# Oracle® Identity Governance

## Configuring the Office 365 Application

12c (12.2.1.3.0)

F12371-05

October 2020

**ORACLE®**

Oracle Identity Governance Configuring the Office 365 Application, 12c (12.2.1.3.0)

F12371-05

Primary Author: Alankrita Prakash

Contributors: Gowri.G.R

# Contents

**ORACLE**

# 3    Configuring the Office 365 Connector

# 4    Performing Postconfiguration Tasks for the Office 365 Connector

# 5    Using the Office 365 Connector

# 6    Extending the Functionality of the Office 365 Connector

# 7    Upgrading the Office 365 Connector

# A    Files and Directories in the Office 365 Connector Installation Package

# List of Figures

# List of Tables

# Preface

This guide describes the connector that is used to onboard Office 365 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`

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`

## Conventions

The following text conventions are used in this document:

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

ORACLE®

# What's New in This Guide?

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

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

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

## Software Updates

These are the updates made to the connector software.

**Software Updates in Release 12.2.1.3.0**

The following are the software updates in release 12.2.1.3.0:

**Support for Onboarding Applications Using the Connector**

From this release onward, the connector bundle includes application onboarding templates required for performing connector operations on the Office 365 target. This helps in quicker onboarding of the applications for Office 365 into Oracle Identity Governance by using an intuitive UI.

**Support for Paging**

From this release onward, the connector uses the Paging feature of the target system for performing full reconciliation.

**Support for Incremental Reconciliation**

From this release onward, the connector supports incremental reconciliation if the target system contains an attribute that holds the timestamp at which an object is created or modified.

For information on enabling incremental reconciliation, see Performing Full Reconciliation and Incremental Reconciliation.

## Documentation-Specific Updates

These are the updates made to the connector documentation.

**Documentation-Specific Updates in Release 12.2.1.3.0**

The following documentation-specific update has been made in revision "05" of this guide:

Logger names present in Enabling Logging have been updated.

The following documentation-specific update has been made in revision "04" of this guide:

Information about Patch O365.12.2.1.3.0B has been added to Connector Features .

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

• A Note regarding supported group types has been added to Supported Connector Operations.

• Performing Delete Reconciliation has been added.

The following documentation-specific updates have been made in revision "02" of this guide:

• The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance release 12*c* PS4 (12.2.1.4.0).

• "Connector Server JDK" and "Oracle Identity Governance or Oracle Identity Manager JDK" rows of Table 1-1 have been updated to include support for JDK 1.8 and later.

• The "Connector Server" row of Table 1-1 has been updated to include support for 11.1.2.1.0 and later versions.

• Several broken links were fixed throughout the document.

• In this revision, the document is updated for editorial corrections.

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

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

# 1
# About the Office 365 Connector

Oracle Identity Governance is a centralized identity management solution that provides self service, compliance, provisioning and password management services for applications residing on-premise or on the Cloud. Oracle Identity Governance connectors are used to integrate Oracle identity Governance with the external identity-aware applications.

The Office 365 connector lets you create and onboard Office 365 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 connector that is deployed using the **Manage Connector** option in Oracle Identity System Administration is referred to as a **CI-based connector** (Connector Installer-based connector).

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Oracle Identity Self Service. This capability lets business users to onboard applications with minimum details and effort. The connector installation package includes a collection of predefined templates (XML files) that contain all the information required for provisioning and reconciling data from a given application or target system. These templates also include basic connectivity and configuration details specific to your target system. The connector uses information from these predefined templates allowing you to onboard your applications quickly and easily using only a single and simplified UI.

**Application onboarding** is the process of registering or associating an application with Oracle Identity Governance and making that application available for provisioning and reconciliation of user information.

The following topics provide a high-level overview of the Office 365 connector:

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

# 1.1 Certified Components

These are the software components and their versions required for installing and using the Office 365 connector.

**Table 1-1    Certified Components**

| Component | Requirement for AOB Application | Requirement for CI-Based Connector |
|---|---|---|
| Oracle Identity Governance or Oracle Identity Manager | You can use any one of the following releases:<br>• Oracle Identity Governance 12*c* (12.2.1.4.0)<br>• Oracle Identity Governance 12*c* (12.2.1.3.0)<br>**Note**: Ensure that you download and apply the patch 25323654 from My Oracle Support. Failing to apply this patch will prevent you from successfully testing connection between Oracle Identity Governance and your target system. | You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:<br>• Oracle Identity Governance 12*c* (12.2.1.4.0)<br>• Oracle Identity Governance 12c (12.2.1.3.0)<br>• Oracle Identity Manager 11*g* Release 2 (11.1.2.3.0) |
| Oracle Identity Governance or Oracle Identity Manager JDK | JDK 1.8 and later | JDK 1.8 and later |
| Target systems | Microsoft Office 365 Enterprise Editions | Microsoft Office 365 Enterprise Editions |
| Connector Server | 11.1.2.1.0 and later | 11.1.2.1.0 and later |
| Connector Server JDK | JDK 1.8 and later | JDK 1.8 and later |
| Target API version | Azure Active Directory (AD) Graph API 1.6 | Azure Active Directory (AD) Graph API 1.6 |

# 1.2 Usage Recommendation

These are the recommendations for the Office 365 connector version that you can deploy and use depending on the Oracle Identity Governance or Oracle Identity Manager version that you are using.

• If you are using Oracle Identity Governance 12c (12.2.1.3.0), then use the latest 12.2.1.*x* version of this connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service.

• If you are using any of the Oracle Identity Manager releases listed in the "Requirement for CI-Based Connector" column in Table 1-1, then use the 11.1.*x* version of the Office 365 connector. If you want to use the 12.2.1.*x* version of this connector, then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0.

> **Note:**
>
> If you are using the latest 12.2.1.*x* version of the Office 365 connector in the CI-based mode, then see *Oracle Identity Manager Connector Guide for Office 365*, Release 11.1.1 for complete details on connector deployment, usage, and customization.

# 1.3 Certified Languages

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- French (Canadian)
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

## 1.4 Supported Connector Operations

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

**Table 1-2    Supported Connector Operations**

| Operation | Supported |
|---|---|
| **User Management** | |
| Create user | Yes |
| Update user | Yes |
| Delete user | Yes |
| Reset Password | Yes |
| **Role Grant Management** | |
| Assign and Revoke Roles | Yes |
| **License Grant Management** | |
| Grant and Revoke Licences | Yes |
| **Group Management** | |
| Add, Update, and Remove Groups | Yes |

> **Note:**
>
> • The Office 365 connector supports the following two groups:
>   – Office 365 Groups
>   – Security Groups
> • All 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.

## 1.5 Connector Architecture

The Office 365 connector is implemented by using the Identity Connector Framework (ICF).

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

Figure 1-1 shows the architecture of the Office 365 connector.

**Figure 1-1    Connector Architecture**
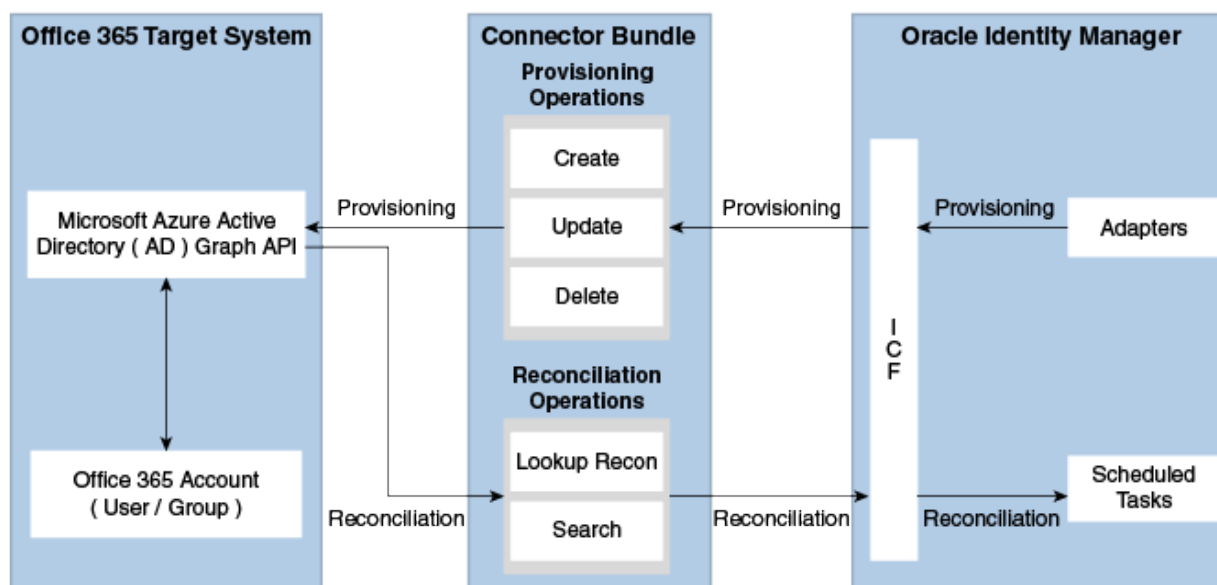


The connector is configured to run in one of the following modes:

- Identity reconciliation

  Identity reconciliation is also known as authoritative or trusted source reconciliation. In this mode, the Office 365 application is used as the trusted source and users are directly created and modified on Oracle Identity Governance. During reconciliation, a scheduled task invokes an ICF operation. ICF inturn invokes a search operation on the Office 365 Identity Connector Bundle and then the bundle calls Office 365 API for Reconciliation operation. The API extracts user records that match the reconciliation criteria and hands them over through the bundle and ICF back to the scheduled task, which brings the records to Oracle Identity Governance.

  Each user record fetched from the target system is compared with existing OIM Users. If a match is found between the target system record and the OIM User, then the OIM User attributes are updated with changes made to the target system record. If no match is found, then the target system record is used to create an OIM User.

- Account management

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

  – Provisioning

    Provisioning involves creating, updating, or deleting users on the target system through Oracle Identity Governance. During provisioning, the Adapters invoke ICF operation, ICF inturn invokes create operation on the Office 365 Identity Connector Bundle and then the bundle calls the target system API (Microsoft Azure Active Directory (AD) Graph API) for provisioning operations. The API on the target system accepts provisioning data from the bundle,

carries out the required operation on the target system, and returns the response from the target system back to the bundle, which passes it to the adapters.

– Target resource reconciliation

During reconciliation, a scheduled task invokes an ICF operation. ICF inturn invokes a search operation on the Office 365 Identity Connector Bundle and then the bundle calls Office 365 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 Office 365 resources that are already provisioned to OIM Users. If a match is found, then the update made to the Office 365 record from the target system is copied to the Office 365 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 Office 365 resource to the OIM User.

The Office 365 Identity Connector Bundle communicates with the Microsoft Azure Active Directory Graph API using the HTTPS protocol. The Microsoft Azure Active Directory Graph API provides programmatic access to Azure Active Directory through REST API endpoints. Apps can use the Microsoft Azure Active Directory Graph API to perform create, read, update, and delete (CRUD) operations on directory data and directory objects, such as users, groups.

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

## 1.6 Use Cases Supported by the Connector

The Office 365 connector is used to integrate Oracle Identity Governance with Office 365 to ensure that all Office 365 accounts are created, updated, and deactivated on an integrated cycle with the rest of the identity-aware applications in your enterprise. The Office 365 connector supports management of identities for Cloud Identity, Synchronized Identity, and Federated Identity models of Office 365. In a typical IT scenario, an organization using Oracle Identity Governance wants to manage accounts, groups, roles and licenses across Office 365 Cloud Service.

