Oracle® Identity Governance

Configuring the Oracle Internet Directory Application

12c (12.2.1.3.0)

F12373-09

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

F12373-09

Primary Author: Maya Chakrapani

Contributors: Balaji Koutharapu

Contents

Preface

What's New In This Guide?

1 About the Oracle Internet Directory Connector

2 Creating an Application By Using the Oracle Internet Directory Connector

3 Configuring the Oracle Internet Directory Connector for OID

4 Configuring the Oracle Internet Directory Connector for OUD, ODSEE, and LDAPv3-Compliant Directory Server

7 Extending the Functionality of the Oracle Internet Directory Connector

8 Upgrading the Oracle Internet Directory Connector

9 Troubleshooting

List of Figures

List of Tables

Preface

This guide describes the Oracle Internet Directory (OID) connector that is used to onboard applications pertaining to LDAP directory servers such as Oracle Internet Directory (OID), Oracle Unified Directory (OUD), and Oracle Directory Server Enterprise Edition (ODSEE) to Oracle Identity Governance.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

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

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

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

http://docs.oracle.com/cd/E22999_01/index.htm

Conventions

The following text conventions are used in this document:

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

What's New In This Guide?

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

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

- Software Updates

  These include updates made to the connector software.
- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

From this release onward, the connector bundle includes application onboarding templates required for performing connector operations on Oracle Internet Directory, Oracle Unified Directory, Oracle Directory Server Enterprise Edition, and any LDAPv3-compliant directory server. This helps in quicker onboarding of the applications for these targets into Oracle Identity Governance by using an intuitive UI.

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following documentation-specific update has been made in revision “8” of this guide:

The “Target Systems” row of Table 1-1 has been updated to include support for NetIQ eDirectory 8.7.3 and 8.8 and 9.2.

The following documentation-specific update has been made in revision “7” of this guide:

The “Target Systems” row of Table 1-1 has been updated to include support for Oracle Unified Directory 12c release (12.2.1.4.0) in both AOB Application and CI-Based Connector.

The following documentation-specific update has been made in revision “4” of this guide:

Information about Oracle Identity Manager versions prior to 11*g* Release 2 PS3 (11.1.2.3.0) has been removed from the guide.

The following documentation-specific update has been made in revision “3” of this guide:

A Note regarding the modifyTimeStamp attribute has been added to Performing Full and Incremental Reconciliation.

The following documentation-specific updates have been made in revision “2” of this guide:

- The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance release 12*c* PS4 (12.2.1.4.0).
- The “Target Systems” row of Table 1-1 has been updated to include support for Oracle Unified Directory 12c release (12.2.1.3.0) in both AOB Application and CI-Based Connector.
- Several broken links have been fixed throughout the document.

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

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

1 About the Oracle Internet Directory Connector

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

The OID connector lets you onboard LDAP directory server applications in Oracle Identity Governance. The various LDAP directory servers that this connector supports are Oracle Internet Directory (OID), Oracle Unified Directory (OUD), and Oracle Directory Server Enterprise Edition (ODSEE).

The connector uses the LDAPv3 protocol, so you can also use the connector for any LDAPv3-compliant directory server such as Open LDAP.

> **Note:**
>
> In this guide, the connector that is deployed using the **Applications** option on the **Manage** tab of Identity Self Service is referred to as an **AOB application**. The connector that is deployed using the **Manage Connector** option in Oracle Identity System Administration is referred to as a **CI-based connector** (Connector Installer-based connector).

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

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

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

- Certified Components
- Usage Recommendation
- Certified Languages
- Supported Connector Operations
- Connector Architecture
- Supported Connector Features Matrix
- Connector Features

Note:

At some places in this guide, ODSEE, OID, OUD, and an LDAPv3-compliant directory server are referred to as the **target system**.

1.1 Certified Components

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

Table 1-1 Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) **Note:** If you are using Oracle Identity Governance 12c (12.2.1.3.0), then ensure to download and apply patches 26616250 and 25323654 from My Oracle Support.	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0)

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Target systems	The target system can be any one of the following: • Oracle Unified Directory 11*g* release (11.1.1.5.0, 11.1.2.0.0, 11.1.2.2.0, and 11.1.2.3.0) and 12c release (12.2.1.3.0 and 12.2.1.4.0) • Oracle Internet Directory release 9.*x,* 10.1.4.*x*,11*g* release 1 (11.1.1.5.0, 11.1.1.6.0, 11.1.1.7.0 and 11.1.1.9.0), and *12c* release (12.2.1.3.0, 12.2.1.4.0) • Oracle Directory Server Enterprise Edition 11*g* release 1 (11.1.1.5.0 and 11.1.1.7.2) • An LDAPv3-compliant directory server	The target system can be any one of the following: • Oracle Unified Directory 11*g* release (11.1.1.5.0, 11.1.2.0.0, 11.1.2.2.0, and 11.1.2.3.0) and 12c release (12.2.1.3.0 and 12.2.1.4.0) • Oracle Internet Directory release 9.*x,* 10.1.4.*x*,11*g* release 1 (11.1.1.5.0, 11.1.1.6.0, 11.1.1.7.0 and 11.1.1.9.0), and 12*c* release (12.2.1.3.0, 12.2.1.4.0) • Oracle Directory Server Enterprise Edition 11*g* release 1 (11.1.1.5.0 and 11.1.1.7.2) • An LDAPv3-compliant directory server • NetIQ eDirectory 8.7.3, 8.8 • NetIQ eDirectory 9.2 **Note:** Currently certified with OID11.1.1.6.0L patch 31366708 only • Oracle Virtual Directory 10*g* and 11*g* release 1 (11.1.1.5.0) • Sun Java System Directory Server Enterprise Edition 6.3 and 7.0 • Sun ONE Directory Server 5.2
Connector Server	11.1.2.1.0	11.1.2.1.0
Connector Server JDK and JRE	JDK or JRE 1.6 and above	JDK or JRE 1.6 and above

1.2 Usage Recommendation

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

> **Note:**
>
> If you are using Oracle Identity Manager release 11.1.*x*, then you can install and use the connector only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0.

- If you are using Oracle Identity Governance 12c (12.2.1.3.0) and want to integrate it with any of the following target systems, then use the latest 12.2.1.*x* version of this connector and deploy it using the **Applications** option on the **Manage** tab of Identity Self Service:
  - Oracle Internet Directory release 9.*x*, 10.1.4.*x*, 11g release 1 (11.1.1.5.0, 11.1.1.6.0, 11.1.1.7.0 and 11.1.1.9.0), and 12c release (12.2.1.3.0, 12.2.1.4.0)
  - Oracle Unified Directory 11g release (11.1.1.5.0, 11.1.2.0.0, 11.1.2.2.0, and 11.1.2.3.0), and 12c release (12.2.1.3.0, 12.2.1.4.0)
  - Oracle Directory Server Enterprise Edition 11g release 1 (11.1.1.5.0 and 11.1.1.7.2)
  - An LDAPv3-compliant directory server
- If you are using Oracle Identity Governance 12c (12.2.1.3.0) and want to integrate it with any of the following target systems, then use the latest 12.2.1.*x* version of this connector and deploy it using the **Manage Connector** option in Oracle Identity System Administration:
  - Oracle Virtual Directory 10g and 11g release 1 (11.1.1.5.0)
  - Novell eDirectory 8.7.3 and 8.8
  - Sun Java System Directory Server Enterprise Edition 6.3 and 7.0
  - Sun ONE Directory Server 5.2
- If you are using any of the Oracle Identity Manager 11.1.*x* releases listed in the “Requirement for CI-Based Connector” column of Table 1-1, then use the 11.1.*x* version of the OID connector. If you want to use the 12.2.1.*x* version of this connector with Oracle Identity Manager 11.1.*x* releases, then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0.

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

- If you are using an Oracle Identity Manager release that is earlier than Oracle Identity Manager 11g Release 1 (11.1.1), then depending on the target system that you are using, install and use one of the following connectors:
  - For Oracle Internet Directory, use the 9.0.4.*x* version of the Oracle Internet Directory connector.
  - For Sun ONE Directory Server and Sun Java System Directory Server Enterprise Edition, use the 9.0.4.*x* version of the Sun Java System Directory connector.
  - For Novell eDirectory, use the 9.0.4.*x* version of the Novell eDirectory connector.

1.3 Certified Languages

These are the languages that the connector supports.

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

- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.4 Supported Connector Operations

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

Table 1-2 Supported Connector Operations

Operation	Supported for OID?	Supported for OUD?	Supported for ODSEE?	Supported for LDAPv3-compliant directory server?	Supported for Novell eDirectory?
User Management					
Create user	Yes	Yes	Yes	Yes	Yes
Update user	Yes	Yes	Yes	Yes	Yes
Delete User	Yes	Yes	Yes	Yes	Yes
Enable user	Yes	Yes	Yes	Yes	Yes
Disable user	Yes	Yes	Yes	Yes	Yes
Reset password	Yes	Yes	Yes	Yes	No
Groups and Organization Units Management					
Create group or organization unit	Yes	Yes	Yes	Yes	Yes
Update group name or organization unit name	Yes	Yes	Yes	Yes	Yes
Delete group or organization unit	Yes	Yes	Yes	Yes	Yes
Update container DN	Yes	Yes	Yes	Yes	Yes
Roles Management					
Create role	Yes	No	Yes	Yes, if your target system supports creation of roles	Yes
Update role name	Yes	No	Yes	Yes	Yes
Delete role	Yes	No	Yes	Yes	Yes

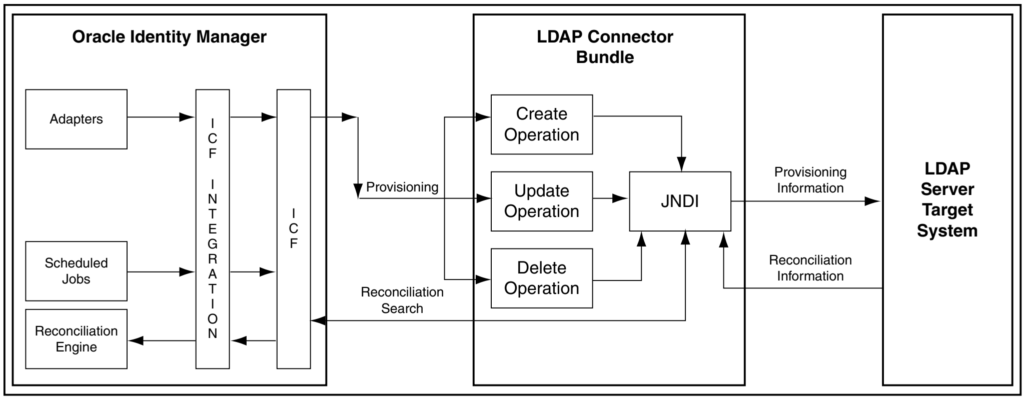
Table 1-2 (Cont.) Supported Connector Operations

Operation	Supported for OID?	Supported for OUD?	Supported for ODSEE?	Supported for LDAPv3-compliant directory server?	Supported for Novell eDirectory?
Update container DN	Yes	No	Yes	Yes	Yes
Entitlement Grant Management					
Add groups	Yes	Yes	Yes	Not applicable	Yes
Revoke groups	Yes	Yes	Yes	Not applicable	Yes
Add roles	No	No	Yes	Not applicable	Yes
Revoke Roles	No	No	Yes	Not applicable	Yes
Add organizations	No	No	No	Not applicable	Yes
Remove organizations	No	No	No	Not applicable	Yes
Add domain scope	Not applicable	Not applicable	Not applicable	Not applicable	Yes
Add profiles	Not applicable	Not applicable	Not applicable	Not applicable	Yes
Add role containers	Not applicable	Not applicable	Not applicable	Not applicable	Yes

1.5 Connector Architecture

The Oracle Internet Directory connector is implemented by using the Identity Connector Framework (ICF). The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Governance connectors. The ICF is shipped along with Oracle Identity Governance. Therefore, you need not configure or modify the ICF.

Figure 1-1 Connector Architecture



The OID connector uses JNDI to access the target system.

This connector can be configured to run in one of the following modes:

- Identity reconciliation

  Identity reconciliation is also known as authoritative or trusted source reconciliation. In this form of reconciliation, OIG Users are created or updated corresponding to the creation of and updates to users on the target system. Note that the identity reconciliation mode supports reconciliation of user objects only.

  See Reconciliation Scheduled Jobs for Groups and Organizational Units Management in OID for information about the LDAP Connector Trusted User Reconciliation scheduled job that is used in this mode.

- Account Management

  Account management is also known as target resource management. This mode of the connector enables the following operations:

  - Provisioning

    Provisioning involves creating, updating, or deleting users, groups, roles, and organizational units (OUs) on the target system through Oracle Identity Governance.

    When you allocate (or provision) a target system resource to an OIG User, the operation results in the creation of an account on the target system for that user. In the Oracle Identity Governance context, the term "provisioning" is also used to mean updates (for example enabling or disabling) made to the target system account through Oracle Identity Governance.

    Users and organizations are organized in hierarchical format on the target system. Before you can provision users to (that is, create users in) the required organizational units (OUs) on the target system, you must fetch into Oracle Identity Governance the list of OUs used on the target system. This is achieved by using the LDAP Connector OU Lookup Reconciliation scheduled job for lookup synchronization.

    Similarly, before you can provision users to the required groups or roles on the target system, you must fetch into Oracle Identity Governance the list of all groups and roles used on the target system. This is achieved by using the LDAP Connector Group Lookup Reconciliation and LDAP Connector Role Lookup Recon scheduled jobs for lookup synchronization.

  - Target resource reconciliation

    To perform target resource reconciliation, the LDAP Connector User Search Reconciliation or LDAP Connector User Sync Reconciliation scheduled jobs is used. The connector applies filters to locate users to be reconciled from the target system and then fetches the attribute values of these users.

    Depending on the data that you want to reconcile, you use different scheduled jobs. For example, you use the LDAP Connector User Search Reconciliation scheduled job to reconcile user data in the target resource mode. See Reconciliation Scheduled Jobs for Groups and Organizational Units Management in OID for more information about scheduled jobs used in this mode.

1.6 Supported Connector Features Matrix

Provides the list of features supported by the AOB application and CI-based connector.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Full reconciliation	Yes	Yes
Incremental reconciliation	Yes	Yes
Limited reconciliation	Yes	Yes
Connection pooling	Yes	Yes
Use connector server	Yes	Yes
Transformation and validation of account data	Yes	Yes
Compatibility with high-availability target system environments	Yes	Yes
SSL communication between the target system and Oracle Identity Governance	Yes	Yes
Reconcile deleted user records	Yes	Yes
Reconcile deleted groups, roles, and organizations	Yes	Yes
Test connection	Yes	No

1.7 Connector Features

The features of the connector include support for connector server, support for high-availability configuration of the target system, connection pooling, reconciliation of deleted user records, support for groovy scripts, and so on.

The following are the features of the connector:

- Full and Incremental Reconciliation
- Limited Reconciliation
- Support for the Connector Server
- Transformation and Validation of Account Data
- Support for High-Availability Configuration of the Target System
- Reconciliation of Deleted User Records
- Reconciliation of Deleted Groups, Roles, and Organizations
- Connection Pooling
- Support for Running Pre and Post Action Scripts
- Secure Communication to the Target System
- Support for Cloning Applications and Creating Instance Applications

1.7.1 Full and Incremental Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Governance. In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance.

After you create the application, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Governance. After the first full reconciliation run, incremental reconciliation is automatically enabled. In incremental reconciliation, user accounts that have been added or modified since the last reconciliation run are fetched into Oracle Identity Governance.

After you create the application, you can first perform full reconciliation. After the first full reconciliation run, incremental reconciliation is automatically enabled.

For more information, see Performing Full and Incremental Reconciliation.

1.7.2 Limited Reconciliation

You can set a reconciliation filter as the value of the Filter attribute of a reconciliation scheduled job. This filter specifies the subset of added and modified target system records that must be reconciled.

For more information, see Performing Limited Reconciliation.

1.7.3 Support for the Connector Server

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

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

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

1.7.4 Transformation and Validation of Account Data

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

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

1.7.5 Support for High-Availability Configuration of the Target System

You can configure the connector for compatibility with high-availability target system environments.

The connector can read information about backup target system hosts from the failover parameter of the Basic Configuration section and apply this information when it is unable to connect to the primary host.

For more information about the Failover parameter, see Basic Configuration Parameters for OID or Basic Configuration Parameters for OUD, ODSEE, and LDAPv3-Compliant Directory Server.

1.7.6 Reconciliation of Deleted User Records

You can use the connector to reconcile user records that are deleted on the target system into Oracle Identity Governance.

For more information about the reconciliation job used for reconciling these deleted records, see one of the following sections:

- For OID: Reconciliation Jobs for OID
- For OUD, ODSEE, or an LDAPv3-compliant directory server: Reconciliation Jobs for OUD, ODSEE, and LDAPv3-Compliant Directory Server

1.7.7 Reconciliation of Deleted Groups, Roles, and Organizations

You can use the connector to reconcile groups, roles, and organizations that are deleted on the target system into Oracle Identity Governance.

For more information about the reconciliation job used for reconciling these deleted records, see one of the following sections:

- For OID: Scheduled Jobs for Reconciliation of Deleted Groups and OUs in OID
- For OUD, ODSEE, or an LDAPv3-compliant directory server: Scheduled Jobs for Reconciliation of Deleted Groups, OUs, and Roles in OUD, ODSEE, and LDAPv3-Compliant Directory Server

1.7.8 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Governance connectors can use these connections to communicate with target systems.

At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each set of basic configuration parameters that you provide while creating an application. For example, if you have three applications for three installations of the target system, then three connection pools will be created, one for each target system installation.

For more information about the parameters that you can configure for connection pooling, see:

- For OID: Advanced Settings Parameters for OID
- For OUD, ODSEE, or an LDAPv3-compliant directory server: Advanced Settings Parameters for OUD, ODSEE, and LDAPv3-Compliant Directory Server

1.7.9 Support for Running Pre and Post Action Scripts

You can run pre and post action scripts on a computer where the connector is deployed. These scripts can be of type SQL/StoredProc/Groovy. You can configure the scripts to run before or after the create, update, or delete an account provisioning operations.

For more information, see Updating the Provisioning Configuration in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.7.10 Secure Communication to the Target System

To provide secure communication to the target system, SSL is required. You can configure SSL between Oracle Identity Governance and the Connector Server and between the Connector Server and the target system.

If you do not configure SSL, passwords can be transmitted over the network in clear text. For example, this problem can occur when you are creating a user or modifying a user's password.

For more information, see Configuring SSL for the Connector.

1.7.11 Support for Cloning Applications and Creating Instance Applications

You can configure this connector for multiple installations of the target system by cloning applications or by creating instance applications.

When you clone an application, all the configurations of the base application are copied into the cloned application. When you create an instance application, it shares all configurations as the base application.

For more information about these configurations, see Cloning Applications and Creating Instance Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

2
Creating an Application By Using the Oracle Internet Directory Connector

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

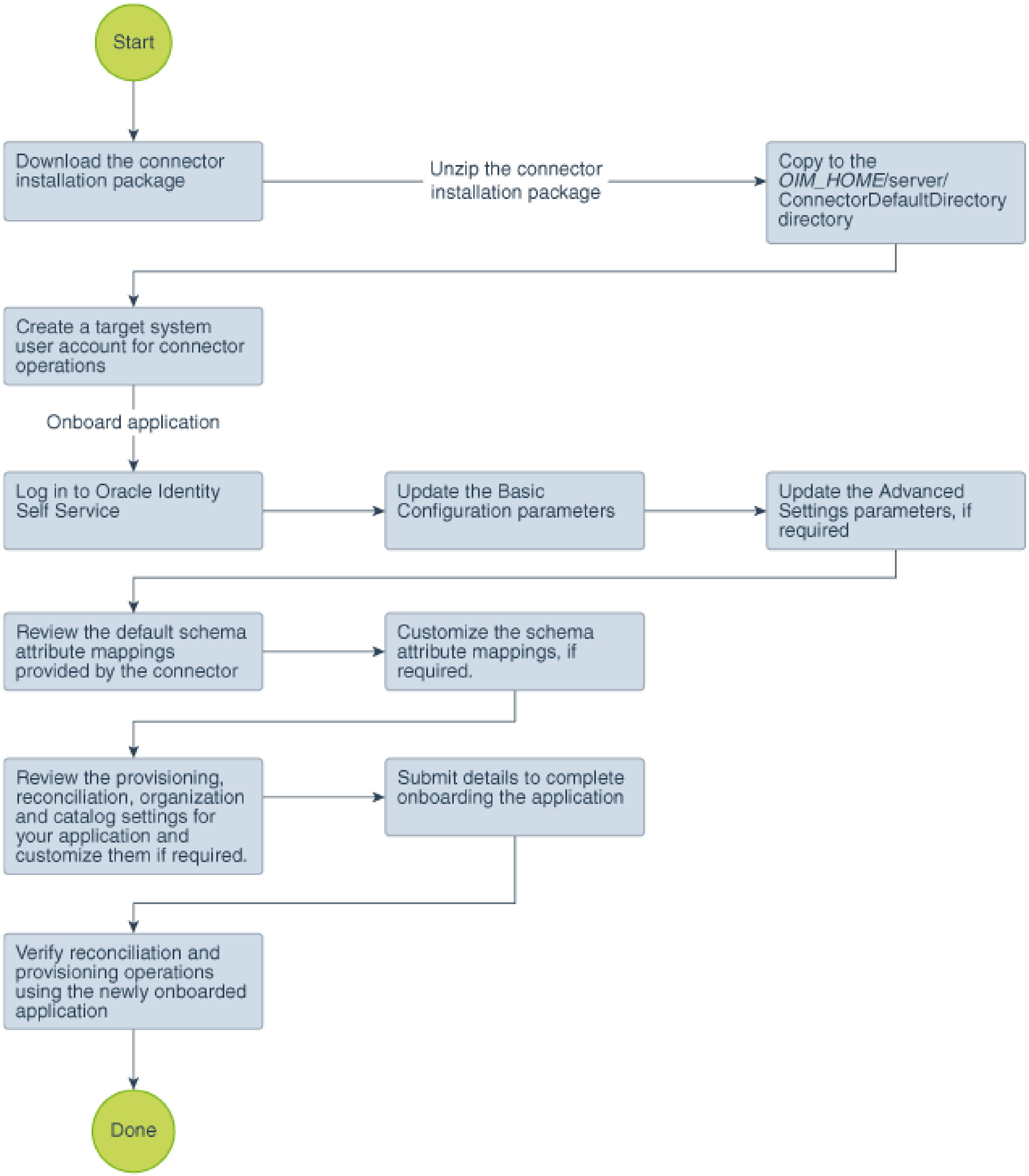
- Process Flow for Creating an Application By Using the Connector
- Prerequisites for Creating an Application By Using the Connector
- Creating an Application By Using the Connector

2.1 Process Flow for Creating an Application By Using the Connector

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

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

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


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

2.2 Prerequisites for Creating an Application By Using the Connector

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

- Downloading the Connector Installation Package
- Creating a Target System User Account for Connector Operations
- Configuring the Connector for LDAP Operation Timeouts

2.2.1 Downloading the Connector Installation Package

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

To download the connector installation package:

1. Navigate to the OTN website at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html.
2. Click **OTN License Agreement** and read the license agreement.
3. Select the **Accept License Agreement** option.

   You must accept the license agreement before you can download the installation package.
4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.*
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

2.2.2 Creating a Target System User Account for Connector Operations

The connector uses a target system account to connect to the target system during reconciliation and provisioning operations.

You must create a target system user account for performing the following functions.

- Create, modify, and delete entries related to the managed objects, including accounts, groups, roles (if supported), and organizational units (ou).
- Update passwords for users.
- Use paging controls that have been configured in the IT resource.

Depending on the target system, create the specific target system account for connector operations as follows:

- Create an admin user account on the ODSEE target system.
- Create an admin user account on the OUD target system.
- Create an admin user, admin group, and ACIs on the OID target system.

To perform this task, you must be an administrator on the OID target system who is familiar with command-line utilities such as `ldapsearch` and `ldapmodify`. If you prefer, you can also use Oracle Directory Services Manager to perform these functions.

The detailed instructions for performing these preinstallation tasks are available in the product documentation of the target system.

2.2.3 Configuring the Connector for LDAP Operation Timeouts

When an LDAP request is made by a client to a server and the server does not respond, the client waits forever for the server to respond until the TCP connection times out. On the client-side, you encounter read timed out exceptions while performing lookup field synchronization such as OID Connector Group Lookup Reconciliation. To avoid encountering such an issue, you must configure read and connect timeouts for your JNDI/LDAP service provider.

> **Note:**
>
> This is an optional procedure and is applicable only if you are using an OID target system.
>
> Perform this procedure if you want to configure timeouts for the LDAP operations.

To do so:

1. In a text editor, open the xml/OID-target-template.xml file located in the connector installation package.
2. In the <advanceConfigurations> section, add new entries for the readTimeout and connectTimeout parameters as follows:

   ```
   <advanceConfig name="readTimeout" value="ENTER_NUM_MILLISECONDS"
   helpText="This property represents an integer value that specifies
   the number of milliseconds after which the LDAP provider must abort
   attempts to read an LDAP operation." dataType="int"
   required="false"/>
   <advanceConfig name="connectTimeout" value="ENTER_NUM_MILLISECONDS"
   helpText="This property represents an integer value that specifies
   the number of milliseconds after which the connection between the
   LDAP server and client times out." dataType="int" required="false"/>
   ```

   In the preceding line, replace ***ENTER_NUM_MILLISECONDS*** with a relevant integer value that specifies the number of milliseconds for the relevant parameters.
3. Save and close the file.
4. Log in to Identity Self Service and create a new application for the newly added parameters to reflect in the Advanced Settings section.

2.3 Creating an Application By Using the Connector

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

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

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

1. Create an application in Identity Self Service. The high-level steps are as follows:
   a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.
   b. Ensure that the **Connector Package** option is selected when creating an application.
   c. Update the basic configuration parameters to include connectivity-related information.
   d. If required, update the advanced setting parameters to update configuration entries related to connector operations.
   e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.
   f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.
   g. Review the details of the application and click **Finish** to submit the application details.

      The application is created in Oracle Identity Governance.
   h. When you are prompted whether you want to create a default request form, click **Yes** or **No**.

