Defining Users with Cloud Identity Console

Overview

In this lab, you will create a Cloud Identity account, verify a domain for use with Cloud Identity, and create Cloud Identity user accounts with the Cloud Identity console. The Cloud Identity console allows you to easily manage users, devices, and apps from one console.

Setup

To complete this lab, you need:

- The latest version of Google Chrome or another modern browser
- A domain name you own and control or ability to register a new domain name
- A credit card to register for the free GCP trial

Objectives

In this lab, you learn how to:

- Register for a free GCP trial account (only if you do not already have a GCP account)
- Sign up for the free edition of Cloud Identity
- Create your Cloud Identity account and first admin user
- Verify your domain for use with Cloud Identity
- Create Cloud Identity user accounts
- Assign a cloud identity user access to a GCP project
- Utilize groups to simplify user management and lower operational overhead

Register a domain name

During this lab, you will need a domain name to link to the cloud identity. Later in the lab, you will need to verify that you own it by creating a specific CNAME record or uploading an html file.

If you have a domain name to use in this lab, and are able to create a CNAME record, you can skip to the next section: Logging into GCP. Otherwise, you will need to register a new domain name.

Note: Domain names can be registered from any of the domain registrars, and a complete list of registrars can be found at: https://www.icann.org/registrar-reports/accredited-list.html.

Google is also a domain registrar and if you would like to use Google to register your domain name, go to https://domains.google.

Step 1
If you do not have a domain name that you own to use for this lab, register a new domain name now. Refer to the Note immediately before this step for information on domain registrars.

Step 2
Once your domain name is registered, continue with this lab.

Sign up for the free edition of Cloud Identity

Duration: 15

Step 1

With a web browser, go to: https://gsuite.google.com/signup/gcpidentity/welcome

Step 2

Click **Next** on the **Cloud Identity** page.

Step 3

Provide a business name, number of employees, and click **Next**.

Step 4

Provide your location, phone number (if prompted), and click **Next**.

Step 5

Provide your email address, and click **Next**.

Step 6

Provide your domain name (this is the domain name you just registered, or one you previously owned), and click **Next**.

Step 7

Verify your domain name and click **Next** again.

Step 8

Provide your first and last name. This information will be used to make you the account admin since you are creating the account. You can assign this role to someone else later if needed.

Click **Next**.

Step 9

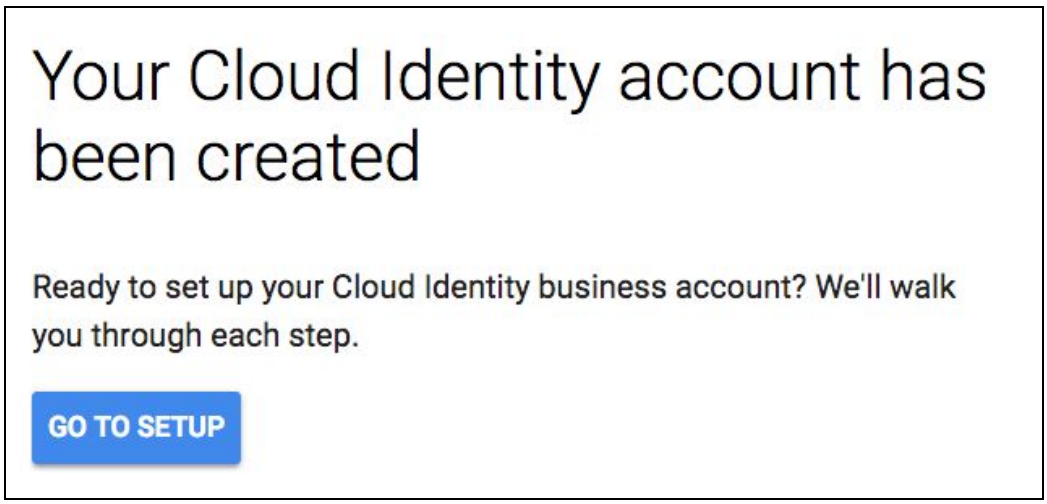
On the **How you'll sign in** page, provide a username (in the form of an email address at your domain name) and a password. This information will be used to create an account to serve as the admin for your Google Cloud Identity users. This password will be the password for your cloud identity admin user and does not need to be the same as your current email password. We will refer to this as the **admin** user.