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

• **Office 365 User Management**

An organization using Office 365 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 Office 365 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.

- **Office 365 Group Management**

  An organization has a number of Office 365 Security Groups allowing its users to set up new groups, manage memberships, and delete groups. The organization now wants to know the list of groups that have not been recently accessed or who have inactive members. In such a scenario, you can use the Office 365 connector to highlight the usage trend for groups. By using the Office 365 connector, you can leverage the reporting capabilities of Oracle Identity Governance to track any operations (such as create, update, delete) performed on groups and changes made in their memberships .

- **Office 365 Admin Role Management**

  In large organizations, it may be necessary for an administrator to designate other employees to act as administrators to serve different functions. For example, you can set admin roles for your IT staff that can act as support agents to other employees, partners, customers and vendors. With the Office 365 connector, you can assign or revoke an Office 365 admin role to users as an entitlement, thus facilitating you to leverage the delegated administration capability of Office 365.

- **Office 365 User License Management**

  Another scenario is one in which an organization is using Office 365 for business and manages user licenses as per the changing needs of the organization by assigning or unassigning licenses for users. What is needed is an effective way to keep track of all the licenses and user rights both in cloud and on-premise servers. In such a scenario, you can use the Office 365 connector to effectively track all user licenses. You can keep track of these license assignment changes by leveraging Oracle Identity Governance capability of auditing and reporting.

# 1.7 Connector Features

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

Table 1-3 provides the list of features supported by the AOB application and CI-based connector.

**Table 1-3    Supported Connector Features Matrix**

| Feature | AOB Application | CI-Based Connector |
|---|---|---|
| Full reconciliation | Yes | Yes |
| Incremental reconciliation | Yes | Yes |

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

| Feature | AOB Application | CI-Based Connector |
|---|---|---|
| Limited reconciliation | Yes | Yes |
| Delete reconciliation | Yes | Yes<br>**Note**: Apply Patch **O365.12.2.1.3.0B** for delete reconciliation to work successfully. |
| Support for authoritative source reconciliation | Yes | Yes |
| Use connector server | Yes | Yes |
| Transformation and validation of account data | Yes | Yes |
| Perform connector operations in multiple domains | Yes | Yes |
| Support for paging | Yes | Yes |
| Test connection | Yes | No |
| Reset password | Yes | Yes |

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

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

## 1.7.1 Full Reconciliation and Incremental Reconciliation

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

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

In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance. During an incremental reconciliation run, the scheduled job fetches only target system records that are added or modified after the time-stamp stored in the Latest Token attribute of the scheduled job.

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

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

## 1.7.2 Limited Reconciliation

You can reconcile records from the target system based on a specified filter criterion. To limit or filter the records that are fetched into Oracle Identity Governance during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled.

You can set a reconciliation filter as the value of the Filter Suffix attribute of the user reconciliation scheduled job. The Filter Suffix attribute helps you to assign filters to the API based on which you get a filtered response from the target system.

For more information, see Performing Limited Reconciliation .

## 1.7.3 Reconciliation of Deleted Users

You can configure the connector for reconciling information about users deleted in the target system.

In target resource mode, if a user is deleted on the target system, then the corresponding user is revoked from Oracle Identity Governance.

See Performing Delete Reconciliation for more information about the scheduled job used for reconciling deleted users.

## 1.7.4 Support for the Connector Server

Connector Server is one of the features provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles.

A Java connector server is useful when you do not wish to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements.

For information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server, see Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

## 1.7.5 Transformation and Validation of Account Data

You can configure transformation and validation of account data that is brought into or sent from Oracle Identity Governance during reconciliation and provisioning operations by writing Groovy scripts while creating your application.

For more information, see Validation and Transformation of Provisioning and Reconciliation Attributes in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

# 2

# Creating an Application by Using the Office 365 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.

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

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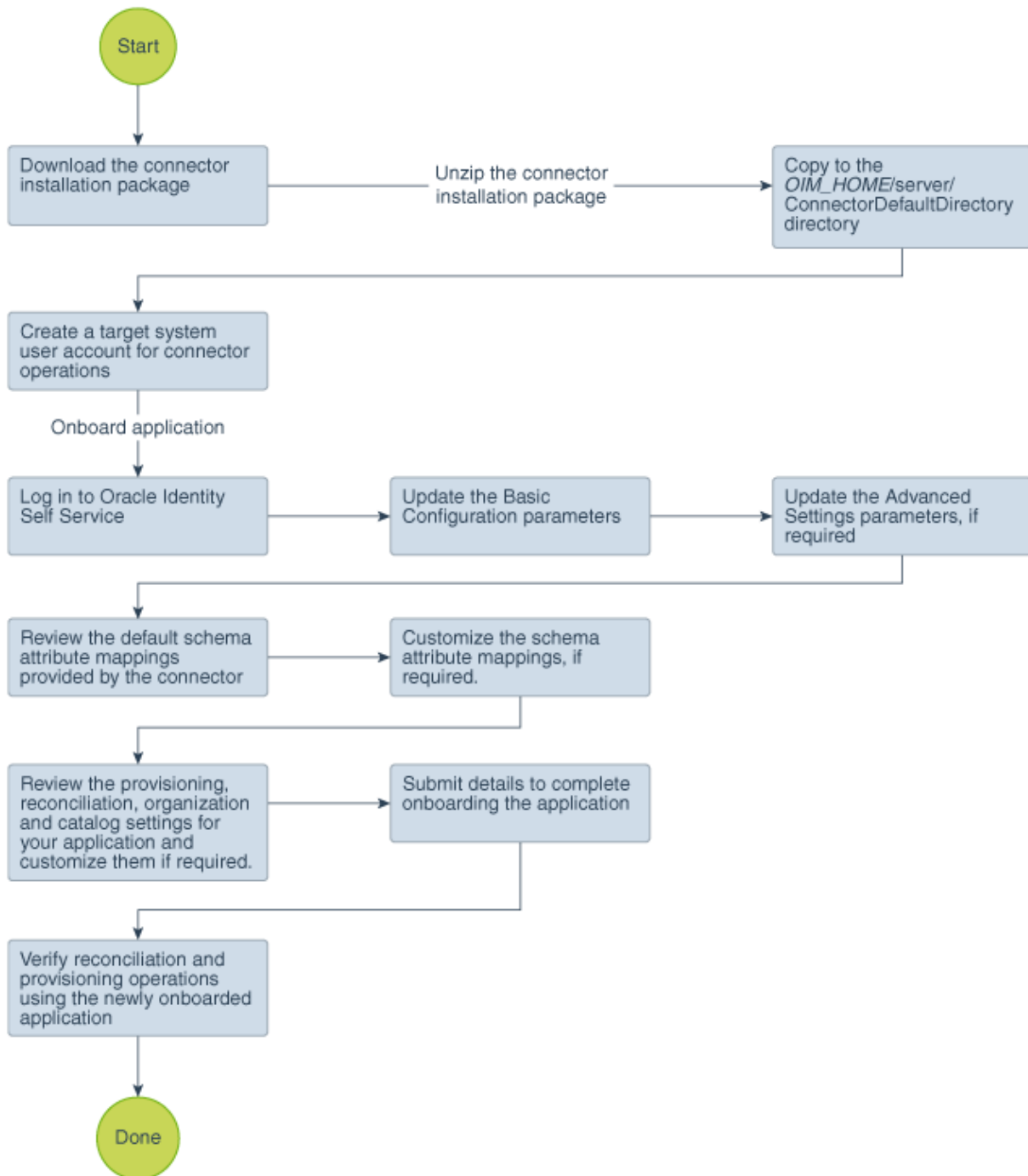


## 2.2 Prerequisites for Creating an Application By Using the Connector

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 Office 365 connector) with the target system is a step that is performed before creating an application instance so that the connector can access Office 365 Graph APIs. It also involves generating the client ID and client secret for authenticating to the target system and setting the permissions for the client application.

Preprovisioning involves performing the following tasks on the target system:

1. Register your client application with Microsoft Azure Active Directory to provide secure sign in and authorization for your services. You can register your client application by creating an application in the Microsoft Azure Management Portal.

2. Generate the client ID and client secret values for your client application. Note down these values as they are required while configuring IT resource parameters.

3. Specify the permissions that the client application requires to access the target system. To do so:

   a. Assign the **Read and write domains** and **Read and write directory data** application permissions that the client application requires on Windows Azure Active Directory.

   b. Assign the following delegated permissions that the client application requires on Windows Azure Active Directory:

      - Read and write directory data
      - Read and write all groups
      - Read all groups
      - Access the directory as the signed-in user
      - Read directory data
      - Read all user's full profiles
      - Read all user's basic profiles
      - Sign in and read user profile

   c. Add the client application to "Company Administrator" and "User Account Administrator" in the Office 365 administrative roles. Visit the following Microsoft support URL for detailed information: https://support.microsoft.com/en-in/kb/3004133

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

## 2.2.2 Downloading the Connector Installation Package

You can obtain the installation package for your connector on the Oracle Technology Network (OTN) website.

To download the connector installation package:

1. Navigate to the OTN website at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html.

2. Click **OTN License Agreement** and read the license agreement.

3. Select the **Accept License Agreement** option.

   You must accept the license agreement before you can download the installation package.

4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.

5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.*

6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

# 2.3 Creating an Application By Using the Connector

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

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

> ✏ **Note:**
>
> For detailed information on each of the steps in this procedure, see Creating Applications of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

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

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

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

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

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

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

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

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

The application is created in Oracle Identity Governance.

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

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

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

---

✎ **See Also:**

- Configuring the Office 365 Connector for details on basic configuration and advanced settings parameters, default user account attribute mappings, default correlation rules, and reconciliation jobs that are predefined for this connector

- Configuring Oracle Identity Governance for details on creating a new form and associating it with your application, if you chose not to create the default form

---

# 3

# Configuring the Office 365 Connector

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

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

## 3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to an Office 365 application. These parameters are common for both target applications and authoritative applications.

