Oracle® Identity Governance

Configuring the Google Cloud Platform Connector

12c (12.2.1.3.0)
F53517-03

Oracle Identity Governance Configuring the Google Cloud Platform Connector, 12c (12.2.1.3.0)

F53517-03

Primary Author: Oracle Corporation

Contents

Preface

This guide describes the connector that is used to onboard Google Cloud Platform applications to Oracle Identity Governance.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For information about installing and using Oracle Identity Governance 12.2.1.4.0, visit the following Oracle Help Center page:

https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/index.html

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

https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.3/index.html

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

https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/index.html

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

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

Conventions

The following text conventions are used in this document:

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

List of Figures

List of Tables

1

Introduction to the Connector

Oracle Identity Governance is a centralized identity management solution that provides self service, compliance, provisioning and password management services for applications residing on-premise or on the Cloud. Oracle Identity Governance connectors are used to integrate Oracle identity Governance with the external identity-aware applications. The Google Cloud Platform Connector lets you onboard applications, pertaining to the Google Cloud Platform target system, in Oracle Identity Governance.

> **Note:**
>
> In this guide, the connector that is deployed using the **Applications** option on the **Manage** tab of Identity Self Service is referred to as an **AOB application**.

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

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

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

1.1 Certified Components

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

Table 1-1 Certified Components

Component	Requirement for AOB Application
Oracle Identity Governance or Oracle Identity Manager	You can use any one of the following releases: Oracle Identity Governance 12c PS4 (12.2.1.4.0) or later version Oracle Identity Governance 12c PS3 (12.2.1.3.0) or later version
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later
Target systems	Google Cloud Platform Connector or SDK version 1.32.1
Connector Server	11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 and later

1.2 Certified Languages

The connector supports the following languages:

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

- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.3 Usage Recommendation

If you are using Oracle Identity Governance 12*c* (12.2.1.3.0) or later, then use the latest 12.2.1.*x* version of this connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service.

1.4 Support for Connector Operations

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

Table 1-2 Supported Connector Operations

Operation	Supported?
User Management	-
Create user	Yes
Update user	Yes
Delete User	Yes
Enable user	Yes
Disable user	Yes
Change or Reset password	Yes
Add Child (Assign/Remove to a user account)	-
Add/Remove Nick Names	Yes
Entitlement Grant Management	-
Add/Remove Admin Role	Yes
Add/Remove Project Role	Yes
Add/Remove Organization Role	Yes
Add/Remove Group	Yes
Group Management	-
Add Group	Yes
Update Group	Yes
Remove Group	Yes

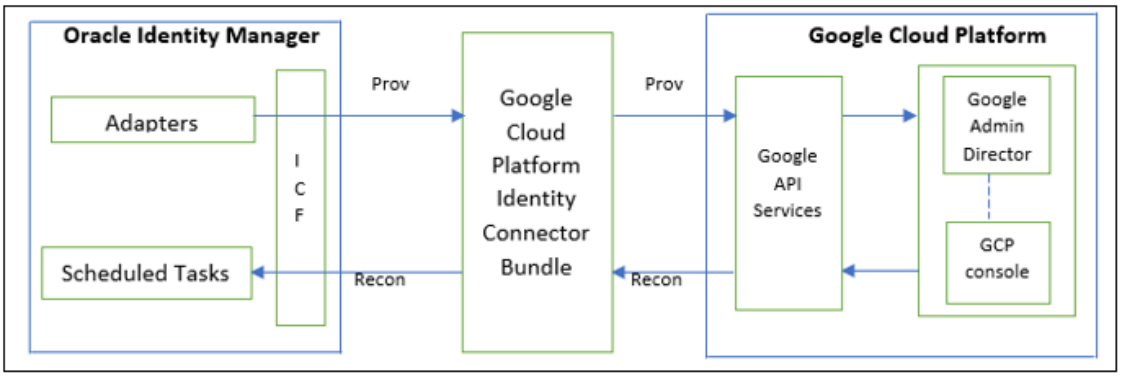
> **Note:**
>
> All the required information is available in the predefined application templates of the connector installation package. For more information about the artifacts related to groups, see Connector Objects Used for Groups Management.

1.5 Connector Architecture

The Google Cloud Platform Connector enables management of accounts on the target system through Oracle Identity Governance.

Figure 1-1 shows architecture of the Google Cloud Platform connector.

Figure 1-1 Architecture of the Google Cloud Platform Connector



As shown in this figure, Google Cloud Platform is configured as a target resource of Oracle Identity Governance. Through provisioning operations performed on Oracle Identity Governance, accounts are created and updated on the Google Admin Directory for OIM Users. Google Cloud Platform perspective, we're managing the GCP specific Project Roles. Through reconciliation, account data that is created and updated directly on the target system is fetched into Oracle Identity Governance and stored against the corresponding OIM Users.

The Google Cloud Platform connector is implemented by using the Identity Connector Framework (ICF). ICF is distributed together with Oracle Identity Governance. You do not need to configure or modify ICF.

During provisioning, the Adapters invoke an ICF operation, ICF in turn invokes an operation on the Google Cloud Platform Identity Connector Bundle and then the bundle calls the appropriate APIs of the Google Cloud Platform Admin SDK. These APIs on the target system accept provisioning data from the bundle, carry out the required operation on the target system, and return the response from the target system back to the bundle, which passes it to the adapters.

During reconciliation, a scheduled task invokes ICF operation, ICF in turn invokes a search operation on the Google Cloud Platform Connector Bundle and then the bundle calls the appropriate APIs of the Google Cloud Platform Admin SDK. These APIs extract user records that match the reconciliation criteria and hand them over through the bundle and ICF back to the scheduled task, which brings the records to Oracle Identity Governance.

See Also:

Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for more information about ICF

.

Each record fetched from the target system is compared with Google Cloud Platform resources that are already provisioned to OIM Users. If a match is found, then the update made to the Google Cloud Platform record from the target system is copied to the Google Cloud Platform resource in Oracle Identity Governance. If no match is found, then the user ID of the record is compared with the user ID of each OIM User. If a match is found, then data in the target system record is used to provision a Google Cloud Platform resource to the OIM User.

The Google Cloud Platform Identity Connector Bundle communicates with the Google Workspace Admin SDK's Directory API using the HTTPS protocol. Internally, the library uses the `java.net.HttpURLConnection` class. When you create an application and start using the connector, it sets the following system properties for configuring the proxy for the connections created by the `HttpURLConnection` class:

- https.proxyPort
- https.proxyHost

> **Note:**
>
> Setting of these system properties might have an impact on the JVM and all other classes that use the `HttpURLConnection` class.

In addition, to support user name/password based proxy authentication, the connector provides and registers an implementation of the `java.net.Authenticator` class.

Depending on your application server configuration, it might be necessary to import Google certificates to application server keystore/truststore.

We are using following Google API Services for our connector operations.

- Google Admin SDK
- Cloud Resource Manager
- Identity and Access Management(IAM)
- Groups Settings

1.6 Connector Features

The features of the connector include support for connector server, connector operations in multiple domains, full reconciliation, batched reconciliation, and reconciliation of account status and deleted account data.

Table 1-3 provides the list of features supported by the AOB application connector.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application
User provisioning	Yes
Full reconciliation	Yes
Limited reconciliation	Yes
Batched reconciliation	Yes
Connection pooling	Yes
Use connector server	Yes

Table 1-3 (Cont.) Supported Connector Features Matrix

Feature	AOB Application
Clone applications or create new application instances	Yes
Transformation and validation of account data	Yes
Reconcile user account status	Yes
Reconcile deleted account data	Yes
Perform connector operations in multiple domains	Yes
Test connection	Yes
Reset password	Yes
Group assignment	Yes
Role Assignment	Yes

The following topics provide more information on the features of the AOB application:

- User Provisioning
- Full Reconciliation
- Limited Reconciliation
- Batched Reconciliation
- Connection Pooling
- Support for the Connector Server
- Support for Cloning Applications and Creating Instance Applications
- Support for Reconciliation of Account Status
- Support for Reconciliation of Deleted Account Data
- Support for Connector Operations in Multiple Domains
- Transformation and Validation of Account Data

1.6.1 User Provisioning

User provisioning involves creating or modifying the account data on the target system through Oracle Identity Governance.