Click **Next.**

Step 10

Complete the reCaptcha to prove you are not a robot, and click the **Agree and Create Account** button.

You should see a message that your cloud identity account has been created.



Step 11

Click the **GO TO SETUP** button.

Step 12

Log in with the email address and password that you specified for the admin account.

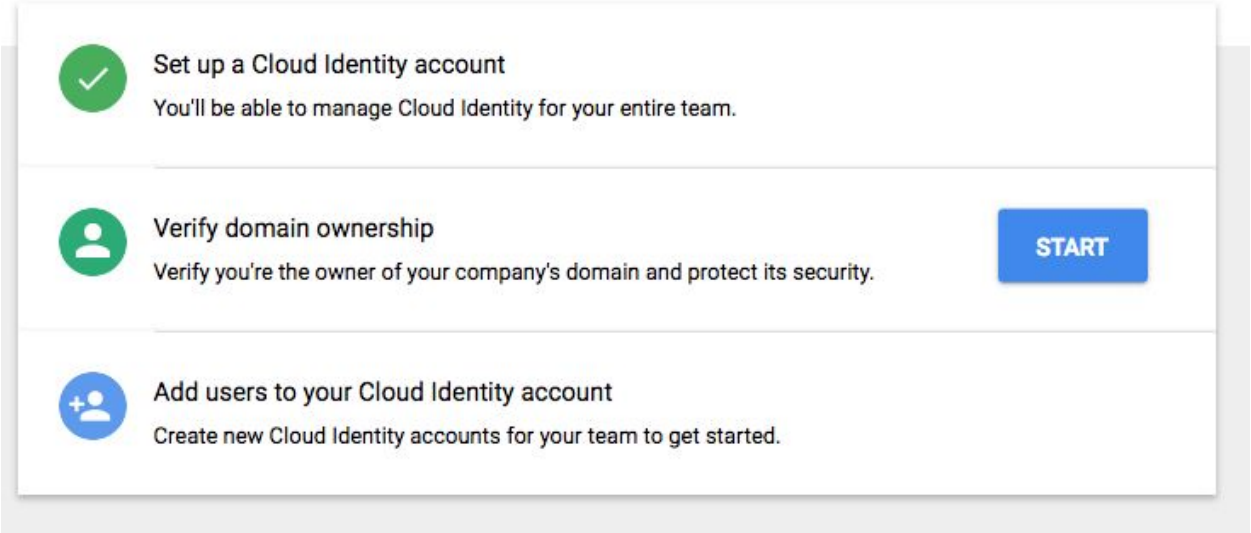
Step 13

If you are prompted to verify your account, provide a phone number and complete the verification.

Step 14

Click the **Accept** button to agree to the Google Terms of Service and the Google Privacy Policy.

You will see a screen indicating Cloud Identity has been setup.



The next step is to verify you own the domain name you are using for cloud identity.

Verify Domain Ownership

Duration: 10

Step 1

Click the **START** button next to **Verify domain ownership**.

Step 2

Follow the instructions provided on screen to verify you own the domain name. This usually involves creating a CNAME record for the domain.

The domain verification can sometimes take some time to complete depending on your DNS provider.

Step 3

Once the domain verification is complete, proceed to the next section.

Creating Your First Users and a GCP Account

Duration: 15

In this section, you will create your first Cloud Identity users and the GCP account that will be tied to the Cloud Identity.

Step 1

Go to https://admin.google.com/. If prompted to sign in again, sign in with the email address and password that you specified for the **admin** account.

Step 2

Click the **START** button next to **Add users to your Cloud Identity account**.

Step 3

Provide a **Firstname**, **Lastname**, and **Username** for your first user. The username is in the form of an email address in your domain. This email address does not have to be a live email account, it is basically just a username that ends in **`@your_domain_name`**.

Click the **ADD** button to add the user.

Step 4

Feel free to add additional users by providing a **Firstname**, **Lastname**, **Username**, and clicking the **ADD** button.

Step 5

When done adding users (you can add more later), check the **I have finished adding users for now** checkbox and click **NEXT**

The next step will be to notify the users that their account has been set up.

