CREATEOP=PUT","__ACCOUNT__.manager.UPDATEOP=PUT","__ACCOUNT__.__ROLE__.UPDATEOP=POST","__ACCOUNT__.assignedLicenses.ADDATTRIBUTE=POST","__ACCOUNT__.assignedLicenses.REMOVEATTRIBUTE=POST","__ACCOUNT__.__OFFICEGROUP__.ADDATTRIBUTE=POST"`

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Description
pageSize	The number of resources/users that appears on a page for a search operation. **Default value**: `100`
pageTokenAttribute	The attribute in response payload that denotes the next page token. **Default value**: `odata.nextLink`
pageTokenRegex	This attribute is used in the URL while reconciliation to support pagination. **Default value**: `(?<=skiptoken=).*`
Any Incremental Recon Attribute Type	By default, during incremental reconciliation, Oracle Identity Governance accepts timestamp information sent from the target system only in Long datatype format. Setting the value of this parameter to `True` indicates that Oracle Identity Governance will accept timestamp information in any datatype format. **Default value**: `True`
jsonResourcesTag	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload. **Default value**: `__ACCOUNT__=value,"__GROUP__=value","__ROLE__=value","assignedLicenses=value","__OFFICEGROUP__=value"`
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`
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__.manager=id,"__GROUP__.member=url","__ROLE__.member=url","__ACCOUNT__.__GROUP__=value","__ACCOUNT__.__ROLE__=value","__ROLE__.member=value","__GROUP__.member=value","__ACCOUNT__.assignedLicenses=value","__ACCOUNT__.__OFFICEGROUP__=value"`

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Description
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__.CREATEOP=SINGLE,"__ACCOUNT__.__GROUP__.UPDATEOP=SINGLE","__ACCOUNT__.manager.CREATEOP=SINGLE","__ACCOUNT__.manager.UPDATEOP=SINGLE","__ACCOUNT__.__ROLE__.CREATEOP=SINGLE","__ACCOUNT__.__ROLE__.UPDATEOP=SINGLE","__ACCOUNT__.assignedLicenses.ADDATTRIBUTE=SINGLE","__ACCOUNT__.assignedLicenses.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.__OFFICEGROUP__.ADDATTRIBUTE=SINGLE","__ACCOUNT__.__OFFICEGROUP__.REMOVEATTRIBUTE=SINGLE"`

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Description
customPayload	This entry lists the payloads for all operations that are not in the standard format. **Default value:**`__ACCOUNT__.__GROUP__.UPDATEOP={\@odata.id\":\"https://graph.microsoft.com/v1.0/directoryObjects/$(__UID__)$\"}","__ACCOUNT__.__GROUP__.CREATEOP={\"@odata.id\":\"https://graph.microsoft.com/v1.0/directoryObjects/$(__UID__)$\"}","__ACCOUNT__.manager.CREATEOP={\"@odata.id\":\"https://graph.microsoft.com/v1.0/directoryObjects/$(manager)$\"}","__ACCOUNT__.manager.UPDATEOP={\"@odata.id\":\"https://graph.microsoft.com/v1.0/directoryObjects/$(manager)$\"}","__ACCOUNT__.__ROLE__.UPDATEOP={\"@odata.id\":\"https://graph.microsoft.com/v1.0/directoryObjects/$(__UID__)$\"}","__ACCOUNT__.__ROLE__.CREATEOP={\"@odata.id\":\"https://graph.microsoft.com/v1.0/directoryObjects/$(__UID__)$\"}","__ACCOUNT__.assignedLicenses.ADDATTRIBUTE={\"addLicenses\":[{\"skuId\": \"$(skuId)$\"}],\"removeLicenses\":[]}","__ACCOUNT__.assignedLicenses.REMOVEATTRIBUTE={\"addLicenses\":[],\"removeLicenses\": [\"$(skuId)$\"]}","__ACCOUNT__.__OFFICEGROUP__.UPDATEOP={\"@odata.id\":\"https://graph.microsoft.com/v1.0/directoryObjects/$(__UID__)$\"}"`
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 `accountEnabled`. **Default value:**`"__ACCOUNT__.accountEnabled"`
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:** `passwordProfile.password`

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Description
targetObjectIdentifier	This entry specifies the key-value pair for replacing place holders in the relURIs. Values are comma separated and in the *KEY*;*VALUE* format. **Default value:** `__ACCOUNT__.__GROUP__=securityEnabled;true,"__ACCOUNT__.__OFFICEGROUP__=securityEnabled;false","__ACCOUNT__.__ROLE__=@odata.type;#microsoft.graph.directoryRole"`
childFieldsWithSingleEnd	This entry specifies special attributes data coming in from a single end point response. **Default value:** `__GROUP__","__ROLE__","__OFFICEGROUP__"`

3.3 Attribute Mappings

The attribute mappings on the Schema page vary depending on whether you are creating a target application or an authoritative application.

- Attribute Mappings for the Target Application
- Attribute Mappings for the Authoritative Application
- MS Teams Management

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.

Default Attributes for Azure AD Target Application

Table 3-3 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Azure AD 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.

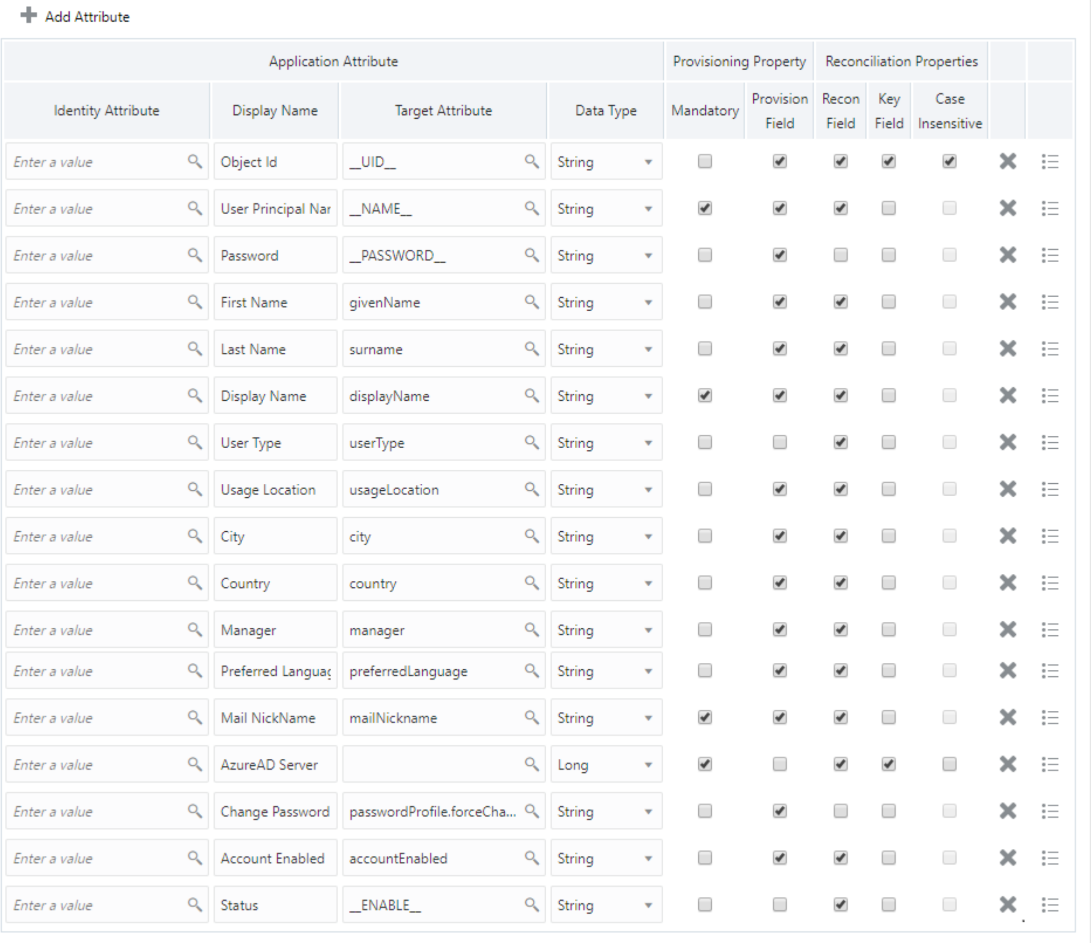
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attributes for Azure AD Target Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?	Advanced Flag Settings
Object Id	__UID__	String	No	Yes	Yes	Yes	Yes	Yes
User Principal Name	__NAME__	String	Yes	Yes	Yes	No	Not applicable	Yes
First Name	givenName	String	No	Yes	Yes	No	Not applicable	Yes
Last Name	surname	String	No	Yes	Yes	No	Not applicable	Yes
Display Name	displayName	String	Yes	Yes	Yes	No	Not applicable	Yes
Usage Location	usageLocation	String	No	Yes	Yes	No	Not applicable	Yes
City	city	String	No	Yes	Yes	No	Not applicable	Yes
Country	country	String	No	Yes	Yes	No	Not applicable	Yes
Manager	manager	String	No	Yes	Yes	No	Not applicable	Yes
Preferred Language	preferredLanguage	String	No	Yes	Yes	No	Not applicable	Yes
Mail NickName	mailNickname	String	Yes	Yes	Yes	No	Not applicable	Yes
Account Enabled	accountEnabled	String	No	Yes	Yes	No	Not applicable	Yes
AzureAD Server		Long	Yes	No	Yes	Yes	Not applicable	Yes
Status	__ENABLE__	String	No	No	Yes	No	Not applicable	Yes
Password	__PASSWORD__	String	No	Yes	No	No	Not applicable	Yes
Change Password On Next Logon	passwordProfile.forceChangePasswordNextLogin	String	No	Yes	No	No	Not applicable	Yes

