Oracle® Identity Manager

Connector Guide for Office 365

Release 11.1.1
E73273-03
May 2020

Oracle Identity Manager Connector Guide for Office 365, Release 11.1.1

E73273-03

Primary Author: Alankrita Prakash

Contributing Authors: Mike Howlett

Contents

Preface

What’s New in Oracle Identity Manager Connector for Office 365?

1 About the Office 365 Connector

3 Using the Office 365 Connector

4 Extending the Functionality of the Office365 Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Office 365.

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 Manager, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E52734_01/index.html

For information about Oracle Identity Manager Connectors 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.

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

What’s New in Oracle Identity Manager Connector for Office 365?

This chapter provides an overview of the updates made to the software and documentation for the Office 365 connector in release 11.1.1.5.0.

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

- Software Updates

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

  These include major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

Software Updates

The following section provides software updates:

Software Updates in Release 11.1.1.5.0

This is the first release of the Oracle Identity Manager connector for Office 365. Therefore, there are no software-specific updates in this release.

Documentation-Specific Updates

The following section provides documentation-specific updates:

Documentation-Specific Updates in Release 11.1.1.5.0

The following is a documentation-specific update in revision "03" 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 12c PS4 (12.2.1.4.0).

The following is a documentation-specific update in revision "02" of this guide:

- The URL of the Office 365 product documentation has been modified in the Preinstallation section.

1 About the Office 365 Connector

The Office 365 connector integrates Oracle Identity Manager (OIM) with the Office 365 service.

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

1.1 Introduction to Office 365 Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. The Office 365 connector enables you to use Office 365 either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.
The Office 365 connector enables you to manage all your user and group identities in Office 365. This connector also provides management of entitlements such as roles, licenses, and groups for your user identities.

> **Note:**
>
> At some places in this guide, Office 365 has been referred to as the target system.

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. This data is used to add or modify resources (that is, accounts) allocated to OIM Users. In addition, you can use Oracle Identity Manager to provision or update Office 365 resources (accounts) assigned to OIM Users. These provisioning operations performed on Oracle Identity Manager translate into the creation or updates to target system accounts.

In the identity reconciliation (trusted source) mode of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

1.2 Certified Components for the Office 365 Connector

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

Table 1-1 lists the required components for the Office 365 Connector.

Table 1-1 Certified Components

Component	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12c (12.2.1.4.0) • Oracle Identity Governance 12c (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0)
Target systems	Microsoft Office 365 Enterprise Editions
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 or Later

1.3 Certified Languages for Office 365 Connector

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English (US)
- Finnish
- French
- French (Canadian)
- German
- Greek
- Hebrew

- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

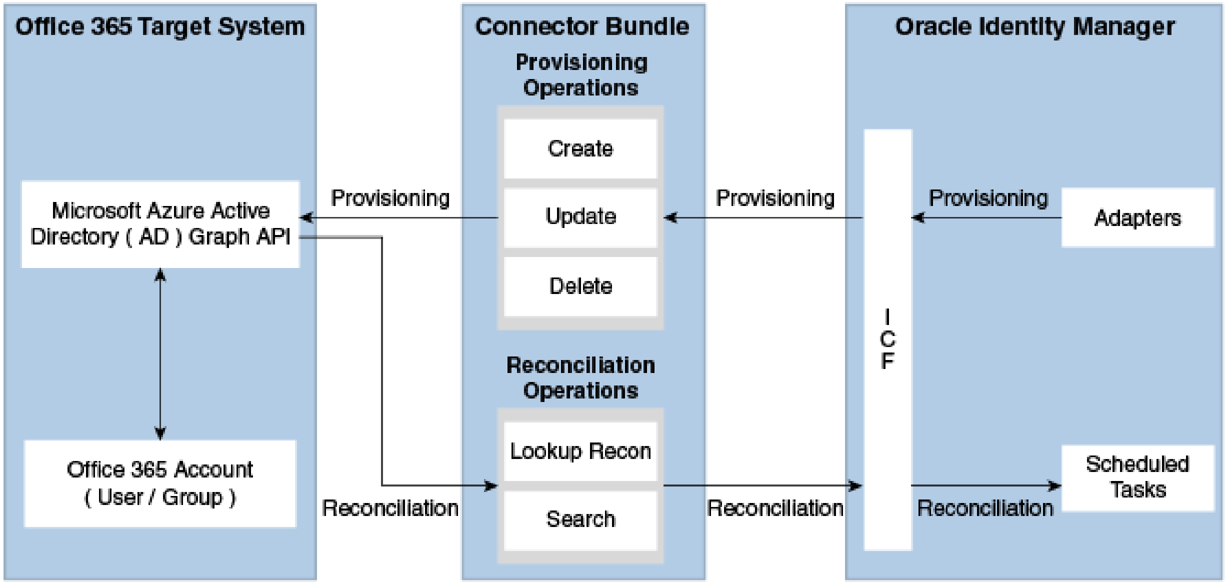
1.4 Connector Architecture of the Office 365 Connector

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 Manager 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 Manager. 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 target system is used as the trusted source and users are directly created and modified on it. 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 Manager.

  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 Manager. 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 Manager.

    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 Manager. If no match is found, then the user ID of the record is compared with the user ID 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 Manager* for more information about ICF

1.5 Use Cases Supported by the Office 365 Connector

The Office 365 connector is used to integrate OIM 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 OIM 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 OIM to manage identities. The organization wants to manage its user identities by creating them in the target system using OIM. The organization also wants to synchronize user identity changes performed directly in the target system with OIM. 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 in the IT resource.

  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 OIM. The connector will run the corresponding SearchOp against the user identities in the target system and fetch all the changes to OIM.

- **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 Manager 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 OIM capability of auditing and reporting.

1.6 Features of the Office 365 Connector

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

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

1.6.1 Full Reconciliation

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

> **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.

See Full Reconciliation for Office 365 Connector.

1.6.2 Support for the Connector Server

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

A Java connector server is useful when you do not want to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements if the bundle works faster when deployed on the same host as the native managed resource.

See Installation.

> **See Also:**
>
> Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about installing and configuring connector server and running the connector server

1.6.3 Limited (Filtered) Reconciliation

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

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

See Limited Reconciliation for Office 365 Connector.

1.6.4 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning.

In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information

- Configuring Transformation of Data During User Reconciliation
- Configuring Validation of Data During Reconciliation and Provisioning

1.7 Lookup Definitions Used During Reconciliation and Provisioning

Lookup definitions used during reconciliation and provisioning are either preconfigured or can be synchronized with the target system.

This section discusses the following categories of lookup definitions:

- Lookup Definitions Synchronized with the Target System
- Preconfigured Lookup Definitions

1.7.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to select a single value from a set of values. For example, you may want to select a role from the Role Name lookup field to specify the role being assigned to the user. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to specific fields in the target system to lookup definitions in Oracle Identity Manager.
After you deploy the connector, the following lookup definitions, which are used as an input source for lookup fields, are automatically created in Oracle Identity Manager:

- Lookup.Office365.Groups
- Lookup.Office365.Roles
- Lookup.Office365.Licenses
- Lookup.Office365.Manager

These lookup definitions are empty by default. They are populated with values fetched from the target system when you run the scheduled jobs for lookup field synchronization. For example, when you run the scheduled job for role lookup field synchronization, all Roles on the target system are fetched to Oracle Identity Manager and populated in the Lookup.Office365.Roles lookup definition.

After lookup field synchronization, data in each of the lookup definitions for lookup field synchronization is stored in the following format:

- **Code Key:** *<IT_RESOURCE_NAME>~<FIELD_VALUE>*

  In this format:

  - *IT_RESOURCE_NAME* is the name of the IT resource in Oracle Identity Manager.
  - *FIELD_VALUE* is the value of the field in the target system.

  For example, for the Lookup.Office365.Roles lookup definition, the code key value for one of its entries is `Office365~System Administrator`. In this example, `Office365` is the name of the IT resource and `System Administrator` is the value of the Role field in the target system.

- **Decode:** *<IT_RESOURCE_KEY>~<FIELD_VALUE_ID>*

  In this format:

- *IT_RESOURCE_KEY* is the numeric code assigned to an IT resource in Oracle Identity Manager.
- *FIELD_VALUE_ID* is the ID of the target system field value.

For example, for the Lookup.Office365.Roles lookup definition, the decode value for one of its entries is `89~1b5d6697-f4a6-4f03-8df7-4fae1512fd16` In this example, `89` is the numeric code assigned to the IT resource associated with the target system and `1b5d6697-f4a6-4f03-8df7-4fae1512fd16` is the ID of the Role in the target system.

Table 1-2 shows sample entries in the Lookup.Office365.Groups lookup definition.

Table 1-2 Sample Entries in the Lookup.Office365.Groups Lookup Definition

Code Key	Decode
Office365~Finance	89~9b3b3faf-e7fb-427e-8038-b8021cfbab30
Office365~HR	89~eb1b204e-2de0-41ec-98e9-1c33684d698a
Office365~ISP	89~4457f158-d1ec-47f2-aeb4-79d5a2be0e38

1.7.2 Preconfigured Lookup Definitions

Preconfigured lookup definitions are the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

The other lookup definitions are as follows:

- Lookup.Office365.Configuration
- Lookup.Office365.UM.Configuration
- Lookup.Office365.UM.ProvAttrMap
- Lookup.Office365.UM.ReconAttrMap
- Lookup.Office365.GM.Configuration
- Lookup.Office365.GM.ProvAttrMap
- Lookup.Office365.GM.ReconAttrMap
- Lookup.Office365.BooleanValues
- Lookup.Office365.Countries
- Lookup.Office365.UsageLocation
- Lookup.Office365.Configuration.Trusted
- Lookup.Office365.UM.Configuration.Trusted
- Lookup.Office365.UM.ReconAttrMap.Trusted
- Lookup.Office365.UM.ReconAttrMap.TrustedDefaults

1.7.2.1 Lookup.Office365.Configuration

The Lookup.Office365.Configuration lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

> **Note:**
>
> Do not modify the entries in this lookup definition.

Table 1-3 Entries in the Lookup.Office365.Configuration Lookup Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.genericrest	This entry holds the name of the connector bundle.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle.
Connector Name	org.identityconnectors.genericrest.GenericRESTConnector	This entry holds the name of the connector class.
Group Configuration Lookup	Lookup.Office365.GM.Configuration	This entry holds the name of the lookup definition that contains group-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of groups.

Table 1-3 (Cont.) Entries in the Lookup.Office365.Configuration Lookup Definition

Code Key	Decode	Description
relURI's	"__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)$","__ACCOUNT__.__LICENSE__.REMOVEATTRIBUTE=/$(tenant_id)$/users/$(__UID__)$/assignLicense?$(api_version)$"	This entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes. For example, the `__ACCOUNT__.CREATEOP=/$(tenant_id)$/users?$(api_version)$` value implies that `/$(tenant_id)$/users?$(api_version)$` is the relative URL for all create provisioning operations performed on the __ACCOUNT__ object class.

Table 1-3 (Cont.) Entries in the Lookup.Office365.Configuration Lookup Definition

Code Key	Decode	Description
User Configuration	Lookup.Office365.UM.Configuration	This entry holds the name of the lookup definition that stores configuration information used during user management operations.
nameAttributes	"__ACCOUNT__.userPrincipalName","__GROUP__.displayName","__ROLE__.displayName","__LICENSE__.skuPartNumber"	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.
uidAttributes	"__ACCOUNT__.objectId","__GROUP__.objectId","__ROLE__.objectId","__LICENSE__.skuId”	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.

Table 1-3 (Cont.) Entries in the Lookup.Office365.Configuration Lookup Definition

Code Key	Decode	Description
statusAttribute	“__ACCOUNT__.accountEnabled”	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.
Any Incremental Recon Attribute Type	True	By default, during incremental reconciliation, OIM accepts timestamp information sent from the target system only in Long datatype format. A decode value of True for the Incremental Recon Attribute Type entry indicates that OIM will accept timestamp information in any datatype format.
customPayload	\"}","__ACCOUNT__.__GROUP__.CREATEOP={\"url \": \<tenant_id>/directoryObjects/ <__UID__> \"}","__ACCOUNT__.manager.CREATEOP={\"url\": \<tenant_id>/directoryObjects/ <manager> \"}","__ACCOUNT__.manager.UPDATEOP={\"url\": \<tenant_id>/directoryObjects/ <manager> \"}","__ACCOUNT__.__ROLE__.UPDATEOP={\"url\": \<tenant_id>/directoryObjects/ <__UID__> \"}","__ACCOUNT__.__ROLE__.CREATEOP={\"url\": \<tenant_id>/directoryObjects/ <__UID__> \"}","__ACCOUNT__.__LICENSE__.ADDATTRIBUTE ={\"addLicenses\": [{\"skuId\": \"<skuId>\"}], \"removeLicenses\": []}","__ACCOUNT__.__LICENSE__.REMOVEATTRIBUTE={\"addLicenses\": [],\"removeLicenses\": [\"<skuId>\"]}"	This entry lists the payloads for all operations that are not in the standard format.
httpHeaderAccept	application/json	This entry holds the accept type expected from the target system in the header.

