ORACLE
Consulting

Connector Administration

Oracle® Identity Manager Connector Guide for Identity Governance Services

Release 1.0.0

Connector Administration

Oracle® Identity Manager Connector Guide for Identity Governance Services

Release 1.0.0

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

Publication date 2023-06-27

Table of Contents

Preface 1
Audience 1
Related Documents 1
Confidentiality 1
Typographical Conventions 1
Symbol Conventions 1
About the Identity Governance SCIM Server Connector 3
Required Components 3
Required Versions 4
Required Patches 4
Usage Recommendation 4
Supported Languages 5
Connector Architecture 5
Provisioning 6
Reconciliation 6
Supported Connector Operations 6
User Management 6
Role Management 6
Tenant Management 6
Entitlement Grant Management 7
Features of the Connector 7
Full and Incremental Reconciliation 7
Limited Reconciliation 7
Reconciliation of Deleted User Records 8
Lookup Fields Synchronized with the Target System 8
Support for the Connector Server 8
Support for Running Pre and Post Action Scripts 8
Transformation of Account Data 8
Secure Communication to the Target System 9
Connection Pooling 9
Support for High-Availability Configuration of the Target System 9
Using the Identity Governance SCIM Server Connector 10
Using the Connector 10
Configuring Reconciliation 10
Performing Provisioning Operations 10
Lookup Definitions Used During Connector Operations 10
Predefined Lookup Definitions 11
Synchronized Lookup Definitions 11
Understanding Reconciliation Scheduled Jobs 11
Scheduled Job for Lookup Field Synchronization 11
Attributes of the Scheduled Jobs 14
Installing and Configuring the Connector 19
Prerequisites for Installing the Connector 19
Creating a Target System User Account for Connector Operations 19
Installation 19
Running the Connector Installer 19
Postinstallation 21
Configuring the IT Resource for the Target System 21
Configuring the IT Resource for the Connector Server 22
Configuring SSL 23
Managing Logging 24
Understanding Log Levels 24
Configure Logging 25

Connector Model 26
Overview 26
Account 26
Attributes 26
Prepopulation 27
Roles 27
Attributes 27
Prepopulation 27
Tenants 27
Attributes 27
Prepopulation 28

Preface

This guide describes the connector that is used to onboard P20 Identity Governanace Service 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 SCIM Server 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 Identity Governance Service 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 SCIM Server 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 SCIM Server 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.

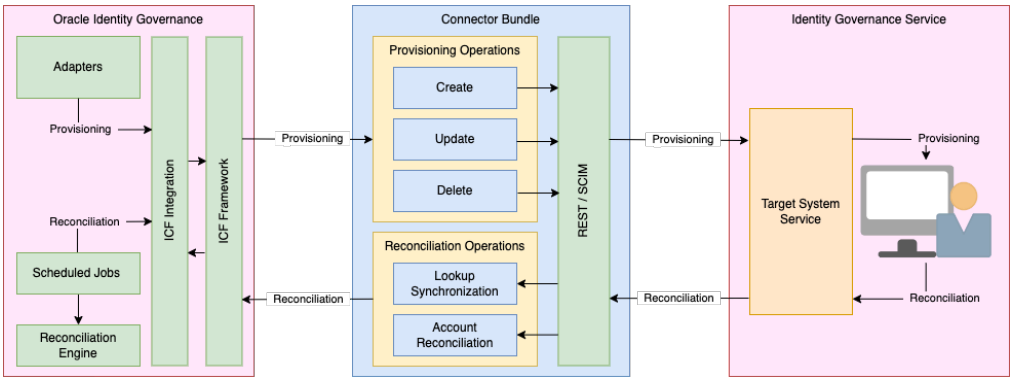

Figure 2.1. Connector Architecture

As shown in this figure, the SCIM server 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 SCIM Server 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 SCIM Server Connector uses REST/SCIM over HTTP(S) 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	Yes
Delete Account	Yes
Enable Account	Yes
Disable Account	Yes
Reset Password	Yes

Role Management

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

Tenant Management

Operation	Supported?
Create Tenant	No

Operation	Supported?
Modify Tenant	No
Delete Tenant	No

Entitlement Grant Management

Operation	Supported?
Assign To Role	Yes
Revoke From Role	Yes
Assign To Tenant	Yes
Revoke Tenant	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.

