

Implementing Security in Dataplex

Enable Dataplex API

1. In the Google Cloud Console, enter **Cloud Dataplex API** in the top search bar.
2. Click on the result for **Cloud Dataplex API** under Marketplace.
3. Click **Enable**.


Task 1. Create a lake, zone, and asset in Dataplex

To apply and test user access to Dataplex resources, you first need to create some Dataplex resources.

In this task, you use the Google Cloud console to create a new Dataplex lake to store customer information, add a raw zone to the lake, and then attach a pre-created Cloud Storage bucket as a new asset in the zone.

To complete this task, **be sure you are logged in as User 1** (`student-03-352aff6d7aa6@qwiklabs.net`), who is a Dataplex Administrator and can create new Dataplex resources in the project.

Create a lake

1. In the Google Cloud Console, in the **Navigation menu** () , navigate to **Analytics > Dataplex**.
- If prompted Welcome to the new Dataplex experience, click **Close**.

2. Under **Manage lakes**, click **Manage**.
3. Click **Create lake**.
4. Enter the required information to create a new lake:

Property	Value
Display Name	Customer Info Lake
ID	Leave the default value.
Region	europa-west4

Leave the other default values.

5. Click **Create**.
- It can take up to 3 minutes for the lake to be created.

Add a zone to the lake

1. On the **Manage** tab, click on the name of your lake.
2. Click **Add zone**.
3. Enter the required information to create a new zone:

Property	Value
Display Name	Customer Raw Zone

ID	Leave the default value.
Type	Raw zone
Data locations	Regional

Leave the other default values.

For example, the option for **Enable metadata discovery** under **Discovery settings** is enabled by default and allows authorized users to discover the data in the zone.

4. Click **Create**.

It can take up to 2 minutes for the zone to be created.

You can perform the next task once the status of the zone is **Active**.

Attach an asset to a zone

1. On the **Zones** tab, click on the name of your zone.
2. On the **Assets** tab, click **Add assets**.
3. Click **Add an asset**.
4. Enter the required information to attach a new asset:

Property	Value
Type	Storage bucket
Display Name	Customer Online Sessions

ID	Leave the default value.
Bucket name	qwiklabs-gcp-02-0b5dd9a1696e-bucket

Leave the other default values.

While the Cloud Storage bucket does not contain any files, you can attach it to the zone now, and newly added files will automatically be integrated into the zone.


5. Click **Done**.
6. Click **Continue**.
7. For **Discovery settings**, select **Inherit** to inherit the Discovery settings from the zone level, and then click **Continue**.
8. Click **Submit**.

Task 2. Assign Dataplex Data Reader role to another user

Following the Google recommendation of least privilege, Dataplex allows Dataplex administrators to grant Dataplex IAM roles to users at the level of the project, lake, zone, and individual assets like a Cloud Storage bucket.

In this task, you use the Google Cloud console to assign the Dataplex Data Reader role to another user, so that they can have read access to the Cloud Storage bucket that is managed as a Dataplex resource.

To complete this task, **remain logged in as User 1** (`student-03-352aff6d7aa6@qwiklabs.net`), who has the appropriate grant Dataplex IAM roles to other users.

1. In the Google Cloud Console, in the **Navigation menu** () , under **Analytics**, navigate to **Dataplex > Secure**.
2. In the **Dataplex resources** menu, expand the arrow next to the project ID (`qwiklabs-gcp-02-0b5dd9a1696e`).
3. Expand the arrow next to the name of your lake.
4. Expand the arrow next to the name of your zone.
5. Click on the asset name (Customer Online Sessions).
6. Click **Grant access**.
7. For **New principals**, enter the email for User 2: `student-04-3140ebc1122c@qwiklabs.net`
8. For **Select a role**, select **Dataplex Data Reader** under **Cloud Dataplex**.
9. Click **Save**.

To see the updated data permissions, refresh the page. It can take a few minutes for the permissions to be applied.