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

Figure 3-1   Default Attribute Mappings for Azure AD User Account



➕ Add Attribute

Application Attribute				Provisioning Property		Reconciliation Properties				
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive		
Enter a value	Object Id	__UID__	String	□	☑	☑	☑	☑	✖	☰
Enter a value	User Principal Nar	__NAME__	String	☑	☑	☑	□	□	✖	☰
Enter a value	Password	__PASSWORD__	String	□	☑	□	□	□	✖	☰
Enter a value	First Name	givenName	String	□	☑	☑	□	□	✖	☰
Enter a value	Last Name	surname	String	□	☑	☑	□	□	✖	☰
Enter a value	Display Name	displayName	String	☑	☑	☑	□	□	✖	☰
Enter a value	User Type	userType	String	□	□	☑	□	□	✖	☰
Enter a value	Usage Location	usageLocation	String	□	☑	☑	□	□	✖	☰
Enter a value	City	city	String	□	☑	☑	□	□	✖	☰
Enter a value	Country	country	String	□	☑	☑	□	□	✖	☰
Enter a value	Manager	manager	String	□	☑	☑	□	□	✖	☰
Enter a value	Preferred Languag	preferredLanguage	String	□	☑	☑	□	□	✖	☰
Enter a value	Mail NickName	mailNickname	String	☑	☑	☑	□	□	✖	☰
Enter a value	AzureAD Server		Long	☑	□	☑	☑	□	✖	☰
Enter a value	Change Password	passwordProfile.forceCha...	String	□	☑	□	□	□	✖	☰
Enter a value	Account Enabled	accountEnabled	String	□	☑	☑	□	□	✖	☰
Enter a value	Status	__ENABLE__	String	□	□	☑	□	□	✖	☰

Roles Entitlement

Table 3-4 lists the roles-specific attribute mappings between the process form fields in Oracle Identity Governance and Azure AD 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.

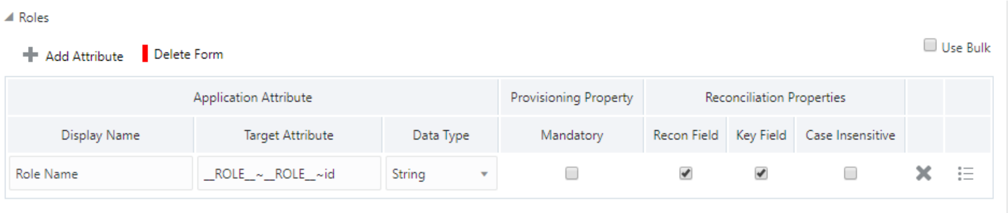
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4   Default Attribute Mappings for Roles

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

Figure 3-2 shows the default roles entitlement mapping.

Figure 3-2   Default Attribute Mappings for Role



◢ Roles

➕ Add Attribute ▌Delete Form ☐ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Role Name	_ROLE_~_ROLE_~id	String ▾	☐	☑	☑	☐	✖	☰

Groups Entitlement

Table 3-5 and Table 3-6 lists the group forms attribute mappings between the process form fields in Oracle Identity Governance and Azure AD 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.

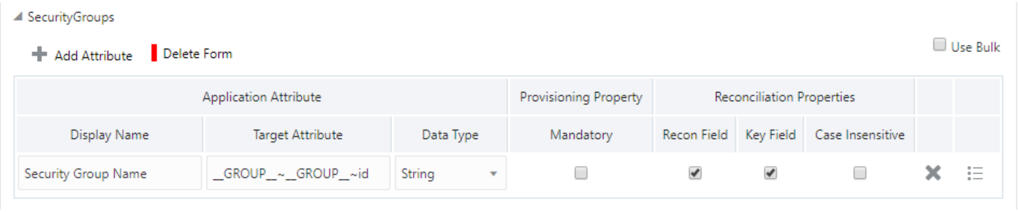
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5   Default Attribute Mappings for Security Groups Forms

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive ?
Security Group Name	__GROUP__~__GROUP__~id	String	No	Yes	Yes	No

Figure 3-3 shows the default attribute security groups mapping.

Figure 3-3   Default Attribute Mappings for Security Groups



◢ SecurityGroups

➕ Add Attribute ▌Delete Form ☐ Use Bulk

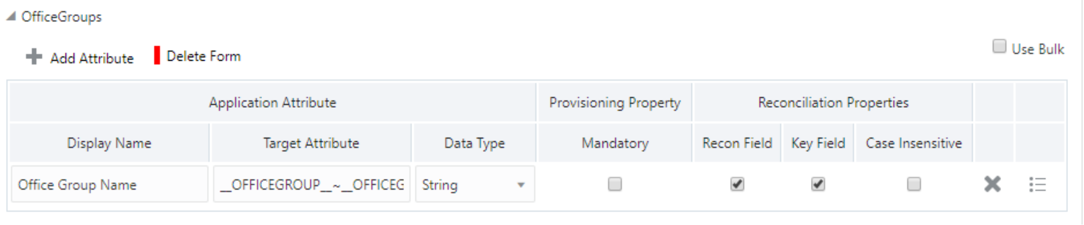
Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Security Group Name	_GROUP_~_GROUP_~id	String ▾	☐	☑	☑	☐	✖	☰

Table 3-6   Default Attribute Mappings for Office Groups Forms

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Office Group Name	__OFFICEGROUP__~__OFFICEGROUP__~id	String	No	Yes	Yes	No

Figure 3-4 shows the default attribute office groups mapping.

Figure 3-4   Default Attribute Mappings for Office Groups



Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Office Group Name	_OFFICEGROUP__~__OFFICEG	String	□	☑	☑	□	✖	☰

Licenses Entitlement

Table 3-7 lists the license attribute mappings between the process form fields in Oracle Identity Governance and Azure AD 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.

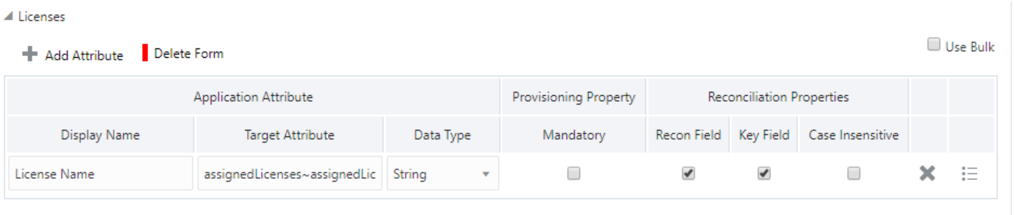
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-7   Default Attribute Mappings for Licenses

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
License Name	assignedLicenses~assignedLicenses~skuId	String	No	Yes	Yes	No

Figure 3-5 shows the default attribute licenses mapping.

Figure 3-5   Default Attribute Mappings for Licenses



Licenses

Add Attribute   Delete Form   □ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
License Name	assignedLicenses~assignedLic	String	□	☑	☑	□	✖	☰

3.3.2 Attribute Mappings for the Authoritative Application

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

Table 3-8 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Azure AD Authoritative application attributes. The table also lists the data type for a given attribute and specified whether it is a mandatory attribute for reconciliation.

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

You may use the default schema that has been set for you or update and change it before continuing to the next step.

The Organization Name, Xellerate Type, and Role identity attributes are mandatory fields on the OIG User form. They cannot be left blank during reconciliation. The target attribute mappings for these identity attributes are empty by default because there are no corresponding columns in the target system. Therefore, the connector provides default values (as listed in the Table 3-8) that it can use during reconciliation. For example, the default target attribute value for the Organization Name attribute is Xellerate Users. This implies that the connector reconciles all target system user accounts into the Xellerate Users organization in Oracle Identity Governance. Similarly, the default attribute value for Xellerate Type attribute is End-User, which implies that all reconciled user records are marked as end users.

