samegoal

# OpenID Connect Identity Provider

Your district can configure SameGoal to authenticate users against an OpenID Connect Identity Provider (IdP). Many districts use OpenID Connect (OIDC) to manage user authentication across a variety of district applications.

SameGoal supports specification compliant OIDC Identity Providers.

- General OpenID Connect Configuration
- Google OpenID Connect Configuration (Google SSO)
  - Create a new Google API project
  - Set up the consent screen
  - Create an OAuth 2.0 Client ID
- Microsoft Azure OpenID Connect Configuration (Azure SSO)
  - Register a new Microsoft Azure application
  - Copy the OAuth 2.0 Client ID
  - Create a new OAuth 2.0 Client Secret ID
- Enter configuration information into SameGoal

## General OpenID Connect Configuration

**Steps** *To configure SSO with any OpenID Connect identity provider:*

1. Configure your external OIDC Identity Provider.
2. Log into SameGoal using an administrative account.
3. Visit **Settings (left menu)** > **District Information** > **OpenID Connect / OIDC**.
4. Enter the **Client ID**, **Client Secret** and **Issuer URL** provided by your IdP.

Tip SameGoal is not responsible for any fees associated with your use of third party identity providers.

Tip If your LEA requires some user accounts in SameGoal which do not exist in your OpenID Connect IdP, they can be configured to use a password.

## Google OpenID Connect Configuration (Google SSO)

These instructions can be used to help districts setup Google SSO using OpenID Connect. Google is a common Identity Provider; as a service to clients, SameGoal provides Google-specific instructions.

Tip SameGoal is not responsible for any fees associated with your use of Google as an OpenID Connect Identity Provider.

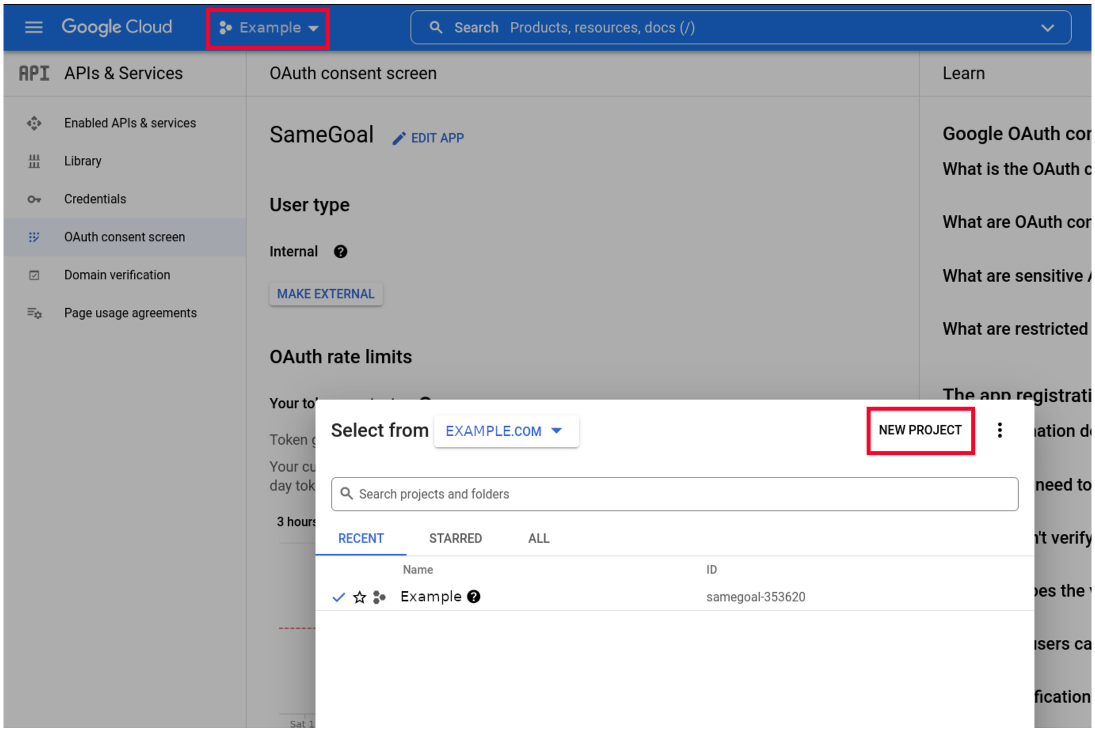
Tip Google frequently changes their user interfaces; directions may not fully match the current Google interface.

### Create a new Google API project

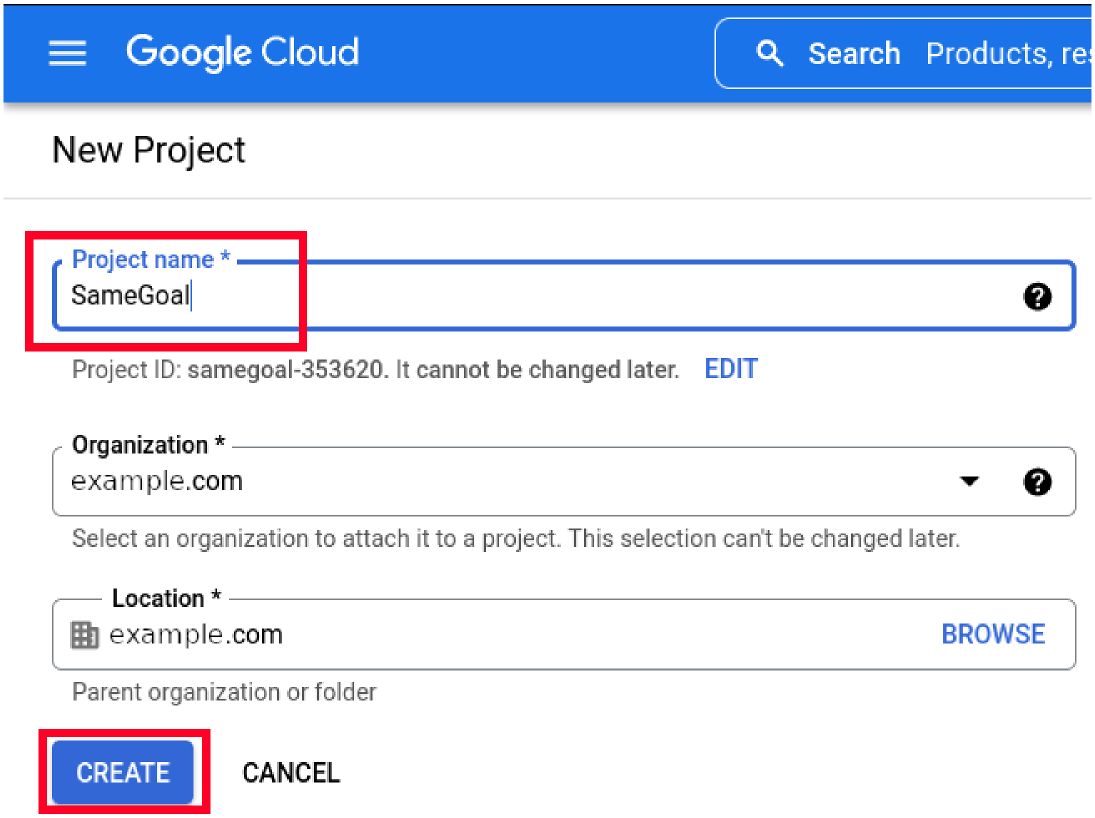
**Steps** *To create a new Google API project:*

Tip If you already have a Google Cloud Platform project that you wish to use, you may skip to the next section.

