

# Oracle® Identity Governance

## Configuring the SharePoint Application



12c (12.2.1.3.0)  
F44394-02

ORACLE®

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

F44394-02

Copyright © 2022, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Preface

---

Audience	ix
Documentation Accessibility	ix
Related Documents	ix
Conventions	ix
Legal Disclaimer	x

## 1 About the SharePoint Connector

---

1.1 Connector Offerings	1-1
1.2 Certified Components for the Microsoft SharePoint Connector	1-2
1.3 Usage Recommendation	1-2
1.4 Certified Languages	1-2
1.5 Supported Connector Operations	1-3
1.6 Connector Architecture	1-4
1.7 Use Cases Supported by the Connector	1-6
1.8 Connector Features	1-7
1.8.1 Full Reconciliation and Incremental Reconciliation	1-7
1.8.2 Limited Reconciliation	1-8
1.8.3 Support for the Connector Server	1-8
1.8.4 Transformation and Validation of Account Data	1-8

## 2 Creating an Application by Using the SharePoint Connector

---

2.1 Process Flow for Creating an Application By Using the Connector	2-1
2.2 Prerequisites for Creating an Application By Using the Connector	2-2
2.2.1 Registering the Client Application	2-2
2.2.2 Downloading the Connector Installation Package	2-4
2.3 Creating an Application By Using the Connector	2-5

## 3 Configuring the Connector

---

3.1 Basic Configuration Parameters	3-1
------------------------------------	-----

3.2	Advanced Setting Parameters	3-6
3.3	Attribute Mappings	3-10
3.3.1	Attribute Mappings for the Target Application	3-10
3.4	Correlation Rules	3-15
3.4.1	Correlation Rules for the Target Application	3-15
3.5	Reconciliation Jobs	3-17

## 4 Performing Postconfiguration Tasks for the SharePoint Connector

---

4.1	Configuring Oracle Identity Manager	4-1
4.1.1	Creating and Activating a Sandbox	4-1
4.1.2	Creating a New UI Form	4-1
4.1.3	Publishing a Sandbox	4-2
4.1.4	Updating an Existing Application Instance with a New Form	4-2
4.2	Harvesting Entitlements and Sync Catalog	4-3
4.3	Managing Logging for the Connector	4-3
4.3.1	Understanding Log Levels	4-3
4.3.2	Enabling Logging	4-4
4.4	Configuring the IT Resource for the Connector Server	4-5
4.5	Localizing Field Labels in UI Forms	4-6
4.6	Configuring SSL	4-8

## 5 Using the Connector

---

5.1	Configuring Reconciliation	5-1
5.1.1	Performing Full Reconciliation and Incremental Reconciliation	5-1
5.1.2	Performing Limited Reconciliation	5-1
5.2	Configuring Reconciliation Jobs	5-2
5.3	Configuring Provisioning	5-3
5.3.1	Guidelines on Performing Provisioning Operations	5-3
5.3.2	Performing Provisioning Operations	5-3
5.4	Connector Objects Used for Groups Management	5-4
5.4.1	Lookup Definitions for Groups Management	5-4
5.4.1.1	Lookup.SharePointOnline.GM.Configuration	5-4
5.4.1.2	Lookup.SharePointOnline.GM.ProvAttrMap	5-5
5.4.1.3	Lookup.SharePointOnline.GM.ReconAttrMap	5-5
5.4.2	Reconciliation Rules and Action Rules for Groups Management	5-6
5.4.2.1	Reconciliation Rule for Groups	5-6
5.4.2.2	Reconciliation Action Rules for Groups	5-6
5.4.2.3	Viewing Reconciliation Rules	5-6
5.4.2.4	Viewing Reconciliation Action Rules	5-7

5.5	Uninstalling the Connector	5-8
-----	----------------------------	-----

## 6 Extending the Functionality of the SharePoint Connector

---

6.1	Configuring Transformation and Validation of Data	6-1
6.2	Configuring Action Scripts	6-1
6.3	Configuring the Connector for Multiple Tenants	6-2

## 7 Troubleshooting the Connector

---

## 8 Known Issues and Limitations

---

## A Files and Directories in the Connector Installation Package

---

---

# Abstract

Documentation for resource administrators and target system integration teams that describes how to on board Microsoft SharePoint applications to Oracle Identity Governance.

## List of Figures

---

1-1	SharePoint Architecture	1-5
2-1	Overall Flow of the Process for Creating an Application By Using the Connector	2-2
3-1	Default Attribute Mappings for Sharepoint Target User Account	3-12
3-2	Default Attribute Mappings for SharePoint Online SPGroups	3-14
3-3	Default Attribute Mappings for AzureADGroups	3-15
3-4	Simple Correlation Rule for SharePoint Online Target Application	3-16
3-5	Predefined Situations and Responses for a SharePoint Online Target Application	3-17
5-1	Reconciliation Rule for Groups	5-7
5-2	Reconciliation Action Rules for Groups	5-8

## List of Tables

---

1-1	Certified Components	1-2
1-2	Supported Connector Features Matrix	1-7
3-1	Default Attributes for SharePoint Online Target Application	3-11
3-2	Default Attribute Mappings for SPGroups	3-13
3-3	Default Attribute Mappings for SharePoint Online AzureADGroups Forms	3-14
3-4	Predefined identity correlation rules	3-16
3-5	Predefined Situations and Responses for a SharePoint Online Target Application	3-17
4-1	Log Levels and ODL Message Type:Level Combinations	4-4
4-2	Parameters of the IT Resource for the SharePoint Online Connector Server	4-6
5-1	Entries in the Lookup.SharePointOnline.GM.ProvAttrMap Lookup Definition	5-5



# Preface

This guide describes the connector that is used to onboard Microsoft SharePoint applications to Oracle Identity Governance.

## Audience

This guide is intended for resource administrators and target system integration teams.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## Related Documents

For information about installing and using Oracle Identity Governance 12.2.1.3.0, visit the following Oracle Help Center page:

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

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

[http://docs.oracle.com/cd/E52734\\_01/index.html](http://docs.oracle.com/cd/E52734_01/index.html)

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

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

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

[http://docs.oracle.com/cd/E22999\\_01/index.htm](http://docs.oracle.com/cd/E22999_01/index.htm)

## Conventions

The following text conventions are used in this document:

---

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

---

## Legal Disclaimer

This Software may enable You to link to, transfer Your Content or Third Party Content to, or otherwise access, third parties' websites, platforms, content, products, services, and information ("Third Party Services"). Oracle does not control and is not responsible for Third Party Services.

