# Oracle® Cloud

# OIG Integration Quick Start

F56595-03
December 2024

Oracle Cloud OIG Integration Quick Start,

F56595-03



Primary Author: Oracle Corporation

# Contents

1

# OIG Integration Quick Start

## Preinstall

**Certified Components**

The target system can be any one of the following:

- Oracle Access Governance supports building an agent for Oracle Identity Governance **Version 12.2.1.4 Bundle Patch Number 11 (12.2.1.4.220703) or later**. If your current version of Oracle Identity Governance is not compatible then contact Oracle Support, who can arrange a patch for your Oracle Identity Governance system

**Prerequisites**

The Oracle Identity Governance source data must meet the following requirements to be eligible for review in Oracle Access Governance:

- Applications and Entitlements in Oracle Identity Governance must be marked as **Certifiable** in order to be ingested by Oracle Access Governance. Log in to the Oracle Identity Governance Self Service application and navigate to **Request Access → Request for Self → [Search for Your App]** and click the information icon, and select the **Certifiable** flag.
- For Roles, log in to the Oracle Identity Governance Self Service application and navigate to **Manage → Roles → Open the Role**. Under Catalog Attributes, select the **Certifiable** check box.
- Any access included in an Oracle Access Governance review must have been granted using one of the following grant types in Oracle Identity Governance:
  - **Direct Provision accounts and Entitlements**
  - **Request Provision accounts and Entitlements**
  - **Reconciled accounts and Entitlements from the targets**
  - **Bulkloaded accounts and Entitlements**
  - **Request or Direct provision Role which are associated with access policy**

## Set Up Oracle Identity Governance Integration

To enable the Oracle Identity Governance agent to connect to Oracle Access Governance, you need to enter connection details and credentials for the target system, and build an agent specific to your environment.

1. In a browser, navigate to the Oracle Access Governance service home page and log in as a user with the **Administrator** application role.
2. On the Oracle Access Governance service home page, click on the  icon and select **Service Administration** and then **Orchestrated Systems**.

3. Select the **Add an orchestrated system** button, to navigate to the **Add an orchestrated system** page to start the workflow.
4. On the **Select system** step of the workflow, you can specify which type of system you would like to onboard. You can search for the required system by name using the Search field.
   a. Select **Oracle Identity Governance**
   b. Select **Next**
5. On the **Enter Details** step, enter the general details for the orchestrated system:
   - Enter a name for the system you want to connect to in the **What do you want to call this application?** field.
   - Enter a description for the system in the **How do you want to describe this application?** field.
   - Click **Next**.
6. On the **Add owners** step:

   You can associate resource ownership by adding primary and additional owners. This drives self-service as these owners can then manage (read, update or delete) the resources that they own. By default, the resource creator is designated as the resource owner. You can assign one primary owner and up to 20 additional owners for the resources.

   > **Note:**
   >
   > When setting up the first Orchestrated System for your service instance, you can assign owners only after you enable the identities from the Manage Identities section.

   To add owners:

   a. Select an Oracle Access Governance active user as the primary owner in the **Who is the primary owner?** field.
   b. Select one or more additional owners in the **Who else owns it?** list. You can add up to 20 additional owners for the resource.

   You can view the **Primary Owner** in the list. All the owners can view and manage the resources that they own.
7. On the **Integration settings** step of the workflow, enter the configuration details required to allow Oracle Access Governance to connect to the required Oracle Identity Governance instance.
   - In the **What is the JDBC URL of your OIG database server?** field, enter the JDBC URL for the OIG database you want to connect with.

**Note:**

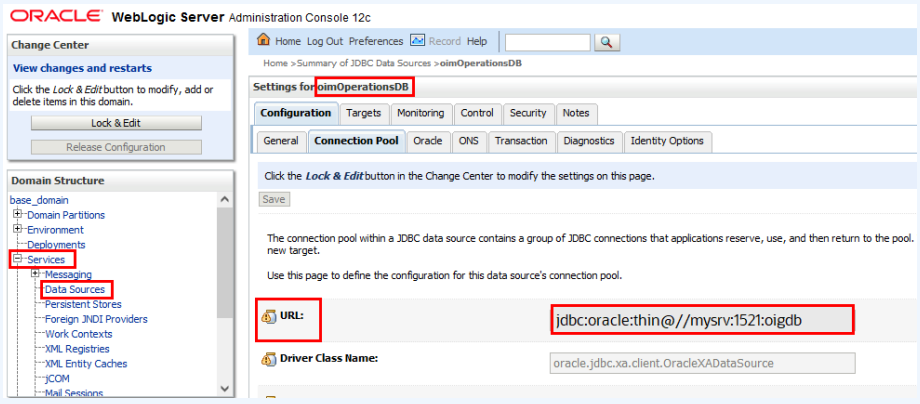
To obtain the JDBC URL:

a. Log on to the Oracle WebLogic Server Administration Console associated with your Oracle Identity Governance instance.