Step 6

On the **Notify your team** screen, provide email addresses for each user. You can just use your own email address for this lab (as a test). This email address will be used to send a message notifying the user their account has been setup.

Also, notice you add custom content to the end of the message. Feel free to add some content to the message if you like.

Step 7

Press the **SEND EMAILS** button.

You have just added your first users to your Cloud Identity domain. You will now continue setting up the GCP account for your domain.

Step 8

On the **Setup is complete** screen, click the **Continue to Cloud Console** button.

Step 9

If prompted, agree to the **Terms of Service** and click the **Accept** button.

Step 10

On the GCP console, click the **Sign Up for Free Trial** button.

Step 11

Provide your Country, opt in or out of the email updates, and read and agree to the terms of service.

Click **AGREE AND CONTINUE**.

Note: On the next step, you are asked to provide your credit card information. This information is used only to make sure you are not a robot. You won't be charged unless you manually upgrade to a paid account.

Step 12

Complete the **Customer info** screen and click **START MY FREE TRIAL**.

Step 13

Read the Welcome message and click **GOT IT.**

You have successfully set up Cloud Identity and a related GCP account. You can now set up GCP permissions for your users. You can also manage your organization's users with the

Cloud Identity admin console.

Managing Cloud Identity Users

Duration: 15

Before people in your organization can begin using your Cloud Identity service, you need to create user accounts for each person. An account provides users with a name and password for signing in to their cloud services. You already added at least 1 user when setting up the Cloud Identity service.

In this part of the lab, you will manually add another user. Feel free to use your own values for the user's information, but the following steps will assume the new user's name is William Thomas.

Step 1

Visit the Google Admin console at https://admin.google.com/. If prompted to sign in again, sign in with the email address and password that you specified for the admin account.

Step 2

Go to the **Users** section, then click the **ADD NEW USER** button 

Step 3

In the **Add new user** dialog box, create the new user's account, entering the following information:

- First name: `William`
- Last name: `Thomas`
- Primary email address: `william.thomas@yourdomain.com`
- You can assign a temporary, randomly generated password or manually set a password. For this exercise, set a manual password of `changeit!23` and enable **Ask for a password change at the next sign-in.**
- Click **ADD NEW USER**.

Step 4

On the **New user added** dialog, click the **More actions,** and select **EMAIL LOGIN INFORMATION.** This allows for the login information to be sent to the new user.

Step 5

Investigate the **Email login info** dialog. Press **CANCEL** when done as we do not want to send the email now.

Now that you have a user, you can investigate some of the user-specific settings.

Step 6

Locate the new user's name in the **Users** list, click their name, and click on **User Information**. Investigate the information that can be specified for a user.

Step 7

Near the top-left of the screen, click the user's name to return to the previous page.

Step 8

Click the **Security** section and notice this is where a user's password can be reset and other security settings changed.

Step 9

Feel free to investigate other properties of the user.

Step 10

You should now have at least 2 additional users in your Cloud Identity account (1 created when setting up the domain and the 1 you just created). Feel free to create additional users if you like.

Creating a new project and adding resources

Duration: 10

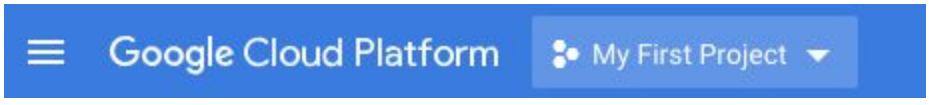
A new GCP project will be created, and a few resources added within the project. These resources will be used to verify user permissions.

Step 1

Visit the GCP Console at https://cloud.google.com/console . If prompted to sign in again, sign in with the email address and password that you specified for the admin account.

Step 2

Click the **Select project** dropdown (*in the header to the right of the words "Google Cloud Platform"*).



Then, click the **New project** button

.

Step 3

In the 'New Project' dialog:

- For **Project name**, enter `demoproject`.
- Make a note of the **Project ID** in the text below the project name box. *You can edit the project ID to make it easier to remember if you would like to. Also, you might want to paste the project id in a text editor so you can refer back to it.*
- The organization and location should already be set to your domain
- Click **Create**. It will take a minute or so for the project to be ready. You can monitor the progress by clicking on the **Notifications** button on the top right of the console.