Using the Identity Governance SCIM Server Connector

You can use the Identity Governance SCIM Server Connector for performing reconciliation and provisioning operations after configuring your application to meet your requirements.

- Guidelines on Using the Connector
- Overview of Lookup Definitions Used During Connector Operations
- Scheduled Jobs for Lookup Field Synchronization

Using the Connector

This section discusses the following topics:

- Configuring Reconciliation
- Performing Provisioning Operations

Configuring Reconciliation

The following are 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.
- The scheduled job for user reconciliation must be run before the scheduled job for reconciliation of deleted user data.

Performing Provisioning Operations

The following are 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.
- Provisioning of groups is not supported by the connecttor.
- Provisioning of tenants is not supported by the connecttor.

Lookup Definitions Used During Connector Operations

Know more about the lookup definitions used during connector operations

It can be categorized as follows:

- Predefined Lookup Definitions

  About Predefined Lookup Definitions
- Understanding Synchronized Lookup Definitions with the Target System

Predefined Lookup Definitions

This connector has no predefined Lookup Definitions.

Synchronized Lookup Definitions

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 may want to select a group from a lookup field to specify the group being assigned to the user.

When you deploy the connector, an empty lookup definition `IGS.Role` is created. The `IGS.Role` lookup definition is used to store values from a child table that must be displayed in a lookup field during provisioning. Depending upon your environment, you can customize the `IGS.Role` lookup definition to suit your requirement. Alternatively, you can create your own lookup definition for storing values to be displayed in a lookup field. See
<insert>link</insert>
Using Lookup Definitions for information about setting up lookup fields.

Lookup field synchronization involves obtaining the most current values from specific tables in the target system to the lookup definitions (used as an input source for lookup fields, for example `IGS.Role`) in Oracle Identity Governance.

The `IGS Group Lookup Reconciliation` scheduled job is used to synchronize values of these lookup definitions with the tables in the target system. While configuring the `IGS Group Lookup Reconciliation` scheduled job, you specify the name of the lookup definition that you want to synchronize as the value of the *Reconciliation Object* attribute. See Scheduled Job for Lookup Field Synchronization for more information about this scheduled task.

After lookup definition synchronization, data is stored in the following format:

Understanding Reconciliation Scheduled Jobs

When you run the Connector Installer, scheduled jobs are automatically created in Oracle Identity Manager.

This section discusses the following topics:

- Scheduled Job for Lookup Field Synchronization
- Understanding Synchronized Lookup Definitions with the Target System

Scheduled Job for Lookup Field Synchronization

> **Note**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
> - Values (either default or user-defined) must be assigned to all required attributes. If even a single attribute value were left empty on those attributes, then reconciliation would not be performed

Scheduled Job for Group Synchronization

The `IGS Group Lookup Reconciliation` scheduled job is used for lookup fields synchronization.

You must specify values for the attributes of this scheduled job.

Attribute	Description
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile records. This attribute is required. Default value: *IGS.Endpoint*
Encoded Value	The name of the entity attribute that has to be stored as the encoded value. This attribute is required. Default value: *__UID__*
Decoded Value	Enter the name of the attribute that is used to populate the *Decode* attribute of the lookup definition (specified as the value of the Lookup Name attribute). This attribute is required. Default value: *__NAME__*
Entitlement Prefix Required	Select the option *Yes* if the entitlements loaded needs to be prefixed with the internal system identifier and/or the name of the *IT Resource*. This attribute is required. Default value: *Yes*
Reconciliation Source	The identifier of the source (aka ObjectClass) that has to be used to reconcile. This attribute is required. Default value: *Group*
Reconciliation Object	The name of the object to reconcile. This attribute is required. Default value: *IGS.Role*
Reconciliation Operation	The operation to perform on the object to reconcile. Has to be either *Refresh* or *Update*. This attribute is required. Default value: *Update*
Last Reconciled	Holds the timestamp when this task was last executed successfully. This attribute is required. Default value: *0*
Gather Only	Select the option *Yes* if the data should only be gathered from the reconciliation source. This attribute is required.