Table 3-8   Default Attributes for Azure AD Authoritative Application

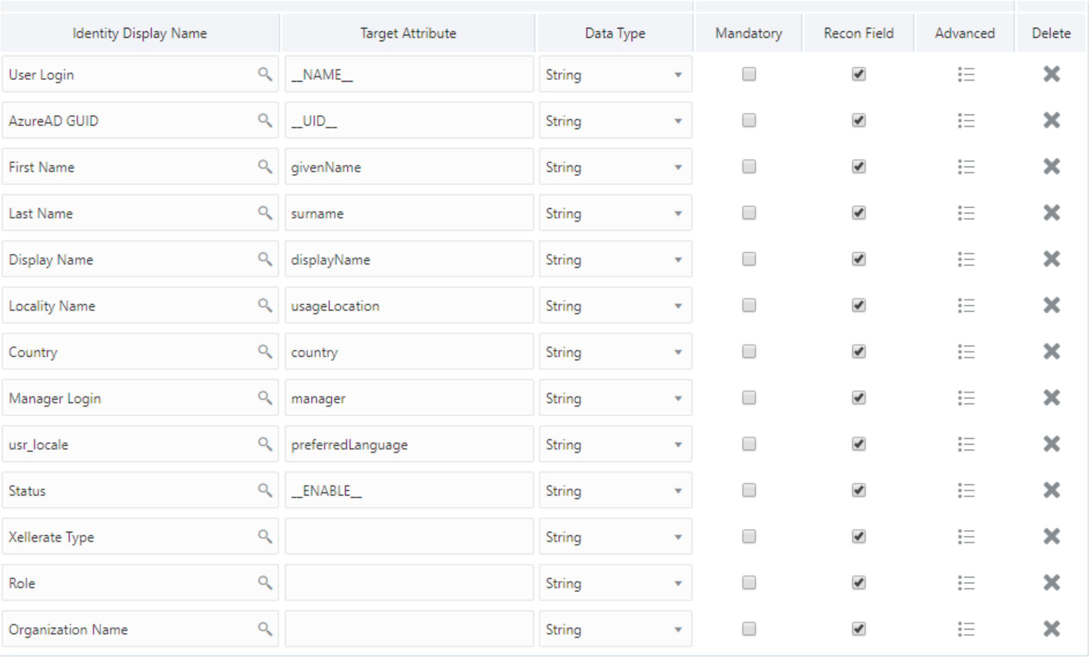
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Advanced Flag Settings	Default Value for Identity Display Name
User Login	__NAME__	String	No	Yes	Yes	NA
Office365 GUID	__UID__	String	No	Yes	Yes	NA
First Name	givenName	String	No	Yes	Yes	NA
Last Name	surname	String	No	Yes	Yes	NA

Table 3-8 (Cont.) Default Attributes for Azure AD Authoritative Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Advanced Flag Settings	Default Value for Identity Display Name
Display Name	displayName	String	No	Yes	Yes	NA
Locality Name	usageLocation	String	No	Yes	Yes	NA
Country	country	String	No	Yes	Yes	NA
Manager Login	manager	String	No	Yes	Yes	NA
usr_locale	preferredLanguage	String	No	Yes	Yes	NA
Xellerate Type		String	No	Yes	Yes	End-User
Role		String	No	Yes	Yes	Full-Time
Organization Name		String	No	Yes	Yes	Xellerate Users
Status	__ENABLE__	String	No	Yes	Yes	NA

Figure 3-6 shows the default User account attribute mappings.

Figure 3-6 Default Attributes for Azure AD Authoritative Application



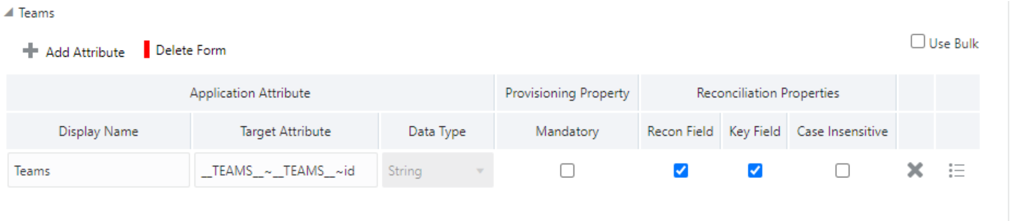
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
User Login	__NAME__	String	□	☑	☰	✖
AzureAD GUID	__UID__	String	□	☑	☰	✖
First Name	givenName	String	□	☑	☰	✖
Last Name	surname	String	□	☑	☰	✖
Display Name	displayName	String	□	☑	☰	✖
Locality Name	usageLocation	String	□	☑	☰	✖
Country	country	String	□	☑	☰	✖
Manager Login	manager	String	□	☑	☰	✖
usr_locale	preferredLanguage	String	□	☑	☰	✖
Status	__ENABLE__	String	□	☑	☰	✖
Xellerate Type		String	□	☑	☰	✖
Role		String	□	☑	☰	✖
Organization Name		String	□	☑	☰	✖

3.3.3 MS Teams Management

The Default Attribute Mappings for Teams lists the MS Teams attribute mappings between the process form fields in Oracle Identity Governance and MS Teams 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 ApplicationCreating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Default Attribute Mappings for MS Teams Group Assignment



◢ Teams

✚ Add Attribute | Delete Form | □ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Teams	__TEAMS__~__TEAMS__~id	String	□	☑	☑	□	✖	☰

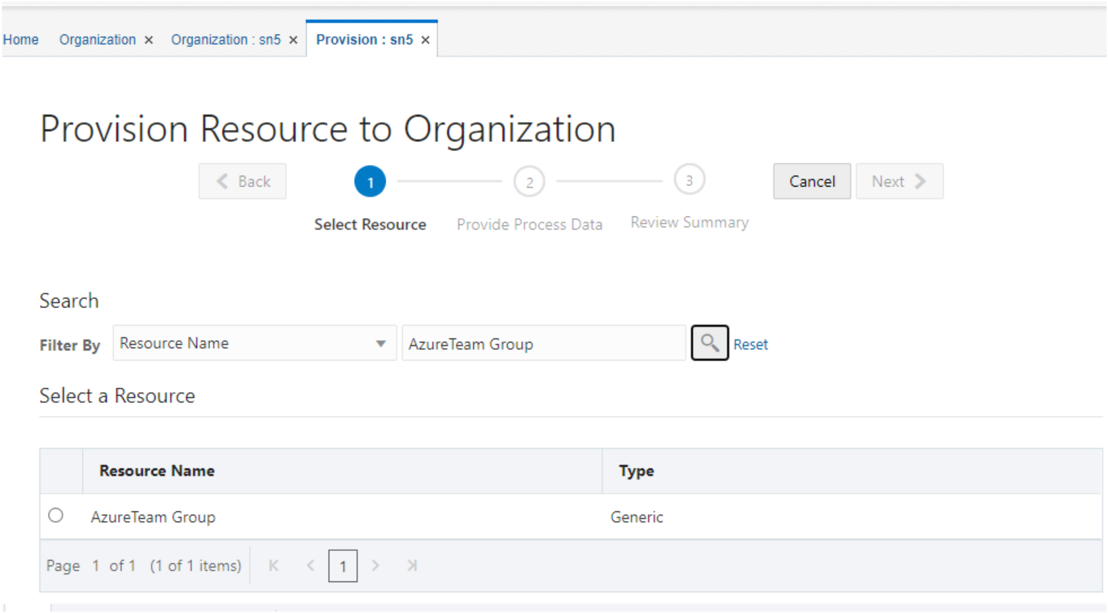
Table 3-9 Default Attribute Mappings for Teams

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Teams	__TEAMS__~__TEAMS__~id	String	No	Yes	Yes	No

Teams Group Assignment

The Provision Resource to Organization figures shows the Microsoft Teams attribute mappings between the process form fields in Oracle Identity Governance and MS Teams target application attributes.