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

See Also:

- Configuring the Oracle Internet Directory Connector for OID or Configuring the Oracle Internet Directory Connector for OUD, ODSEE, and LDAPv3-Compliant Directory Server for details on basic configuration and advanced settings parameters, default user account attribute mappings, default correlation rules, and reconciliation jobs that are predefined for this connector
- Configuring Oracle Identity Governance for details on creating a new form and associating it with your application, if you chose not to create the default form

3

Configuring the Oracle Internet Directory Connector for OID

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

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

3.1 Basic Configuration Parameters for OID

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

Table 3-1 Parameters in the Basic Configuration Section for OID

Parameter	Mandatory?	Description
Base Contexts	Yes	Enter the base contexts for operations on the target system. Sample value: `"dc=example,dc=com"` **Note**: In a multilevel base context, each base context must be specified within double quotes (") and separated by a comma (,).
Principal	Yes	Enter the bind DN for performing operations on the target system. Sample value for ODSEE or OUD: `cn=Directory` Manager Sample value for OID: `cn=orcladmin` Sample value for eDirectory: `cn=Admin,dc=idc` **Note:** For eDirectory, the bind DN should be the complete DN name.

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

Parameter	Mandatory?	Description
Password	Yes	Enter the password to connect to the target system. **Note:** This parameter is available only when you are creating a Target application.
credentials	Yes	Enter the credentials to connect to the target system. **Note:** This parameter is available only when you are creating an Authoritative application.
Host	Yes	Enter the host name or IP address of the target system. Sample values: `myhost`, `172.20.55.120`
Port	Yes	Enter the port number to connect to the target system. Default value: `389`
Connector Server Name	No	If you are using this connector with a Connector Server, then enter the name of Connector Server IT resource.
Failover	No	Enter the complete URL of LDAP backup server or servers that the connector must switch to if the primary LDAP server fails or becomes unavailable. The URL is a fully qualified host name or an IP address in the following format: `ldap://host:port` The following example shows an IP address for one backup LDAP server: `ldap://172.20.55.191:389` If you specify more than one URL, each URL must be enclosed in double quotes (") and separated by a comma (,). For example: `"ldap://172.20.55.191:389","ldap://172.20.55.171:387"`

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

Parameter	Mandatory?	Description
SSL	No	Specifies whether communication with the target system must be secured using SSL. Default value: `true` **Note:** You can set the value to true, when SSL is enabled between Oracle Identity Manager and the Connector Server or between Oracle Identity Manager and the target system. Set the `UseSSL` IT Resource parameter for the Connector Server to `true`, as described in Configuring the IT Resource for the Connector Server. To configure SSL, see Configuring the Java Connector Server with SSL for Oracle Identity Governance in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

3.2 Advanced Settings Parameters for OID

Advanced configuration parameters vary depending on whether you are creating a target application or an authoritative application.

- Advanced Settings Parameters for an OID Target Application
- Advanced Settings Parameters for an OID Authoritative Application

3.2.1 Advanced Settings Parameters for an OID Target Application

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

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

Table 3-2 Advanced Settings Parameters for an OID Target Application

Parameter	Mandatory?	Description
Standard Change Log	No	This parameter specifies how the connector accesses the changelog attribute. Default value: `true` **Note:** Do *not* modify this value.
readSchema	No	This parameter specifies whether the schema must be read from the server. Default value: `true`
Connector Package Version	No	This parameter holds the version of the connector. Default value: `12.3.0`
usePagedResultControl	No	This parameter specifies whether simple paged search is preferred over VLV index search when both are available. Default value: `true`
filterwithOrInsteadOfAnd	No	This parameter specifies whether the changelog filter is built using an OR or AND filter. Enter `true` if the changelog filter is built using an OR filter instead of AND filter. Otherwise, enter `false`. An OR filter is in the following the following format: `(|(changeNumber=1)(changeNumber=2) . . .(changeNumber=xxx))` An AND filter is of the following format: `(&(changeNumber>=0)(changeNumber<=xxx))`
disabledValue	No	This parameter specifies the value to use for the attribute defined by the enabledAttribute parameter whenever an account is disabled. Default value: `DISABLED`
enabledWhenNoAttribute	No	This parameter defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the parameter. Default value: `true`

Table 3-2 (Cont.) Advanced Settings Parameters for an OID Target Application

Parameter	Mandatory?	Description
changelogUidAttribute	No	This parameter holds the name of the attribute that contains the unique ID of the modified entry in the changelog. Default value: `orclguid`
attributesToSynchronize	No	This parameter holds the list of attributes that the connector must return whenever a SyncOp is run. Default value: `"cn","uid"`
groupMemberAttribute	No	This parameter holds the LDAP attribute that stores the member for non-POSIX static groups. Default value: `uniqueMember`
enabledValue	No	This parameter specifies the value that the connector must use for the attribute defined by the enabledAttribute parameter whenever an account is enabled. Default value: `ENABLED`
Connector Package Name	Yes	This parameter holds the name of the connector package. Default value: `org.identityconnectors.ldap`
respectResourcePasswordPolicyChangeAfterReset	No	By default, this value is set to `true`. Do not modify the value if the connector throws exceptions (for example, PasswordExpiredException) appropriately when binding check for the Password Expired control and Password Policy control. Otherwise, enter `false`. Default value: `true`
vlvSortAttribute	No	This parameter is used as the sort key for the VLV index. Default value: `uid`
blockSize	No	This parameter holds the block size for simple paged results and VLV index searches. Default value: `100`

Table 3-2 (Cont.) Advanced Settings Parameters for an OID Target Application

Parameter	Mandatory?	Description
Connector Name	Yes	This parameter holds the name of the connector class. Default value: `org.identityconnectors.ldap.LdapConnector` Do *not* modify this parameter.
synchronizeWithModifyTimestamps	No	This parameter specifies whether the connector must use the modify timestamps attribute instead of the changelog attribute during a SyncOp operation. Default value: `false`
enabledAttribute	No	This parameter holds the name of the attribute that is required to enable or disable accounts. Default value: `orclIsEnabled`
objectClassesToSynchronize	No	This parameter holds the object classes to synchronize. The change log is for all objects; this filters updates the listed object classes. You should not list the superclasses of an object class unless you intend to synchronize objects with any of the superclass values. Default value: `"inetOrgPerson","groupOfNames","groupOfUniqueNames","organizationalUnit"`
accountObjectClasses	No	This parameter holds the list of object classes required for a USER object. Default value: `"top","person","organizationalPerson","inetOrgPerson","orclUserV2"`
accountUserNameAttribute	No	This parameter holds attributes that contain the name of a USER object. Default value: `cn`

Table 3-2 (Cont.) Advanced Settings Parameters for an OID Target Application

Parameter	Mandatory?	Description
changelogBaseDn	No	This parameter holds the baseDN where the connector is to find the changelog attribute value. Default value: `cn=changelog`
uidAttribute	No	This parameter holds the LDAP attribute to which the connector must map predefined UID attribute. Default value: `orclguid`
removeLogEntryObjectClassFromFilter	No	This parameter specifies whether the changelog filter contains a condition on the changelog objectclass. Default value: `true`
accountSearchFilter	No	This parameter holds a search filter that any account needs to match in order to be returned. Default value: `objectClass=*`
accountSynchronizationFilter	No	This parameter holds a filter for all the entries that the connector returns during the SyncOp operation that must match. Default value: `objectClass=*`
changeNumberAttribute	No	This parameter holds the attribute name that connector must use for changelog. Default value: `changeNumber`
maintainPosixGroupMembership	No	This parameter specifies whether the connector modifies POSIX group membership of renamed or deleted user entries. Default value: `false`
passwordAttribute	No	This parameter holds the name of the attribute to which the predefined PASSWORD attribute is written to. Default value: `userPassword`
maintainLdapGroupMembership	No	This parameter specifies whether the connector modifies group membership of renamed and deleted user entries. Default value: `true`

Table 3-2 (Cont.) Advanced Settings Parameters for an OID Target Application

Parameter	Mandatory?	Description
changeLogBlockSize	No	This parameter holds the block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation. Default value: `100`
Any Incremental Recon Attribute Type	No	This parameter indicates that the connector accepts any format of token during reconciliation. Default value: `true`
ldapGroupFilterBehavior	No	This parameter specifies the behavior for an LDAP group filter. Default value: `reject`
ldapGroupMembershipAttribute	No	This parameter specifies the value for the LDAP group membership attribute. Default value: `ismemberof`
dateFormat	No	This parameter specifies the format of date data on the target system. Default value: `yyyyMMddHHmmss`
dateTypeAttrNames	No	This parameter specifies the list of target system attributes that the connector must format to match the date format that you specify in the dateFormat parameter. Default value: `"orclActiveStartDate","orclActiveEndDate"`
pwdMaxFailure	No	This parameter indicates the number of consecutive failed bind attempts after which a user account is locked. If the value of this parameter is 0 (zero), then the account is not locked due to failed bind attempts, and the value of the password lockout policy is ignored. Default value: `10`
Pool Max Idle	No	Maximum number of idle objects in a pool. Default value: `10`

Table 3-2 (Cont.) Advanced Settings Parameters for an OID Target Application

Parameter	Mandatory?	Description
Pool Max Size	No	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	No	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`
Pool Min-Evict Idle	No	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	No	Minimum number of idle objects in a pool. Default value: `1`

3.2.2 Advanced Settings Parameters for an OID Authoritative Application

These are the configuration-related entries that the connector uses during reconciliation runs against an authoritative application.

Table 3-3 Advanced Settings Parameters for OID Authoritative Application

Parameter	Mandatory?	Description
changeNumberAttribute	No	This entry holds the attribute name used for changelog. Default value: `changeNumber`
enabledValue	No	This entry specifies the value to use for the attribute defined by the enabledAttribute parameter whenever an account is enabled. Default value: `ENABLED`
disabledValue	No	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is disabled. Default value: `DISABLED`
Bundle Name	Yes	This entry holds the name of the connector bundle package. Default value: `org.identityconnectors.ldap`

Table 3-3 (Cont.) Advanced Settings Parameters for OID Authoritative Application

Parameter	Mandatory?	Description
enabledWhenNoAttribute	No	This entry defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the entry. Default value: `true`
Connector Name	No	This entry holds the name of the connector class. Do not modify this entry. Default value: `org.identityconnectors.ldap.LdapConnector`
objectClassesToSynchronize	No	This entry holds the list of object classes that the connector must synchronize. Any synchronized entry in order to be returned must have at least one object class from this list. If this list of object classes is empty or the value is missing, then the connector does not perform filtering on the object classes. Default value: `"inetOrgPerson","groupOfNames","groupOfUniqueNames","organizationalUnit"`
Bundle Version	No	This entry holds the version of the connector bundle class. Default value: `12.3.0`
uidAttribute	No	This entry holds the LDAP attribute to which the predefined UID attribute must be mapped to. Default value: `orclguid`
enabledAttribute	No	This entry holds the name of the attribute that is required to enable or disable accounts. Default value: `orclIsEnabled`
changeLogBlockSize	No	This entry holds the block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation. Default value: `100`
accountObjectClasses	No	This entry holds the list of object classes required for a USER object. Default value: `"top","person","organizationalPerson","inetOrgPerson","orclUserV2"`

Table 3-3 (Cont.) Advanced Settings Parameters for OID Authoritative Application

Parameter	Mandatory?	Description
usePagedResultControl	No	This entry specifies whether simple paged search is preferred over VLV index search when both are available. Default value: `true`
Any Incremental Recon Attribute Type	No	This parameter indicates that the connector accepts any format of token during reconciliation. Default value: `true`
pwdMaxFailure	No	Indicates the number of consecutive failed bind attempts after which the connector locks a user account. If the value of this parameter is 0 (zero), then the account is not locked due to failed bind attempts, and the connector ignores the value of the password lockout policy. Default value: `10`
Pool Max Idle	No	Maximum number of idle objects in a pool. Default value: 10
Pool Max Size	No	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	No	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`
Pool Min-Evict Idle	No	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	No	Minimum number of idle objects in a pool. Default value: `1`

3.3 Attribute Mappings for OID

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

- Attribute Mappings for an OID Target Application
- Attribute Mappings for an OID Authoritative Application

3.3.1 Attribute Mappings for an OID Target Application

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

Default Attributes for an OID Target Application

Table 3-4 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and OID Target application attributes. The table also lists whether a specific attribute is used during provisioning or reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

Table 3-4 Default Attributes for an OID Target Application

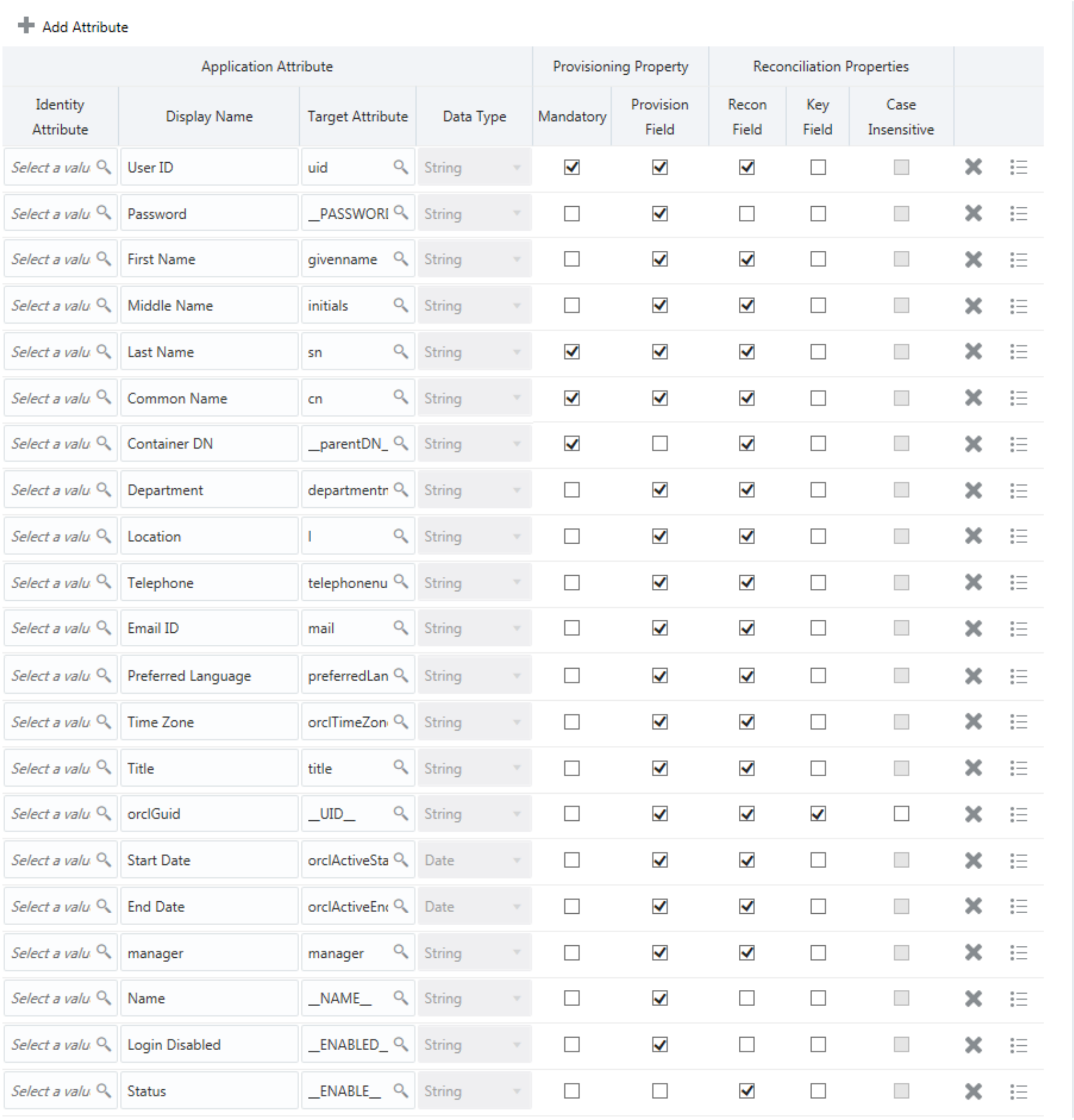
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User ID	uid	String	Yes	Yes	Yes	No	Not applicable
First Name	givenname	String	No	Yes	Yes	No	Not applicable
Middle Name	initials	String	No	Yes	Yes	No	Not applicable
Last Name	sn	String	Yes	Yes	Yes	No	Not applicable
Common Name	cn	String	Yes	Yes	Yes	No	Not applicable
Container DN	__parentDN__	String	Yes	No	Yes	No	Not applicable
Department	departmentnumber	String	No	Yes	Yes	No	Not applicable
Location	l	String	No	Yes	Yes	No	Not applicable
Telephone	telephonenumber	String	No	Yes	Yes	No	Not applicable
Email ID	mail	String	No	Yes	Yes	No	Not applicable
Preferred Language	preferredLanguage	String	No	Yes	Yes	No	Not applicable
Time Zone	orclTimeZone	String	No	Yes	Yes	No	Not applicable
Title	title	String	No	Yes	Yes	No	Not applicable

Table 3-4 (Cont.) Default Attributes for an OID Target Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
orclGuid	__UID__	String	No	Yes	Yes	Yes	No
Start Date	orclActiveStartDate	String	No	Yes	Yes	No	Not applicable
End Date	orclActiveEndDate	String	No	Yes	Yes	No	Not applicable
manager	manager	String	No	Yes	Yes	No	Not applicable
Status	__ENABLE__	String	No	No	Yes	No	Not applicable
Name	__NAME__	String	No	Yes	No	No	Not applicable
Login Disabled	__ENABLED__	String	No	Yes	No	No	Not applicable
Password	__PASSWORD__	String	No	Yes	No	No	Not applicable

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

Figure 3-1 Default Attribute Mappings for an OID User Account



Application Attribute				Provisioning Property		Reconciliation Properties				
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive		
Select a valu	User ID	uid	String	☑	☑	☑	☐	☐	✖	☰
Select a valu	Password	__PASSWORI	String	☐	☑	☐	☐	☐	✖	☰
Select a valu	First Name	givenname	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	Middle Name	initials	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	Last Name	sn	String	☑	☑	☑	☐	☐	✖	☰
Select a valu	Common Name	cn	String	☑	☑	☑	☐	☐	✖	☰
Select a valu	Container DN	__parentDN_	String	☑	☐	☑	☐	☐	✖	☰
Select a valu	Department	departmentr	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	Location	l	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	Telephone	telephonenu	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	Email ID	mail	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	Preferred Language	preferredLan	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	Time Zone	orclTimeZon	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	Title	title	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	orclGuid	__UID__	String	☐	☑	☑	☑	☐	✖	☰
Select a valu	Start Date	orclActiveSta	Date	☐	☑	☑	☐	☐	✖	☰
Select a valu	End Date	orclActiveEn	Date	☐	☑	☑	☐	☐	✖	☰
Select a valu	manager	manager	String	☐	☑	☑	☐	☐	✖	☰
Select a valu	Name	__NAME__	String	☐	☑	☐	☐	☐	✖	☰
Select a valu	Login Disabled	__ENABLED_	String	☐	☑	☐	☐	☐	✖	☰
Select a valu	Status	__ENABLE__	String	☐	☐	☑	☐	☐	✖	☰

Groups Entitlement

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

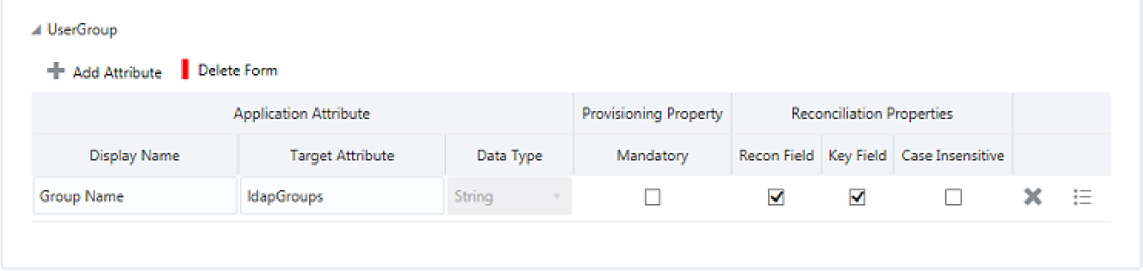
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5   Default Attribute Mappings for Groups Forms

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

Figure 3-2 shows the default attribute groups mapping.

Figure 3-2   Default Attribute Mappings for Groups



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

3.3.2 Attribute Mappings for an OID Authoritative Application

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

Table 3-6 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and OID Authoritative application attributes. The table also lists the data type for a given attribute and specified whether it is a mandatory attribute for reconciliation.

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

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

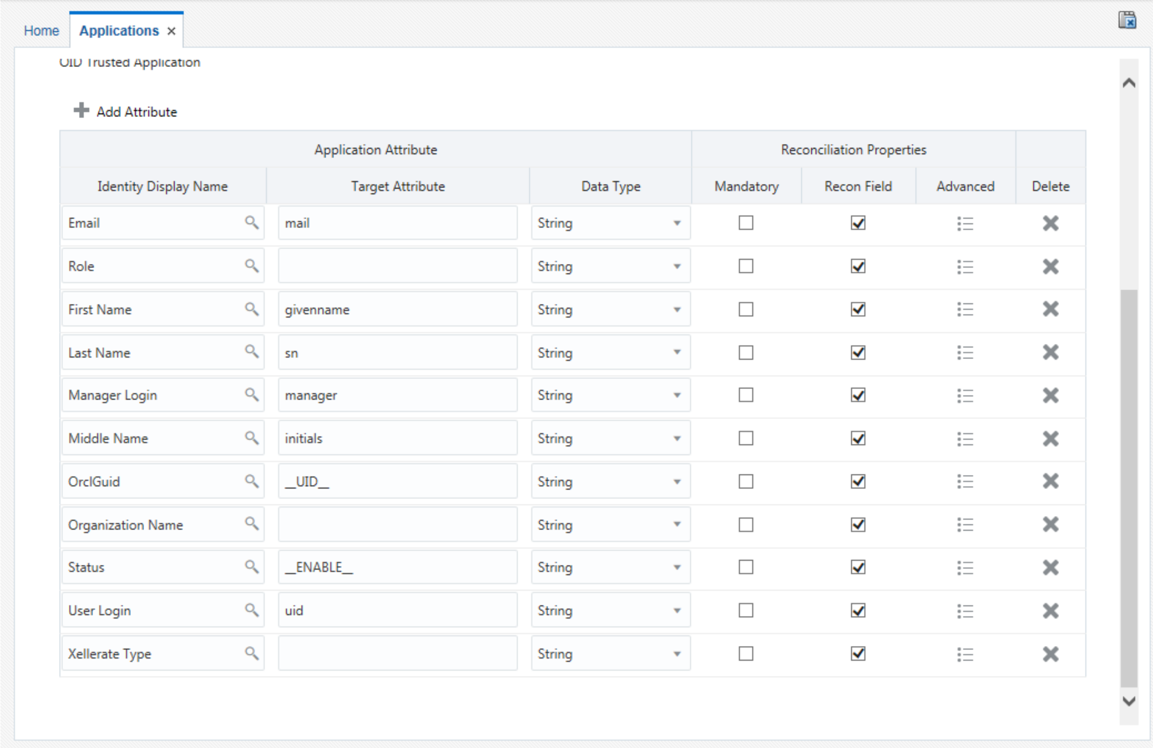
The Organization Name, Xellerate Type, and Role identity attributes are mandatory fields on the OIG User form. They cannot be left blank during reconciliation. The target attribute mappings for these identity attributes are empty by default because there are no corresponding columns in the target system. Therefore, the connector provides default values (as listed in the “Default Value for Identity Display Name” column of Table 3-6) that it can use during reconciliation. For example, the default target attribute value for the Organization Name attribute is Xellerate Users. This implies that the connector reconciles all target system user accounts into the Xellerate Users organization in Oracle Identity Governance. Similarly, the default attribute value for Xellerate Type attribute is End-User, which implies that all reconciled user records are marked as end users.

Table 3-6 Default Attributes for an OID Authoritative Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Advanced Flag Settings	Default Value for Identity Display Name
Email	mail	String	No	Yes	Yes	NA
Role	NA	String	No	Yes	Yes	Full-Time
First Name	givenname	String	No	Yes	Yes	NA
Last Name	sn	String	No	Yes	Yes	NA
Manager Login	manager	String	No	Yes	Yes	NA
Middle Name	initials	String	No	Yes	Yes	NA
OrclGuid	__UID__	String	No	Yes	Yes	NA
Organization Name	NA	String	No	Yes	Yes	Xellerate Users
Status	__ENABLE__	String	No	Yes	Yes	NA
User Login	uid	String	No	Yes	Yes	NA
Xellerate Type	NA	String	No	Yes	Yes	End-User

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

Figure 3-3 Default Attributes for an OID Authoritative Application



Home | Applications ×

OID Trusted Application

+ Add Attribute

Application Attribute			Reconciliation Properties			
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
Email	mail	String	☐	☑	☰	✖
Role		String	☐	☑	☰	✖
First Name	givenname	String	☐	☑	☰	✖
Last Name	sn	String	☐	☑	☰	✖
Manager Login	manager	String	☐	☑	☰	✖
Middle Name	initials	String	☐	☑	☰	✖
OrclGuid	_UID_	String	☐	☑	☰	✖
Organization Name		String	☐	☑	☰	✖
Status	_ENABLE_	String	☐	☑	☰	✖
User Login	uid	String	☐	☑	☰	✖
Xellerate Type		String	☐	☑	☰	✖

3.4 Correlation Rules for OID

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

- Correlation Rules for an OID Target Application
- Correlation Rules for an OID Authoritative Application

3.4.1 Correlation Rules for an OID Target Application

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

Predefined Identity Correlation Rules

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

Table 3-7 lists the default simple correlation rule for OID. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Reconciliation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-7 Predefined Identity Correlation Rule for OID

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
uid	Equals	User Login	No
__UID__	Equals	OrclGuid	No

In the first correlation rule element:

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

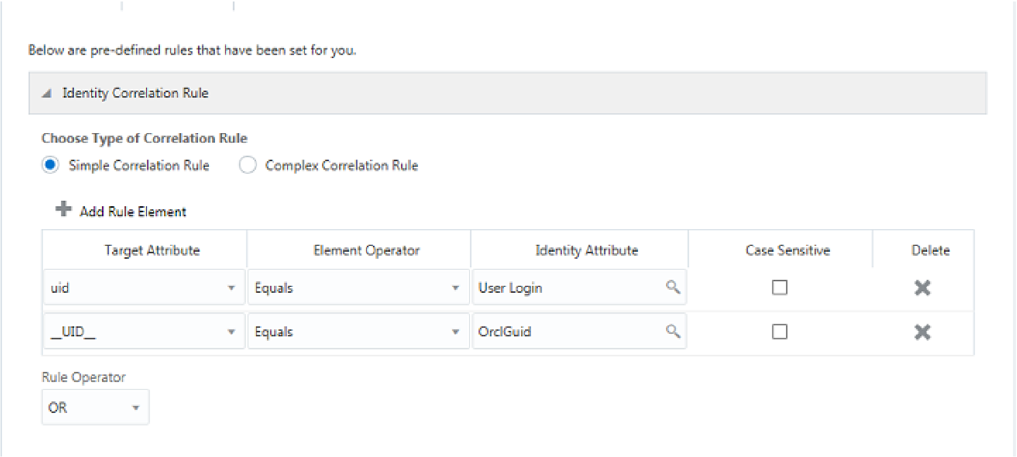
In the second correlation rule element:

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

Rule operator: OR

Figure 3-4 shows the simple correlation rule for an OID Target application.