For more information about it, see Performing Provisioning Operations.

1.6.2 Full Reconciliation

In full reconciliation, all records are fetched from the target system to Oracle Identity Governance.

> **Note:**
>
> The connector cannot support incremental reconciliation because the target system does not provide a way for tracking the time at which account data is created or modified.

For more information, see Performing Full Reconciliation.

1.6.3 Limited Reconciliation

You can reconcile records from the target system based on a specified filter criterion. To limit or filter the records that are fetched into Oracle Identity Governance during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled.

You can set a reconciliation filter as the value of the Filter Suffix attribute of the user reconciliation scheduled job. The Filter Suffix attribute helps you to assign filters to the API based on which you get a filtered response from the target system.

For more information, see Performing Limited Reconciliation.

1.6.4 Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

For more information, see Performing Batched Reconciliation.

1.6.5 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 Advanced Settings Parameters.

1.6.6 Support for the Connector Server

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

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

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

1.6.7 Support for Cloning Applications and Creating Instance Applications

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

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

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

1.6.8 Support for Reconciliation of Account Status

Support for reconciliation of account status is one of the features where the connector fetches the status information during a reconciliation operation.

During a reconciliation run, the connector can fetch status information along with the rest of the account data.

1.6.9 Support for Reconciliation of Deleted Account Data

The Google Cloud Platform Target Resource User Delete Reconciliation scheduled task can be used to fetch details of deleted target system users.

This information is used to revoke the corresponding Google Cloud Platform resources from OIM Users.

1.6.10 Support for Connector Operations in Multiple Domains

By default, this connector supports reconciliation and provisioning operations within a single domain. However, you can configure the connector for performing connector operations in more than one domain by specifying a value for the `supportMultipleDomain` parameter in Advance Settings.

For more information, see Advanced Settings Parameters.

1.6.11 Transformation and Validation of Account Data

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

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

2

Creating an Application By Using the Google Cloud Platform Connector

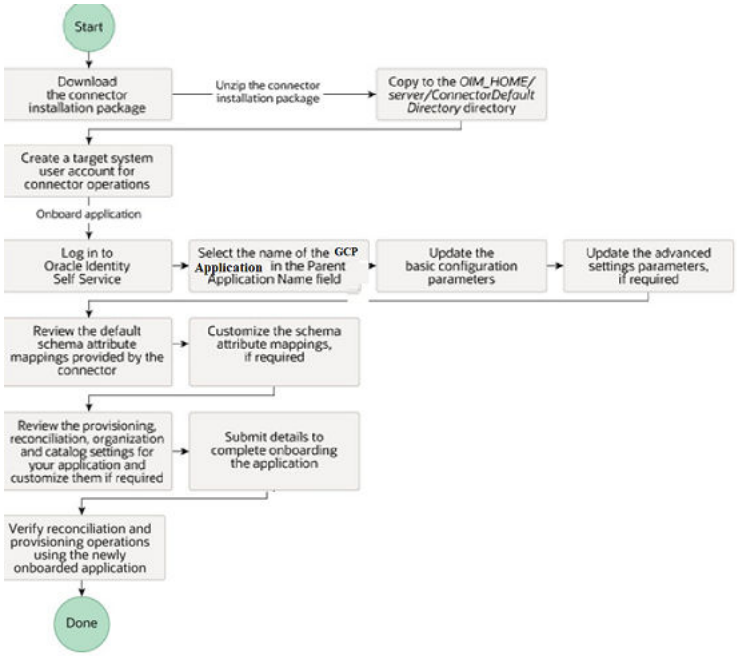
The following are the list of topics:

2.1 Process Flow for Creating an Application By Using the Connector

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

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

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



2.2 Prerequisites for Creating an Application By Using the Connector

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

- Downloading the Connector Installation Package
- Configuring the Target System

2.2.1 Downloading the Connector Installation Package

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

To download the connector installation package:

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

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

2.2.2 Configuring the Target System

This is a high-level summary about the tasks to be performed on the target system before you create the application.

The pre-installation process involves performing the following tasks:

> **Note:**
>
> The detailed instructions for performing each of these tasks are available in the Google Cloud Platform Documentation at `https://cloud.google.com/docs/`

1. Create a project and register your client application with the Google Cloud Platform in Google Cloud Console .
2. Select **APIs & Services**, and then select **Enabled APIs & services**. Search for **Admin SDK**, **Group Settings**, **Cloud Resource Manager**, **IAM** (Identity and Access Management) API Services and enable them.
3. Select **APIs & Services**, and then select **Credentials**. Click **Create Credentials** to create a API key, an OAuth client ID, and a Service account.

a. To create OAuth client ID, configure your consent screen. Click **CONFIGURE CONSENT SCREEN**, select the User Type as **Internal**, and then click **Create**.

b. Enter the application name, user-supported email, and developer email address, and then click **SAVE AND CONTINUE**.

c. Click **ADD OR REMOVE SCOPES** and add all the required scopes and then click **SAVE AND CONTINUE** to create an application.

d. To create an OAuth client ID, choose the Application type as web application, enter the name, and then click **CREATE**. You will get a client ID and a client secret.

4. Open the service account created by you, note down the email ID. Click **Create Google Workspace Marketplace-compatible OAuth Client** and select **Continue** and the copy the client ID.
5. Click the **Keys** tab, click **ADD Key**, and then click **Create new key**. Select the Key type as P12 and click **Create**. The Private key is downloaded to the local computer.
6. Specify the location of this Private key in the **Service Account Private Key** field when you perform the procedure as described in Basic Configuration Parameters.
7. Add scopes and authorize the registered client application. To do so:

   a. Login to the Google Admin Console using the https://admin.google.com link with an account that has administrative privileges in the Google instance.

   b. Choose **Security** and click **Access and data controls**.

   c. Click **API Controls** and search for *Domain-wide delegation* option, and click **MANAGE DOMAIN-WIDE DELEGATION**.

   d. Click **Add new** next to API clients, enter the multi-digit Client Number that was provided during the Google Service Account creation.

   e. In the **One or More API Scopes** field, enter the scopes listed in the **Google Applications Scope** field. These scope values must be separated by commas, but ensure that the double quotes (") are removed.

   f. Click **Authorize**.

   Once this is completed, the **Test Application** button will successfully run and connect to the Google Application instance.
8. Create a user account on the target system. The connector uses this account to connect to the target system during each connector operation. Post account creation, assign the **Groups Admin** and **User Management Admin** admin roles to the newly created account.
9. Enable access to various Google administrative APIs available in the Google Cloud Platform Business Domain. The administrative API allows you to manage user accounts and synchronizes Google Cloud Platform user accounts with your own user account
10. Enable external user access to groups in Google Cloud Platform. Perform this step only if you want external users to access groups in Google Cloud Platform.

2.3 Creating an Application By Using the Google Cloud Platform Connector

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

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

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

1. To create an application in the Identity Self Service, follow the following high-level steps:
   a. Log in to Identity Self Service either by using the **System Administration** account, or using an account with the **ApplicationInstanceAdministrator** admin role.
   b. Ensure the **Connector Package** option is selected while creating an application.
   c. Update the basic configuration parameters to include connectivity-related informa
   d. If required, update the advanced setting parameters to update configuration entries related to connector operations.
   e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.
   f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.
   g. Review the details of the application and click **Finish** to submit the application details. The application is created in Oracle Identity Governance.
   h. When you are prompted whether you want to create a default request form, click **Yes** or **No**.
   If you click **Yes**, then the default form is automatically created and is attached with the newly created application. The default form is created with the same name as the application. The default form cannot be modified later. Therefore, if you want to customize it, click **No** to manually create a new form and attach it with your application.
2. Verify reconciliation and provisioning operations on the newly created application.

