Federating GCP with Azure Active Directory: Configuring provisioning and single sign-on

This tutorial shows you how to set up user account synchronization and single sign-on between your Microsoft Azure AD (https://azure.microsoft.com/en-us/services/active-directory/) tenant and Google Cloud Platform (GCP) by using Cloud Identity (https://cloud.google.com/identity/) and SAML Federation (https://www.oasis-open.org/standards#samlv2.0).

The tutorial assumes that you already use Microsoft Office 365 or Azure AD in your organization and want to use Azure AD for allowing users to authenticate with GCP. Azure AD itself might be connected to an on-premises Active Directory and might use AD FS federation, pass-through authentication, or password hash synchronization.

Objectives

- Set up Azure AD to automatically provision user accounts and, optionally, groups in GCP.
- Configure single sign-on to allow users to sign in to GCP using an Azure AD account or an account that has been synchronized from Active Directory to Azure AD.

Costs

If you are using the free edition of Cloud Identity (https://support.google.com/cloudidentity/answer/7431902?hl=en), running this tutorial won't use any billable components of GCP.

Check the Azure AD pricing page (https://azure.microsoft.com/en-us/pricing/details/active-directory/) for any fees that might apply to using Azure AD.

Before you begin

- Make sure you understand the differences between connecting GCP to Azure AD versus directly connecting GCP to Active Directory (https://cloud.google.com/solutions/federating-gcp-with-active-directory-introduction).
- Decide how you want to map identities, groups, and domains. Specifically, answer the following questions:
    - Do you plan to use email addresses or User Principal Names (UPNs) as common identifiers for user accounts?
    - Do you plan to synchronize groups? If so, do you plan to map groups by email address or by name?
    - Do you plan to provision all users to GCP or only a select subset of users?
- Before connecting your production Azure AD tenant to GCP, consider using an Azure AD test tenant for setting up and testing account synchronization.
- Sign up for Cloud Identity (https://gsuite.google.com/signup/gcpidentity/welcome?&_ga=2.104797888.-157260409.1512652371) if you don't have an account already.
- If you're using the free edition of Cloud Identity (https://support.google.com/cloudidentity/answer/7431902) and intend to synchronize more than 50 users, request an increase (https://support.google.com/cloudidentity/answer/7295541?hl=en) of the total number of free Cloud Identity users through your support contact.
- If you suspect that any of the domains you plan to use for Cloud Identity could have been used by employees to register consumer accounts, consider migrating these accounts first. For more details, see migrating consumer accounts (https://cloud.google.com/solutions/migrating-consumer-accounts-to-cloud-identity-or-g-suite).

Note: This article refers to the G Suite gallery app from the Microsoft Azure marketplace (https://azuremarketplace.microsoft.com/en-us/marketplace/apps/aad.googleapps). This app is a Microsoft product and is neither maintained nor supported by Google.

Configuring Cloud Identity

Create a Cloud Identity user account for synchronization

To perform synchronization, Azure AD must interact with Cloud Identity, and to do so requires a Cloud Identity account. When you signed up for Cloud Identity, you created one Super Admin account. Although you could use this account for Azure AD, it's preferable to create a separate account that is used exclusively by Azure AD.

1. Open the Admin Console (https://admin.google.com) and log in using the Super Admin account created when you signed up for Cloud Identity.
2. In the menu, navigate to **Directory** > **Users** and click **+** to create a user.
3. Provide an appropriate name and email address such as:
   a. **First Name**: `Azure AD`
   b. **Last Name**: `Synchronizer`
   c. **Primary email**: `azuread-synchronizer`
   d. Keep the primary domain for the email address, even if it doesn't correspond to the forest you are synchronizing from.
4. Set **Automatically generate a new password** to **Disabled** and enter a password.
5. Set **Ask for a password change at the next sign-in** to **Disabled**.
6. Click **Add new user**.
7. Click **Done**.

To enable Azure AD to create, list, and delete user accounts and groups, you must give the account additional privileges. Also, it's a good idea to exempt the account from single sign-on—otherwise, you might not be able to re-authorize Azure AD when experiencing single sign-on problems. Do both by making the account a Super Admin:

1. Locate the newly created user in the list and open it.
2. Under **Admin roles and privileges**, click **Assign roles**.
3. Enable the Super Admin role.
4. Click **Save**.

Enable API access

Azure AD uses the Cloud Identity API to synchronize accounts. If you haven't enabled this API already, you must enable it:

1. In the menu of the Admin Console (https://admin.google.com), navigate to **Security** > **Settings**.
2. Click **API reference** to view API-related settings.