Figure 3-4 Simple Correlation Rule for an OID Target Application



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

Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

Add Rule Element

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
uid	Equals	User Login	□	✖
__UID__	Equals	OrclGuid	□	✖

Rule Operator: OR

Predefined Situations and Responses

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

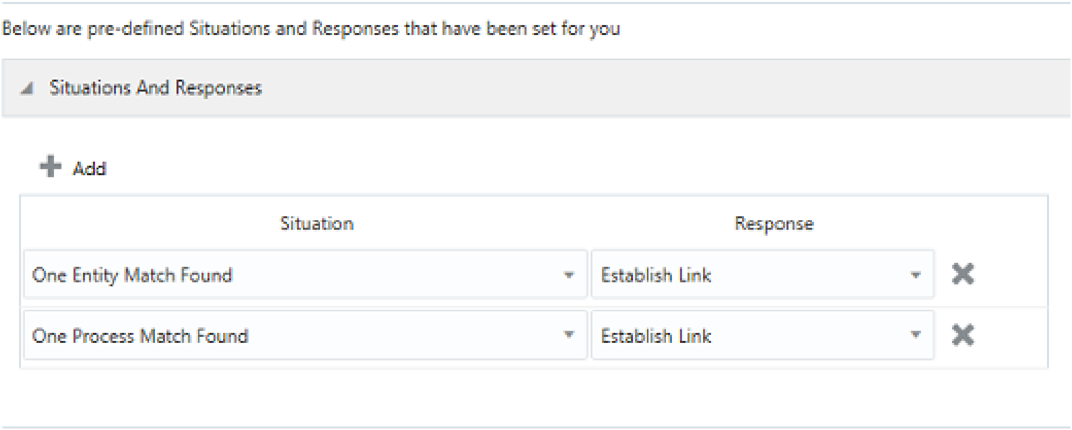
Table 3-8 lists the default situations and responses for an OID Target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-8 Predefined Situations and Responses for an OID Target Application

Situation	Response
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Figure 3-5 shows the situations and responses that the connector provides by default when you create a Target application for OID.

Figure 3-5   Predefined Situations and Responses for an OID Target Application



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

Situation	Response
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

3.4.2 Correlation Rules for an OID Authoritative Application

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

Predefined Identity Correlation Rules

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

Table 3-9 lists the default simple correlation rule for an OID connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Creating an Authoritative Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-9   Predefined Identity Correlation Rule for an OID Authoritative Application

Authoritative Attribute	Element Operator	Identity Attribute	Case Sensitive?
uid	Equals	User Login	No

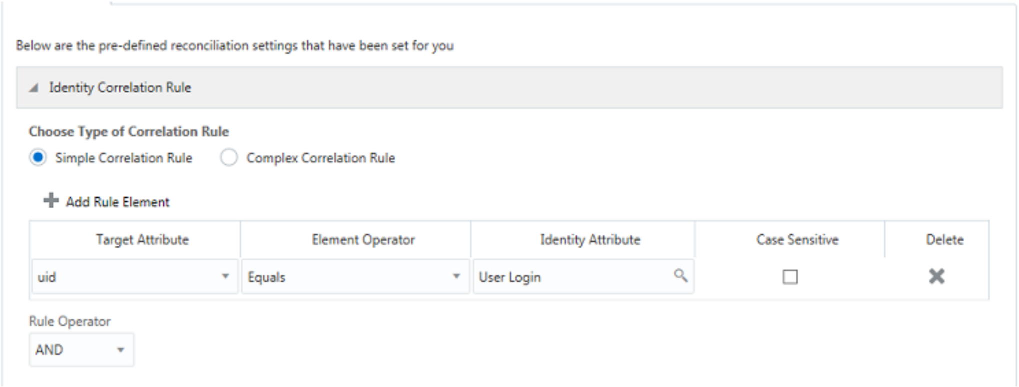
Correlation Rule element: uid Equals User Login

In this correlation rule element:

- uid is the unique login name of a user.
- User Login is the User ID field of the OIG User form.

Figure 3-6 shows the simple correlation rule for an OID Authoritative application.

Figure 3-6   Simple Correlation Rule for an OID Authoritative Application



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

Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

Add Rule Element

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

Rule Operator: AND

Predefined Situations and Responses

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

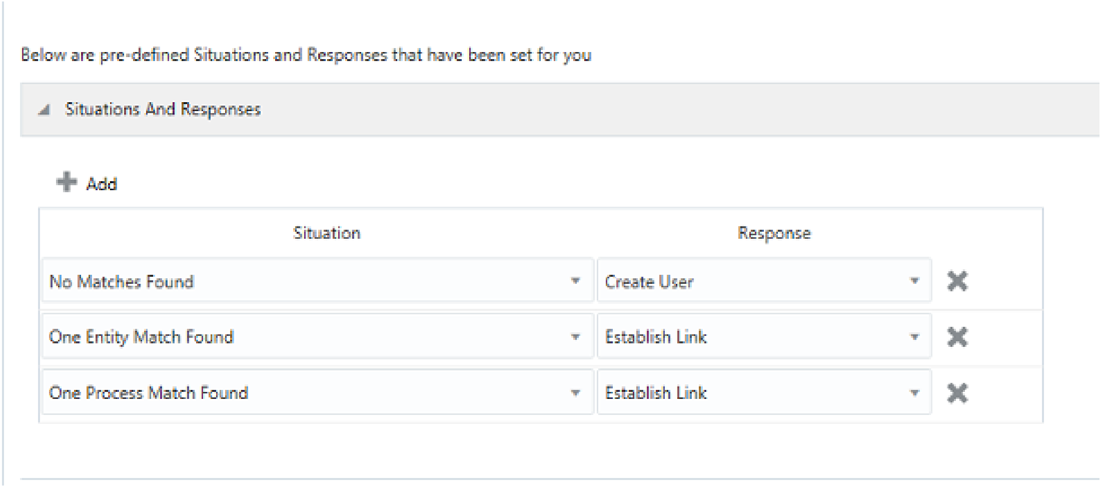
Table 3-10 lists the default situations and responses for an OID Authoritative Application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating an Authoritative Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.*

Table 3-10   Predefined Situations and Responses for an OID Authoritative Application

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

Figure 3-7 shows the situations and responses that the connector provides by default when you create an Authoritative application for OID.

Figure 3-7 Predefined Situations and Responses for an OID Authoritative Application



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

◢ Situations And Responses

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

3.5 Reconciliation Jobs for OID

Learn about reconciliation jobs that are automatically created in Oracle Identity Governance after you create a target or an authoritative application for your target system.

- Reconciliation Jobs for an OID Target Application
- Reconciliation Jobs for an OID Authoritative Application

3.5.1 Reconciliation Jobs for an OID Target Application

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

Reconciliation Jobs for an OID Target Application

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

The following reconciliation jobs are available for reconciling user data:

- OID Connector User Search Reconciliation: Use this reconciliation job to reconcile user data from a Target application. Use this job if either of the following conditions is true:
  - You want to perform Full or Incremental Reconciliation.
  - Your target system supports the modifyTimestamp attribute.
- OID Connector User Sync Reconciliation: Use this reconciliation job to reconcile user data from a Target application. Use this job if either of the following conditions is true:
  - You want to perform incremental reconciliation.
  - Your target system supports the changelog attribute.
- OID Connector User Search Delete Reconciliation: Use this reconciliation job to reconcile user records that are deleted from a Target application.

Table 3-11 describes the parameters of the OID Connector User Search Reconciliation job.

Table 3-11 Parameters of the OID Connector User Search Reconciliation Job

Parameter	Description
Application name	Name of the AOB application with which the reconciliation job is associated. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
Filter	Enter the expression for filtering records that this job must reconcile. **Sample value**: `equalTo('__UID__','EXAMPLEUSER')` For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.
Object Type	This parameter holds the type of object you want to reconcile. **Default value**: `User` Do *not* modify the value of this parameter.
Incremental Recon Attribute	Name of the target system attribute that holds the timestamp at which the user record was modified. **Default value**:`modifyTimestamp`
Scheduled Task Name	Name of the scheduled task used for reconciliation. **Note:** For the scheduled job included with this connector, you must not change the value of this parameter. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter.
Latest Token	This parameter holds the value of the target system attribute that is specified as the value of the Incremental Recon Attribute parameter. The connector uses the Latest Token parameter 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**: `<String>20120516115131Z</String>`

Table 3-12 describes the parameters of the OID Connector User Sync Reconciliation job.

Table 3-12 Parameters of the OID Connector User Sync Reconciliation Job

Parameter	Description
Application name	Name of the AOB Application with which the job is associated. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
Sync Token	You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time this job is run, the connector updates the value of Sync Token parameter. Browse the changelog attribute of the target system to determine a value from the changelog that the connector must use to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Governance. Or, you can also leave this field blank, which causes the entire changelog to be read. As OID is a target system for which the value of the standardChangelog advanced settings parameter is set to `true`, this parameter stores values in the following format: `<Integer>`*`VALUE`*`</Integer>` Sample value: `Integer>476</Integer>`
Object Type	This parameter holds the type of object you want to reconcile. **Default value**: `User` Do *not* modify the value of this parameter.
Scheduled Task Name	Name of the scheduled task used for reconciliation. **Note:** For the scheduled job included with this connector, you must not change the value of this parameter. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter.

Table 3-13 describes the parameters of the OID User Search Delete Reconciliation job.

Table 3-13 Parameters of the OID User Search Delete Reconciliation Job

Attribute	Description
Application name	Name of the AOB Application with which the job is associated. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.

Table 3-13   (Cont.) Parameters of the OID User Search Delete Reconciliation Job

Attribute	Description
Object Type	This parameter holds the type of object you want to reconcile. **Default value**: `User` Do *not* modify the value of this parameter.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- OID Connector Group Lookup Reconciliation: Use this job to search for and reconcile all group data in the target system into lookup fields in Oracle Identity Governance.
- OID Connector OU Lookup Reconciliation: Use this job to search for and reconcile all organization data in the target system into lookup fields in Oracle Identity Governance.

The parameters for both these reconciliation jobs are the same.

Table 3-14   Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
Lookup Name	Enter the name of the lookup definition in Oracle Identity Governance that the connector must populate with values it fetches from the target system. Depending on the reconciliation job that you are using, the default values are as follows: • OID Connector Group Lookup Reconciliation: `Lookup.OID.Group` • OID Connector OU Lookup Reconciliation:`Lookup.OID.Organization` 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 parameter.

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

Parameter	Description
Object Type	This parameter holds the type of object you want to reconcile. Depending on the reconciliation job that you are using, the default values are as follows: • OID Connector Group Lookup Reconciliation: `Group` • OID Connector OU Lookup Reconciliation : `OU` **Note**: Do *not* change the value of this parameter.
Code Key Attribute	Name of the connector or target system attribute that the connector uses to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name parameter). Default value: `dn` Do *not* modify this value.
Decode Attribute	Name of the connector or target system attribute that the connector uses to populate the Decode column of the lookup definition (specified as the value of the Lookup Name parameter). Depending on the reconciliation job that you are using, the default values are as follows: • OID Connector Group Lookup Reconciliation: `cn` • OID Connector OU Lookup Reconciliation : `ou`
Filter	Expression for filtering records that must be reconciled by the scheduled job. **Sample value**: `startsWith('cn','Samrole1')`

3.5.2 Reconciliation Jobs for an OID Authoritative Application

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

User Reconciliation Jobs for an OID Authoritative Application

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

The following reconciliation jobs are available for reconciling user data:

- OID Connector Trusted User Reconciliation: Use this reconciliation job to reconcile user data from an Authoritative application.

> **Note:**
>
> Before you run this job, ensure that the accounts in the target system have a unique User ID. Otherwise, you might observe unexpected results while running the job.

- OID Connector Trusted User Delete Reconciliation: Use this reconciliation job to reconcile user records that are deleted from an Authoritative Application.

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

Table 3-15 Parameters of the OID Connector Trusted User Reconciliation Job

Parameter	Description
Application name	Name of the AOB Application with which the job is associated. This value is the same as the value that you provided for the Application Name field while creating your authoritative application. Do *not* modify this value.
Filter	Enter the search filter for fetching user records from the authoritative application during a reconciliation run. **Sample value**: `startsWith('cn','Samrole1')`
Object Type	This parameter holds the type of object you want to reconcile. **Default value**: `User` Do *not* modify the value of this parameter.
Incremental Recon Attribute	Name of the target system attribute that holds the timestamp at which the user record was modified. **Default value**:`modifyTimestamp`
Scheduled Task Name	Name of the scheduled task used for reconciliation. **Note:** For the scheduled job included with this connector, you must not change the value of this parameter. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter.

Table 3-15 (Cont.) Parameters of the OID Connector Trusted User Reconciliation Job

Parameter	Description
Latest Token	This parameter holds the value of the target system attribute that is specified as the value of the Incremental Recon Attribute parameter. The connector uses the Latest Token parameter 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 for this attribute after execution. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only user accounts that have been modified after the time stamp specified as the value of this attribute are reconciled. If you want to perform a full reconciliation, then clear the value in this field. **Sample value**: `<String>20120516115131Z</String>`

Table 3-16 describes the parameters of the OID Connector Trusted User Delete Reconciliation job.

Table 3-16 Parameters of the OID Connector Trusted User Delete Reconciliation Job

Parameter	Description
Application name	Name of the AOB Application with which the job is associated. This value is the same as the value that you provided for the Application Name field while creating your authoritative application. Do *not* modify this value.
Object Type	This parameter holds the type of object you want to reconcile. **Default value**: `User` Do *not* modify the value of this parameter.

4

Configuring the Oracle Internet Directory Connector for OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

- Basic Configuration Parameters for OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Advanced Settings Parameters for OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Attribute Mappings for OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Correlation Rules for OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Reconciliation Jobs for OUD, ODSEE, and LDAPv3-Compliant Directory Server

4.1 Basic Configuration Parameters for OUD, ODSEE, and LDAPv3-Compliant Directory Server

These are the connection-related parameters that Oracle Identity Governance requires to connect to OUD, ODSEE, or an LDAPv3-compliant directory server. These parameters are common for both target applications and authoritative applications.

Table 4-1 Basic Configuration Parameters for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
baseContexts	Yes	Enter the base contexts for operations on the target system. Sample value: `dc=example,dc=com` **Note:** In a multilevel base context, each base context must be specified within double quotes (") and separated by a comma (,). For example: `"dc=example,dc=com","dc=mydc,dc=com"`

Table 4-1 (Cont.) Basic Configuration Parameters for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
principal	Yes	Enter the bind DN for performing operations on the target system. Sample value: `cn=Directory Manager` **Note**: If you are using OpenLDAP as the target system, then set the value of this parameter in the following format: *user DN*,*baseContexts* Sample value: `cn=admin,dc=example,dc=com` In this sample value, `cn=admin` is the user DN value and `dc=example,dc=com` is the baseContexts value.
credentials	Yes	Enter the bind password associated with the bind DN.
host	Yes	Enter the host name or the IP address of the target system. Sample value: `myhost` or `192.0.2.10`
port	Yes	Enter the port number to connect to the target system. Sample value: `1389`
Connector Server Name	No	By default, this field is blank. If you use a Connector Server, then enter the name of Connector Server IT resource.
failover	No	Enter the complete URL of LDAP backup server or servers that the connector must switch to if the primary LDAP server fails or becomes unavailable. The URL is a fully qualified host name or an IP address in the following format: ldap://*host*:*port* The following example shows an IP address for one backup LDAP server: `ldap://172.20.55.191:389` If you specify more than one URL, each URL must be enclosed in double quotes (") and separated by a comma (,). For example: `"ldap://172.20.55.191:389","ldap://172.20.55.171:387"`
ssl	No	This parameter specifies whether communication with the target system must be secured using SSL. By default, this field is blank. Enter `true` if you want to configure SSL between Oracle Identity Governance and the Connector Server or between Oracle Identity Governance and the target system. Otherwise, enter `false`. Set the `UseSSL` IT Resource parameter for the Connector Server to `true`, as described in Configuring the IT Resource for the Connector Server. To configure SSL, see Configuring the Java Connector Server with SSL for Oracle Identity Governance in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.2 Advanced Settings Parameters for OUD, ODSEE, and LDAPv3-Compliant Directory Server

These are the configuration-related parameters that the connector uses during reconciliation and provisioning operations. These parameters vary depending on whether you are creating a target application or an authoritative application.

- Advanced Settings Parameters for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Advanced Settings Parameters for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

4.2.1 Advanced Settings Parameters for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

These are the configuration-related parameters that are applicable to a target application. By default, the connector displays attribute values for an OUD target system. You can update these values for the ODSEE and LDAPv3-compliant directory server target systems, as specified in the table.

Table 4-2 Advanced Settings Parameters for a Target Application for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
disabledValue	No	Specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is disabled. Default value: `true`
blockSize	No	Block size for simple paged results and VLV index searches. Default value: `100`
Bundle Version	No	Version of the connector bundle class. Default value: `12.3.0`
Connector Name	No	Name of the connector class. Default value: `org.identityconnectors.ldap.LdapConnector`
standardChangelog	No	Flag that indicates whether the connector must access the changelog attribute by using the standard format or a specific mechanism during a SyncOp operation. **Note**: If you are using OUD as the target system, then set the value of this parameter to `false`. For ODSEE or an LDAPv3-compliant directory server, set the value of this parameter to `true`.
enabledAttribute	No	Name of the attribute that is required to enable or disable accounts. Default value: `ds-pwp-account-disabled` **Note**: If you are using ODSEE or an LDAPv3-compliant directory server as the target system, then set the value of this parameter to `nsaccountlock`.

Table 4-2 (Cont.) Advanced Settings Parameters for a Target Application for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
synchronizeWithModifyTimestamps	No	Specifies whether the connector must use the modify timestamps attribute instead of the changelog attribute during a SyncOp operation. Default value: `false`
vlvSortAttribute	No	Attribute used as the sort key for the VLV index. Default value: `uid`
enabledValue	No	Specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is enabled. Default value: `false`
accountSynchronizationFilter	No	Filter for all of the entries returned during the SyncOp operation that must match. Default value: `objectClass=*`

filterWithOrInsteadOfAnd	No	Specifies whether the changelog filter is built using an OR or AND filter. The default value is `false`.
		Enter `true` if the changelog filter is built using an OR filter instead of AND filter.
		An OR filter is in the following format:
		`(|(changeNumber=1) (changeNumber=2) . . . (changeNumber=xxx))`
		An AND filter is of the following format:
		`(&(changeNumber>=0) (changeNumber<=xxx))`

usePagedResultControl	No	Specifies whether simple paged search is preferred over VLV index search when both are available. Default value: `true`
objectClassesToSynchronize	No	This entry holds the list of object classes to be synchronized. Any synchronized entry in order to be returned must have at least one object class from this list. If this list of object classes is empty or the code key is missing, then no filtering is performed on the object classes. Default value: `"inetOrgPerson","groupOfNames","groupOfUniqueNames","organizationalUnit"` **Note**: If you are using ODSEE or an LDAPv3-compliant directory server as the target system, then set the value of this parameter to `"inetOrgPerson","groupOfNames","groupOfUniqueNames","nsRoleDefinition","organizationalUnit"`.
changeLogBlockSize	No	Block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation. Default value: `100`
maintainPosixGroupMembership	No	Specifies whether the connector modifies group membership of renamed or deleted user entries. Default value: `false`

Table 4-2 (Cont.) Advanced Settings Parameters for a Target Application for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
groupMemberAttribute	No	LDAP attribute that stores the member for non-POSIX static groups. Default value: `uniqueMember`
accountObjectClasses	No	List of object classes required for a USER object. Default value: `"top","person","organizationalPerson","inetOrgPerson"`
passwordAttribute	No	Name of the attribute to which the predefined PASSWORD attribute is written to. Default value: `userPassword`
respectResourcePasswordPolicyChangeAfterReset	No	By default, this value is set to `true`. Do not modify the value if the connector throws exceptions (for example, PasswordExpiredException) appropriately when binding check for the Password Expired control and Password Policy control. Otherwise, enter `false`.
maintainLdapGroupMembership	No	Specifies whether the connector modifies group membership of renamed or deleted user entries. Default value: `true`
attributesToSynchronize	No	List of attributes to return whenever a SyncOp is run. Default value: `"cn","uid"`
readSchema	No	Specifies whether the schema must be read from the server. Default value: `true`
uidAttribute	No	LDAP attribute to which the predefined UID attribute must be mapped to. Default value: `entryUUID` **Note**: If you are using ODSEE as the target system, then set the value of this parameter to `nsuniqueid`. For OpenLDAP server, set the value of this parameter to `entryUUID`. For other LDAPv3-compliant directory servers, set the value based on the directory server you are using.
enabledWhenNoAttribute	No	Defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the entry. Default value: `true`
accountSearchFilter	No	Search filter that any account needs to match in order to be returned. Default value: `objectClass=*`
Bundle Name	No	Name of the connector bundle package. Default value: `org.identityconnectors.ldap`
changeNumberAttribute	No	Attribute name used for changelog. Default value: `changelogcookie` **Note**: If you are using ODSEE or an LDAPv3-compliant directory server as the target system, then set the value of this parameter to `changeNumber`.

Table 4-2 (Cont.) Advanced Settings Parameters for a Target Application for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
removeLogEntryObjectClassFromFilter	No	Specifies whether the changelog filter contains a condition on the changelog objectclass. Default value: `true`
disabledRoleName	No	Name of the role that must be present in the entry when an account is disabled and that the enabledBaseOnRole is set to `true`. Sample value: `cn=nsmanageddisabledrole,dc=example,dc=com`
changelogBaseDn	No	BaseDN where the connector is to find the changelog attribute value. Default value: `cn=changelog`
accountUserNameAttribute	No	Attributes that contain the name of a USER object. Default value: `cn`
enabledBasedOnRole	No	Specifies whether enabling or disabling a user must be controlled by a role instead of the enabledAttribute attribute. When you set the value of this entry to `true`, it takes precedence over all the other enabled or disabled-related flags. Default value: `false`
changelogUidAttribute	No	Name of the attribute that contains the uniqueId of the modified entry in the changelog. Default value: `targetEntryUUID` **Note**: If you are using ODSEE or an LDAPv3-compliant directory server as the target system, then set the value of this parameter to `targetuniqueid`.
Any Incremental Recon Attribute Type	No	Indicates that any format of token is accepted during reconciliation. Default value: `true`
ldapGroupFilterBehavior	No	Specifies the behavior for an LDAP group filter. Default value: `accept`
ldapGroupMembershipAttribute	No	Specifies the value for the LDAP group membership attribute. Default value: `ismemberof`
pwdMaxFailure	No	Indicates the number of consecutive failed bind attempts after which a user account is locked. If the value is 0 (zero), then the account is not locked due to failed bind attempts and the value of the password lockout policy is ignored. Default value: `10`
Pool Max Idle	No	Maximum number of idle objects in a pool. Default value: `10`
Pool Max Size	No	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	No	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`

Table 4-2 (Cont.) Advanced Settings Parameters for a Target Application for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
Pool Min Evict Idle Time	No	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	No	Minimum number of idle objects in a pool. Default value: `1`

4.2.2 Advanced Settings Parameters for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

These are the configuration-related parameters that are applicable to an authoritative application. By default, the connector displays attribute values for an OUD target system. You can update these values for the ODSEE and LDAPv3-compliant directory server target systems, as specified in the table.

Table 4-3 Advanced Settings Parameters for an Authoritative Application for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
Bundle Name	No	Name of the connector bundle package. Default value: `org.identityconnectors.ldap`
Bundle Version	No	Version of the connector bundle class. Default value: `12.3.0`
changeNumberAttribute	No	Attribute name used for changelog. Default value: `changelogcookie` **Note**: If you are using ODSEE or an LDAPv3-compliant directory server as the target system, then set the value of this parameter to `changeNumber`.
objectClassesToSynchronize	No	List of object classes to be synchronized. Any synchronized entry in order to be returned must have at least one object class from this list. If this list of object classes is empty or the code key is missing, then no filtering is performed on the object classes. Default value: `"inetOrgPerson","groupOfNames","groupOfUniqueNames","organizationalUnit"` **Note**: If you are using ODSEE or an LDAPv3-compliant directory server as the target system, then set the value of this parameter to `"inetOrgPerson","groupOfNames","organizationalUnit"`.
changeLogBlockSize	No	Block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation. Default value: `100`

Table 4-3 (Cont.) Advanced Settings Parameters for an Authoritative Application for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
User Configuration Lookup	No	Name of the lookup definition that contains user-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of users. Do *not* modify this entry. Default value: `Lookup.LDAP.UM.Configuration.Trusted`
enabledAttribute	No	Name of the attribute that is required to enable or disable accounts. Default value: `ds-pwp-account-disabled` **Note**: If you are using ODSEE or an LDAPv3-compliant directory server as the target system, then set the value of this parameter to `nsaccountlock`.
enabledWhenNoAttribute	No	Defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the entry. Default value: `true`
disabledValue	No	Specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is disabled. Default value: `true`
enabledValue	No	Specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is enabled. Default value: `false`
usePagedResultControl	No	Specifies whether simple paged search is preferred over VLV index search when both are available. Default value: `true`
Any Incremental Recon Attribute Type	No	Indicates that any format of token is accepted during reconciliation. Default value: `true`
Connector Name	No	Name of the connector class. Default value: `org.identityconnectors.ldap.LdapConnector`
uidAttribute	No	LDAP attribute to which the Uid must be mapped to. Default value: `entryUUID` **Note**: If you are using ODSEE as the target system, then set the value of this parameter to `nsuniqueid`. For OpenLDAP server, set the value of this parameter to `entryUUID`. For other LDAPv3-compliant directory servers, set the value based on the directory server you are using.
pwdMaxFailure	No	Indicates the number of consecutive failed bind attempts after which a user account is locked. If this attribute is not present, or if the value is 0 (zero), then the account is not locked due to failed bind attempts, and the value of the password lockout policy is ignored. Default value: `10`
Pool Max Idle	No	Maximum number of idle objects in a pool. Default value: `10`

Table 4-3 (Cont.) Advanced Settings Parameters for an Authoritative Application for OUD, ODSEE, or an LDAPv3-Compliant Directory Server

Parameter	Mandatory?	Description
Pool Max Size	No	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	No	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`
Pool Min Evict Idle Time	No	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	No	Minimum number of idle objects in a pool. Default value: `1`

4.3 Attribute Mappings for OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

- Attribute Mappings for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Attribute Mappings for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

4.3.1 Attribute Mappings for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

LDAP User Account Attributes

Table 4-4 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and target system attributes. The table also lists whether a specific attribute is used during provisioning or reconciliation and whether it is a matching key field for fetching records during reconciliation.