Attribute	Description
	Default value: *No*
Lookup Group	The value written to *Lookup Group* attribute in case the operation on a particular Lookup Definition has to create it (Reconciliation Operation set as *Refresh*). This attribute is required. Default value: *IGS*
Dependent Job	Specifies the name of the Job that will be started by this Job on successfully completion.

Scheduled Job for Tenant Synchronization

The `IGS Tenant Lookup Reconciliation` scheduled job is used for lookup fields synchronization.

You must specify values for the attributes of this scheduled job.

Attribute	Description
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile records. This attribute is required. Default value: *IGS.Endpoint*
Encoded Value	The name of the entity attribute that has to be stored as the encoded value. This attribute is required. Default value: *__UID__*
Decoded Value	Enter the name of the attribute that is used to populate the *Decode* attribute of the lookup definition (specified as the value of the Lookup Name attribute). This attribute is required. Default value: *__NAME__*
Entitlement Prefix Required	Select the option *Yes* if the entitlements loaded needs to be prefixed with the internal system identifier and/or the name of the *IT Resource*. This attribute is required. Default value: *Yes*
Reconciliation Source	The identifier of the source (aka ObjectClass) that has to be used to reconcile. This attribute is required. Default value: *Tenant*
Reconciliation Object	The name of the object to reconcile. This attribute is required. Default value: *IGS.Tenant*
Reconciliation Operation	The operation to perform on the object to reconcile. Has to be either *Refresh* or *Update*.

Attribute	Description
	This attribute is required. Default value: *Update*
Last Reconciled	Holds the timestamp when this task was last executed successfully. This attribute is required. Default value: *0*
Gather Only	Select the option *Yes* if the data should only be gathered from the reconciliation source. This attribute is required. Default value: *No*
Lookup Group	The value written to *Lookup Group* attribute in case the operation on a particular Lookup Definition has to create it (Reconciliation Operation set as *Refresh*). This attribute is required. Default value: *IGS*
Dependent Job	Specifies the name of the Job that will be started by this Job on successfully completion.

Attributes of the Scheduled Jobs

> **Note**
> Only account reconciliation is supported by the connector.

This section discusses the attributes of the following scheduled jobs:

- Reconciliation of User Records
- Incremental Reconciliation of User Records
- Reconciliation of Deleted Users Records

Reconciliation of User Records

After you create the connector, the scheduled task for user data reconciliation is automatically created in Oracle Identity Manager. The `IGS Account Reconciliation` scheduled job, which is an instance of this scheduled task is used to reconcile user data from the target system.

You must specify values for the attributes of this scheduled job.

Attribute	Description
Batch Size	Specifies the size of a batch read from the Service Provider. This attribute is optional. Default value: *500*
Thread Pool Size	Specifies that how many threads this task should create to distribute the workload. This attribute is optional. Default value: *1*

Attribute	Description
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. This attribute is required. Default value: *IGS.Endpoint*
Reconciliation Object	Enter the name of the resource object that is used for reconciliation. This attribute is required. Default value: *IGS Account*
Reconciliation Descriptor	Enter the path to the descriptor which specifies the mapping between the incomming field names and the reconciliation fields of the resource object to reconcile. This attribute is required. Default value: */metadata/ocs-features-reconciliation/dbs/ofs-account-reconciliation.xml*
Ignore Dublicates	Select the option *Yes* to prevent event creation and processing of target system records that already exists in Identity Governance; otherwise select option *No* This attribute is required. Default value: *Yes*
Search Filter	Specifies which filter criteria has to be applied to retrieve entries. Must be a valid Service Provider search filter. This attribute is optional.
Last Reconciled	Holds the timestamp when this task was last executed successfully. This attribute is required. Default value: *0*
Gather Only	Select the option *Yes* if the data should only be gathered from the reconciliation source. This attribute is required. Default value: *No*
Dependent Job	Specifies the name of the Job that will be started by this Job on successfully completion.

Incremental Reconciliation of User Records

Reconciliation of Deleted Users Records

After you create the connector, the scheduled task for reconciling data about deleted users records is automatically created in Oracle Identity Manager. The `IGS Account Delete Reconciliation` scheduled job, which is an instance of this scheduled task is used to reconcile user data from the target system.