3. Make sure the **Enable API access** box is checked.
4. At the bottom, click **Save**.

Register domains

In Cloud Identity, users and groups are identified by email address. The domains used by these email addresses must be registered and verified first.

Prepare a list of DNS domains that you need to register to map users:

- If you plan to map users by UPN, include all domains used by UPNs. If in doubt, include all custom domains of your Azure AD tenant.
- If you plan to map users by email address, include all domains used in email addresses. The list of domains might be different from the list of custom domains of your Azure AD tenant.

If you plan to synchronize groups, amend the list of DNS domains:

- If you plan to map groups by email address, include all domains used in group email addresses. If in doubt, include all custom domains of your Azure AD tenant.
- If you plan to map groups by name, include a dedicated subdomain like `groups.[PRIMARY-DOMAIN]`, where `[PRIMARY-DOMAIN]` is the primary domain name of your Cloud Identity account.

Now that you've identified the list of DNS domains, you can register any missing domains in Cloud Identity. For each domain on the list not yet registered, perform the following steps:

1. In the Admin Console, navigate to **Account** > **Domains**.
2. Click **Add/remove domains**.
3. Click **Add a domain or a domain alias**.
4. In the dialog, select **Add another domain**.
5. In the text box below, enter the domain name.
6. Click **Continue and verify domain ownership**.

   If the domain is a subdomain of another domain that has been verified before, then the domain is immediately usable. Otherwise, you are asked to verify the domain.
7. Click **Select your domain registrar or provider** to select the registrar or provider of the respective DNS domain.

8. You now see a set of instructions specific to the registrar or provider selected. Follow these instructions to verify ownership of the domain.

Configuring Azure AD provisioning

Create an enterprise application

You are now ready to configure Azure AD to connect to Cloud Identity. Azure AD doesn't support Cloud Identity natively. However, Cloud Identity uses the same APIs as G Suite, so you can use the G Suite gallery app (https://azuremarketplace.microsoft.com/en-us/marketplace/apps/aad.googleapps) instead.

The G Suite gallery app can be configured for provisioning users and groups to Cloud Identity and for handling single sign-on. If you use one instance of the app for both purposes, however, you risk running into a limitation of Azure AD (https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-provisioning-config-problem-storage-limit)
. To avoid this risk, you use two instances of the G Suite gallery app.

First, create an enterprise application to handle user provisioning:

1. Open the Azure portal (https://portal.azure.com/) and sign in using an account with *global administrator* privileges, navigate to **Azure Active Directory** > **Enterprise applications**.
2. Click **New application**.
3. Search for **G Suite**, and then click the **G Suite** item in the result list.
4. Enter `Google Cloud Platform (Provisioning)`.
5. Click **Add**.
6. Adding the application may take a few seconds, you should then be redirected to a page titled **Google Cloud Platform (Provisioning) - Overview**.
7. In the menu on the left, click **Manage** > **Properties**:
    a. Set **Enabled for users to sign-in** to **No**.
    b. Set **User assignment required** to **No**.
    c. Set **Visible to users** to **No**.
    d. Click **Save**.
8. In the menu on the left, click **Manage** > **Provisioning**:

a. Change **Provisioning Mode** to **Automatic**.

b. Click **Admin Credentials** > **Authorize**.

c. Sign in using the `azuread-synchronizer@[CLOUDIDENTITY-DOMAIN]` user you created earlier, where `[CLOUDIDENTITY-DOMAIN]` is the domain of your Cloud Identity account.

d. Because this is the first time you've signed on using this user, you are asked to accept the Google Terms of Service and privacy policy.

e. If you agree to the terms, click **Accept**.

f. Confirm access to the Cloud Identity API by clicking **Allow**.

g. Click **Test Connection** to verify that Azure AD can successfully authenticate with Cloud Identity.

h. Click **Save**.

Configure user provisioning

The right way to configure user provisioning depends on whether you intend to map users by email address or by UPN.

MAP BY UPN MAP BY EMAIL ADDR...

- If you map users by UPN, keep the default settings.

Configure group provisioning

The right way to configure group provisioning also depends on whether you intend to map groups by email address or by UPN.

NO GROUP MAPPING MAP BY EMAIL ADDR... MAP BY NAME

1. Under **Mappings**, click **Synchronize Azure Active Directory Groups to GoogleApps**.
2. Set **Enabled** to **No**.
3. Click **Save**.
4. Confirm that saving changes will result in users and groups being resynchronized by clicking **Yes**.
5. Click **X** to close the **Attribute Mapping** dialog.