Step 4

When the project is created, click the **Select project** dropdown again, click the **All** tab, and then select the `demoproject` project just created.

Step 5

In the GCP Console, click the **Navigation menu** icon i*n the upper-left corner* to open the Navigation menu. Then click **Compute Engine** to display the Compute Engine dashboard and ensure that there are no errors.

Important! By navigating to **Compute Engine**, the default network is setup and and some APIs are enabled.

Step 6

Wait for compute engine to finish initializing

Step 7

On the Google Cloud Platform menu, click **Activate Google Cloud Shell** ( )to open Cloud Shell. If prompted, click **START CLOUD SHELL**.

Step 8

Run the following commands to create a Compute Engine instance, create a storage bucket, create a sample file, and upload the file into the bucket.

```
gcloud compute instances create default-us-vm --zone=us-central1-a
gsutil mb gs://$DEVSHELL_PROJECT_ID
echo "this is a sample file" > sample.txt
gsutil cp sample.txt gs://$DEVSHELL_PROJECT_ID
```

Step 9

Wait for the commands to complete. You should now see an instance running in the Compute Engine dashboard.

Step 10
Select the checkbox next to the running instance. Do not modify the instance at this time, but notice the **STOP**, **RESET**, and **DELETE** buttons are all enabled. The user you are currently logged in as is the project owner.

Step 11

Go to the Storage dashboard (**Navigation menu > Storage > Browser**). You will see the storage bucket that was created.

Step 12

Click on the storage bucket and you will see the **sample.txt** file that was uploaded in the last section.

Step 13

Do not modify the bucket or file at this time, but if you select the checkbox next to the file the Delete button is enabled. This user has full admin permissions.

Assigning GCP Access to Cloud Identity Users

Duration: 15

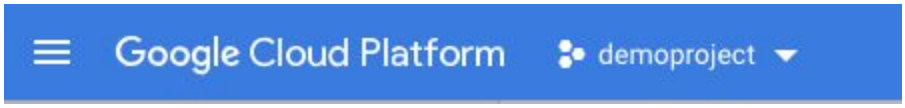
The cloud identity users you have added can now be given permission to a GCP project.

Step 1

Visit the GCP Console at https://cloud.google.com/console . If prompted to sign in again, sign in with the email address and password that you specified for the admin account.

Step 2

In the GCP Console, verify the demoproject is the active project. If not, click on the **Select project** dropdown and select the demoproject project.



Step 3

Click the **Navigation menu** icon i*n the upper-left corner* to open the Navigation menu. Then click **IAM and admin**.

Step 4

Click the **+ ADD**  button.

Step 5

In the new member field, start typing the name of one of the users you added to your Cloud Identity. For example, if you added William Thomas, type “wi”. You will see a popup displaying that user’s name and email.

Step 6

Select the user.

Step 7

For the **Role**, select **Project > Viewer**.

Step 8

Click **SAVE**.

Before the next step, verify you know the password to the user you just made **Project Viewer**. If you do not, you can go to the admin console and reset the password.

Step 9

Sign out of the GCP Console.

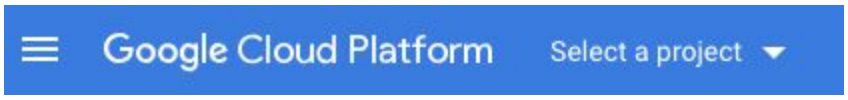
Step 10

Log back into https://cloud.google.com/console with the user you added as a project viewer. Since this is the first time this user has logged in, you will need to perform a few steps:

- **Accept** the account
- Change the password
- Agree to the email and terms of service

Step 11

Click the **Select project** dropdown:



And click the **Select from** dropdown and select your organization:

Step 12

Click the **All** tab, and select the **demoproject**. If you do not see the **demoproject**, type `demo` in the **Search projects and folders** field. The project should then be displayed.

Step 13

Go to the Compute engine dashboard (**Navigation menu** > **Compute Engine > VM Instances)**. You should see the instance started earlier from the admin account.

Step 14

Select the checkbox next to the running instance. Notice you do not have permissions to modify the instance (Start, Stop, Delete, etc.). This is because this user just has Project viewer rights.