ORACLE PROVIDES ACCESS TO THE THIRD PARTY SERVICES "AS IS". ORACLE DOES NOT MAKE ANY COMMITMENTS OR PROVIDE WARRANTIES OR REPRESENTATIONS ABOUT THE THIRD PARTY SERVICES, THE FUNCTIONS OF THE THIRD PARTY SERVICES, OR THE RELIABILITY, AVAILABILITY, OR ABILITY OF THE THIRD PARTY SERVICES. TO THE EXTENT PERMITTED BY LAW, ORACLE EXCLUDES ALL WARRANTIES WITH REGARD TO THE THIRD PARTY SERVICES.

Your use of the Third Party Services are governed by Your agreement with the Third Party. You are solely responsible for: (a) complying with the terms of access and use of Third Party Services, including any Third Party Privacy Policy; and (b) ensuring that such access and use, including through passwords, credentials or tokens issued or otherwise made available to You, is authorized by the terms of access and use for such Third Party Services.

You agree to continue to comply with the terms of the Agreement for the Software and that Oracle may discontinue Your access to the Third Party Services at any time without liability to You.

# 1

## About the SharePoint 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 SharePoint connector lets you create and on board SharePoint 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**.

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

- [Connector Offerings](#)
- [Certified Components for the Microsoft SharePoint Connector](#)
- [Usage Recommendation](#)
- [Certified Languages](#)
- [Supported Connector Operations](#)
- [Connector Architecture](#)
- [Supported Use Cases](#)
- [Supported Connector Features Matrix](#)
- [Connector Features](#)

### 1.1 Connector Offerings

SharePoint Online Connector supports the Azure AD features along with SharePoint Online features.

- Parent Form attributes which are supported for both the Provisioning and Reconciliation using the Microsoft Graph API's. These attribute values are maintained in Azure AD.
- Supports Add/Remove and Reconciliation of the SharePoint Online groups to the Azure AD user.
- Microsoft Office365 Groups which are part of SharePoint Online Group will be supporting only in user reconciliation.
- Supports SharePoint Online Groups and Microsoft Office365 Groups Lookup Reconciliation.
- SharePoint Online Group management (CRUD Operations) supporting in this connector.

- This connector doesn't support Role Grant Management, License Grant Management, Security Group Management

## 1.2 Certified Components for the Microsoft SharePoint Connector

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

**Table 1-1 Certified Components**

Component	Requirement for AOB Application
Oracle Identity Manager or Oracle Identity Manager	You can use any one of the following releases: <ul style="list-style-type: none"> <li>• Oracle Identity Governance 12c (12.2.1.4.0)</li> <li>• Oracle Identity Governance 12c (12.2.1.3.0)</li> </ul>
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later
Target systems Connector Server	Microsoft SharePoint Online, Microsoft Azure AD 11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 and later
Target API version	SharePoint REST API v1, Azure Active Directory (AD) Microsoft graph API v1.0

### Note:

Ensure that you download and apply the patch 27861122 from [My Support Oracle](#) for 12c PS3. Failing to apply this patch prevents you from successfully testing connection between Oracle Identity Governance and your target system.

## 1.3 Usage Recommendation

If you are using Oracle Identity Governance 12c (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.

[Supported Connector Operations](#) Supported Connector Operations

Operation	Supported
<b>User Management</b>	
Create user	Yes
Update user	Yes
Enable user	Yes
Disable user	Yes
Delete user	Yes

Operation	Supported
Reset Password	Yes
<b>SharePoint Online Group Management</b>	
Create, Update, Revoke Group	Yes
<b>SharePoint Online Group Grant Management</b>	
Assign and Remove Groups	Yes
Microsoft <b>Office365 Groups Grant Management</b>	
Microsoft Office365 Group Reconciliation	Yes

 **Note:**

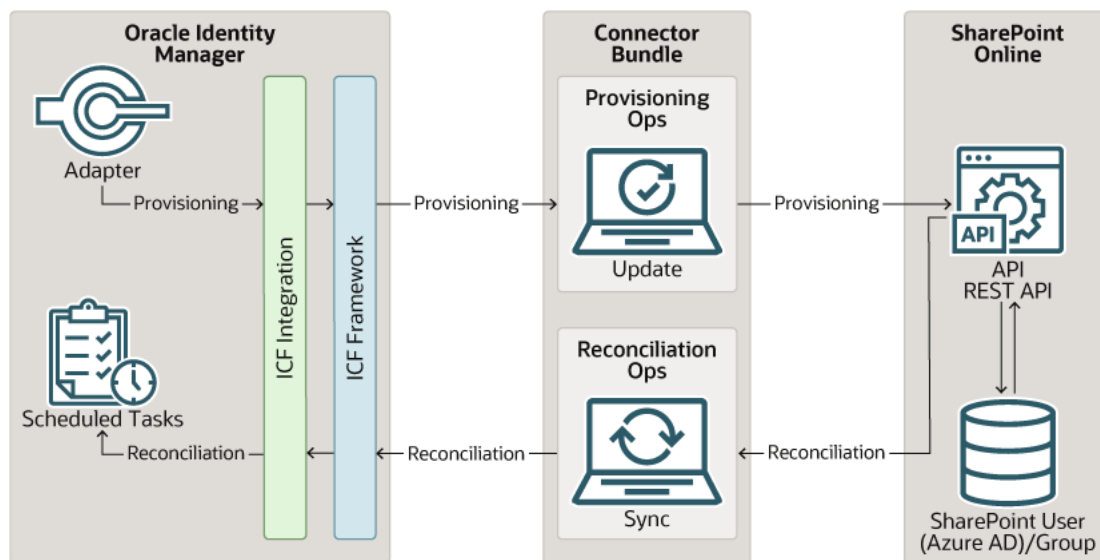
1. Microsoft Office365 Groups that are part of the SharePoint Online Groups are supported only during user reconciliation.
2. All the connector artifacts required for managing groups as an object (for example groups attribute mappings, reconciliation rules, jobs, and so on) are not visible in the **Applications** 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 SharePoint Online 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 SharePoint Architecture



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

- **Account management**

Account management is also known as target resource management. In this mode, the target system is used as a target resource and the connector enables the following operations:

- **Provisioning**

Provisioning involves creating, updating and deleting users on the target system through Oracle Identity Governance. During provisioning, the Adapters invoke ICF operation, ICF in turn invokes create operation on the SharePoint Online Identity Connector Bundle and then the bundle calls the target system API (Microsoft Azure Active Directory (AD) Graph API and SharePoint Online API) for provisioning operations. The API on the target system accepts provisioning data from the bundle, carries out the required operation on the target system, and returns the response from the target system back to the bundle, which passes it to the adapters.