Table 1-3 (Cont.) Entries in the Lookup.Office365.Configuration Lookup Definition

Code Key	Decode	Description
httpHeaderContentType	application/json	This entry holds the content type expected by the target system in the header.
jsonResourcesTag	"__ACCOUNT__=value","__GROUP__=value","__ROLE__=value","__LICENSE__=value"	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload.
opTypes	“__ACCOUNT__.CREATEOP=POST","__ACCOUNT__.UPDATEOP=PATCH","__ACCOUNT__.SEARCHOP=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"	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).
passwordAttribute	passwordProfile.password	This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute of the connector in OIM.

Table 1-3 (Cont.) Entries in the Lookup.Office365.Configuration Lookup Definition

Code Key	Decode	Description
specialAttributeHandling	"__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"	This entry lists the special attributes whose values should be send to target 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.
specialAttributeTargetFormat	"__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"	This entry lists the format in which an attribute is present in the target system endpoint. For example, the alias attribute will be present as aliases.alias in the target system endpoint. Values are comma separated and are presented in the following format: *OBJ_CLASS.ATTR_NAME= TARGET_FORMAT*

Table 1-3 (Cont.) Entries in the Lookup.Office365.Configuration Lookup Definition

Code Key	Decode	Description
targetObjectIdentifier	"__ACCOUNT__.__GROUP__=objectType;Group","__ACCOUNT__.__ROLE__=objectType;Role"	This entry specifies the key-value pair for replacing place holders in the relURIs. Values are comma separated and in the *KEY*;*VALUE* format.

1.7.2.2 Lookup.Office365.UM.Configuration

The Lookup.Office365.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations.

Table 1-4 Entries in the Lookup.Office365.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.Office365 UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. This lookup definition is used during user provisioning operations.
Recon Attribute Map	Lookup.Office365 UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes.. This lookup definition is used during reconciliation.

1.7.2.3 Lookup.Office365.UM.ProvAttrMap

The Lookup.Office365.UM.ProvAttrMap lookup definitions hold mappings between process form fields and target system attributes.

This lookup definition is preconfigured and used during provisioning. Table 1-5 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Adding New User or Group Attributes for Provisioning.

1.7.2.4 Lookup.Office365.UM.ReconAttrMap

The Lookup.Office365.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes.

This lookup definition is preconfigured and used during target resource reconciliation. Table 1-12 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for target resource reconciliation. See Adding New User or Group Attributes for Reconciliation.

1.7.2.5 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.

Do *not* modify the entries in this lookup definition.

Table 1-5   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 maps process form fields and target system attributes. This lookup definition is discussed later in the guide.
Recon Attribute Map	Lookup.Office365 GM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. This lookup definition is discussed later in the guide.

1.7.2.6 Lookup.Office365.GM.ProvAttrMap

The Lookup.Office365.GM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes.

This lookup definition is preconfigured and used during group provisioning operations.Table 1-17 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Adding New User or Group Attributes for Provisioning.

1.7.2.7 Lookup.Office365.GM.ReconAttrMap

The Lookup.Office365.GM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes.

This lookup definition is preconfigured and used during target resource reconciliation of groups. Table 1-13 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Adding Attributes to the Resource Object for more information.

1.7.2.8 Lookup.Office365.BooleanValues

The Lookup.Office365.BooleanValues lookup definition maps boolean values that are used for some of the fields in the target system with the corresponding boolean values to be displayed in the fields of the OIM User form.

Table 1-6 lists the default entries in the Lookup.Office365.BooleanValues lookup definition.

Table 1-6 Entries in the Lookup.Office365.BooleanValues Lookup Definition

Code Key (Resource Object Field)	Decode (Office 365 Field)
true	True
false	False

1.7.2.9 Lookup.Office365.Countries

The Lookup.Office365.Countries lookup definition holds information about country names that you can select for a target system account that you create through Oracle Identity Manager. This is a static lookup definition.

You must populate the entries of this lookup definition manually. The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** 2–letter ISO code for a country
- **Decode:** Country name

Table 1-7 lists the default entries in the Lookup.Office365.Countries lookup definition:

Table 1-7 Default Entries in the Lookup.Office365.Countries Lookup Definition

Code Key (Resource Object Field)	Decode (Office 365 Field)
US	United States
UK	United Kingdom

1.7.2.10 Lookup.Office365.UsageLocation

The Lookup.Office365.UsageLocation lookup definition holds information about license usage locations that you can select for a target system account that you create through Oracle Identity Manager. This is a static lookup definition.

You must populate the entries of this lookup definition manually. The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** 2–letter ISO code for a country
- **Decode:** Country name

Table 1-8 lists the default entries in this lookup definition.

Table 1-8 Default Entries in the Lookup.Office365.UsageLocation Lookup Definition

Code Key (Resource Object Field)	Decode (Office 365 Field)
US	United State
UK	United Kingdom
JP	Japan

1.7.2.11 Lookup.Office365.Configuration.Trusted

The Lookup.Office365.UM.Configuration.Trusted lookup definition holds configuration entries that are used during trusted source reconciliation.

> **Note:**
>
> Do not modify the entries in this lookup definition

Table 1-9 Entries in the Lookup.Office365.Configuration.Trusted

Code Key	Decode	Description
Bundle Name	org.identityconnectors.genericrest	This entry holds the name of the connector bundle.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle.
Connector Name	org.identityconnectors.genericrest.GenericRESTConnector	This entry holds the name of the connector class.
relURI's	"__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)$""	The entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes. For example, the `__ACCOUNT__.SEARCHOP=/$(tenant_id)$/users?$(api_version)$/$(Filter Suffix)$` value implies that `/$(tenant_id)$/users?$(api_version)$/$(Filter Suffix)$` is the relative URL for all reconciliation runs performed against the __ACCOUNT__ object class.
User Configuration Lookup	Lookup.Office365.UM.Configuration.Trusted	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do not modify this entry.

Table 1-9 (Cont.) Entries in the Lookup.Office365.Configuration.Trusted

Code Key	Decode	Description
nameAttributes	"__ACCOUNT__.userPrincipal Name "	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.
uidAttributes	"__ACCOUNT__.objectId"	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 corresponds to the uid attribute of user accounts in the target system.
statusAttribute	"__ACCOUNT__.accountEnabled"	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.
Any Incremental Recon Attribute Type	True	By default, during incremental reconciliation, OIM accepts timestamp information sent from the target system only in Long datatype format. A decode value of True for the Incremental Recon Attribute Type entry indicates that OIM will accept timestamp information in any datatype format.
httpHeaderAccept	application/json	This entry holds the accept type expected from the target system in the header.
httpHeaderContentType	application/json	This entry holds the content type expected by the target system in the header.

Table 1-9 (Cont.) Entries in the Lookup.Office365.Configuration.Trusted

Code Key	Decode	Description
jsonResourcesTag	"__ACCOUNT__=value"	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload.
opTypes	"__ACCOUNT__.SEARCHOP=GET"	This entry specifies the HTTP operation type for each object class supported by the connector. Values must be comma separated and must be in the following format: *OBJ_CLASS.OP=HTTP_OP* In this format, replace*OBJ_CLASS* with the connector object class, *OP* with the connector operation (for example, CreateOp, UpdateOp, SearchOp), and *HTTP_OP* with the HTTP operation (GET or POST)
specialAttributeTargetFormat	"__ACCOUNT__.manager=userPrincipalName"	This entry lists the format in which an attribute is present in the target system endpoint. For example, the alias attribute will be present as aliases.alias in the target system endpoint. Values are comma separated and are presented in the following format: *OBJ_CLASS.ATTR_NAME=TARGET_FORMAT*

1.7.2.12 Lookup.Office365.UM.Configuration.Trusted

The Lookup.Office365.UM.Configuration.Trusted lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during trusted source user reconciliation runs.

Table 1-10 lists the default entries in this lookup definition:

Table 1-10 Entries in the Lookup.Office365.UM.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Recon Attribute defaults	Lookup.Office365.UM.ReconAttrMap.TrustedDefaults	This entry holds the name of the lookup definition that maps reconciliation fields to their default values. This lookup definition is discussed later in this guide.

Table 1-10 (Cont.) Entries in the Lookup.Office365.UM.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Recon Attribute Map	Lookup.Office365. UM.ReconAttrMap.Trusted	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. This lookup definition is discussed later in this guide.

1.7.2.13 Lookup.Office365.UM.ReconAttrMap.Trusted

The Lookup.Office365.UM.ReconAttrMap.Trusted lookup definition holds mappings between resource object fields and target system attributes.

This lookup definition is preconfigured and used during trusted source user reconciliation runs. Trusted Source Reconciliation Action Rules for Users lists the default entries.

You can add entries in this lookup definition if you want to map new target system attributes for trusted source reconciliation.

1.7.2.14 Lookup.Office365.UM.ReconAttrMap.TrustedDefaults

The Lookup.Office365.UM.ReconAttrMap.Trusted.Defaults lookup definition holds mappings between reconciliation fields and their default values.

This lookup definition is used when there is a mandatory field on the OIM User form, but no corresponding field in the target system from which values can be fetched during trusted source reconciliation. This is explained in the following example:

For example, Employee Type is a mandatory field on the OIM User form. The target system contains no field that stores information about the employee type for a user account. During reconciliation, no value for the Employee Type field is fetched from the target system. However, as the Employee Type field cannot be left empty, the connector uses the decode value of the Employee Type entry of this lookup definition. This implies that the value of the Employee Type field on the OIM User form displays `Full-Time` for all user accounts reconciled from the target system.

Table 1-11 lists the default entries in this lookup definition. Do *not* add or modify entries to this lookup definition

Table 1-11 Entries in the Lookup.Office365.UM.ReconAttrMap.TrustedDefaults Lookup Definition

Code Key (Resource Object Field)	Decode (Office 365 Field)
Employee Type	Full-Time
Organization	Xellerate Users
User Type	End-User

1.8 Connector Objects Used During Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified accounts on the target system and using this data to add or modify resources assigned to OIM Users.

The Office 365 Target Resource User Reconciliation scheduled job is used to initiate a reconciliation run. This scheduled job is discussed in Reconciliation Scheduled Jobs for Office 365 Connector.

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for generic information about connector reconciliation

This section discusses the following topics

- User Fields for Target Resource Reconciliation
- Group Fields for Reconciliation
- Reconciliation Rules for Target Resource Reconciliation
- Reconciliation Action Rules for Target Resource Reconciliation

1.8.1 User Fields for Target Resource Reconciliation

The Lookup.Office365.UM.ReconAttrMap lookup definition maps resource object fields with target system attributes. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, entries are in the following format:

- **Code Key:** Reconciliation field of the resource object
- **Decode:** Name of the target system user attribute at the Graph API level

Table 1-12 lists the entries in this lookup definition.

Table 1-12 Entries in the Lookup.Office365.UM.ReconAttrMap Lookup Definition

Code Key (Resource Object Field)	Decode (Office 365 Field)
User Principal Name	__NAME__
Preferred Language	preferredLanguage
Account Enabled	accountEnabled="$(accountEnabled)"
Roles~Role Name[Lookup]	__ROLE__~__ROLE__~objectId
Country	country
Display Name	displayName

Table 1-12 (Cont.) Entries in the Lookup.Office365.UM.ReconAttrMap Lookup Definition

Code Key (Resource Object Field)	Decode (Office 365 Field)
Licenses~Licesnse Name[Lookup]	assignedLicenses~assignedLicenses~skuId
Last Name	surname
Mail NickName	mailNickname
Manager[LOOKUP]	manager
Status	__ENABLE__
Object Id	__UID__
City	city
Group Names~Group Name[Lookup]	__GROUP__~__GROUP__~objectId
Usage Location	usageLocation
FirstName	givenName

Roles, Groups, and Licenses are embedded objects that are listed in this table using the naming convention followed to name embedded object lookup definitions.

1.8.2 Group Fields for Reconciliation

The Lookup.Office365.GM.ReconAttrMap lookup definition maps user resource object fields and target system attributes. This lookup definition is used for performing target resource group reconciliation runs.

In this lookup definition, entries are in the following format:

- **Code Key:** Reconciliation field of the resource object
- **Decode:** Name of the target system group attribute at the Graph API level

Table 1-13 lists the group fields of the target system from which values are fetched during reconciliation. The Office365 Group Recon scheduled job is used to reconcile group data:

Table 1-13 Entries in the Lookup.Office365.GM.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Office 365 Field
ObjectId	__UID__
Description	Description
Mail Enabled	mailEnabled="${mailEnabled}"
Mail NickName	mailNickname
Display Name	__NAME__
Security Enabled	securityEnabled

Table 1-13 (Cont.) Entries in the Lookup.Office365.GM.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Office 365 Field
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 Manager.

1.8.3 Reconciliation Rules for Target Resource Reconciliation

Reconciliation rules for target resource reconciliation are used by the reconciliation engine to determine the identity to which Oracle Identity Manager must assign a newly discovered account on the target system.

This section discuss the following topics related to users and groups reconciliation rule for target resource reconciliation:

- Target Resource Reconciliation Rules for Users and Groups
- Viewing Reconciliation Rules for Target Resource Reconciliation

1.8.3.1 Target Resource Reconciliation Rules for Users and Groups

Reconciliation rules for target resource reconciliation are used by the reconciliation engine to determine the identity to which Oracle Identity Manager must assign a newly discovered account on the target system. The Office 365 connector can perform reconciliation of both users and groups. Therefore, the connector has reconciliation rules defined for both users and groups.