You must specify values for the attributes of this scheduled job.

Attribute	Description
Batch Size	Specifies the size of a batch read from the Service Provider. This attribute is optional. Default value: *500*
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. This attribute is required. Default value: *IGS.Endpoint*
Reconciliation Object	Enter the name of the resource object that is used for reconciliation. This attribute is required. Default value: *IGS Account*
Reconciliation Descriptor	Enter the path to the descriptor which specifies the mapping between the incomming field names and the reconciliation fields of the resource object to reconcile. This attribute is required. Default value: */metadata/ocs-features-reconciliation/dbs/ofs-account-reconciliation.xml*
Last Reconciled	Holds the timestamp when this task was last executed successfully. This attribute is required. Default value: *0*
Dependent Job	Specifies the name of the Job that will be started by this Job on successfully completion. This attribute is optional.

Configuring Scheduled Jobs

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

- Lookup Field Synchronization and Reconciliation
- Configuring Scheduled Jobs

Lookup Field Synchronization and Reconciliation

<insert>table-link</insert>
lists the scheduled jobs that you can configure.

Scheduled Job	Description
IGS Group Lookup Reconciliation	This scheduled job is used for lookup field synchronization. See Scheduled Jobs for Lookup Field Synchronization for information about this scheduled job.
IGS Tenant Lookup Reconciliation	This scheduled job is used for lookup field synchronization. See Scheduled Jobs for Lookup Field Synchronization for information about this scheduled job.

Scheduled Job	Description
IGS Account Reconciliation	This scheduled job is used for user reconciliation when the target system is configured as a target resource. See Scheduled Jobs for Reconciliation of User Records for more information.
IGS Account Delete Reconciliation	This scheduled job is used for reconciliation of deleted user records when the target system is configured as a target resource. See Scheduled Jobs for Reconciliation of Deleted Users Records for more information.

Configuring Scheduled Jobs

To configure a scheduled job:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled task as follows:
    a. On the left pane, 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 following parameters:
    - **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.

      > **Note**
      > See *Creating Jobs* in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

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

Note

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
- Attributes of the scheduled task are discussed in Attributes of the Scheduled Jobs.

Installing and Configuring the Connector

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

The procedure to install and configure the connector can be divided into the following stages:

- Prerequisites for Installing the Connector
- Postinstallation

Prerequisites for Installing the Connector

Prerequisite for the connector involves creating a target system user account and configuring the database.

Perform the following preinstallation procedures on your target system:

- Creating a Target System User Account for Connector Operations
- About Configuring Oracle Database

Creating a Target System User Account for Connector Operations

Oracle Identity Governance uses a target system user account to provision to and reconcile data from the target system. For all target systems certified for this connector, the following are the minimum rights to be assigned to the target system user account:

- For reconciliation:

  The user account must have permissions to run search statements on the SCIM API that must be managed by this connector.

- For provisioning:

  The user account must have permissions to perform lookup, create, modify, and delete operations on the SCIM API to be managed by this connector.

See the target system documentation for the procedure to create a target system user account with the preceding permissions required for performing connector operations.

Installation

Installation on Oracle Identity Governance consists of the following procedures:

Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:
2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of Oracle Identity Manager Administrative and User Console Guide.
3. Click **Deployment Management** and then click **Install Connector**.

4. From the Connector List, select **Openfire Database Connector Configuration 1.0.0.0**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/`ConnectorDefaultDirectory`.

   If you have copied the installation files into a different directory, then:

   1. In the **Alternative Directory** field, enter the full path and name of that directory.
   2. To repopulate the list of connectors in the Connector List, click **Refresh**.
   3. From the Connector List, select **Identity Governance SCIM Connector Configuration 1.0.0.0**.
5. Click **Load**.
6. To start the installation process, click **Continue**.

   The following tasks are performed, in sequence:

   1. Configuration of connector libraries.
   2. Import of the connector XML files (by using the Deployment Manager).
   3. Compilation of adapters.
7. On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   1. Retry the installation by clicking **Retry**
   2. **Cancel** the installation and begin again from Step 4.
8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of steps that you must perform after the installation is displayed. These steps are as follows:

   1. Ensuring that the prerequisites for using the connector are addressed.
   2. Configuring the IT resource for the connector.