- **Target resource reconciliation**

During reconciliation, a scheduled task invokes an ICF operation. ICF in turn invokes a search operation on the SharePoint Online Identity Connector Bundle and then the bundle calls Microsoft Graph API and SharePoint Online 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 SharePoint Online resources that are already provisioned to OIM Users. If a match is found, then the update made to the SharePoint Online record from the target system is copied to the SharePoint Online 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 SharePoint Online resource to the OIM User.

The SharePoint Online Identity Connector Bundle communicates with the Microsoft Graph API and SharePoint Online API using the HTTPS protocol. The Microsoft Graph API and SharePoint Online API provides programmatic access through REST API endpoints. Apps

can use the Microsoft Graph API and SharePoint Online API to perform create, read, update, and delete (CRUD) operations on directory data and directory objects, such as users, groups.

 **Note:**

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 SharePoint Online connector is used to integrate Oracle Identity Governance with SharePoint Online 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 SharePoint Online 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 across Sharepoint online Cloud Service and groups across SharePoint Online Cloud Service.

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

- **SharePoint Online User Management**  
An organization using SharePoint Online 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 SharePoint Online 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.
- **SharePoint Online Groups Management**  
An organization has a number of SharePoint Online Groups allowing its users to set up new groups, update groups 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 SharePoint Online connector to highlight the usage trend for groups. By using the SharePoint Online, you can leverage the reporting capabilities of Oracle Identity Governance to track any operations (such as create, update and delete) performed on groups and changes made in their memberships.



## 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 1-2](#) provides the list of features supported by the AOB application.

**Table 1-2 Supported Connector Features Matrix**

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

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 time stamp at which an object is created or modified. In the SharePoint Online 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 time stamp at which an object is created or modified.

 **Note:**

The connector supports incremental reconciliation if the target system contains an attribute that holds the time stamp 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.



### Note:

Refer to *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 SharePoint Connector

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

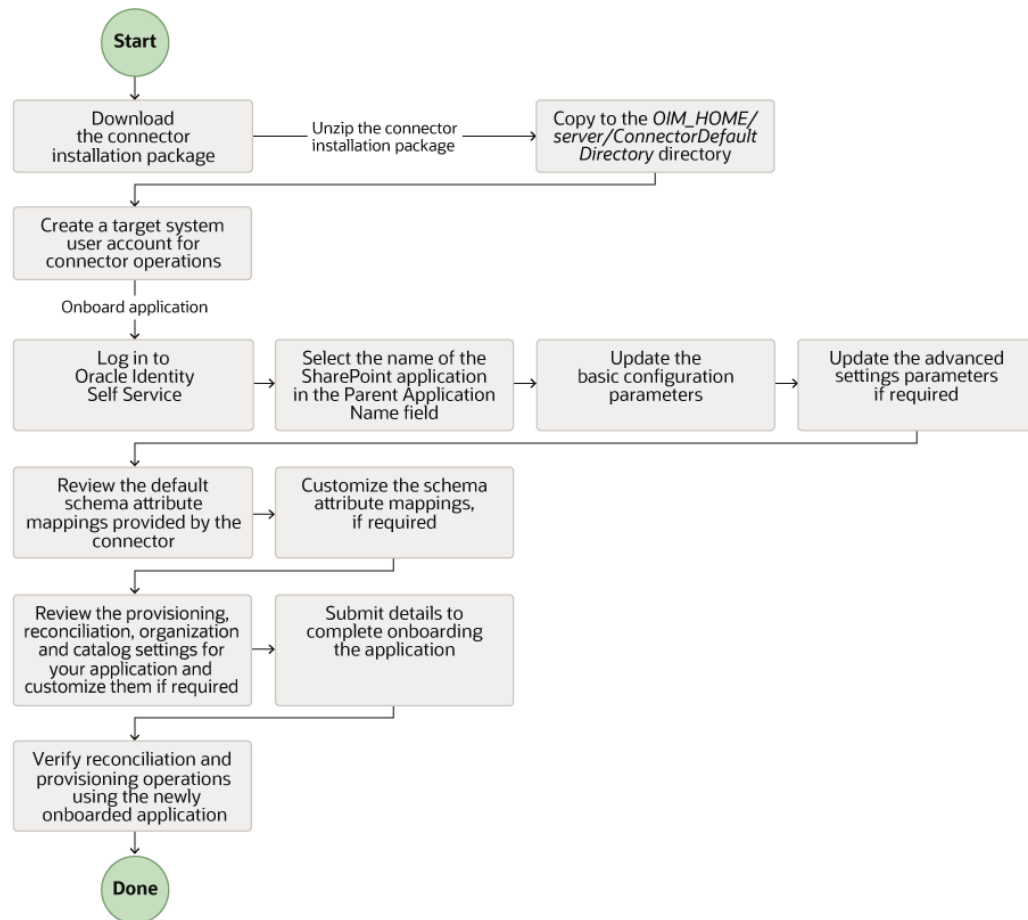
- [Process Flow for Creating an Application By Using the Connector](#)
- [Prerequisites for Creating an Application By Using the Connector](#)
- [Creating an Application By Using the Connector](#)

### 2.1 Process Flow for Creating an Application By Using the Connector

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

[#unique\\_34/unique\\_34\\_Connect\\_42\\_FIG\\_PVB\\_MGG\\_LMB](#) is a flowchart depicting high-level steps for creating an application in Oracle Identity Governance by using the connector installation package.

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



## 2.2 Prerequisites for Creating an Application By Using the Connector

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

- [Registering the Client Application](#)
- [Downloading the Connector Installation Package](#)

### 2.2.1 Registering the Client Application

Registering a client application (that is, the SharePoint Online connector) with the target system is a step that is performed before creating an application instance so that the connector can access SharePoint Online 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.

Pre provisioning involves performing the following tasks on the Azure AD target system:

1. Register your client application with SharePoint Online to provide secure sign in and authorization for your services. You can register your client application by creating an application in the SharePoint Online 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 SharePoint Online.
  - b. Assign the following delegated permissions that the client application requires on SharePoint Online:
    - 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. You can refer 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.