- Log into your Google account.
- Navigate to the Google API Console.
- Select your organization from the menu in the top-left corner.
- In the popup window choose "NEW PROJECT".



- In the dialog box that appears, enter "SameGoal" as the project name and leave the organization and location unchanged.
- Click the "CREATE" button.



Project name * SameGoal

Project ID: samegoal-353620. It cannot be changed later.

Organization * example.com

Select an organization to attach it to a project. This selection can't be changed later.

Location * example.com

Parent organization or folder

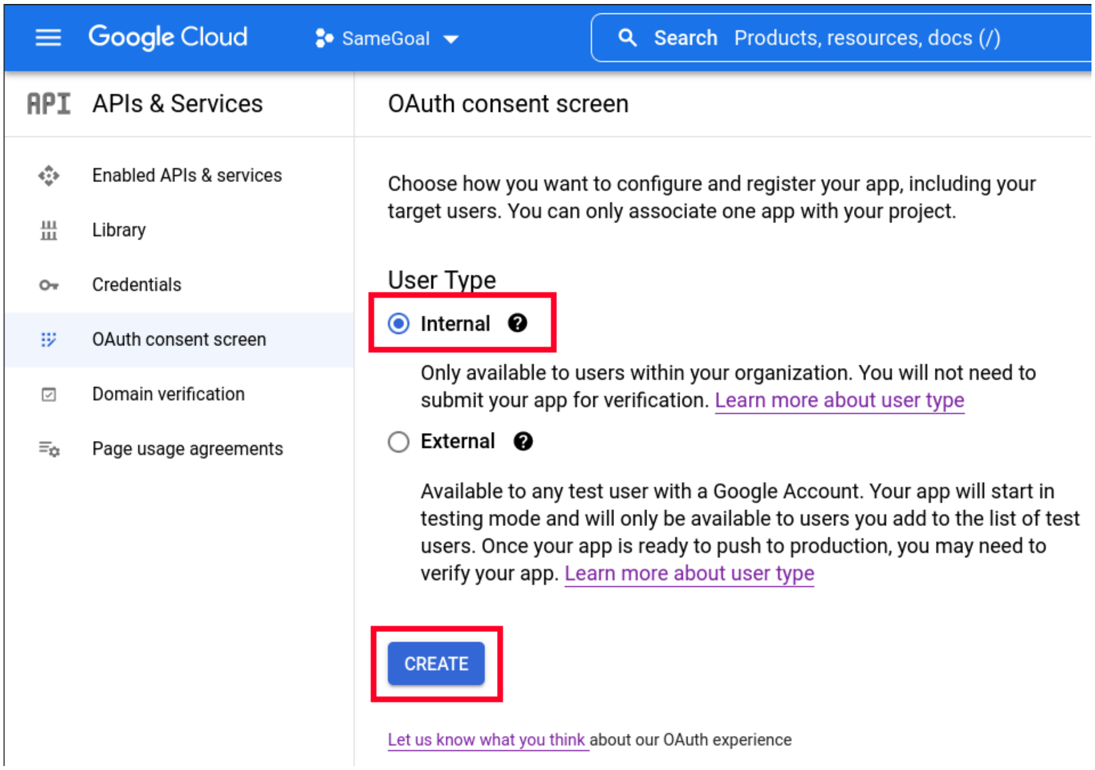
- When the activity completes, continue below.

## Set up the consent screen

**Steps** *To setup the consent screen:*

Tip If you have already configured your Google Credentials Consent Screen, you may skip to the next section.

- Navigate to the Google OAuth Consent Screen.
- Select "Internal" for the application type and click "CREATE".



OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

● Internal

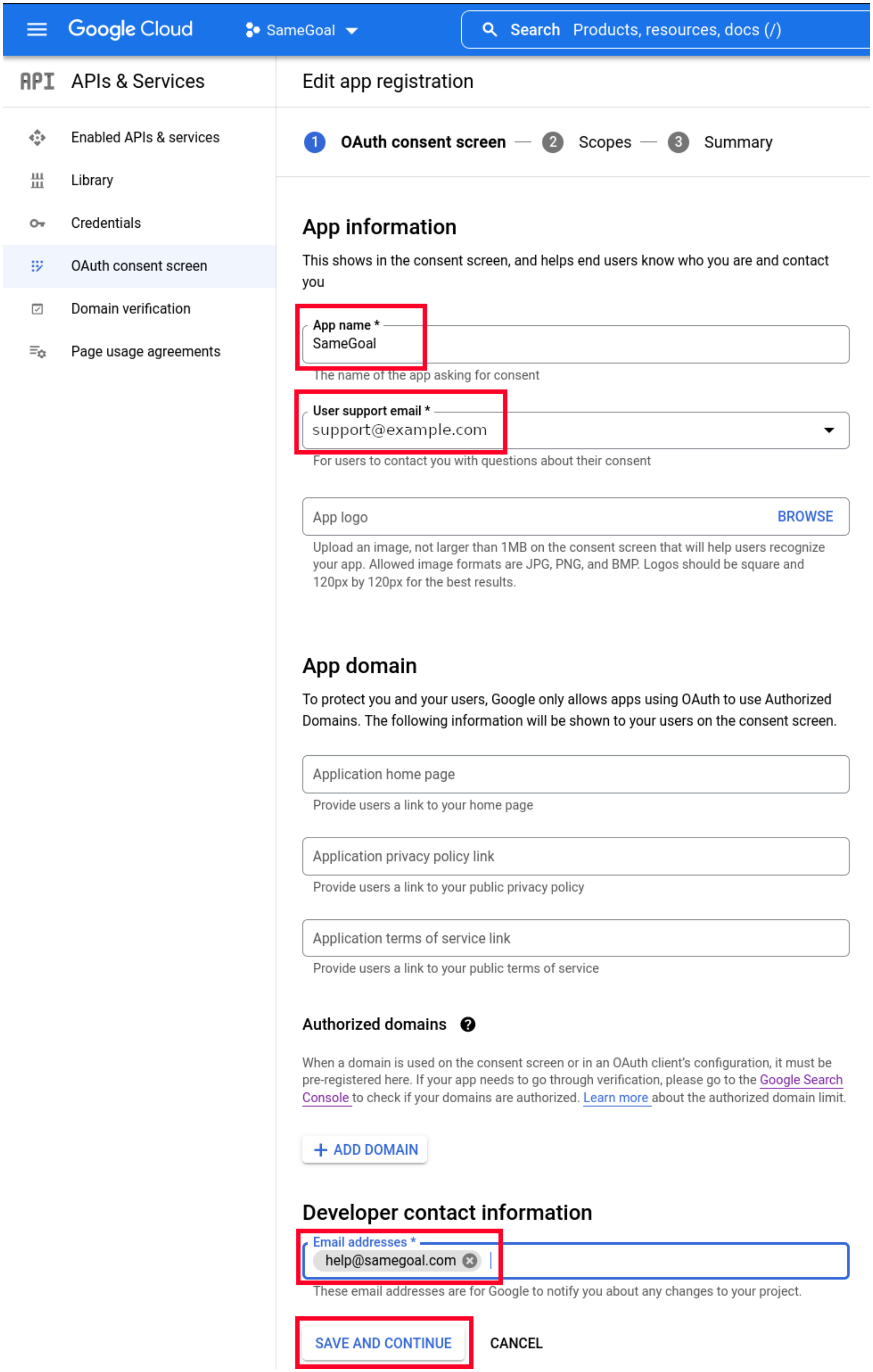
Only available to users within your organization. You will not need to submit your app for verification. Learn more about user type