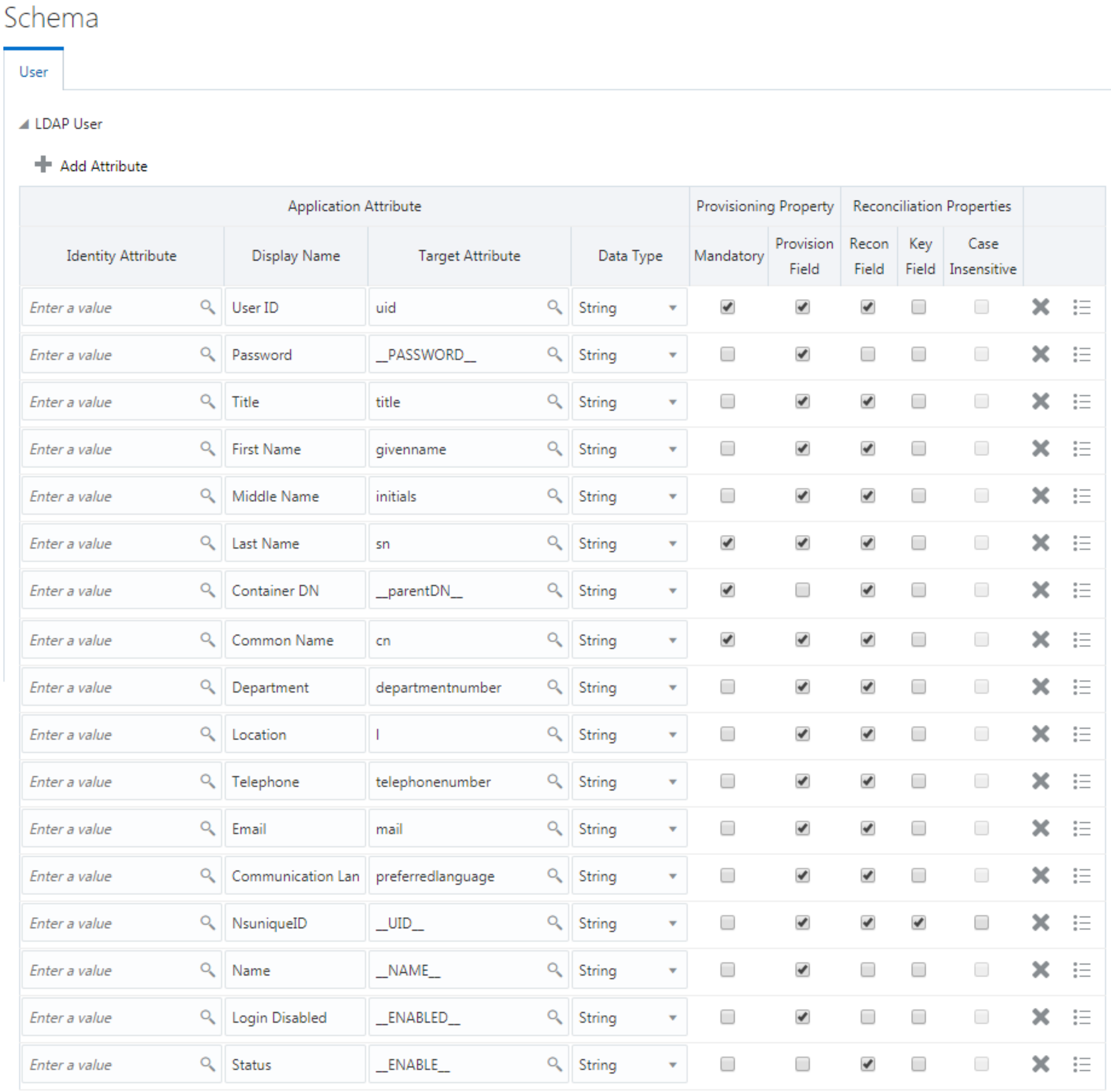
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 4-4   Default Attribute Mappings for LDAP User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User ID	uid	String	Yes	Yes	Yes	No	Not applicable
Title	title	String	No	Yes	Yes	No	Not applicable
First Name	givenname	String	No	Yes	Yes	No	Not applicable
Middle Name	initials	String	No	Yes	Yes	No	Not applicable
Last Name	sn	String	Yes	Yes	Yes	No	Not applicable
Common Name	cn	String	Yes	Yes	Yes	No	Not applicable
Department	departmentnumber	String	No	Yes	Yes	No	Not applicable
Location	l	String	No	Yes	Yes	No	Not applicable
Telephone	telephonenumber	String	No	Yes	Yes	No	Not applicable
Email	mail	String	No	Yes	Yes	No	Not applicable
Communication Lan	preferredlanguage	String	No	Yes	Yes	No	Not applicable
NsuniqueID	__UID__	String	No	Yes	Yes	Yes	Not applicable
Container DN	__parentDN__	String	Yes	No	Yes	No	Not applicable
Status	__ENABLE__	String	No	No	Yes	No	Not applicable
Password	__PASSWORD__	String	No	Yes	No	No	Not applicable
Name	__NAME__	String	No	Yes	No	No	Not applicable
Login Disabled	__ENABLED__	String	No	Yes	No	No	Not applicable

Figure 4-1 shows the default LDAP User account attribute mappings in a target application.

Figure 4-1 Default Attribute Mappings for an LDAP User Account in a Target Application



Application Attribute				Provisioning Property		Reconciliation Properties			
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive	
Enter a value	User ID	uid	String	☑	☑	☑	☐	☐	✖ ☰
Enter a value	Password	__PASSWORD__	String	☐	☑	☐	☐	☐	✖ ☰
Enter a value	Title	title	String	☐	☑	☑	☐	☐	✖ ☰
Enter a value	First Name	givenname	String	☐	☑	☑	☐	☐	✖ ☰
Enter a value	Middle Name	initials	String	☐	☑	☑	☐	☐	✖ ☰
Enter a value	Last Name	sn	String	☑	☑	☑	☐	☐	✖ ☰
Enter a value	Container DN	__parentDN__	String	☑	☐	☑	☐	☐	✖ ☰
Enter a value	Common Name	cn	String	☑	☑	☑	☐	☐	✖ ☰
Enter a value	Department	departmentnumber	String	☐	☑	☑	☐	☐	✖ ☰
Enter a value	Location	l	String	☐	☑	☑	☐	☐	✖ ☰
Enter a value	Telephone	telephonenumber	String	☐	☑	☑	☐	☐	✖ ☰
Enter a value	Email	mail	String	☐	☑	☑	☐	☐	✖ ☰
Enter a value	Communication Lan	preferredlanguage	String	☐	☑	☑	☐	☐	✖ ☰
Enter a value	NsuniqueID	__UID__	String	☐	☑	☑	☑	☐	✖ ☰
Enter a value	Name	__NAME__	String	☐	☑	☐	☐	☐	✖ ☰
Enter a value	Login Disabled	__ENABLED__	String	☐	☑	☐	☐	☐	✖ ☰
Enter a value	Status	__ENABLE__	String	☐	☐	☑	☐	☐	✖ ☰

Group Entitlement Attributes

Table 4-5 lists the attribute mappings for Group entitlement between the process form fields in Oracle Identity Governance and target system attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

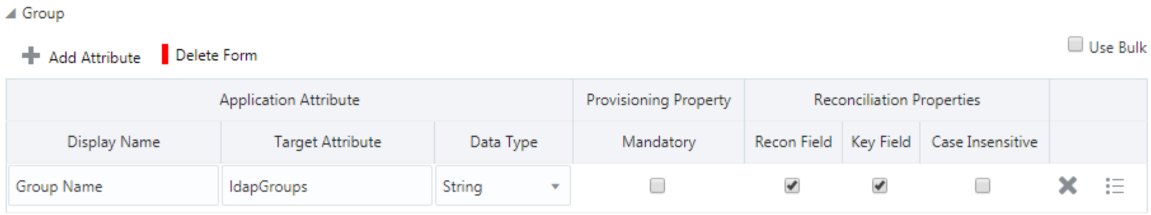
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 4-5 Default Attribute Mappings for Group Entitlement

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

Figure 4-2 shows the default Group entitlement attribute mapping.

Figure 4-2 Default Attribute Mappings for Group Entitlement



◢ Group

✚ Add Attribute | Delete Form

□ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Group Name	ldapGroups	String ▾	□	☑	☑	□	✖	☰

Role Entitlement Attributes

Table 4-6 lists the attribute mappings for Role entitlement between the process form fields in Oracle Identity Governance and target system attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

> **Note:**
>
> Roles are not supported by the OUD and OpenLDAP target systems. Therefore, these attribute mappings for Role entitlement are applicable only to ODSEE and the LDAPv3-compliant directory server target systems that support Roles.

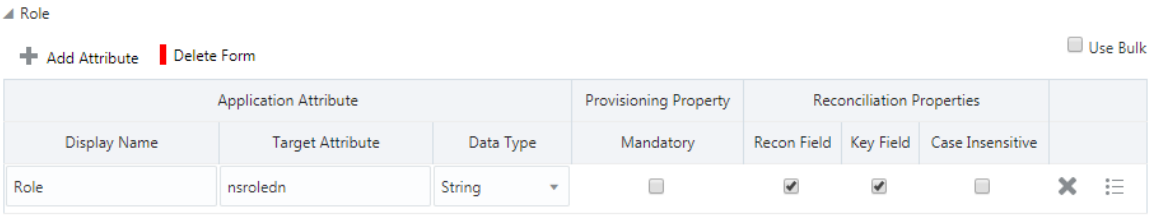
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 4-6 Default Attribute Mappings for Role Entitlement

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

Figure 4-3 shows the default Role child attribute mapping.

Figure 4-3   Default Attribute Mappings for Role Entitlement



◢ Role

➕ Add Attribute   Delete Form   □ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties			
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive	
Role	nsroledn	String ▾	□	☑	☑	□	✖ ☰

4.3.2 Attribute Mappings for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

Table 4-7 lists the user-specific attribute mappings between the reconciliation fields in Oracle Identity Governance and target system columns. The table also lists the data type for a given attribute and specified whether it is a mandatory attribute for reconciliation.

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

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

The Organization Name, Role, Xellerate Type, and Status identity attributes are mandatory fields on the OIG User form. They cannot be left blank during reconciliation. The target attribute mappings for these identity attributes are empty by default because there are no corresponding columns in the target system. Therefore, the connector provides default values (as listed in the “Default Value for Identity Display Name” column of Table 4-7) that it can use during reconciliation. For example, the default target attribute value for the Organization Name attribute is Xellerate Users. This implies that the connector reconciles all target system user accounts into the Xellerate Users organization in Oracle Identity Governance. Similarly, the default attribute value for Xellerate Type attribute is End-User, which implies that all reconciled user records are marked as end users.

Table 4-7   LDAP Trusted User Schema Attributes

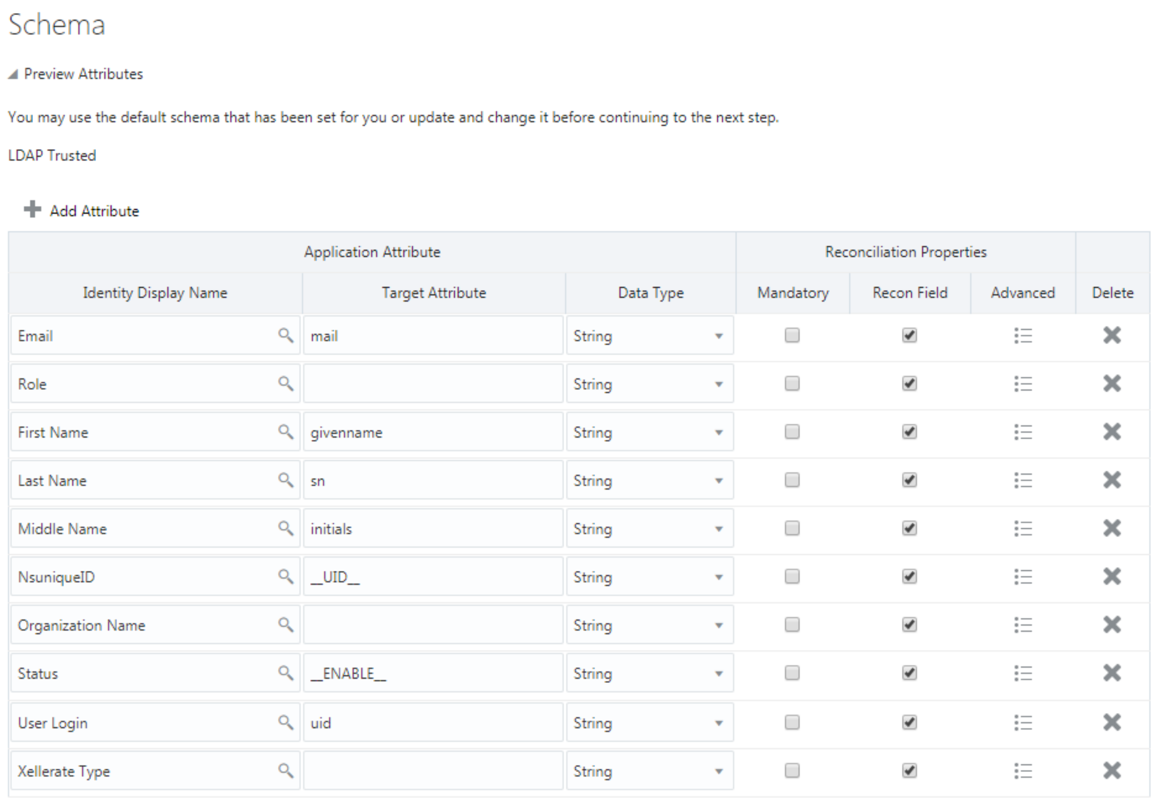
Identity Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Default Value for Identity Display Name
Email	mail	String	No	Yes	NA
Role	NA	String	No	Yes	Full-Time
First Name	givenname	String	No	Yes	NA
Last Name	sn	String	No	Yes	NA
Middle Name	initials	String	No	Yes	NA
NsuniqueID	__UID__	String	No	Yes	NA

Table 4-7 (Cont.) LDAP Trusted User Schema Attributes

Identity Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Default Value for Identity Display Name
Organization Name	NA	String	No	Yes	Xellerate Users
Status	__ENABLE__	String	No	Yes	NA
User Login	uid	String	No	Yes	NA
Xellerate Type	NA	String	No	Yes	End-User

Figure 4-4 shows the default LDAP Trusted user account attribute mappings in an authoritative application.

Figure 4-4 Default Attribute Mappings for LDAP Trusted User Account in an Authoritative Application



Schema

◢ Preview Attributes

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

LDAP Trusted

+ Add Attribute

Application Attribute			Reconciliation Properties			
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
Email	mail	String	☐	☑	☰	✖
Role		String	☐	☑	☰	✖
First Name	givenname	String	☐	☑	☰	✖
Last Name	sn	String	☐	☑	☰	✖
Middle Name	initials	String	☐	☑	☰	✖
NsuniqueID	__UID__	String	☐	☑	☰	✖
Organization Name		String	☐	☑	☰	✖
Status	__ENABLE__	String	☐	☑	☰	✖
User Login	uid	String	☐	☑	☰	✖
Xellerate Type		String	☐	☑	☰	✖

4.4 Correlation Rules for OUD, ODSEE, and LDAPv3-Compliant Directory Server

Learn about the predefined rules, responses and situations for target and authoritative applications. The connector use these rules and responses for performing reconciliation.

- Correlation Rules for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Correlation Rules for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

4.4.1 Correlation Rules for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

Predefined Identity Rules

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

Table 4-8 lists the default simple correlation rule for the connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 4-8 Predefined Identity Correlation Rule for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
uid	Equals	User Login	No
__UID__	Equals	NsuniqueID	No

In first identity rule:

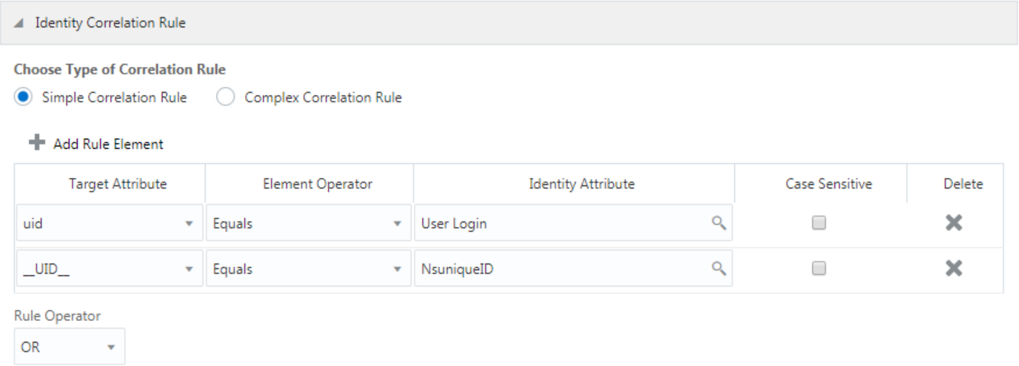
- uid is the unique login name of a user.
- User Login is the field on the OIG User form.

In second identity rule:

- __UID__ is an attribute on the target system that uniquely identifies the user account.
- NsuniqueID is the field on the OIG User form.

Figure 4-5 shows the simple correlation rule that the connector uses when you create a target application for OUD, ODSEE, and LDAPv3-compliant directory server.

Figure 4-5 Simple Correlation Rule for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server



Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

Add Rule Element

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
uid	Equals	User Login	□	✖
__UID__	Equals	NsuniqueID	□	✖

Rule Operator

OR

Predefined Situations and Responses

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

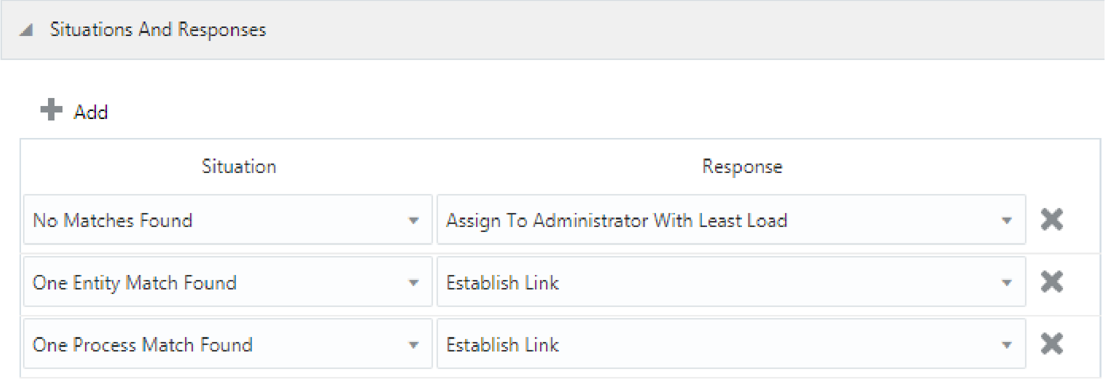
Table 4-9 lists the default situations and responses for the application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 4-9 Predefined Situations and Responses for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

Situation	Response
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Figure 4-6 shows the situations and responses that the connector provides by default when you create a target application for OUD, ODSEE, and LDAPv3-compliant directory server.

Figure 4-6 Predefined Situations and Responses for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server



Situation	Response
No Matches Found	Assign To Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

4.4.2 Correlation Rules for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

Predefined Identity Correlation Rules

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

Table 4-10 lists the default simple correlation rule for an authoritative application. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 4-10 Predefined Identity Correlation Rule for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

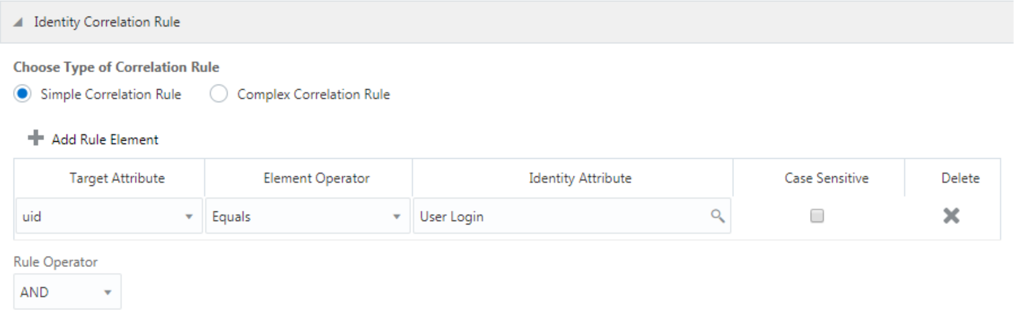
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
uid	Equals	User Login	No

In this identity rule:

- uid is the unique login name of a user.
- User Login is the field on the OIG User form.

Figure 4-7 shows the simple correlation rule when you create an authoritative application for OUD, ODSEE, and LDAPv3-compliant directory server.

Figure 4-7 Simple Correlation Rule for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server



Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

Add Rule Element

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

Rule Operator: AND

Predefined Situations and Responses

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

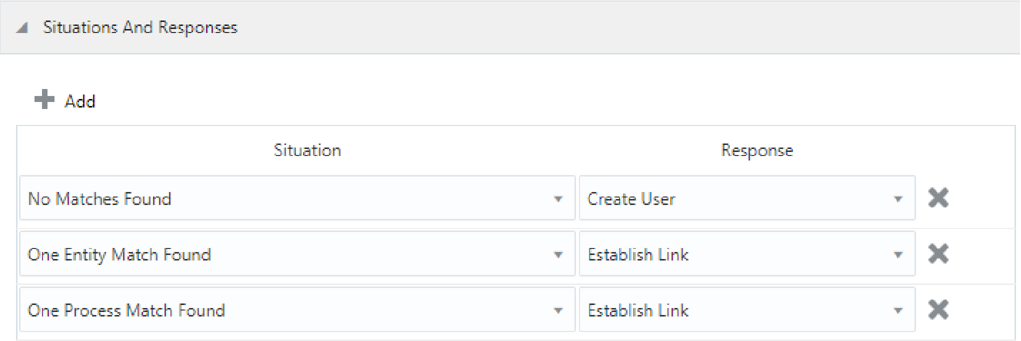
Table 4-11 lists the default situations and responses. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 4-11 Predefined Situations and Responses for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

Figure 4-8 shows the situations and responses that the connector provides by default when you create an authoritative application for OUD, ODSEE, and LDAPv3-compliant directory server.

Figure 4-8 Predefined Situations and Responses for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server



Situations And Responses

Add

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

4.5 Reconciliation Jobs for OUD, ODSEE, and LDAPv3-Compliant Directory Server

Learn about reconciliation jobs that are automatically created in Oracle Identity Governance after you create a target or an authoritative application for OUD, ODSEE, and LDAPv3-compliant directory server.

- Reconciliation Jobs for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Reconciliation Jobs for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

4.5.1 Reconciliation Jobs for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

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

LDAP Connector User Search Reconciliation Job

Use the LDAP Connector User Search Reconciliation job to perform full reconciliation, which involves reconciling all user records from a target application into Oracle Identity Governance. If your target system supports modifyTimestamp, then you can use this reconciliation job to perform incremental reconciliation.

Table 4-12 Parameters of the LDAP Connector User Search Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Filter	Enter the expression for filtering records that the scheduled job must reconcile. Sample value: `equalTo('__UID__','SEPT12USER1')` For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `User` Do not change the default value.

Table 4-12 (Cont.) Parameters of the LDAP Connector User Search Reconciliation Job

Parameter	Description
Incremental Recon Attribute	Name of the target system column that holds the timestamp at which the user record is modified. Default value: `modifyTimestamp` Do not change the default value.
Scheduled Task Name	Name of the scheduled task **Note**: For the scheduled task shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the task, then you can enter the unique name for that scheduled task as the value of this attribute.
Latest Token	The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The Latest Token parameter is used for internal purposes. By default, this attribute is empty. Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute.

LDAP Connector User Sync Reconciliation Job

If your target system supports changelog, use the LDAP Connector User Sync Reconciliation job to perform incremental reconciliation. During incremental reconciliation, only the records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance.

Table 4-13 Parameters of the LDAP Connector User Sync Reconciliation Job

Parameter	Value
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Object Type	Type of object you want to reconcile Default value: `User`
Scheduled Task Name	Name of the scheduled task **Note**: For the scheduled task shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the task, then you can enter the unique name for that scheduled task as the value of this attribute.
Sync Token	Time stamp at which the last reconciliation run started **Note**: Do not enter a value for this attribute. The reconciliation engine automatically enters a value for this attribute. If you set this attribute to an empty value, then incremental reconciliation operations fetch all the records (perform full reconciliation).

LDAP Connector User Search Delete Reconciliation Job

Use the LDAP Connector User Search Delete Reconciliation job to reconcile data about deleted user accounts from a target application.

Table 4-14 Parameters of the LDAP Connector User Search Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `User` Do not change the default value.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- LDAP Connector Role Lookup Reconciliation
- LDAP Connector Group Lookup Reconciliation
- LDAP Connector OU Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 4-15 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. **Note**: Do not modify this value.
Filter	Enter the search filter for fetching user records from the target system during a reconciliation run. The following is a sample value for the LDAP Connector Group Lookup Reconciliation job: `containsAllValues('ldapGroups','cn=grp1,ou=groups,dc=example,dc=com')`
Object Type	Enter the type of object whose values must be synchronized. Depending on the reconciliation job you are using, the default values are as follows: • For LDAP Connector Role Lookup Reconciliation: `Role` • For LDAP Connector Group Lookup Reconciliation: `Group` • For LDAP Connector OU Lookup Reconciliation: `OU` **Note:** Do not change the value of this attribute.