Reconciliation Rule for Users

The following is the process-matching rule for users:

Rule name: Office 365 User Recon Rule

Rule element: User Login Equals User Principal Name

In this rule:

- `User Login` is the User ID field of the OIM User form.
- `User Principal Name` is the unique login name for user in target.

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:

- `Organization Name` is the Organization Name field on the OIM User form.

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

1.8.3.2 Viewing Reconciliation Rules for Target Resource Reconciliation

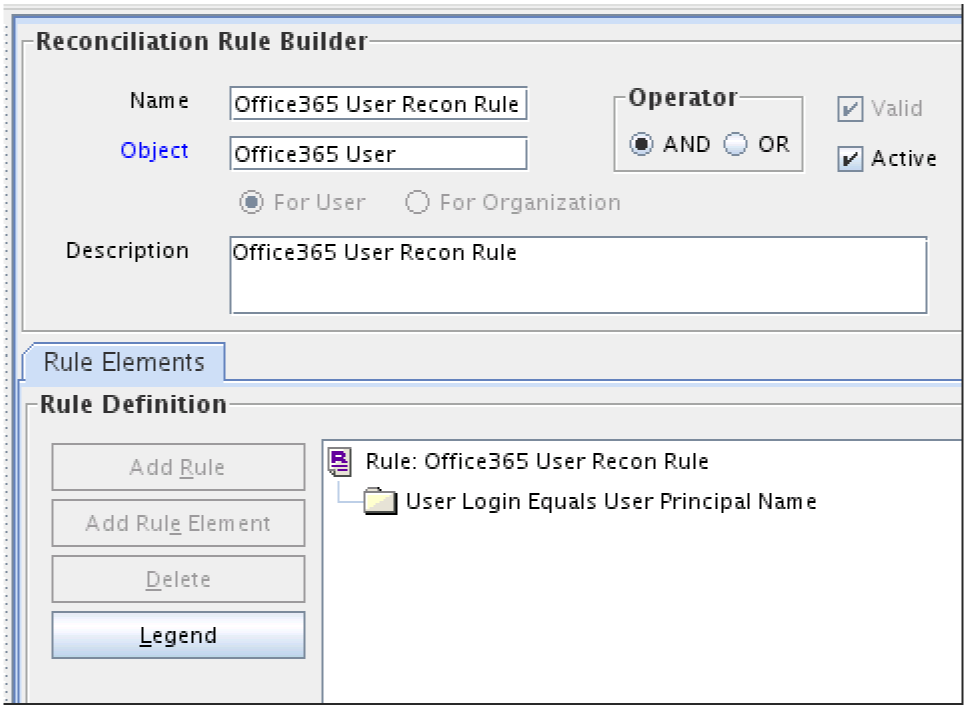
After you deploy the connector, you can view the reconciliation rules for users and groups on the Reconciliation Rule Builder form in Oracle Identity Manager Design Console.

To view the reconciliation rule for target resource reconciliation of users and groups:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools** and then double-click **Reconciliation Rules.**
3. Search for and open one of the following reconciliation rules:
   - For Users: **Office365 User Recon Rule**

     Figure 1-2 shows the target resource reconciliation rule for users.

Figure 1-2 Reconciliation Rule for Target Resource Reconciliation of Users



Reconciliation Rule Builder

Name: Office365 User Recon Rule

Object: Office365 User

Operator: ● AND ○ OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: Office365 User Recon Rule

Rule Elements

Rule Definition

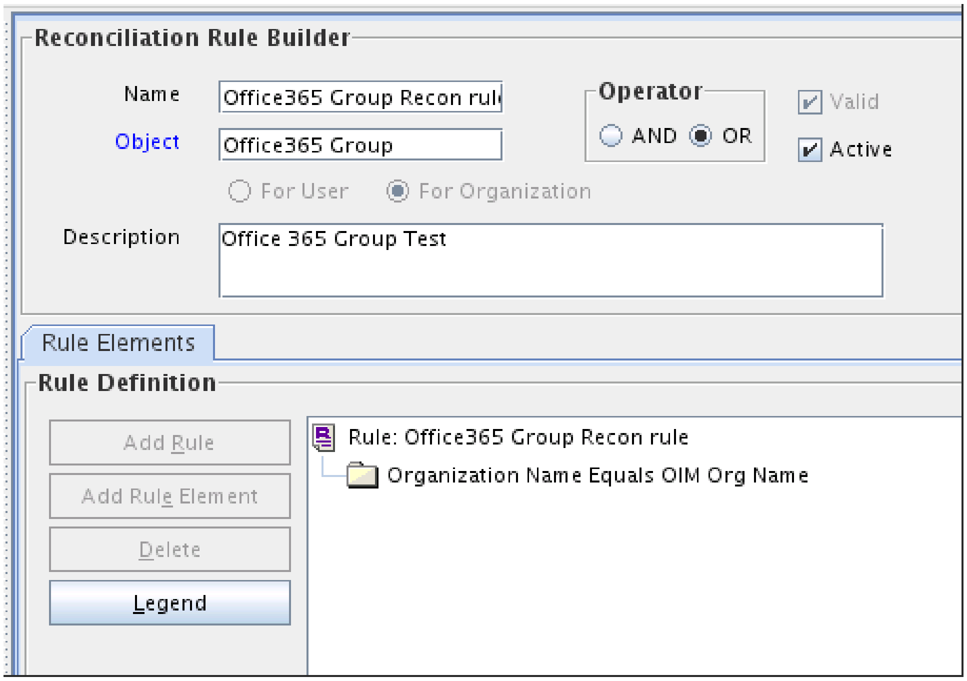
Rule: Office365 User Recon Rule

User Login Equals User Principal Name

   - For Groups: **Office365 Groups Recon Rule**

     Figure 1-3 shows the target resource reconciliation rule for groups.

Figure 1-3 Reconciliation Rule for Target Resource Reconciliation of Groups



Reconciliation Rule Builder

Name: Office365 Group Recon rul

Object: Office365 Group

○ For User ● For Organization

Operator: ○ AND ● OR

☑ Valid

☑ Active

Description: Office 365 Group Test

Rule Elements

Rule Definition

Rule: Office365 Group Recon rule

Organization Name Equals OIM Org Name

1.8.4 Reconciliation Action Rules for Target Resource Reconciliation

Reconciliation action rules define that actions the connector must perform based on the reconciliation rules defined for Users and Groups.

This section discusses the following topics related to reconciliation action rules for target resource reconciliation:

- Target Resource Reconciliation Action Rules for Users and Groups
- Viewing Reconciliation Action Rules for Target Resource Reconciliation

1.8.4.1 Target Resource Reconciliation Action Rules for Users and Groups

Reconciliation action rules specify the actions the connector must perform based on the result of the processing of a reconciliation event. The reconciliation action rules for both users and groups are the same.

Table 1-14 Action Rules for Target Resource Reconciliation of Users and Groups

Rule Condition	Action
No Matches Found	Create User
One Process Match Found	Establish Link
One Entity Match Found	Establish Link

1.8.4.2 Viewing Reconciliation Action Rules for Target Resource Reconciliation

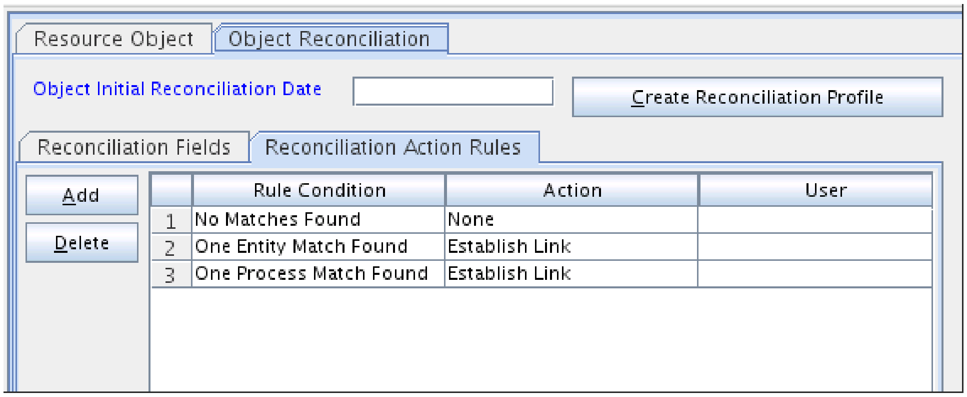
After you deploy the connector, you can view reconciliation action rules on the Object Reconciliation tab of a resource object in Oracle Identity Manager Design Console.

To view reconciliation action rules for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and then double-click **Resource Objects**.
3. Search for and open one of the following resource objects:
   - For Users: **Office365 User**
   - For Groups: **Office365 Group**
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 1-4 shows the reconciliation action rules for target resource reconciliation of both users and groups.

Figure 1-4 Reconciliation Action Rules for Target Resource Reconciliation of Users and Groups


Resource Object
Object Reconciliation
Object Initial Reconciliation Date
Create Reconciliation Profile
Reconciliation Fields
Reconciliation Action Rules
Add
Delete

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

1.9 Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

This section discusses the following topics:

- Provisioning Functions
- User Fields for Provisioning
- Group Fields for Provisioning

1.9.1 Provisioning Functions

These are the supported provisioning functions and the adapters that perform these functions for the Office 365 connector.

The Adapter column in Table 1-15 gives the name of the adapter that is used when the function is performed.

Table 1-15 User Provisioning Functions

Function	Adapter
Create User	adpOFFICE365CREATEOBJECT
Update User	adpOFFICE365UPDATEATTRIBUTEVALUE
Delete user	adpOFFICE365DELETEOBJECT
Enable user	adpOFFICE365ENABLETASK
Disable user	adpOFFICE365DISABLETASK
Change or reset password	adpOFFICE365UPDATEATTRIBUTEVALUE
Update child table values	adpOFFICE365UPDATECHILDTABLEVALUE
Add child table values	adpOFFICE365ADDCHILDTABLEVALUES
Remove child table values for a user	adpOFFICE365REMOVECHILDTABLEVALUES

1.9.2 User Fields for Provisioning

The Lookup.Office365.UM.ProvAttrMap lookup definition maps process form fields with Office 365 fields. This lookup definition is used for performing user provisioning operations.

In this lookup definition, entries are in the following format:

- **Code Key:** Name of the process form field
- **Decode:** Name of the target system user attribute at the Graph API level

Table 1-16 lists the entries in this lookup definition.

Table 1-16 Entries in the Lookup.Office365.UM.ProvAttrMap Lookup Definition

Code Key (Process Form Field)	Decode (Office 365 Field)
User Principal Name	__NAME__
Change Password On Next Login	passwordProfile.forceChangePasswordNextLogin
Preferred Language	preferredLanguage
Account Enabled	accountEnabled=”$(accountEnabled)”
Roles~Role Name[Lookup]	__ROLE__~__ROLE__~objectId
Country	country
Display Name	displayName
Licenses~Licesnse Name[Lookup]	assignedLicenses~assignedLicenses~skuId

Table 1-16 (Cont.) Entries in the Lookup.Office365.UM.ProvAttrMap Lookup Definition

Code Key (Process Form Field)	Decode (Office 365 Field)
Status	__ENABLE__
Object Id	__UID__
City	city
Group Names~Group Name[Lookup]	__GROUP__~__GROUP__~objectId
Usage Location	usageLocation
FirstName	givenName
Last Name	surname
Manager	manager
Mail NickName	mailNickname

1.9.3 Group Fields for Provisioning

The Lookup.Office365.GM.ProvAttrMap lookup definition maps user resource object fields and target system attributes. This lookup definition is used for performing group provisioning operations.

In this lookup definition, entries are in the following format:

- **Code Key:** Name of the process form field
- **Decode:** Name of the target system group attribute at the Graph API level

Table 1-17 lists the group fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-17 Entries in the Lookup.Office365.GM.ProvAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Office 365 Field
ObjectId	__UID__
Description	description
Mail Enabled	mailEnabled
Mail Nickname	mailNickname
Display Name	__NAME__
Security Enabled	securityEnabled

1.10 Connector Objects Used During Trusted Source Reconciliation

Trusted source reconciliation involves fetching data about newly created or modified accounts on the target system and using that data to create or update OIM Users.

The Office365 Trusted User Reconciliation scheduled task is used to initiate a trusted source reconciliation run. This scheduled task is discussed in Office365 Trusted User Reconciliation.

> **See Also:**
>
> Trusted Source Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for generic information about connector reconciliation

This section discusses the following connector objects:

- User Fields for Trusted Source Reconciliation
- Reconciliation Rule for Trusted Source Reconciliation
- Reconciliation Action Rules for Trusted Source Reconciliation

1.10.1 User Fields for Trusted Source Reconciliation

The Lookup.Office365.UM.ReconAttrMap.Trusted lookup definition maps user fields of the OIM User form with corresponding field names in the target system. This lookup definition is used for performing trusted source reconciliation runs. Values for the user identity fields in this lookup definition are fetched from the target system during a trusted source reconciliation run.

Table 1-18 Entries in the Lookup.Office365.UM.ReconAttrMap.Trusted Lookup Definition

Code Key (Resource Object Field)	Decode (Office 365 Field)
User Principal Name	__NAME__
Preferred Language	preferredLanguage
Country	country
Display Name	displayName
Status[TRUSTED]	__ENABLE__
Object Id	__UID__
Last Name	surname
Usage Location	UsageLocation
FirstName	givenName
Manager	manager

1.10.2 Reconciliation Rule for Trusted Source Reconciliation

Reconciliation rule for trusted source reconciliation is invoked when Oracle Identity Manager tries to determine the user record that is associated with a change on your target system (a trusted source).