Pre-provisioning involves performing the following tasks on the SharePoint Online target system:



**Note:**

For registering and granting access use the SharePoint app only. Refer to the link: [Microsoft Link](#).

1. Log in to the following URL with an account having the global administrator role and generate **Client Id** and **Client Secret**: [https://<sitename>.SharePoint.com/\\_layouts/15/appregnew.aspx](https://<sitename>.SharePoint.com/_layouts/15/appregnew.aspx)

Fields	Values
1. Title	Add-In
2. AppDomain	localhost
3. RedirectUrl	https://localhost

2. Click **Create** button, which registers the **Add-In** and returns the success message with created information. Grant permissions to **Add-In** to access the SharePoint data.

 **Note:**

Provide **Full Control** permission level to the tenant scope, to enable read, write and manage the Site Collections information.

3. Navigate to the SharePoint site and enter the following URL to redirect to Grant permission page: **[https://<sitename>-admin.sharepoint.com/\\_layouts/15/appinv.aspx](https://<sitename>-admin.sharepoint.com/_layouts/15/appinv.aspx)** in the browser
4. Enter the **Client Id** created in Step 1 in **AppId** textbox and click the **Lookup** button. This would populate the value to other textboxes in **Title**, **App Domain** and **Redirect URL**.
5. Enter the following permission request in XML format:
  - `<AppPermissionRequests AllowAppOnlyPolicy="true">`
  - `<AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />`
  - `</AppPermissionRequests>`For permission scope URIs, refer [link](#).
6. Click **Create** button. This redirects you to a page where you must click on **Trust**, the add-in proceeds further.

## 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 Manager](#) 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 Setting Parameters](#)
- [Attribute Mappings](#)
- [Correlation Rules](#)
- [Reconciliation Jobs](#)


### 3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to SharePoint Online application.


Parameter	Mandatory ?	Description
authenticationType	Yes	Enter the type of authentication used by your Azure AD target system. For this connector, the target system OAuth2.0 client credentials. This is a mandatory attribute while creating an application. Do <i>not</i> modify the value of the parameter. <b>Default value:</b> client_credentials
authenticationServerUrl	Yes	Enter the URL of the authentication server that validates the client ID and client secret for your Azure AD target system. <b>Sample value:</b> 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.

Parameter	Mandatory ?	Description
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.
Scope	Yes	Enter the scope of your client application. <b>Default value:</b> https://graph.microsoft.com/.default
host	Yes	Enter the host name of the machine hosting your target system. This is a mandatory attribute while creating an application. <b>Sample value:</b> graph.microsoft.com
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. <b>Sample value:</b> "api_version;v1.0"
sharePointAuthenticationType	Yes	Enter the type of authentication used by your SharePointOnline target system. For this connector, the target system OAuth2.0 client credentials. This is a mandatory attribute while creating an application. Do <i>not</i> modify the value of the parameter. <b>Default value:</b> client_credentials
sharePointAuthServerUrl	Yes	Enter the URL of the authentication server that validates the client ID and client secret for your sharePoint target system. <b>Sample value:</b> https://accounts.accesscontrol.windows.net/db7b9691-7572-47c7-ac7b-a164135f9636/tokens/OAuth/2

Parameter	Mandatory ?	Description
sharePointClientId	Yes	<div data-bbox="1307 304 1458 1073" style="border: 1px solid #0070c0; padding: 5px;"> <b>Note:</b> Enter the Client ID generated during the SharePoint registration.</div> <p><b>Sample value:</b> 35d2479f-48b7-4ada-8b9e-0103 4b885864@db7b9691-7572-47c 7-ac7b-a164135f9636</p>

Parameter	Mandatory ?	Description
sharePointClientSecret	Yes	<div data-bbox="1307 304 1458 1102" style="border: 1px solid #0070C0; padding: 5px; background-color: #E6F2FF;">  <b>Note:</b> Enter the generated Client Secret during the SharePoint app registration.                 </div> <p><b>Sample value:</b> WS3bSZxC2zQWH1eDXyBcB0vWFSeHDYD04dR3PTwtjY=</p>
sharePointHost	Yes	<p><b>Sample value:</b> idmconnector.sharepoint.com</p>

Parameter	Mandatory ?	Description
resource	Yes	

 **Note:**

Enter the resource 00000003-0000-0ff1-0000-00000000/TE NANT-NAME.s harepoint.com@TE NANT-ID.

**Sample value:**  
00000003-0000-0ff1-

Parameter	Mandatory ?	Description
		ce00-000000000000/ idmconnector.sharepoint.com@d b7b9691-7572-47c7-ac7b- a164135f9636
username	Yes	<b>Sample value:</b> balaji.s@idmconnector.onmicro soft.com
password	Yes	Enter the password for basic authentication type
port	No	Enter the port number at which the target system is listening. <b>Sample value:</b> 443
proxyHost	No	Enter the name of the proxy host used to connect to an external target.
proxyPassword	No	Enter the password of the proxy user ID of the target system user account that Oracle Identity Governance uses to connect to the target system.
proxyPort	No	Enter the proxy port number.
proxyUser	No	Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system. <b>Sample value:</b> 80
sslEnabled	No	If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false. <b>Default value:</b> true