○ External

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. Learn more about user type

Let us know what you think about our OAuth experience

- In the "App name" field, enter "SameGoal".
- Select a "User support email" (can be an email address or a Google Group email address that you manage).
- In the "Developer contact information" section, enter "help@samegoal.com" into the "Email addresses" field.
- Leave all other fields unchanged and click "SAVE AND CONTINUE".



Edit app registration

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *: SameGoal

The name of the app asking for consent

User support email *: support@example.com

For users to contact you with questions about their consent

App logo

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application terms of service link

Provide users a link to your public terms of service

Authorized domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the Google Search Console to check if your domains are authorized. Learn more about the authorized domain limit.

Developer contact information

Email addresses *: help@samegoal.com

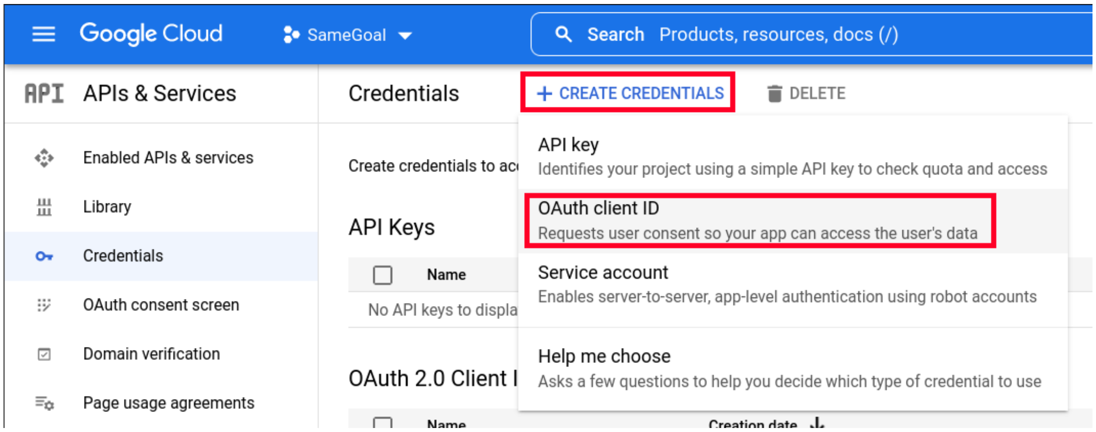
These email addresses are for Google to notify you about any changes to your project.

- On the scopes screen, leave the scopes unchanged and click "SAVE AND CONTINUE".
- On the summary screen, click "BACK TO DASHBOARD".

## Create an OAuth 2.0 Client ID

**Steps** *To create an OAuth 2.0 Client ID:*

- On the Google Credentials Screen, select "CREATE CREDENTIALS" then "OAuth client ID".



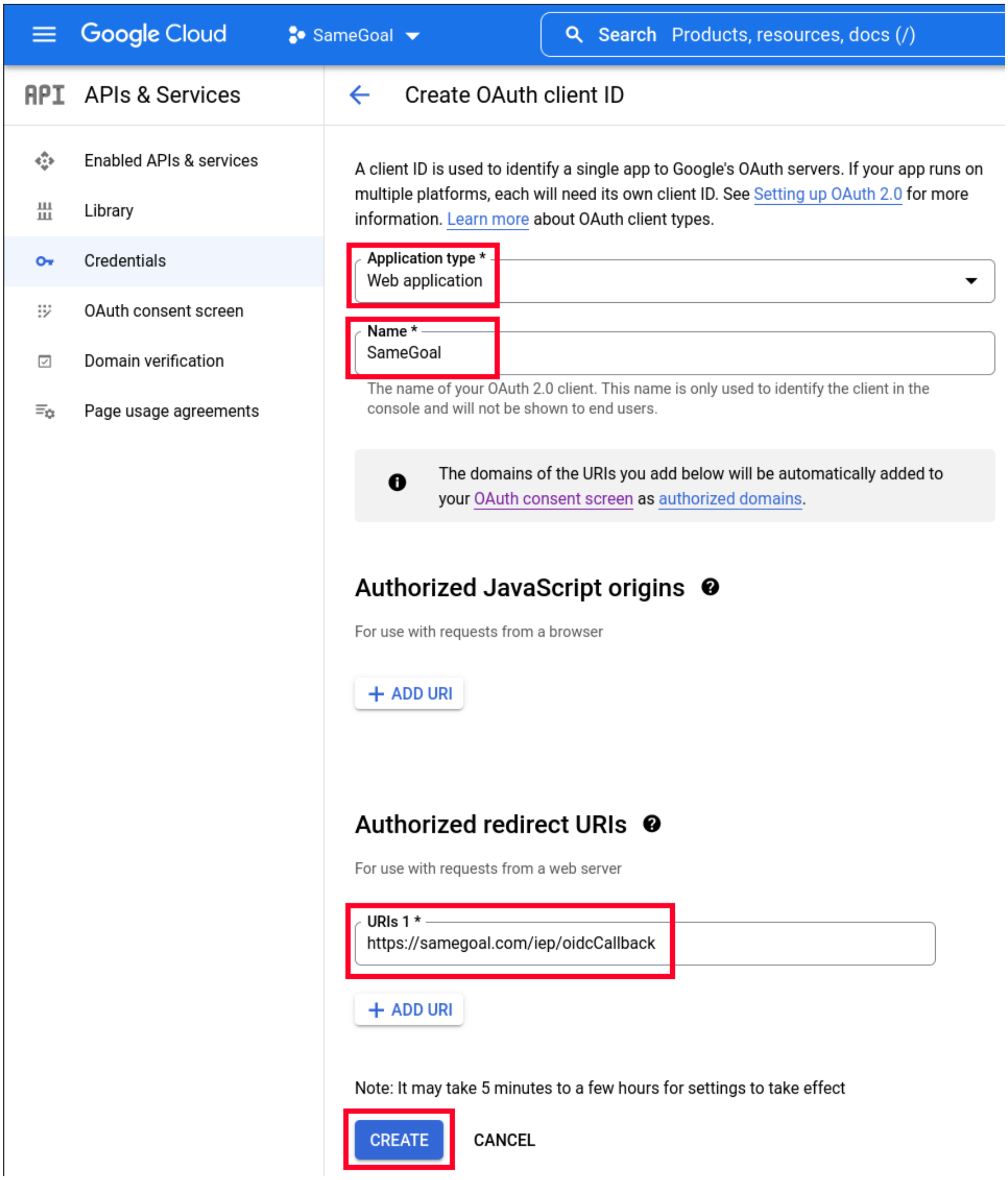
API key
Identifies your project using a simple API key to check quota and access