This section discusses the following topics related to reconciliation rule for trusted source reconciliation:

- Trusted Source Reconciliation Rule for Users
- Viewing Reconciliation Rules for Trusted Source Reconciliation

1.10.2.1 Trusted Source Reconciliation Rule for Users

Reconciliation rule for trusted source reconciliation is invoked when Oracle Identity Manager tries to determine the user record that is associated with a change on your target system (a trusted source).

The following is the entity matching rule for users:

Rule name: Office 365 User Trusted Rule

Rule element: (User Login Equals User Principal Name) OR (Office365 GUID Equals Object Id)

In this first rule component:

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

In the second rule component:

- `Office365 GUID` is a UDF (user-defined field) for mapping target object ID with an OIM User.
- `Object Id` is the Object Id for an Office365 user.

1.10.2.2 Viewing Reconciliation Rules for Trusted Source Reconciliation

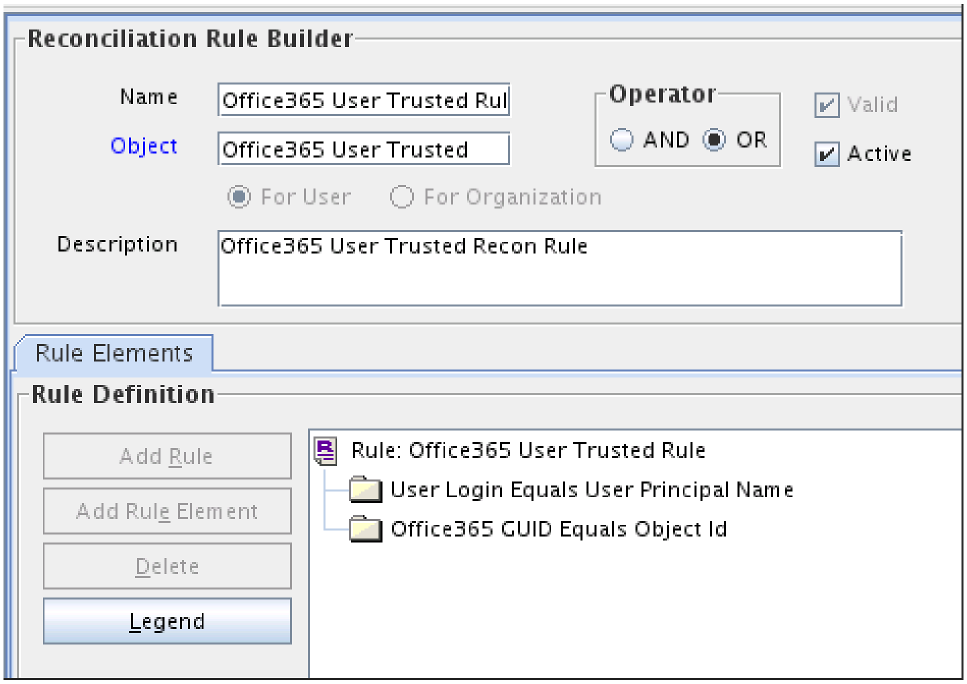
After you deploy the connector, you can view the reconciliation rules on the Reconciliation Rule Builder form in Oracle Identity Manager Design Console.

To view the reconciliation rule for trusted source reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools.**
3. Double-click **Reconciliation Rules.**
4. Search for **Office 365 User Trusted Rule.**

   Figure 1-5 shows the reconciliation rule for trusted source reconciliation.

Figure 1-5 Reconciliation Rule for Trusted Source Reconciliation



Name: Office365 User Trusted Rul

Object: Office365 User Trusted

● For User ○ For Organization

Description: Office365 User Trusted Recon Rule

Operator: ○ AND ● OR

☑ Valid

☑ Active

Rule: Office365 User Trusted Rule
- User Login Equals User Principal Name
- Office365 GUID Equals Object Id

5. Enter the text of the second step here.

1.10.3 Reconciliation Action Rules for Trusted Source Reconciliation

Reconciliation action rules specify the actions the connector must perform based on the result of the processing of a reconciliation event.

This section discusses the following topics related to reconciliation action rules:

- Trusted Source Reconciliation Action Rules for Users
- Viewing Reconciliation Action Rules for Trusted Source Reconciliation

1.10.3.1 Trusted Source Reconciliation Action Rules for Users

Reconciliation action rules specify the actions the connector must perform based on the result of the processing of a reconciliation event.

Table 1-19 Action Rules for Trusted Source Reconciliation

Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.10.3.2 Viewing Reconciliation Action Rules for Trusted Source Reconciliation

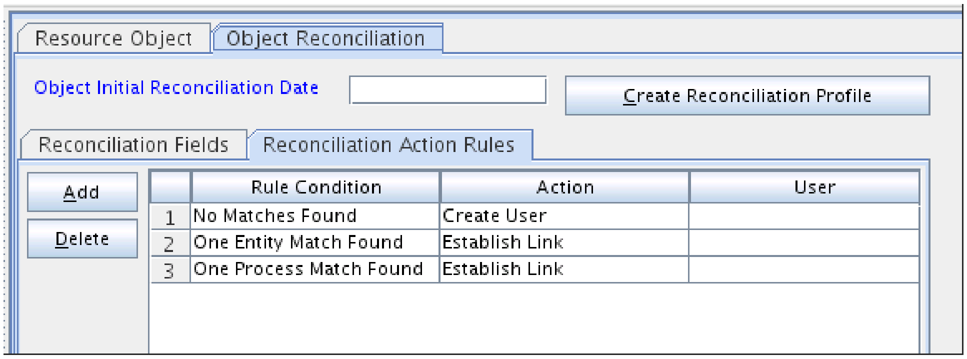
After you deploy the connector, you can view reconciliation action rules on the Object Reconciliation tab of a resource object in Oracle Identity Manager Design Console

To view reconciliation action rules for trusted source reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management.**
3. Double-click **Resource Objects.**
4. Locate the **Office365 User Trusted** resource object.
5. Click the **Object Reconciliation** tab, and then the **Reconciliation Action Rules** tab.

   The Reconciliation Action Rules tab displays the action rules defined for this connector.
   Figure 1-6 shows the reconciliation action rule for trusted source reconciliation.

Figure 1-6 Reconciliation Action Rules for Trusted Source Reconciliation


Resource Object
Object Reconciliation
Object Initial Reconciliation Date
Create Reconciliation Profile
Reconciliation Fields
Reconciliation Action Rules
Add
Delete

	Rule Condition	Action	User
1	No Matches Found	Create User	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

1.11 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Deploying the Office 365 Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Using the Office 365 Connector describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Extending the Functionality of the Office365 Connector describes procedures that you can perform if you want to extend the functionality of the connector.
- Files and Directories on the Office 365 Connector Installation Media lists the files and directories that comprise the connector installation media.

2 Deploying the Office 365 Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, and postinstallation.

The following topics discuss these stages:

- Preinstallation
- Installation
- Postinstallation

> **Note:**
>
> Some of the procedures described in this chapter must be performed on the target system. To perform these procedures, you must use an Office 365 account with administrator privileges.

2.1 Preinstallation

Preinstallation for the Office 365 connector involves registering a client application (that is, the Office 365 connector) with the target system 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.

Preinstallation involves performing the following tasks on the target system:

> **Note:**
>
> The detailed instructions for performing these preinstallation tasks are available in the Office 365 product documentation at https://docs.microsoft.com/en-us/microsoft-365/.

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 Installation

You must install the Office 365 connector in Oracle Identity Manager and if required, place the connector code bundle in the Connector Server.

The following topics discuss installing the Office 365 connector:

- Understanding Installation of the Office 365 Connector
- Running the Connector Installer
- Configuring the IT Resource for the Target System

2.2.1 Understanding Installation of the Office 365 Connector

You can run the connector code either locally in Oracle Identity Manager or remotely in a Connector Server.

Depending on where you want to run the connector code (bundle), the connector provides the following installation options:

- Run the connector code locally in Oracle Identity Manager. In this scenario, you deploy the connector in Oracle Identity Manager. Deploying the connector in Oracle Identity Manager involves performing the procedures described in Running the Connector Installer and Configuring the IT Resource for the Target System
- Run the connector code remotely in a Connector Server. In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server. See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server.

2.2.2 Running the Connector Installer

When you run the Connector Installer, it automatically copies the connector files to directories in Oracle Identity Manager, imports connector XML files, and compiles adapters used for provisioning.

> **Note:**
>
> In this guide, the term Connector Installer has been used to refer to the Install Connectors feature of Oracle Identity Manager Administrative and User Console.

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory: *OIM_HOME*/server/ConnectorDefaultDirectory.

    > **Note:**
    >
    > If you are doing it for the first time place the bundle in connector server bundle directory, in that case you need to unzip the bundle before starting the installation.

2. Log in to Oracle Identity System Administration.
3. From the left pane, expand the **Provisioning Configuration** tab and click **Manage Connector**.
4. In the Manage Connector page, click **Install**.
5. From the Connector List, select **Office365 Connector *RELEASE_NUMBER***.

    This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.
    If you have copied the installation files into a different directory, then:

    a. In the **Alternative Directory** field, enter the full path and name of that directory.
    b. To repopulate the list of connectors in the Connector List list, click **Refresh.**
    c. From the Connector List list, select **Office365 Connector *RELEASE_NUMBER.***

6. Click **Load.**
7. To start the installation process, click **Continue.**

    The following tasks are performed in sequence:

    a. Configuration of connector libraries
    b. Import of the connector XML files (by using the Deployment Manager)
    c. Compilation of adapters

    On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. If a task fails, then make the required correction and perform one of the following steps:

   a. Retry the installation by clicking **Retry.**
   b. Cancel the installation and begin again from Step 3.

8. Click **Exit** to finish the installation procedure.

   If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed.

      > **Note:**
      >
      > At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Clearing Content Related to Connector Resource Bundles from the Server Cache for information about running the PurgeCache utility. There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector.

      Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks that are created when you installed the connector. Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide. When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table A-1.

2.2.3 Configuring the IT Resource for the Target System

The IT resource for the target system is created during connector installation. This IT resource contains connection information about the target system. Oracle Identity Manager uses this information during reconciliation and provisioning.

The Office365 IT resource is automatically created when you run the Connector Installer. To specify values for the parameters of the IT resource:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **IT Resource**.
3. In the **IT Resource Name** field on the Manage IT Resource page, enter `Office365` and then click **Search**.
4. Click the Edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource. Table 2-1 describes each parameter.

Table 2-1 Parameters of the Office 365 IT Resource

Parameter	Description
Configuration Lookup	Name of the lookup definition that stores configuration information used during reconciliation and provisioning operation. If you have configured your target system as a target resource, then enter `Lookup.Office365.Configuration`. If you have configured your target system as a trusted source, then enter `Lookup.Office365.Configuration.Trusted`. Default value: `Lookup.Office365.Configuration`
Connector Server Name	If you have deployed the Office 365 connector in the Connector Server, then enter the name of the IT resource for the Connector Server.
proxyHost	Name of the proxy host used to connect to an external target. Sample value: `www.example.com.`
proxyPort	Proxy port number. Sample value: `80`
proxyUser	Proxy user name of the target system user account that Oracle Identity Manager uses to connect to the target system.
proxyPassword	Password of the proxy user ID of the target system user account that Oracle Identity Manager uses to connect to the target system.
authenticationServerUrl	Enter the URL of the authentication server that validates the client ID and client secret for your target system. Sample value: `https:// login.windows.net/ mydomain / oauth2/token?api-version=1.0`
authenticationType	Type of authentication used by your target system. For this connector, the target system OAuth2.0 client credentials. Default value: `client_credentials` Do *not* modify the value of the parameter.
clientId	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 Preinstallation.

Table 2-1 (Cont.) Parameters of the Office 365 IT Resource

Parameter	Description
clientSecret	Enter the secret key used to authenticate the identity of your client application. You obtained the secret key while performing the procedure described in Preinstallation.
Host	Enter the host name of the computer hosting your target system. Sample value: `graph.windows.net`
Port	Enter the port number at which the target system is listening. Sample value: 443
sslEnabled	If the target system requires SSL connectivity, then set the value of this parameter to `true.` Otherwise set the value to `false`. Default value: `true`
uriPlaceHolder	Key-value pair for replacing place holders in the relURIs. The URI place holder consists of values which are repeated in every relative URL. Values must be comma separated. For example, tenant ID and API version values are a part of every request URL. Therefore, we replace it with a key-value pair. Sample value: `"tenant_id;domain name","api_version;api-version=1.6"`

7. To save the values, click **Update**.

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- Configuring Oracle Identity Manager
- Localizing Field Labels in UI Forms
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Managing Logging for the Office 365 Connector
- Configuring SSL for Office 365

2.3.1 Configuring Oracle Identity Manager

You must create a UI form and an application instance for the resource against which you want to perform reconciliation and provisioning operations. In addition, you must run entitlement and catalog synchronization jobs.

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

- Creating and Activating a Sandbox

- Creating a New UI Form
- Creating an Application Instance
- Publishing a Sandbox
- Harvesting Entitlements and Sync Catalog
- Updating an Existing Application Instance with a New Form

2.3.1.1 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 and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.3.1.2 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 Manager*.