## 3.2 Advanced Setting 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.

Parameter	Description
relURIs	<p>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.</p> <p><b>Default value:</b> "<code>__ACCOUNT__.CREATEOP=/(api_version)/users,"__ACCOUNT__.UPDATEOP=/(api_version)/users/(__UID__),"__ACCOUNT__.SEARCHOP=/(api_version)/users?\$(Filter Suffix)&amp;&amp;\$select=userType,displayName,givenName,userPrincipalName,id,city,usageLocation,accountEnabled,mailNickname,surname,country&amp;\$top=\$(PAGE_SIZE)&amp;&amp;\$skiptoken=\$(PAGE_TOKEN),"__ACCOUNT__=/(api_version)/users/(__UID__)?\$select=displayName,givenName,userPrincipalName,id,city,usageLocation,accountEnabled,mailNickname,country,surname,userType,"__ACCOUNT__.__SHAREPOINTGROUP__.SEARCHOP=/_api/Web/GetUserById(\$(__UID__))/Groups,"__ACCOUNT__.__SHAREPOINTGROUP__.UPDATEOP=/_api/web/sitegroups/GetById(\$(__SHAREPOINTGROUP__.Id))/users,"__ACCOUNT__.__SHAREPOINTGROUP__.REMOVEATTRIBUTE=/_api/web/sitegroups/GetById(\$(__SHAREPOINTGROUP__.Id))/users/removebyloginname('i%3A0%23.f%7Cmembership%7C\$(__UID__\$)'),"__SHAREPOINTGROUP__.SEARCHOP=/_api/web/sitegroups,"__OFFICEGROUP__.SEARCHOP=/(api_version)/groups?&amp;\$filter=securityEnabled+eq+false&amp;groupTypes/any(c:c+eq+'Unified')&amp;\$top=\$(PAGE_SIZE)&amp;&amp;\$skiptoken=\$(PAGE_TOKEN),"__ACCOUNT__.__OFFICEGROUP__.SEARCHOP=/_api/Web/GetUserById(\$(__UID__))/Groups,"__ACCOUNT__.__SHAREPOINTUSERLIST__=/_api/Web/siteusers('i%3A0%23.f%7Cmembership%7C\$(__UID__\$)'),"__ACCOUNT__.__SHAREPOINTGROUPUSERS__=/_api/web/sitegroups/GetById(\$(__UID__))/users,"__ACCOUNT__.manager.SEARCHOP=/(api_version)/users/(\$(__UID__))/manager,"__ACCOUNT__.manager=/(api_version)/users/(\$(__UID__))/manager/\$ref"</code></p>

Parameter	Description
nameAttributes	<p>This entry holds the name attribute for all the objects that are handled by this connector.</p> <p>For example, for the <code>__ACCOUNT__</code> object class that it used for User accounts, the name attribute is <code>userPrincipalName</code>.</p> <p><b>Default value:</b>  <code>"__ACCOUNT__.userPrincipalName","__SHAREPOINTGROUP__.Title","__OFFICEGROUP__.displayName"</code></p>
uidAttributes	<p>This entry holds the uid attribute for all the objects that are handled by this connector.</p> <p>For example, for User accounts, the uid attribute is <code>objectId</code>.</p> <p>In other words, the value <code>__ACCOUNT__.objectId</code> in <code>decode</code> implies that the <code>__UID__</code> attribute (that is, GUID) of the connector for <code>__ACCOUNT__</code> object class is mapped to <code>objectId</code> which is the corresponding uid attribute for user accounts in the target system.</p> <p><b>Default value:</b>  <code>"__ACCOUNT__.id","__SHAREPOINTGROUP__.Id","__OFFICEGROUP__.id"</code></p>
opTypes	<p>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: <code>OBJ_CLASS.OP=HTTP_OP</code></p> <p>In this format, <code>OBJ_CLASS</code> is the connector object class, <code>OP</code> is the connector operation (for example, <code>CreateOp</code>, <code>UpdateOp</code>, <code>SearchOp</code>), and <code>HTTP_OP</code> is the HTTP operation (<code>GET</code>, <code>PUT</code>, or <code>POST</code>).</p> <p><b>Default value:</b>  <code>"__ACCOUNT__.CREATEOP=POST","__ACCOUNT__.UPDATEOP=PATCH","__ACCOUNT__.SEARCHOP=GET","__ACCOUNT__.TESTOP=GET","__ACCOUNT__.__SHAREPOINTGROUP__.UPDATEOP=POST","__ACCOUNT__.__SHAREPOINTGROUP__.REMOVEATTRIBUTE=POST","__ACCOUNT__.manager.CREATEOP=PUT","__ACCOUNT__.manager.UPDATEOP=PUT"</code></p>
pageSize	<p>The number of resources/users that appears on a page for a search operation.</p> <p><b>Default value:</b> 100</p>
pageTokenAttribute	<p>The attribute in response payload that denotes the next page token.</p> <p><b>Default value:</b> <code>@odata.nextLink</code></p>
pageTokenRegex	<p>This attribute is used in the URL while reconciliation to support pagination.</p> <p><b>Default value:</b> <code>(?&lt;=skiptoken=).*</code></p>



Parameter	Description
Any Incremental Recon Attribute Type	<p>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.</p> <p><b>Default value:</b> True</p>
jsonResourcesTag	<p>This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload.</p> <p><b>Default value:</b> "__ACCOUNT__=value", "__SHAREPOINTGROUP__=value", "__OFFICEGROUP__=value"</p>
httpHeaderContentType	<p>This entry holds the content type expected by the target system in the header.</p> <p><b>Default value:</b> application/json</p>
httpHeaderAccept	<p>This entry holds the accept type expected from the target system in the header.</p> <p><b>Default value:</b> application/json</p>
specialAttributeTargetFormat	<p>This entry lists the format in which an attribute is present in the target system endpoint.</p> <p>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: <i>OBJ_CLASS.ATTR_NAME=TARGET_FORMAT</i></p> <p><b>Default value:</b> "__ACCOUNT__.__SHAREPOINTGROUP__=value", "__ACCOUNT__.__OFFICEGROUP__=value", "__ACCOUNT__.manager=id"</p>
specialAttributeHandling	<p>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: <i>OBJ_CLASS.ATTR_NAME.PROV_OP=SINGLE</i></p> <p>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.</p> <p><b>Default value:</b> "__ACCOUNT__.__SHAREPOINTGROUP__.UPDATEOP=SINGLE", "__ACCOUNT__.__SHAREPOINTGROUP__.ADDATTRIBUTE=SINGLE", "__ACCOUNT__.__SHAREPOINTGROUP__.REMOVEATTRIBUTE=SINGLE", "__ACCOUNT__.manager.CREATEOP=SINGLE", "__ACCOUNT__.manager.UPDATEOP=SINGLE"</p>