OAuth client ID
Requests user consent so your app can access the user's data

Service account
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use

- For "Application Type", select "Web application".
- In the "Name" field, enter "SameGoal".
- In the "Authorized redirect URIs" section, add **https://samegoal.com/iep/oidcCallback**
- Click the "Create" button.



Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See Setting up OAuth 2.0 for more information. Learn more about OAuth client types.

Application type *: Web application

Name *: SameGoal

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

The domains of the URIs you add below will be automatically added to your OAuth consent screen as authorized domains.

Authorized JavaScript origins

For use with requests from a browser

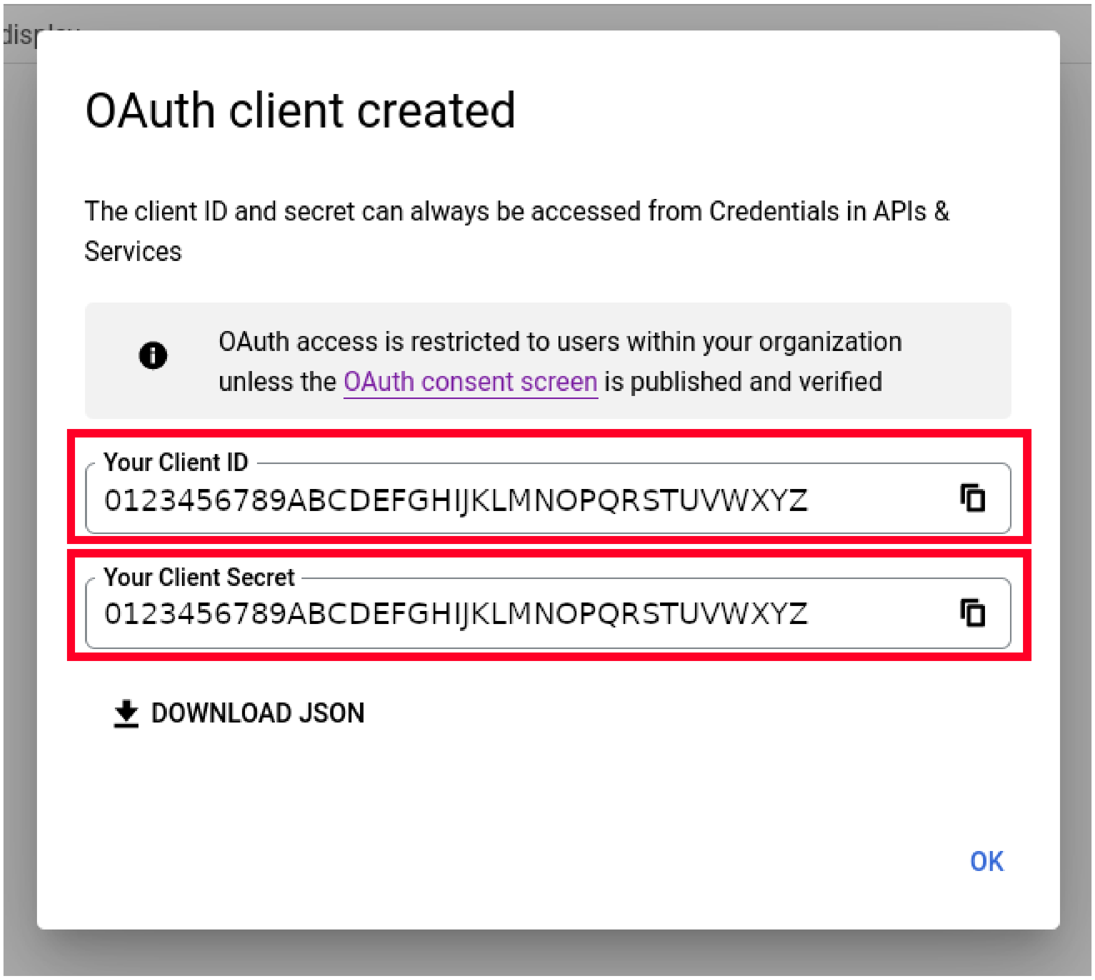
Authorized redirect URIs

For use with requests from a web server

URIs 1 *: https://samegoal.com/iep/oidcCallback

Note: It may take 5 minutes to a few hours for settings to take effect

- In the dialog which displays, copy "Your Client ID" and "Your Client Secret".
- Your **Issuer URL** will be **https://accounts.google.com**.
- Enter your configuration information into SameGoal.



## OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth access is restricted to users within your organization unless the OAuth consent screen is published and verified

Your Client ID: 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

Your Client Secret: 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

## Microsoft Azure OpenID Connect Configuration (Azure SSO)

These instructions can be used to help districts setup Microsoft Azure SSO using OpenID Connect. Microsoft Azure is a common Identity Provider; as a service to clients, SameGoal provides Microsoft Azure-specific instructions.

💡 Tip SameGoal is not responsible for any fees associated with your use of Microsoft Azure as an OpenID Connect Identity Provider.