> **Note:**
>
> - Configuring the Google Cloud Platform Connector for details on basic configuration and advanced settings parameters, default user account attribute mappings, default correlation rules, and reconciliation jobs that are predefined for this connector
> - Configuring Oracle Identity Governance for details on creating a new form and associating it with your application, if you chose not to create the default form

2.4 Deploying the Connector Bundle in a Connector Server

You can deploy the connector either locally in Oracle Identity Manager or remotely in the Connector Server. A Connector Server is an application that enables remote execution of an Identity Connector, such as the GCP connector.

To deploy the connector bundle remotely in a Connector Server, follow the instructions at **Creating an Application By Using the Google Cloud Platform Connector** .

> **Note:**
>
> - You can download the Connector Server from the Oracle Technology Network web page.
> - See Creating the IT Resource for the Connector Server for related information.
> - See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about installing, configuring, and running the Connector Server.

To install the connector into the Connector Server:

1. Stop the Connector Server.
2. Copy the Google Cloud Platform connector bundle into the *CONNECTOR_SERVER_HOME*/bundles directory.
3. Start the Connector Server. See Options Supported by the connectorserver.sh Script for information about starting the Connector Server.

3
Configuring the Google Cloud Platform Connector

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

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to Google Cloud Platform Connector.

Table 3-1 Basic Configuration Parameters for Google Cloud Platform Connector

Parameter	Mandatory?	Description
Service Account ID	Yes	Enter the email address of the service account created.
Service Account User	Yes	Enter the user name of account that you created to log in to the client application. **Sample value**: admin@mydomain.com
Service Account Private Key	Yes	Enter the name and complete the path to the directory containing the private key. This is the same location to which the private key is saved in when you perform the procedure described in Configuring the Target System. **Sample value**: /scratch/34567890sdfghjk.p12
Google Application Name	Yes	Enter the name of the project that was created as part of registering the client application.
Google Domain Name	Yes	Enter the name of your Google Cloud Platform Connector domain. **Sample value**: mydomain.com

Table 3-1 (Cont.) Basic Configuration Parameters for Google Cloud Platform Connector

Parameter	Mandatory?	Description
GCP Project ID	Yes	Enter the name of Google Cloud Platform Project ID
Scope	Yes	Enter the scope of your client application. **Default value**: `"https://www.googleapis.com/auth/cloud-platform", "https://www.googleapis.com/auth/admin.directory.user", "https://www.googleapis.com/auth/admin.directory.group", "https://www.googleapis.com/auth/admin.directory.group.member", "https://www.googleapis.com/auth/admin.directory.rolemanagement", "https://www.googleapis.com/auth/admin.directory.orgunit", "https://www.googleapis.com/auth/apps.groups.settings"`
Connector Server Name	No	Enter the name of Connector Server IT resource, if you are using the Google Cloud Connector together with a Java Connector Server.
Proxy Host	No	Enter the proxy host name. This is useful when a connector must be used in the network protected by the web proxy. Check with your network administrator
Proxy Password	No	Enter the proxy password. This is useful when a connector must be used in the network protected by the web proxy. Check with your network administrator
Proxy Port	No	Enter the proxy port number. This is useful when a connector must be used in the network protected by the web proxy. Check with your network administrator for more information about proxy configuration.

Table 3-1 (Cont.) Basic Configuration Parameters for Google Cloud Platform Connector

Parameter	Mandatory?	Description
Proxy Username	No	Enter the proxy user name. This is useful when a connector is to be used in the network protected by the web proxy. Check with your network administrator for more
GCP Organisation ID	Yes	Enter the unique ID of Google Cloud Platform “organization”.

3.2 Advanced Settings Parameters

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

Table 3-2 Advanced Settings Parameters

Parameter	Mandatory?	Description
Connector Name	Yes	This parameter holds the name of the connector class. **Default value:** org.identityconnectors.gcp.GCPConnector
Connector Package Name	Yes	This parameter holds the name of the connector bundle package. **Default value:** org.identityconnectors.gcp
Connector Package Version	Yes	This parameter hods the version of the connector bundle class. **Default value:** 12.3.0
supportMultipleDomain	No	This entry specifies whether the connector can perform connector operations in a single or multiple domain. By default, the connector performs connector operations only on the domain specified as the value of the Google Domain Name basic configuration parameter. Set the value of this entry to true if you want the connector to perform connector operations in all the domains present in Google Cloud Platform Connector. **Default value:** false

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
supportDeleteIdentity	No	This entry specifies whether the connector can delete the account in directory or just remove the entitlements & keeps the account. Set the value to true if you want to delete the account in Directory as well. **Default value:** false
Pool Max Idle	No	Maximum number of idle objects in a pool. **Sample value:** 10
Pool Max Size	No	Maximum number of connections that the pool can create. **Sample value:** 10
Pool Max Wait	No	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. **Sample value:** 150000
Pool Min Evict Idle Time	No	Minimum time, in milliseconds, the connector must wait before evicting an idle object. **Sample value:** 120000
Pool Min Idle	No	Minimum number of idle objects in a pool. **Sample value:** 1

3.3 Attribute Mappings

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

Google Cloud Platform Connector User Account Attributes

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

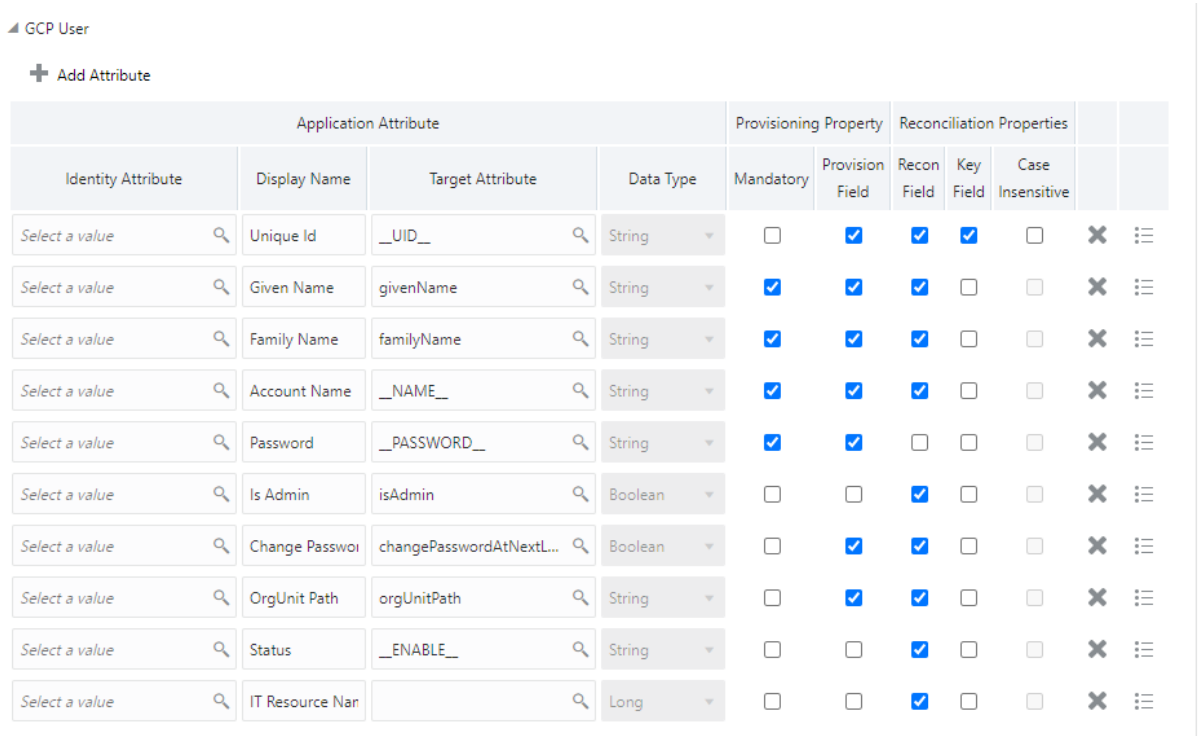
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attribute Mappings for Google Cloud Platform Connector User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Unique Id	__UID__	String	No	Yes	Yes	Yes	No
Given Name	givenName	String	Yes	Yes	Yes	No	Not applicable
Family Name	familyName	String	Yes	Yes	Yes	No	Not applicable
Account Name	__NAME__	String	Yes	Yes	Yes	No	Not applicable
Password	__PASSWORD__	String	Yes	Yes	No	No	Not applicable
Is Admin	isAdmin	Boolean	No	No	Yes	No	Not applicable
Change Password At Next Login	changePasswordAtNextLogin	Boolean	No	Yes	Yes	No	Not applicable
OrgUnit Path	orgUnitPath	String	No	Yes	Yes	No	Not applicable
Status	__ENABLE__	String	No	No	Yes	No	Not applicable
IT Resource Name	-	Long	No	No	Yes	No	Not applicable