Parameter	Description
customPayload	<p>This entry lists the payloads for all operations that are not in the standard format.</p> <p><b>Default value:</b>  <code>"__ACCOUNT__._SHAREPOINTGROUP__UPDATEOP={ \"__metadata\": { \"type\": \"SP.User\"}, \"LoginName\": \"i:0#.f membership \$(__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)\$\\}\"}</code></p>
statusAttributes	<p>This entry lists the name of the target system attribute that holds the status of an account. For example, for the <code>__ACCOUNT__</code> object class that it used for User accounts, the status attribute is <code>accountEnabled</code>.</p> <p><b>Default value:</b> <code>"__ACCOUNT__.accountEnabled"</code></p>
passwordAttribute	<p>This entry holds the name of the target system attribute that is mapped to the <code>__PASSWORD__</code> attribute of the connector in OIM.</p> <p><b>Default value:</b> <code>passwordProfile.password</code></p>
targetObjectIdentifier	<p>This entry specifies the key-value pair for replacing place holders in the relURIs. Values are comma separated and in the <code>KEY;VALUE</code> format.</p> <p><b>Default value:</b>  <code>"__ACCOUNT__._OFFICEGROUP__=securityEnabled;false"</code></p>
urlIdentifierKeys	<p>This entry is used to identify SharePointOnline url. These values should be comma separated.</p> <p><b>Default value:</b> <code>"site","/_api/Web/"</code></p>

## 3.3 Attribute Mappings

The following topic provides the details of attribute mappings on the Schema page:

- [Attribute Mappings for the Target Application](#)

### 3.3.1 Attribute Mappings for the Target Application

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

#### Default Attributes for SharePoint Online Target Application

[Table 3-1](#) lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and SharePoint Online 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 attribute as described in [Creating a Target Application](#) in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 3-1 Default Attributes for SharePoint Online 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	Not Applicable	Yes
User Principal Name	__NAME__	String	Yes	Yes	Yes	No	Yes	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.forceChangePasswordNextLogon	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 Sharepoint Target 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			
Select a value	Object Id	_UID_	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	User Principal N	_NAME_	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Password	_PASSWORD_	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	First Name	givenName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Last Name	surname	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Display Name	displayName	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	User Type	userType	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Usage Location	usageLocation	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	City	city	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Country	country	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Manager	manager	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

### SharePointOnline SPGroups Entitlement

Table 3-2 lists the group forms attribute mappings between the process form fields in Oracle Identity Governance and SharePoint Online 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*.

 **Note:**

In the Table 3-2 list only the attribute **Group Name** is updated during provisioning, the remaining attributes will be updated during recon.

**Table 3-2 Default Attribute Mappings for SPGroups**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Group Name	__SHAREPO INTGROUP_ ~__SHARE POINTGRO UP__~Id	String	Yes	Yes	Yes	No
Owner Title	__SHAREPO INTGROUP_ ~__SHARE POINTGRO UP__~OwnerTitle	String	No	Yes	No	Not applicable
Group Type	__SHAREPO INTGROUP_ ~__SHARE POINTGRO UP__~odata.type	String	No	Yes	No	Not applicable
AutoAcceptRequestToJoinLeave	__SHAREPO INTGROUP_ ~__SHARE POINTGRO UP__~AutoAcceptRequestToJoinLeave	String	No	Yes	No	Not applicable
AllowRequestToJoinLeave	__SHAREPO INTGROUP_ ~__SHARE POINTGRO UP__~AllowRequestToJoinLeave	String	No	Yes	No	Not applicable
OnlyAllowMembersViewMembership	__SHAREPO INTGROUP_ ~__SHARE POINTGRO UP__~OnlyAllowMembersViewMembership	String	No	Yes	No	Not applicable
AllowMembersEditMembership	__SHAREPO INTGROUP_ ~__SHARE POINTGRO UP__~AllowMembersEditMembership	String	No	Yes	No	Not applicable

**Table 3-2 (Cont.) Default Attribute Mappings for SPGroups**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Group Url	__SHAREPOINTGROUP__~__SHAREPOINTGROUP__~odata.id	String	No	Yes	No	Not applicable
PrincipalType	__SHAREPOINTGROUP__~__SHAREPOINTGROUP__~PrincipalType	String	No	Yes	No	Not applicable

Figure 3-2 shows the default SPGroups entitlement mapping

**Figure 3-2 Default Attribute Mappings for SharePoint Online SPGroups**

Application Attribute		Provisioning Property	Reconciliation Properties			
Display Name	Target Attribute	Mandatory	Recon Field	Key Field	Case Insensitive	
Group Name	__SHAREPOINTGROUP__~__SI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Owner Title	__SHAREPOINTGROUP__~__SI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Group Type	__SHAREPOINTGROUP__~__SI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AutoAcceptRequestToJoinLea	__SHAREPOINTGROUP__~__SI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AllowRequestToJoinLeave	__SHAREPOINTGROUP__~__SI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
OnlyAllowMembersViewMem	__SHAREPOINTGROUP__~__SI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AllowMembersEditMembersh	__SHAREPOINTGROUP__~__SI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Group Url	__SHAREPOINTGROUP__~__SI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PrincipalType	__SHAREPOINTGROUP__~__SI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Table 3-3 Default Attribute Mappings for SharePoint Online AzureADGroups Forms**

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

**Table 3-3 (Cont.) Default Attribute Mappings for SharePoint Online AzureADGroups 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 3-3 shows the default attribute mappings for AzureADGroups.

**Figure 3-3 Default Attribute Mappings for AzureADGroups**

The screenshot shows the configuration interface for SharePoint Online AzureADGroups. It includes a table with columns for Application Attribute, Provisioning Property, and Reconciliation Properties. The table contains two rows of attribute mappings.

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
SharePointOnline Group Name	__OFFICEGROUP__~__OFFICEGROUP__~id	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Office Group Name	__OFFICEGROUP__~__OFFICEGROUP__~id	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## 3.4 Correlation Rules

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

- [Correlation Rules for the Target Application](#)

### 3.4.1 Correlation Rules for the Target Application

When you create a target application, the connector uses correlation rules to determine the identity to which Oracle Identity Governance must assign a resource.

#### Predefined Identity Correlation Rules

By default, the SharePoint Online 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.