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

**Table 3-1    Parameters in the Basic Configuration**

| Parameter | Mandatory ? | Description |
|---|---|---|
| authenticationType | Yes | Enter the type of authentication used by your target system. For this connector, the target system OAuth2.0 client credentials. This is a mandatory attribute while creating an application. Do *not* modify the value of the parameter. **Default value**: `client_credentials` |

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

| Parameter | Mandatory ? | Description |
| --- | --- | --- |
| host | Yes | Enter the host name of the machine hosting your target system. This is a mandatory attribute while creating an application.<br><br>**Sample value**: `graph.windows.net` |
| authenticationServerUrl | Yes | Enter the URL of the authentication server that validates the client ID and client secret for your target system.<br><br>**Sample value**: `https:// login.windows.net/ <mydomain> /oauth2/ token?api-version=1.0` |
| clientId | Yes | Enter the client identifier (a unique string) issued by the authorization server to your client application during the registration process. You obtained the client ID while performing the procedure described in Configuring the Newly Added Application. |
| clientSecret | Yes | Enter the secret key used to authenticate the identity of your client application. You obtained the secret key while performing the procedure described in Configuring the Newly Added Application. |
| uriPlaceHolder | Yes | Enter the key-value pair for replacing place holders in the relURIs. The URI place holder consists of values which are repeated in every relative URL. Values must be comma separated.<br><br>For example, tenant ID and API version values are a part of every request URL. Therefore, we replace it with a key-value pair.<br><br>**Sample value**: `"tenant_id;<domain name>","api_version;api -version=1.6"` |

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

| Parameter | Mandatory ? | Description |
|---|---|---|
| Connector Server Name | No | If you have deployed the Office 365 connector in the Connector Server, then enter the name of the IT resource for the Connector Server.<br>**Sample value**: `Connector Server` |
| port | No | Enter the port number at which the target system is listening.<br>**Sample value**: `80` |
| 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.<br>**Sample value**: `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`.<br>**Default value:** `true` |

# 3.2 Advanced Settings Parameters

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

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

**Table 3-2    Advanced Settings Parameters**

| Parameter | Description |
|---|---|
| relURIs | This entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes. This is a mandatory attribute while creating an application.<br><br>**Default value**:<br>&quot;\_\_ACCOUNT\_\_.CREATEOP=/$(tenant_id)$/users?$(api_version)$&quot;,&quot;\_\_ACCOUNT\_\_.UPDATEOP=/$(tenant_id)$/users/$(\_\_UID\_\_)$?$(api_version)$&quot;,&quot;\_\_ACCOUNT\_\_.SEARCHOP=/$(tenant_id)$/users?$(api_version)$/$(Filter Suffix)$&amp;$top=$(PAGE_SIZE)$&amp;$skiptoken=$(PAGE_TOKEN)$&quot;,&quot;\_\_ACCOUNT\_\_=/$(tenant_id)$/users/$(\_\_UID\_\_)$?$(api_version)$&quot;,&quot;\_\_ACCOUNT\_\_.manager.SEARCHOP=/$(tenant_id)$/users/$(\_\_UID\_\_)$/manager?$(api_version)$&quot;,&quot;\_\_ACCOUNT\_\_.manager=/$(tenant_id)$/users/$(\_\_UID\_\_)$/$links/manager?$(api_version)$&quot;,&quot;\_\_ACCOUNT\_\_.\_\_GROUP\_\_.SEARCHOP=/$(tenant_id)$/users/$(\_\_UID\_\_)$/memberOf?$(api_version)$&amp;$top=$(PAGE_SIZE)$&amp;$skiptoken=$(PAGE_TOKEN)$&quot;,&quot;\_\_ACCOUNT\_\_.\_\_GROUP\_\_.DELETEOP=/$(tenant_id)$/groups/$(\_\_GROUP\_\_.objectId)$/$links/members/$(\_\_UID\_\_)$?$(api_version)$&quot;,&quot;\_\_ACCOUNT\_\_.\_\_GROUP\_\_=/$(tenant_id)$/groups/$(\_\_GROUP\_\_.objectId)$/$links/members?$(api_version)$&quot;,&quot;\_\_GROUP\_\_.CREATEOP=/$(tenant_id)$/groups?$(api_version)$&quot;,&quot;\_\_GROUP\_\_.UPDATEOP=/$(tenant_id)$/groups/$(\_\_UID\_\_)$?$(api_version)$&quot;,&quot;\_\_GROUP\_\_.SEARCHOP=/$(tenant_id)$/groups?$(api_version)$/$(Filter Suffix)$&amp;$top=$(PAGE_SIZE)$&amp;$skiptoken=$(PAGE_TOKEN)$&quot;,&quot;\_\_GROUP\_\_=/$(tenant_id)$/groups/$(\_\_UID\_\_)$?$(api_version)$&quot;,&quot;\_\_GROUP\_\_.member=/$(tenant_id)$/groups/$ |

**Table 3-2 (Cont.) Advanced Settings Parameters**

| Parameter | Description |
|---|---|
| | (__UID__)$/$links/members?$ (api_version)$&quot;,&quot;__ROLE__. SEARCHOP=/$(tenant_id)$/ directoryRoles?$(api_version)$/$ (Filter Suffix)$&quot;,&quot;__ACCOUNT__.__R OLE__=/$(tenant_id)$/ directoryRoles/$ (__ROLE__.objectId)$/$links/ members?$ (api_version)$&quot;,&quot;__ACCOUNT __.__ROLE__.DELETEOP=/$(tenant_id)$/ directoryRoles/$ (__ROLE__.objectId)$/$links/ members/$(__UID__)$?$ (api_version)$&quot;,&quot;__ROLE__. member=/$(tenant_id)$/ directoryRoles/$(__UID__)$/$links/ members?$ (api_version)$&quot;,&quot;__ACCOUNT __.__ROLE__.SEARCHOP=/$(tenant_id)$/ users/$(__UID__)$/memberOf?$ (api_version)$&amp;$top=$ (PAGE_SIZE)$&amp;$skiptoken=$ (PAGE_TOKEN)$&quot;,&quot;__LICENSE_ _.SEARCHOP=/$(tenant_id)$/ subscribedSkus?$(api_version)$/$ (Filter Suffix)$&quot;,&quot;__ACCOUNT__.__L ICENSE__.ADDATTRIBUTE=/$ (tenant_id)$/users/$(__UID__)$/ assignLicense?$ (api_version)$&quot;,&quot;__ACCOUNT __.__LICENSE__.REMOVEATTRIBUTE=/$ (tenant_id)$/users/$(__UID__)$/ assignLicense?$(api_version)$&quot; |
| nameAttributes | This entry holds the name attribute for all the objects that are handled by this connector. For example, for the __ACCOUNT__ object class that it used for User accounts, the name attribute is userPrincipalName. **Default value**: &quot;__ACCOUNT__.userPrincipalName& quot;,&quot;__GROUP__.displayName&qu ot;,&quot;__ROLE__.displayName&quot; ,&quot;__LICENSE__.skuPartNumber&quo t; |

**Table 3-2    (Cont.) Advanced Settings Parameters**

| Parameter | Description |
| --- | --- |
| uidAttributes | This entry holds the uid attribute for all the objects that are handled by this connector. |
| | For example, for `User accounts`, the uid attribute is `objectId`. |
| | In other words, the value `__ACCOUNT__.objectId` in decode implies that the `__UID__` attribute (that is, GUID) of the connector for `__ACCOUNT__` object class is mapped to `objectId` which is the corresponding uid attribute for user accounts in the target system. |
| | **Default value**:&quot;__ACCOUNT__.objectId&quot;,&quot;__GROUP__.objectId&quot;,&quot;__ROLE__.objectId&quot;,&quot;__LICENSE__.skuId&quot; |
| Bundle Name | This entry holds the name of the connector bundle. |
| | **Default value**: `org.identityconnectors.genericrest` |
| Bundle Version | This entry holds the version of the connector bundle. |
| | **Default value**: `12.3.0` |
| Connector Name | This entry holds the name of the connector class. |
| | **Default value**: `org.identityconnectors.genericrest.GenericRESTConnector` |
| opTypes | This entry specifies the HTTP operation type for each object class supported by the connector. Values are comma separated and are in the following format: *OBJ_CLASS.OP=HTTP_OP* |
| | In this format, *OBJ_CLASS* is the connector object class, `OP` is the connector operation (for example, CreateOp, UpdateOp, SearchOp), and `HTTP_OP` is the HTTP operation (GET, PUT, or POST). |
| | **Default value**: `"__ACCOUNT__.CREATEOP=POST","__ACCOUNT__.UPDATEOP=PATCH","__ACCOUNT__.SEARCHOP=GET","__ACCOUNT__.TESTOP=GET","__ACCOUNT__.__GROUP__.UPDATEOP=POST","__ACCOUNT__.manager.CREATEOP=PUT","__ACCOUNT__.manager.UPDATEOP=PUT","__ACCOUNT__.__ROLE__.UPDATEOP=POST","__ACCOUNT__.__LICENSE__.ADDATTRIBUTE=POST","__ACCOUNT__.__LICENSE__.REMOVEATTRIBUTE=POST"` |

**Table 3-2    (Cont.) Advanced Settings Parameters**

| Parameter | Description |
|---|---|
| pageSize | The number of resources/users that appears on a page for a search operation.<br>**Default value**: `100` |
| pageTokenAttribute | The attribute in response payload that denotes the next page token.<br>**Default value**: `odata.nextLink` |
| pageTokenRegex | This attribute is used in the URL while reconciliation to support pagination.<br>**Default value**: `(?<=skiptoken=).*` |
| Any Incremental Recon Attribute Type | By default, during incremental reconciliation, Oracle Identity Governance accepts timestamp information sent from the target system only in Long datatype format. Setting the value of this parameter to `True` indicates that Oracle Identity Governance will accept timestamp information in any datatype format.<br>**Default value**: `True` |
| jsonResourcesTag | This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload.<br>**Default value**:<br>`&quot;__ACCOUNT__=value&quot;,&quot;__GROUP__=value&quot;,&quot;__ROLE__=value&quot;,&quot;__LICENSE__=value&quot;` |
| httpHeaderContentType | This entry holds the content type expected by the target system in the header.<br>**Default value**: `application/json` |
| httpHeaderAccept | This entry holds the accept type expected from the target system in the header.<br>**Default value**: `application/json` |
| specialAttributeTargetFormat | This entry lists the format in which an attribute is present in the target system endpoint.<br>For example, the alias attribute will be present as `aliases.alias` in the target system endpoint. Values are comma separated and are presented in the following format: *OBJ_CLASS.ATTR_NAME=TARGET_FORMAT*<br>**Default value**`"__ACCOUNT__.manager=objectId","__GROUP__.member=url","__ROLE__.member=url","__ACCOUNT__.__GROUP__=value","__ACCOUNT__.__ROLE__=value","__ROLE__.member=value","__GROUP__.member=value","__ACCOUNT__.__LICENSE__=value.skuId"` |

**Table 3-2    (Cont.) Advanced Settings Parameters**

| Parameter | Description |
| --- | --- |
| specialAttributeHandling | This entry lists the special attributes whose values should be sent to the target system one by one ("SINGLE"). Values are comma separated and are in the following format: |
| | *OBJ_CLASS.ATTR_NAME.PROV_OP*=SINGLE |
| | For example, the `__ACCOUNT__.manager.UPDATEOP=SINGLE` value in decode implies that during an update provisioning operation, the `manager` attribute of the `__ACCOUNT__` object class must be sent to the target system one-by-one. |
| | **Default value**`"__ACCOUNT__.__GROUP__.CREATEOP=SINGLE","__ACCOUNT__.__GROUP__.UPDATEOP=SINGLE","__ACCOUNT__.manager.CREATEOP=SINGLE","__ACCOUNT__.manager.UPDATEOP=SINGLE","__ACCOUNT__.__ROLE__.CREATEOP=SINGLE","__ACCOUNT__.__ROLE__.UPDATEOP=SINGLE","__ACCOUNT__.__LICENSE__.ADDATTRIBUTE=SINGLE","__ACCOUNT__.__LICENSE__.REMOVEATTRIBUTE=SINGLE"` |