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

Figure 3-1 Default Attribute Mappings for Google Cloud Platform Connector User Account



Nick Names Child Attributes

Table 3-4 lists the attribute mappings for nick names between the process form fields in Oracle Identity Governance and Google Cloud Platform Connector attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

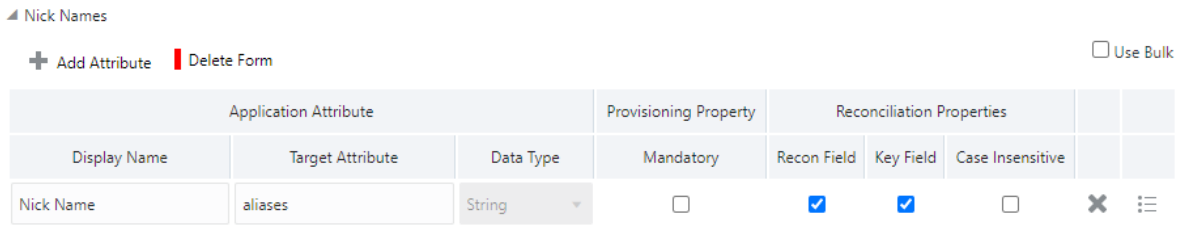
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4 Default Attribute Mappings for Google Cloud Platform Connector Nick Name

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

Figure 3-2 shows the default Nick Names child attribute mapping.

Figure 3-2 Default Attribute Mappings for the Nick Name



Group Names Child Attributes

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

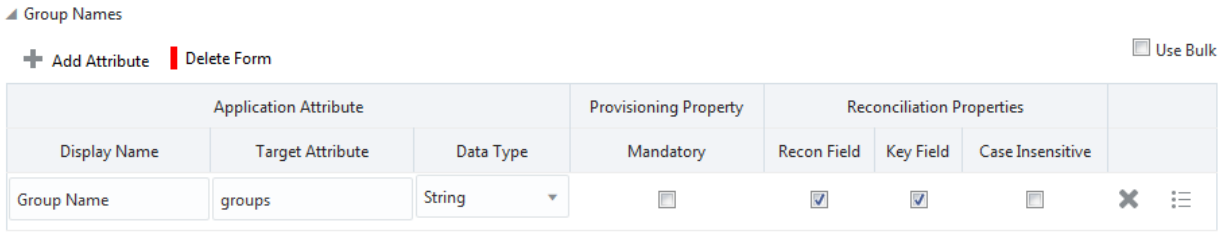
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5 Default Attribute Mappings for Google Cloud Platform Connector Group Name

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

Figure 3-3 shows the default Group Names child attribute mapping.

Figure 3-3 Default Attribute Mappings for the Group Name



Admin Role Names Child Attributes

Table 3-6 lists the attribute mappings Admin Role Name between the process form fields in Oracle Identity Governance and Google Cloud Platform Connector attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

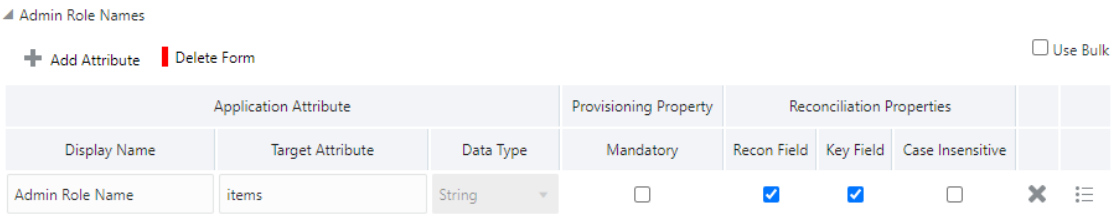
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-6 Default Attribute Mappings for Google Cloud Platform Connector Admin Role Name

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

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

Figure 3-4 Default Attribute Mappings for the Admin Role Name



Project Role Names Child Attributes

Table 3-7 lists the attribute mappings Project Role Names between the process form fields in Oracle Identity Governance and Google Cloud Platform Connector attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

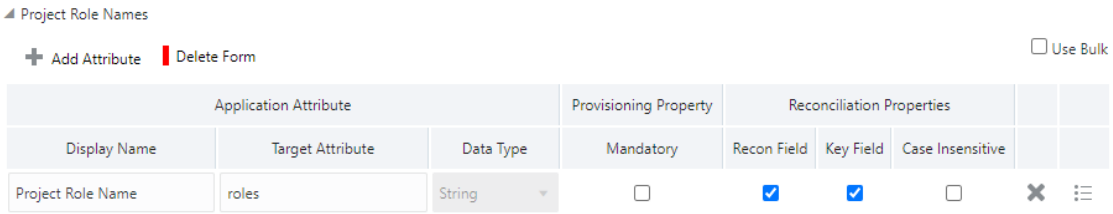
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-7 Default Attribute Mappings for Google Cloud Platform Connector Project Role Name

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

Figure 3-5 shows the default Project Role Names child attribute mapping.

Figure 3-5 Default Attribute Mappings for the Project Role Name



Organization Role Name

Table 3-8 lists the attribute mappings **Organization Role Name** between the process form fields in Oracle Identity Governance and Google Cloud Platform Connector attributes. The table lists whether or not a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

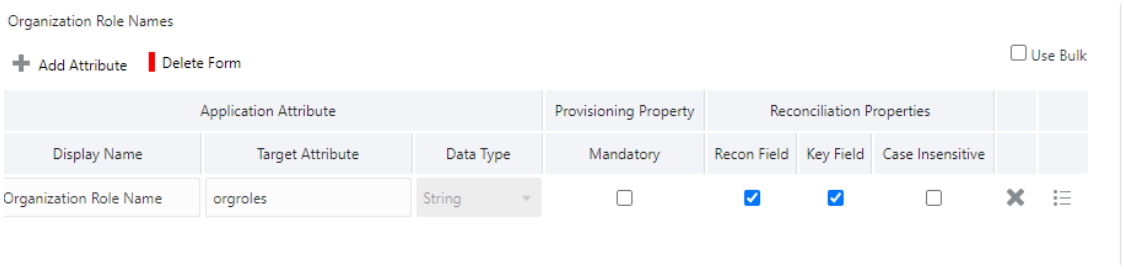
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-8 Default Attribute Mappings for Google Cloud Platform Connector Organization Role Names

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

Default Attribute Mappings for the Organization Role Name shows the default Organization Role Name child attribute mapping.

Figure 3-6 Default Attribute Mappings for the Organization Role Names



3.3.1 Supported Attributes

While the Google Cloud Platform Connector provides support for few single-valued attributes and few multi-valued attributes, it does not extend support for other multi-valued attributes or single valued custom attributes such as Department or Job Title.