Figure 3-7   Provision Resource to Organization



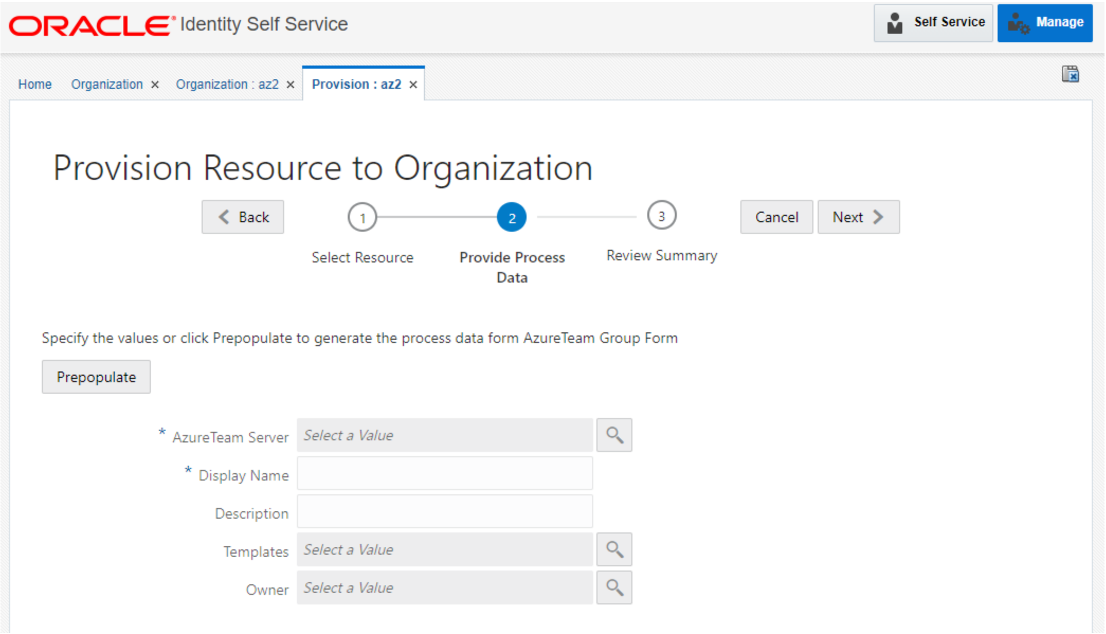
Provision Resource to Organization

Filter By: Resource Name — AzureTeam Group

Select a Resource

	Resource Name	Type
○	AzureTeam Group	Generic

Figure 3-8   Process Data Provision Resource to Organization



Provision Resource to Organization

Specify the values or click Prepopulate to generate the process data form AzureTeam Group Form

* AzureTeam Server	Select a Value
* Display Name	
Description	
Templates	Select a Value
Owner	Select a Value

3.4 Correlation Rules

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

- Correlation Rules for the Target Application

- Correlation Rules for the Authoritative 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 Azure AD 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 3-10 lists the default simple correlation rule for an Azure AD connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-10 Predefined Identity Correlation Rule for an Azure AD Connector

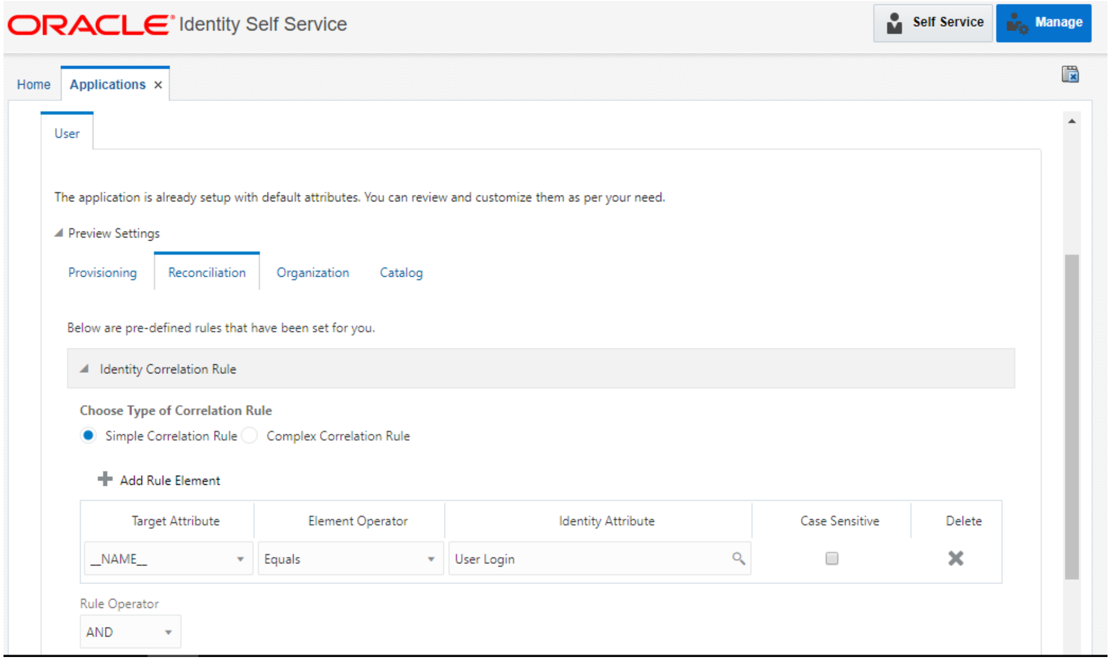
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

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 an Azure AD target application.

Figure 3-9 Simple Correlation Rule for an Azure AD Target Application



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

Preview Settings

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

Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

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

Rule Operator: AND

Predefined Situations and Responses

The Azure AD 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.

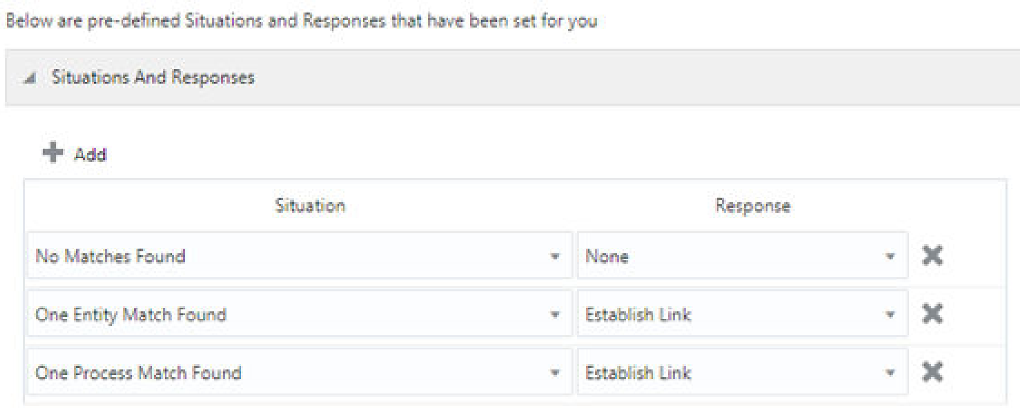
Table 3-11 lists the default situations and responses for an Azure AD Target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-11 Predefined Situations and Responses for an Azure AD Target Application

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

Figure 3-10 shows the situations and responses for an Azure AD that the connector provides by default.

Figure 3-10 Predefined Situations and Responses for an Azure AD Target Application



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

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

3.4.2 Correlation Rules for the Authoritative Application

When you create an authoritative application, the connector uses correlation rules to determine the identity that must be reconciled into Oracle Identity Governance.

Predefined Identity Correlation Rules

By default, the Azure AD connector provides a simple correlation rule when you create an authoritative 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 3-12 lists the default simple correlation rule for an Azure AD connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-12 Predefined Identity Correlation Rule for an Azure AD Authoritative Application

Authoritative Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No
UID	Equals	AzuzreAD GUID	No

Correlation Rule element: (__NAME__Equals __User Login) OR (_UID_Equals AzuzreAD GUID)

In the first correlation rule element:

- User Login is the User ID field of the OIM User form.
- __NAME__ is the unique login name of a user.

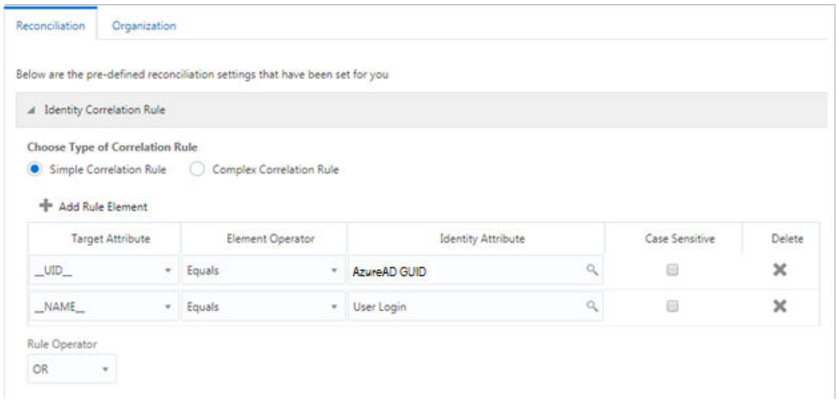
In the second correlation rule element:

- AzuzreAD GUID is a UDF (user defined field) for mapping target object ID with an OIM user.
- _UID_ is the Object Id for an AzuzreAD user.

Rule operator: OR

Figure 3-11 shows the simple correlation rule for an Azure AD Authoritative application.