Configure user assignment

If you know that only a certain subset of users need access to GCP (https://cloud.google.com/solutions/federating-gcp-with-azure-active-directory#onboarding), you can optionally restrict the set of users to be provisioned by assigning the enterprise app (https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal) to specific users or groups of users.

If you want all users to be provisioned, you can skip the following steps.

1. In the menu on the left, click **Manage** > **Users and groups**.
2. Click **Add user**.
3. Select **Users and groups/None Selected**.
4. Select the users or groups you want to provision. If you select a group, all members of this group are automatically provisioned.
5. Click **Select**.
6. Click **Assign**.

Enable automatic provisioning

The next step is to configure Azure AD to automatically provision user accounts to Cloud Identity:

1. In the menu on the left, click **Manage** > **Provisioning**.
2. Under **Settings**, set **Provisioning Status** to **On**.
3. Set **Scope** to one of the following:
    a. **Sync only assigned users and groups** if you have configured user assignment.
    b. **Sync all users and groups** otherwise.

   If this box to set the scope isn't displayed, click **Save** and refresh the page.
4. Click **Save**.

Azure AD starts an initial synchronization. Depending on the number of user accounts and groups in the directory, this synchronization can take several minutes or hours. You can refresh the browser page to see the status of the synchronization at the bottom of the page or select **Audit Logs** in the menu to see more details.

Troubleshooting

If the synchronization doesn't start within five minutes, you can force it to start by doing the following:

1. Set **Provisioning Status** to **Off**.
2. Click **Save**.
3. Set **Provisioning Status** to **On**.
4. Click **Save**.
5. Check **Clear current state and restart synchronization**.
6. Click **Save**.
7. Confirm restarting the synchronization by clicking **Yes**.

If synchronization still doesn't start, click **Test Connection** to verify that your credentials have been saved successfully.

Configuring Azure AD for single sign-on

Although all relevant Azure AD accounts are now automatically being provisioned to Cloud Identity, you cannot use these accounts to sign in yet. To allow users to sign in, you still need to configure single sign-on.

Create an enterprise application

Create a second enterprise application to handle single sign-on:

1. In the Azure portal (https://portal.azure.com/), navigate to **Azure Active Directory** > **Enterprise applications**.
2. Click **New application**.
3. Search for **G Suite**, and then click **G Suite** in the result list.
4. Enter `Google Cloud Platform`.
5. Click **Add**.

   Adding the application may take a few seconds. You are then redirected to a page titled **Google Cloud Platform - Overview**.
6. In the menu on the left, click **Manage** > **Properties**.
7. Set **Enabled for users to sign-in** to **Yes**.

8. Set **User assignment required** to **Yes** unless you want to allow all users to use single sign-on.
9. Download the GCP Console logo (https://cloud.google.com/solutions/images/cloud-console-logo.png) to your local disk, and then choose this file as **Logo**.
10. Click **Save**.

Configure user assignment

If you already know that only a certain subset of users need access to GCP (https://cloud.google.com/solutions/federating-gcp-with-azure-active-directory#onboarding), you can optionally restrict the set of users to be allowed to sign in by assigning the enterprise app (https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal) to specific users or groups of users.

If you set **User assignment required** to **No** before, then you can skip the following steps.

1. In the menu on the left, click **Manage** > **Users and groups**.
2. Click **Add user**.
3. Select **Users and groups/None Selected**.
4. Select the users or groups you want to allow single sign-on for.
5. Click **Select**.
6. Click **Assign**.

Configure SAML settings

To enable Cloud Identity to use Azure AD for authentication, you must adjust some settings:

1. In the menu on the left, click **Manage** > **Single sign-on**.
2. On the ballot screen, click the **SAML** card.
3. On the **Basic SAML Configuration** card, click the ✏ icon.
4. In the **Basic SAML Configuration** dialog, enter the following settings:
    a. **Sign on URL**: `https://www.google.com/a/[CLOUDIDENTITY-DOMAIN]/ServiceLogin?continue=https://console.cloud.google.com/`, replacing `[CLOUDIDENTITY-DOMAIN]` with the domain name used for Cloud Identity.