b. Navigate to **Services** → **Data Sources**.

c. Select **oimOperationsDB** from the **Configurations** tab.

d. Select **Connections Pool**, and copy the value from the **URL:** field to use as the JDBC URL for Oracle Identity Governance.



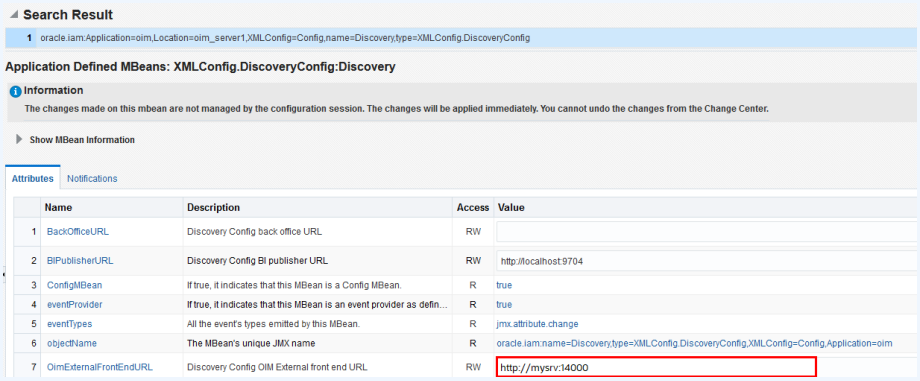

- In the **What is the OIG database user name?** field, enter the database user to connect to the OIG database.

**Note:**

This can be any user with read access to the OIG database.

- In the **Password** field, enter the password for the OIG database user you have specified.
- In the **What is the URL of your OIG server?** field, enter the URL of the OIG server you want to integrate with.

> **Note:**
>
> To obtain the OIG Server URL:
>
> – Log on to the Oracle Enterprise Manager Fusion Middleware Control.
>
> – Navigate to the **System MBean Browser** and locate the **XMLConfig.DiscoveryConfig** MBean.
>
> – Copy the value of the **OimExternalFrontEndURL** attribute and use this as the value for the Oracle Identity Governance Server URL.




- In the **What is the OIG server user name?** field, enter the OIG user used for remediation and schema discovery.

> **Note:**
>
> The Oracle Identity Governance Server user can be any user that is a member of the **System Administrator** administration role. This role is required to perform the remediation process, and to support schema discovery for custom attributes. In the case where only remediation support is needed then user can be a member of the **OrclOAGIntegrationAdmin** administration role. With this user the schema discovery operation will fail.

- In the **OIG server password** field, enter to authenticate the OIG server user when calling OIG APIs to perform remediation.

> **Note:**
>
> Information about the Oracle Identity Governance Server (URL, Username, and Password), and Oracle Identity Governance datasource (JDBC URL, Username, and Password) is required to integrate Oracle Access Governance and Oracle Identity Governance. Oracle Access Governance will use the Oracle Identity Governance data source to load the data and the Oracle Identity Governance Server URL to perform remediation operations. In case of a connection failure, the Oracle Access Governance agent automatically retries a maximum of three times to secure a connection with the Oracle Identity Governance server.

8. Optionally, you can select to perform data loads using OIG database incremental data load. If you select the **Do you want to enable OIG database incremental data load?** option then Day-N data loads will use an event-driven mode which applies changes to

Oracle Access Governance as they happen, rather than as a periodic snapshot. If you select this option, ensure that you have completed the prerequisite tasks in the OIG database defined in Database Setup Steps for Event-driven Data Load.

> **Note:**
>
> You should use this option if you want to see events from OIG in real-time rather than periodically. For example, if your organization creates an identity for a user which needs to be reflected in Oracle Access Governance immediately then you should use this option. When the identity is added, the event is noted by the integration and reconciled with AG. The default snapshot data load will not reconcile the new identity until its next scheduled run, when it will run a data load of all changes since the last. With the event-driven data load, changes are identified in real-time and loaded into Oracle Access Governance as each event takes place.