Log out of the project as User 1

Log out of the project as User 1. In the next task, you log in to the project as User 2.

1. Click on the profile icon on the top right of the Google Cloud console.
2. Click **Sign out**.


If asked to confirm, click **Leave**.

Task 3. Test access to Dataplex resources as a Dataplex Data Reader

Users who have been granted only the Dataplex Data Reader role on an asset have access to view the Dataplex asset but cannot modify it. For example, users with only the Dataplex Data Reader role on a Cloud Storage bucket cannot add new files to the bucket that is managed as a Dataplex asset.

In this task, you use the Google Cloud console to test access for User 2 to Dataplex resources by attempting to add a new file to the pre-created Cloud Storage bucket.

To complete this task, **log in to the project as User 2** (`student-04-3140ebc1122c@qwiklabs.net`).

1. In the Google Cloud Console, in the **Navigation menu** () , navigate to **Cloud Storage > Buckets**.
2. Click on the bucket that has been precreated for you: `qwiklabs-gcp-02-0b5dd9a1696e-bucket`
3. Click **Upload files**.
4. Select any file of your choice.

If you need a sample file, you can download the following [test CSV file](#), and use it as the upload file.

5. Click **Open**.

Notice that you receive an error, and no files are uploaded to the bucket.

User 2 is denied access to upload a new file to the Cloud Storage bucket because the user has only been granted read access to the Dataplex asset.

Log out of the project as User 2

Log out of the project as User 2. In the next task, you log in to the project as User 1.


1. Click on the profile icon on the top right of the Google Cloud console.
2. Click **Sign out**.

If asked to confirm, click **Leave**.

Task 4. Assign Dataplex Writer role to another user

In this task, you use the Google Cloud console to assign the Dataplex Writer Role on the bucket to User 2, so that they can modify the bucket by adding new files.

To complete this task, **log in to the project as User 1** (`student-03-352aff6d7aa6@qwiklabs.net`), who has the appropriate grant Dataplex IAM roles to other users.

1. In the Google Cloud Console, in the **Navigation menu** () , under **Analytics**, navigate to **Dataplex > Secure**.
2. In the **Dataplex resources** menu, expand the arrow next to the project ID (`qwiklabs-gcp-02-0b5dd9a1696e`).
3. Expand the arrow next to the name of your lake.
4. Expand the arrow next to the name of your zone.
5. Click on the asset name (Customer Online Sessions).
6. Click on **Edit principal** (pencil icon) next to the email for User 2: `student-04-3140ebc1122c@qwiklabs.net`
7. For **Role**, select **Dataplex Data Writer** under **Cloud Dataplex**.
8. Click **Save**.

To see the updated data permissions, refresh the page. It can take a few minutes for the permissions to be applied. **Log out of the project as User 1**

Log out of the project as User 1. In the next task, you log in to the project as User 2.

1. Click on the profile icon on the top right of the Google Cloud console.

2. Click **Sign out**.


If asked to confirm, click **Leave**.

Task 5. Upload new file to Cloud Storage bucket as a Dataplex Data Writer

Users who have been granted the Dataplex Writer Reader role on an asset have access to modify the asset, including the ability to add new files to a Cloud Storage bucket that is managed as a Dataplex asset.

In this task, you use the Google Cloud console to test access again for User 2 to Dataplex resources by successfully adding a new file to the pre-created Cloud Storage bucket.

To complete this task, **log in to the project as User 2** (`student-04-3140ebc1122c@qwiklabs.net`).

1. In the Google Cloud Console, in the **Navigation menu** () , navigate to **Cloud Storage > Buckets**.
2. Click on the bucket that has been precreated for you: `qwiklabs-gcp-02-0b5dd9a1696e-bucket`
3. Click **Upload files**.
4. Select any file of your choice.

If you need a sample file, you can download the following [test CSV file](#), and use it as the upload file.

5. Click **Open**.

User 2 can successfully upload a new file to the Cloud Storage bucket as a Dataplex Data Writer.