**Table 3-2    (Cont.) Advanced Settings Parameters**

| Parameter | Description |
| --- | --- |
| customPayload | This entry lists the payloads for all operations that are not in the standard format.<br><br>**Default value:**`"__ACCOUNT__.__GROUP__.UPDATEOP ={\"url\":\"https:// graph.windows.net/ oimconnect.onmicrosoft.com/ directoryObjects/$(__UID__)$ \"}","__ACCOUNT__.__GROUP__.CREATEOP ={\"url\":\"https:// graph.windows.net/ oimconnect.onmicrosoft.com/ directoryObjects/$(__UID__)$ \"}","__ACCOUNT__.manager.CREATEOP={ \"url\":\"https://graph.windows.net/ oimconnect.onmicrosoft.com/ directoryObjects/$(manager)$ \"}","__ACCOUNT__.manager.UPDATEOP={ \"url\":\"https://graph.windows.net/ oimconnect.onmicrosoft.com/ directoryObjects/$(manager)$ \"}","__ACCOUNT__.__ROLE__.UPDATEOP ={\"url\":\"https:// graph.windows.net/ oimconnect.onmicrosoft.com/ directoryObjects/$(__UID__)$ \"}","__ACCOUNT__.__ROLE__.CREATEOP ={\"url\":\"https:// graph.windows.net/ oimconnect.onmicrosoft.com/ directoryObjects/$(__UID__)$ \"}","__ACCOUNT__.__LICENSE__.ADDATT RIBUTE={\"addLicenses\": [{\"skuId\": \"$(skuId)$ \"}],\"removeLicenses\": []}","__ACCOUNT__.__LICENSE__.REMOVE ATTRIBUTE={\"addLicenses\": [],\"removeLicenses\": [\"$(skuId)$ \"]}"` |
| statusAttributes | This entry lists the name of the target system attribute that holds the status of an account. For example, for the __ACCOUNT__ object class that it used for User accounts, the status attribute is `accountEnabled`.<br><br>**Default value:**`"__ACCOUNT__.accountEnabled"` |
| passwordAttribute | This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute of the connector in OIM.<br><br>**Default value:** `passwordProfile.password` |

**Table 3-2    (Cont.) Advanced Settings Parameters**

| Parameter | Description |
|---|---|
| targetObjectIdentifier | This entry specifies the key-value pair for replacing place holders in the relURIs. Values are comma separated and in the *KEY*;*VALUE* format.<br><br>**Default value:**<br>`&quot;__ACCOUNT__.__GROUP__=objectTy pe;Group&quot;,&quot;__ACCOUNT__.__R OLE__=objectType;Role&quot;` |

# 3.3 Attribute Mappings

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

- Attribute Mappings for the Target Application
- Attribute Mappings for the Authoritative Application

## 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 Office 365 Target Application**

Table 3-3 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Office 365 target application attributes. The table also lists whether a specific attribute is used during provisioning or reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

**Table 3-3    Default Attributes for Office 365 Target Application**

| Display Name | Target Attribute | Data Type | Mandatory Provisioning Property? | Provision Field? | Recon Field? | Key Field? | Case Insensitive? | Advanced Flag Settings |
|---|---|---|---|---|---|---|---|---|
| Object Id | __UID__ | String | No | Yes | Yes | Yes | Yes | Yes |
| User Principal Name | __NAME__ | String | Yes | Yes | Yes | No | Not applicable | Yes |

**Table 3-3    (Cont.) Default Attributes for Office 365 Target Application**

| Display Name | Target Attribute | Data Type | Mandatory Provisioning Property? | Provision Field? | Recon Field? | Key Field? | Case Insensitive? | Advanced Flag Settings |
|---|---|---|---|---|---|---|---|---|
| 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 |
| Office365 Server | | Long | Yes | No | Yes | Yes | Not applicable | Yes |
| Status | __ENABLE__ | String | No | No | Yes | No | Not applicable | Yes |
| Password | __PASSWORD__ | String | Yes | Yes | No | No | Not applicable | Yes |
| Change Password On Next Logon | passwordProfile.forceChangePasswordNextLogin | String | No | Yes | No | No | Not applicable | Yes |

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

**Figure 3-1    Default Attribute Mappings for Office 365 User Account**

| 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 ▾ | ☐ | ☑ | ☑ | ☑ | ☐ | ✖ ☰ |
| Select a value 🔍 | User Principal Nar | __NAME__ 🔍 | String ▾ | ☑ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Password | __PASSWORD__ 🔍 | String ▾ | ☑ | ☑ | ☐ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | First Name | givenName 🔍 | String ▾ | ☐ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Last Name | surname 🔍 | String ▾ | ☐ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Display Name | displayName 🔍 | String ▾ | ☑ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Usage Location | usageLocation 🔍 | String ▾ | ☐ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | City | city 🔍 | String ▾ | ☐ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Country | country 🔍 | String ▾ | ☐ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Manager | manager 🔍 | String ▾ | ☐ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Preferred Langua | preferredLanguage 🔍 | String ▾ | ☐ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Mail NickName | mailNickname 🔍 | String ▾ | ☑ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Office365 Server | 🔍 | Long ▾ | ☑ | ☐ | ☑ | ☑ | ☐ | ✖ ☰ |
| Select a value 🔍 | Change Password | passwordProfile.forceCh... 🔍 | String ▾ | ☐ | ☑ | ☐ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Account Enabled | accountEnabled 🔍 | String ▾ | ☐ | ☑ | ☑ | ☐ | ☐ | ✖ ☰ |
| Select a value 🔍 | Status | __ENABLE__ 🔍 | String ▾ | ☐ | ☐ | ☑ | ☐ | ☐ | ✖ ☰ |

**Roles Entitlement**

Table 3-4 lists the roles-specific attribute mappings between the process form fields in
Oracle Identity Governance and Office 365 target application attributes. The table lists
whether a given attribute is mandatory during provisioning. It also lists whether a given
attribute is used during reconciliation and whether it is a matching key field for fetching
records during reconciliation.

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

**Table 3-4     Default Attribute Mappings for Roles**

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

Figure 3-2 shows the default roles entitlement mapping.

**Figure 3-2     Default Attribute Mappings for Role**



**Groups Entitlement**

Table 3-5 lists the group forms attribute mappings between the process form fields in Oracle Identity Governance and Office 365 target application attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

**Table 3-5     Default Attribute Mappings for Groups Forms**

| Display Name | Target Attribute | Data Type | Mandatory Provisioning Property? | Recon Field? | Key Field? | Case Insensitive? |
|---|---|---|---|---|---|---|
| Group Name | __GROUP_ _~__GROU P__~objectI d | String | No | Yes | Yes | No |

Figure 3-3 shows the default attribute groups mapping.

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



**Licenses Entitlement**

Table 3-6 lists the license attribute mappings between the process form fields in Oracle Identity Governance and Office 365 target application attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

**Table 3-6    Default Attribute Mappings for Licenses**

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

Figure 3-4 shows the default attribute licenses mapping.

**Figure 3-4    Default Attribute Mappings for Licenses**

## 3.3.2 Attribute Mappings for the Authoritative Application

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

Table 3-7 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Office 365 Authoritative application attributes. The table also lists the data type for a given attribute and specified whether it is a mandatory attribute for reconciliation.
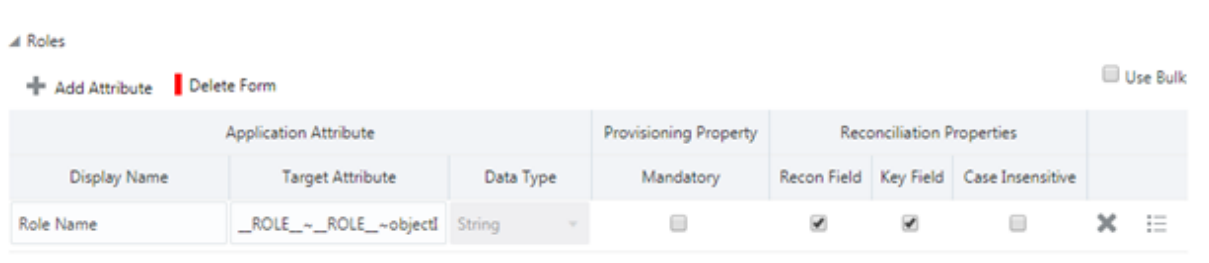
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating an Authoritative Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

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

The Organization Name, Xellerate Type, and Role identity attributes are mandatory fields on the OIG User form. They cannot be left blank during reconciliation. The target attribute mappings for these identity attributes are empty by default because there are no corresponding columns in the target system. Therefore, the connector provides default values (as listed in the Table 3-7 ) that it can use during reconciliation. For example, the default target attribute value for the Organization Name attribute is Xellerate Users. This implies that the connector reconciles all target system user accounts into the Xellerate Users organization in Oracle Identity Governance. Similarly, the default attribute value for Xellerate Type attribute is End-User, which implies that all reconciled user records are marked as end users.

**Table 3-7    Default Attributes for Office 365 Authoritative Application**

| Display Name | Target Attribute | Data Type | Mandatory Provisioning Property? | Recon Field? | Advanced Flag Settings | Default Value for Identity Display Name |
|---|---|---|---|---|---|---|
| User Login | __NAME__ | String | No | Yes | Yes | NA |
| Office365 GUID | __UID__ | String | No | Yes | Yes | NA |
| First Name | givenName | String | No | Yes | Yes | NA |
| Last Name | surname | String | No | Yes | Yes | NA |
| Display Name | displayName | String | No | Yes | Yes | NA |
| Locality Name | usageLocation | String | No | Yes | Yes | NA |
| Country | country | String | No | Yes | Yes | NA |
| Manager Login | manager | String | No | Yes | Yes | NA |
| usr_locale | preferredLanguage | String | No | Yes | Yes | NA |

**Table 3-7    (Cont.) Default Attributes for Office 365 Authoritative Application**

| Display Name | Target Attribute | Data Type | Mandatory Provisioning Property? | Recon Field? | Advanced Flag Settings | Default Value for Identity Display Name |
|---|---|---|---|---|---|---|
| Xellerate Type | | String | No | Yes | Yes | End-User |
| Role | | String | No | Yes | Yes | Full-Time |
| Organization Name | | String | No | Yes | Yes | Xellerate Users |
| Status | __ENABLE__ | String | No | Yes | Yes | NA |

Figure 3-5 shows the default User account attribute mappings.

**Figure 3-5    Default Attributes for Office 365 Authoritative Application**



## 3.4 Correlation Rules

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

- Correlation Rules for the Target Application
- Correlation Rules for the Authoritative Application

## 3.4.1 Correlation Rules for the Target Application

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

**Predefined Identity Correlation Rules**

By default, the Office 365 connector provides a simple correlation rule when you create a target application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the target system repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

Table 3-8 lists the default simple correlation rule for an Office 365 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 3-8    Predefined Identity Correlation Rule for an Office 365 Connector**

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

In this identity rule:

- __NAME__ is a single-valued attribute on the target system that identifies the user account.
- User Login is the field on the OIG User form.

Figure 3-6 shows the simple correlation rule for an Office 365 target application.

**Figure 3-6    Simple Correlation Rule for an Office 365 Target Application**

**Predefined Situations and Responses**

The Office 365 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 3-9 lists the default situations and responses for an Office 365 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 3-9    Predefined Situations and Responses for an Office 365 Target Application**

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

Figure 3-7 shows the situations and responses for an Office 365 that the connector provides by default.

**Figure 3-7    Predefined Situations and Responses for an Office 365 Target Application**



## 3.4.2 Correlation Rules for the Authoritative Application

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

**Predefined Identity Correlation Rules**

By default, the Office 365 connector provides a simple correlation rule when you create an authoritative application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the target system repository,

determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

Table 3-10 lists the default simple correlation rule for an Office 365 connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 3-10    Predefined Identity Correlation Rule for an Office 365 Authoritative Application**

| Authoritative Attribute | Element Operator | Identity Attribute | Case Sensitive? |
|---|---|---|---|
| __NAME__ | Equals | User Login | No |
| _UID_ | Equals | Office365 GUID | No |

**Correlation Rule element**: (__NAME__Equals __User Login) OR (_UID_Equals Office365 GUID)

In the first correlation rule element:

• User Login is the User ID field of the OIM User form.