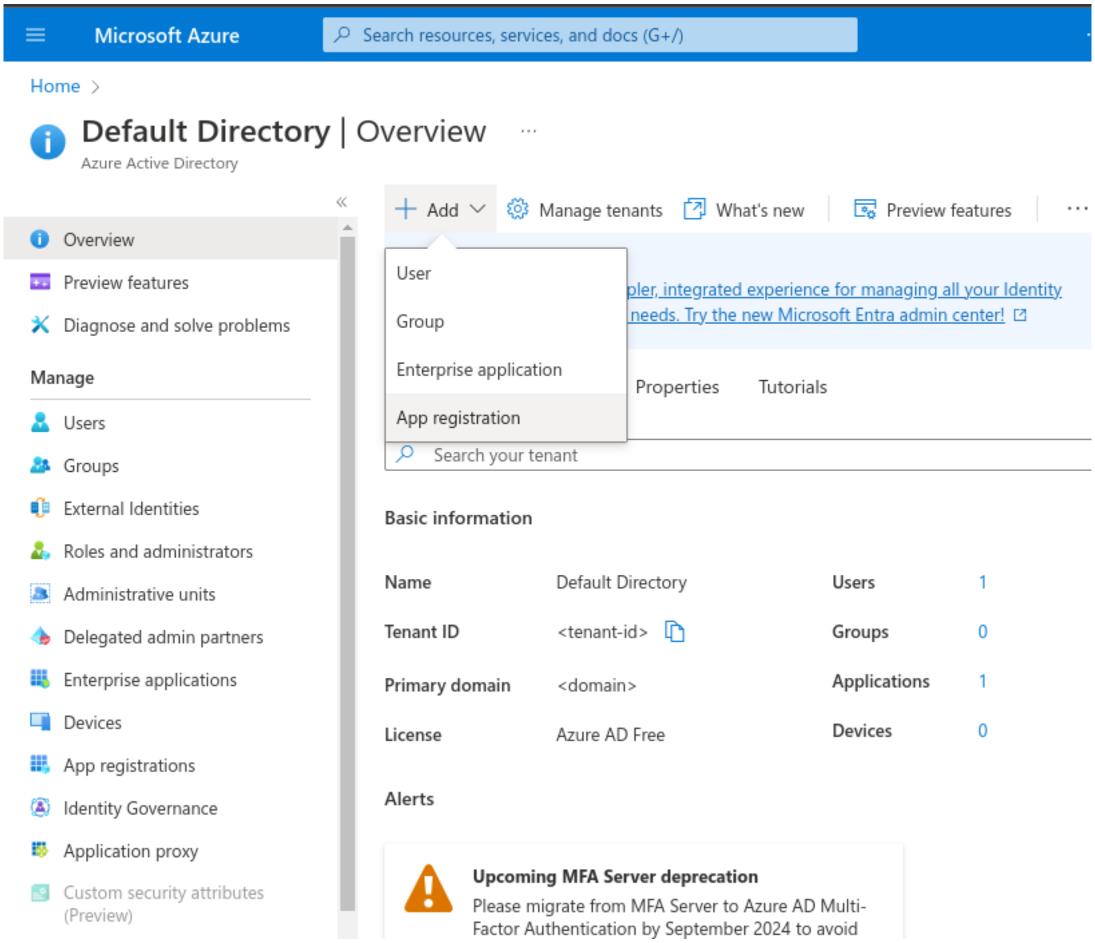
💡 Tip Microsoft Azure frequently changes their user interfaces; directions may not fully match the current Microsoft Azure interface.

### Register a new Microsoft Azure application

**Steps** *To register a new Microsoft Azure application:*

💡 Tip If you already have a Microsoft Azure Active Directory application that you wish to use, you may skip to the next section.

- Log into your Microsoft Azure account.
- Navigate to the Azure Active Directory console
- In the "+ Add" dropdown choose "App registration".



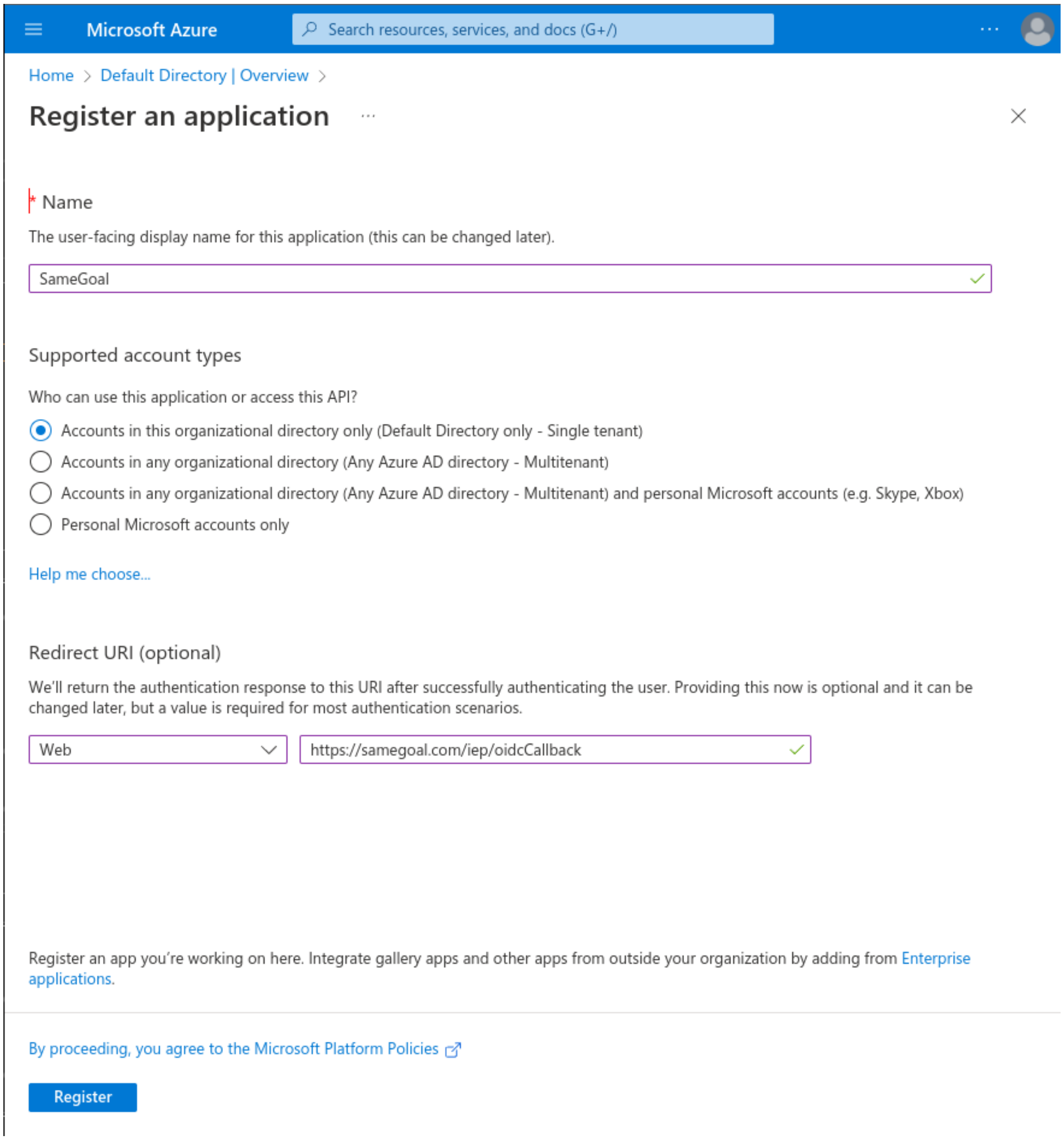
Basic information

| | | | |
|---|---|---|---|
| Name | Default Directory | Users | 1 |
| Tenant ID | <tenant-id> | Groups | 0 |
| Primary domain | <domain> | Applications | 1 |
| License | Azure AD Free | Devices | 0 |

Alerts

**Upcoming MFA Server deprecation**
Please migrate from MFA Server to Azure AD Multi-Factor Authentication by September 2024 to avoid

- In the "Register and application" page that appears, enter "SameGoal" as the user-facing display name.
- In the "Supported account types" select "Accounts in this organizational directory only".
- In the "Redirect URI" section, select "Web" and enter **https://samegoal.com/iep/oidcCallback**.
- Click the "Register" button.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory | Overview >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SameGoal

Supported account types

Who can use this application or access this API?