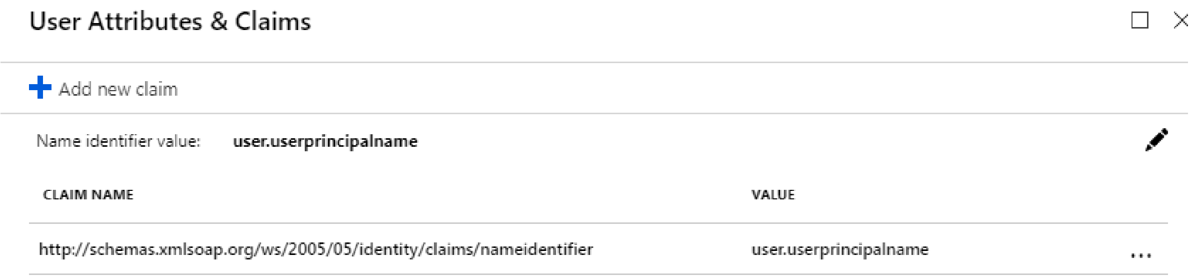
   b. **Identifier (Entity ID)**: `google.com`

5. Click **Save**, and then dismiss the dialog by clicking **X**.
6. On the **SAML Signing Certificate** card, find the entry labeled **Certificate (Raw)** and click **Download** to download the certificate to your local computer.
7. On the **Set up Google Cloud Platform** card, look for **Login URL** and **Logout URL**. You need these URLs shortly.

The remaining steps differ depending on whether you map users by email address or by UPN.

MAP BY UPN   MAP BY EMAIL ADDR...

1. On the **User Attributes & Claims** card, click the ✎ icon.
2. Delete all claims listed under **Additional claims**. You can delete records by clicking the **...** button and selecting **Delete**.
3. The list of attributes and claims should now look like this:



User Attributes & Claims

+ Add new claim

Name identifier value: user.userprincipalname

CLAIM NAME	VALUE
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname

4. Dismiss the dialog by clicking **X**.

Configuring Cloud Identity for single sign-on

Now that you've prepared Azure AD for single sign-on, you can enable single sign-on in Cloud Identity:

1. Open the Admin Console (https://admin.google.com) and log in using the Super Admin account created when you signed up for Cloud Identity.
2. In the menu, navigate to **Security** > **Settings**.
3. Click **Set up single sign-on (SSO)**.
4. Under **Verification certificate**, click **Choose File**, and then pick the token signing certificate you downloaded previously.
5. Click **Upload**.

6. Click **Save**.
7. Ensure that **Setup SSO with third party identity provider** is enabled.
8. Enter the following settings:
   a. **Sign-in page URL**: Enter the **Login URL** from the **Set up Google Cloud Platform** card in the Azure Portal.
   b. **Sign-out page URL**: Enter the **Logout URL** from the **Set up Google Cloud Platform** card in the Azure Portal.
   c. **Change password URL**: `https://account.activedirectory.windowsazure.com/changepassword.aspx`
9. Click **Save**.
10. On the next page, confirm that you intend to enable single sign-on and click **I understand and agree**.
11. Sign out of the Admin Console by clicking the avatar on the top right. Then click **Sign out**.

Note: The token signing certificate has limited validity. When the certificate expires, single sign-in stops working and you must replace the certificate in both Azure AD and Cloud Identity. Consider configuring Azure AD to send you notification emails (https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-certificates-for-federated-single-sign-on#add-email-notification-addresses-for-certificate-expiration) ahead of certificate expiration to avoid certificate expiration from impacting users.

Testing single sign-on

Now that you've completed the single sign-on configuration in both Azure AD and Cloud Identity, you can access GCP in two ways:

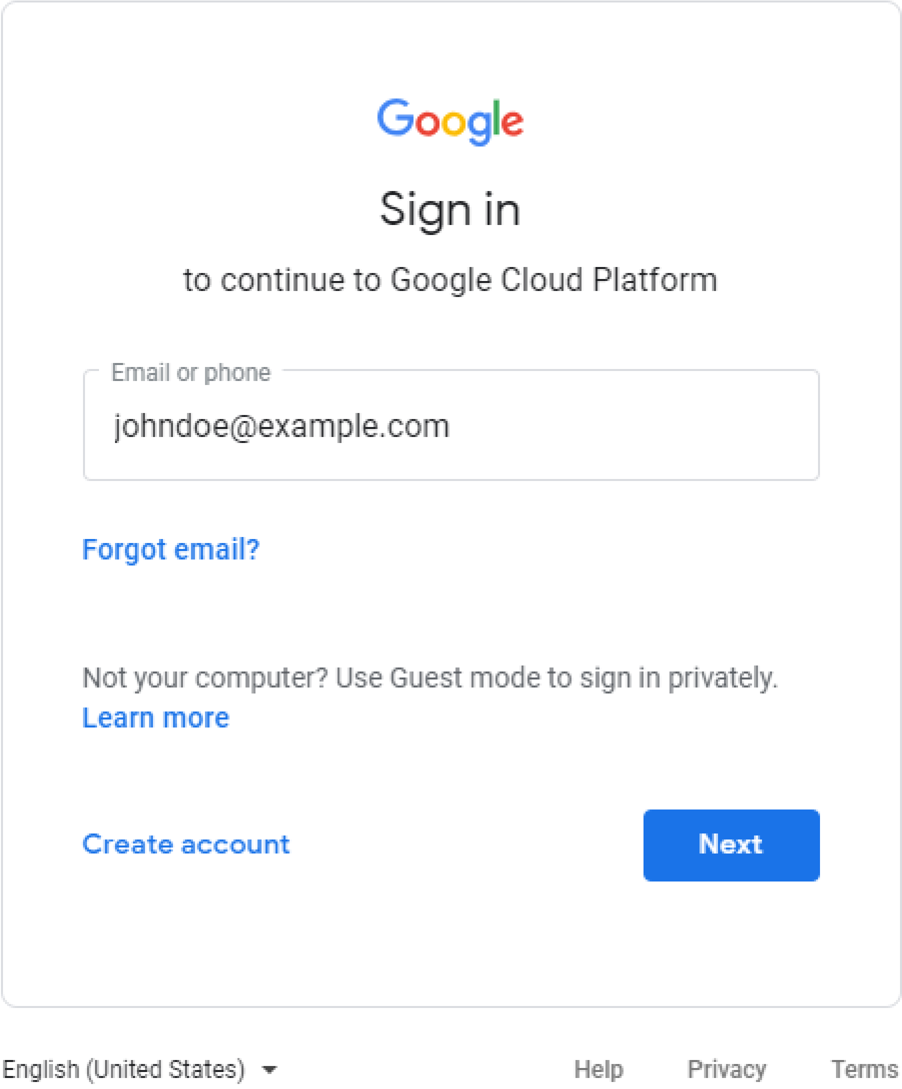
- Through the list of apps in your Microsoft Office portal (https://www.office.com/).
- Directly by opening https://console.cloud.google.com/ (https://console.cloud.google.com/).

To check that the second option works as intended, run the following test:

1. Pick an Azure AD user account that has been synchronized to Cloud Identity and that doesn't have Super Admin privileges assigned. User accounts with Super Admin

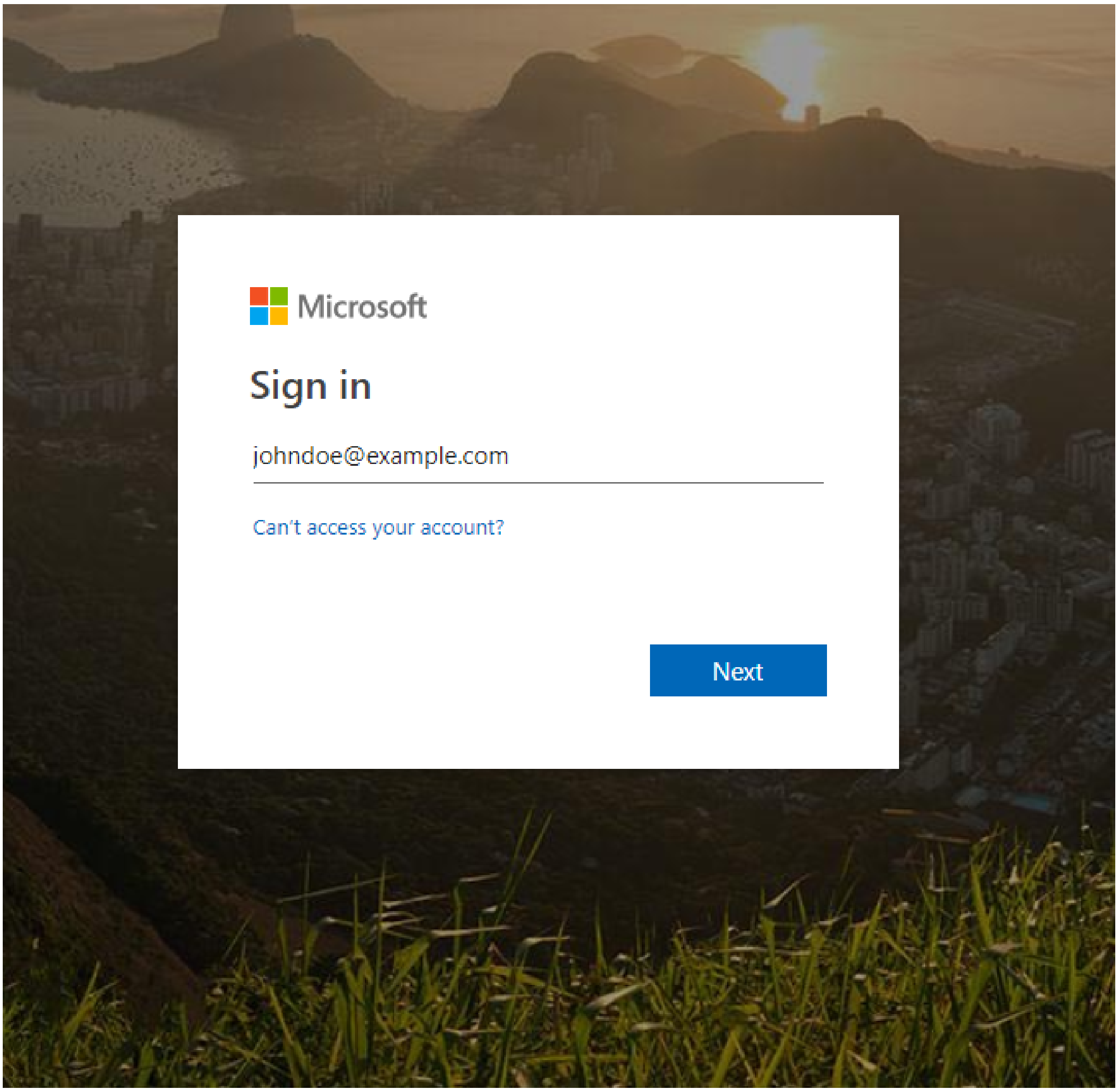
privileges always have to sign in using Google credentials and are therefore not suitable for testing single sign-on.