Figure 3-11   Simple Correlation Rule for an Azure AD Authoritative Application



Reconciliation | Organization

Below are the pre-defined reconciliation settings that have been set for you

Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

Add Rule Element

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
UID	Equals	AzureAD GUID	□	✕
NAME	Equals	User Login	□	✕

Rule Operator

OR

Predefined Situations and Responses

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

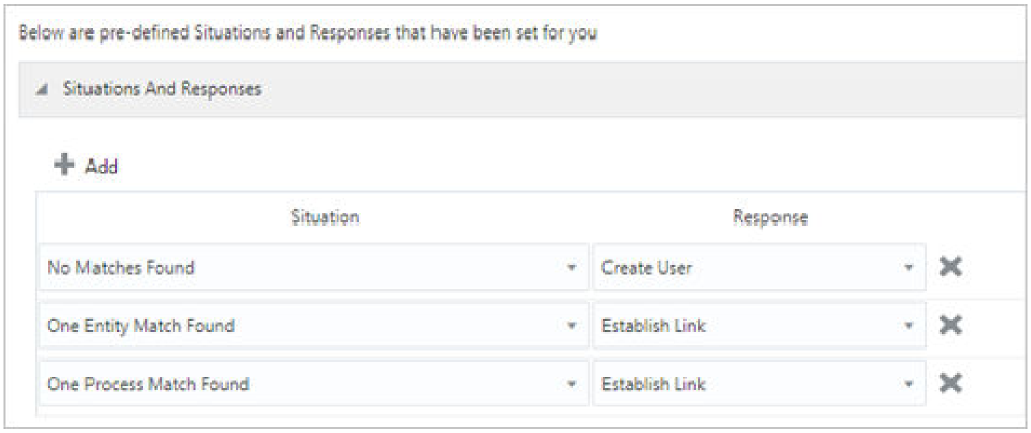
Table 3-13 lists the default situations and responses for an Azure AD Authoritative Application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.*

Table 3-13   Predefined Situations and Responses for an Azure AD Authoritative Application

Situation	Response
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Figure 3-12 shows the situations and responses for an Azure AD that the connector provides by default.

Figure 3-12   Simple Correlation Rule for an Azure AD Authoritative Application



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

Situations And Responses

Situation	Response
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

3.5 Reconciliation Jobs

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

User Reconciliation Jobs

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

The following reconciliation jobs are available for reconciling user data:

- Azure AD Full User Reconciliation: Use this reconciliation job to reconcile user data from a target application.
- Azure AD User Trusted Reconciliation: Use this reconciliation job to reconcile user data from an authoritative application.

Table 3-14 describes the parameters of the Azure AD Full User Reconciliation job.

Table 3-14   Parameters of the Azure AD 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 3-14   (Cont.) Parameters of the Azure AD Full User Reconciliation Job

Parameter	Description
Latest Token	This parameter holds the value of the target system attribute that is specified as the value of the Incremental Recon Attribute parameter. The Latest Token parameter is used for internal purposes. By default, this value is empty. **Note**: Do not enter a value for this parameter. The reconciliation engine automatically enters a value in this parameter. **Sample value**: `<String>2017-11-30T04:44:29Z</String>`
Object Type	This parameter holds the name of the object type for the reconciliation run. **Default value**: `User` Do *not* change the default value.
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. **Sample value when incremental recon is enabled**: `$filter=startswith(displayName,'user1')` **Sample value when incremental recon is not enabled**: `&$filter=startswith(displayName,'user1')` For more information about creating filters, see Performing Limited Reconciliation .
Scheduled Task Name	Name of the scheduled task used for reconciliation. Do *not* modify the value of this parameter.
Incremental Recon Attribute	Enter the name of the attribute that holds the timestamp at which the token record was modified.

Table 3-15 describes the parameters of Azure AD User Trusted Reconciliation job.

Table 3-15   Parameters of the Azure AD User Trusted Reconciliation Job

Parameter	Description
Application name	Name of the AOB Application with which the 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* modify this value.

Table 3-15 (Cont.) Parameters of the Azure AD User Trusted Reconciliation Job

Parameter	Description
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. **Sample value**: `$filter=startswith(displayName,'user1')` For more information about creating filters, see Performing Limited Reconciliation .
Incremental Recon Attribute	Attribute that holds the timestamp at which the token record was modified.
Latest Token	This parameter holds the value of the attribute that is specified as the value of the Incremental Recon Attribute attribute. The Latest Token parameter is used for internal purposes. By default, this value is empty. **Note:** If an appropriate Increment Recon attribute has been specified, then do not enter a value for this parameter. Sample value: `<String>2017-11-30T04:44:29Z</String>`
Object Type	This parameter holds the name of the object type for the reconciliation run. Default value: `User` **Note:** 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 Azure AD User Target Delete Recon job is used to reconcile data about deleted users from a target application. During a reconciliation run, for each deleted user account on the target system, the Azure AD resource is revoked for the corresponding OIM User.

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

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.

Table 3-16 (Cont.) Parameters of the AzureAD Target User Delete Reconciliation Job

Parameter	Description
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.

Trusted Delete User Reconciliation Job

The Azure AD User Trusted Delete Recon job is used to reconcile data about deleted users from an Authoritative application. During a reconciliation run, for each deleted target system user account, the corresponding OIM User is deleted.

Table 3-17 Parameters of the AzureAD Trusted 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:

- AzureAD Office Groups Lookup Reconciliation
- AzureAD Security Groups Lookup Reconciliation
- AzureAD Licenses Lookup Reconciliation
- AzureAD Roles Lookup Reconciliation
- AzureAD Manager Lookup Reconciliation
- AzureADTeams Lookup Reconciliation

> **Note:**
>
> The Teams support is applicable from 12.2.1.3.0B

The parameters for all the reconciliation jobs are the same.

Table 3-18   Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Current AOB application name with which the reconciliation job is associated. Default value: `AzureAD` 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 AzureAD Office Groups Lookup Reconciliation: `Lookup.AzureAD.OfficeGroups` • For AzureAD Security Groups Lookup Reconciliation: `Lookup.AzureAD.SecurityGroups` • For Azure AD Licenses Lookup Reconciliation: `Lookup.AzureAD.Licenses` • For Azure AD Roles Lookup Reconciliation: `Lookup.AzureAD.Roles` • For Azure AD Manager Lookup Reconciliation: `Lookup.AzureAD.Manager` • ForAzure AD Teams Lookup Reconciliation: Lookup.Teams.TeamsGroup **Note:** The Teams support is applicable from 12.2.1.3.0B. 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.

Table 3-18 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
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 Azure AD Office Groups Lookup Reconciliation: `__OFFICEGROUP__` • For Azure AD Security Groups Lookup Reconciliation: `__GROUP__` • For Azure AD Licenses Lookup Reconciliation: `__LICENSE__` • For Azure AD Roles Lookup Reconciliation: `__ROLE__` • For Azure AD Manager Lookup Reconciliation: `__USER__` • ForAzure AD Teams Lookup Reconciliation: __TEAMS__ **Note**: Do not change the value of this parameter. The Teams support is applicable from 12.2.1.3.0B.

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 Manager 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 Manager 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 Manager to continue running.
- WARNING

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

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

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

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

These message types are mapped to ODL message type and level combinations as shown in the below table.

Table 4-1   Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path: `DOMAIN_HOME/config/fmwconfig/servers/OIM_SERVER/logging.xml`

Here, `DOMAIN_HOME` and `OIM_SEVER` are the domain name and server name specified during the installation of Oracle Identity Manager.

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='AzureAD-handler'
level='[LOG_LEVEL]'class='oracle.core.ojdl.logging.ODLHandlerFactory'>

    <property name='logreader:' value='off'/>
    <property name='path' value='[FILE_NAME]'/>
    <property name='format' value='ODL-Text'/>
    <property name='useThreadName' value='true'/>
    <property name='locale' value='en'/>
    <property name='maxFileSize' value='5242880'/>
    <property name='maxLogSize' value='52428800'/>
    <property name='encoding' value='UTF-8'/>
</log_handler>


<logger name="ORG.IDENTITYCONNECTORS.GENERICREST" level="[LOG_LEVEL]"
useParentHandlers="false">
    <handler name="AzureAD-handler"/>
    <handler name="console-handler"/>
</logger>


<logger name="ORG.IDENTITYCONNECTORS.RESTCOMMON" level="[LOG_LEVEL]"
useParentHandlers="false">
    <handler name="AzureAD-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='AzureAD-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.GENERICREST"
level="NOTIFICATION:1" useParentHandlers="false">
    <handler name="AzureAD-handler"/>
    <handler name="console-handler"/>
</logger>
```

```
<logger name="ORG.IDENTITYCONNECTORS.RESTCOMMON"
level="NOTIFICATION:1" useParentHandlers="false">
    <handler name="AzureAD-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, the connector creates a default IT resource for the Connector Server. The name of this default IT resource is `AzureAD Connector Server`.