While creating the UI form, ensure that you select the resource object corresponding to the Office 365 connector that you want to associate the form with. In addition, select the **Generate Entitlement Forms** check box.

2.3.1.3 Creating an Application Instance

See Creating Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

2.3.1.4 Publishing a Sandbox

Before you publish a sandbox, perform the following procedure as a best practice to validate all sandbox changes made till this stage as it is hard to revert changes once a sandbox is published:

1. In the System Administration console, deactivate the sandbox.
2. Log out of the System Administration console.
3. Log in to the Self Service console using the xelsysadm user credentials and then activate the sandbox that you deactivated in Step 1.
4. In the Catalog, ensure that the Office 365 application instance form appears with correct fields.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.3.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Scheduled Jobs for Lookup Field Synchronization for Office 365 Connector.

2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

2.3.1.6 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, 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. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
2. Create a new UI form for the resource. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
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 Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.3.2 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 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_en.xlf"
   ```

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.BaseRuntimeResource
      Bundle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.us
      erEO.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.Offic
      e365FormEO.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.BaseRuntimeResource
      Bu ndle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.us
      e 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.entity
       sEO.UD_GA_USR_ACCOUNT_NAME__c_LABEL"><source>Account Name</source>
      <target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target> </trans-unit>
      ```

   f. Repeat Steps 6.a through 6.d for all attributes of the process form.

   g. Save the file as BizEditorBundle_*LANG_CODE.xlf.* In this file name, replace *LANG_CODE* with the code of the language to which you are localizing. Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

> **See Also:**
>
> Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about exporting and importing metadata files

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

2.3.3 Clearing Content Related to Connector Resource Bundles from the Server Cache

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, switch to the *OIM_HOME*/server/bin directory.
2. Enter one of the following commands:
   - **On Microsoft Windows:** `PurgeCache.bat All`
   - **On UNIX:** `PurgeCache.sh All`

   > **Note:**
   >
   > You can use the PurgeCache utility to purge the cache for any content category. Run PurgeCache.bat *CATEGORY_NAME* on Microsoft Windows or PurgeCache.sh *CATEGORY_NAME* on UNIX. The *CATEGORY_NAME* argument represents the name of the content category that must be purged.
   > For example, the following commands purge Metadata entries from the server cache:
   >
   > - `PurgeCache.bat MetaData`
   > - `PurgeCache.sh MetaData`
   >
   > Before running the PurgeCache utility, ensure the WL_HOME and JAVA_HOME environment variables are set.

   When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

   t3://*OIM_HOST_NAME*:*OIM_PORT_NUMBER*

   In this format:

   - Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.

- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

2.3.4 Managing Logging for the Office 365 Connector

Oracle Identity Manager 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

2.3.4.1 Understanding Log Levels

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. ODL is the principle logging service used by Oracle Identity Manager and is based on java.util.Logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.
- SEVERE

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

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

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

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

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

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

Table 2-2 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

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

Java Level	ODL Message Type:Level
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE16
FINEST	TRACE32

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

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

2.3.4.2 Enabling Logging

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


<logger name="ORG.IDENTITYCONNECTORS.OFFICE365" 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. Table 2-2 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.ODLHandlerFactory'>
    <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.OFFICE365" level="NOTIFICATION:
1" useParentHandlers="false">
    <handler name="Office365-handler"/>
    <handler name="console-handler"/>
</logger>
```

With these sample values, when you use Oracle Identity Manager, 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.

2.3.5 Configuring SSL for Office 365

Configure SSL to secure data communication between Oracle Identity Manager and Office 365.

