

Implementing Security in Dataplex

experiment Lab    schedule 1 hour    universal\_currency\_alt No cost

show\_chart Introductory



**GSP1157**



**Google Cloud Self-Paced Labs**

## Overview

Dataplex is an intelligent data fabric that enables organizations to centrally discover, manage, monitor, and govern their data across data lakes, data warehouses, and data marts to power analytics at scale.

Dataplex provides a flexible security model that allows you to manage who can access and perform actions on Dataplex resources. Specifically, Dataplex security is implemented using different Dataplex IAM roles that allow users to administer Dataplex lakes, access data in the lake through the attached assets such as a Cloud Storage bucket or BigQuery dataset, or access metadata about the data connected to a lake.

In this lab, you learn how to implement security in Dataplex by logging in to a Google Cloud project as a Dataplex administrator, creating new Dataplex resources, and assigning and testing Dataplex IAM roles to other users. You conclude the lab by successfully uploading a new file to a Cloud Storage bucket as a user that has been granted the appropriate IAM role to modify that specific Dataplex asset.

# What you'll do

- Create a lake, zone, and asset in Dataplex
- Assign Dataplex IAM roles to other users
- Test access to a Dataplex asset as different users with differing Dataplex IAM roles
- Upload a new file to a Cloud Storage bucket managed as a Dataplex asset

## Setup and requirements

After you start the lab, **log in to the Google Cloud console as User 1 ( `student-03-4df865a3b3d1@qwiklabs.net` )** to begin the first task.

## Before you click the Start Lab button

Read these instructions. Labs are timed and you cannot pause them. The timer, which starts when you click **Start Lab**, shows how long Google Cloud resources will be made available to you.

This hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that you use to sign in and access Google Cloud for the duration of the lab.

To complete this lab, you need:

- Access to a standard internet browser (Chrome browser recommended).

**Note:** Use an Incognito or private browser window to run this lab. This prevents any conflicts between your personal account and the Student account, which may cause extra charges incurred to your personal account.

- Time to complete the lab---remember, once you start, you cannot pause a lab.

**Note:** If you already have your own personal Google Cloud account or project, do not use it for this lab to avoid extra charges to your account.

## How to start your lab and sign in to the Google Cloud console

1. Click the **Start Lab** button. If you need to pay for the lab, a pop-up opens for you to select your payment method. On the left is the **Lab Details** panel with the following:
  - The **Open Google Cloud console** button
  - Time remaining
  - The temporary credentials that you must use for this lab
  - Other information, if needed, to step through this lab
2. Click **Open Google Cloud console** (or right-click and select **Open Link in Incognito Window** if you are running the Chrome browser).

The lab spins up resources, and then opens another tab that shows the **Sign in** page.

*Tip:* Arrange the tabs in separate windows, side-by-side.

**Note:** If you see the **Choose an account** dialog, click **Use Another Account**.

3. If necessary, copy the **Username** below and paste it into the **Sign in** dialog.

student-03-4df865a3b3d1@qwiklabs.net

content\_c

You can also find the **Username** in the **Lab Details** panel.

4. Click **Next**.
5. Copy the **Password** below and paste it into the **Welcome** dialog.

x5XjYY67zCP6

content\_co

You can also find the **Password** in the **Lab Details** panel.

#### 6. Click **Next**.

**Important:** You must use the credentials the lab provides you. Do not use your Google Cloud account credentials.

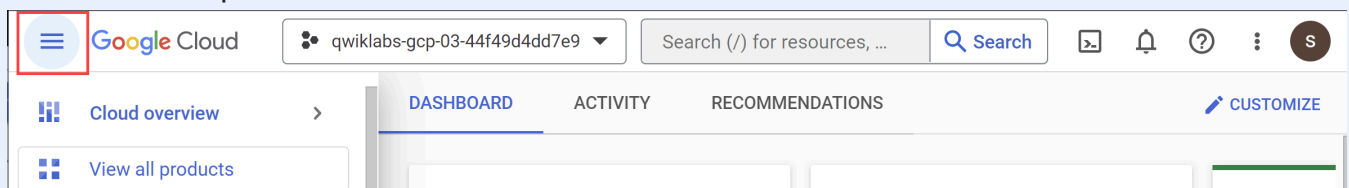
**Note:** Using your own Google Cloud account for this lab may incur extra charges.