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

      Record the names of the Scheduled Jobs displayed on this page. The procedure to configure these Scheduled Jobs is described later in this guide

When you run the Connector Installer, it uploads the connector files and external code files to database connected to Oracle Identity Governance. These files are listed in following table:

File in the Installation Media Directory	Destination Location
lib/igs.identity.connector.adapter-12.2.1.3.jar	JavaTasks
lib/igs.identity.connector.scheduler-12.2.1.3.jar	ScheduleTask
lib/igs.identity.connector.common-12.2.1.3.jar	ThirdParty
lib/igs.identity.connector.bundle-12.2.1.3.jar	bundle
Files in the resources directory	connectorResources

Postinstallation

Configuring the IT Resource for the Target System

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

Parameter	Description
Server Name	Enter the host name or IP address of the Database Service computer (target system host computer) on which Database Service is installed. Samples `hardy`, `hardy.example.com`, `192.168.64.131`
Server Port	Enter the number of the port at which the service is listening at the target host computer. **Samples**: `443`
Server Feature	???? **Default**: `GMT+01:00`
Secure Socket	Enter `yes` to specify that you will configure SSL between Oracle Identity Governance and the target system. Otherwise, enter `no`. **Default**: `no`
Root Context	????
Principal Name	Enter the name of the user account that you create by performing the procedure described in Creating a Target System User Account for Connector Operations. **Samples**: `igssysadmin`
Principal Password	Enter the password of the user account that you create by performing the procedure described in Creating a Target System User Account for Connector Operations.
Locale Language	The name of language the target system is using. Default: `en`
Locale Country	The name of language region the target system is using. Default: `US`
Locale TimeZone	The time zone the target system is using.

Parameter	Description
	Default: `GMT+01:00`
Connection Timeout	????
Response Timeout	????

Configuring the IT Resource for the Connector Server

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

After you create the application for your target system, the connector creates a default IT resource for the Connector Server. The name of this default IT resource is `OFS Endpoint`.

In Oracle Identity System Administration, search for and edit the openfire™ IT resource to specify values for the parameters of IT resource for the Connector Server listed in Table 4-2. For more information about searching for IT resources and updating its parameters, see Managing *Managing IT Resources* in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. **Sample**: `HostName`
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. **Sample**: `8757`
Port	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Governance times out. If the value is zero or if no value is specified, the timeout is unlimited. **Sample**: `0`(recommended value)
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter `false`. **Default**:`false` **Note** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see *SSL for Connector Server and OIM* in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

Configuring SSL

Configure SSL to secure data communication between Oracle Identity Governance and the target system.

1. Obtain the SSL certificate by obtaining the public key certificate of the target system.
2. Copy the public key certificate of the target system to the computer hosting Oracle Identity Governance.
3. Run the following keytool command to import the public key certificate into the identity key store in Oracle Identity Governance:

   ```
   keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -file CERT_FILE_NAME -storepass PASSWORD
   ```

   In this command:

Parameter	Meaning
WEBLOGIC_HOME	The ...
CERT_FILE_NAME	The full path and name of the certificate file.
PASSWORD	The password of the keystore.

   The following is a sample value for this command:

   ```
   keytool -import -keystore /opt/oracle/product/fwm/12.2.1/wlserver/server/lib/DemoTrust.jks -file /home/target.cert -storepass changeit
   ```

   Note

   Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool arguments.

Managing Logging

Oracle Identity Governance uses 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
- Configure Logging

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:

Level	Description
SEVERE.intValue()+100	This level enables logging of information about fatal errors.
SEVERE	This level enables logging of information about errors that might allow Oracle Identity Governance to continue running.
WARNING	This level enables logging of information about potentially harmful situations.
INFO	This level enables logging of messages that highlight the progress of the application.
CONFIG	This level enables logging of information about fine-grained events that are useful for debugging.
FINE, FINER, FINEST	These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These message types are mapped to ODL message type and level combinations as shown in Table 4-1.

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	TRACE1
FINER	TRACE16
FINEST	TRACE32

The configuration file for ODL is logging.xml is located at the following path:

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

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

Configure Logging

To enable logging in Oracle WebLogic Server:

Connector Model

Overview

The figure below shows an overview of the data model of the connector.