Table 4-15 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Lookup Name	This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched. Depending on the reconciliation job you are using, the default values are as follows: • For LDAP Connector Role Lookup Reconciliation: `Lookup.LDAP.Role` • For LDAP Connector Group Lookup Reconciliation: `Lookup.LDAP.Group` • For LDAP Connector OU Lookup Reconciliation: `Lookup.LDAP.Organization`
Decode Attribute	Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the reconciliation job you are using, the default values are as follows: • For LDAP Connector Role Lookup Reconciliation and LDAP Connector Group Lookup Reconciliation: `cn` • For LDAP Connector OU Lookup Reconciliation: `ou`
Code Key Attribute	Enter the name of the connector or target system 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: `dn` **Note:** Do not change the value of this attribute.

4.5.2 Reconciliation Jobs for an Authoritative Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server

These are the reconciliation jobs that are automatically created in Oracle Identity Governance after you create an authoritative application for your target system.

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

LDAP Connector Trusted User Reconciliation Job

Use the LDAP Connector Trusted User Reconciliation job to perform full reconciliation, which involves reconciling all user records created or modified directly on an authoritative application into Oracle Identity Governance. The connector uses this data to create or update the corresponding OIG Users. If your target system supports modifyTimestamp, then you can use this reconciliation job to perform incremental reconciliation.

Table 4-16 Parameters of the LDAP Connector Trusted User Reconciliation Job

Parameter	Value
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Filter	Enter the expression for filtering records that the scheduled job must reconcile. Sample value: `equalTo('__UID__','SEPT12USER1')` For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `User` Do not change the default value.
Incremental Recon Attribute	Name of the target system column that holds the timestamp at which the user record is modified. Default value: `modifyTimestamp` Do not change the default value.
Scheduled Task Name	Name of the scheduled task **Note**: For the scheduled task shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the task, then you can enter the unique name for that scheduled task as the value of this attribute.
Latest Token	The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The Latest Token parameter is used for internal purposes. By default, this attribute is empty. Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute.

LDAP Connector Trusted User Delete Reconciliation Job

The LDAP Connector Trusted User Delete Reconciliation job is used to reconcile data about deleted user accounts from an authoritative application.

> **Note:**
>
> Before running this reconciliation job, ensure that all users on the target system are assigned a unique value for the `User ID` target attribute otherwise unexpected errors might occur.

Table 4-17   Parameters of the LDAP Connector Trusted User Delete Reconciliation Job

Parameter	Value
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Object Type	Type of object you want to reconcile. Default value: `User`

5

Performing the Postconfiguration Tasks for the Oracle Internet Directory Connector

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

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

5.1 Configuring Oracle Identity Governance

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

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

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

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

5.1.1 Creating and Activating a Sandbox

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

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

5.1.2 Creating a New UI Form

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

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

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

5.1.3 Publishing a Sandbox

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

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

5.1.4 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

1. Create and activate a sandbox.
2. Create a new UI form for the resource.
3. Open the existing application instance.
4. In the Form field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox.

See Also:

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

5.2 Harvesting Entitlements and Sync Catalog

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

To harvest entitlements and sync catalog:

1. Run the reconciliation jobs for entitlements lookup field synchronization listed in Reconciliation Jobs for an OID Target Application or Reconciliation Jobs for a Target Application for OUD, ODSEE, and LDAPv3-Compliant Directory Server.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

See Also:

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

5.3 Managing Logging for the Oracle Internet Directory Connector

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

5.3.1 Understanding Log Levels

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

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

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

These message types are mapped to ODL message type and level combinations as shown in Table 5-2.

Table 5-1 Log Levels and ODL Message Type:Level Combinations

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

Table 5-2 Log Levels and ODL Message Type:Level Combinations

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

Table 5-2 (Cont.) Log Levels and ODL Message Type:Level Combinations

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

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

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

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

5.3.2 Enabling Logging

Edit the logging.xml file located in the *DOMAIN_HOME*/config/fmwconfig/servers/*OIM_SERVER* directory to enable logging in Oracle WebLogic Server.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

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

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 5-2 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='OIMCP.LDAP' 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.LDAP" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="OIMCP.LDAP"/>
     <handler name="console-handler"/>
   </logger>
```

With these sample values, when you use Oracle Identity Governance, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

   Replace ***FILENAME*** with the location and name of the file to which you want to redirect the output.
4. Restart the application server.

5.4 Managing Logging for the Connector Server

The conf directory contains the logging.properties file, which you can edit to meet your requirements.

The following topics provide detailed information about logging:

- Understanding Logging on the Connector Server
- Enabling Logging for the Connector Server

5.4.1 Understanding Logging on the Connector Server

When you enable logging, the connector server stores in a log file information about events that occur during the course of provisioning and reconciliation operations for different statuses. By default, the connector server logs are set at INFO level and you can change this level to any one of these.

- Error

This level enables logging of information about errors that might allow connector server 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 operation.

- FINE, FINER, FINEST

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

5.4.2 Enabling Logging for the Connector Server

Edit the logging.properties file located in the *CONNECTOR_SERVER_HOME*/Conf directory to enable logging.

To do so:

1. Navigate to the *CONNECTOR_SERVER_HOME*/Conf directory.
2. Open the logging.properties file in a text editor.
3. Edit the following entry by replacing INFO with the required level of logging:

   ```
   .level=INFO
   ```

4. Save and close the file.
5. Restart the connector server.

5.5 Localizing Field Labels in UI Forms

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

> **Note:**
>
> Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.*x* or later and you want to localize UI form field labels.

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

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:

SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf

> **Note:**
>
> You will not be able to view the BizEditorBundle.xlf unless you complete creating the application for your target system or perform any customization such as creating a UDF.

6. Edit the BizEditorBundle.xlf file in the following manner:

   a. Search for the following text:

   ```
   <file source-language="en"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   b. Replace with the following text:

   ```
   <file source-language="en" target-language="LANG_CODE"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   In this text, replace *LANG_CODE* with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

   ```
   <file source-language="en" target-language="ja"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   c. Search for the application instance code. This procedure shows a sample edit for Oracle Internet Directory application instance. The original code is:

   ```
   <trans-unit id="$
   {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
   e']
   ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
   UD_OID_USR_FNAME__c_description']}">
   <source>Username</source>
   </target>
   </trans-unit>
   <trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.adform.entity.oidformEO.U
   D_OID_USR_FNAME__c_LABEL">
   <source>Username</source>
   </target>
   </trans-unit>
   ```

   d. Open the resource file from the connector package, for example OID_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_OID_USR_FNAME=\u540D.

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

   ```
   <trans-unit id="$
   {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
   e']
   ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
   UD_OID_USR_FNAME__c_description']}">
   <source>Username</source>
   <target>\u30E6\u30FC\u30B6\u30FC\u540D</target>
   ```

```
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.OracleDBForm.entity.OracleDBFor
m.UD_OID_USR_FNAME__c_LABEL">
<source>Username</source>
<target>\u30E6\u30FC\u30B6\u30FC\u540D</target>
</trans-unit>
```

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

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

   Sample file name: BizEditorBundle_ja.xlf.

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

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

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

5.6 Configuring the IT Resource for the Connector Server

If you have used the Connector Server, then you must configure values for the parameters of the Connector Server IT resource.

After you create the application for your target system, you must create an IT resource for the Connector Server as described in Creating IT Resource of *Oracle Fusion Middleware Administering Oracle Identity Governance*. While creating the IT resource, ensure to use to select **Connector Server** from the **IT Resource Type** list.

In addition, specify values for the parameters of the IT resource for the Connector Server listed in Table 5-3.

Table 5-3 Parameters of the IT Resource for the LDAP Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. Sample value: `myhost.com`
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. By default, this value is blank. You must enter the port number that is displayed on the terminal when you start the Connector Server. For example: `8759`
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Governance times out. Recommended value: `0` A value of 0 means that the connection never times out.

Table 5-3 (Cont.) Parameters of the IT Resource for the LDAP Connector Server

Parameter	Description
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter `false`. Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see Configuring the Java Connector Server with SSL for Oracle Identity Governance in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

5.7 Configuring SSL for the Connector

You must configure SSL to secure communication between Oracle Identity Governance and your target system.

This section provides information about configuring SSL for the connector:

- Configuring SSL on the Target System
- Configuring Oracle Identity Governance for SSL

Caution:

Configuring SSL is an optional procedure; however, it is recommended that you configure SSL. If you do not configure SSL, passwords can be transmitted over the network in clear text. For example, this problem can occur when you are creating a user or modifying a user's password.

5.7.1 Configuring SSL on the Target System

Configuring SSL on the target system involves generating a certificate and exporting its public key, and then importing the certificate into the JRE of the target system.

1. On the target system, ensure that SSL is enabled and a port is specified for the Directory Server to accept connections from LDAPS clients.

   For more information, refer to the documentation for your specific target system .

2. Generate a self-signed certificate.
3. Export the public key for the certificate you generated in the previous step.

   For example, on an OUD target system:

   ```
   keytool -exportcert -alias server-cert -file config/server-cert.txt -rfc
   -keystore config/keystore -storetype JKS
   ```

   Or, on an ODSEE target system:

   ```
   odsee-instance/bin/dsadm export-cert -o /tmp/odsee.cert . defaultCert
   ```

   Or, on an eDirectory target system, you can export the trust certificate from the JDK key store on which eDirectory is installed:

```
keytool -J-ns -import -alias ALIAS_NAME -file FULL_PATH\trustedrootcert.der -
keystore sys:java\lib\security\cacerts
```

Choose and confirm the PKCS#12 file password.

4. Import the server certificate into the JRE of the target system.

   For example, on an OUD target system:

   ```
   keytool -importcert -alias server-cert -file config/server-cert.txt
   -keystore config/truststore -storetype JKS
   ```

5.7.2 Configuring Oracle Identity Governance for SSL

Configuring SSL on Oracle Identity Governance involves importing the target system certificate into both the JDK used by Oracle Identity Governance and Oracle WebLogic Server keystore.

1. Import the target system certificate into the JDK (or JRE) used by Oracle Identity Governance. For example:

   ```
   keytool -import -keystore my_cacerts -file cert_file_name -storepass password
   ```

   In this command:

   - *my_cacerts* is the full path and name of the certificate store (the default is cacerts).
   - *cert_file_name* is the full path and name of the certificate file.
   - *password* is the password of the keystore.

   For example:

   ```
   keytool -import -keystore /home/OIM/java/jdk/lib/security/cacerts
   -file /home/target.cert -storepass kspassword
   ```

2. Import the target system certificate into the Oracle WebLogic Server keystore. For example:

   ```
   keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks
   -file cert_file_name -storepass password
   ```

   In this command:

   - *cert_file_name* is the full path and name of the certificate file.
   - *password* is the password of the keystore.

   For example:

   ```
   keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks
   -file /home/target.cert -storepass DemoTrustKeyStorePassPhrase
   ```

6 Using the Oracle Internet Directory Connector

You can use the Oracle Internet Directory connector for performing reconciliation and provisioning operations after configuring your application to meet your requirements.

6.1 Guidelines on Using the Connector

These are the guidelines that you must apply while configuring reconciliation, performing provisioning operations, and using the connector for dynamic or virtual static groups.

6.1.1 Guidelines on Configuring Reconciliation

These are the guidelines that you must apply while configuring reconciliation.

- Before a target resource reconciliation run is performed, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled jobs for lookup field synchronization must be run before user reconciliation runs.
- The scheduled job for user reconciliation must be run before the scheduled job for reconciliation of deleted user data.
- There is no support for group entities in Oracle Identity Governance. Therefore, apply the following guidelines before you run the scheduled job for groups reconciliation:
  - If you are using the default connector configuration, for every group in the target system, create a corresponding organizational unit (with the same group name) in

Oracle Identity Governance. This ensures that all groups from the target system are reconciled into their newly created organizational units, respectively.

  - You can also configure the connector to reconcile groups under one organization. See Reconciling OID, OUD, and ODSEE Groups Under One Organization in Oracle Identity Governance.

- For OUD target system, the OUD changelog is based on the replication database. By default, the replication keeps changelog entries for only 100 hours. The replication purge delay must be tuned based on your specific requirements. The database size on disk will vary accordingly. For more information, see the changelog documentation for the OUD target system.
- Reconciliation of roles is supported only for ODSEE target system.
- Run the User Search Reconciliation scheduled job, if only changes with regard to group membership are made to a user. This is because neither the changelog nor modifiedTimestamp attribute is updated. Therefore, performing full reconciliation by running the User Search Reconciliation scheduled job should reconcile such changes.
- If you are reconciling a large number of records for an OID target system, then you must specify values for the following advanced settings parameters to optimize performance:
  - **For target resource configuration**

    Change or increase the values of the blockSize and changeLogBlockSize parameters to suit the requirements of your environment.

    Specify values for the readTimeout and connectTimeout parameters. If these parameters are not available in the Advanced Settings section, then you can manually add these parameters by updating the xml/OID-target-template.xml file as described in Configuring the Connector for LDAP Operation Timeouts.
  - **For trusted source configuration**

    Set the value of the usePagedResultControl parameter to `true`.

6.1.2 Guidelines on Performing Provisioning Operations

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

- Before you perform provisioning operations, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled tasks for lookup field synchronization must be run before provisioning operations.
- If you want to provision a User, Group, Role, or an Organizational Unit directly under base context, then set the baseContexts basic configuration parameter to the base context name.

  Sample value: `dc=example,dc=com`
- On the Oracle Internet Directory target system, the Manager Name field accepts only DN values. Therefore, when you set or modify the Manager Name field in Oracle Identity Governance, you must enter the DN value.

  For example: `cn=abc,ou=lmn,dc=corp,dc=com`
- Provisioning of roles is supported only for ODSEE target system.

- You perform Group provisioning in Oracle Identity Governance by provisioning the `LDAP Group` resource object to the Oracle Identity Governance organization. The connector uses `groupOfUniqueNames` as the object class for groups.
- You perform Organizational unit provisioning in Oracle Identity Governance by provisioning the `LDAP Organisation Unit` resource object to the Oracle Identity Governance organization. The connector uses the `organizationalUnit` object class for organizational unit provisioning.

6.1.3 Guidelines on Using the Connector for Dynamic and Virtual Static Groups

This connector does not support dynamic and virtual static groups in LDAP, by default. If you want to use the connector for dynamic or virtual static groups, then you must apply these guidelines.

- Ensure referential integrity in OUD is enabled.
- Set the value of the maintainLdapGroupMembership advanced settings parameter to `false`.

6.2 Configuring Reconciliation

Reconciliation involves duplicating in Oracle Identity Governance the creation of and modifications to user accounts on the target system.

This section provides details on the following topics related to configuring reconciliation:

- Performing Full and Incremental Reconciliation
- Performing Limited Reconciliation

> **Note:**
>
> Consider this scenario. You provision a user to an organization (org1) and then move the user to a second organization (org2). You run Trusted Reconciliation and Target User Sync reconciliation. As result, two resources are attached to the user: revoked and provisioned.
>
> This behavior is normal for the connector. After moving the user to org2, the target directory considers the user in org1 to be deleted (revoked) even though the user still exists in org1. However, in org2 the user also exists and is considered to be provisioned.

6.2.1 Performing Full and Incremental Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Governance. During incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance.

After you deploy the connector, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Governance.

Full reconciliation: To perform a full reconciliation run, ensure that a value is **not** specified for the Filter and Latest Token attributes of the search reconciliation scheduled job for users, groups, or roles.

Incremental reconciliation: If the target system supports changelog, Sync reconciliation can be used for performing incremental reconciliation. To perform an incremental reconciliation run, specify a value for the Sync Token attribute in the sync reconciliation scheduled job for users, groups, or roles. From the next run onward, only records created or modified after the value in the Sync Token attribute are considered for reconciliation.

Incremental reconciliation can also be performed by filtered search based on the modifyTimestamp value. The timestamp value is updated in the search reconciliation scheduled task after full reconciliation. From the next run onward, the task runs in incremental reconciliation mode.

> **Note:**
>
> As a pre-requisite, configure **modifyTimeStamp** as an indexed and searchable attribute.

See Reconciliation Jobs for OID and Reconciliation Jobs for OUD, ODSEE, and LDAPv3-Compliant Directory Server for information about these reconciliation jobs.

6.2.2 Performing Limited Reconciliation

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.

The following are the ways in which limited reconciliation can be achieved:

- Performing Limited Reconciliation By Using Filters
- Performing Limited Reconciliation Based on Group Membership

6.2.2.1 Performing Limited Reconciliation By Using Filters

You can perform limited reconciliation by creating filters for the reconciliation module, and reconcile records from the target system based on a specified filter criterion.

This connector provides a Filter attribute (a scheduled task attribute) that allows you to use any of the OID resource attributes to filter the target system records.

For detailed information about ICF Filters, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

While creating the application, follow the instructions in Configuring Reconciliation Jobs to specify attribute values.

6.2.2.2 Performing Limited Reconciliation Based on Group Membership

Limited Reconciliation can be performed based on Group Membership. You can reconcile only the users associated with a particular group by configuring the filter.

- For ODSEE and OUD:
  - Set the `ldapGroupFilterBehavior` advanced settings parameter to `accept`.
  - Set the `ldapGroupMembershipAttribute` advanced settings parameter to `ismemberof`.

  Specify the filter as:

  ```
  containsAllValues('ldapGroups','cn=grp1,ou=groups,dc=example,dc=com')
  ```
- For OID:
  - Set the `ldapGroupFilterBehavior` advanced settings parameter to `ignore`.
  - Set the `ldapGroupMembershipAttribute` advanced settings parameter to `ismemberof`.

  Specify the filter as:

  ```
  containsAllValues('ldapGroups','cn=grp1,ou=groups,dc=example,dc=com')
  ```

In these examples, grp1 is the group with which users are associated.

6.3 Reconciling Newly Created Objects for OUD Release 11.1.1.5.0

If you create a new object (User, OU, or Group) on OUD release 11.1.1.5.0 and run a search reconciliation job with modifyTimestamp in Incremental Recon Attribute, the reconciliation events are not created for new objects. To reconcile newly created objects, you must perform full reconciliation with createTimestamp in Incremental Recon Attribute.

To create a new reconciliation job for reconciling newly created objects separately:

1. Using Identity Self Service, create a new full reconciliation job.
2. Set the **Job Name** depending on the object type that you want to reconcile (User, OU, or Group). For example, `OUD New Users Search Reconciliation`.
3. Set the **Object Type** to `User`, `OU` or `Group`, depending on the object type you want to reconcile.
4. Add the `Incremental Recon Attribute` parameter and set the value to `createTimestamp`.
5. Add the `Scheduled Task Name` parameter and set the value to the job name that you specified in Step 2.
6. Add the `Filter` and `Latest Token` parameters depending on your requirements.
7. Click **Apply** to save the job.

> **See Also:**
>
> Updating Reconciliation Jobs in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for instructions on creating a new reconciliation job

6.4 Reconciling OID, OUD, and ODSEE Users Under Their Corresponding Organizations in Oracle Identity Governance

Perform this optional task to reconcile users from the OID, OUD, or ODSEE target system under their corresponding organizations in Oracle Identity Governance. You do so by updating the default schema that has been set for an authoritative application.

To reconcile users from the OID, OUD, or ODSEE target system under their corresponding organizations in Oracle Identity Governance:

1. Ensure that you have created the corresponding organizations with the same names from the target system in Oracle Identity Governance.

   You create an organization from the Create Organization page in Identity Self Service.

2. In LDAP Trusted User Schema Attributes on the Schema page, update the value of the `Organization Name` identity attribute. To do so, in the Target Attribute column corresponding to the `Organization Name` identity attribute, enter `__PARENTRDNVALUE__`.

> **See Also:**
>
> Creating an Organization in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

6.5 Reconciling OID, OUD, and ODSEE Groups Under One Organization in Oracle Identity Governance

Perform this task to reconcile groups from the OID, OUD, or ODSEE target system under the corresponding organization in Oracle Identity Governance.

1. Log in to Oracle Identity Manager Design Console.

2. Depending on the target system you are using, edit the lookup definition as follows:

   For OID: Search for and add the following entry in the **Lookup.OID.Group.Configuration** lookup definition:

   - **code**: `Recon Attribute Defaults`
   - **decode**: `Lookup.OID.Group.Defaults`

   For OUD and ODSEE: Search for and add the following entry in the **Lookup.LDAP.Group.Configuration** lookup definition:

- **code**: `Recon Attribute Defaults`
- **decode**: `Lookup.LDAP.Group.Defaults`

The specified decode values are examples, and you can set your own lookup names.

3. Depending on the target system you are using, create a new lookup definition:
   - **For OID**: `Lookup.OID.Group.Defaults`
   - **For OUD and ODSEE**: `Lookup.LDAP.Group.Defaults`
4. Add the following entry:
   - **code**: `Org Name`
   - **decode**: `Group1`

   The specified decode value is an example of the name of the Oracle Identity Governance organization under which all groups need to be reconciled.
5. Depending on the target system you are using, search for the lookup definition:
   - **For OID**: **Lookup.OID.Group.ReconAttrMap**
   - **For OUD and ODSEE**: **Lookup.LDAP.Group.ReconAttrMap**
6. Delete the row with the code **Org Name**.
7. Depending on the target system you are using, search for and edit one of the following reconciliation rule:
   - **For OID**: **OID Group Recon**
   - **For OUD and ODSEE**: **LDAP Group Recon**
8. Change the current rule **Organization Name Equals Group Name** to **Organization Name Equals Org Name**.
9. Double-click the rule element and change the attribute **Group Name** to **Org Name**.
10. Save the rule.
11. Depending on the target system you are using, open one of the following resource objects and click **Create Reconciliation Profile**.
    - **For OID**: **OID Group**
    - **For OUD and ODSEE**: **LDAP Group**
12. Create an organization with the organization name `Group1`.

    You create an organization from the Create Organization page in Identity Self Service.
13. Depending on the target system you are using, run one of the following reconciliation jobs:
    - **For OID**: OID Connector Group Search Recon job
    - **For OUD and ODSEE**: LDAP Connector Group Lookup Reconciliation job

    After the job is complete, all groups are reconciled from the target system into the **Group1** organization in Oracle Identity Governance. You can view the entitlements published to the open organization on the Available Entitlement tab in Identity Self Service.

> **See Also:**
>
> - Creating an Organization in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for instructions on creating organizations in Oracle Identity Governance
> - Parameters of the Reconciliation Jobs for Entitlements for details about the parameters of the LDAP Connector Group Lookup Reconciliation job
> - Configuring Reconciliation Jobs for instructions on performing reconciliation runs

6.6 Reconciling ODSEE Roles Under One Organization in Oracle Identity Governance

Perform this task to configure ODSEE roles to be reconciled under one organization.

1. Log in to the Oracle Identity Manager Design Console.
2. Search for the **Lookup.LDAP.Role.Configuration** lookup definition, and add the following entry:
   - **code**: Recon Attribute Defaults
   - **decode**: Lookup.LDAP.Role.Defaults

   The specified decode value is an example, and you can set your own lookup name.
3. Create a new lookup definition with the name **Lookup.LDAP.Role.Defaults**, and add the following entry:
   - **code**: Org Name
   - **decode**: Role1

   The decode value is an example of the name of the Oracle Identity Governance organization under which all roles need to be reconciled.
4. Search for the **Lookup.LDAP.Role.ReconAttrMap** lookup definition, and delete the row with code **Org Name**.
5. Search for and edit the reconciliation rule **LDAP Role Recon**:
   a. Change the current rule **Organization Name Equals Role Name** to **Organization Name Equals Org Name**.
   b. Double-click the rule element and change the attribute **Role Name** to **Org Name**.
   c. Save the rule.
6. Open the **LDAP Role** resource object and click **Create Reconciliation Profile**.
7. Create an organization with the organization name **Role1**.

   You create an organization from the Create Organization page in Identity Self Service.
8. Run the LDAP Connector Role Search Reconciliation job.

After the job is complete, all roles are reconciled from the target system into the **Role1** organization in Oracle Identity Governance. You can view the entitlements published to the open organization on the Available Entitlement tab in Identity Self Service.

> **See Also:**
>
> - Creating an Organization in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for instructions on creating organizations in Oracle Identity Governance
> - Parameters of the Reconciliation Jobs for Entitlements for details about the parameters of the LDAP Connector Role Search Reconciliation job
> - Configuring Reconciliation Jobs for instructions on performing reconciliation runs

6.7 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

1. Log in to Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the parameters of the scheduled task:
   - **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

   In addition to modifying the job details, you can enable or disable a job.
5. On the **Job Details** tab, in the Parameters region, specify values for the attributes of the scheduled task.

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

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

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

6.8 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance:

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

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

6.9 Connector Objects Used for Groups and Organizational Units Management in OID

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

- Preconfigured Lookup Definitions for Groups Management in OID
- Preconfigured Lookup Definitions for Organizational Units Management in OID
- Reconciliation Scheduled Jobs for Groups and Organizational Units Management in OID

6.9.1 Preconfigured Lookup Definitions for Groups Management in OID

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

This section provides information about the following lookup definitions for group operations:

- Lookup.OID.Group.Configuration
- Lookup.OID.Group.ProvAttrMap
- Lookup.OID.Group.ReconAttrMap

6.9.1.1 Lookup.OID.Group.Configuration

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

Table 6-1 lists the default entries in this lookup definition.

Table 6-1 Entries in the Lookup.OID.Group.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.OID.Group.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes.
Recon Attribute Map	Lookup.OID.Group.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes.

6.9.1.2 Lookup.OID.Group.ProvAttrMap

The Lookup.OID.Group.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during group provisioning operations. This lookup definition is preconfigured.

Table 6-2 lists the default entries. You can add entries in this lookup definitions if you want to map new target system attributes for provisioning.

Table 6-2 Entries in the Lookup.OID.Group.ProvAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
Container DN[IGNORE,LOOKUP]	container
Group Name	cn
Name	__NAME__="cn=${Group_Name},${Container_DN}"
OrclGuid	__UID__

6.9.1.3 Lookup.OID.Group.ReconAttrMap

The Lookup.OID.Group.ReconAttrMap lookup definition holds mappings between resource object fields for groups and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured.