#### 7. Click through the subsequent pages:

- Accept the terms and conditions.
- Do not add recovery options or two-factor authentication (because this is a temporary account).
- Do not sign up for free trials.

After a few moments, the Google Cloud console opens in this tab.

**Note:** To view a menu with a list of Google Cloud products and services, click the **Navigation menu** at the top-left.



## 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-03-4df865a3b3d1@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	us-central1

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-04-edd6e4183fb1 -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**.

Click *Check my progress* to verify the objective.



Create a lake, zone, and asset in Dataplex

Check my progress


*Assessment Completed!*

## 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-03-4df865a3b3d1@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-04-edd6e4183fb1 ).
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-da7f1856095c@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.

Click *Check my progress* to verify the objective.





Assign Dataplex Data Reader role to another user

Check my progress

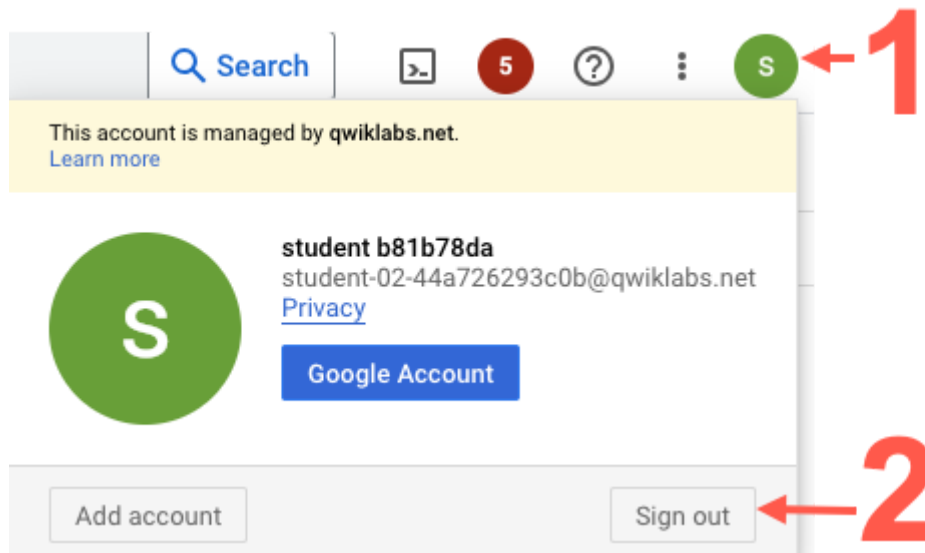
*Assessment Completed!*

## 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-da7f1856095c@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-04-edd6e4183fb1` -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.

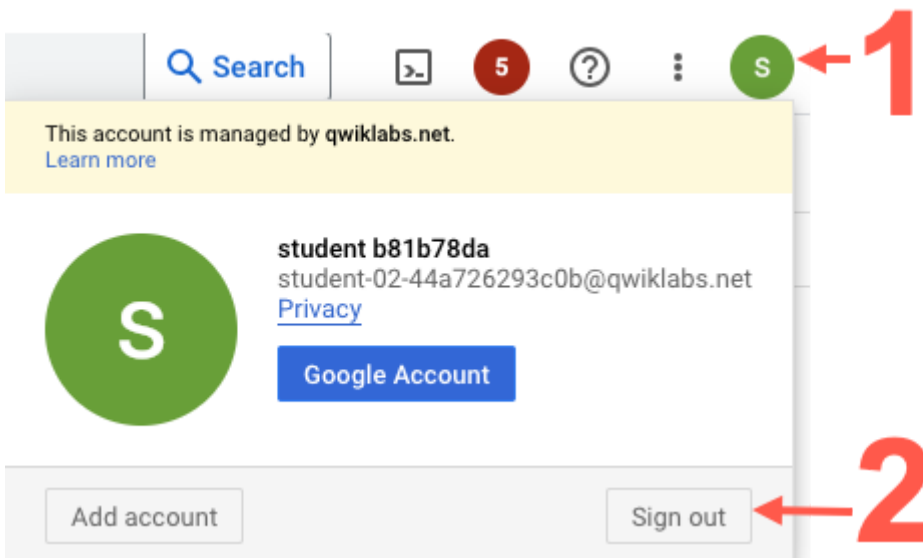
User 2 is denied access to upload a new file to the Cloud Storage bucket because the user has only been granted read access to the Dataplex asset.