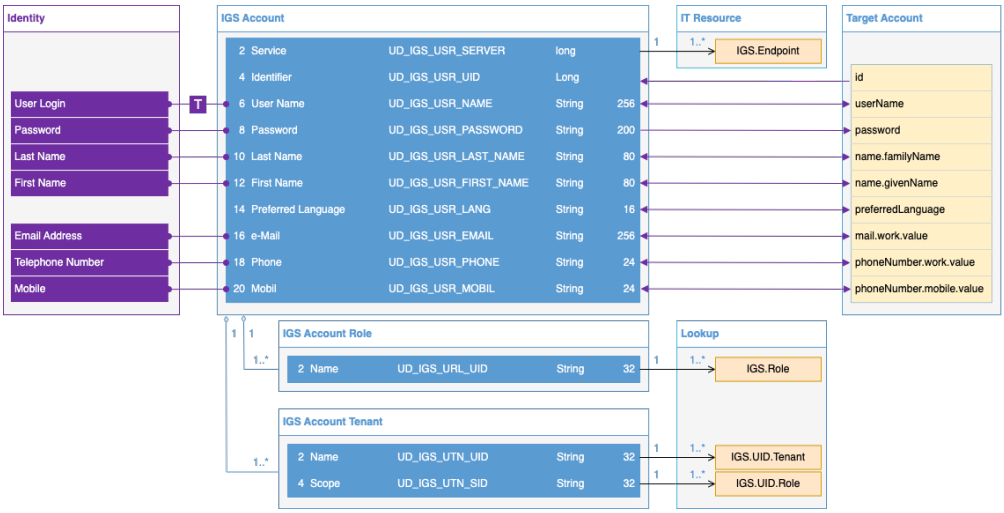

Figure 6.1. Connector Model

In addition to the Account data model required by an Identity Governance Service, the data model of the connector supports the storage of roles and tenants.

- Roles
- Tenants

Account

The account data are stored in the form UD_IGS_USR.

Attributes

Label	Name	Type	Length
Service	UD_IGS_USR_SVC	Long	
Identifier	UD_IGS_USR_UID	Long	
User Name	UD_IGS_USR_NAME	String	256
Password	UD_IGS_USR_PWD	String	200
Last Name	UD_IGS_USR_SN	String	80
First Name	UD_IGS_USR_GN	String	80
Preferred Language	UD_IGS_USR_LANG	String	16
e-Mail	UD_IGS_USR_MAIL	String	256
Phone	UD_IGS_USR_PHONE	String	24
Mobile	UD_IGS_USR_MOBILE	String	24

Prepopulation

Rules are implemented for some of the attributes described above, which derive values for such an attribute from the profile of an identity the account belongs to.

Label	Adapter		Rule
User Name	OCS String	PrePopulate Converted	Derives the value from *User Definition* attribute **User Login** and converts it to lower case.
Password	OCS String	PrePopulate	Derives the value from *User Definition* attribute **Password**.case.
Last Name	OCS String	PrePopulate	Derives the value from *User Definition* attribute **Last Name**.
First Name	OCS String	PrePopulate	Derives the value from *User Definition* attribute **First Name**.
Preferred Language	OCS String	PrePopulate	Derives the value from *User Definition* attribute **Preferred Language**.
e-Mail	OCS String	PrePopulate	Derives the value from *User Definition* attribute **Email Address**.
Phone	OCS String	PrePopulate	Derives the value from *User Definition* attribute **Telephone Number**.
Mobil	OCS String	PrePopulate	Derives the value from *User Definition* attribute **Mobile**.

Roles

The roles assigned to a user account are stored in the UD_IGS_URL form.

Attributes

Label	Name	Type	Length
Name	UD_IGS_URL_UID	String	32

Prepopulation

The form is not subject to any rules for prepopulating values.

Tenants

The tenants and their scopes assigned to a user account are stored in the UD_IGS_UTN form.

Attributes

Label	Name	Type	Length
Name	UD_IGS_UTN_UID	String	32
Scope	UD_IGS_UTN_RID	String	32

Prepopulation

The form is not subject to any rules for prepopulating values.