Table 6-3 lists the default entries. You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation.

Table 6-3 Entries in the Lookup.OID.Group.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
Group Name	cn
OrclGuid	__UID__
Org Name	__PARENTRDNVALUE__

6.9.2 Preconfigured Lookup Definitions for Organizational Units Management in OID

The lookup definitions for Organizational Units are automatically created in Oracle Identity Governance after you create the application by using the connector. These lookup definitions are prepopulated with values after you create the application.

This section describes the following lookup definitions for organizational unit operations:

- Lookup.OID.OU.Configuration
- Lookup.OID.OU.ProvAttrMap
- Lookup.OID.OU.ReconAttrMap

6.9.2.1 Lookup.OID.OU.Configuration

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

Table 6-4 lists the default entries in this lookup definition.

Table 6-4 Entries in the Lookup.OID.OU.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.OID.OU.ProvAttrMap	Lookup used during provisioning.
Recon Attribute Map	Lookup.OID.OU.ReconAttrMap	Lookup used during reconciliation.

6.9.2.2 Lookup.OID.OU.ProvAttrMap

The Lookup.OID.OU.ProvAttrMap lookup definition maps process form fields for organizations and target system attributes. This lookup definition is used for performing organizational unit provisioning operations.

Table 6-5 lists the organizational unit fields of the target system for which you can specify or modify values during provisioning operations.

Table 6-5   Entries in the Lookup.OID.OU.ProvAttrMap Lookup Definition

Organization Field on Oracle Identity Manager	Target System Field
Container DN[IGNORE,LOOKUP]	Not used.
Name	__NAME__="ou=${Organisation_Unit_Name},${Container_DN}"
OrclGuid	__UID__
Organisation Unit Name	ou

6.9.2.3 Lookup.OID.OU.ReconAttrMap

This lookup definition is used during reconciliation. Table 6-6 lists the entries in this lookup definition.

Table 6-6   Entries in the Lookup.OID.OU.ReconAttrMap Lookup Definition

Code Key	Decode
Container DN[LOOKUP]	__parentDN__
OrclGuid	__UID__
Organisation Unit Name	ou
Org Name	__PARENTRDNVALUE__

6.9.3 Reconciliation Scheduled Jobs for Groups and Organizational Units Management in OID

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

This topic provides information about the following scheduled jobs

- Scheduled Jobs for Reconciliation of Groups and OUs in OID
- Scheduled Jobs for Reconciliation of Deleted Groups and OUs in OID

6.9.3.1 Scheduled Jobs for Reconciliation of Groups and OUs in OID

Depending on whether you want to perform groups management or organizational units management, you must specify values for the attributes of the following scheduled jobs.

- OID Connector Group Search Reconciliation
- OID Connector Group Sync Reconciliation
- OID Connector OU Search Reconciliation
- OID Connector OU Sync Reconciliation

The following sections describe the scheduled jobs and their attributes for groups and organizational units management:

- OID Connector Group Search Reconciliation and OID Connector OU Search Reconciliation Scheduled Jobs
- OID Connector Group Sync Reconciliation and OID Connector OU Sync Reconciliation Scheduled Jobs

6.9.3.1.1 OID Connector Group Search Reconciliation and OID Connector OU Search Reconciliation Scheduled Jobs

The OID Connector Group Search Reconciliation scheduled job is used to reconcile group data from OID. Similarly, the OID Connector OU Search Reconciliation scheduled job is used to reconcile OU data from OID. You must use these scheduled jobs if either of the following conditions is true:

- Your target system does not contain a changelog attribute.
- You want to reconcile into Oracle Identity Governance changes made to group, or OU memberships on the target system.

Table 6-7 describes the attributes of these scheduled jobs.

Table 6-7 Attributes of the OID Connector Group Search Reconciliation and OID Connector OU Search Reconciliation Scheduled Jobs

Attribute	Description
Filter	Expression for filtering records that must be reconciled by the scheduled job. Sample value: `startsWith('cn','Samrole1')` Default value: None See Performing Limited Reconciliation for the syntax of this expression.
Incremental Recon Attribute	Enter the name of the target system attribute that holds the time stamp at which the last reconciliation run started. The value in this attribute is used during incremental reconciliation to determine the newest or latest record reconciled from the target system. The default value is the same for all Search Recon Tasks: `modifyTimestamp`
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile group or role data. Value: `OID Server`
Latest Token	This attribute holds the time stamp value of the Incremental Recon Attribute. **Note:** The reconciliation engine automatically enters a value for this attribute after execution. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only user accounts that have been modified after the time stamp specified as the value of this attribute are reconciled. If you want to perform a full reconciliation, clear the value in this field. Sample value: `<String>20120516115131Z</String>`

Table 6-7 (Cont.) Attributes of the OID Connector Group Search Reconciliation and OID Connector OU Search Reconciliation Scheduled Jobs

Attribute	Description

Object Type	Type of object to be reconciled.
	Depending on the scheduled job you are using, the default values are as follows:
	• For OID Connector Group Search Reconciliation
	`Group`
	• For OID Connector OU Search Reconciliation
	`OU`

Resource Object Name	Name of the resource object that is used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For OID Connector Group Search Reconciliation
	`OID Group`
	• For OID Connector OU Search Reconciliation
	`OID Organisation Unit`

Scheduled Task Name	Name of the scheduled task used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For OID Connector Group Search Reconciliation
	`OID Connector Group Search Reconciliation`
	• For OID Connector OU Search Reconciliation
	`OID Connector OU Search Reconciliation`

6.9.3.1.2 OID Connector Group Sync Reconciliation and OID Connector OU Sync Reconciliation Scheduled Jobs

The OID Connector Group Sync Reconciliation scheduled job is used to reconcile group data from OID. Similarly, the OID Connector OU Sync Reconciliation scheduled job is used to reconcile OU from the OID target system. You must use these scheduled jobs if your target system supports the changelog attribute.

Table 6-8 describes the attributes these scheduled jobs.

Table 6-8 Attributes of the OID Connector Group Sync Reconciliation and OID Connector OU Sync Reconciliation Scheduled Jobs

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile group or role data. Value: `OID Server`

Object Type	Type of object to be reconciled.
	Depending on the scheduled job you are using, the default values are as follows:
	• For OID Connector Group Sync Reconciliation
	`Group`
	• For OID Connector OU Sync Reconciliation
	`OU`

Table 6-8 (Cont.) Attributes of the OID Connector Group Sync Reconciliation and OID Connector OU Sync Reconciliation Scheduled Jobs

Attribute	Description

Resource Object Name	Name of the resource object that is used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For OID Connector Group Sync Reconciliation
	`OID Group`
	• For OID Connector OU Sync Reconciliation
	`OID Organisation Unit`

Scheduled Task Name	Name of the scheduled task used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For OID Connector Group Sync Reconciliation
	`OID Connector Group Sync Reconciliation`
	• For OID Connector OU Sync Reconciliation
	`OID Connector OU Sync Reconciliation`

Sync Token	You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time sync reconciliation is run, Sync Token is updated. Browse the changelog attribute of the target system to determine a value from the changelog that must be used to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Governance. Or, you can also leave this field blank, which causes the entire changelog to be read. This attribute stores values in the following formats: <Integer>*VALUE*</Integer> Sample value: `<Integer>476</Integer>`

6.9.3.2 Scheduled Jobs for Reconciliation of Deleted Groups and OUs in OID

Depending on whether you want to perform deleted groups reconciliation of deleted OUs reconciliation, the following scheduled jobs are available:

- OID Connector Group Search Delete Reconciliation: Use this scheduled job to reconcile data about deleted groups from the target system.
- OID Connector OU Search Delete Reconciliation: Use this scheduled job to reconcile data about deleted OUs from the target system.

Table 6-9 describes the attributes of these scheduled jobs.

Table 6-9 Attributes of the Scheduled Jobs for Deleted Groups and Organizational Units Reconciliation

Attribute	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Default value: `OID Server`

Table 6-9 (Cont.) Attributes of the Scheduled Jobs for Deleted Groups and Organizational Units Reconciliation

Attribute	Description
Object Type	This attribute holds the type of object you want to reconcile. Depending on the scheduled job you are using, the default values are as follows: • For OID Connector Group Search Delete Reconciliation: `Group` • For OID Connector OU Search Delete Reconciliation: `OU`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Depending on the scheduled job you are using, the default values are as follows: • For OID Connector Group Search Delete Reconciliation: `OID Group` • For OID Connector OU Search Delete Reconciliation: `OID OU`

6.10 Connector Objects Used for Groups, Organizational Units, and Roles Management in OUD, ODSEE, and LDAPv3-Compliant Directory Server

Learn about the objects that are used by the connector to perform organizational unit management operations such as create, update, and delete.

- Preconfigured Lookup Definitions for Groups Management in OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Preconfigured Lookup Definitions for Organizational Units Management in OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Preconfigured Lookup Definitions for Roles Management in ODSEE
- Reconciliation Scheduled Jobs for Groups, Organizational Units, and Roles Management in OUD, ODSEE, and LDAPv3-Compliant Directory Server

6.10.1 Preconfigured Lookup Definitions for Groups Management in OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

This section provides information about the following lookup definitions for group operations:

- Lookup.LDAP.Group.Configuration
- Lookup.LDAP.Group.ProvAttrMap
- Lookup.LDAP.Group.ReconAttrMap

6.10.1.1 Lookup.LDAP.Group.Configuration

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

Table 6-10 lists the default entries in this lookup definition.

Table 6-10 Entries in the Lookup.LDAP.Group.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.Group.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.Group.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.Group.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.Role.ProvAttrMap for more information about this lookup definition.

6.10.1.2 Lookup.LDAP.Group.ProvAttrMap

The Lookup.LDAP.Group.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is preconfigured and is used during group provisioning operations.

Table 6-11 lists the default entries. You can add entries in this lookup definitions if you want to map new target system attributes for provisioning.

Table 6-11 Entries in the Lookup.LDAP.Group.ProvAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
Container DN[IGNORE,LOOKUP]	container
Group Name	cn
Name	__NAME__="cn=${Group_Name},${Container_DN}"
NsuniqueID	__UID__

6.10.1.3 Lookup.LDAP.Group.ReconAttrMap

The Lookup.LDAP.Group.ReconAttrMap lookup definition holds mappings between resource object fields for groups and target system attributes. This lookup definition is preconfigured and is used during reconciliation.

Table 6-12 lists the default entries. You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation.

Table 6-12 Entries in the Lookup.LDAP.Group.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
Group Name	cn
NsuniqueID	__UID__
Org Name	__PARENTRDNVALUE__

6.10.2 Preconfigured Lookup Definitions for Organizational Units Management in OUD, ODSEE, and LDAPv3-Compliant Directory Server

The lookup definitions for Organizational Units are automatically created in Oracle Identity Governance after you create the application by using the connector. These lookup definitions are prepopulated with values after you create the application.

This section provides information about the following lookup definitions for organizational unit operations:

- Lookup.LDAP.OU.Configuration
- Lookup.LDAP.OU.ProvAttrMap
- Lookup.LDAP.OU.ReconAttrMap

6.10.2.1 Lookup.LDAP.OU.Configuration

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

Table 6-13 lists the default entry in this lookup definition.

Table 6-13 Entries in the Lookup.LDAP.OU.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.OU.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.OU.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.OU.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.OU.ReconAttrMap for more information about this lookup definition.

6.10.2.2 Lookup.LDAP.OU.ProvAttrMap

The Lookup.LDAP.OU.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is preconfigured and is used during provisioning.

Table 6-14 lists the default entries. You can add entries in this lookup definition if you want to map new target system attributes for provisioning.

Table 6-14 Entries in the Lookup.LDAP.OU.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Container DN[IGNORE,LOOKUP]	not used
Name	__NAME__="ou=${Organisation_Unit_Name},${Container_DN}"
NsuniqueID	__UID__

Table 6-14 (Cont.) Entries in the Lookup.LDAP.OU.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Organisation Unit Name	ou

6.10.2.3 Lookup.LDAP.OU.ReconAttrMap

The Lookup.LDAP.OU.ReconAttrMap lookup definition holds mappings between resource object fields for organizational units (OUs) and target system attributes. This lookup definition is preconfigured and is used during reconciliation.

Table 6-15 lists the default entries. You can add entries in this lookup definition if you want to map new target system attributes for provisioning.

Table 6-15 Entries in the Lookup.LDAP.OU.ReconAttrMap Lookup Definition

OU Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
NsuniqueID	__UID__
Organisation Unit Name	ou
Org Name	__PARENTRDNVALUE__

6.10.3 Preconfigured Lookup Definitions for Roles Management in ODSEE

The lookup definitions for Roles are automatically created in Oracle Identity Governance after you create the application by using the connector. These lookup definitions are prepopulated with values after you create the application.

This section provides information about the following lookup definitions for role operations:

- Lookup.LDAP.Role.Configuration
- Lookup.LDAP.Role.ProvAttrMap
- Lookup.LDAP.Role.ReconAttrMap

6.10.3.1 Lookup.LDAP.Role.Configuration

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

Table 6-16 Entries in the Lookup.LDAP.Role.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.Role.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.Role.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.Role.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.Role.ReconAttrMap for more information about this lookup definition.

6.10.3.2 Lookup.LDAP.Role.ProvAttrMap

The Lookup.LDAP.Role.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is preconfigured and is used during role provisioning operations.

Table 6-17 lists the default entries in this lookup definition. You can add entries in this lookup definitions if you want to map new target system attributes for provisioning.

Table 6-17 Entries in the Lookup.LDAP.Role.ProvAttrMap Lookup Definition

Role Field on Oracle Identity Manager	Target System Field
Container DN[IGNORE,LOOKUP]	not used
Name	__NAME__="cn=${Role_Name},${Container_DN}"
NsuniqueID	__UID__
Role Name	cn

6.10.3.3 Lookup.LDAP.Role.ReconAttrMap

The Lookup.LDAP.Role.ReconAttrMap lookup definition holds mappings between resource object fields for roles and target system attributes. This lookup definition is preconfigured and is used during reconciliation.

Table 6-18 lists the default entries. You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation.

Table 6-18 Entries in the Lookup.LDAP.Role.ReconAttrMap Lookup Definition

Role Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
NsuniqueID	__UID__
Org Name	__PARENTRDNVALUE__
Role Name	cn

6.10.4 Reconciliation Scheduled Jobs for Groups, Organizational Units, and Roles Management in OUD, ODSEE, and LDAPv3-Compliant Directory Server

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

This topic provides information about the following scheduled jobs:

- Scheduled Jobs for Reconciliation of Groups, OUs, and Roles in OUD, ODSEE, and LDAPv3-Compliant Directory Server
- Scheduled Jobs for Reconciliation of Deleted Groups, OUs, and Roles in OUD, ODSEE, and LDAPv3-Compliant Directory Server

6.10.4.1 Scheduled Jobs for Reconciliation of Groups, OUs, and Roles in OUD, ODSEE, and LDAPv3-Compliant Directory Server

Depending on whether you want to perform groups management or organizational units management, you must specify values for the attributes of the following scheduled jobs.

- LDAP Connector Group Search Reconciliation
- LDAP Connector Group Sync Reconciliation
- LDAP Connector OU Search Reconciliation
- LDAP Connector OU Sync Reconciliation
- LDAP Connector Role Search Reconciliation
- LDAP Connector Role Sync Reconciliation

> **Note:**
>
> The LDAP Connector Role Search Reconciliation and LDAP Connector Role Sync Reconciliation scheduled jobs are available only for ODSEE.

The following sections describe the scheduled jobs and their attributes for groups, organizational units, and roles management:

- LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Reconciliation Scheduled Jobs
- LDAP Connector Group Sync Reconciliation, LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation Scheduled Jobs

6.10.4.1.1 LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Reconciliation Scheduled Jobs

The LDAP Connector Group Search Reconciliation and LDAP Connector OU Search Reconciliation scheduled jobs are used to reconcile group and organizational unit data from OUD, ODSEE, and LDAPv3-compliant directory server target systems. The LDAP Connector Role Search Reconciliation scheduled job is used to reconcile role data from the ODSEE target system. You must use these scheduled jobs if either of the following conditions is true:

- Your target system does not contain a changelog attribute.
- You want to reconcile into Oracle Identity Governance changes made to group, OU, or role memberships on the target system.

Table 6-19 describes the attributes of these scheduled jobs.

Table 6-19 Attributes of the LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Scheduled Jobs

Attribute	Description
Filter	Expression for filtering records that must be reconciled by the scheduled job. Sample value: `startsWith('cn','Samrole1')` Default value: None See Performing Limited Reconciliation for the syntax of this expression.
Incremental Recon Attribute	Enter the name of the target system attribute that holds the time stamp at which the last reconciliation run started. The value in this attribute is used during incremental reconciliation to determine the newest or latest record reconciled from the target system. The default value is the same for all Search Recon Tasks: `modifyTimestamp`
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile group or role data. Default value: `DSEE Server`
Latest Token	This attribute holds the time stamp value of the Incremental Recon Attribute. **Note:** The reconciliation engine automatically enters a value for this attribute after execution. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only user accounts that have been modified after the time stamp specified as the value of this attribute are reconciled. If you want to perform a full reconciliation, clear the value in this field. Sample value: `<String>20120516115131Z</String>`

Object Type	Type of object to be reconciled.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Search Reconciliation
	`Group`
	• For LDAP Connector OU Search Reconciliation
	`OU`
	• For LDAP Connector Role Search Reconciliation
	`Role`

Table 6-19 (Cont.) Attributes of the LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Scheduled Jobs

Attribute	Description

Resource Object Name	Name of the resource object that is used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Search Reconciliation
	`LDAP Group`
	• For LDAP Connector OU Search Reconciliation
	`LDAP Organisation Unit`
	• For LDAP Connector Role Search Reconciliation
	`LDAP Role`

Scheduled Task Name	Name of the scheduled task used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Search Reconciliation
	`LDAP Connector Group Search Reconciliation`
	• For LDAP Connector OU Search Reconciliation
	`LDAP Connector OU Search Reconciliation`
	• For LDAP Connector Role Search Reconciliation
	`LDAP Connector Role Search Reconciliation`

6.10.4.1.2 LDAP Connector Group Sync Reconciliation, LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation Scheduled Jobs

The LDAP Connector Group Sync Reconciliation and LDAP Connector OU Sync Reconciliation scheduled jobs are used to reconcile group and organizational unit data from OUD, ODSEE, and LDAPv3-compliant directory server target systems. The LDAP Connector Role Sync Reconciliation scheduled job is used to reconcile role data from the ODSEE target system. You must use these scheduled jobs if your target system supports the changelog attribute.

Table 6-20 describes the attributes these scheduled jobs.

Table 6-20 Attributes of the LDAP Connector Group Sync Reconciliation, LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation Scheduled Jobs

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile group or role data. Value: `DSEE Server`

Object Type	Type of object to be reconciled.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Sync Reconciliation
	`Group`
	• For LDAP Connector OU Sync Reconciliation
	`OU`
	• For LDAP Connector Role Sync Reconciliation
	`Role`

Table 6-20 (Cont.) Attributes of the LDAP Connector Group Sync Reconciliation, LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation Scheduled Jobs

Attribute	Description

Resource Object Name	Name of the resource object that is used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Sync Reconciliation
	`LDAP Group`
	• For LDAP Connector OU Sync Reconciliation
	`LDAP Organisation Unit`
	• For LDAP Connector Role Sync Reconciliation
	`LDAP Role`

Scheduled Task Name	Name of the scheduled task used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Sync Reconciliation
	`LDAP Connector Group Sync Reconciliation`
	• For LDAP Connector OU Sync Reconciliation
	`LDAP Connector OU Sync Reconciliation`
	• For LDAP Connector Role Sync Reconciliation
	`LDAP Connector Role Sync Reconciliation`

Sync Token	You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time sync reconciliation is run, Sync Token is updated. Browse the changelog attribute of the target system to determine a value from the changelog that must be used to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Governance. Or, you can also leave this field blank, which causes the entire changelog to be read. This attribute stores values in one of the following formats: • If you are using a target system for which the value of the standardChangelog entry in the Configuration lookup definition is set to `true`, then this attribute stores values in the following format: <Integer>*VALUE*</Integer> Sample value: `<Integer>476</Integer>` • If you are using a target system (for example, OUD) for which the value of the standardChangelog entry in the Configuration lookup definition is set to `false`, then this attribute stores values in the following format: <String>*VALUE*</String> Sample value: `<String>dc=example,dc=com:0000013633e514427b6600000013;</String>`

6.10.4.2 Scheduled Jobs for Reconciliation of Deleted Groups, OUs, and Roles in OUD, ODSEE, and LDAPv3-Compliant Directory Server

Depending on whether you want to perform reconciliation of deleted groups, OUs, or roles, the following scheduled jobs are available:

- LDAP Connector Group Search Delete Reconciliation: Use this scheduled job to reconcile data about deleted groups from the OUD, ODSEE, or LDAPv3-compliant directory server target systems.
- LDAP Connector OU Search Delete Reconciliation: Use this scheduled job to reconcile data about deleted OUs from the OUD, ODSEE, or LDAPv3-compliant directory server target systems.
- LDAP Connector Role Search Delete Reconciliation: Use this scheduled job to reconcile data about deleted roles from the ODSEE target system.

Table 6-21 describes the attributes of these scheduled jobs.

Table 6-21 Attributes of the Scheduled Jobs for Deleted Groups and Organizational Units Reconciliation

Attribute	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Default value: `DSEE Server`
Object Type	This attribute holds the type of object you want to reconcile. Depending on the scheduled job you are using, the default values are as follows: • For LDAP Connector Group Search Delete Reconciliation: `Group` • For LDAP Connector OU Search Delete Reconciliation: `OU` • For LDAP Connector Role Search Delete Reconciliation: `Role`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Depending on the scheduled job you are using, the default values are as follows: • For LDAP Connector Group Search Delete Reconciliation: `LDAP Group` • For LDAP Connector OU Search Delete Reconciliation: `LDAP OU` • For LDAP Connector Role Search Delete Reconciliation: `LDAP Role`

6.11 Uninstalling the Connector

Uninstalling the Oracle Internet Directory connector deletes all the account-related data associated with its resource objects.

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

For example: `OID User; OID Group`

Note:

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

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

7

Extending the Functionality of the Oracle Internet Directory Connector

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

This chapter discusses the following sections:

- Adding New Multivalued Fields for Target Resource Reconciliation
- Adding New Multivalued Fields for Provisioning
- Configuring Transformation and Validation of Data
- Configuring the Connector for User-Defined Object Classes
- Configuring the Connector to Support POSIX Groups and Accounts
- Using the Enable or Disable User Accounts Feature with OpenLDAP

7.1 Adding New Multivalued Fields for Target Resource Reconciliation

You can add new multivalued fields for target resource reconciliation of users, groups, organizational units, and roles.

- Adding New Multivalued Fields for Reconciling Users from a Target Application
- Adding New Multivalued Fields for Target Resource Reconciliation of Groups, Organizational Units, and Roles

7.1.1 Adding New Multivalued Fields for Reconciling Users from a Target Application

By default, the multivalued fields listed on the Schema page for your application in Identity Self Server are mapped for reconciliation between Oracle Identity Governance and the target system. If required, you can add new multivalued fields for target resource reconciliation.

To add new multivalued fields for reconciling users from a target application (or target resource reconciliation):

1. Log in to Oracle Identity System Administration and create a lookup that can hold the list of values for the multivalued field that you want to add.
2. Create a child form and add attributes as follows:
   a. Log in to Identity Self Service.
   b. Search for and open the application you created for your target system for editing.
   c. On the Schema page, add a new child form and its attributes.

      For example, enter the following values:

- **Display Name**: `Car License`
- **Target Attribute**: `carLicense`
- Ensure that the **Recon Field** option is selected.

> **Note:**
>
> - When you add attributes to the child form, from the Advanced Settings option, ensure to mark the newly added attribute as a **Lookup**.
> - In the List of values field, enter the name of the lookup created in Step 1.

d. Apply your changes.

3. Log in to Identity System Administration, create a new form and associate it with your application.

> **See Also:**
>
> - Creating a Lookup Type in *Oracle Fusion Middleware Administering Oracle Identity Governance* for details about create lookups for your multivalued fields
> - Adding Child Forms in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for information about creating a child form and adding attributes
> - Configuring Oracle Identity Governance for information about creating a new form and associating it with your application

7.1.2 Adding New Multivalued Fields for Target Resource Reconciliation of Groups, Organizational Units, and Roles

By default, the multivalued fields listed in the respective lookup definitions are mapped for reconciliation between Oracle Identity Governance and the target system. If required, you can add new multivalued fields for target resource reconciliation of groups, organizational units, and roles.

> **Note:**
>
> - This section describes an optional procedure. Perform this procedure only if you want to add multivalued fields for target resource reconciliation.
> - You can apply this procedure to add group, organizational unit, or role fields.
> - You must ensure that new fields you add for reconciliation contain only string-format data. Binary fields must not be brought into Oracle Identity Governance natively.

To add a new multivalued field for target resource reconciliation, perform the following procedures:

- Creating a Form for the Multivalued Field
- Adding the Form as a Child Form of the Process Form
- Associating a New Form With the Application Instance
- Adding the New Multivalued Field to the Resource Object Reconciliation Fields
- Creating an Entry for the Field in the Lookup Definition for Reconciliation
- Creating a Reconciliation Field Mapping for the New Field

7.1.2.1 Creating a Form for the Multivalued Field

To create a form for the multivalued field:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools** and double-click **Form Designer**.
3. Create a form by specifying a table name and description, and then click **Save**.
4. Click **Add** and enter the details of the field.
5. Click **Save** and then click **Make Version Active**. For example:

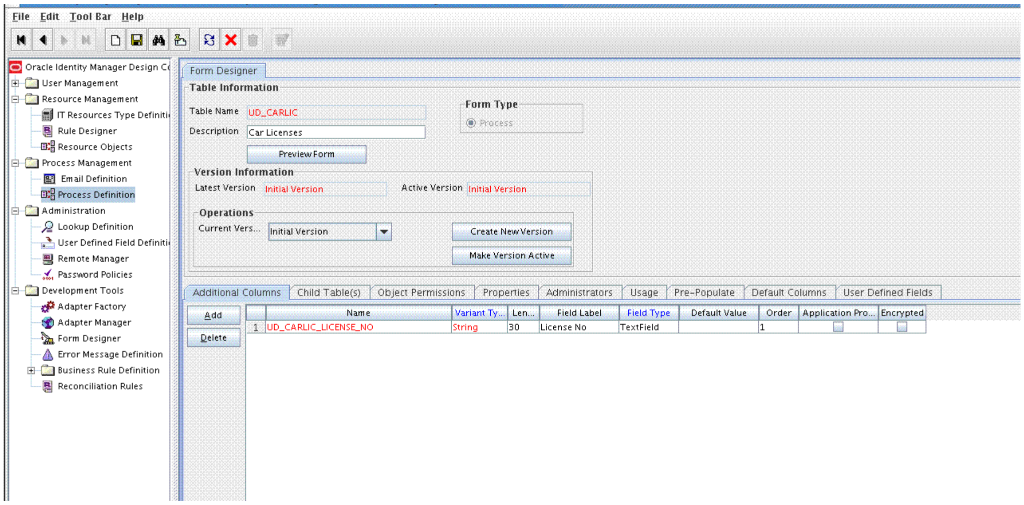


Table Information

Table Name: UD_CARLIC

Description: Car Licenses

Form Type: ● Process

Version Information

Latest Version: Initial Version

Active Version: Initial Version

Operations

Current Vers...: Initial Version

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value	Order	Application Pro...	Encrypted
1	UD_CARLIC_LICENSE_NO	String	30	License No	TextField		1	□	□

7.1.2.2 Adding the Form as a Child Form of the Process Form

Add the form created for the multivalued field as a child form of the process form.