.

9. Enter filter attributes which will be used to filter the data that is returned from OIG.

   You can add up to three filter name/value pairs which will be used to restrict the users and accounts ingested from Oracle Identity Governance by Oracle Access Governance. You can also set the search filter values separator to a character of your choice if required (default is ~).
   Details of the attributes you can use to set filters against can be found in Supported Attributes for User Data Load Filtering.

10. Verify the details entered are correct, and click the **Add** button

11. On the **Download Agent** step, select the **Download** link and download the agent zip file to the environment in which the agent will run.

    After downloading the agent, follow the instructions explained in the Agent Administration article.

12. You are given a choice whether to further configure your orchestrated system before running a data load, or accept the default configuration and initiate a data load. Select one from:

    - **Customize before enabling the system for data loads**
    - **Activate and prepare the data load with the provided defaults**: If you select this option, the default matching rule for **Oracle Identity Governance** orchestrated system will be used.

**Table 1-1 Default Matching Rule**

| Mode | |
|---|---|
| Authoritative Source | `userName = userName` |
| Managed System | Default rule is not supported. Matching is based on UID. |

You can also follow the instructions provided in the Set Up Identity Orchestration between Oracle Access Governance and Oracle Identity Governance (OIG) tutorial.

# Supported Attributes for User Data Load Filtering

When configuring an Orchestrated System to on-board data from Oracle Identity Governance, it is possible to filter the user data you want to ingest in Oracle Access Governance. You can restrict which users are on-boarded by setting filters on identity attributes such as department, employee type, location, and others.

### User Data Load Filtering Characteristics

You should be aware of the following characteristics of user data load filtering befire configuring filters in your Orchestrated System.

- Matching of user search filters and user data values filtering is case sensitive. For example. a filter of `department = Human Resources` would not return users with a value of `department = HUMAN RESOURCES`, or `Department = Human Resources`.
- If no users or accounts match the user data load filter, then no data will be ingested from Oracle Identity Governance by Oracle Access Governance. In this case, however, the data load itself will be labelled as successful in the activity log, even though no identities or accounts are on-boarded.
- User data load filter values cannot exceed 1000 for any given filter attribute.
- If an agent is already installed, an agent upgrade is required to enable user data load filters. See Agent Example Usage for details on how to upgrade your agent.

### List of Supported Attributes for User Data Load Filtering

You can filter users ingested from Oracle Identity Governance based on the following attributes.

**Table 1-2 List of Supported Attributes for User Data Load Filtering**

| Oracle Access Governance Attribute Name | Oracle Identity Governance Attribute Name |
|---|---|
| employeeType | usr_emp_type |
| jobCode | usr_job_code |
| department | usr_dept_no |
| location | usr_location |
| state | usr_state |
| postalCode | usr_postal_code |
| country | usr_country |
| managerUid | usr_manager_key |
| managerLogin | usr_login<br>(usr_login of manager) |
| organizationUid | act_key |
| organizationName | act_name<br>act_name of act table |
| territory | usr_territory |

### Example User Data Load Filters

Some examples of usecases you can configure using the User Data Load Filter functionality are provided below:

**Table 1-3 Example User Data Load Filters**

| Usecase | Configuration Parameters |
|---|---|
| User with **department=Product Development** and **jobCode=IC004 or M0003** | • userFilter1Name=department<br>• userFilter1Value=Product Development<br>• userFilter2Name=jobCode<br>• userFilter2Value=IC004~M0003<br>• userFilter3Name=<br>• userFilter3Value=<br>• filterValueDelimiter=~ |
| User with **state =Kent** and **organizationUid=1 or 4** | • userFilter1Name=state<br>• userFilter1Value=Kent<br>• userFilter2Name=organizationUid<br>• userFilter2Value=1~4<br>• userFilter3Name=<br>• userFilter3Value=<br>• filterValueDelimiter=~ |
| User with **postalCode = 78045 or 12204** with **custom delimiter ##** | • userFilter1Name=postalCode<br>• userFilter1Value=78045##12204<br>• userFilter2Name=<br>• userFilter2Value=<br>• userFilter3Name=<br>• userFilter3Value=<br>• filterValueDelimiter=## |
| User with **managerUid = 17981 or 17854** and **managerLogin = DINORAH.PREWITT or JOELLA.SHANNON** | • userFilter1Name=managerUid<br>• userFilter1Value=17981~17854<br>• userFilter2Name=managerLogin<br>• userFilter2Value=DINORAH.PREWITT~SHIRLEY.THOMAS<br>• userFilter3Name=<br>• userFilter3Value=<br>• filterValueDelimiter=~ |