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

   ```
   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 Manager is in sync with the validity date of the SSL certificate to avoid any errors during SSL communication.

3

Using the Office 365 Connector

You can use the connector for performing reconciliation and provisioning operations after configuring it to meet your requirements.

This chapter is discusses the following topics:

> **Note:**
>
> These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- Scheduled Jobs for Lookup Field Synchronization for Office 365 Connector
- Configuring Reconciliation for Office 365 Connector
- Configuring Scheduled Jobs
- Guidelines on Performing Provisioning Operations
- Performing Provisioning Operations
- Uninstalling the Connector

3.1 Scheduled Jobs for Lookup Field Synchronization for Office 365 Connector

Scheduled jobs for lookup field synchronization fetch the most recent values from specific fields in the target system to lookup definitions in Oracle Identity Manager. These lookup definitions are used as an input source for lookup fields in Oracle Identity Manager.

The following scheduled jobs are used for lookup fields synchronization:

- Office365 Group Lookup Reconciliation
- Office365 Licenses Lookup Reconciliation
- Office365 Roles Lookup Reconciliation
- Office365 Manager Lookup Reconciliation

The following scheduled jobs are used for lookup fields synchronization:

Values fetched by these scheduled jobs from the target system are populated in the Lookup.Office365.Groups, Lookup.Office365.Licenses, Lookup.Office365.Roles and Lookup.Office365.Manager lookup definitions, respectively..

The attributes for all the scheduled jobs for lookup field synchronization are the same. Table 3-1describes the attributes of the scheduled jobs. The procedure to configure scheduled jobs is described later in this guide.

Table 3-1 Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Name of the connector attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). . Default value: `__UID__`
Decode Attribute	Name of the connector attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: `__NAME__`
IT Resource Name	Name of the IT resource for the target system installation from which you want reconcile user records. Default value: `Office365`
Lookup Name	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Depending on the scheduled job that you are using, the default values are as follows: • For Office365 Group Lookup Reconciliation: `Lookup.Office365.Groups` • For Office365 Licenses Lookup Reconciliation: `Lookup.Office365.Licenses` • For Office365 Roles Lookup Reconciliation: `Lookup.Office365.Roles` • For Office365 Manager Lookup Reconciliation: `Lookup.Office365.Manager` If you create a copy of any of these lookup definitions, then enter the name of that new lookup definition as the value of the Lookup Name attribute.
Object Type	Enter the type of object you want to reconcile. Depending on the scheduled job that you are using, the default values are as follows: • For Office365 Group Lookup Reconciliation: `__GROUP__` • For Office365 Licenses Lookup Reconciliation: `__LICENSE__` • For Office365 Roles Lookup Reconciliation: `__ROLE__` • For Office365 Manager Lookup Reconciliation: `User`

3.2 Configuring Reconciliation for Office 365 Connector

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

This section discusses the following topics related to configuring reconciliation:

- Full Reconciliation for Office 365 Connector
- Limited Reconciliation for Office 365 Connector
- Reconciling Large Number of Records
- Reconciliation Scheduled Jobs for Office 365 Connector

3.2.1 Full Reconciliation for Office 365 Connector

Full reconciliation involves reconciling all existing user or group records from the target system into Oracle Identity Manager.

After you deploy the connector, you must first perform full reconciliation. To perform a full reconciliation run, ensure that no value is specified for the Filter attribute of the scheduled job for reconciling users and groups. If the target system contains more number of records than what it can return in a single response, then use the Flat File connector to perform full reconciliation. See Reconciling Large Number of Records.

3.2.2 Limited Reconciliation for Office 365 Connector

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. This connector provides a Filter Suffix attribute (a scheduled task attribute) that allows you to use any of the attributes of the target system to filter target system records. You specify a value for the Filter Suffix attribute while configuring the user reconciliation scheduled job.

> **Note:**
>
> If the target system contains more number of records than what it can return in a single response, then use the Flat File connector to perform limited reconciliation. See Reconciling Large Number of Records.

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.

3.2.3 Reconciling Large Number of Records

During a reconciliation run, if the target system contains more number of records than what it can return in a single response, then you must use the Flat File connector to fetch all the records into Oracle Identity Manager.

To reconcile a large number of records from the target system into Oracle Identity Manager:

1. Export all users in the target system to a flat file.
2. Copy the flat file to a location that is accessible from Oracle Identity Manager.
3. Create a schema file representing the structure of the flat file. See Creating a Schema File in *Oracle Identity Manager Connector Guide for Flat File*.
4. Install the Flat File connector. See Running the Connector Installer in *Oracle Identity Manager Connector Guide for Flat File*.
5. Configure the Flat File IT resource. See Configuring the IT Resource in *Oracle Identity Manager Connector Guide for Flat File*.
6. If you want to perform trusted source reconciliation, then configure and run the Flat File Users Loader scheduled job.

   While configuring this scheduled job, ensure that you set the value of the **Target IT Resource Name** attribute to `Office365` and **Target Resource Object Name** to `Office365 User Trusted`.

   See Flat File Users Loader and IT_RES_NAME Flat File Users Loader in *Oracle Identity Manager Connector Guide for Flat File* for information about the attributes of the Flat File Users Loader scheduled job.
7. If you want to perform target resource reconciliation, then configure and run the Flat File Accounts Loader scheduled job.

   While configuring this scheduled job, ensure that you set the value of the **Target IT Resource Name** attribute to `Office365` and **Target Resource Object Name** to `Office365 User`.

   See Flat File Accounts Loader and IT_RES_NAME Flat File Accounts Loader in *Oracle Identity Manager Connector Guide for Flat File* for information about the attributes of the Flat File Accounts Loader scheduled job.

3.2.4 Reconciliation Scheduled Jobs for Office 365 Connector

When you run the Connector Installer, reconciliation scheduled jobs are automatically created in Oracle Identity Manager: You must configure these scheduled jobs to suit your requirements by specifying values for its attributes.

This section discusses the following scheduled jobs that you can configure for reconciliation:

- Office365 User Reconciliation
- Office365 Group Recon
- Office365 Trusted User Reconciliation

3.2.4.1 Office365 User Reconciliation

You use the Office365 Target Resource User Reconciliation scheduled job to reconcile user account data from the target system in the target resource (account management) mode of the connector.

Table 3-2 Attributes of the Office365 User Reconciliation Scheduled Task

Attribute	Description
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. See Limited Reconciliation for Office 365 Connector.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `Office365`
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `User` Do *not* change the default value.
Resource Object Name	Name of the resource object against which reconciliation runs are performed. Default value: `Office365 User` Do *not* change the default value.
Incremental Recon Attribute	Attribute that holds the timestamp at which the token record was modified.
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. **Note:** Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: `1354753427000`

3.2.4.2 Office365 Group Recon

You use the Office365 Group Recon scheduled job to reconcile group data from the target system in target resource (account management) mode of the connector.

Table 3-3 Attributes of the Office365 Group Recon Scheduled Job

Attribute	Description
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. See Limited Reconciliation for Office 365 Connector for more information about this attribute.

Table 3-3 (Cont.) Attributes of the Office365 Group Recon Scheduled Job

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `Office365`
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `Group` **Note:** Do not change the default value.
Organization Name	Enter the name of the Oracle Identity Manager organization in which reconciled groups must be created or updated.
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: `Office365 Group` **Note:** Do not change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: `Office365 Group Recon`
Incremental Recon Attribute	Attribute that holds the timestamp at which the token record was modified.
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. **Note:** Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: `1354753427000`

3.2.4.3 Office365 Trusted User Reconciliation

You use the Office365 Trusted User Reconciliation scheduled job to reconcile user account data in the trusted source (identity management) mode of the connector.

Table 3-4 Attributes of the Office365 User Reconciliation Scheduled Job

Attribute	Description
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. See Limited Reconciliation for Office 365 Connector.
IT Resource Name	Enter the name of the IT resource for the system installation from which you want to reconcile user records. Default value: `Office365`

Table 3-4 (Cont.) Attributes of the Office365 User Reconciliation Scheduled Job

Attribute	Description
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `User` **Note:** Do not change the default value.
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: `Office365 User Trusted` **Note:** Do not change the default value.
Incremental Recon Attribute	Attribute that holds the timestamp at which the token record was modified.
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. **Note:** Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: `1354753427000`

3.3 Configuring Scheduled Jobs

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

You can apply this procedure to configure the scheduled jobs for lookup field synchronization and reconciliation.

To configure a scheduled job:

1. Log in to Oracle 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 Manager*.

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:**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
> - 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.
> - See Reconciliation Scheduled Jobs for Office 365 Connector for the list of scheduled tasks and their attributes.

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

> **Note:**
>
> The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

3.4 Guidelines on Performing Provisioning Operations

These guidelines provide information on what to do when performing provisioning operations.

The following are guidelines that you must apply while performing a provisioning operation:

- 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.

3.5 Performing Provisioning Operations

You create a new user in Oracle 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 Manager:

1. Log in to Oracle 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 created in Creating an Application Instance, and then click **Checkout.**
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.
7. If you want to provision entitlements, then:
    a. On the Entitlements tab, click **Request Entitlements**.
    b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout**.
    c. Click **Submit**.

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

3.6 Uninstalling the Connector

Uninstalling the connector deletes all the account related data associated with resource objects of the connector.

If you want to uninstall the connector for any reason, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4

Extending the Functionality of the Office365 Connector

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

This chapter discusses the following topics:

> **Note:**
>