[Predefined identity correlation rules](#) lists the default simple correlation rule for a SharePoint Online 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 3-4 Predefined identity correlation rules**

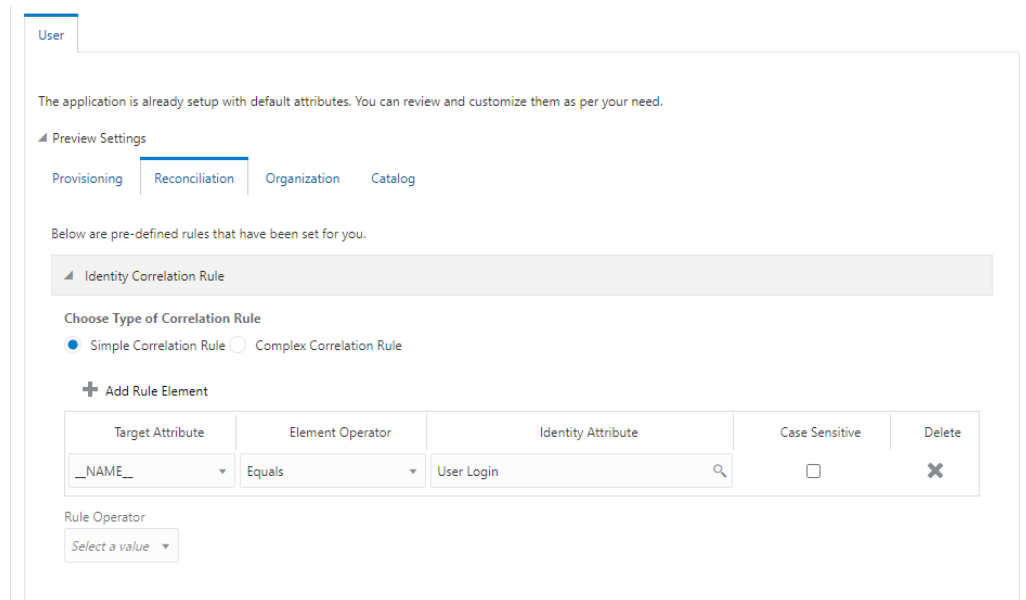
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

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 3-4 shows the simple correlation rule for SharePoint Online target application.

**Figure 3-4 Simple Correlation Rule for SharePoint Online Target Application**



### Predefined Situations and Responses

The SharePoint Online 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.

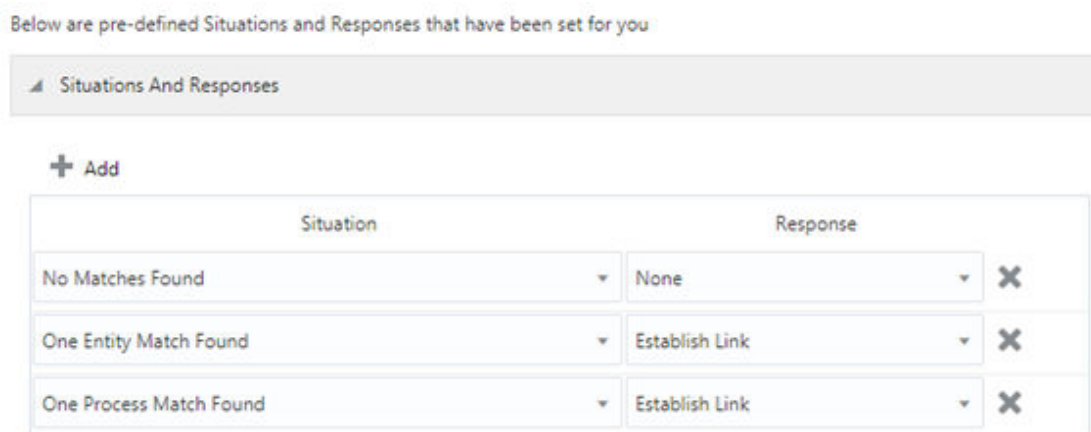
Table 3-5 lists the default situations and responses for a SharePoint Online Target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance



**Table 3-5 Predefined Situations and Responses for a SharePoint Online Target Application**

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

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

**Figure 3-5 Predefined Situations and Responses for a SharePoint Online Target Application**

## 3.5 Reconciliation Jobs

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

### User Reconciliation Jobs

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

The following reconciliation jobs are available for reconciling user data:

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

[Parameters of the SharePoint Online Full User Reconciliation Job](#) describes the parameters of the SharePoint Online 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 <i>not</i> change the default value.
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.  <b>Note:</b> Do not enter a value for this parameter. The reconciliation engine automatically enters a value in this parameter.  <b>Sample value:</b> <String>2017-11-30T04:44:29Z</String>
Object Type	This parameter holds the name of the object type for the reconciliation run.  <b>Default value:</b> User  Do <i>not</i> change the default value.
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run.  <b>Sample value when incremental recon is enabled:</b> &\$filter=displayName+eq+'JAN2KKA1'  <b>Sample value when incremental recon is not enabled:</b> &\$filter=displayName+eq+'JAN2KKA1'  For more information about creating filters, see <a href="#">Performing Limited Reconciliation</a> .
Scheduled Task Name	Name of the scheduled task used for reconciliation.  Do <i>not</i> 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.

# 4

## Performing Postconfiguration Tasks for the SharePoint Connector

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

- [Configuring Oracle Identity Governance](#)
- [Harvesting Entitlements and Sync Catalog](#)
- [Managing Logging](#)
- [Understanding Log Levels](#)
- [Enabling Logging](#)
- [Configuring the IT Resource for the Connector Server](#)
- [Localizing Field Labels in UI Forms](#)
- [Configuring SSL for the Connector](#)

### 4.1 Configuring Oracle Identity Manager

You must create a UI form and an application instance for the resource against which you want to perform reconciliation and provisioning operations.

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

- [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\_SERVER 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='SharePoint-handler'
level=' [LOG_LEVEL]'class='oracle.core.ojdl.logging.ODLHandlerFact
ory'> <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.SHAREPOINTONLINE"
level=" [LOG_LEVEL]" useParentHandlers="false"> <handler
name="SharePoint-handler"/> <handler name="console-handler"/> </
logger>
```

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='SharePoint-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.SHAREPOINTONLINE"  
level="NOTIFICATION:1" useParentHandlers="false"> <handler  
name="SharePoint-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 SharePoint Online 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 SharePoint Online Connector Server**

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. Sample value: <code>HostName</code>
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. Sample value: <code>8763</code>
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: <code>0</code> (recommended value)
UseSSL	Enter <code>true</code> to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter <code>false</code> . Default value: <code>false</code> <b>Note:</b> It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see <i>Configuring SSL for Java Connector Server</i> in <i>Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance</i> .

## 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.BaseRuntimeResourceBu
ndle']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.user
EO.UD_USER_PRINCIPAL_NAME__c_description']">
<source>User Principal Name</source><target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.RSAForm.entity.AzureAD
FormEO.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.BaseRuntimeResourceBu
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.entity
sEO.UD_GA_USR_ACCOUNT_NAME__c_LABEL">
<source>Account Name</source>
<target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit>

```

- f. Repeat Steps 6.a through 6.d for all attributes of the process form.
  - g. Save the file as `BizEditorBundle_LANG_CODE.xlf`. In this file name, replace `LANG_CODE` with the code of the language to which you are localizing. Sample file name: `BizEditorBundle_ja.xlf`.
7. Repackage the ZIP file and import it into MDS.