## 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-03-4df865a3b3d1@qwiklabs.net` ), who has the appropriate grant Dataplex IAM roles to other users.

1. In the Google Cloud Console, in the **Navigation menu** ( $\equiv$ ), under **Analytics**, navigate to **Dataplex > Secure**.
2. In the **Dataplex resources** menu, expand the arrow next to the project ID ( `qwiklabs-gcp-04-edd6e4183fb1` ).
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-da7f1856095c@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.

Click *Check my progress* to verify the objective.



Assign Dataplex Data Writer role to another user

Check my progress

*Assessment Completed!*

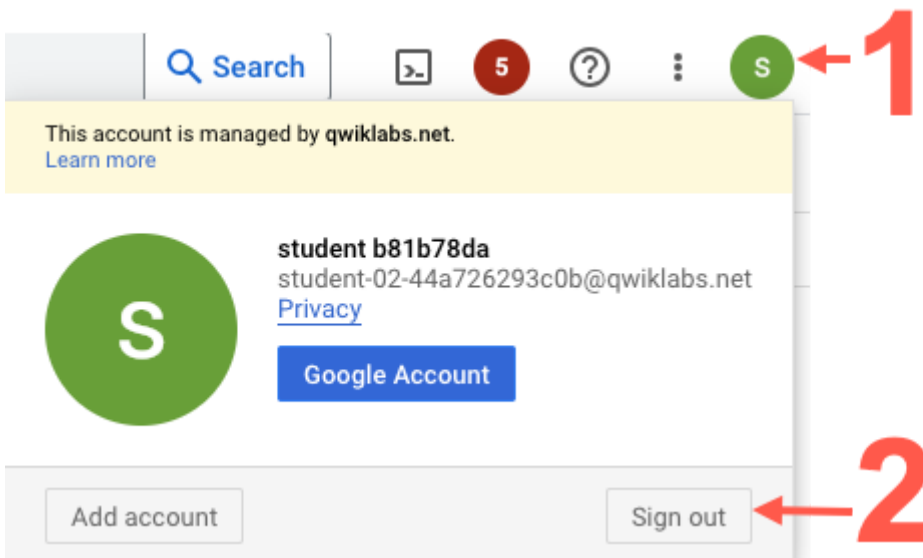
## Log out of the project as User 1

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-da7f1856095c@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-04-edd6e4183fb1` -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.

Click *Check my progress* to verify the objective.



Upload a file to the Cloud Storage bucket as a Dataplex Data Writer

Check my progress

*Assessment Completed!*

## Congratulations!

You implemented security in Dataplex by assigning and testing the appropriate Dataplex IAM role to another user, so that the user can successfully modify the files in a Cloud Storage bucket that is managed as a Dataplex asset.

## Google Cloud training and certification

...helps you make the most of Google Cloud technologies. Our classes include technical skills and best practices to help you get up to speed quickly and continue your learning journey. We offer fundamental to advanced level training, with on-demand, live, and virtual options to suit your busy schedule. Certifications help you validate and prove your skill and expertise in Google Cloud technologies.

**Manual Last Updated June 27, 2023**

**Lab Last Tested June 27, 2023**

Copyright 2024 Google LLC All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are

associated.