ORACLE
Consulting

Connector Administration

Oracle® Identity Manager Connector Guide for openfire™ Server

Release 1.0.0

ORACLE

Connector Administration

Oracle® Identity Manager Connector Guide for openfire™ Server

Release 1.0.0

by Sophie Strecke, Dieter Steding, and Sylvert Bernet

Table of Contents

Preface

Audience

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

Related Documents

For information about installing and using Oracle® Identity and Access Management, visit the following Oracle® Help Center page:

- *https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html*

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

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

Confidentiality

The material contained in this documentation represents proprietary, confidential information pertaining to Oracle® products and methods.

The audience agrees that the information in this documentation shall not be disclosed outside of Oracle, and shall not be duplicated, used, or disclosed for any purpose other than to evaluate this procedure.

Typographical 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.

About the Connector

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. Identity Governance connectors are used to integrate Identity Governance with external, identity-aware applications.

The Generic Directory Service connector lets you onboard LDAP directory server applications in Identity Governance. The various LDAP directory servers that this connector supports are

- Oracle Internet Directory (OID)
- Oracle Unified Directory (OUD)
- Oracle Directory Server Enterprise Edition (ODSEE)

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

From Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of 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 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:

- Components
- Usage Recommendation
- Languages
- Connector Operations
- Connector Architecture
- Connector Feature 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**.

Components

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

Usage Recommendation

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

> **Note**
>
> If you are using 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 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, and 11g release 1 (11.1.1.5.0, 11.1.1.6.0, 11.1.1.7.0 and 11.1.1.9.0)
    - 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)
    - 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 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 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 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 Generic Directory Service connector. If you want to use the 12.2.1.x version of this connector with 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**
  >
  > f you are using the latest 12.2.1.x version of the Oracle Internet Directory connector in the CI-based mode, then see Identity Manager Connector Guide for Internet Directory, Release 11.1.1 for complete details on connector deployment, usage, and customization.

- If you are using an 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.

Languages

The connector supports the following languages:

- English
- French
- German

Supported Connector Operations

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

Operation	OID?	OUD?	ODSEE?	LDAPv3?	Novell eDirectory?
User Management					
Create Account	Yes	Yes	Yes	Yes	Yes
Modify Account	Yes	Yes	Yes	Yes	Yes
Delete Account	Yes	Yes	Yes	Yes	Yes
Enable Account	Yes	Yes	Yes	Yes	Yes
Disable Account	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

Operation	OID?	OUD?	ODSEE?	LDAPv3?	Novell eDirectory?
Update container DN	Yes	Yes	Yes	Yes	Yes
Entitlement Grant Management					
Add groups	Yes	Yes	Yes	Yes	Yes
Revoke groups	Yes	Yes	Yes	Yes	Yes
Add roles	Yes	Yes	Yes	Yes	Yes
Revoke Roles	Yes	Yes	Yes	Yes	Yes
Add organizations	No	No	No	n.a	Yes
Remove organizations	No	No	No	n.a	Yes
Add domain scope	n.a	n.a	n.a	n.a	Yes
Add profiles	n.a	n.a	n.a	n.a	Yes
Add role containers	n.a	n.a	n.a	n.a	Yes

Connector Architecture

The Generic Directory Service 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 Identity Governance connectors. The ICF is shipped along with Identity Governance. Therefore, you need not configure or modify the ICF.

<image> </image>

The Generic Directory Service connector uses JNDI to access the target system.

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

Supported Connector Features Matrix

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

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 of account data	Yes	Yes
Secure communication	Yes	Yes
Reconcile deleted user records	Yes	Yes

Feature	AOB Application	CI-Based Connector
Reconcile deleted groups, roles, and organizations	Yes	Yes
Test connection	Yes	No

Features of the Connector

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.

- Full and Incremental Reconciliation
- Limited Reconciliation
- Reconciliation of Deleted User Records
- Support for the Connector Server
- Support for Running Pre and Post Action Scripts
- Transformation of Account Data
- Secure Communication to the Target System
- Connection Pooling
- Support for High-Availability Configuration of the Target System
- Connector Features

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.

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.

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:

<insert>link</insert>

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*.

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*.

Transformation of Account Data

You can configure transformation 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*.

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
<insert>link</insert>
.

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:

<insert>link</insert>

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
<insert>link</insert>