Step 15

Go to the Storage dashboard (**Navigation menu > Storage > Browser**). You should be able to view the storage bucket created by the admin account, but are unable to modify it.

Utilize groups for less lower operational overhead

Duration: 15

You have successfully used Cloud Identity to provide GCP access to a user in your custom domain. However, giving individual users access to GCP can become difficult to manage. It is easier and less of an operational overhead to assign and revoke IAM permissions utilizing groups instead.

It is best practice to define the required groups of users for your organization and assign GCP permissions to each group. Then just manage which users belong to the groups. If you remove a user from a group the user no longer has access, add them back into the group and access is restored. No need to update or manage the IAM policies for individual users.

Step 1

Sign out of the GCP Console.

Step 2

Go to the Cloud Identity Admin console: https://admin.google.com/. Sign in with the email address and password that you specified for the **admin** account.

Step 3

Go to the **Group** section, then click **Create a group**.

Step 4

On the **Create new group** dialog, use the following values:

- **Name of the group**: `Storage Admin`
- **Group email address**: `storageadmin [@your_domain_name]`
- **Description**: `Organizational group for storage admins`
- **Access Level**: `Team`

Click the **CREATE** button

You will see the new Storage Admin group created and currently it has 0 users in the group.

Step 5

Click on **Manage users in Storage Admin**.

Step 6

In the **Add new members** textarea, start typing the name of one of the users you created earlier. When their email pops up, click on it to add them to the group.

Step 7

Feel free to add another user to the group if you like.

Step 8

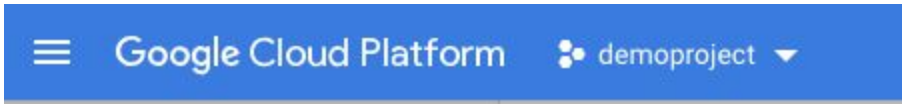
Verify the **Add as** is set to **Member**, and click the **Add** button. The added users will appear at the bottom of the screen.

Step 9

Open a new browser tab and go to the GCP console (https://cloud.google.com/console). Verify you are signed in with your admin account.

Step 9

Verify the **`demoproject`** is the selected in the project dropdown:



Step 10

Go to the IAM dashboard (**Navigation menu** > **IAM and admin > IAM)**.

Step 11

Locate the line for the user you gave project viewer role to earlier (they will have a role of **Viewer**). Click the **Delete** (trash can) button for that user. Select to remove the user from all roles and click **REMOVE**. This does not delete the user, just their role in this project.

Step 12

Click the **+ ADD** button.

Step 13

In the new member field, type: **`storageadmin@[your_domain_name]`**

Step 14

For the **Role**, select **Storage > Storage Object Admin**. We are only giving this group permissions to storage, it will not have permissions to even view Compute Engine or any other resource.

Step 15

Click **SAVE**.

Step 16

Sign out of the GCP console.

Step 17

Sign back in to the GCP console (https://cloud.google.com/console) as the user you used to test earlier. Verify you are viewing the demoproject.

Step 18

Go to the Compute engine dashboard (**Navigation menu** > **Compute Engine > VM Instances)**.
You should not have permissions to view instances.

Step 19
Go to the Storage dashboard (**Navigation menu > Storage > Browser**).
You should be able to view the storage bucket created by the admin

Managing storage admins is now quite easy. For anyone who needs to be a storage admin, just be added to the **storageadmin** group in the Google Admin console. There is no need to modify or edit the IAM policies in GCP.

Finish up

Duration: 1

In this lab, you had the chance to do the following:

1. Register for a free GCP trial account (only if you do not already have a GCP account)
2. Sign up for the free edition of Cloud Identity
3. Create your Cloud Identity account and first admin user
4. Verify your domain for use with Cloud Identity
5. Create Cloud Identity user accounts
6. Assign a cloud identity user access to a GCP project
7. Utilize groups to simplify user management and lower operational overhead

Also, If your organization has a large, pre-established directory, Google Cloud Directory Sync (GCDS) is a secure tool that we provide that can help you sync your users into your Cloud Identity domain. GCDS allows you to synchronize your user data in your Cloud Identity domain with your Microsoft® Active Directory® or LDAP server. GCDS will ensure that your Google users, groups, and shared contacts are synchronized to match the information in your LDAP server.