The following out-of-the-box and additional single valued attributes are supported by the Google Cloud Platform Connector:

Table 3-9 Supported Attributes

Supported Out of the Box Attributes	Supported Additional Attributes
__NAME__	isDelegatedAdmin
__UID__	agreedToTerms
__PASSWORD__	hashFunction
familyName	suspended
givenName	suspensionReason
isAdmin	ipWhitelisted
orgunitpath	customerId
changePasswordAtNextLogin	isMailboxSetup
groups	includeInGlobalAddressList
aliases	thumbnailPhotoUrl
items	lastLoginTime
roles	creationTime
	deletionTime

3.4 Correlation Rules

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

Predefined Identity Rules

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

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

The following block of code lists the default complex correlation rule for a Google Cloud Platform Connector application:

```
"ruleOperator": "OR",
    "ruleElement": [
        {
            "targetAttribute": "__UID__",
            "userAttribute": "GCP User GUID",
            "elementOperator": "Equals",
            "transformName": "None"
        },
        {
            "targetAttribute": "__NAME__",
            "userAttribute": "User Login",
            "elementOperator": "Equals",
            "transformName": "Tokenize",
            "transformParams": [
                {
                    "name": "Space Delimiter",
                    "value": "FALSE"
                },
                {
                    "name": "Token Number",
                    "value": "1"
                },
                {
                    "name": "Delimiters",
                    "value": "'@'"
                }
            ]
        }
    ]
}
```

The preceding complex rule consists of 2 rule elements that are joined by the rule operator OR.

The first rule element is:

__UID__ equals GCP User GUID.

In this rule element:

- __UID__ is an attribute on the target system that uniquely identifies the user account.
- GCP User GUID is a field on the OIM User form that holds the unique ID of the Google Cloud Platform Connector user.

The second rule element is:

Tokenize (__NAME__) equals User Login.

In this rule element:

- Tokenize (__NAME__) is the name part in the email address of the Google Cloud Platform Connector account.
- User Login is the field on the OIM User form.

Predefined Situations and Responses

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

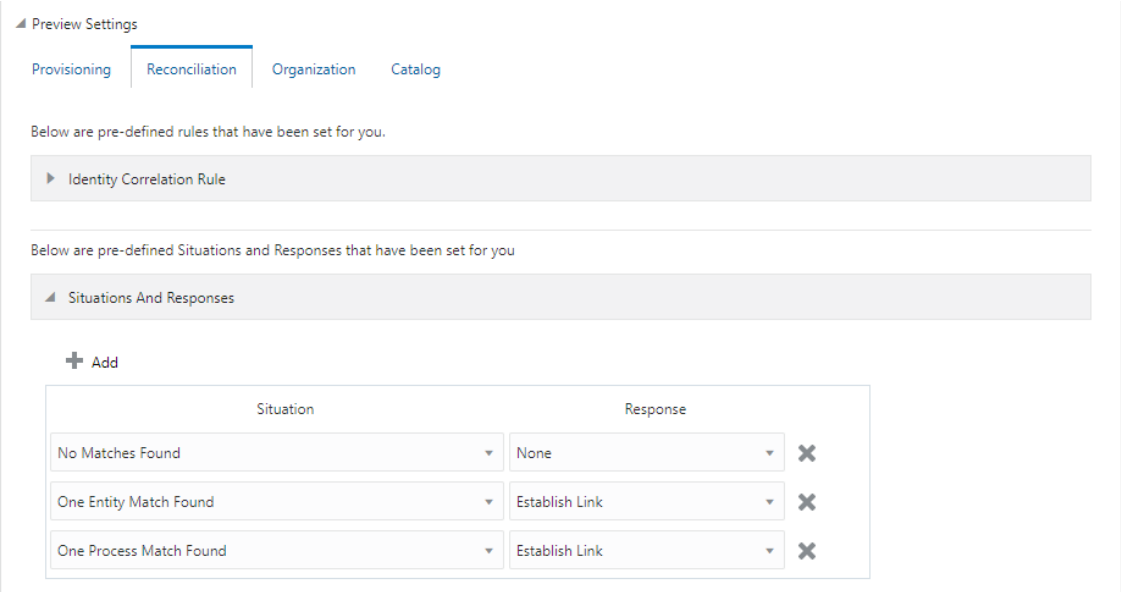
Table 3-10 lists the default situations and responses for the Google Cloud Platform Connector application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.*

Table 3-10 Predefined Situations and Responses for Google Cloud Platform Connector

Situation	Response
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Figure 3-7 shows the situations and responses that the connector provides by default.

Figure 3-7 Predefined Situations and Responses for Google Cloud Platform Connector



3.5 Reconciliation Jobs

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

User Reconciliation Job

You can either use these predefined jobs or edit them to meet your requirements. Alternatively, you can create custom reconciliation jobs. For information about editing these predefined jobs

or creating new ones, see Updating Reconciliation Jobs in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.*

The Google Cloud Platform Connector Target Resource User Reconciliation job is used to reconcile user data from a target application.

Table 3-11 Parameters of the Google Cloud Platform Connector Target Resource User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system.
Filter	This attribute holds the ICF Filter written using ICF-Common Groovy DSL. See Performing Limited Reconciliation for more information about this attribute.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: User Do not change the default value.

Delete User Reconciliation Job

The Google Cloud Platform Connector Target Resource User Delete Reconciliation job is used to reconcile deleted user data from a target application.

Table 3-12 Parameters of the Google Cloud Platform Connector Target Resource User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: User Do not change the default value.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- GCP Group Lookup Reconciliation
- GCP OrgUnit Lookup Reconciliation

- GCP Admin Roles Lookup Reconciliation
- GCP Project Roles Lookup Reconciliation
- GCP Organisation Roles Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-13 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Lookup Name	This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched. Depending on the Reconciliation job that you are using, the default values are as follows: • For GCP Group Lookup Reconciliation: Lookup.GCP.Groups • For GCP OrgUnit Lookup Reconciliation: Lookup.GCP.OrgUnits • For GCP Admin Roles Lookup Reconciliation: Lookup.GCP.AdminRoles • For GCP Project Roles Lookup Reconciliation: Lookup.GCP.ProjectRoles • For GCP Organisation Roles Lookup Reconciliation: Lookup.GCP.OrganizationRoles
Object Type	Enter the type of object whose values must be synchronized. Depending on the reconciliation job that you are using, the default values are as follows: • For GCP Group Lookup Reconciliation: `Group` • For GCP OrgUnit Lookup Reconciliation: `__ORGUNIT__` • For GCP Admin Roles Lookup Reconciliation: `__ROLE__` • For GCP Project Roles Lookup Reconciliation: `__GCPROLE__` • For GCP Organisation Roles Lookup Reconciliation: __GCPORGROLE__ **Note:** Do not change the value of this attribute.

Table 3-13 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the reconciliation job that you are using, the default values are as follows: • For GCP Group Lookup Reconciliation: `__NAME__` • For GCP OrgUnit Lookup Reconciliation: `__UID__` • For GCP Admin Roles Lookup Reconciliation: `__UID__` • For GCP Project Roles Lookup Reconciliation: __UID__ • For GCP Organisation Roles Lookup Reconciliation: __UID__ **Note:** Do not change the value of this attribute.
Decode Attribute	Name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the reconciliation job that you are using, the default values are as follows: • For GCP Group Lookup Reconciliation: `__NAME__` • For GCP OrgUnit Lookup Reconciliation: `__UID__` • For GCP Admin Roles Lookup Reconciliation: `__NAME__` • For GCP Project Roles Lookup Reconciliation: `__NAME__` • For GCP Organisation Roles Lookup Reconciliation: __NAME__ **Note:** Do not change the value of this attribute.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system. **Note:** It is applicable for "GCP Group Lookup Reconciliation".

4

Performing the Post-configuration Tasks for the Google Cloud Platform Connector

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

The following are the topics that describe the post-configuration tasks for the Google Cloud Platform Connector:

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

4.1 Configuring Oracle Identity Governance

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

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

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

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

4.1.1 Creating and Activating a Sandbox

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

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

4.1.2 Creating a New UI Form

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

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

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

4.1.3 Publishing a Sandbox

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

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

4.1.4 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

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

See Also:

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

4.2 Harvesting Entitlements and Sync Catalog

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

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Reconciliation Jobs.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See for more information about this scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

See Also:

- Reconciliation Jobs for a list of jobs for entitlements (lookup field synchronization)
- Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for information about the Entitlement List and Catalog Synchronization Job scheduled jobs

4.3 Managing Logging

Oracle Identity Governance uses Oracle Java Diagnostic Logging (OJDL) for recording all types of events pertaining to the connector. OJDL is based on java.util.logger.