• __NAME__ is the unique login name of a user.

In the second correlation rule element:

• Office365 GUID is a UDF (user defined field) for mapping target object ID with an OIM user.

• _UID_ is the Object Id for an Office365 user.

**Rule operator**: OR

Figure 3-8 shows the simple correlation rule for an Office 365 Authoritative application.

**Figure 3-8    Simple Correlation Rule for an Office 365 Authoritative Application**

**Predefined Situations and Responses**

The Office 365 connector provides a default set of situations and responses when you create an Authoritative application. These situations and responses specify the action that Oracle Identity Governance must take based on the result of a reconciliation event.

Table 3-9 lists the default situations and responses for an Office 365 Authoritative Application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.*

**Table 3-11    Predefined Situations and Responses for an Office 365 Authoritative Application**

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

Figure 3-9 shows the situations and responses for an Office 365 that the connector provides by default.

**Figure 3-9    Predefined Situations and Responses for an Office 365 Authoritative Application**
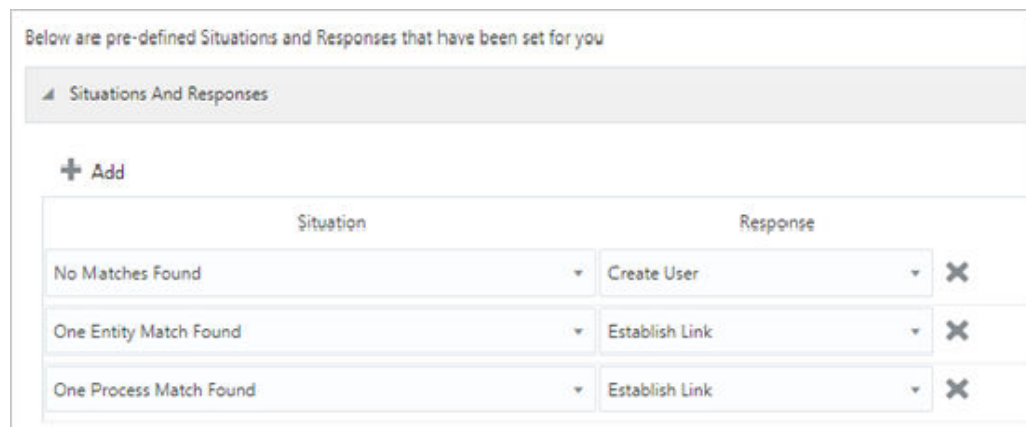


# 3.5 Reconciliation Jobs

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:

- Office365 Full User Reconciliation: Use this reconciliation job to reconcile user data from a target application.

- Office365 User Trusted Reconciliation: Use this reconciliation job to reconcile user data from an authoritative application.

Table 3-12 describes the parameters of the Office365 Full User Reconciliation job.

**Table 3-12    Parameters of the Office365 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.<br><br>Do *not* 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.<br><br>**Note**: Do not enter a value for this parameter. The reconciliation engine automatically enters a value in this parameter.<br><br>**Sample value**: `<String>2017-09-19T14:16:24Z</String>` |
| Object Type | This parameter holds the name of the object type for the reconciliation run.<br><br>**Default value**: `User`<br><br>Do *not* change the default value. |
| Filter Suffix | Enter the search filter for fetching user records from the target system during a reconciliation run.<br><br>**Sample value when incremental recon is enabled**: `%20and%20startswith(displayName,'user1')`<br><br>**Sample value when incremental recon is not enabled**: `&$filter=startswith(displayName,'user1')`<br><br>For more information about creating filters, see Performing Limited Reconciliation . |
| Scheduled Task Name | Name of the scheduled task used for reconciliation.<br><br>Do *not* modify the value of this parameter. |

**Table 3-12    (Cont.) Parameters of the Office365 Full User Reconciliation Job**

| Parameter | Description |
| --- | --- |
| Incremental Recon Attribute | Enter the name of the attribute that holds the timestamp at which the token record was modified.<br><br>**Sample value**: `lastDirSyncTime` |

Table 3-13 describes the parameters of Office365 User Trusted Reconciliation job.

**Table 3-13    Parameters of the Office365 User Trusted Reconciliation Job**

| Parameter | Description |
| --- | --- |
| Application name | Name of the AOB Application with which the job is associated. This value is the same as the value that you provided for the Application Name field while creating your target application.<br><br>Do *not* modify this value. |
| Filter Suffix | Enter the search filter for fetching user records from the target system during a reconciliation run.<br><br>**Sample value**:<br>`%20and%20startswith(displayName,'tap')`<br><br>For more information about creating filters, see Performing Limited Reconciliation . |
| Incremental Recon Attribute | Attribute that holds the timestamp at which the token record was modified. |
| Latest Token | This parameter holds the value of the attribute that is specified as the value of the Incremental Recon Attribute attribute. The Latest Token parameter is used for internal purposes. By default, this value is empty.<br><br>**Note:** If an appropriate Increment Recon attribute has been specified, then do not enter a value for this parameter.<br><br>Sample value: `<String>2017-11-30T04:44:29Z</String>` |
| Object Type | This parameter holds the name of the object type for the reconciliation run.<br><br>Default value: `User`<br><br>**Note:** Do not change the default value. |
| Scheduled Task Name | Name of the scheduled task used for reconciliation.<br><br>Do *not* modify the value of this parameter. |

**Reconciliation Jobs for Entitlements**

The following jobs are available for reconciling entitlements:

- Office365 Group Lookup Reconciliation

- Office365 Licenses Lookup Reconciliation

- Office365 Roles Lookup Reconciliation

- Office365 Manager Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

**Table 3-14    Parameters of the Reconciliation Jobs for Entitlements**

| Parameter | Description |
| --- | --- |
| Application Name | Current AOB application name with which the reconciliation job is associated. <br><br> Default value: `Office365` <br><br> Do *not* modify this value. |
| Code Key Attribute | Name of the connector attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). <br><br> Default value: `__UID__` <br><br> Do *not* modify this value. |
| Decode Attribute | Name of the connector attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). <br><br> Default value: `__NAME__` |
| Lookup Name | Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system. <br><br> Depending on the Reconciliation job that you are using, the default values are as follows: <br><br> • For Office365 Group Lookup Reconciliation: `Lookup.Office365.Groups` <br> • For Office365 Licenses Lookup Reconciliation: `Lookup.Office365.Licenses` <br> • For Office365 Roles Lookup Reconciliation: `Lookup.Office365.Roles` <br> • For Office365 Manager Lookup Reconciliation: `Lookup.Office365.Manager` <br><br> If you create a copy of any of these lookup definitions, then enter the name of that new lookup definition as the value of the Lookup Name attribute. |

**Table 3-14    (Cont.) Parameters of the Reconciliation Jobs for Entitlements**

| Parameter | Description |
|---|---|
| Object Type | Enter the type of object you want to reconcile.<br><br>Depending on the reconciliation job that you are using, the default values are as follows:<br><br>• For Office365 Group Lookup Reconciliation: `__GROUP__`<br>• For Office365 Licenses Lookup Reconciliation: `__LICENSE__`<br>• For Office365 Roles Lookup Reconciliation: `__ROLE__`<br>• For Office365 Manager Lookup Reconciliation: `__USER__`<br><br>**Note**: Do not change the value of this parameter. |

# 4

# Performing Postconfiguration Tasks for the Office 365 Connector

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

- Configuring Oracle Identity Governance
- Harvesting Entitlements and Sync Catalog
- Managing Logging for the Connector
- Configuring the IT Resource for the Connector Server
- Localizing Field Labels in UI Forms
- Configuring SSL

## 4.1 Configuring Oracle Identity Governance

During application creation, if you did not choose to create a default form, then you must create a UI form for the application that you created by using the connector.

> ✎ **Note:**
>
> Perform the procedures described in this section only if you did not choose to create the default form during creating the application.

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

- Creating and Activating a Sandbox
- Creating a New UI Form
- Publishing a Sandbox
- Updating an Existing Application Instance with a New Form

### 4.1.1 Creating and Activating a Sandbox

You must create and activate a sandbox to begin using the customization and form management features. You can then publish the sandbox to make the customizations available to other users.

See Creating a Sandbox and Activating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

## 4.1.2 Creating a New UI Form

You can use Form Designer in Oracle Identity System Administration to create and manage application instance forms.

See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

While creating the UI form, ensure that you select the resource object corresponding to the newly created application that you want to associate the form with. In addition, select the **Generate Entitlement Forms** check box.

## 4.1.3 Publishing a Sandbox

Before publishing a sandbox, perform this procedure as a best practice to validate all sandbox changes made till this stage as it is difficult to revert the changes after a sandbox is published.

1. In Identity System Administration, deactivate the sandbox.

2. Log out of Identity System Administration.

3. Log in to Identity Self Service using the xelsysadm user credentials and then activate the sandbox that you deactivated in Step 1.

4. In the Catalog, ensure that the application instance form for your resource appears with correct fields.

5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

## 4.1.4 Updating an Existing Application Instance with a New Form

For any changes that you do in the schema of your application in Identity Self Service, you must create a new UI form and update the changes in an application instance.

To update an existing application instance with a new form:

1. Create and activate a sandbox.

2. Create a new UI form for the resource.

3. Open the existing application instance.

4. In the Form field, select the new UI form that you created.

5. Save the application instance.

6. Publish the sandbox.

> **See Also:**
>
> - Creating a Sandbox and Activating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*
> - Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*
> - Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*

## 4.2 Harvesting Entitlements and Sync Catalog

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

To harvest entitlements and sync catalog:

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

2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.

3. Run the Catalog Synchronization Job scheduled job.

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

## 4.3 Managing Logging for the Connector

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

## 4.3.1 Understanding Log Levels

When you enable logging, Oracle Identity Governance automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations.

ODL is the principle logging service used by Oracle Identity Governance and is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

*   SEVERE.intValue()+100

    This level enables logging of information about fatal errors.

*   SEVERE

    This level enables logging of information about errors that might allow Oracle Identity Governance to continue running.

*   WARNING

    This level enables logging of information about potentially harmful situations.

*   INFO

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

*   CONFIG

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

*   FINE, FINER, FINEST

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

These message types are mapped to ODL message type and level combinations as shown in Table 4-2.

**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 |

**Table 4-2    Log Levels and ODL Message Type:Level Combinations**

| Java Level | ODL Message Type:Level |
|---|---|
| SEVERE.intValue()+100 | INCIDENT_ERROR:1 |

**Table 4-2    (Cont.) Log Levels and ODL Message Type:Level Combinations**

| Java Level | ODL Message Type:Level |
|---|---|
| SEVERE | ERROR:1 |
| WARNING | WARNING:1 |
| INFO | NOTIFICATION:1 |
| CONFIG | NOTIFICATION:16 |
| FINE | TRACE:1 |
| FINER | TRACE:16 |
| FINEST | TRACE:32 |

The configuration file for OJDL is logging.xml, which is located at the following path:

*DOMAIN_HOME*/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name specified during the installation of Oracle Identity Governance.

## 4.3.2 Enabling Logging

Perform this procedure to enable logging in Oracle WebLogic Server.