2. Open a new browser window and navigate to https://console.cloud.google.com/ (https://console.cloud.google.com/).
3. In the Google sign-in page that appears, enter the email address of the user account and click **Next**. If you use domain substitution, this address must be the email address with the substitution applied.



Email or phone: johndoe@example.com

4. You are redirected to Azure AD and will see another sign-in prompt. Enter the email address of the user account (without domain substitution) and click **Next**.



Sign in

johndoe@example.com

5. After entering your password, you are prompted whether to stay signed in or not. For now, choose **No**.

   After successful authentication, Azure AD should redirect you back to Google Identity Platform. Because this is the first time you've signed in using this user, you are asked to accept the Google Terms of Service and privacy policy.

6. If you agree to the terms, click **Accept**.

   You are redirected to the GCP Console, which asks you to confirm preferences and accept the Google Cloud Terms of Service.

7. If you agree to the terms, choose **Yes** and click **Agree and continue**.
8. Click the avatar icon on the top left of the page, and then click **Sign out**.

   You are redirected to an Azure AD page confirming that you have been successfully signed out.

Keep in mind that user accounts with Super Admin privileges are exempted from single sign-on, so you can still use the Admin Console to verify or change settings.

Cleaning up

To avoid incurring charges to your Google Cloud Platform account for the resources used in this tutorial:

To disable single sign-on in Cloud Identity, perform the following steps:

- Open the Admin Console (https://admin.google.com) and log in using the Super Admin account created when signing up for Cloud Identity.
- In the menu, navigate to **Security** > **Settings**.
- Click **Set up single sign-on (SSO)**.
- Ensure that **Setup SSO with third party identity provider** is disabled.

You can remove single sign-on and synchronization settings in Azure AD as follows:

- In the Azure portal (https://portal.azure.com/), navigate to **Azure AD** > **Enterprise applications**.
- From the list of applications, choose **Google Cloud Platform**.
- In the menu on the left, click **Manage** > **Single sign-on**.
- Click **Delete**.
- Confirm the deletion by clicking **Yes**.

What's next

- Learn more about Cloud IAM (https://cloud.google.com/iam/docs/overview).
- Read about best practices for setting up an enterprise organization in GCP (https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations).
- Acquaint yourself with our best practices for managing Super Admin accounts. (https://cloud.google.com/resource-manager/docs/super-admin-best-practices)
- Try out other Google Cloud Platform features for yourself. Have a look at our tutorials (https://cloud.google.com/docs/tutorials).

Last updated October 16, 2019.