In Oracle Identity System Administration, search for and edit the AzureAD Connector Server IT resource to specify values for the parameters of IT resource for the Connector Server listed in the below table. For more information about searching for IT resources and updating its parameters, see Managing IT Resources in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

Table 4-2 Parameters of the IT Resource for the Azure AD 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)

Table 4-2   (Cont.) Parameters of the IT Resource for the Azure AD Connector Server

Parameter	Description
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 SSL for Java Connector Server 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 AzureAD Application instance. The original code is:

```
 <trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.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.Az
ureADFormEO.UD_USER_PRINCIPAL_NAME __c_LABEL"><source>First
Name</source><target/>
</trans-unit>
```

d. Open the resource file from the connector package, for example AzureActiveDirectory_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.AzureAD.entit
y 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 Azure AD 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 Azure AD.
2. Copy the public key certificate of Azure AD 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
   ```

   The following are sample values for this command:

   -
     ```
     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.

- Configuring Reconciliation
- Configuring Reconciliation Jobs
- Configuring Provisioning
- Connector Objects Used for Groups Management
- Uninstalling the Connector

5.1 Configuring Reconciliation

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

This section discusses the following topics related to configuring reconciliation:

- Performing Full Reconciliation and Incremental Reconciliation
- Performing Limited Reconciliation

5.1.1 Performing Full Reconciliation and Incremental 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 Latest Token and Filter suffix parameters and run one of the reconciliation jobs listed in the Reconciliation Jobs section.

In the Azure AD connector, the incremental reconciliation option is not enabled by default. The connector supports incremental reconciliation only if the target system contains an attribute that holds the timestamp at which an object is created or modified.

Configuring Incremental Reconciliation

If you want to perform incremental reconciliation runs, then configure incremental reconciliation as follows:

> **Note:**
>
> In the Azure AD connector, the incremental reconciliation option is not enabled by default. The connector supports incremental reconciliation only if the target system contains an attribute that holds the timestamp at which an object is created or modified.
>
> For example, consider `lastDirSyncTime` as a sample `Incremental Recon Attribute` that you specify for the AzureAD User Reconciliation Scheduled job. After the first full reconciliation run, the connector populates the `Latest Token` parameter with a timestamp. In subsequent reconciliation runs, the connector fetches only the user records that are created or updated after the `Latest Token` timestamp.

1. Before running an incremental reconciliation job, first run a full Trusted/Target User Reconciliation job and configure the value of `Incremental Recon Attribute` as `lastDirSyncTime`.

   > **Note:**
   >
   > The `lastDirSyncTime` is a sample attribute. This attribute name may be different in your production instance.

2. After a successful reconciliation job run, the `Latest Token` attribute gets updated.

   Sample latest token value: `<String>2020-05-06T17:27:34Z</String>`

3. Open Identity Self-Service application.
4. Click **Manage**.
5. Click **Application**.
6. Search and open the application you have created.
7. Expand the **Advanced Settings** option and modify the value of `relURIs` as per your requirement.
   - To support Incremental Reconciliation for both Users and Groups, perform step 8.
   - To support Incremental Reconciliation only for Users, perform step 9.
8. To use both User and Group Reconciliation jobs, modify relURIs as follows:
   - For **Authoritative Application**, modify `relURIs` as:

     ```
     "__ACCOUNT__.CREATEOP=/$(api_version)$/
     users?","__ACCOUNT__.UPDATEOP=/$(api_version)$/users/$
     (__UID__)$","__ACCOUNT__.SEARCHOP=/$(api_version)$/users?$filter=$
     (Incremental Recon Attribute)$+ge+$(Latest
     Token)$&$select=assignedLicenses,displayName,userType,givenName,use
     rPrincipalName,id,$(Incremental Recon
     Attribute)$,city,usageLocation,accountEnabled,mailNickname,country&
     $top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__=/$
     (api_version)$/users/$
     (__UID__)$?$select=displayName,givenName,userPrincipalName,id,prefe
     ```

```
rredLanguage,usageLocation,accountEnabled,surname,country","__ACCOUNT__.m
anager.SEARCHOP=/$(api_version)$/users/$(__UID__)$/
manager","__ACCOUNT__.manager=/$(api_version)$/users/$(__UID__)$/
manager/$ref"
```

- For **Target Application**, modify `relURIs` as:

```
"__ACCOUNT__.CREATEOP=/$
(api_version)$/users?","__ACCOUNT__.UPDATEOP=/$(api_version)$/users/$
(__UID__)$","__ACCOUNT__.SEARCHOP=/$(api_version)$/users?$filter=$
(Incremental Recon Attribute)$+ge+$(Latest
Token)$&$select=assignedLicenses,displayName,userType,givenName,userPrinc
ipalName,id,$(Incremental Recon
Attribute)$,city,usageLocation,accountEnabled,mailNickname,country&$top=$
(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__=/$(api_version)$/
users/$
(__UID__)$?$select=assignedLicenses,displayName,givenName,userPrincipalNa
me,id,createdDateTime,city,usageLocation,accountEnabled,mailNickname,coun
try","__ACCOUNT__.manager.SEARCHOP=/$(api_version)$/users/$(__UID__)$/
manager","__ACCOUNT__.manager=/$(api_version)$/users/$(__UID__)$/
manager/$ref","__ACCOUNT__.__GROUP__.SEARCHOP=/$(api_version)$/users/$
(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$
(PAGE_TOKEN)$","__ACCOUNT__.__GROUP__.DELETEOP=/$(api_version)$/groups/$
(__GROUP__.id)$/members/$(__UID__)$/$ref","__ACCOUNT__.__GROUP__=/$
(api_version)$/groups/$(__GROUP__.id)$/
members/$ref","__GROUP__.CREATEOP=/$(api_version)$/
groups","__GROUP__.UPDATEOP=/$(api_version)$/groups/$
(__UID__)$","__GROUP__.SEARCHOP=/$(api_version)$/groups?
&$filter=securityEnabled+eq+true+and+(Incremental Recon Attribute)$+ge+$
(Latest Token)$&$top=$(PAGE_SIZE)$&$skiptoken=$
(PAGE_TOKEN)$","__OFFICEGROUP__.SEARCHOP=/$(api_version)$/groups?
&$filter=securityEnabled+eq+false+and+(Incremental Recon Attribute)$+ge+$
(Latest Token)$&$top=$(PAGE_SIZE)$&$skiptoken=$
(PAGE_TOKEN)$","__GROUP__=/$(api_version)$/groups/$
(__UID__)$","__GROUP__.member=/$(api_version)$/groups/$(__UID__)$/
members/$ref?","__ROLE__.SEARCHOP=/$(api_version)$/directoryRoles?/$
(Filter Suffix)$","__ACCOUNT__.__ROLE__=/$(api_version)$/directoryRoles/$
(__ROLE__.id)$/members/$ref","__ACCOUNT__.__ROLE__.DELETEOP=/$
(api_version)$/directoryRoles/$(__ROLE__.id)$/members/$
(__UID__)$/$ref","__ROLE__.member=/$(api_version)$/directoryRoles/$
(__UID__)$/members/$ref","__ACCOUNT__.__ROLE__.SEARCHOP=/$(api_version)$/
users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$
(PAGE_TOKEN)$","assignedLicenses.SEARCHOP=/$(api_version)$/
subscribedSkus?/$(Filter
Suffix)$","__ACCOUNT__.assignedLicenses.ADDATTRIBUTE=/$(api_version)$/
users/$(__UID__)$/
assignLicense","__ACCOUNT__.assignedLicenses.REMOVEATTRIBUTE=/$
(api_version)$/users/$(__UID__)$/
assignLicense","__ACCOUNT__.__OFFICEGROUP__=/$(api_version)$/groups/$
(__OFFICEGROUP__.id)$/
members/$ref","__ACCOUNT__.__OFFICEGROUP__.DELETEOP=/$(api_version)$/
groups/$(__OFFICEGROUP__.id)$/members/$
(__UID__)$/$ref","__ACCOUNT__.__OFFICEGROUP__.SEARCHOP=/$(api_version)$/
users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$"
```

9. To use only User Reconciliation jobs, modify relURIs as follows:

- For **Authoritative Application**, modify `relURIs` as: `:"__ACCOUNT__.CREATEOP=/$(api_version)$/users?","__ACCOUNT__.UPDATEOP=/$(api_version)$/users/$(__UID__)$","__ACCOUNT__.SEARCHOP=/$(api_version)$/users?$filter=$(Incremental Recon Attribute)$+ge+$(Latest Token)$&$select=assignedLicenses,displayName,userType,givenName,userPrincipalName,id,$(Incremental Recon Attribute)$,city,usageLocation,accountEnabled,mailNickname,country&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__=/$(api_version)$/users/$(__UID__)$?$select=displayName,givenName,userPrincipalName,id,preferredLanguage,usage`