> From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See Managing Lookups in *Oracle Fusion Middleware Administering Oracle Identity Manager* for information about managing lookups by using the Form Designer in the Oracle Identity Manager System Administration console.

- Adding New User or Group Attributes for Reconciliation
- Adding New User or Group Attributes for Provisioning
- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During User Reconciliation
- Configuring the Connector for Multiple Installations of the Target System
- About Defining the Connector

4.1 Adding New User or Group Attributes for Reconciliation

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

The default attribute mappings for reconciliation are listed in Table 1-12 and Table 1-13.

> **Note:**
>
> - This connector supports configuration of already existing (standard) attributes of Office 365 for reconciliation.
> - Only single-valued attributes can be mapped for reconciliation.

The following topics discuss the procedure to add new attributes for users or groups:

- Adding New Attributes on the Process Form
- Adding Attributes to the Resource Object
- Creating Reconciliation Field Mapping
- Creating Entries in Lookup Definitions
- Performing Changes in a New UI Form

4.1.1 Adding New Attributes on the Process Form

You add a new attribute on the process form in the Form Designer section of Oracle Identity Manager Design Console.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open one of the following process forms:
   - For Users: **UD_O365_USR**
   - For Groups: **UD_O365_GRP**
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the field.

   For example, if you are adding the TELEPHONENUMBER field, enter `UD_O365_USR_TELEPHONENUMBER` in the Name field and then enter other details such as Variable Type, Length, Field Label, and Field Type.
6. Click the Save icon, and then click **Make Version Active**. The following screenshot shows the new field added to the process form.

Figure 4-1 New Field Added to the Process Form

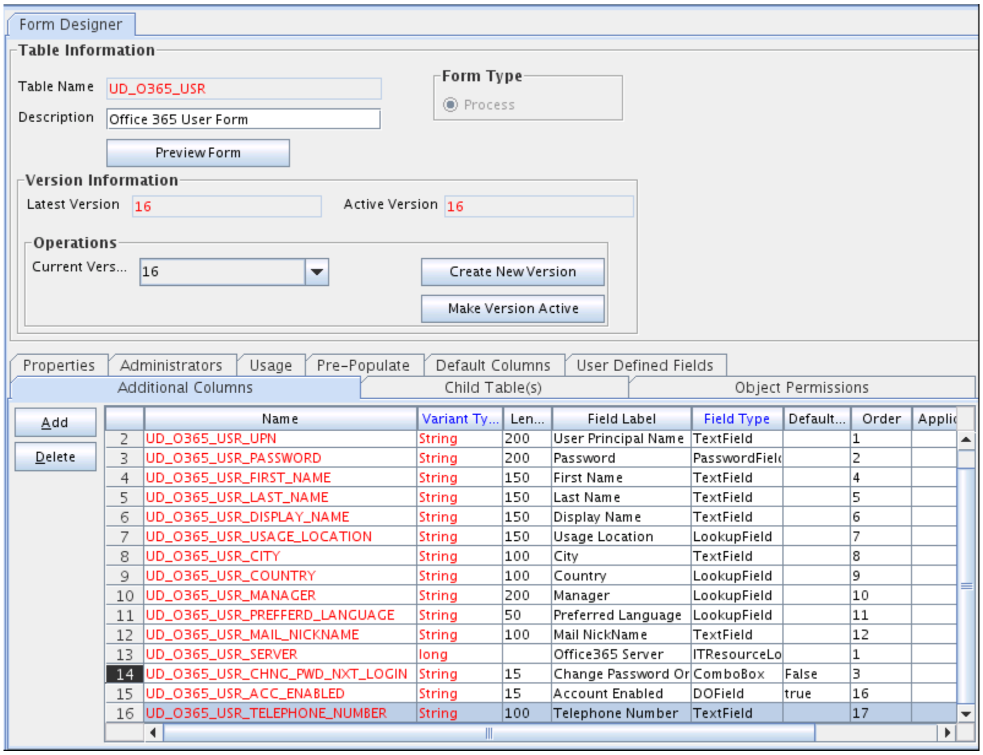


Table Information

Table Name: UD_O365_USR

Description: Office 365 User Form

Form Type: ● Process

Version Information

Latest Version: 16

Active Version: 16

Operations

Current Vers...: 16

	Name	Variant Ty...	Len...	Field Label	Field Type	Default...	Order	Applic
2	UD_O365_USR_UPN	String	200	User Principal Name	TextField		1	
3	UD_O365_USR_PASSWORD	String	200	Password	PasswordFiel(		2	
4	UD_O365_USR_FIRST_NAME	String	150	First Name	TextField		4	
5	UD_O365_USR_LAST_NAME	String	150	Last Name	TextField		5	
6	UD_O365_USR_DISPLAY_NAME	String	150	Display Name	TextField		6	
7	UD_O365_USR_USAGE_LOCATION	String	150	Usage Location	LookupField		7	
8	UD_O365_USR_CITY	String	100	City	TextField		8	
9	UD_O365_USR_COUNTRY	String	100	Country	LookupField		9	
10	UD_O365_USR_MANAGER	String	200	Manager	LookupField		10	
11	UD_O365_USR_PREFFERD_LANGUAGE	String	50	Preferred Language	LookupField		11	
12	UD_O365_USR_MAIL_NICKNAME	String	100	Mail NickName	TextField		12	
13	UD_O365_USR_SERVER	long		Office365 Server	ITResourceLo		1	
14	UD_O365_USR_CHNG_PWD_NXT_LOGIN	String	15	Change Password Or	ComboBox	False	3	
15	UD_O365_USR_ACC_ENABLED	String	15	Account Enabled	DOField	true	16	
16	UD_O365_USR_TELEPHONE_NUMBER	String	100	Telephone Number	TextField		17	

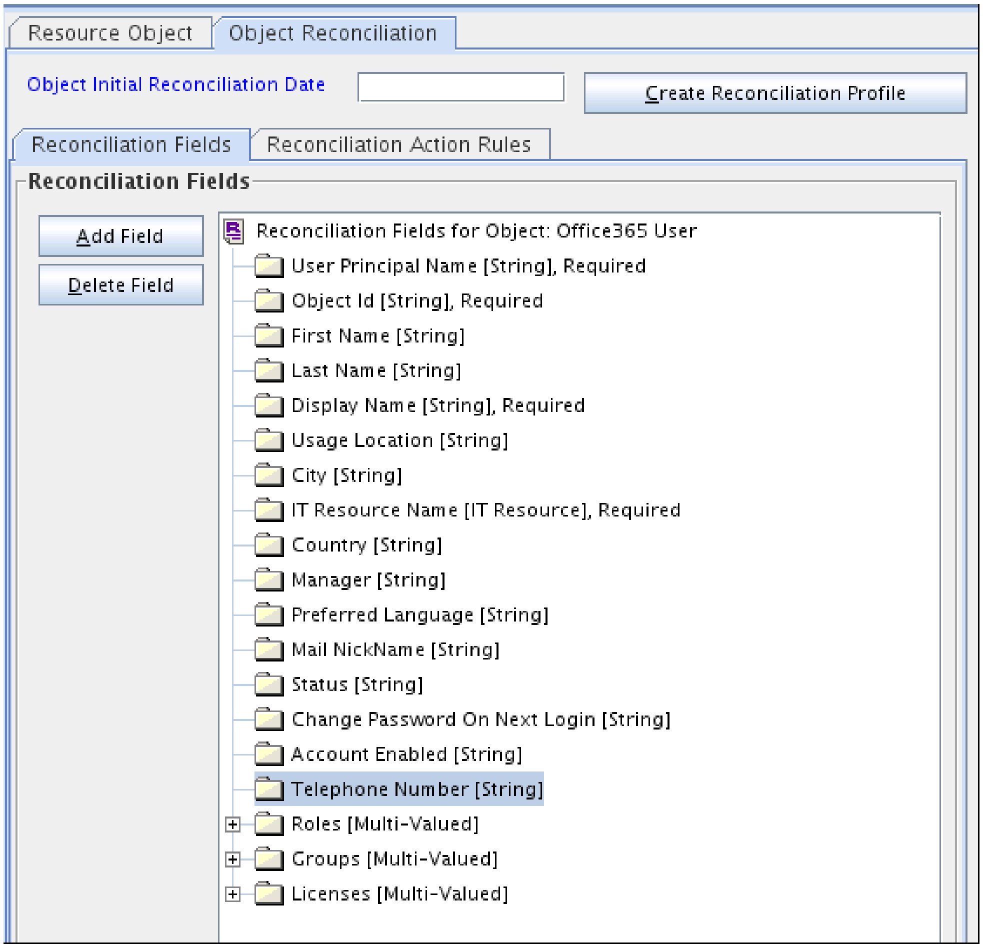
4.1.2 Adding Attributes to the Resource Object

You can add the new attribute to the resource object in the Resource Objects section of Oracle Identity Manager Design Console.

1. Expand **Resource Management**, and double-click **Resource Objects**.
2. Search for and open one of the following resource objects:
   - For Users: **Office365 User**
   - For Groups: **Office365 Group**
3. On the Object Reconciliation tab, click **Add Field**.
4. Enter the details of the field.

   For example, enter `TELEPHONE NUMBER` in the **Field Name** field and select **String** from the **Field Type** list. Later in this procedure, you enter the field name as the Code value of the entry that you create in the lookup definition for reconciliation.
5. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:

Figure 4-2 New Reconciliation Field Added to the Resource Object



Reconciliation Fields for Object: Office365 User

- User Principal Name [String], Required
- Object Id [String], Required
- First Name [String]
- Last Name [String]
- Display Name [String], Required
- Usage Location [String]
- City [String]
- IT Resource Name [IT Resource], Required
- Country [String]
- Manager [String]
- Preferred Language [String]
- Mail NickName [String]
- Status [String]
- Change Password On Next Login [String]
- Account Enabled [String]
- Telephone Number [String]
- Roles [Multi-Valued]
- Groups [Multi-Valued]
- Licenses [Multi-Valued]

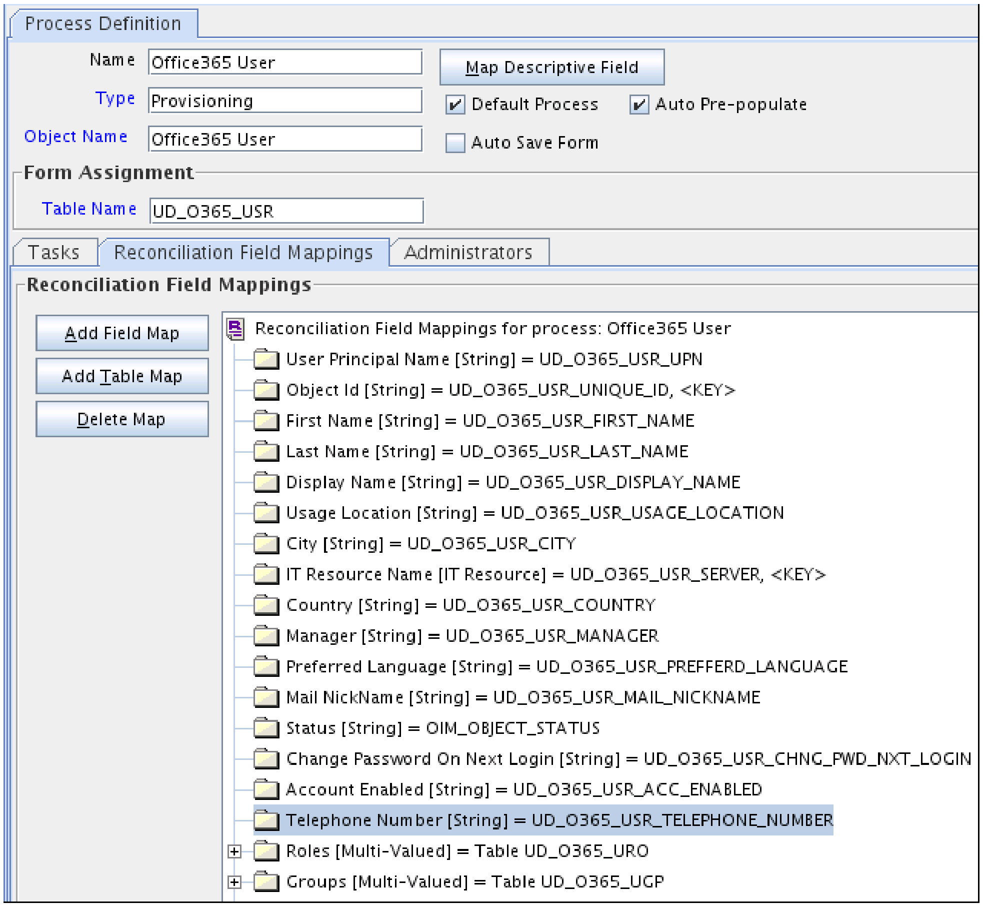
6. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.

4.1.3 Creating Reconciliation Field Mapping

You create a reconciliation field mapping for the new attribute in the Process Definition section of Oracle Identity Manager Design Console.

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open one of the following process definitions:
   - For Users: **Office365 User**
   - For Groups: **Office365 Group**
3. On the Reconciliation Field Mappings tab of the process definition, click **Add Field Map**.
4. From the Field Name list, select the field that you want to map.
5. Double-click the **Process Data Field** field, and then select the column for the attribute. For example, select **UD_TELEPHONENUMBER**.
6. Click the **Save** icon. The following screenshot shows the new reconciliation field mapped to a process data field in the process definition:

Figure 4-3 New Reconciliation Field Mapped to a Process Data Field in the Process Definition



Name: Office365 User

Type: Provisioning

Object Name: Office365 User

☑ Default Process ☑ Auto Pre-populate

□ Auto Save Form

Table Name: UD_O365_USR

Reconciliation Field Mappings

- Reconciliation Field Mappings for process: Office365 User
  - User Principal Name [String] = UD_O365_USR_UPN
  - Object Id [String] = UD_O365_USR_UNIQUE_ID, <KEY>
  - First Name [String] = UD_O365_USR_FIRST_NAME
  - Last Name [String] = UD_O365_USR_LAST_NAME
  - Display Name [String] = UD_O365_USR_DISPLAY_NAME
  - Usage Location [String] = UD_O365_USR_USAGE_LOCATION
  - City [String] = UD_O365_USR_CITY
  - IT Resource Name [IT Resource] = UD_O365_USR_SERVER, <KEY>
  - Country [String] = UD_O365_USR_COUNTRY
  - Manager [String] = UD_O365_USR_MANAGER
  - Preferred Language [String] = UD_O365_USR_PREFFERD_LANGUAGE
  - Mail NickName [String] = UD_O365_USR_MAIL_NICKNAME
  - Status [String] = OIM_OBJECT_STATUS
  - Change Password On Next Login [String] = UD_O365_USR_CHNG_PWD_NXT_LOGIN
  - Account Enabled [String] = UD_O365_USR_ACC_ENABLED
  - Telephone Number [String] = UD_O365_USR_TELEPHONE_NUMBER
  - Roles [Multi-Valued] = Table UD_O365_URO
  - Groups [Multi-Valued] = Table UD_O365_UGP

4.1.4 Creating Entries in Lookup Definitions

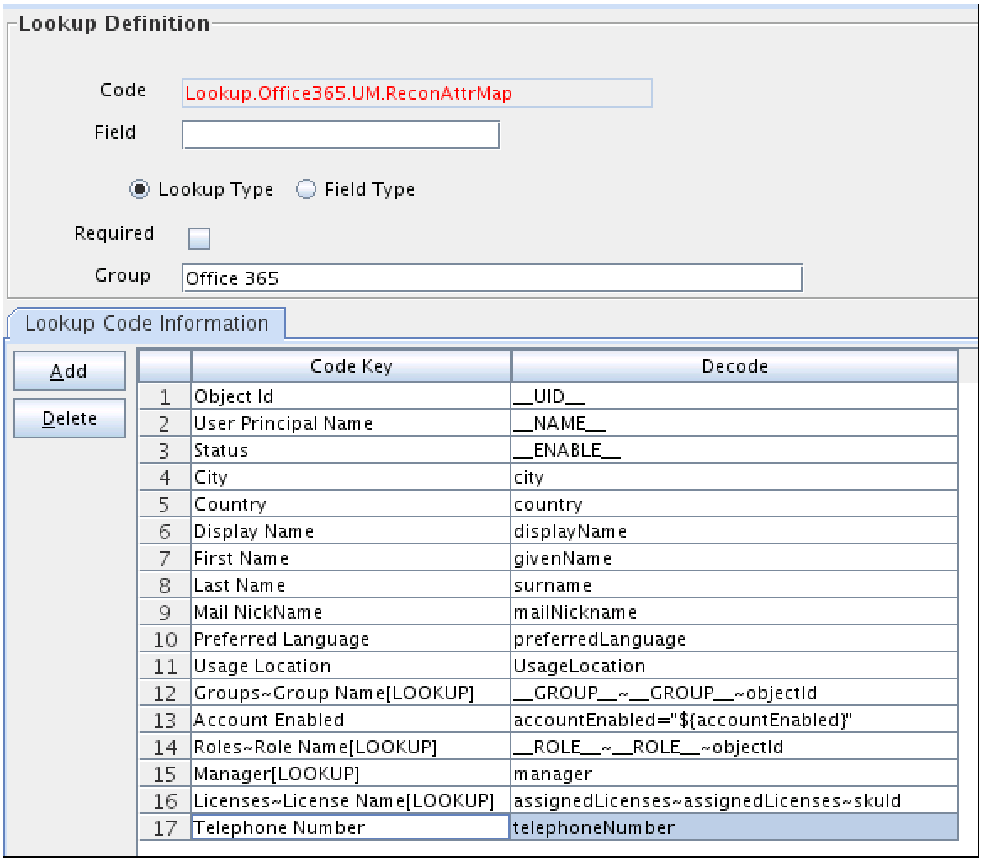
You create an entry for the newly added attribute in the lookup definition that holds attribute mappings for reconciliation.

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open one of the following lookup definitions.
   - For Users: **Lookup.Office365.UM.ReconAttrMap**
   - For Groups: **Lookup.Office365.GM.ReconAttrMap**
4. Click **Add** and enter the Code Key and Decode values for the field.

   The Code Key value must be the name of the field in the resource object. The Decode value must be the name of the target system field in the Graph API. Refer to the following Microsoft Developer Network page for the names of target system attributes in the Graph API: https://msdn.microsoft.com/en-gb/library/azure/ad/graph/api/entity-and-complex-type-reference#UserEntity
5. Click the Save icon.

   The following screenshot shows the entry added to the lookup definition:

Figure 4-4   Entry Added to the Lookup Definition



Lookup Definition

Code: Lookup.Office365.UM.ReconAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: Office 365

Lookup Code Information

	Code Key	Decode
1	Object Id	__UID__
2	User Principal Name	__NAME__
3	Status	__ENABLE__
4	City	city
5	Country	country
6	Display Name	displayName
7	First Name	givenName
8	Last Name	surname
9	Mail NickName	mailNickname
10	Preferred Language	preferredLanguage
11	Usage Location	UsageLocation
12	Groups~Group Name[LOOKUP]	__GROUP__~__GROUP__~objectId
13	Account Enabled	accountEnabled="${accountEnabled}"
14	Roles~Role Name[LOOKUP]	__ROLE__~__ROLE__~objectId
15	Manager[LOOKUP]	manager
16	Licenses~License Name[LOOKUP]	assignedLicenses~assignedLicenses~skuId
17	Telephone Number	telephoneNumber

4.1.5 Performing Changes in a New UI Form

You must replicate all changes made to the Form Designer of the Design Console in a new UI form.

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form, and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

4.2 Adding New User or Group Attributes for Provisioning

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

The default attribute mappings for provisioning are listed in Table 1-16 and Table 1-17.

The following topics discuss the procedure to add new user or group attributes for provisioning:

- Adding New Attributes for Provisioning
- Creating Entries in Lookup Definitions for Provisioning
- Creating a Task to Enable Update Operations
- Replicating Form Designer Changes to a New UI Form

4.2.1 Adding New Attributes for Provisioning

You add a new attribute on the process form in the Form Designer section of Oracle Identity Manager Design Console.

> **Note:**
>
> If you have already added an attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open one of the following the process form.
   - For Users: **UD_O365_USR**
   - For Groups: **UD_O365_GRP**
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the attribute.

   For example, if you are adding the TELEPHONENUMBER field, enter `UD_TELEPHONENUMBER` in the Name field, and then enter the rest of the details of this field.
6. Click the Save icon, and then click **Make Version Active**.

   The following screenshot shows the new field added to the process form:

Figure 4-5 New Field Added to the Process Form

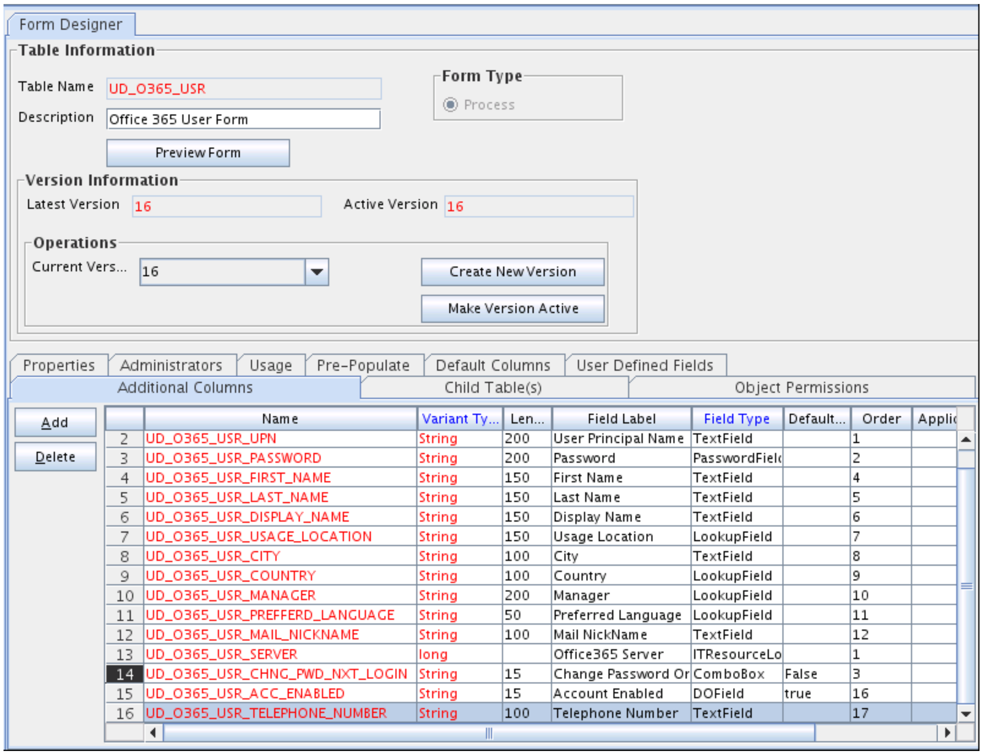


Table Name: UD_O365_USR

Description: Office 365 User Form

Latest Version: 16

Active Version: 16

Current Vers...: 16

	Name	Variant Ty...	Len...	Field Label	Field Type	Default...	Order	Applic
2	UD_O365_USR_UPN	String	200	User Principal Name	TextField		1	
3	UD_O365_USR_PASSWORD	String	200	Password	PasswordFiel		2	
4	UD_O365_USR_FIRST_NAME	String	150	First Name	TextField		4	
5	UD_O365_USR_LAST_NAME	String	150	Last Name	TextField		5	
6	UD_O365_USR_DISPLAY_NAME	String	150	Display Name	TextField		6	
7	UD_O365_USR_USAGE_LOCATION	String	150	Usage Location	LookupField		7	
8	UD_O365_USR_CITY	String	100	City	TextField		8	
9	UD_O365_USR_COUNTRY	String	100	Country	LookupField		9	
10	UD_O365_USR_MANAGER	String	200	Manager	LookupField		10	
11	UD_O365_USR_PREFFERD_LANGUAGE	String	50	Preferred Language	LookupField		11	
12	UD_O365_USR_MAIL_NICKNAME	String	100	Mail NickName	TextField		12	
13	UD_O365_USR_SERVER	long		Office365 Server	ITResourceLo		1	
14	UD_O365_USR_CHNG_PWD_NXT_LOGIN	String	15	Change Password Or	ComboBox	False	3	
15	UD_O365_USR_ACC_ENABLED	String	15	Account Enabled	DOField	true	16	
16	UD_O365_USR_TELEPHONE_NUMBER	String	100	Telephone Number	TextField		17	

4.2.2 Creating Entries in Lookup Definitions for Provisioning

You create an entry for the newly added attribute in the lookup definition that holds attribute mappings for provisioning.

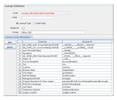
1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open one of the following lookup definitions.
    - For Users: **Lookup.Office365.UM.ProvAttrMap**
    - For Groups: **Lookup.Office365.GM.ProvAttrMap**
4. Click **Add** and then enter the Code Key and Decode values for the attribute.

    Note that the Decode value must be the name of the target system field in the Graph API. Refer to the following Microsoft Developer Network page for the names of target system attributes in the Graph API:

    https://msdn.microsoft.com/en-gb/library/azure/ad/graph/api/entity-and-complex-type-reference#UserEntity

    For example, enter `TELEPHONENUMBER` in the Code Key column and then enter `telephoneNumber` in the Decode column. The following screenshot shows the entry added to the lookup definition:

Figure 4-6 Entry Added to the Lookup Definition



Lookup Definition

Code: Lookup.Office365.UM.ProvAttrMap

Field:

● Lookup Type ○ Field Type

Required: □

Group: Office 365

	Code Key	Decode
1	UD_O365_GP~Group Name[LOOKUP]	__GROUP__~__GROUP__~objectId
2	UD_O365_LIC~License Name[LOOKUP]	__LICENSE__~__LICENSE__~skuId
3	User Principal Name	__NAME__
4	Password	__PASSWORD__
