ORACLE
Consulting

Connector Administration

Oracle® Identity Manager Connector Guide for Identity Governance Provisioning

Release 1.0.0

Connector Administration

Oracle® Identity Manager Connector Guide for Identity Governance Provisioning Release 1.0.0

by Sophie Strecke, Dieter Steding, Sylvert Bernet, Adrian Farkas, Tomas Sebo, and Jovan Lakic

Publication date 2021-06-08

Table of Contents

Preface

This guide describes the connector that is used to onboard Oracle Identity Governance itself as an applications into Oracle Identity Governance.

Audience

This document is intended for people who deal with the administration of resources as well as teams who deal with the integration of target systems.

Related Documents

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

- *https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html*
- *https://docs.oracle.com/en/middleware/idm/suite/12.2.1.4/index.html*

For information about Identity Manager Connector#s documentation, visit the following Oracle Help Center page:

- *https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/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 table describes the typographic conventions that 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.

Symbol Conventions

The following table explains symbols that might be used in this document.

Convention	Meaning
[ ]	Contains optional arguments and command options.
{ | }	Contains a set of choices for a required command option.
${ }	Indicates a variable reference.
-	Joins simultaneous multiple keystrokes.
+	Joins consecutive multiple keystrokes.
>	Indicates menu item selection in a graphical user interface.

About the Identity Governance Provisioning 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 Oracle® Identity Manager Connectors lets you create and onboard Oracle® Identity Governance itself as an applications in Oracle® Identity Governance.

> **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 Oracle® 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:

- Required Components
- Usage Recommendation
- Supported Languages
- Connector Architecture
- Supported Connector Operations
- Connector Features

> **Note**
>
> At some places in this guide, Identity Governance Service are referred to as the **target system**.

Required Components

The platform-specific hardware and software requirements listed in this document are valid as of the date this document was created. Since new platforms and operating systems may be certified after this document is published, it is recommended to consult the certification matrix on Oracle Technology Network. The current statements about certified platforms and operating systems can be found there.

The respective certification matrix for Oracle Identity and Access Management Suite products are available at the following URLs:

- *Oracle® Fusion Middleware 12c (12.2.1.4.0)*
- *Oracle® Fusion Middleware 12c (12.2.1.3.0)*

Required Versions

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

Component	Version
Oracle® Java Development Kit	JDK 1.8.0_131 or higher
Oracle® Infrastruktur	Oracle® WebLogic 12c (12.2.1.3.0)
Oracle® Database	Oracle® RDBMS 12c (12.2.0.1.0) or higher
Oracle® Identity Governance	Oracle® Identity Governance 12c Release 12.2.1.3.0
Connector Server	Identity Connectore Server Release 12.2.1.3.0
Target System	Identity Governance Provisioning Release 1.0.0.0

Required Patches

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

Component	Version
Oracle® Identity Governance	Patch 30735905 Oracle® Identity Governance Bundle Patch ID:200108.2108)

Usage Recommendation

These are the recommendations for the Identity Governance Provisioning Connector versions that you can deploy and use depending Oracle Identity Governance version that you are using.

> **Note**
> Oracle® Identity Governance release 11.1.x, is not supported by this connector.

If you are using Identity Governance 12c (12.2.1.4.0) and want to integrate it the target system, then use the latest 12.2.1.x version of this connector and deploy it using either the **Applications** option on the **Manage** tab of Identity Self Service or the **Manage Connector** option in Oracle® Identity System Administration.

If you are using Identity Governance 12c (12.2.1.3.0) and want to integrate it the target system, then use the latest 12.2.1.x version of this connector and deploy it using either the **Applications** option on the **Manage** tab of Identity Self Service or the **Manage Connector** option in Oracle® Identity System Administration.

Below provides the list of features supported by the *AOB* application and *CI*-based connector.

Feature	AOB	CI
Account Full Reconciliation	Yes	Yes
Account Incremental Reconciliation	Yes	Yes

Feature	AOB	CI
Account Limited Reconciliation	Yes	Yes
Account Delete Reconciliation	Yes	Yes
Role Reconciliation	Yes	Yes
Tenant Reconciliation	Yes	Yes
Secure Communication	Yes	Yes
Test connection	Yes	No
Connector Server	Yes	Yes

Supported Languages

The connector supports the following languages:

- English
- French
- German

Connector Architecture

With the connector you can manage user accounts on the target system. Account management is also known as target resource management.