- For **Target Application**, modify `relURIs` as: `"__ACCOUNT__.CREATEOP=/$(api_version)$/users?","__ACCOUNT__.UPDATEOP=/$(api_version)$/users/$(__UID__)$","__ACCOUNT__.SEARCHOP=/$(api_version)$/users?$filter=$(Incremental Recon Attribute)$+ge+$(Latest Token)$&$select=assignedLicenses,displayName,userType,givenName,userPrincipalName,id,city,$(Incremental Recon Attribute)$,usageLocation,accountEnabled,mailNickname,country&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__=/$(api_version)$/users/$(__UID__)$?$select=assignedLicenses,displayName,givenName,userPrincipalName,id,city,createdDateTime,usageLocation,accountEnabled,mailNickname,country","__ACCOUNT__.manager.SEARCHOP=/$(api_version)$/users/$(__UID__)$/manager","__ACCOUNT__.manager=/$(api_version)$/users/$(__UID__)$/manager/$ref","__ACCOUNT__.__GROUP__.SEARCHOP=/$(api_version)$/users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__.__GROUP__.DELETEOP=/$(api_version)$/groups/$(__GROUP__.id)$/members/$(__UID__)$/$ref","__ACCOUNT__.__GROUP__=/$(api_version)$/groups/$(__GROUP__.id)$/members/$ref","__GROUP__.CREATEOP=/$(api_version)$/groups","__GROUP__.UPDATEOP=/$(api_version)$/groups/$(__UID__)$","__GROUP__.SEARCHOP=/$(api_version)$/groups?&$filter=securityEnabled+eq+true&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__OFFICEGROUP__.SEARCHOP=/$(api_version)$/groups?&$filter=securityEnabled+eq+false&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__GROUP__=/$(api_version)$/groups/$(__UID__)$","__GROUP__.member=/$(api_version)$/groups/$(__UID__)$/members/$ref?","__ROLE__.SEARCHOP=/$(api_version)$/directoryRoles?/$(Filter Suffix)$","__ACCOUNT__.__ROLE__=/$(api_version)$/directoryRoles/$(__ROLE__.id)$/members/$ref","__ACCOUNT__.__ROLE__.DELETEOP=/$(api_version)$/directoryRoles/$(__ROLE__.id)$/members/$(__UID__)$/$ref","__ROLE__.member=/$(api_version)$/directoryRoles/$(__UID__)$/members/$ref","__ACCOUNT__.__ROLE__.SEARCHOP=/$(api_version)$/users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","assignedLicenses.SEARCHOP=/$(api_version)$/subscribedSkus?/$(Filter Suffix)$","__ACCOUNT__.assignedLicenses.ADDATTRIBUTE=/$(api_version)$/users/$(__UID__)$/assignLicense","__ACCOUNT__.assignedLicenses.REMOVEATTRIBUTE=/$(api_version)$/users/$(__UID__)$/`

```
assignLicense","__ACCOUNT__.__OFFICEGROUP__=/$(api_version)$/groups/$
(__OFFICEGROUP__.id)$/
members/$ref","__ACCOUNT__.__OFFICEGROUP__.DELETEOP=/$(api_version)$/
groups/$(__OFFICEGROUP__.id)$/members/$
(__UID__)$/$ref","__ACCOUNT__.__OFFICEGROUP__.SEARCHOP=/$(api_version)$/
users/$(__UID__)$/memberOf?&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$"
Location,accountEnabled,surname,country","__ACCOUNT__.manager.SEARCHOP=/$
(api_version)$/users/$(__UID__)$/manager","__ACCOUNT__.manager=/$
(api_version)$/users/$(__UID__)$/manager/$ref"
```

10. Run the user reconciliation scheduled job to perform incremental reconciliation. The connector only fetches records created or modified after the time stamp (populated in the Latest Token attribute).

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 1.6 is as follows:

Filter Suffix value : `&$filter=startswith(displayName,'john.doe')`

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.

Note:

Specify a value for the Filter Suffix attribute in a format that is supported by the Azure AD APIs you are using.

For example:

- If you have configured incremental reconciliation and you are using version 1.6 of the API, then set a value for the Filter Suffix attribute in the following format:

  Sample Filter Suffix for API version 1.6:
  `%20and%20startswith(displayName,'user1')`

- If you have *not* configured incremental reconciliation and you are using version 1.6 of the API, then set a value for the Filter Suffix attribute in the following format:

  Sample Filter Suffix for API version 1.6:
  `&$filter=startswith(displayName,'user1')`

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 Azure AD 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.

- For a Create User provisioning operation, you must specify a value for the User Principal Name field along with the domain name. For example, jdoe@example.com, it is mandatory field, other mandatory fields are Display Name, Password, MailNickname, and Usage Location.
- During a group provisioning operation you must enter a value for the DisplayName and MailNickname fields. The value in the MailNickname field should not include spaces.

5.3.2 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance:

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

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

5.4 Connector Objects Used for Groups Management

Learn about the objects that are used by the connector to perform group management operations such as create and delete.

- Lookup Definitions for Groups Management
- Reconciliation Rules and Action Rules for Groups Management
- Reconciliation Scheduled Jobs for Groups Management

5.4.1 Lookup Definitions for Groups Management

The lookup definitions for Groups are automatically created in Oracle Identity Governance after you create the application by using the connector.

- Lookup.AzureAD.GM.Configuration
- Lookup.AzureAD.GM.ProvAttrMap
- Lookup.AzureAD.GM.ReconAttrMap

5.4.1.1 Lookup.AzureAD.GM.Configuration

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

Table 5-1 Entries in the Lookup.AzureAD.GM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.AzureAD.GM.ProvAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Governance and the target system. This lookup definition is used during provisioning operations.
Recon Attribute Map	Lookup.AzureAD.GM.ReconAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Governance and the target system. This lookup definition is used during reconciliation.

5.4.1.2 Lookup.AzureAD.GM.ProvAttrMap

Lookup.AzureAD.GM.ProvAttrMap lookup definition holds mappings between process form fields (Code Key values) and target system attributes (Decode). This lookup definition is preconfigured and is used during group provisioning operations.

Table 5-2 Entries in the Lookup.AzureAD.GM.ProvAttrMap Lookup Definition

Group Field on Oracle Identity Governance	AzureAD Field
ObjectId	__UID__
Description	description
Mail Enabled	mailEnabled
Mail Nickname	mailNickname
Display Name	__NAME__
Security Enabled	securityEnabled

5.4.1.3 Lookup.AzureAD.GM.ReconAttrMap

The Lookup.AzureAD.GM.ReconAttrMap lookup definition holds mappings between resource object fields (Code Key values) and target system attributes (Decode). This lookup definition is preconfigured and is used during target resource group reconciliation runs.

Table 5-3 Entries in the Lookup.AzureAD.GM.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Governance	AzureAD Field
ObjectId	__UID__
Description	description
Mail Enabled	mailEnabled=”${mailEnabled}”
Mail Nickname	mailNickname
Display Name	__NAME__
Security Enabled	securityEnabled="${securityEnabled}"
OIM Org Name	OIM Organization Name **Note**: This is a connector attribute. The value of this attribute is used internally by the connector to specify the organization of the groups in Oracle Identity Governance.

5.4.2 Reconciliation Rules and Action Rules for Groups Management

Reconciliation rules are used by the reconciliation engine to determine the identity to which Oracle Identity Governance must assign a newly discovered account on the target system. Reconciliation action rules define that actions the connector must perform based on the reconciliation rules.

- Reconciliation Rule for Groups
- Reconciliation Action Rules for Groups
- Viewing Reconciliation Rules
- Viewing Reconciliation Action Rules

5.4.2.1 Reconciliation Rule for Groups

The following is the process-matching rule for groups:

Rule name: AzureAD Groups Recon Rule

Rule element: Organization Name Equals OIM Org Name

In this rule element:

- Organization Name is the Organization Name field of the OIM User form.
- OIM Org Name is the organization name of the groups in Oracle Identity Governance. OIM Org Name is the value specified in the Organization Name attribute of the AzureAD Group Recon scheduled job.

5.4.2.2 Reconciliation Action Rules for Groups

Table 5-4 lists the action rules for groups reconciliation.