5	UD_O365_URO~Role Name[LOOKUP]	__ROLE__~__ROLE__~objectId
6	Object Id	__UID__
7	Account Enabled	accountEnabled
8	City	city
9	Country	country
10	Display Name	displayName
11	First Name	givenName
12	Mail NickName	mailNickname
13	Manager[LOOKUP]	manager
14	Change Password On Next Logon	passwordProfile.forceChangePasswordNextLogin
15	Preferred Language	preferredLanguage
16	Last Name	surname
17	Telephone Number	telephoneNumber
18	Usage Location	usageLocation

4.2.3 Creating a Task to Enable Update Operations

Create a task to enable updates on the new user or group attribute during provisioning operations.

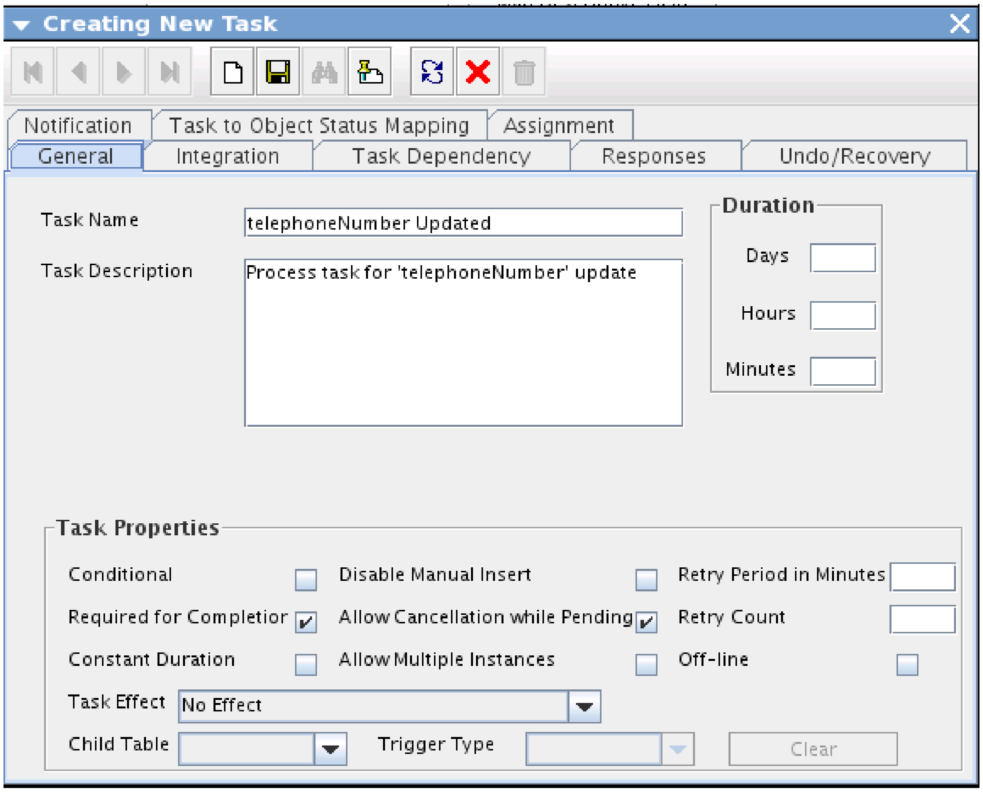
If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of the attribute during provisioning operations, add a process task for updating the new user or group attribute as follows:

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open one of the following process definitions.
   - For Users: **Office365 User**
   - For Groups: **Office365 Group**
3. Click **Add.**
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
   - Conditional
   - Required for Completion
   - Allow Cancellation while Pending
   - Allow Multiple Instances
5. Click the Save icon.

   The following screenshot shows the new task added to the process definition:

Figure 4-7 New task Added to the Process Definition



Task Name: telephoneNumber Updated

Task Description: Process task for 'telephoneNumber' update

Conditional	□	Disable Manual Insert	□	Retry Period in Minutes	
Required for Completior	☑	Allow Cancellation while Pending	☑	Retry Count	
Constant Duration	□	Allow Multiple Instances	□	Off-line	□

Task Effect: No Effect

Child Table:

Trigger Type:

6. In the provisioning process, select the adapter name in the Handler Type section as follows:

   a. Go to the Integration tab, click **Add.**

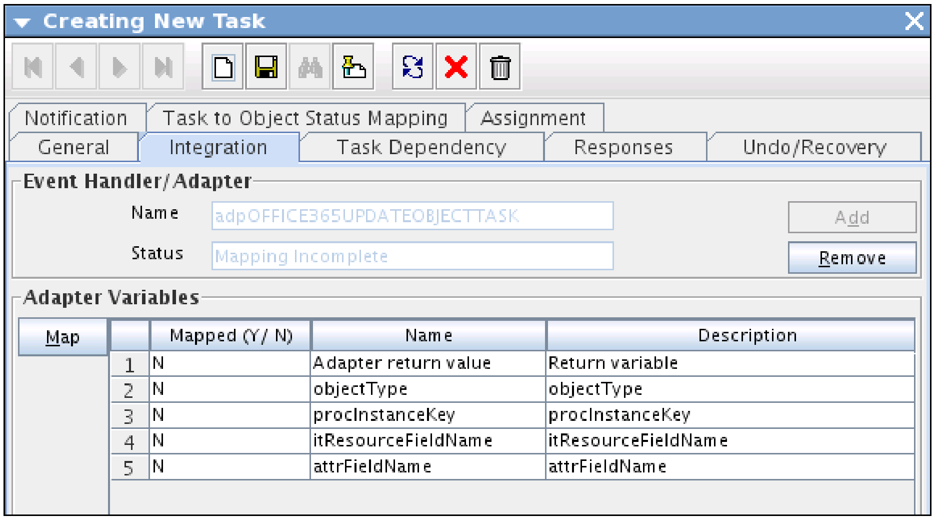
   b. In the Handler Selection dialog box, select **Adapter**.

   c. From the Handler Name column, select **adpOFFICEUPDATEOBJECTTASK.**.

   d. Click Save and close the dialog box.

      The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:

Figure 4-8 List of Adapter Variables



Name: adpOFFICE365UPDATEOBJECTTASK

Status: Mapping Incomplete

	Mapped (Y/ N)	Name	Description
1	N	Adapter return value	Return variable
2	N	objectType	objectType
3	N	procInstanceKey	procInstanceKey
4	N	itResourceFieldName	itResourceFieldName
5	N	attrFieldName	attrFieldName

7. In the Adapter Variables region, click the **ParentFormProcessInstanceKey** variable.

8. In the dialog box that is displayed, create the following mapping:

   - **Variable Name:** ParentFormProcessInstanceKey
   - **Map To:** Process Data
   - **Qualifier:**Process Instance

9. Click Save and close the dialog box.

10. If you are enabling update provisioning operations for a User attribute, then repeat Steps 7 through 9 for the remaining variables listed in the Adapter Variables region.

    The following table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
Adapter Return Value	Response Code	NA	NA
Object Type	Literal	String	User
itResourceFieldName	Literal	String	UD_O365_USR_SERVER
attributeFieldName	Literal	String	telephoneNumber

11. If you are enabling update provisioning operations for a Group attribute, then repeat Steps 7 through 9 for the remaining variables listed in the Adapter Variables region.

    The following table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
ParentFormProcessInstanceKey	Process Data	Process Instance	NA

Variable	Map To	Qualifier	Literal Value
Adapter Return Value	Response Code	NA	NA
Object Type	Literal	String	User
itResourceFieldName	Literal	String	UD_O365_GRP_SERVER
attributeFieldName	Literal	String	*NAME_OF_THE_NEW_GROUP_ATTRIBUTE*

12. On the Responses tab, click Add to add at least the SUCCESS response code, with Status C. This ensures that if the task is successfully run, then the status of the task is displayed as `Completed`.
13. Click the Save icon and close the dialog box, and then save the process definition.

4.2.4 Replicating Form Designer Changes to a New UI Form

You must replicate all changes made to the Form Designer of the Design Console in a new UI form.

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form, and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

4.3 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements.

For example, you can validate data fetched from the User Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the User Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations. For data that fails the validation check, the following message is displayed or recorded in the log file: Validation failed for attribute *ATTRIBUTE_NAME*.

Note:

This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

   The validation class must implement validate method with the following method signature:

   ```
   boolean validate(HashMap hmUserDetails, HashMap hmEntitlementDetails,
   String field)
   ```

   The following sample validation class checks if the value in the User Name attribute contains the number sign (#):

   ```
   public boolean validate(HashMap hmUserDetails,
   HashMap hmEntitlementDetails, String field) { /*
   *    You must write code to validate attributes. Parent
   *    data values can be fetched by using hmUserDetails.get(field)
   *    For child data values, loop through the
   *    ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
   *    Depending on the outcome of the validation operation,
   *    the code must return true or false.
   */
   /*
   *    In this sample code, the value "false" is returned if the field
   *    contains the number sign (#). Otherwise, the value "true" is
   *    returned.
   */
                  boolean valid=true;
                     String sUserName=(String) hmUserDetails.get(field);
   for(int i=0;i<sUserName.length();i++){
   if (sUserName.charAt(i) == '#'){ valid=false;
   break;}
                 }
            return valid;
                    }
   ```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file to Oracle Identity Manager database.

   Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

> **Note:**
>
> Before you use this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

- For Microsoft Windows: *OIM_HOME*/server/bin/UploadJars.bat
- For UNIX: *OIM_HOME*/server/bin/UploadJars.sh

When you run the 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 1 as the value of the JAR type.

4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.Office365.UM.ReconValidation** .
   c. Save the changes to the lookup definition.
   d. Search for and open the **Lookup.Office365.UM.Configuration** lookup definition.
   e. In the Code Key column, enter `Recon Validation Lookup`. In the Decode column, enter `Lookup.Office365.UM.ReconValidation`.
   f. Save the changes to the lookup definition.
5. Add an entry in the Lookup.Office365.UM.Configuration lookup definition to enable transformation as follows:
   a. Expand Administration, and then double-click **Lookup Definition**.
   b. Search for and open the **Lookup.Office365.UM.Configuration** lookup definition.
   c. In the Code Key column, enter `Recon Transformation Lookup`. In the Decode column, enter `Lookup.Office365.UM.ReconTransformation`.
   d. Save the changes to the lookup definition.

4.4 Configuring Transformation of Data During User Reconciliation

You can configure transformation of reconciled single-valued account data according to your requirements.

For example, you can use User Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

Note:

This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure transformation of single-valued account data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class.

   The transformation class must implement the transform method with the following method signature:

   ```
   Object transform(HashMap hmUserDetails, HashMap hmEntitlementDetails,
   String sField)
   ```

   The following sample transformation class creates a value for the Full Name attribute by using values fetched from the User Name and Last Name attributes of the target system:

   ```
   package oracle.iam.connectors.common.transform;
   import java.util.HashMap;
   public class TransformAttribute {
   /*
   Description:Abstract method for transforming the attributes
   param hmUserDetails< String,Object>
   HashMap containing parent data details
   param hmEntitlementDetails < String,Object>
   HashMap containing child data details
   */
   public Object transform(HashMap hmUserDetails, HashMap
   hmEntitlementDetails,String sField) {
   /*
   *    You must write code to transform the attributes. Parent data
   attribute values can be fetched by using hmUserDetails.get("Field
   Name").
   *To fetch child data values, loop through the
   *    ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
   *    Return the transformed attribute.
   */
   String sUserName= (String)hmUserDetails.get("User Name"); String
   sLastName= (String)hmUserDetails.get("Last Name"); String
   sFullName=sUserName+"."+sLastName;
   return sFullName;
   }
   }
   ```

2. Create a JAR file to hold the Java class.

3. Copy the JAR file to Oracle Identity Manager database.

   Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

> **Note:**
>
> Before you use this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

- For Microsoft Windows: OIM_HOME/server/bin/UploadJars.bat
- For UNIX: OIM_HOME/server/bin/UploadJars.sh

When you run the 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 1 as the value of the JAR type.

4. If you created the Java class for transforming a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.Office365.UM.ReconTransformation**.
   c. In the Code Key column, enter the resource object field name on which you want to apply transformation. For example, User Name. In the Decode column, enter the name of the class that implements the transformation logic. For example, oracle.iam.connectors.common.transform.TransformAttribute.
   d. Save the changes to the lookup definition.
5. Add an entry in the **Lookup.Office365.UM.Configuration** lookup definition to enable transformation as follows:
   a. Expand Administration, and then double-click **Lookup Definition**.
   b. Search for and open the **Lookup.Office365.UM.Configuration** lookup definition.
   c. In the Code Key column, enter Recon Transformation Lookup. In the Decode column, enter Lookup.Office365.UM.ReconTransformation.
   d. Save the changes to the lookup definition.

4.5 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector 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. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must create copies of the connector. See Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4.6 About Defining the Connector

Defining a connector is equivalent to registering the connector with Oracle Identity Manager. By using Oracle Identity Manager Administrative and User Console, you can define a customized or reconfigured connector.

A connector is automatically defined when you install it using the Install Connectors feature or when you upgrade it using the Upgrade Connectors feature. You must manually define a connector if:

- You import the connector by using the Deployment Manager.
- You customize or reconfigure the connector.
- You upgrade Oracle Identity Manager.

The following events take place when you define a connector:

- A record representing the connector is created in the Oracle Identity Manager database. If this record already exists, then it is updated.
- The status of the newly defined connector is set to Active. In addition, the status of a previously installed release of the same connector automatically is set to Inactive.

See Defining Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

5 Known Issues and Workarounds for the Office 365 Connector

There are no known issues associated with this release of the connector.

A

Files and Directories on the Office 365 Connector Installation Media

These are the components of the connector installation media that comprise the connector.

Table A-1   Files and Directories on the Office 365 Connector Installation Media

File in the Installation Media Directory	Description
bundle/ org.identityconnectors.genericrest-1.0.1115.jar	This JAR is the ICF connector bundle.
configuration/Office365-CI.xml	This XML file contains configuration information that is used 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 the Oracle Identity Manager database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages.
xml/Office365-ConnectorConfig.xml	This XML file contains definitions for the following connector objects: • IT resource definition • Process forms • Process tasks and adapters • Lookup definitions • Resource objects • Process definition • Scheduled tasks • Reconciliation rules

Index