**Note:**

Filter value name and the value of the filter are both case sensitive. Using the example above, any of the following would be an invalid filter, and return no results:

- Example 1:
  - userFilter1Name=**MANAGERUID**
  - userFilter1Value=17981~17854
  - userFilter2Name=managerLogin
  - userFilter2Value=DINORAH.PREWITT~SHIRLEY.THOMAS
- Example 2:
  - userFilter1Name=managerUid
  - userFilter1Value=17981~17854
  - userFilter2Name=managerLogin
  - userFilter2Value=**Dinorah.Prewitt**~SHIRLEY.THOMAS
  - Example 3:
    - **USERFilter1Name**=managerUid
    - userFilter1Value=17981~17854
    - userFilter2Name=managerLogin
    - userFilter2Value=DINORAH.PREWITT~SHIRLEY.THOMAS
- Example 4:
  - userFilter1Name=managerUid
  - userFilter1Value=17981~17854
  - userFilter2Name=managerLogin
  - **USERFILTER2VALUE**=DINORAH.PREWITT~SHIRLEY.THOMAS

# Database Setup Steps for Event-driven Data Load

When creating or updating an Oracle Access Governance orchestrated system you can enable the event-driven data load option. This option switches Day-N data load from the default snapshot-based model, to an event-driven one. A prerequisite for this option requires you to create a read-only user in the OIG database and grant required roles and system privileges.

To add a read-only user in the OIG database for the event-driven data load option, complete the following steps:

1. Connect to the OIG database as SYS and create a read-only user in the OIG database that will be used by Oracle Access Governance to connect to access change events:

```
create user <username> identified by <password>;
```

For example:

```
create user ag2oigro identified by mypassword;
```

2. Connect to the OIG database as SYS and grant the required roles and system privileges to the read-only user you created in the previous step:

```
GRANT CREATE SESSION TO <read-only user>;
GRANT SELECT ANY TABLE TO <read-only user>;
GRANT CREATE ANY TRIGGER TO <read-only user>;
GRANT ADMINISTER DATABASE TRIGGER TO <read-only user>;
GRANT CREATE TABLE TO <read-only user>;
GRANT CREATE SYNONYM TO <read-only user>;
GRANT UNLIMITED TABLESPACE TO <read-only user>;

GRANT CONNECT TO <read-only user>;
GRANT RESOURCE TO <read-only user>;
```

For example:

```
GRANT CREATE SESSION TO ag2oigro;
GRANT SELECT ANY TABLE TO ag2oigro;
GRANT CREATE ANY TRIGGER TO ag2oigro;
GRANT ADMINISTER DATABASE TRIGGER TO ag2oigro;
GRANT CREATE TABLE TO ag2oigro;
GRANT CREATE SYNONYM TO ag2oigro;
GRANT UNLIMITED TABLESPACE TO ag2oigro;

GRANT CONNECT TO ag2oigro;
GRANT RESOURCE TO ag2oigro;
```

3. Connect to the OIG database as the OIG DB Schema Owner and run the following command to create a script that will create synonyms for OIG tables for the read-only user:

```
setheading on
setlinesize 1500
setnumformat 99999999999999999999
setpagesize 25000
spool synon.out
SELECT 'create synonym <read-only user>.'||TNAME||' for
<OIG_SCHEMA_USER_NAME>.'||TNAME||';'
FROM TAB
WHERE tabtype = 'TABLE';
spool off
```

For example:

```
setheading on
setlinesize 1500
setnumformat 99999999999999999999
setpagesize 25000
spool synon.sql
SELECT 'create synonym ag2oigro.'||TNAME||' for <OIG_SCHEMA_USER_NAME>.'||
TNAME||';'
```

```
FROM TAB
WHERE tabtype = 'TABLE';
spool off
```

4. Connect to the OIG database as the read-only user, and create the synonyms using the script created in the previous step:

   ```
   @<scriptname>
   ```

   For example:

   ```
   @synon.sql
   ```