Table 5-4 Action Rules for Groups Reconciliation

Rule Condition	Action
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

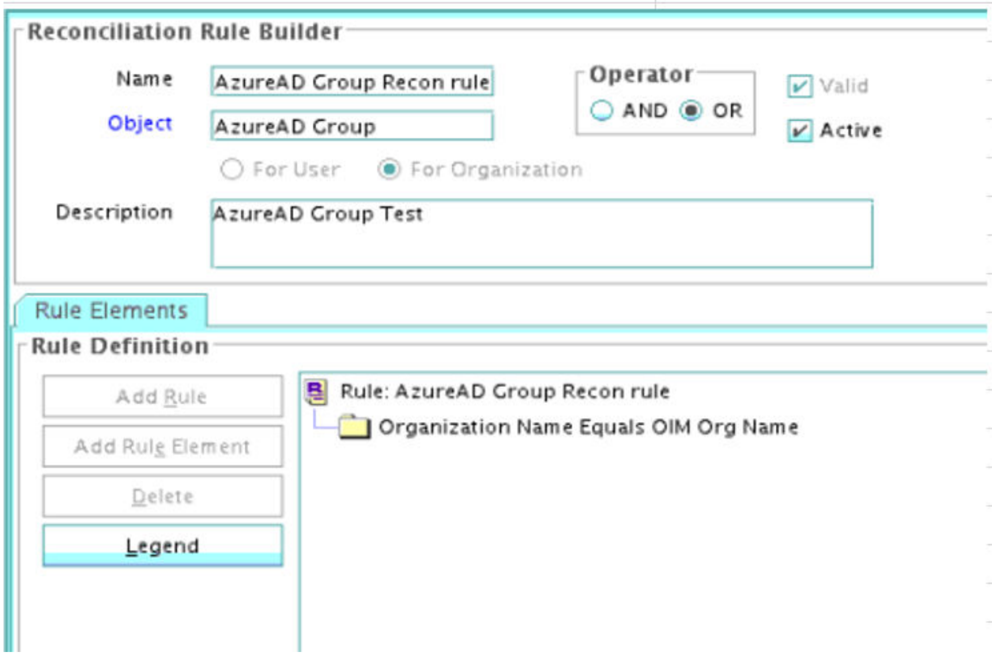
5.4.2.3 Viewing Reconciliation Rules

After you create the application by using the connector, you can view the reconciliation rule by performing the following steps:

1. Log in to the Oracle Identity Governance Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for the **AzureAD Groups Recon Rule** rule.

   Figure 5-1 shows the reconciliation rule for groups.

Figure 5-1   Reconciliation Rule for Groups



Reconciliation Rule Builder

Name: AzureAD Group Recon rule

Object: AzureAD Group

Operator: ○ AND ● OR

☑ Valid

☑ Active

○ For User ● For Organization

Description: AzureAD Group Test

Rule Elements

Rule Definition

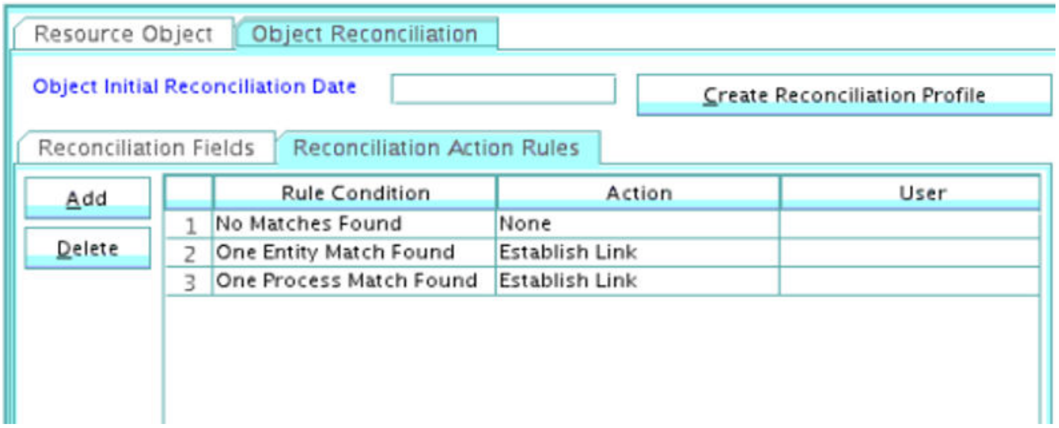
Rule: AzureAD Group Recon rule
Organization Name Equals OIM Org Name

5.4.2.4 Viewing Reconciliation Action Rules

After you create the application by using connector, you can view the reconciliation action rules for groups by performing the following steps:

1. Log in to the Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. Search for and open the **AzureAD Group** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 5-2 shows the reconciliation action rules for groups.

Figure 5-2   Reconciliation Action Rules for Groups



Object Initial Reconciliation Date:

	Rule Condition	Action	User
1	No Matches Found	None	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

5.4.3 Reconciliation Scheduled Jobs for Groups Management

After you create an application, reconciliation scheduled jobs are automatically created in Oracle Identity Governance. You must configure these scheduled jobs to suit your requirements by specifying values for its attributes.

You must specify values for the attributes for Azure AD Group Recon. Table 5-5 describes the attributes of the AzureAD Group Reconciliation job.

Table 5-5 Attributes of the AzureAD Group Reconciliation Job

Attribute	Description
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: `Group` **Note:** Do not change the default value.
Incremental Recon Attribute	Attribute that holds the timestamp at which the token record was modified.
OIM Organization Name	Enter the name of the Oracle Identity Governance organization in which reconciled groups must be created or updated.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `AzureAD`
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: `AzureAD Group` **Note:** Do not change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: `Azure Group Recon` Do *not* modify the value of this attribute.

5.5 Uninstalling the Connector

Uninstalling the Azure AD 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: `AzureAD User; AzureAD 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 Tenants

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

6.2 Configuring Action Scripts

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

These scripts can be configured to run before or after the create, update, or delete an account provisioning 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*.

6.3 Configuring the Connector for Multiple Tenants

You must clone the application of your base application to configure it for multiple tenants.

The following example illustrates this requirement:
XYZ corporation has multiple tenants including an independent schema. To meet the requirement posed by such a scenario, you must clone your application which copies all configurations of the base application into the cloned application. For more information about cloning applications, see Cloning Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

7 Troubleshooting the Connector

This is a solution to a problem you might encounter while using the Azure Active Directory connector.

Table 7-1 Troubleshooting the Azure AD Connector

Problem	Solution
OIG Users are not created after running the Azure Active Directory User Trusted Recon scheduled job. The following message is displayed In the reconciliation event generated for the user: `'Data Validation Failed' as the current status and 'Invalid ManagerLogin : <Manager ID>' as Note.` **Note**: When you remove a manager from the Azure AD target system, a corresponding event will not be created in Oracle Identity Self Service Console.	This issue is encountered due to the dependency of manager information of users. OIG User creation fails if the manager of the user is not already present in Oracle Identity Governance. To fix this issue, you must remove the manager field mapping, run the Azure Active Directory User Trusted Recon scheduled job, and then add back the manager field mapping as follows: In Identity Self Service, remove the Manager field mapping as follows: 1. Log in to Identity Self Service. 2. Search for and open the Authoritative application corresponding to your target system for editing. For example, search for the **Azure Active Directory** application. 3. From the Schema page, uncheck the **Manager Login** reconciliation mapping. 4. Apply the changes. Run the Azure Active Directory User Trusted Recon scheduled job. In Identity Self Service, add the manager field mapping as follows: 1. Log in to Identity Self Service. 2. Search for and open the Authoritative application corresponding to your target system for editing. For example, search for the **Azure Active Directory** application. 3. From the Schema page, select the **Manager Login** reconciliation mapping checkbox. 4. Apply the changes. Clear the value in the latest token parameter of the Azure Active Directory User Trusted Recon scheduled job and run it.

8

Known Issues and Limitations

This is a known issues and limitation associated with the Azure Active Directory connector.

Preconfig XML file does not get imported as expected when another generic connector is already installed

If you are creating the Azure AD connector application in a scenario when another generic connector is already installed or created, then the xml/AzureActiveDirectory-preconfig.xml file will not get imported as expected.

Workaround: As a workaround, perform the Deployment Manager import.

Note: Verify prepopulation status of the static lookup definition. If the lookup data is not getting populated, you must import the xml/AzureActiveDirectory-preconfig.xml pre config XML file manually. For example, Lookup.AzureAD.Languages.

A

Files and Directories in the Connector Installation Package

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

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

File in the Installation Package	Description
bundle/ org.identityconnectors.genericrest-12.3.0.jar	This JAR is the ICF connector bundle. **Note**: If you try to install any other generic rest connector like Eloqua on top of the AzureAD connector, then the generic rest bundle jar `org.identityconnectors.genericrest-12.3.0.jar` must be replaced with the latest generic rest jar or replaced with the AzureAD bundle jar.
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/AzureActiveDirectory-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/AzureActiveDirectory-auth-template.xml	This file contains definitions for the connector objects required for creating an Authoritative 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/AzureActiveDirectory-preconfig.xml	This XML file contains definitions for the connector objects associated with any non-User object such as Groups.