To enable logging in Oracle WebLogic Server:

1.  Edit the logging.xml file as follows:

    a.  Add the following blocks in the file:

```
<log_handler name='Office365-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.GENERICREST"
level="[LOG_LEVEL]" useParentHandlers="false">
    <handler name="Office365-handler"/>
    <handler name="console-handler"/>
</logger>


<logger name="ORG.IDENTITYCONNECTORS.RESTCOMMON"
level="[LOG_LEVEL]" useParentHandlers="false">
    <handler name="Office365-handler"/>
```

```
<handler name="console-handler"/>
</logger>
```

b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. #unique_63/ unique_63_Connect_42_LOGLEVELSANDODLMESSAGETYPELEVELCOMB-FAC17AE6 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='Office365-handler'
level='NOTIFICATION:1'class='oracle.core.ojdl.logging.ODLHandlerF
actory'>
    <property name='logreader:' value='off'/>
    <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1
\servers\oim_server1\logs\oim_server1-diagnostic-1.log'/>
    <property name='format' value='ODL-Text'/>
    <property name='useThreadName' value='true'/>
    <property name='locale' value='en'/>
    <property name='maxFileSize' value='5242880'/>
    <property name='maxLogSize' value='52428800'/>
    <property name='encoding' value='UTF-8'/>
</log_handler>

<logger name="ORG.IDENTITYCONNECTORS.GENERICREST"
level="NOTIFICATION:1" useParentHandlers="false">
    <handler name="Office365-handler"/>
    <handler name="console-handler"/>
</logger>

<logger name="ORG.IDENTITYCONNECTORS.RESTCOMMON"
level="NOTIFICATION:1" useParentHandlers="false">
    <handler name="Office365-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 `Office365 Connector Server`.

In Oracle Identity System Administration, search for and edit the Office365 Connector Server IT resource to specify values for the parameters of IT resource for the Connector Server listed in Table 4-3. 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 4-3    Parameters of the IT Resource for the Office 365 Connector Server**

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

## 4.5 Localizing Field Labels in UI Forms

You can localize UI form field labels by using the resource bundle corresponding to the language you want to use. Resource bundles are available in the connector installation media.

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

1. Log in to Oracle Enterprise Manager.

2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**

3. In the right pane, from the Application Deployment list, select **MDS Configuration.**

4. On the MDS Configuration page, click **Export** and save the archive (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer**.**

5. Extract the contents of the archive, and open the following file in a text editor:

```
SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xl
f
```

> **✏ 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 Office365 Application instance. The original code is:

   ```
    <trans-unit id="$
   {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
   rceBundle']
   ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
   .userEO.UD_ USER_PRINCIPAL_NAME__c_description']}">
   <source>User Principal Name</source><target/>
   </trans-unit>
   <trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.RSAForm.entity.Of
   fice365FormEO.UD_USER_PRINCIPAL_NAME __c_LABEL"><source>First
   Name</source><target/>
   </trans-unit>
   ```

d. Open the resource file from the connector package, for example Office365_ja.properties, and get the value of the attribute from the file, for example,

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

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBu ndle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.use rEO.UD_GA_USR_ USER_PRINCIPAL_NAME __c_description']}">
<source>Account Name</source>
<target>u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit> <trans-
unitid="sessiondef.oracle.iam.ui.runtime.form.model.Office365.ent
ity 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 Office 365 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 Office 365.

2. Copy the public key certificate of Office 365 to the computer hosting Oracle Identity Governance.

3. Run the following `keytool` command to import the public key certificate into the identity key store in Oracle Identity Governance:

```
keytool -import -alias ALIAS -trustcacerts -file CERT_FILE_NAME -
keystore KEYSTORE_NAME -storepass PASSWORD
```
In this command:

- *ALIAS* is the public key certificate alias.

- *CERT_FILE_NAME* is the full path and name of the certificate store (the default is cacerts).

- *KEYSTORE_NAME* is the name of the keystore.

- *PASSWORD* is the password of the keystore.

The following is a sample value for this command:

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

> **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 Office 365 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
- Performing Delete 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 Office 365 connector, the incremental reconciliation option is not enabled by default. The connector supports incremental reconciliation only if the target system contains an attribute that holds the timestamp at which an object is created or modified.

**Configuring Incremental Reconciliation**

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

> **Note:**
>
> The connector supports incremental reconciliation only if the target system contains an attribute that holds the timestamp at which an object is created or modified.
>
> For example, consider `lastDirSyncTime` as a sample `Incremental Recon Attribute` that you specify for the Office365 User Reconciliation Scheduled job. After the first full reconciliation run, the connector populates the `Latest Token` parameter with a timestamp. In subsequent reconciliation runs, the connector fetches only the user records that are created or updated after the `Latest Token` timestamp.

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

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

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

   **Sample latest token value**: `2017-08-21T05:48:54Z`

3. Open Identity Self-Service application.

4. Click **Manage**.

5. Click **Application**.

6. Search and open the application you have created.

7. Expand the **Advanced Settings** option and modify the value of `relURIs` as per your requirement.

   - To support Incremental Reconciliation for both Users and Groups, perform step 8.

   - To support Incremental Reconciliation only for Users, perform step 9.

8. To use both User and Group Reconciliation jobs, modify relURIs as follows:

   - For **Authoritative Application**,
     modify `relURIs` as: `"__ACCOUNT__.SEARCHOP=/$(tenant_id)$/users?$(api_version)$&$filter=$(Incremental Recon Attribute)$%20ge%20datetime'$(Latest Token)$'/$(Filter Suffix)$&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__=/$(tenant_id)$/users/$(__UID__)$?$(api_version)$","__ACCOUNT__.manager.SEARCHOP=/$(tenant_id)$/users/$(__UID__)$/manager?$(api_version)$","__ACCOUNT__.manager=/$(tenant_id)$/users/$(__UID__)$/$links/manager?$(api_version)$"`

- For **Target Application**, modify
  `relURIs` as: `"__ACCOUNT__.CREATEOP=/$(tenant_id)$/users?$(api_version)$","__ACCOUNT__.UPDATEOP=/$(tenant_id)$/users/$(__UID__)$?$(api_version)$","__ACCOUNT__.SEARCHOP=/$(tenant_id)$/users?$(api_version)$&$filter=$(Incremental Recon Attribute)$%20ge%20datetime'$(Latest Token)$'/$(Filter Suffix)$&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__=/$(tenant_id)$/users/$(__UID__)$?$(api_version)$","__ACCOUNT__.manager.SEARCHOP=/$(tenant_id)$/users/$(__UID__)$/manager?$(api_version)$","__ACCOUNT__.manager=/$(tenant_id)$/users/$(__UID__)$/$links/manager?$(api_version)$","__ACCOUNT__.__GROUP__.SEARCHOP=/$(tenant_id)$/users/$(__UID__)$/memberOf?$(api_version)$&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__.__GROUP__.DELETEOP=/$(tenant_id)$/groups/$(__GROUP__.objectId)$/$links/members/$(__UID__)$?$(api_version)$","__ACCOUNT__.__GROUP__=/$(tenant_id)$/groups/$(__GROUP__.objectId)$/$links/members?$(api_version)$","__GROUP__.CREATEOP=/$(tenant_id)$/groups?$(api_version)$","__GROUP__.UPDATEOP=/$(tenant_id)$/groups/$(__UID__)$?$(api_version)$","__GROUP__.SEARCHOP=/$(tenant_id)$/groups?$(api_version)$&$filter=$(Incremental Recon Attribute)$%20ge%20datetime'$(Latest Token)$'/$(Filter Suffix)$&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__GROUP__=/$(tenant_id)$/groups/$(__UID__)$?$(api_version)$","__GROUP__.member=/$(tenant_id)$/groups/$(__UID__)$/$links/members?$(api_version)$","__ROLE__.SEARCHOP=/$(tenant_id)$/directoryRoles?$(api_version)$/$(Filter Suffix)$","__ACCOUNT__.__ROLE__=/$(tenant_id)$/directoryRoles/$(__ROLE__.objectId)$/$links/members?$(api_version)$","__ACCOUNT__.__ROLE__.DELETEOP=/$(tenant_id)$/directoryRoles/$(__ROLE__.objectId)$/$links/members/$(__UID__)$?$(api_version)$","__ROLE__.member=/$(tenant_id)$/directoryRoles/$(__UID__)$/$links/members?$(api_version)$","__ACCOUNT__.__ROLE__.SEARCHOP=/$(tenant_id)$/users/$(__UID__)$/memberOf?$(api_version)$&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__LICENSE__.SEARCHOP=/$(tenant_id)$/subscribedSkus?$(api_version)$/$(Filter Suffix)$","__ACCOUNT__.__LICENSE__.ADDATTRIBUTE=/$(tenant_id)$/users/$(__UID__)$/assignLicense?$(api_version)$","__ACCOUNT__.__LICENSE__.REMOVEATTRIBUTE=/$(tenant_id)$/users/$(__UID__)$/assignLicense?$(api_version)$"`

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

   - For **Authoritative Application**,
     modify `relURIs` as: **:**`"__ACCOUNT__.SEARCHOP=/$(tenant_id)$/users?$(api_version)$&$filter=$(Incremental Recon Attribute)$%20ge%20datetime'$(Latest Token)$'/$(Filter Suffix)$&$top=$(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__ACCOUNT__=/$(tenant_id)$/users/$(__UID__)$?$(api_version)$","__ACCOUNT__.manager.SEARCHOP=/$(tenant_id)$/users/$(__UID__)$/manager?$(api_version)$","__ACCOUNT__.manager=/$(tenant_id)$/users/$(__UID__)$/$links/manager?$(api_version)$"`

- For **Target Application**, modify
  relURIs as: `"__ACCOUNT__.CREATEOP=/$(tenant_id)$/`
  `users?$(api_version)$","__ACCOUNT__.UPDATEOP=/$(tenant_id)$/users/$`
  `(__UID__)$?$(api_version)$","__ACCOUNT__.SEARCHOP=/$(tenant_id)$/`
  `users?$(api_version)$&$filter=$(Incremental Recon`
  `Attribute)$%20ge%20datetime'$(Latest Token)$'/$`
  `(Filter Suffix)$&$top=$(PAGE_SIZE)$&$skiptoken=$`
  `(PAGE_TOKEN)$","__ACCOUNT__=/$(tenant_id)$/users/$(__UID__)$?$`
  `(api_version)$","__ACCOUNT__.manager.SEARCHOP=/$(tenant_id)$/`
  `users/$(__UID__)$/manager?$(api_version)$","__ACCOUNT__.manager=/$`
  `(tenant_id)$/users/$(__UID__)$/$links/manager?$`
  `(api_version)$","__ACCOUNT__.__GROUP__.SEARCHOP=/$`
  `(tenant_id)$/users/$(__UID__)$/memberOf?$`
  `(api_version)$&$top=$(PAGE_SIZE)$&$skiptoken=$`
  `(PAGE_TOKEN)$","__ACCOUNT__.__GROUP__.DELETEOP=/$`
  `(tenant_id)$/groups/$(__GROUP__.objectId)$/$links/members/$`
  `(__UID__)$?$(api_version)$","__ACCOUNT__.__GROUP__=/$`
  `(tenant_id)$/groups/$(__GROUP__.objectId)$/$links/members?$`
  `(api_version)$","__GROUP__.CREATEOP=/$(tenant_id)$/groups?$`
  `(api_version)$","__GROUP__.UPDATEOP=/$(tenant_id)$/groups/$`
  `(__UID__)$?$(api_version)$","__GROUP__.SEARCHOP=/$(tenant_id)$/`
  `groups?$(api_version)$/$(Filter Suffix)$&$top=$`
  `(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__GROUP__=/$(tenant_id)$/`
  `groups/$(__UID__)$?$(api_version)$","__GROUP__.member=/$`
  `(tenant_id)$/groups/$(__UID__)$/$links/members?$`
  `(api_version)$","__ROLE__.SEARCHOP=/$(tenant_id)$/directoryRoles?$`
  `(api_version)$/$(Filter Suffix)$","__ACCOUNT__.__ROLE__=/$`
  `(tenant_id)$/directoryRoles/$(__ROLE__.objectId)$/$links/`
  `members?$(api_version)$","__ACCOUNT__.__ROLE__.DELETEOP=/$`
  `(tenant_id)$/directoryRoles/$(__ROLE__.objectId)$/$links/`
  `members/$(__UID__)$?$(api_version)$","__ROLE__.member=/$`
  `(tenant_id)$/directoryRoles/$(__UID__)$/$links/members?$`
  `(api_version)$","__ACCOUNT__.__ROLE__.SEARCHOP=/$(tenant_id)$/`
  `users/$(__UID__)$/memberOf?$(api_version)$&$top=$`
  `(PAGE_SIZE)$&$skiptoken=$(PAGE_TOKEN)$","__LICENSE__.SEARCHOP=/$`
  `(tenant_id)$/subscribedSkus?$(api_version)$/$(Filter`
  `Suffix)$","__ACCOUNT__.__LICENSE__.ADDATTRIBUTE=/$`
  `(tenant_id)$/users/$(__UID__)$/assignLicense?$`
  `(api_version)$","__ACCOUNT__.__LICENSE__.REMOVEATTRIBUTE=/$`
  `(tenant_id)$/users/$(__UID__)$/assignLicense?$(api_version)$"`