- ● Accounts in this organizational directory only (Default Directory only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://samegoal.com/iep/oidcCallback

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

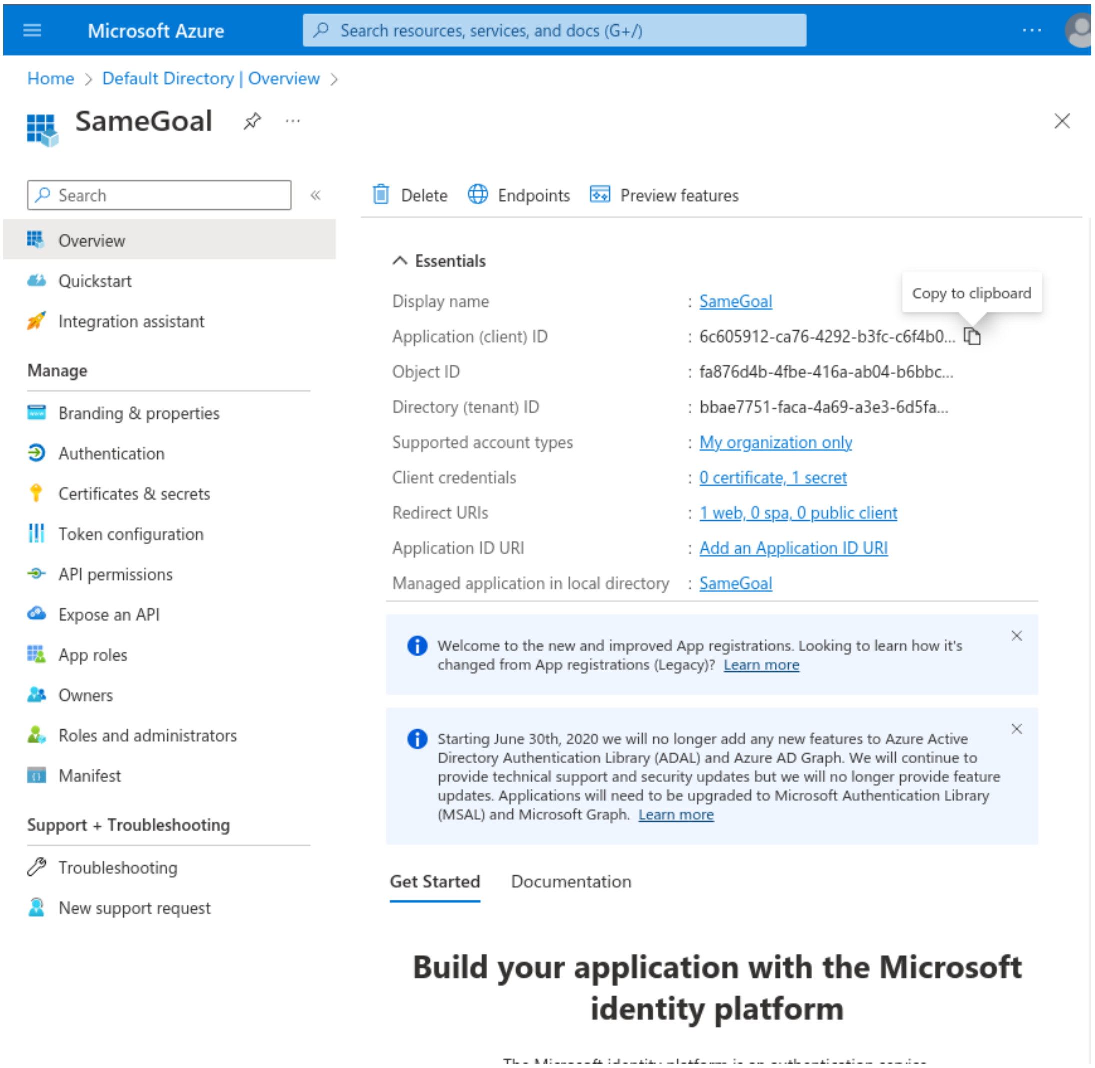
By proceeding, you agree to the Microsoft Platform Policies

- When the activity completes, continue below.

## Copy the OAuth 2.0 Client ID

**Steps** *To copy the OAuth 2.0 Client ID:*

- On the Microsoft Azure Default Directory - SameGoal Overview Screen, copy the "Application (client) ID".
- This Client ID will later be pasted into SameGoal.



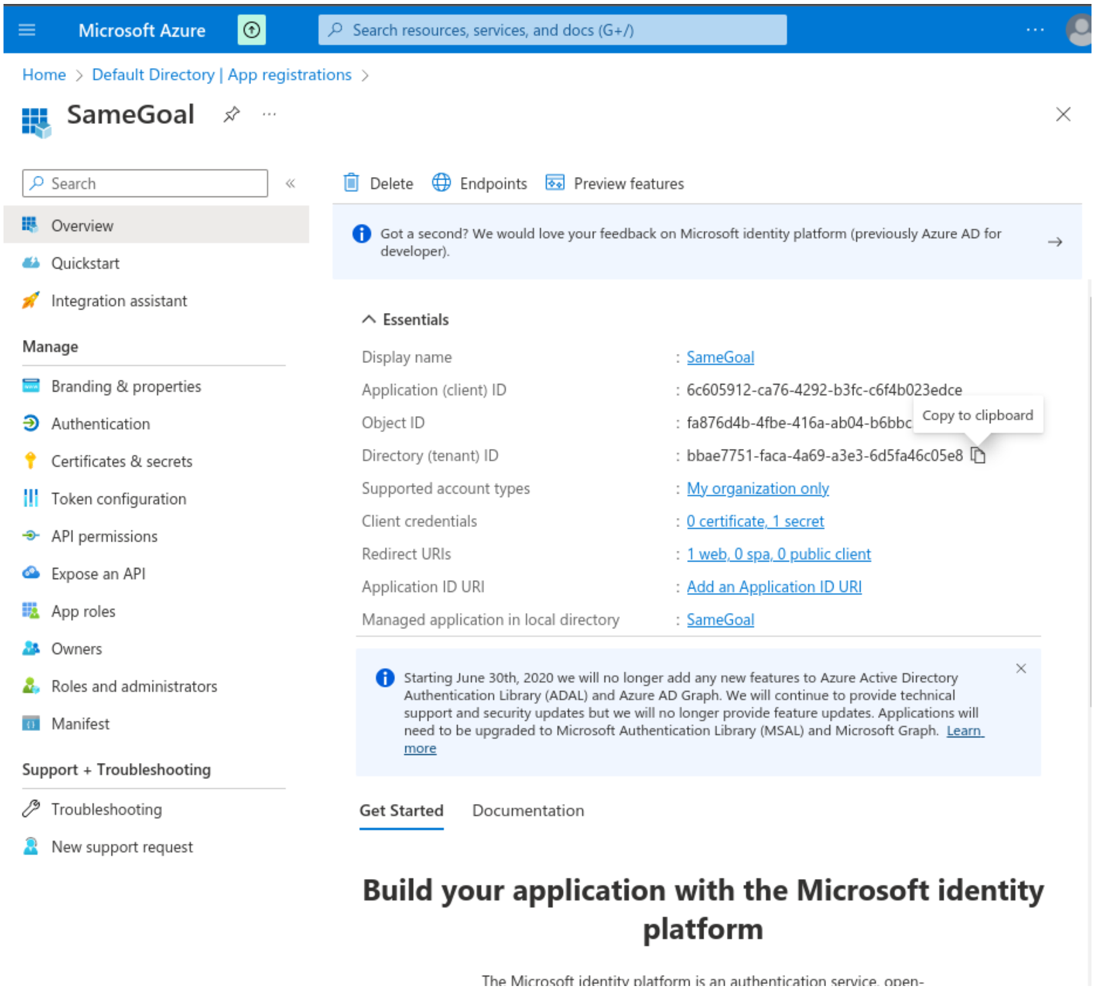
| | |
|---|---|
| Display name | : SameGoal |
| Application (client) ID | : 6c605912-ca76-4292-b3fc-c6f4b0... |
| Object ID | : fa876d4b-4fbe-416a-ab04-b6bbc... |
| Directory (tenant) ID | : bbae7751-faca-4a69-a3e3-6d5fa... |
| Supported account types | : My organization only |
| Client credentials | : 0 certificate, 1 secret |
| Redirect URIs | : 1 web, 0 spa, 0 public client |
| Application ID URI | : Add an Application ID URI |
| Managed application in local directory | : SameGoal |