1. Search for and open one of the following process forms:
   - For groups: **UD_LDAP_GR** or **UD_OID_GR**
   - For organizational units: **UD_LDAP_OU** or **UD_OID_OU**
   - For roles: **UD_LDAP_RL**
2. Click **Create New Version**.
3. Click the **Child Table(s)** tab.
4. Click **Assign**.
5. In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK**.
6. Click **Save** and then click **Make Version Active**. For example:

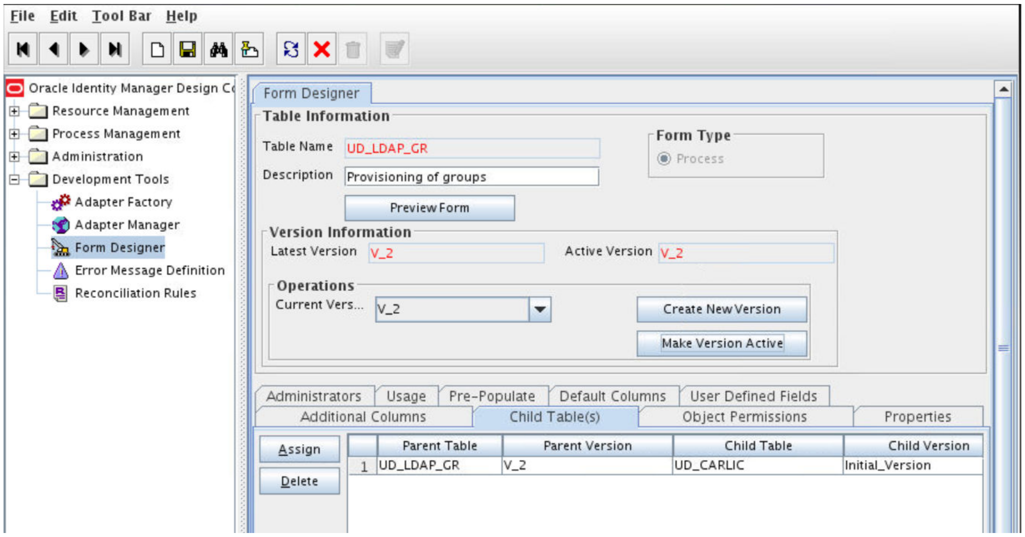


Table Name: UD_LDAP_GR

Description: Provisioning of groups

Form Type: ● Process

Latest Version: V_2

Active Version: V_2

Current Vers...: V_2

	Parent Table	Parent Version	Child Table	Child Version
1	UD_LDAP_GR	V_2	UD_CARLIC	Initial_Version

7.1.2.3 Associating a New Form With the Application Instance

If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form.

To do so:

1. Log in to Oracle Identity System Administration.
2. Create and active a sandbox.
3. Create a new UI form to view the newly added field along with the rest of the fields.
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 (created in Step 4.c), and then save the application instance.

5. Publish the sandbox.

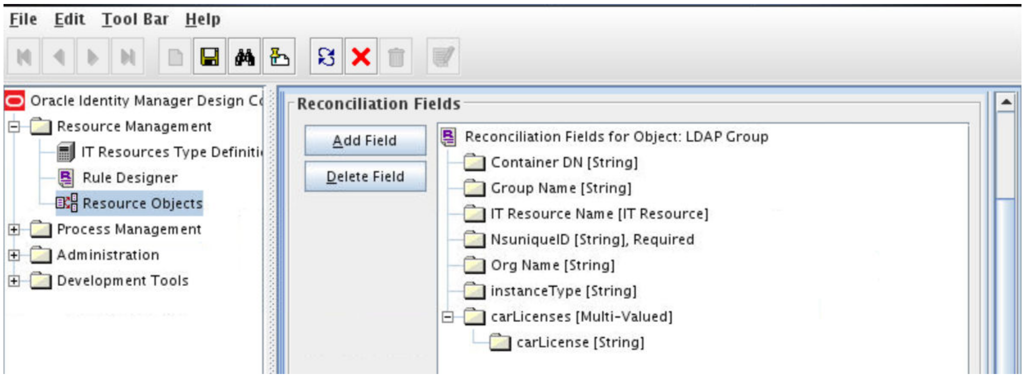
> **See Also:**
>
> - Creating a Sandbox and Activating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*
> - Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*
> - Publishing a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

7.1.2.4 Adding the New Multivalued Field to the Resource Object Reconciliation Fields

Add the new multivalued field to the list of reconciliation fields in the resource object.

1. Expand **Resource Management** and then double-click **Resource Objects**.
2. Search for and open one of the following resource objects:
   - For groups: **LDAP Group** or **OID Group**
   - For organizational units: **LDAP Organizational Unit** or **OID Organizational Unit**
   - For roles: **LDAP Role**
3. On the Object Reconciliation tab, click **Add Field**.
4. In the Add Reconciliation Fields dialog box, enter the details of the field.

   For example, enter `carlicenses` in the **Field Name** field and select **Multi-Valued Attribute** from the Field Type list.



5. Click **Save** and then close the dialog box.
6. Right-click the newly created field and select **Define Property Fields**.
7. In the Add Reconciliation Fields dialog box, enter the details of the newly created field.

   For example, enter `carlicense` in the Field Name field and select **String** from the Field Type list.

8. Click **Save**, and then close the dialog box.
9. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.

7.1.2.5 Creating an Entry for the Field in the Lookup Definition for Reconciliation

Create an entry for the newly added field in the lookup definition for reconciliation.

To do so:

1. Expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open one of the following lookup definitions:
   - For groups: **Lookup.LDAP.Group.ReconAttrMap** or **Lookup.OID.Group.ReconAttrMap**
   - For organizational units: **Lookup.LDAP.OU.ReconAttrMap** or **Lookup.OID.OU.ReconAttrMap**
   - For roles: **Lookup.LDAP.Role.ReconAttrMap**

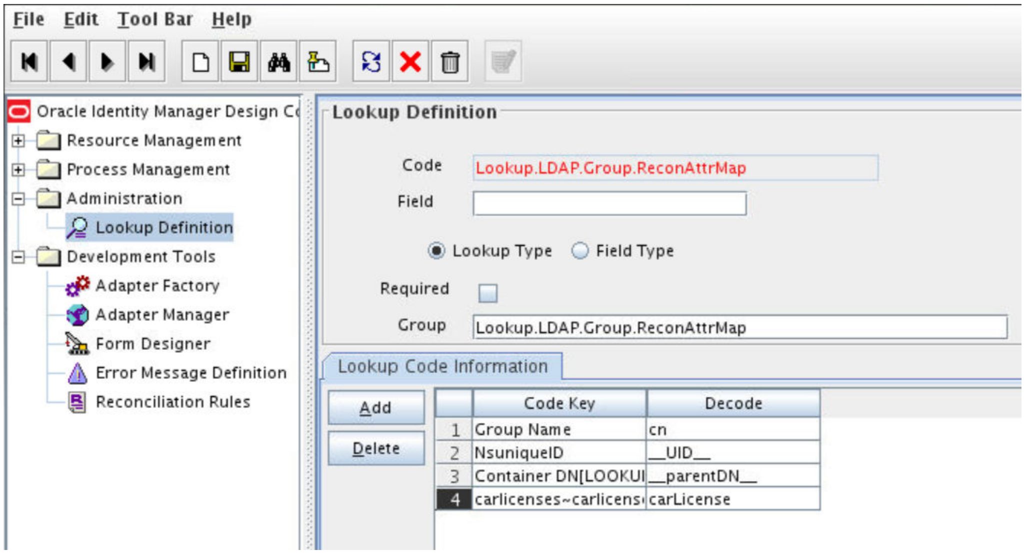
   > **Note:**
   >
   > For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

3. Click **Add** and enter the Code Key and Decode values for the field, and then Click **Save**. The Code Key and Decode values must be in the following format:

   Code Key: *MULTIVALUED_FIELD_NAME~CHILD_RESOURCE_OBJECT_FIELD_NAME*

   Decode: Corresponding target system attribute.

   For example, enter `carlicenses~carlicense` in the Code Key field and then enter `carlicense` in the Decode field.



Code: Lookup.LDAP.Group.ReconAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: Lookup.LDAP.Group.ReconAttrMap

	Code Key	Decode
1	Group Name	cn
2	NsuniqueID	__UID__
3	Container DN[LOOKUI	__parentDN__
4	carlicenses~carlicens	carLicense

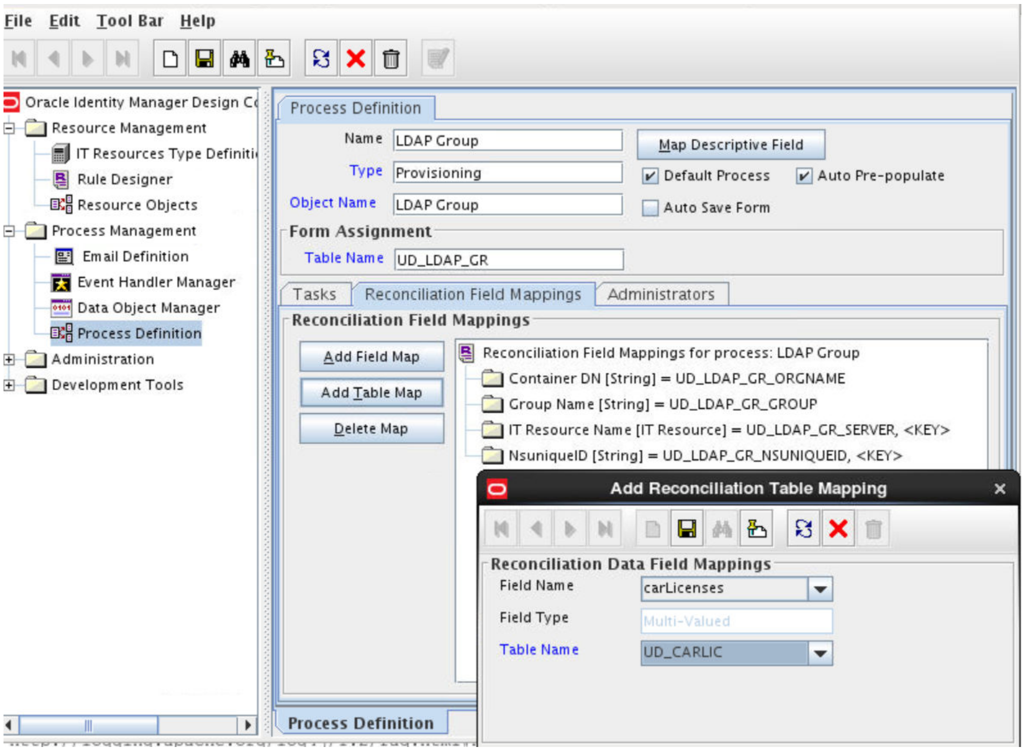
7.1.2.6 Creating a Reconciliation Field Mapping for the New Field

Create a reconciliation field mapping for the newly added field.

To do so:

1. Expand **Process Management** and double-click **Process Definition**.
2. Search for and open one of the following process definitions:
   - For groups: **LDAP Group** or **OID Group**
   - For organizational units: **LDAP Organizational Unit** or **OID Organizational Unit**
   - For roles: **LDAP Role**
3. On the Reconciliation Field Mappings tab of one of the following process definitions, click **Add Table Map**:
   - For groups: **LDAP Group** or **OID Group**
   - For organizational units: **LDAP Organizational Unit** or **OID Organizational Unit**
   - For roles: **LDAP Role**

   For example:



Name: LDAP Group
Type: Provisioning
Object Name: LDAP Group
☑ Default Process ☑ Auto Pre-populate
☐ Auto Save Form

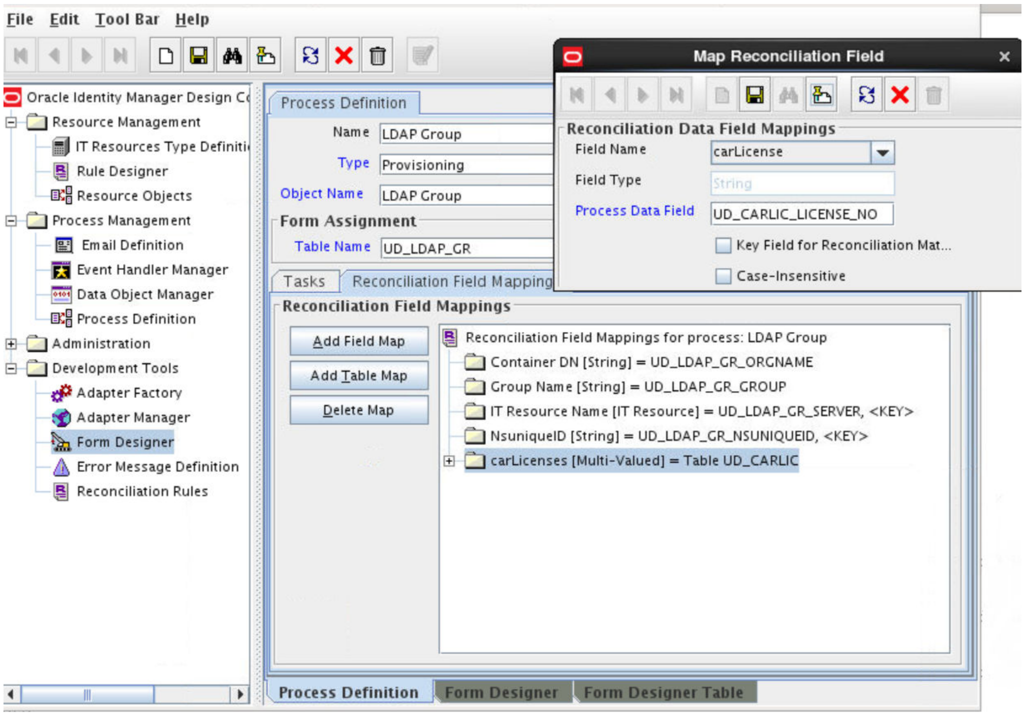
Form Assignment
Table Name: UD_LDAP_GR

Reconciliation Field Mappings
Reconciliation Field Mappings for process: LDAP Group
- Container DN [String] = UD_LDAP_GR_ORGNAME
- Group Name [String] = UD_LDAP_GR_GROUP
- IT Resource Name [IT Resource] = UD_LDAP_GR_SERVER, <KEY>
- NsuniqueID [String] = UD_LDAP_GR_NSUNIQUEID, <KEY>

Add Reconciliation Table Mapping

Reconciliation Data Field Mappings
Field Name: carLicenses
Field Type: Multi-Valued
Table Name: UD_CARLIC

4. In the Add Reconciliation Table Mapping dialog box, select the field name and table name from the list, click **Save**, and then close the dialog box. For example:



Name: LDAP Group
Type: Provisioning
Object Name: LDAP Group

Form Assignment
Table Name: UD_LDAP_GR

Map Reconciliation Field

Reconciliation Data Field Mappings
Field Name: carLicense
Field Type: String
Process Data Field: UD_CARLIC_LICENSE_NO
☐ Key Field for Reconciliation Mat...
☐ Case-Insensitive

Reconciliation Field Mappings
Reconciliation Field Mappings for process: LDAP Group
- Container DN [String] = UD_LDAP_GR_ORGNAME
- Group Name [String] = UD_LDAP_GR_GROUP
- IT Resource Name [IT Resource] = UD_LDAP_GR_SERVER, <KEY>
- NsuniqueID [String] = UD_LDAP_GR_NSUNIQUEID, <KEY>
- carLicenses [Multi-Valued] = Table UD_CARLIC

5. Right-click the newly created field, and select **Define Property Field Map**.
6. In the Field Name field, select the value for the field that you want to add.
7. Double-click the **Process Data Field** field, and then select **UD_CARLICEN**.

8. Select **Key Field for Reconciliation Field Matching** and click **Save**.

7.2 Adding New Multivalued Fields for Provisioning

You can add new multivalued fields for provisioning of users, groups, organizational units, and roles.

- Adding New Multivalued Fields for User Provisioning
- Adding New Multivalued Fields for Groups, Organizational Units, and Roles Provisioning

7.2.1 Adding New Multivalued Fields for User Provisioning

By default, the multivalued fields listed on the Schema page for your application in Identity Self Server are mapped for provisioning between Oracle Identity Governance and the target system. If required, you can add new multivalued fields for provisioning.

To add new multivalued fields for User provisioning:

1. Log in to Oracle Identity System Administration and create a lookup that can hold the list of values for the multivalued field that you want to add.
2. Create a child form and add attributes as follows:
   a. Log in to Identity Self Service.
   b. Search for and open the application you created for your target system for editing.
   c. On the Schema page, add a new child form and its attributes.

      For example, enter the following values:

      - **Display Name**: `Car License`
      - **Target Attribute**: `carLicense`
      - Ensure that the **Recon Field** option is selected.

      > **Note:**
      >
      > - When you add attributes to the child form, from the Advanced Settings option, ensure to mark the newly added attribute as a **Lookup**.
      > - In the List of values field, enter the name of the lookup created in Step 1.

   d. Apply your changes.
3. Log in to Identity System Administration, create a new form and associate it with your application.

See Also:

- Creating a Lookup Type in *Oracle Fusion Middleware Administering Oracle Identity Governance* for details about create lookups for your multivalued fields
- Adding Child Forms in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for information about creating a child form and adding attributes
- Configuring Oracle Identity Governance for information about creating a new form and associating it with your application

7.2.2 Adding New Multivalued Fields for Groups, Organizational Units, and Roles Provisioning

By default, the multivalued fields listed in the respective lookup definitions are mapped for provisioning between Oracle Identity Governance and the target system. If required, you can add new multivalued fields for provisioning of groups, organizational units, and roles.

Note:

This section describes an optional procedure. Perform this procedure only if you want to add multivalued fields for provisioning of Groups, Organizational Units, or Roles.

Before starting the following procedure, perform the procedures described in Creating a Form for the Multivalued Field through Associating a New Form With the Application Instance. If these steps have been performed while adding new multivalued fields for target resource reconciliation, then you need not repeat the steps.

To add new multivalued fields for provisioning, perform the following procedures:

- Creating an Entry for the Field in the Lookup Definition for Provisioning
- Adding the Task for Provisioning Multivalued Attributes in the Process Definition
- Updating the Request Dataset
- Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS

Note:

7.2.2.1 Creating an Entry for the Field in the Lookup Definition for Provisioning

Create an entry for the field in the lookup definition for provisioning as follows:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Administration** and double-click **Lookup Definition.**
3. Search for and open one of the lookup definitions, depending on your target system:
   - For a group field, open **Lookup.LDAP.Group.ProvAttrMap** or **Lookup.OID.Group.ProvAttrMap**
   - For a organizational unit field, open **Lookup.LDAP.OU.ProvAttrMap** or **Lookup.OID.OU.ProvAttrMap**
   - For a role field, open **Lookup.LDAP.Role.ProvAttrMap**
4. Click **Add** and then enter the Code Key and Decode values for the field. The Code Key and Decode values must be in the following format:

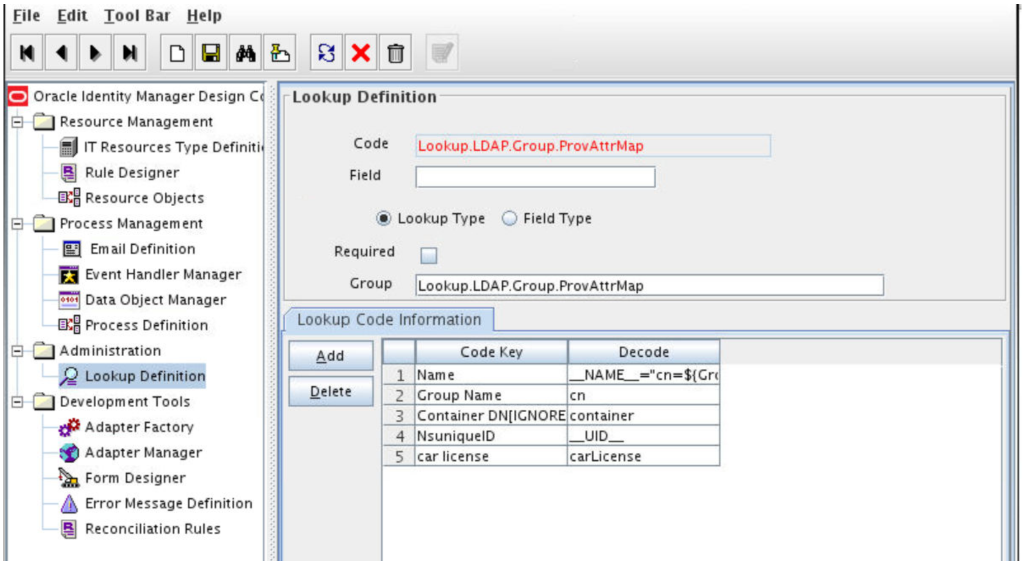
   Code Key: *CHILD_FORM_NAME~CHILD_FIELD_LABEL*

   In this format, *CHILD_FORM_NAME* specifies the name of the child form. *CHILD_FIELD_NAME* specifies the name of the field on the OIM User child form in the Administrative and User Console.

   Decode: Corresponding target system attribute

   > **Note:**
   >
   > For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

   For example, enter `UD_CARLICEN~Car License` in the **Code Key** field and then enter `carLicense` in the **Decode** field.



Lookup Definition

Code: Lookup.LDAP.Group.ProvAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: Lookup.LDAP.Group.ProvAttrMap

Lookup Code Information

	Code Key	Decode
1	Name	__NAME__="cn=${Gr
2	Group Name	cn
3	Container DN[IGNORE	container
4	NsuniqueID	__UID__
5	car license	carLicense

7.2.2.2 Adding the Task for Provisioning Multivalued Attributes in the Process Definition

To add the task for provisioning multivalued attributes in the process definition, perform the following procedures:

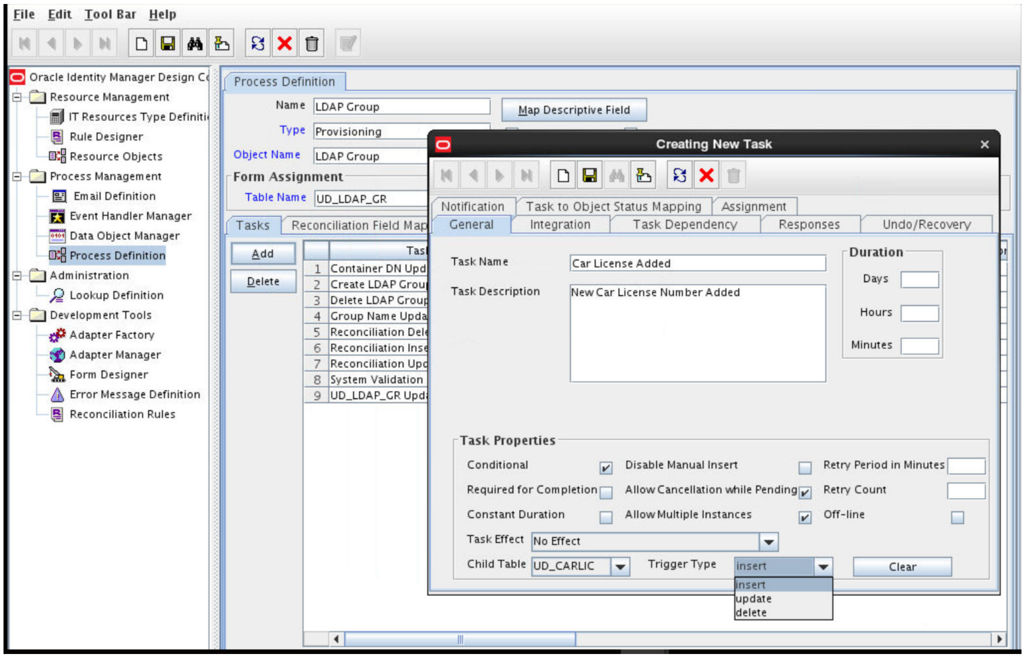
- Updating the Process Definition
- Selecting the Adapter
- Creating the Adapter Variables Mapping
- Updating the Process Tasks

7.2.2.2.1 Updating the Process Definition

In the process definition, add the task for provisioning multivalued attributes as follows:

1. Expand **Process Management**.
2. Double-click **Process Definition**.
3. Search for and open one of the following process definitions:
   - For groups: **LDAP Group** or **OID Group**
   - For organizational units: **LDAP Organizational Unit** or **OID Organizational Unit**
   - For roles: **LDAP Role**
4. Click **Add** and enter the task name and description. For example, enter `Car License Added` as the task name and task description.
5. In the Task Properties section, select the following:
   - Conditional
   - Allow cancellation while Pending
   - Allow Multiple Instances
   - **UD_CARLICEN**, to add the child table from the Child Table list
   - **Insert**, to add the data from the Trigger Type list

     For example:



Name: LDAP Group

Type: Provisioning

Object Name: LDAP Group

Table Name: UD_LDAP_GR

	Tas
1	Container DN Upd
2	Create LDAP Grou
3	Delete LDAP Group
4	Group Name Upda
5	Reconciliation Dele
6	Reconciliation Inse
7	Reconciliation Upc
8	System Validation
9	UD_LDAP_GR Upd

Task Name: Car License Added

Task Description: New Car License Number Added

Days: Hours: Minutes:

Conditional ☑ Disable Manual Insert □ Retry Period in Minutes

Required for Completion □ Allow Cancellation while Pending ☑ Retry Count

Constant Duration □ Allow Multiple Instances ☑ Off-line □

Task Effect: No Effect

Child Table: UD_CARLIC Trigger Type: insert (insert, update, delete)

6. Click **Save**.

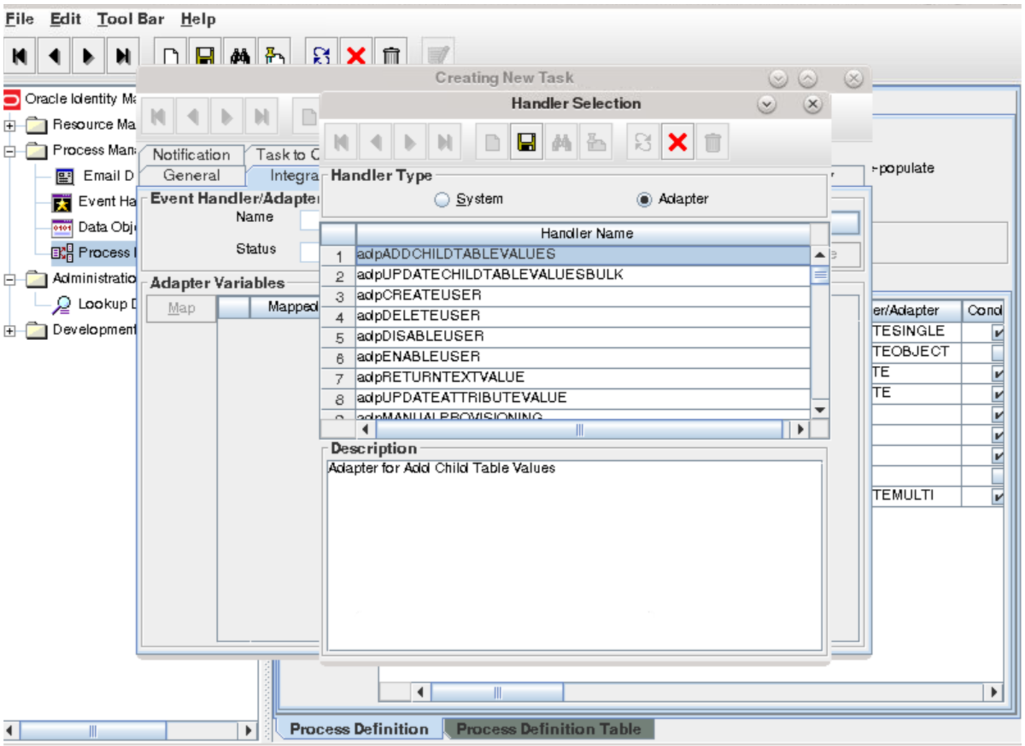
7.2.2.2.2 Selecting the Adapter

Select the adapter as follows:

1. On the Integration tab in the one of the following provisioning processes, click **Add** and then select **Adapter**:

   - For groups: **LDAP Group** or **OID Group**
   - For organizational units: **LDAP Organizational Unit** or **OID Organizational Unit**

   From the list of adapters, select **adpLDAPADDCHILDTABLEVALUE** or **adpOIDADDCHILDTABLEVALUE**.