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

## 5.1.2 Performing Limited Reconciliation

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

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

records that must be reconciled. You do this by creating filters for the reconciliation module.

You can perform limited reconciliation by creating filters for the reconciliation module. An example `Filter Suffix` value that is valid in the API version 1.6 is as follows:

Filter Suffix value : `%20and%20startswith(displayName,'tap')`

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.

For information about Office 365 filters, visit the following Microsoft Developer Network page: https://msdn.microsoft.com/library/azure/ad/graph/howto/azure-ad-graph-api-supported-queries-filters-and-paging-options.

> **✏ Note:**
>
> Specify a value for the Filter Suffix attribute in a format that is supported by the Office 365 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')`

## 5.1.3 Performing Delete Reconciliation

You can configure the connector for reconciling information about users deleted in the target system.

To perform delete reconciliation, you must add the delete reconciliation schedule job while application on-boarding. To do so:

1. Open Identity Self-Service application.
2. Click **Manage**.
3. Click **Application**.
4. Search and open the application you have created.
5. Select **Application Settings**.
6. Click the **Reconciliation** tab and expand Reconciliation Jobs.

7. Add the delete reconciliation schedule job and create the scheduler with below values:

   • Job Name: **Office365 Target User Delete Reconciliation**

   • Object Type: **User**

   • Application Name: **Office365Application**

8. Click **Submit**.

# 5.2 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

1. Log in to Identity System Administration.

2. In the left pane, under System Management, click **Scheduler**.

3. Search for and open the scheduled job as follows:

   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

   b. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. On the Job Details tab, you can modify the parameters of the scheduled task:

   • **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

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

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

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

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

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

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

# 5.3 Configuring Provisioning

You can configure the provisioning operation for the Office 365 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.Office365.GM.Configuration
- Lookup.Office365.GM.ProvAttrMap
- Lookup.Office365.GM.ReconAttrMap

### 5.4.1.1 Lookup.Office365.GM.Configuration

The Lookup.Office365.GM.Configuration lookup definition holds configuration entries that are specific to the group object type. This lookup definition is used during group management operations when your target system is configured as a target resource.

**Table 5-1    Entries in the Lookup.Office365.GM.Configuration Lookup Definition**

| Code Key | Decode | Description |
|---|---|---|
| Provisioning Attribute Map | Lookup.Office365 GM.ProvAttrMap | This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Governance and the target system. This lookup definition is used during provisioning operations. |
| Recon Attribute Map | Lookup.Office365 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.Office365.GM.ProvAttrMap

Lookup.Office365.GM.ProvAttrMap lookup definition holds mappings between process form fields (Code Key values) and target system attributes (Decode). This lookup definition is preconfigured and is used during group provisioning operations. Table 5-2 lists the default entries.

**Table 5-2    Entries in the Lookup.Office365.GM.ProvAttrMap Lookup Definition**

| Group Field on Oracle Identity Governance | Office365 Field |
| --- | --- |
| ObjectId | __UID__ |
| Description | description |
| Mail Enabled | mailEnabled |
| Mail Nickname | mailNickname |
| Display Name | __NAME__ |
| Security Enabled | securityEnabled |

## 5.4.1.3 Lookup.Office365.GM.ReconAttrMap

The Lookup.Office365.GM.ReconAttrMap lookup definition holds mappings between resource object fields (Code Key values) and target system attributes (Decode). This lookup definition is preconfigured and is used during target resource group reconciliation runs.Table 5-3 lists the default entries.

**Table 5-3    Entries in the Lookup.Office365.GM.ReconAttrMap Lookup Definition**

| Group Field on Oracle Identity Governance | Office365 Field |
| --- | --- |
| ObjectId | __UID__ |
| Description | description |
| Mail Enabled | mailEnabled="${mailEnabled}" |
| Mail Nickname | mailNickname |
| Display Name | __NAME__ |
| Security Enabled | securityEnabled="${securityEnabled}" |
| OIM Org Name | OIM Organization Name |
|  | **Note**: This is a connector attribute. The value of this attribute is used internally by the connector to specify the organization of the groups in Oracle Identity Governance. |

## 5.4.2 Reconciliation Rules and Action Rules for Groups Management

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

## 5.4.2.1 Reconciliation Rule for Groups

The following is the process-matching rule for groups:

**Rule name:** Office365 Groups Recon Rule

**Rule element:** Organization Name Equals OIM Org Name

In this rule element:

- Organization Name is the Organization Name field of the OIM User form.

- OIM Org Name is the organization name of the groups in Oracle Identity Governance. OIM Org Name is the value specified in the Organization Name attribute of the Office365 Group Recon scheduled job.

## 5.4.2.2 Reconciliation Action Rules for Groups

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

**Table 5-4    Action Rules for Groups Reconciliation**

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

## 5.4.2.3 Viewing Reconciliation Rules

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

1. Log in to the Oracle Identity Governance Design Console.

2. Expand **Development Tools**.

3. Double-click **Reconciliation Rules**.

4. Search for the **Office365 Groups Recon Rule** rule.

   Figure 5-1 shows the reconciliation rule for groups.

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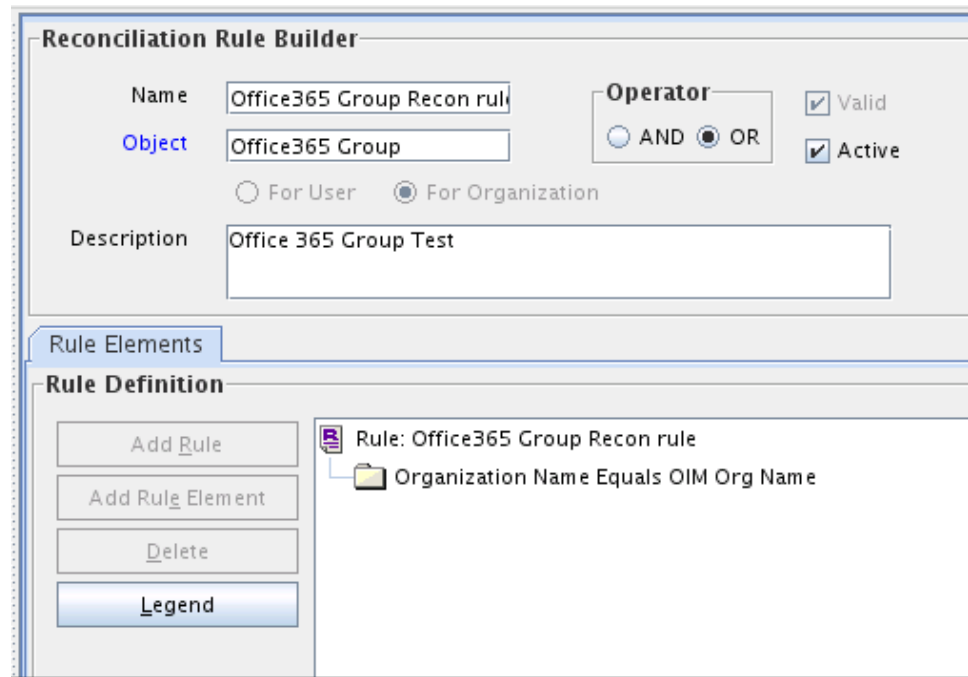


## 5.4.2.4 Viewing Reconciliation Action Rules

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

1. Log in to the Design Console.

2. Expand **Resource Management**, and double-click **Resource Objects**.

3. Search for and open the **Office365 Group** resource object.

4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 5-2 shows the reconciliation action rules for groups.

**Figure 5-2    Reconciliation Action Rules for Groups**
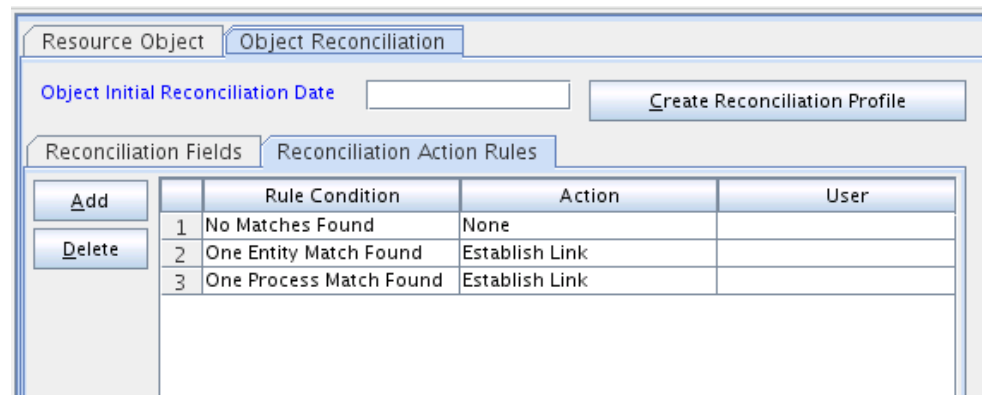
## 5.4.3 Reconciliation Scheduled Jobs for Groups Management

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

You must specify values for the attributes for Office 365 Group Recon. Table 5-5 describes the attributes of the Office365 Group Reconciliation job.