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

- On the Microsoft Azure Default Directory - SameGoal Overview Screen, copy the "Directory (tenant) ID".
- This Tenant ID will later be pasted into SameGoal as the "Issuer URL" formatted as **https://login.microsoftonline.com/{directory tenant id}/v2.0**.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).

Display name : SameGoal
Application (client) ID : 6c605912-ca76-4292-b3fc-c6f4b023edce
Object ID : fa876d4b-4fbe-416a-ab04-b6bbc
Directory (tenant) ID : bbae7751-faca-4a69-a3e3-6d5fa46c05e8
Supported account types : My organization only
Client credentials : 0 certificate, 1 secret
Redirect URIs : 1 web, 0 spa, 0 public client
Application ID URI : Add an Application ID URI
Managed application in local directory : SameGoal

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

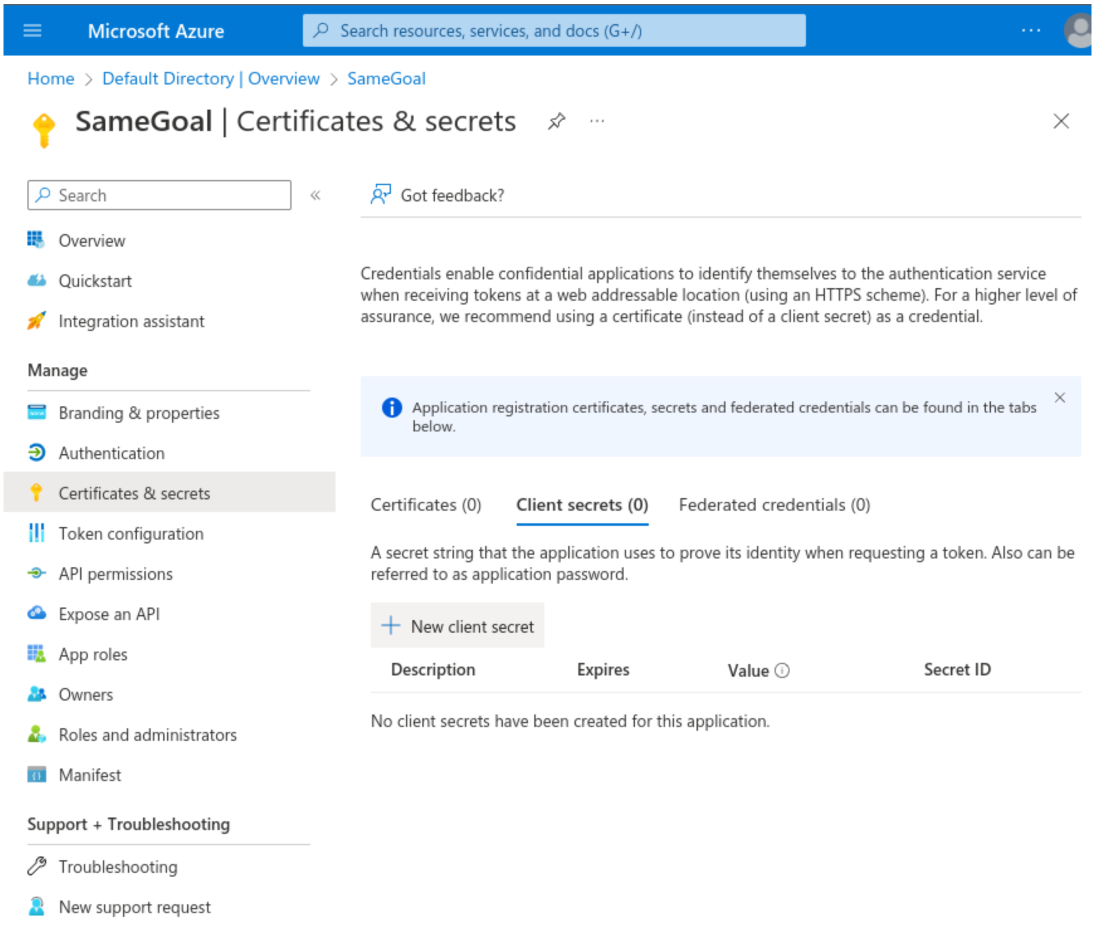
Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-

## Create a new OAuth 2.0 Client Secret ID

**Steps** *To create a new OAuth Client Secret ID:*

- On the Microsoft Azure Default Directory - SameGoal Overview Screen, select the "Certificates & secrets" option on the left side.
- On the "SameGoal | Certificates & secrets" page that opens, click the "+ New client secret" button.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