#### See Also:

Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for more information about exporting and importing metadata files

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

## 4.6 Configuring SSL

Configure SSL to secure data communication between Oracle Identity Governance and the Azure AD and the SharePoint Online 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 and SharePoint Online
2. Copy the public key certificate of Azure AD and SharePoint Online 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 Sharepoint Online connector, the incremental reconciliation option is not enabled by default. The connector supports incremental reconciliation only if the Azure AD target system contains an attribute that holds the timestamp at which an object is created or modified. Incremental reconciliation does not work, if changes made only Sharepoint Online target.

#### 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:
  - a. **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
  - b. **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. See [Creating Jobs](#) in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

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.SharePointOnline.GM.Configuration](#)
- [Lookup.SharePointOnline.GM.ProvAttrMap](#)
- [Lookup.SharePointOnline.GM.ReconAttrMap](#)

#### 5.4.1.1 Lookup.SharePointOnline.GM.Configuration

The Lookup.SharePointOnline.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.

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.SharePointOnline.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.

Code Key	Decode	Description
Recon Attribute Map	Lookup.SharePointOnline.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.SharePointOnline.GM.ProvAttrMap

Lookup.SharePointOnline.GM.ProvAttrMap

This lookup definition is preconfigured and is used during group provisioning operations.

**Table 5-1 Entries in the Lookup.SharePointOnline.GM.ProvAttrMap Lookup Definition**

Group Field on Oracle Identity Governance	SharePointOnline Field
Title	__NAME__
Object Id	__UID__
Allow Members Edit Membership	AllowMembersEditMembership
Allow Request To Join/Leave	AllowRequestToJoinLeave
Auto Accept Request To Join/Leave	AutoAcceptRequestToJoinLeave
Description	Description
Only Allow Members View Membership	OnlyAllowMembersViewMembership
Request To Join Leave Email Setting	RequestToJoinLeaveEmailSetting

### 5.4.1.3 Lookup.SharePointOnline.GM.ReconAttrMap

The Lookup.SharePointOnline.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.

Group Field on Oracle Identity Governance	SharePointOnline Field
Title	__NAME__
ObjectId	__UID__
Allow Members Edit Membership	AllowMembersEditMembership
Allow Request To Join/Leave	AllowRequestToJoinLeave
Auto Accept Request To Join/Leave	AutoAcceptRequestToJoinLeave
Description	Description
OIM Org Name	OIM Organization Name <b>Note:</b> 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.
Only Allow Members View Membership	OnlyAllowMembersViewMembership
Request To Join Leave Email Setting	RequestToJoinLeaveEmailSetting



## 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

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.

The following is the process-matching rule for groups:

**Rule name:** SharePoint Group 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 SharePointOnline Group Recon scheduled job.

### 5.4.2.2 Reconciliation Action Rules for Groups

[Action rules for groups reconciliation](#) lists the 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 **SharePoint Group Recon rule**.  
The [Reconciliation Rule for Groups](#) shows the reconciliation rule for groups.

**Figure 5-1 Reconciliation Rule for Groups**

The screenshot shows the 'Reconciliation Rule Builder' window. At the top, the 'Name' field contains 'SharePoint Group Recon ru', the 'Object' field contains 'SharePointOnline Group', and the 'Description' field contains 'SharePointOnline Group Test'. The 'Operator' section has radio buttons for 'AND' and 'OR', with 'OR' selected. There are checkboxes for 'Valid' and 'Active', both of which are checked. Below these fields are radio buttons for 'For User' and 'For Organization', with 'For Organization' selected. The 'Rule Elements' section is expanded to show 'Rule Definition'. On the left, there are buttons for 'Add Rule', 'Add Rule Element', 'Delete', and 'Legend'. The main area of the 'Rule Definition' pane shows a tree view with a folder icon and the text 'Rule: SharePoint Group Recon rule' and 'Organization Name Equals OIM Org Name'. At the bottom of the window, there is a tab labeled 'Reconciliation Rules'.

#### 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 **SharePointOnline Groupresource** object.
4. Click **Object Reconciliation** tab.
5. Click **Reconciliation Action Rules** tab.

The **Reconciliation Action Rules** tab displays the action rules defined for this connector. [Reconciliation Action Rules for Groups](#) shows the reconciliation action rules for groups.

Figure 5-2 Reconciliation Action Rules for Groups

The screenshot shows a web interface for 'Object Reconciliation'. At the top, there are tabs for 'Resource Object' and 'Object Reconciliation'. Below the tabs, there is a field for 'Object Initial Reconciliation Date' and a 'Create Reconciliation Profile' button. The main section is titled 'Reconciliation Action Rules' and contains a table with three columns: 'Rule Condition', 'Action', and 'User'. There are also 'Add' and 'Delete' buttons on the left side of the table.

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

## 5.5 Uninstalling the Connector

Uninstalling the SharePointOnline 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: `Sharepoint1; SharePointOnline Group`

Sharepoint1 is SharePointOnline connector, Application created Usered Resource Object.

### 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 SharePoint Connector

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

This section provides more information about 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 SharePoint Online connector

# 8

## Known Issues and Limitations

The following are the list of known issues and limitation associated with the SharePoint Online connector:

- Adding Groups during provisioning of the account is not allowed. You can add Groups only after the account creation in target is successful.
- Since the **Last Modified Date** attribute is not available in the target, the Incremental reconciliation operation is not supported.
- If the SharePoint online group is removed from the User Account in OIG, the Groups associated with SharePoint online groups will still remain in the OIG. It can be removed only after the user reconciliation.
- When SharePoint online group is assigned to the User Account in the target and you perform the user reconciliation, it reconciles both the Share point Online group and office groups associated with same share point online group.

# A

## Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the SharePoint Online connector.

File in the Installation Package	Description
bundle/ org.identityconnectors.sharepointonline-12.3.0.jar	This JAR is the ICF connector bundle.
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. <b>Note:</b> A <b>resource bundle</b> 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/SharePointOnline-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/SharePointOnline-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User object such as Groups.