**Table 5-5    Attributes of the Office365 Group Reconciliation Job**

| Attribute | Description |
|---|---|
| Filter Suffix | Enter the search filter for fetching user records from the target system during a reconciliation run. See Performing Limited Reconciliation for more information about this attribute. |
| Object Type | This attribute holds the name of the object type for the reconciliation run.<br>Default value: `Group`<br>**Note:** Do not change the default value. |
| Incremental Recon Attribute | Attribute that holds the timestamp at which the token record was modified. |
| OIM Organization Name | Enter the name of the Oracle Identity Governance organization in which reconciled groups must be created or updated. |
| IT Resource Name | Enter the name of the IT resource for the target system installation from which you want to reconcile user records.<br>Default value: `Office365` |
| Resource Object Name | This attribute holds the name of the resource object used for reconciliation.<br>Default value: `Office365 Group`<br>**Note:** Do not change the default value. |
| Latest Token | This attribute holds the value of the attribute that is specified as the value of the Incremental Recon Attribute attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty.<br>**Note:** Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute.<br>Sample value: `<String>2017-11-30T04:44:29Z</String>` |
| Scheduled Task Name | Name of the scheduled task used for reconciliation.<br>Default value: `Office365 Group Recon`<br>Do *not* modify the value of this attribute. |

# 5.5 Uninstalling the Connector

Uninstalling the Office 365 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: `Office365 User; Office365 Group`

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

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

# 6

# Extending the Functionality of the Office 365 Connector

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

This section discusses the following topics:

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

## 6.1 Configuring Transformation and Validation of Data

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

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

Similarly, you can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

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

Following is a sample transformation script for reference:

```
def getBeneficiaryAttrFromContext(attrName)
{
 if (context.beneficiary != null)
  {
    return context.beneficiary.getAttribute(attrName);
  }

 return null;
}

 def getBeneficiaryPwdFromContext()
 {
   return context.beneficiaryPassword;
```

```
        }

      if (binding.variables != null)
       {
        if (binding.variables.containsKey("context"))
          {
           if (context.operationType != null)
             {
              if(context.operationType.equalsIgnoreCase("create"))
             {
                if (context.provisionMechanism != null)
                {
                  if(context.provisionMechanism.equalsIgnoreCase("POLICY"))
                   {
                     User_Principal_Name =
getBeneficiaryAttrFromContext("User Login");
                     First_Name = getBeneficiaryAttrFromContext("First
Name");
                     Last_Name = getBeneficiaryAttrFromContext("Last
Name");
                     Display_Name = First_Name +" "+Last_Name;
                     Mail_NickName = First_Name +Last_Name;
                     Password = getBeneficiaryPwdFromContext();
                   }

                 else if
(context.provisionMechanism.equalsIgnoreCase("REQUEST") ||
context.provisionMechanism.equalsIgnoreCase("ADMIN"))
                   {
                     if (User_Principal_Name == null ||
User_Principal_Name == "")
                       { User_Principal_Name =
getBeneficiaryAttrFromContext("User Login");}
                     if (First_Name == null || First_Name == "")
                       { First_Name = getBeneficiaryAttrFromContext("First
Name");}
                     if (Last_Name == null || Last_Name == "")
                       { Last_Name = getBeneficiaryAttrFromContext("Last
Name");}
                     if (Display_Name == null || Display_Name == "")
                       { Display_Name =
getBeneficiaryAttrFromContext("First Name") +"
"+getBeneficiaryAttrFromContext("Last Name");}
                     if (Mail_NickName == null || Mail_NickName == "")
                       { Mail_NickName =
getBeneficiaryAttrFromContext("First Name") +
getBeneficiaryAttrFromContext("Last Name");}
                     if (Password == null || Password == "")
                       { Password = getBeneficiaryPwdFromContext();}

                   }
                }
             }
          }

      }
```

```
                }
            }
```

## 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 Installations of the Target System

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

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

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

# 7

# Upgrading the Office 365 Connector

If you have already deployed the 11.1.1.5.0 version of the Office 365 connector, then you can upgrade the connector to version 12.2.1.3.0 by uploading the new connector JAR files to the Oracle Identity Manager database.

The following sections discuss the procedure to upgrade the connector:

- Upgrade Steps
- Postupgrade Steps

> ✎ **See Also:**
>
> About Upgrading Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information on these steps

## 7.1 Upgrade Steps

This is a summary of the procedure to upgrade the connector for both staging and production environments.

> ✎ **Note:**
>
> Before you perform the upgrade procedure
>
> - It is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
>
> - As a best practice, perform the upgrade procedure in a test environment initially.

Depending on the environment in which you are upgrading the connector, perform one of the following steps:

- Staging Environment

  Perform the upgrade procedure by using the wizard mode. See Wizard Mode Upgrade in Staging Environment in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

- Production Environment

  Perform the upgrade procedure by using the silent mode.

> **✎ Note:**
>
> While running Step 4 in the upgrade wizard, in the `Office365 Users Process Definitions` screen, under the `Define Process Definition Mappings` tab ensure that you do not retain the `Process Tasks` for `Enable User` and `Disable User` options.

# 7.2 Postupgrade Steps

Postupgrade steps involve uploading new connector JAR to Oracle Identity Manager database.

Perform the following procedure:

1. Delete the old Connector JARs. Run the Oracle Identity Manager Delete JARs (`$ORACLE_HOME/bin /DeleteJars.sh`) utility to delete the existing ICF bundle `org.identityconnectors.genericrest-1.0.11150.jar` from the Oracle Identity Manager database.

   When you run the Delete JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being deleted, and the name of the JAR file to be removed. Specify `4` as the value of the JAR type.

2. Upload the new connector JARs:

   a. Run the Oracle Identity Manager Upload JARs (`$ORACLE_HOME/bin/ UploadJars.sh`) utility to upload the connector JARs.

   b. Upload the `org.identityconnectors.genericrest-12.3.0.jar` bundle as an ICF Bundle. Run the Oracle Identity Manager Upload JARs utility to post the new ICF bundle `org.identityconnectors.genericrest-12.3.0.jar` file to the Oracle Identity Manager database.

   When you run the Upload JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify `4` as the value of the JAR type.

   c. Delete the following **Code Key** and **Decode** entries in the `Lookup.Office365.Configuration` lookup definition:

   - **Code Key**: `Bundle Version`; **Decode**: 1.0.1115
   - **Code Key**: `relURIs`

      **Decode**:

      ```
      "__ACCOUNT__.CREATEOP=/$(tenant_id)$/users?$
      (api_version)$","__ACCOUNT__.UPDATEOP=/$(tenant_id)$/
      users/$(__UID__)$?$
      (api_version)$","__ACCOUNT__.SEARCHOP=/$(tenant_id)$/
      users?$(api_version)$/$(Filter
      Suffix)$","__ACCOUNT__=/$(tenant_id)$/users/$
      ```

```
(__UID__)$?$
(api_version)$","__ACCOUNT__.manager.SEARCHOP=/$
(tenant_id)$/users/$(__UID__)$/manager?$
(api_version)$","__ACCOUNT__.manager=/$(tenant_id)$/
users/$(__UID__)$/$links/manager?$
(api_version)$","__ACCOUNT__.__GROUP__.SEARCHOP=/$
(tenant_id)$/users/$(__UID__)$/memberOf?$
(api_version)$","__ACCOUNT__.__GROUP__.DELETEOP=/$
(tenant_id)$/groups/$(__GROUP__.objectId)$/$links/
members/$(__UID__)$?$
(api_version)$","__ACCOUNT__.__GROUP__=/$(tenant_id)$/
groups/$(__GROUP__.objectId)$/$links/members?$
(api_version)$","__GROUP__.CREATEOP=/$(tenant_id)$/
groups?$(api_version)$","__GROUP__.UPDATEOP=/$
(tenant_id)$/groups/$(__UID__)$?$
(api_version)$","__GROUP__.SEARCHOP=/$(tenant_id)$/
groups?$(api_version)$/$(Filter Suffix)$","__GROUP__=/$
(tenant_id)$/groups/$(__UID__)$?$
(api_version)$","__GROUP__.member=/$(tenant_id)$/
groups/$(__UID__)$/$links/members?$
(api_version)$","__ROLE__.SEARCHOP=/$(tenant_id)$/
directoryRoles?$(api_version)$/$(Filter
Suffix)$","__ACCOUNT__.__ROLE__=/$(tenant_id)$/
directoryRoles/$(__ROLE__.objectId)$/$links/members?$
(api_version)$","__ACCOUNT__.__ROLE__.DELETEOP=/$
(tenant_id)$/directoryRoles/$
(__ROLE__.objectId)$/$links/members/$(__UID__)$?$
(api_version)$","__ROLE__.member=/$(tenant_id)$/
directoryRoles/$(__UID__)$/$links/members?$
(api_version)$","__ACCOUNT__.__ROLE__.SEARCHOP=/$
(tenant_id)$/users/$(__UID__)$/memberOf?$
(api_version)$","__LICENSE__.SEARCHOP=/$(tenant_id)$/
subscribedSkus?$(api_version)$/$(Filter
Suffix)$","__ACCOUNT__.__LICENSE__.ADDATTRIBUTE=/$
(tenant_id)$/users/$(__UID__)$/assignLicense?$
(api_version)$","__ACCOUNT__.__LICENSE__.REMOVEATTRIBUT
E=/$(tenant_id)$/users/$(__UID__)$/assignLicense?$
(api_version)$"
```

d. Delete the following **Code Key** and **Decode** entry in the `Lookup.Office365.Configuration.Trusted` lookup definition:

- **Code Key**: `Bundle Version`; **Decode**: 1.0.1115

- **Code Key**: `relURIs`;
  **Decode**: `"__ACCOUNT__.SEARCHOP=/$(tenant_id)$/users?$`
  `(api_version)$/$(Filter Suffix)$","__ACCOUNT__=/$`
  `(tenant_id)$/users/$(__UID__)$?$`
  `(api_version)$","__ACCOUNT__.manager.SEARCHOP=/$`
  `(tenant_id)$/users/$(__UID__)$/manager?$`
  `(api_version)$","__ACCOUNT__.manager=/$(tenant_id)$/`
  `users/$(__UID__)$/$links/manager?$(api_version)$"`

e. Delete the following **Code Key** and **Decode** entries in the `Lookup.Office365.UM.ReconAttrMap` lookup definition:

**Code Key**: `Usage Location`; **Decode**: `UsageLocation`

f. Delete the following **Code Key** and **Decode** entries in the `Lookup.Office365.UM.ReconAttrMap.Trusted` lookup definition:

**Code Key**: `Usage Location`; **Decode**: `UsageLocation`

3. Restart Oracle Identity Manager.

4. If the connector is deployed on a Connector Server, then:

a. Stop the connector server.

b. Replace the existing bundle JAR file `org.identityconnectors.genericrest-1.0.1115.jar` with the new bundle JAR file `org.identityconnectors.genericrest-12.3.0.jar`.

c. Start the connector server.

> **Note:**
>
> - To configure incremental reconciliation, see Configuring Incremental Reconciliation.
>
> - If you have configured the connector for multiple versions of target system, then refer to Configuring the Connector for Multiple Installations of the Target System for more information.

# A
# Files and Directories in the Office 365 Connector Installation Package

These are the components of the connector installation package that comprise the Office 365 connector.

**Table A-1    Files and Directories in the Office 365 Connector Installation Package**

| File in the Installation Package | Description |
| --- | --- |
| bundle/ org.identityconnectors.genericrest-12.3.0.jar | This JAR is the ICF connector bundle. |
| Office365-CI.xml | This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the Connector Installer during connector installation. |
| Files in the resources directory | Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to Oracle Identity database.<br><br>**Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages. |
| xml/Office365-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/Office365-auth-template.xml | This file contains definitions for the connector objects required for creating an Authoritative application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs. |
| xml/Office365-pre-config.xml | This XML file contains definitions for the connector objects associated with any non-User object such as Groups. |
| xml/Office365-ConnectorConfig.xml | This XML file contains definitions for the connector components. These components include the following:<br>• IT resource type<br>• Process form<br>• Process task and adapters (along with their mappings)<br>• Resource object<br>• Provisioning process<br>• Prepopulate rules<br>• Lookup definitions<br>• Scheduled tasks |