Handler Type: ○ System ● Adapter

	Handler Name
1	adpADDCHILDTABLEVALUES
2	adpUPDATECHILDTABLEVALUESBULK
3	adpCREATEUSER
4	adpDELETEUSER
5	adpDISABLEUSER
6	adpENABLEUSER
7	adpRETURNTEXTVALUE
8	adpUPDATEATTRIBUTEVALUE
9	adpMANUALPROVISIONING

Description

Adapter for Add Child Table Values

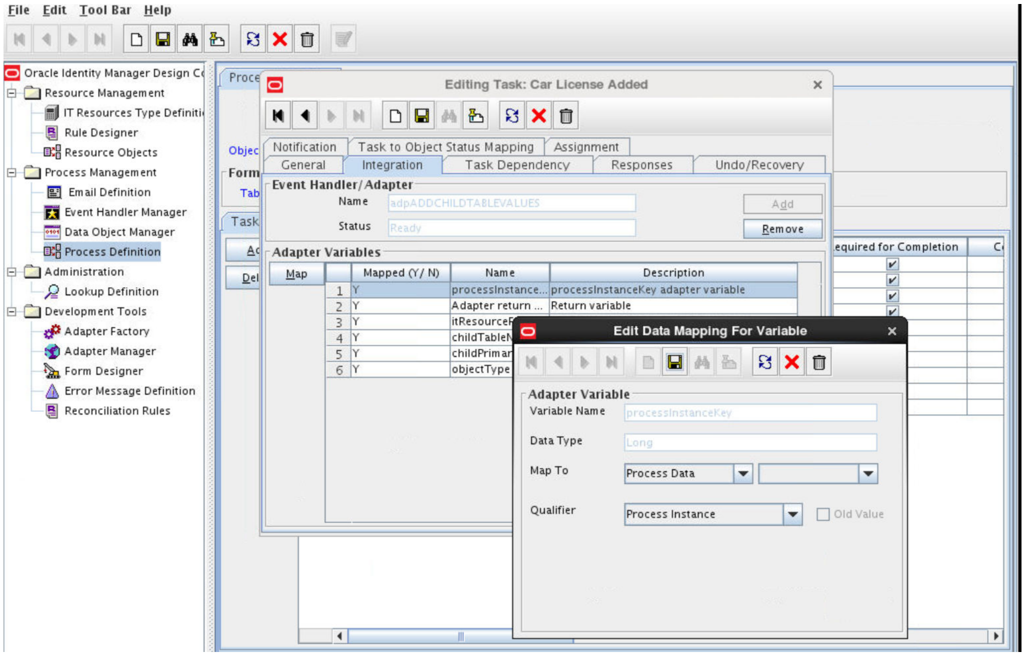
2. Click **Save** and then close the dialog box.

7.2.2.2.3 Creating the Adapter Variables Mapping

Create the adapter variables mapping as follows:

1. In the Adapter Variables region, click the **procInstanceKey** variable.
2. In the dialog box that is displayed, create the following mapping:
    - **Variable Name:** `procInstanceKey`
    - **Map To:** `Process Data`
    - **Qualifier:** `Process Instance`

   For example:



Event Handler/Adapter
Name: adpADDCHILDTABLEVALUES
Status: Ready

Adapter Variables

	Mapped (Y/ N)	Name	Description
1	Y	processInstance...	processInstanceKey adapter variable
2	Y	Adapter return ...	Return variable
3	Y	itResourceR	
4	Y	childTableN	
5	Y	childPrimar	
6	Y	objectType	

Adapter Variable
Variable Name: processInstanceKey
Data Type: Long
Map To: Process Data
Qualifier: Process Instance
□ Old Value

3. Click **Save** and close the dialog box.
4. Perform one of the following steps:

For groups:

Repeat Steps 1 through 3 for all the variables listed in the following table. This 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
procInstanceKey	Process Data	Process Instance	NA
Adapter Return Variable	Response Code	NA	NA
itResourceName	Literal	String	UD_LDAP_USR_SERVER, UD_OID_USR_SERVER, or UD_EDIR_USR_SERVER
childTableName	Literal	String	UD_*CHILD_PROCESS_FORM_NAME*
objectType	Literal	String	Group
childPrimarykey	Process Data (Child Table description)	Child Primary Key	NA

For organizational units:

Repeat Steps 1 through 3 for all the variables listed in the following table. This 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
procInstanceKey	Process Data	Process Instance	NA

Variable	Map To	Qualifier	Literal Value
Adapter Return Variable	Response Code	NA	NA
itResourceName	Literal	String	UD_LDAP_USR_SERVER, UD_OID_USR_SERVER, or UD_EDIR_USR_SERVER
childTableName	Literal	String	UD_*CHILD_PROCESS_FORM_NAME*
objectType	Literal	String	OU
childPrimarykey	Process Data (Child Table description)	Child Primary Key	NA

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

7.2.2.2.4 Updating the Process Tasks

Update the process tasks as follows:

1. Add the Car License Update process task by performing the procedures described in Updating the Process Definition through Creating the Adapter Variables Mapping with the following difference:
   - While performing Step 5 of Updating the Process Definition, instead of selecting **UD_CARLICEN** from the Child Table list, select **UD_CARLICN**. Similarly, instead of selecting **Insert** from the Trigger Type list, select **Update**.
   - While performing Step 4 of Creating the Adapter Variables Mapping, the childPrimarykey variable will not appear. Instead, map the following variable with its respective values in addition to the other variables:

Variable	Map To	Qualifier	Literal Value
taskInstanceKey	Task Information	Task Instance Key	NA

2. Add the Car License Delete process task by performing the procedures described in Updating the Process Definition through Creating the Adapter Variables Mapping with the following difference:
   - While performing Step 5 of Updating the Process Definition, instead of selecting **UD_CARLICEN** from the Child Table list, select **UD_CARLICN**. Similarly, instead of selecting **Insert** from the Trigger Type list, select **Delete**.
   - While performing Step 4 of Creating the Adapter Variables Mapping, the childPrimarykey variable will not appear. Instead, map the following variable with its respective values in addition to the other variables:

Variable	Map To	Qualifier	Literal Value
taskInstanceKey	Task Information	Task Instance Key	NA

3. Click **Save** on Process Task.

> **Note:**
>
> During a provisioning operation, you can either add or remove values of multivalued fields. You cannot update these values.

7.2.2.3 Updating the Request Dataset

Update the request dataset.

> **Note:**
>
> Perform the steps in this section and Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS only if you enabled request-based provisioning.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

1. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.
2. Add the AttributeReference element and specify values for the mandatory attributes of this element.

   For example, if you added Car License as an attribute on the process form, then enter the following line:

   ```
   <AttributeReference
   name = "Car License"
   attr-ref = "Car License"
   type = "String"
   widget = "text"
   length = "50"
   available-in-bulk = "false"/>
   ```

   In this AttributeReference element:

   - For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

     For example, if UD_CAR_LICENSE is the value in the Name column of the process form, then you must specify `Car License` as the value of the name attribute in the AttributeReference element.
   - For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form.
   - For the type attribute, enter the value that you entered in the Variant Type column of the process form.
   - For the widget attribute, enter the value that you entered in the Field Type column of the process form.
   - For the length attribute, enter the value that you entered in the Length column of the process form.

- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you add more than one attribute on the process form, then repeat this step for each attribute added.

3. Save and close the XML file.

7.2.2.4 Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS

Run the PurgeCache utility to clear content related to request datasets from the server cache.

See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about the PurgeCache utility.

Import into MDS the request dataset definitions in XML format.

7.3 Configuring Transformation and Validation of Data

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

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

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

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

7.4 Configuring the Connector for User-Defined Object Classes

By default, depending on the target system that you are using, the connector supports the Users, Groups, Organizational Units, or Roles object class. You can configure the connector for user-defined or custom object classes for connector operations.

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to configure the connector for user-defined object classes.

To configure the connector for user-defined object classes:

1. Create the object class and assign mandatory and optional attributes to the object class.

   Refer to the target system documentation for information about creating the object class.

   > **Note:**
   >
   > Assign the user object class as the parent of the object class that you create.

2. Refresh the schema.
3. Add the mandatory and optional attributes of the object class for provisioning by performing the procedure described in Providing Schema Information for Target Application or Providing Schema Information for Authoritative Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.
4. In the Advanced Settings section for your application,.
   - Update the values for the **objectClassesToSynchronize** and **accountObjectClasses** parameters to include the new object class name.
   - Set the value of the **readSchema** parameter to `true`.

7.5 Configuring the Connector for Multiple Trusted Source Reconciliation

You can configure this connector for multiple installations of the target system by cloning applications which copies all configurations of the base application into the cloned application or by creating instance applications which shares the configurations as the base application.

For more information about these configurations, see Cloning Applications and Creating Instance Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

> **Note:**
>
> Perform this procedure only if you want to configure the connector for multiple trusted source reconciliation.

The following are examples of scenarios in which there is more than one trusted source for user data in an organization:

- One of the target systems is a trusted source for data about employees. The second target system is a trusted source for data about contractors. The third target system is a trusted source for data about interns.
- One target system holds the data of some of the identity fields that constitute an OIG User. Two other systems hold data for the remaining identity fields. In other words, to create an OIM User, data from all three systems would need to be reconciled.

If the operating environment of your organization is similar to that described in either one of these scenarios, then this connector enables you to use the target system as one of the trusted sources of user data in your organization.

7.6 Configuring the Connector to Support POSIX Groups and Accounts

You can configure the connector to support POSIX groups (posixGroups) and POSIX accounts (posixAccounts).

> **Note:**
>
> You can perform this procedure only for a Target application.

After you complete this configuration:

- The connector will support POSIX groups.
- The sync reconciliation operation will not return the POSIX group membership changes. You must use the full search reconciliation task to get these changes.

To configure the connector to support POSIX groups and accounts:

1. Log in to Identity Self Service.
2. Search for and open the application you created for the connector for editing.
3. In the Advanced Settings section for your application:
   a. Set the value of the **maintainPosixGroupMembership** parameter to `true`.
   b. Update the **accountObjectClasses** parameter to include `"posixGroup","posixAccount"`.
   c. Update the **objectClassesToSynchronize** parameter to include `"posixGroup","posixAccount"`.
   d. Set the value of the **readSchema** parameter to `true`.
4. On the Schema page, update the table under the UserGroup section as follows:
   a. In the Target Attribute column, replace the **ldapGroups** value with `posixGroups`.
   b. Update the table to include the following values:

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
GID NUMBER	gidNumber	String	Yes	Yes	No	No
UID NUMBER	uidNumber	String	Yes	Yes	No	No

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
HOME DIRECTORY	homedirectory	String	Yes	Yes	No	No

c. Save your changes.

5. Log in to Oracle Identity Design Console.
6. In the **Lookup.LDAP.Group.ProvAttrMap** and **Lookup.LDAP.Group.ReconAttrMap** lookup definitions, add the following mapping as a String:

   GID NUMBER to gidNumber

   For OID, update the **Lookup.OID.Group.ProvAttrMap** and **Lookup.OID.Group.ReconAttrMap** lookup definitions.
7. In the **LDAP Group**, **OID Group**, or **eDirectory Group** resource object, add the GID NUMBER field as follows:

   Select the group (**LDAP Group**, **OID Group**), **Object Reconciliation**, **Add Field**, and then add GID NUMBER.
8. In the **LDAP Group**, **OID Group**, process form, add the GID NUMBER field.
9. In the **LDAP Group**, **OID Group**, process definition, add the mapping as a String for GID Number.
10. After you are finished, click **Create Reconciliation Profile**.

7.7 Using the Enable or Disable User Accounts Feature with OpenLDAP

Perform these steps in OpenLDAP to use the enable or disable user accounts feature with OpenLDAP.

1. Ensure you have the following entries in /etc/openldap/slapd.conf:

```
include         /etc/openldap/schema/ppolicy.schema
modulepath /usr/lib64/openldap
moduleload ppolicy.la
overlay ppolicy
ppolicy_default "cn=default,ou=Password
Policies,dc=example,dc=com"
ppolicy_use_lockout
```

2. Restart OpenLDAP.

   /etc/rc.d/init.d/ldap restart
3. Create new file named /tmp/policy.ldif with the following content and modify it as needed:

```
# add default policy to DIT
# attributes preceded with # indicate the defaults and
# can be omitted
# passwords must be reset every 30 days,
# have a minimum length of 6 and users will
# get a expiry warning starting 1 hour before
# expiry, when the consecutive fail attempts exceed 5
# the count will be locked and can only be reset by an
# administrator, users do not need to supply the old
# password when changing
dn: cn=default,ou=Password Policies,dc=example,dc=com
objectclass: top
objectclass: person
objectClass: pwdPolicy
cn: default
pwdMaxAge: 2592000
#pwdExpireWarning: 3600
#pwdInHistory: 0
#pwdCheckQuality: 0
pwdMaxFailure: 5
pwdLockout: TRUE
#pwdLockoutDuration: 0
#pwdGraceAuthNLimit: 0
#pwdFailureCountInterval: 0
pwdMustChange: TRUE
pwdMinLength: 6
#pwdAllowUserChange: TRUE
pwdSafeModify: FALSE
pwdAttribute: userPassword
sn: default
```

4. Import the policy to OpenLDAP. For example:

```
ldapmodify -D cn=admin,dc=example,dc=com -W -a -f /tmp/policy.ldif
```

5. Set the following advanced settings configuration values:

```
enabledAttribute=pwdAccountLockedTime
enabledValue=dummy
disabledValue=000001010000Z
enabledWhenNoAttribute=true
allowOtherValuesForEnabledAttribute=true
enabledWhenOtherValue=false
```

> **Note:**
>
> Enabling or disabling a user account might be server-specific. If you are using another LDAPv3-compliant directory server, check how this feature is implemented for that server.
>
> The connector behavior can be configured using the advanced settings parameters that are mentioned in Step 5, such as enabledAttribute, enabledValue, disabledValue, enabledWhenNoAttribute, allowOtherValuesForEnabledAttribute, and enabledWhenOtherValue.

8

Upgrading the Oracle Internet Directory Connector

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

- If you have deployed the 9.0.4.14 or earlier version of the Oracle Internet Directory connector, you must first upgrade the connector to version 11.1.1.5.0. See Upgrading the Connector in *Oracle Identity Manager Connector Guide for Oracle Internet Directory*.
- Before you perform the upgrade procedure:
  - It is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
  - As a best practice, perform the upgrade procedure in a test environment initially.

The following sections discuss the procedure to upgrade the connector:

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

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

8.1 Preupgrade Steps

Preupgrade steps involve performing a reconciliation run, defining the source connector, and disabling all the scheduled tasks.

Perform the following preupgrade steps:

1. Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
2. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector.
3. If required, create the connector XML file for a clone of the source connector.
4. Disable all the scheduled tasks.

8.2 Upgrade Steps

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

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

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.

  > **Note:**
  >
  > Do not upgrade IT resource type definition. In order to retain the default setting, you must map the IT resource definition to "None".

- Production Environment

  Perform the upgrade procedure by using the silent mode.

See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the wizard and silent modes.

8.3 Postupgrade Steps

Postupgrade steps involve uploading new connector JARs, configuring the upgraded IT resource of the source connector, updating the Connector Server JARs, configuring the latest token and sync token values of the scheduled job, and deleting duplicate entries for lookup definitions.

Perform the following postupgrade steps:

1. Upload new connector JARs as follows:
   a. Run the Upload JARs utility ($*ORACLE_HOME*/bin/UploadJars.sh) for uploading connector JARs.
   b. Upload bundle/org.identityconnectors.ldap-12.3.0.jar as ICFBundle.
   c. Upload OID-oim-integration.jar and TrustedUserIdTransformation.jar as JavaTask.
2. Replicate all changes made to the Form Designer of the Design Console in a new UI form as follows:
   a. Log in to Oracle Identity System Administration.
   b. Create and activate a sandbox.
   c. Create a new UI form to view the upgraded fields.
   d. 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 (created in Step 2 c) and then save the application instance.
   e. Publish the sandbox.

3. Configure the upgraded IT resource of the source connector.
4. If you are using the Connector Server, update the Connector Server JARs as follows:
   a. Navigate to the bundles directory in your Connector Server directory, and replace the existing connector server bundle JAR with the new JAR.
   b. Restart the Connector Server.
5. Configure the Latest Token and Sync Token values for the following scheduled jobs:

   For OID:

   - OID Connector User Search Reconciliation
   - OID Connector User Sync Reconciliation
   - OID Connector Trusted User Reconciliation

   For OUD, ODSEE, and LDAPv3-compliant directory server:

   - LDAP Connector User Search Reconciliation
   - LDAP Connector User Sync Reconciliation
   - LDAP Connector Trusted User Reconciliation

   After upgrading the connector, you can perform either full reconciliation or incremental reconciliation. This ensures that records created or modified since the last reconciliation run are fetched into Oracle Identity Manager. From the next reconciliation run onward, the reconciliation engine automatically enters a value for the Latest Token and Sync Token attributes.
6. If any of the previous connector artifacts are retained after a successful upgrade operation, then log in to Oracle Identity Manager Design Console and delete duplicate entries for the following lookup definitions:
   - Lookup.LDAP.Configuration
   - Lookup.LDAP.Configuration.Trusted
   - Lookup.LDAP.OUD.Configuration
   - Lookup.LDAP.OUD.Configuration.Trusted

> **See Also:**
>
> - Configuring Oracle Identity Governance for information about creating, activating, and publishing a sandbox, and creating a new UI form
> - Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about deploying the Connector Server
> - Configuring Reconciliation for more information about performing full or incremental reconciliation

9 Troubleshooting

This chapter provides solutions to problems you might encounter with the Oracle Internet Directory connector.

Table 9-1 Troubleshooting for the OID Connector

Problem	Solution
User Sync Reconciliation initiation fails against OUD 11.1.1.5.0 with an error message. For example: `Can not use cookie based sync strategy because control 1.3.6.1.4.1.26027.1.5.4 is not supported for OUD`	This problem can be caused by either: • You are not using OUD Release 2 or later. Upgrade to supported release of OUD, as listed in Certified Components. • You did not enable the changelog. The OUD changelog is automatically enabled when enabling replication.

The OID Connector Group Search Delete Reconciliation job fails with the following error message:
`java.lang.IllegalArgumentException: The method is only for single value attributes`
	This problem can be caused if more than one group name is preconfigured for the `cn` field on the OID target system. For example:
	`OracleDASEditGroup` and `OracleResourceAccessGroup`
	or
	`OracleDASEditGroup` and `oraclemanageextendedpreferences`
	Before running the OID Connector Group Search Delete Reconciliation job, you must remove additional `cn` entries from the OID target system and ensure that only one group name is configured.

Multiple reconciliation events are generated during reconciliation of groups that are deleted and then created again on the target system. For example: 1. Create two groups in the target system, create similar organizations in Oracle Identity Governance, and then run group reconciliation. The events are linked. 2. Delete the two groups and run group delete reconciliation. The events are linked and then revoked. 3. Create the same two groups in the target system again and run target reconciliation. Result: Four reconciliation events are created for the two groups (two reconciliation events per group). Two events are linked, and two are not linked.	This result is the expected behavior by the connector. The sync reconciliation task reads the changelog, and every record (create, update, or delete) related to the specific object class is returned from the connector.

Table 9-1 (Cont.) Troubleshooting for the OID Connector

Problem	Solution
A group provisioning operation fails when you try to provision it to a user that already has another virtual static group provisioned. The same happens during a delete provisioning operation as well.	This problem is caused because virtual static groups are not supported by default. To use the connector for dynamic or virtual static groups, you must apply the following guidelines: • Ensure referential integrity in OUD is enabled. • Set the value of the maintainLdapGroupMembership entry in the Lookup.LDAP.OUD.Configuration lookup definition to `false`.

10 Known Issues and Workarounds

This is a known issue associated with this release of the connector.

Failure in Provisioning a User with a Backslash

Provisioning a user with a backslash in the uid and other mandatory fields fails.

Workaround:

Avoid using backslash in the uid and other mandatory fields.

A

Files and Directories in the Oracle Internet Directory Connector Installation Package

These are the components of the connector installation package that comprise the Oracle Internet Directory connector.

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

File in the Installation Media Directory	Description
bundle/org.identityconnectors.ldap-12.3.0.jar	This JAR file contains the connector bundle. The connector bundle includes the required version of the LDAP Booster Pack (ldapbp.jar file).
configuration/OID-CI.xml configuration/ODSEE-OUD-LDAPV3-CI.xml configuration/eDirectory-CI.xml	These XML files contain configuration information that is used during the connector installation process. • **For an OID target system:** OID-CI.xml • **For an ODSEE or OUD target system:** ODSEE-OUD-LDAPV3-CI.xml • **For an eDirectory target system:** eDirectory-CI.xml
Files in the javadoc directory	his directory contains information about the Java APIs used by the connector.
lib/OID-oim-integration.jar	This JAR file is used during transformation of user data. **Note:** This file is applicable only for a CI-based connector.
lib/TrustedUserIdTransformation.jar	This JAR file is used for transformation purposes during trusted source reconciliation runs. **Note:** This file is applicable only for a CI-based connector.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied to the Oracle Identity Governance database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages. Three sets of resource bundles are available: One each for ODSEE-OUD, OID, and eDirectory.
Files in the test-utility directory: ldap-config.groovy README test-utility.jar	These files are used by the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system. • The ldap-config.groovy file is a sample configuration that can be used to set the connection properties of the target system and the connector. • The README file contains instructions to configure and run the testing utility. • The test-utility.jar file contains the class files used by the testing utility. **Note:** These files are applicable only for a CI-based connector.

Table A-1 (Cont.) Files and Directories in the Connector Installation Package

File in the Installation Media Directory	Description
xml/OID-target-template.xml xml/ODSEE-OUD-LDAPV3-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system . It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/OID-auth-template.xml xml/ODSEE-OUD-LDAPV3-auth-template.xml	This file contains definitions for the connector objects required for creating an Authoritative application. It includes certain details required to connect Oracle Identity Governance with the target system . It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/OID-pre-config.xml xml/ODSEE-OUD-LDAPV3-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User objects such as Groups, Roles, and so on.
ConnectorConfig files in the xml directory: OID-ConnectorConfig.xml ODSEE-OUD-LDAPV3-ConnectorConfig.xml eDirectory-ConnectorConfig.xml	These XML files contain definitions for the following connector components: • Resource objects • IT resource types • IT resource instance • Process forms • Process tasks and adapters • Process definition • Prepopulate rules • Lookup definitions • Reconciliation rules • Scheduled tasks **Note:** These files are applicable only for a CI-based connector.
Datasets files in the xml directory: OID-Datasets.xml ODSEE-OUD-LDAPV3-Datasets.xml eDirectory-Datasets.xml **Note:** The dataset XML files are applicable only if you are using Oracle Identity Manager release 11.1.1.*x*.	These XML files contain dataset-related definitions for the create and modify user provisioning operations. Use one of the following files if you want to enable request-based provisioning by using the deployment manager: • **For an OID target system:** OID-Datasets.xml • For an **ODSEE or OUD target system:** ODSEE-OUD-LDAPV3-Datasets.xml • **For an eDirectory target system:** eDirectory-Datasets.xml **Note:** These files are applicable only for a CI-based connector.

Index