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

4.3.1 Understanding Log Levels

> **Note:**
>
> When you enable logging, Oracle Identity Governance automatically stores in a log file information about events that occur during 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:

To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Manager 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.

Table 4-1 Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

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

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

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

4.3.2 Enabling Logging

Perform this procedure to enable logging in Oracle WebLogic Server.

1. Edit the logging.xml file as follows:
   a. Add the following blocks in the file:

```
<log_handler name='gcp-handler' level='[LOG_LEVEL]'
          class='oracle.core.ojdl.logging.ODLHandlerFactory'><property
name='logreader:' value='off'/>     <property name='path'
            value='[FILE_NAME]'/>     <property name='format'
          value='ODL-Text'/>     <property name='useThreadName'
          value='true'/>     <property name='locale'
          value='en'/>     <property name='maxFileSize'
          value='5242880'/>     <property name='maxLogSize'
          value='52428800'/>     <property name='encoding'
          value='UTF-8'/>   </log_handler>

<logger name="ORG.IDENTITYCONNECTORS.GCP" level="[LOG_LEVEL]"
          useParentHandlers="false">     <handler
          name="gcp-handler"/>     <handler
          name="console-handler"/>   </logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 4-1 lists the supported message type and level combinations.

      Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

      The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]**:

```
<log_handler name='gcp-handler' level='NOTIFICATION:1'
          class='oracle.core.ojdl.logging.ODLHandlerFactory'><property
name='logreader:' value='off'/>     <property name='path'

value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\oim_ser
ver1\logs\oim_server1-diagnostic-1.log'/>     <property name='format'
          value='ODL-Text'/>     <property name='useThreadName'
          value='true'/>     <property name='locale'
          value='en'/>     <property name='maxFileSize'
          value='5242880'/>     <property name='maxLogSize'
          value='52428800'/>     <property name='encoding'
          value='UTF-8'/>   </log_handler>Copy<logger
name="ORG.IDENTITYCONNECTORS.GCP" level="NOTIFICATION:1"
          useParentHandlers="false">     <handler
          name="gcp-handler"/>     <handler
          name="console-handler"/>   </logger>
```

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

2. Save and close the file.

3. Set the following environment variable to redirect the server logs to a file:

   - For Microsoft Windows:

     ```
     set WLS_REDIRECT_LOG=FILENAME
     ```

   - For UNIX:

     ```
     export WLS_REDIRECT_LOG=FILENAME
     ```

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

4. Restart the application server.

4.4 Creating the IT Resource for the Connector Server

Perform the procedure described in this section only if you have deployed the connector bundle remotely in a Connector Server.

Note:

Before you deploy the connector bundle remotely in a Connector Server, you must deploy the connector in Oracle Identity Manager by performing the procedures described in Managing IT Resources.

Table 4-2 Parameters of the IT Resource for the Google Cloud Platform Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. Sample value: HostName
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. Sample value: 8763
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Governance times out. If the value is zero or if no value is specified, the timeout is unlimited. Sample value: 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 value: false **Note**: It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see Setting SSL for Connector Server and Oracle Identity Governance in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.5 Localizing Field Labels in UI Forms

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

To localize field label that you add to in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear**.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.
4. On the MDS Configuration page, click **Export** and save the archive (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer.
5. Extract the contents of the archive, and open one of the following files in a text editor if you are using Oracle Identity Governance 12c PS3 (12.2.1.3.0) and later:

   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:
   a. Search for the following text:

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

   b. Replace with the following text:

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

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

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

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

      ```
      <trans-unit
                id="$
      {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_AD_US
      ERNAME__c_description']}"><source>Username</source></target></trans-unit><trans-
      unit

      id="sessiondef.oracle.iam.ui.runtime.form.model.gcp.entity.gcpEO.UD_GCP_USR_ACCOU
      NT_NAME__c"><source>Username</source></target></trans-unit>
      ```

   d. Open the resource file from the connector package, for example GoogleCloudPlatform_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_GCP_USR_ACCOUNT_NAME=\u30A2\u30AB\u30A6\u30F3\u30C8\u540D..
   e. Replace the original code shown in Step 6.c with the following:

```
<trans-unit
          id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_GCP_U
SR_ACCOUNT_NAME__c_description']}"><source>Account Name</
source><target>u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target></trans-unit><trans-
unit

id="sessiondef.oracle.iam.ui.runtime.form.model.gcp.entity.gcpEO.UD_GCP_USR_ACCOU
NT_NAME__c_LABEL"><source>Account Name</
source><target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target></trans-unit>
```

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

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

   Sample file name: BizEditorBundle_ja.xlf.

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

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

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

4.6 Configuring SSL

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

> **Note:**
>
> If you are using this connector along with a Connector Server, then there is no need to configure SSL. You can skip this section.

To configure SSL:

1. Obtain the SSL public key certificate of Google Cloud Platform.
2. Copy the public key certificate of Google Cloud Platform 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 -alias ALIAS -trustcacerts -file CERT_FILE_NAME -keystore KEYSTORE_NAME -storepass PASSWORD
   In this command
   - ALIAS is the public key certificate alias.
   - CERT_FILE_NAME is the full path and name of the certificate store (the default is cacerts).
   - KEYSTORE_NAME is the name of the keystore.

- PASSWORD is the password of the keystore.
  The following are sample values for this command:

```
keytool -import -keystore <JAVA_HOME>/jre/lib/security/cacerts -file
<Cert_Location>/fileName.crt -storepass changeit -alias GCP• keytool -
import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file
<Cert_Location>/fileName.crt -storepass DemoTrustKeyStorePassPhrase -
alias GCP
```

> **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. Example:
>
> ```
> keytool -import -keystore /home/oracle/12cPS4/Middleware/wlserver/
> server/lib/DemoTrust.jks -file /home/oracle/12cPS4/GCP_CERT/
> cloudGoogle.cer -storepass DemoTrustKeyStorePassPhrase -alias
> cloudGooglecert1
> keytool -import -keystore /home/oracle/java/jdk1.8.0_191/jre/lib/
> security/cacerts -file /home/oracle/12cPS4APR28/GCP_CERT/
> cloudGoogle.cer -storepass changeit -alias cloudGooglecert2
> ```
>
> – In the Oracle Identity Governance cluster, perform this procedure on each node of the cluster and then restart each node.
>
> – Ensure that the system date for Oracle Identity Governance is in sync with the validity date of the SSL certificate to avoid any errors during SSL communication.

5

Using the Google Cloud Platform Connector

You can use the Google Cloud Platform Connector for performing reconciliation and provisioning operations after configuring the application to meet your requirements.

This chapter is divided into the following sections:

5.1 Configuring Reconciliation

You can configure the connector to specify the type of reconciliation and its schedule. This section provides information on the following topics related to configuring reconciliation:

Topics

5.1.1 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Governance.

After you create the application, you must first perform full reconciliation. To perform a full reconciliation run, ensure that no value is specified for the Filter parameter of the job for reconciling users and groups.

5.1.2 Performing Limited Reconciliation

By default, all target system records are reconciled during the current reconciliation run. You can customize this process by specifying the subset of target system records that must be reconciled.

You can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a Filter attribute (a scheduled task attribute) that allows you to use Google Cloud Platform resource attributes to filter the target system records.

Due to the limited functionality support of Google Cloud Platform target system with respect to filtering query for string data type fields, the connector only supports startsWith and equalTo filters. Below are examples for both filters:

- startsWith: startsWith('__NAME__','John')

  In this example, all records whose email address begins with 'John' are reconciled.

- equalTo: equalTo('givenName','John')

  In this example, all records whose givenName is 'John' are reconciled.

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

5.1.3 Performing Batched Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete. You can configure batched reconciliation to avoid such problems.

To configure batched reconciliation, specify a value for the Batch Size attribute of the reconciliation job for user and group reconciliation. You use the Batch Size attribute to specify the number of records that must be included in each batch fetched from the target system.

5.2 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

> **Note:**
>
> If you are using OIG 12cPS4 with 2022OCTBP or later version, log in to **Identity Console**, click **Manage**, and then under System Configuration, click **Scheduler**.

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

In addition to modifying the job details, you can enable or disable a job.

1. On the **Job Details** tab, in the Parameters region, specify values for the attributes of the scheduled task.

Note:

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

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

Note:

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

5.3 Configuring Provisioning

You can configure the provisioning operation for the Google Cloud Platform connector.

This section provides information on the following topics:

- Guidelines on Performing Provisioning Operations
- Performing Provisioning Operations

5.3.1 Guidelines on Performing Provisioning Operations

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

- For a Create User provisioning operation, you must specify a value for the Account Name field along with the domain name. For example, `jdoe@example.com`.
- During a group provisioning operation, if you select **ANYONE_CAN_JOIN** as the value of the Who Can Join field, then you must set the value of the Allow External Members field to **True.** Before you perform the group provisioning operation with the values discussed in this point, ensure you have performed the procedure described in Configuring the Target System.

5.3.2 Performing Provisioning Operations

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

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

Creating a User in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance for details about the fields on the Create User page.

5.4 Connector Objects Used for Groups Management

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

- Lookup Definitions for Groups Management
- Reconciliation Rules and Action Rules for Groups Management
- Reconciliation Scheduled Jobs for Groups Management

5.4.1 Lookup Definitions for Groups Management

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

- Lookup.GCP.GM.Configuration
- Lookup.GCP.GM.ProvAttrMap
- Lookup.GCP.GM.ReconAttrMap

5.4.1.1 Lookup.GCP.GM.Configuration

The `Lookup.GCP.GM.Configuration` lookup definition holds mappings between process form fields (Code Key values) and target system attributes (Decode). This lookup definition is preconfigured and is used during group provisioning operations.

Table 5-1 lists the default entries.

Table 5-1 Entries in the Lookup.GCP.GM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.GCP.GM.ProvAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during provisioning operations.
Recon Attribute Map	Lookup.GCP.GM.ReconAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during reconciliation.

5.4.1.2 Lookup.GCP.GM.ProvAttrMap

The Lookup.GCP.GM.ProvAttrMap lookup definition holds mappings between process form fields (Code Key values) and target system attributes (Decode). This lookup definition is preconfigured and is used during group provisioning operations.

Table 5-3 lists the default entries.

Table 5-2 Entries in the Lookup.GCP.GM.ProvAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Google Cloud Platform Connector Field
Unique Id	__UID__
Allow External Members	allowExternalMembers
Description	description
Email Address	email
Is Archived	isArchived
Group Name	name
Who Can Join	whoCanJoin
Who Can View Group	whoCanViewGroup
Who Can View Membership	whoCanViewMembership

5.4.1.3 Lookup.GCP.GM.ReconAttrMap

The `Lookup.GCP.GM.ReconAttrMap lookup` definition holds mappings between resource object fields (Code Key values) and target system attributes (Decode). This lookup definition is pre-configured and is used during target resource group reconciliation runs.

The Table 5-3 lists the entries.

Table 5-3 Entries in the Lookup.GCP.GM.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Google Cloud Platform Connector Field
OIM Org Name	Organization Name **Note:** This is a connector attribute. The value of this attribute is used internally by the connector to specify the organization of the groups in Oracle Identity Manager.
Unique Id	__UID__
Allow External Members	allowExternalMembers
Description	description
Email Address	email
Is Archived	isArchived
Group Name	name
Who Can Join	whoCanJoin
Who Can View Group	whoCanViewGroup
Who Can View Membership	whoCanViewMembership

5.4.2 Reconciliation Rules and Action Rules for Groups Management

Reconciliation rules are used by the reconciliation engine to determine the identity to which Oracle Identity Governance must assign a newly discovered account on the target system. Reconciliation action rules define that actions the connector must perform based on the reconciliation rules.