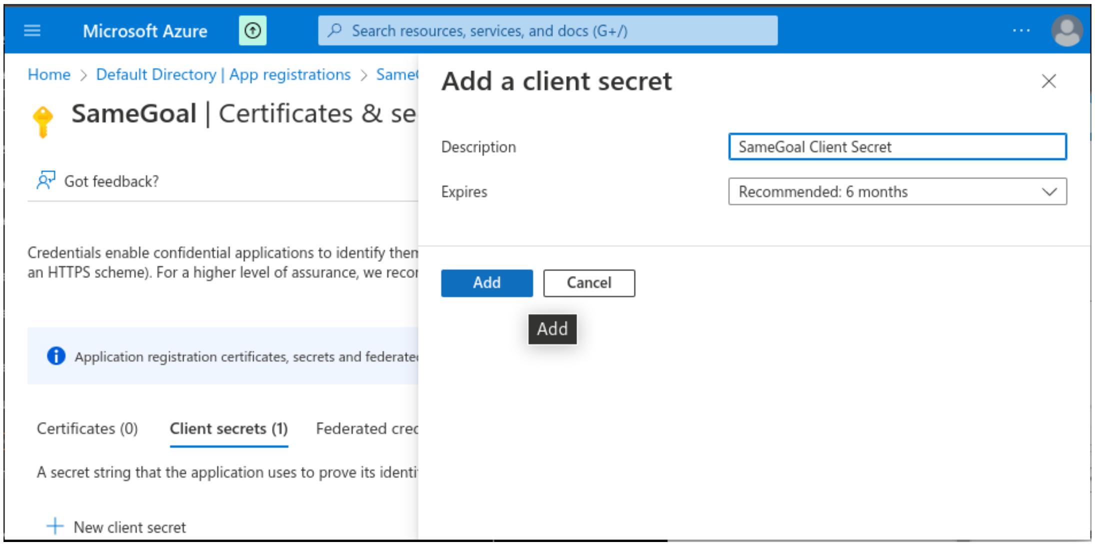
| Description | Expires | Value | Secret ID |
|---|---|---|---|

No client secrets have been created for this application.

- In the "Add a client secret" dialog that appears, enter "SameGoal Client Secret" as the description and set an expiration.

Tip The shorter the expiration, the more often this setup must occur.

- Click the "Add" button.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory | App registrations > Same(
SameGoal | Certificates & se
Got feedback?
Certificates (0)
Client secrets (1)
Federated cred
New client secret
Add
Cancel
Add

Credentials enable confidential applications to identify then an HTTPS scheme). For a higher level of assurance, we recor

Application registration certificates, secrets and federatec

A secret string that the application uses to prove its identi

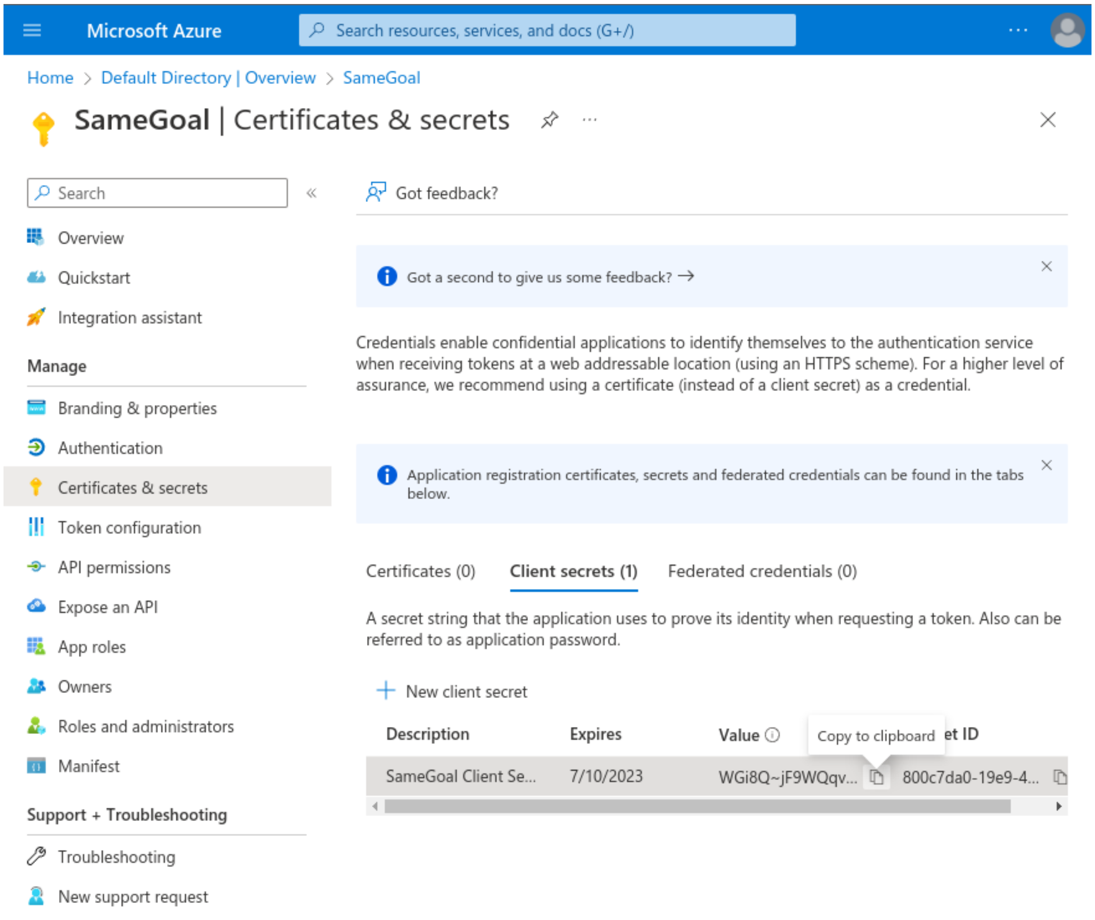
Add a client secret

Description: SameGoal Client Secret

Expires: Recommended: 6 months

- Copy the "SameGoal Client Secret" value.

- This secret value will later be pasted into SameGoal as the "Client Secret".



Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

| Description | Expires | Value ⓘ | Copy to clipboard et ID |
|---|---|---|---|
| SameGoal Client Se... | 7/10/2023 | WGi8Q~jF9WQqv... | 800c7da0-19e9-4... |

- Enter configuration information into SameGoal.

## Enter configuration information into SameGoal

**Steps** *To enter configuration information into SameGoal:*

- Log into SameGoal using an administrative account.
- Visit **Settings (left menu)** > **District Information** > **OpenID Connect / OIDC**.
- Enter the **Client ID**, **Client Secret** and **Issuer URL** copied above.
- Test logging in.

💡 Tip It may take 5 minutes to a few hours for settings to take effect.

💡 Tip If you are using Google SSO, the **Issuer URL** should be **https://accounts.google.com**

💡 Tip If your LEA requires some user accounts in SameGoal which do not exist in your OpenID Connect IdP, they can be configured to use a password.

### OIDC Subject Identifier

The OIDC Subject Identifier is a unique and never reassigned identifier within the Identity Provider for the end user. This case-sensitive string must not exceed 255 ASCII characters. If empty, this field is automatically populated on first use when a user signs into SameGoal via the Identity Provider (IdP).