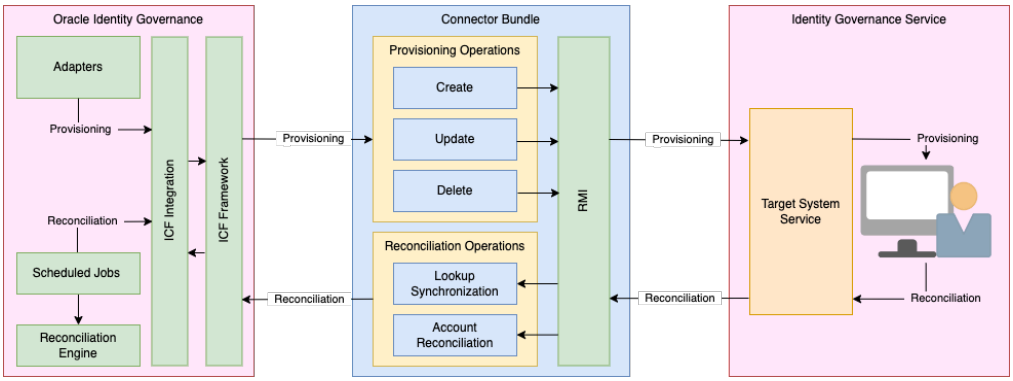

Figure 2.1. Connector Architecture

As shown in this figure, the backend of Identity Governance Service is configured as a target resource by Oracle® Identity Governance. Provisioning, performed in Oracle Identity Governance, creates and updates accounts for identities on the target system. Through the reconciliation, account data that is created and updated directly on the target system is fetched in Oracle® Identity Governance and saved against the corresponding identities.

The Identity Governance Provisioning Connector is implemented by using the Identity Connector Framework (ICF). ICF is a component that is required to use Identity Connectors and provides basic reconciliation and provisioning operations that are common to all Identity Governance connectors. In addition, ICF offers general functions that developers would otherwise have to implement themselves, e.g. connection pooling, buffering, timeouts and filtering. The ICF is shipped along with Identity Governance. Therefore, you need not configure or modify the ICF.

The Identity Governance Provisioning Connector uses RMI to access the target system.

This connector supports Account Management only. This mode of the connector enables the following operations:

Provisioning

Provisioning involves creating, updating, or deleting users on the target system through Oracle® Identity Governance. When you allocate (or provision) a target system resource to an identity, the operation results in the creation of an account on the target system for that identity. 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.

Before you can provision users to the required groups or tenants on the target system, you must fetch into Oracle® Identity Governance the list of all groups and tenants used on the target system. This is achieved by using the IGS Role Lookup Reconciliation and IGS Tenant Lookup Reconciliation scheduled jobs for lookup synchronization.

Reconciliation

During the target resource reconciliation, data on newly created and changed user accounts in the target system are compared and linked to existing identities and provisioned resources. To perform target resource reconciliation, scheduled jobs are used. The connector applies filters to locate users to be reconciled from the target system and then fetches the attribute values of these users.

Supported Connector Operations

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

User Management

Operation	Supported?
Create Account	Yes
Modify Account	No
Delete Account	Yes
Enable Account	No
Disable Account	No
Reset Password	No

Role Management

Operation	Supported?
Create Role	No
Modify Role	No
Delete Role	No

Organization Management

Operation	Supported?
Create Organization	No

Operation	Supported?
Modify Organization	No
Delete Organization	No

AdminRole Management

Operation	Supported?
Create AdminRole	No
Modify AdminRole	No
Delete AdminRole	No

Entitlement Grant Management

Operation	Supported?
Assign To Role	Yes
Revoke From Role	Yes
Assign To AdminRole	Yes
Revoke AdminRole	Yes

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
- Lookup Fields Synchronized with the Target System
- 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

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

Lookup Fields Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Country lookup field to select a country from the list of countries in the lookup field.

When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle® Identity Governance. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle® Identity Governance.

For more information about the reconciliation job used for reconciling lookup definitions, see one of the following sections: insert link

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, TLS/SSL is required. You can configure TLS/SSL between Oracle® Identity Governance and the Connector Server and between the Connector Server and the target system.

If you do not configure TLS/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.

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

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.