- Reconciliation Rule for Groups
- Reconciliation Action Rules for Groups
- Viewing Reconciliation Rules

- Viewing Reconciliation Action Rules

5.4.2.1 Reconciliation Rule for Groups

The following is the process-matching rule for groups:

Rule name: GCP Groups Recon Rule

Rule element: Organization Name Equals OIM Org Name

In this rule element:

- Organization Name is the Organization Name field of the OIM User form.
- OIM Org Name is the organization name of the groups in Oracle Identity Manager. OIM Org Name is the value specified in the Organization Name attribute of the GCP Group Recon scheduled job

5.4.2.2 Reconciliation Action Rules for Groups

Table 5-4lists the action rules for groups reconciliation.

Table 5-4 Action Rules for Reconciliation

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

5.4.2.3 Viewing Reconciliation Rules

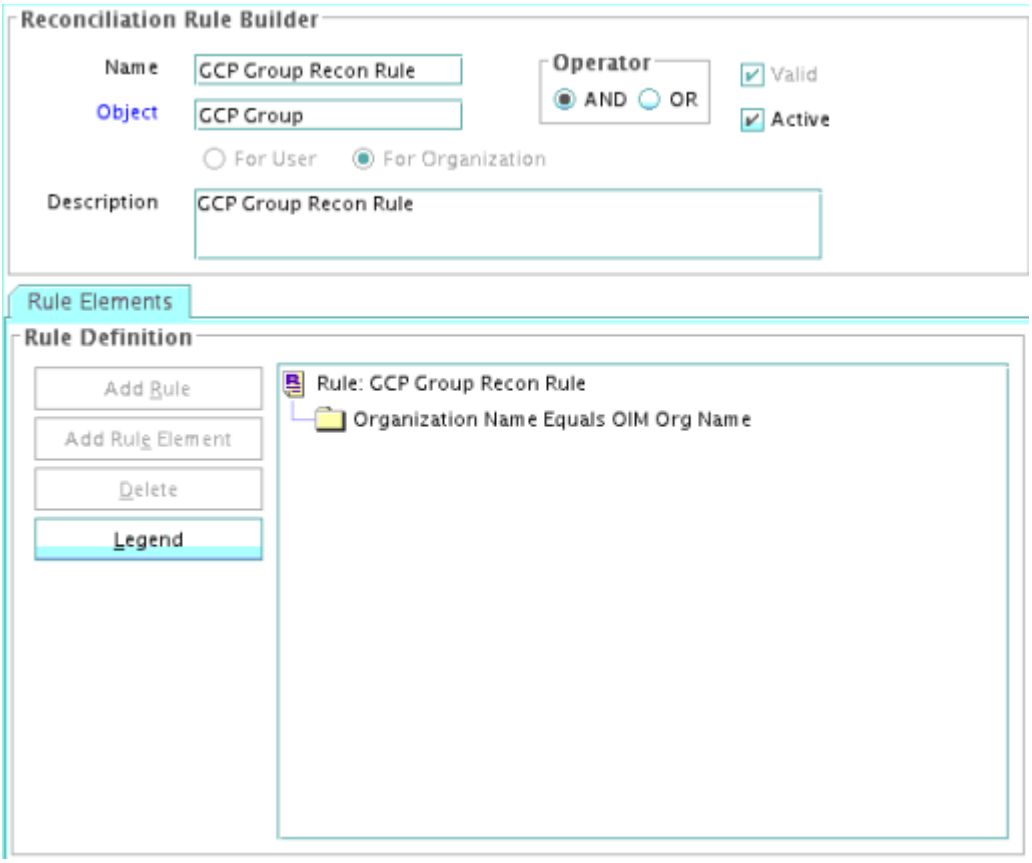
After you deploy the connector, you can view the reconciliation rule for reconciliation by performing the following steps:

> **Note:**
>
> Perform the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for the **GCP Group Recon Rule**.

Figure 5-1 shows the reconciliation rule for groups.

Figure 5-1 Reconciliation Rule for Groups

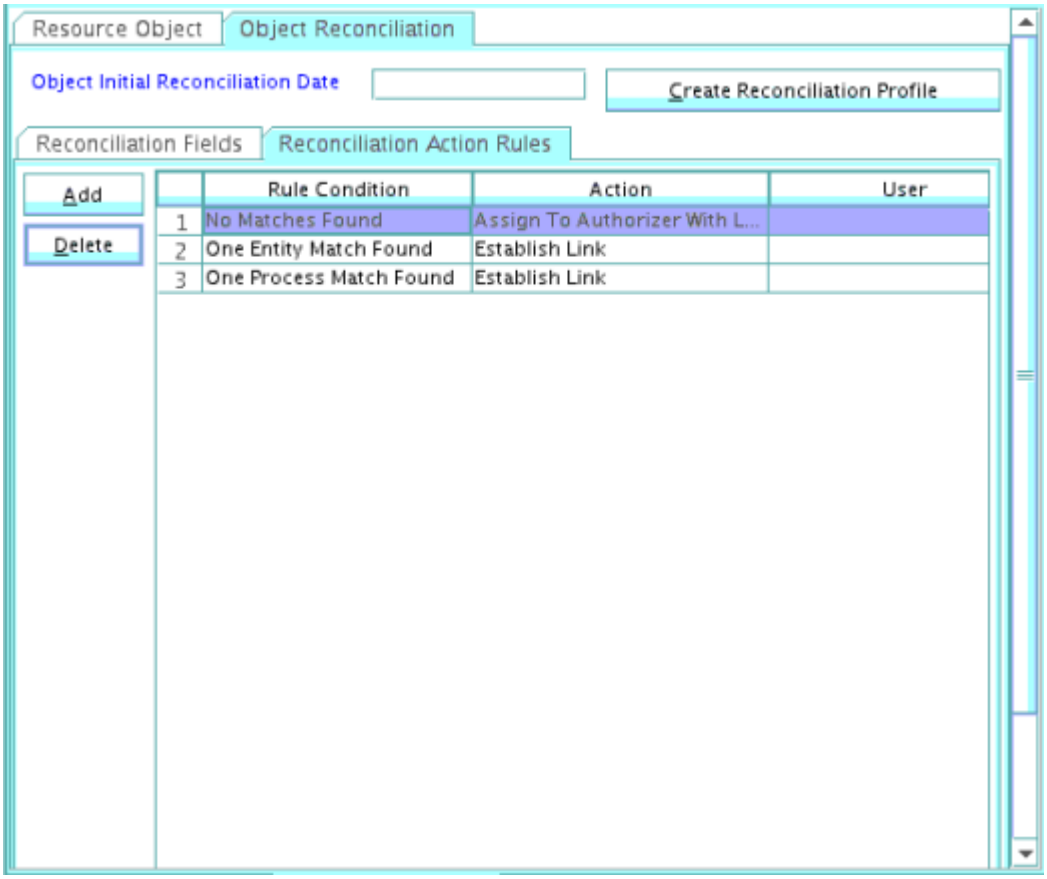


5.4.2.4 Viewing Reconciliation Action Rules

After you create the application by using connector, you can view the reconciliation action rules for groups by performing the following steps:

1. Log in to the Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. Search for and open the **GCP Group** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. shows the reconciliation action rules for groups.

Figure 5-2 Reconciliation Action Rules for Groups



5.4.3 Reconciliation Scheduled Jobs for Groups Management

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

You must specify values for the attributes of the following scheduled jobs:

- GCP Group Recon
- GCP Group Delete Recon

5.4.3.1 GCP Group Recon

You use the GCP Group Recon scheduled job to reconcile group data from the target system.

Table 5-5describes the attributes of this scheduled job.

Table 5-5 Attributes of the GCP Group Recon Scheduled Job

Attribute	Description
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: `GCPGroup` **Note:** You must not change the default value.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `GCPGroup`
Organization Name	Enter the name of the Oracle Identity Manager organization in which reconciled groups must be created or updated.
Filter	This attribute holds the ICF Filter written using ICF-Common Groovy DSL. See Performing Limited Reconciliation for more information about this attribute.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: `GCP Group Recon`
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `Group` Do not change the default value.

5.4.3.2 GCP Group Delete Recon

You use the GCP Group Delete Recon scheduled job to reconcile deleted groups from the target system.

Table 5-6 describes the attributes of this scheduled job.

Table 5-6 Attributes of the GCP Group Delete Recon Scheduled Job

Attribute	Description
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: `GCPGroup`
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `GCPGroup`

Table 5-6 (Cont.) Attributes of the GCP Group Delete Recon Scheduled Job

Attribute	Description
Organization Name	Enter the name of the Oracle Identity Manager organization from which reconciled groups must be deleted.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `Group` Do not change the default value.

6

Extending the Functionality of the Google Cloud Platform Connector

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

This chapter contains the following topics:

6.1 Configuring Transformation and Validation of Data

Configure transformation and validation of user account data by writing Groovy script logic while creating your application.

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Governance.

Similarly, you can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

To configure transformation or validation of user account data, you must write Groovy scripts while creating your application. For more information about writing Groovy script-based validation and transformation logic, see Validation and Transformation of Provisioning and Reconciliation Attributes of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.2 Configuring Action Scripts

You can configure **Action Scripts** by writing your own Groovy scripts while creating your application.

These scripts can be configured to run before or after the enable, disable, or delete an account provisioning operations. For example, you can configure a script to run before every user creation operation.

For information on adding or editing action scripts, see Updating the Provisioning Configuration in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.3 Configuring the Connector for Multiple Installations of the Target System

You must create copies of configurations of your base application to configure it for multiple installations of the target system.

For more information about cloning applications, see Cloning Applications Cloning Applications in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Part I
Appendices

This section contains the following topics:

A

Known Issues and Limitations

The following are the solutions to the commonly encountered issues associated with the GoogleCloudPlatfrom connector:

1. Adding Unsupported **Predefined Role** does not allow to SetIamPolicy for Project resource.
2. Reconciling a User shows the roles (predefined and custom) for project specific only, not for organization.
3. Evoking the account in OIM results in removal of entitlement such as **Project Roles** and **Groups**.
4. Updating **Account Name** (Primary email) for a user, creates a new alternative email addresses(email alias) as previous Account Name.

B

Troubleshooting the Google Cloud Platform Connector

This chapter provides solutions to problems you might encounter after you deploy or while using the Google Cloud Platform Connector

Table B-1 lists solutions to some commonly encountered issues associated with the Google Cloud Platform Connector.

Table B-1 Troubleshooting

Problem	Solution
The following javax.net.ssl.SSLKeyException occurs during reconciliation and provisioning: javax.net.ssl.SSLKeyException: [Security:090504]Certificate chain received from www-proxy.example.com - 148.87.19.20 --> apps-apis.google.com failed hostname verification check. Certificate contained *.google.com but check expected apps-apis.google.com javax.net.ssl.SSLKeyException: [Security:090504]Certificate chain received from www-proxy.example.com - 148.87.19.20 --> apps-apis.google.com failed hostname verification check. Certificate contained *.google.com but check expected apps-apis.google.com	If Oracle Identity Manager is deployed on WebLogic application server with Host Name Verification feature enabled, then you can disable it or use the Custom Host Name Verification feature. However, it is recommended to use Custom Host Name Verification for production environments. For more information, see Using Host Name Verification in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server* for more details.

C

Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the Google Cloud Platform connector.

Table C-1 Files and Directories in the Google Cloud Platform Connector Installation Package

File in the Installation Package	Description
/bundle/org.identityconnectors.gcp-12.3.0	This JAR is the ICF connector bundle.
configuration/GoogleCloudPlatform-CI.xml	This XML file contains configuration information.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to Oracle Identity database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
xml/GoogleCloudPlatform-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/ GoogleCloudPlatform-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User object such as Groups.