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
- Portal Applications & Dashboard Tiles (SP-Initiated SSO)
- 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 Entra OpenID Connect Configuration (Entra SSO)
  - Register a new Microsoft Entra application
  - Copy the OAuth 2.0 Client ID
  - Create a new OAuth 2.0 Client Secret ID
- Enter configuration information into SameGoal
- OIDC Subject Identifier

General OpenID Connect Configuration

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

1. Configure your external OIDC Identity Provider with the following settings:
   - **Authorized Redirect / Callback URI: https://samegoal.com/iep/oidcCallback**
   - **Scopes:** Your OIDC Identity Provider must request and authorize both **openid** and **email** scopes.
   - **ID Token Claims:** The ID token claims returned by your provider must include the user's primary email address mapped to the standard, lowercase **email**

claim attribute.

2. Log in to 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 strictly enforces Service Provider (SP)-initiated authentication with CSRF state validation. Direct IdP-initiated launches that bypass SameGoal are rejected.

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.

Portal Applications & Dashboard Tiles (SP-Initiated SSO)

If your district uses an identity portal or app launcher (such as RapidIdentity, ClassLink, Clever, or Microsoft My Apps), dashboard tiles must be configured as **Bookmarks / Web Links** rather than IdP-initiated OIDC applications.

Because SameGoal supports mixed authentication (SSO and password logins), initiating a 1-click SSO login from a portal requires passing the user's username in the URL.

Steps *To configure a portal bookmark tile for 1-click login:*

- Set the tile URL to: **https://samegoal.com/iep/a/{district_domain}?username={user_email}** *(Replace **{district_domain}** with your SameGoal instance domain, and **{user_email}** with your identity portal's macro/variable for the user's email address, e.g., **{mail}** or **%email%**).*
- When clicked, SameGoal receives the preflight request, generates the necessary secure session state, and redirects the user through your IdP automatically.

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.

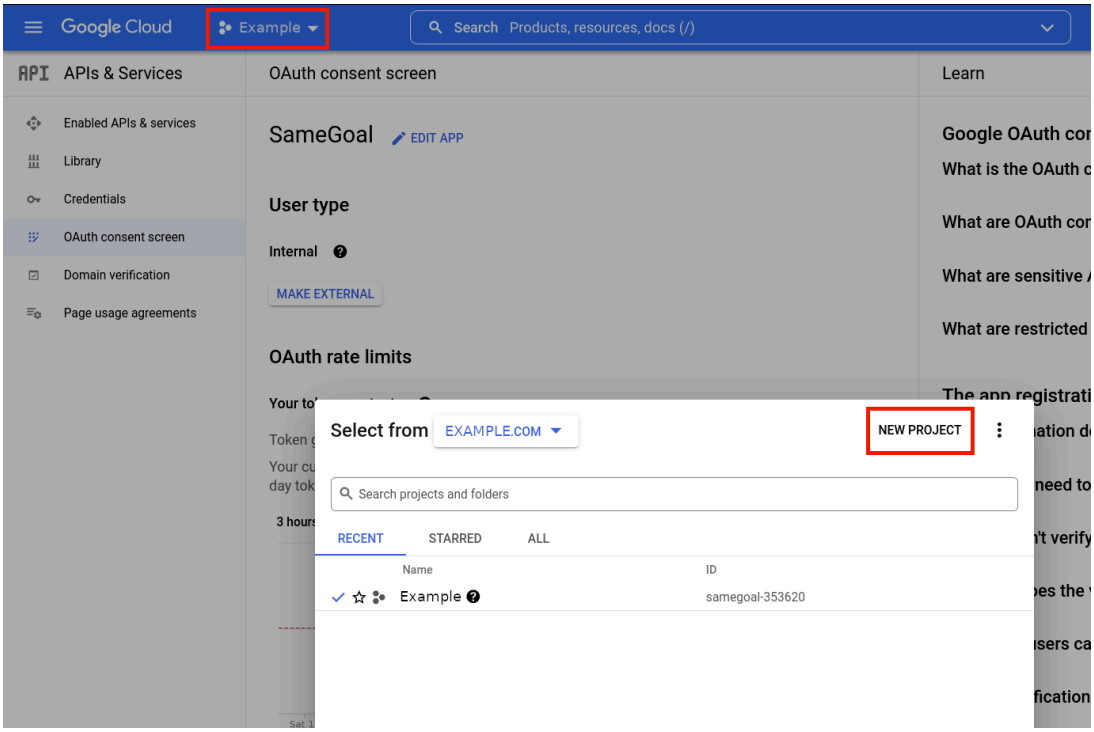
Tip Google frequently changes their user interfaces; directions may not fully match the current Google interface.

Create a new Google API project

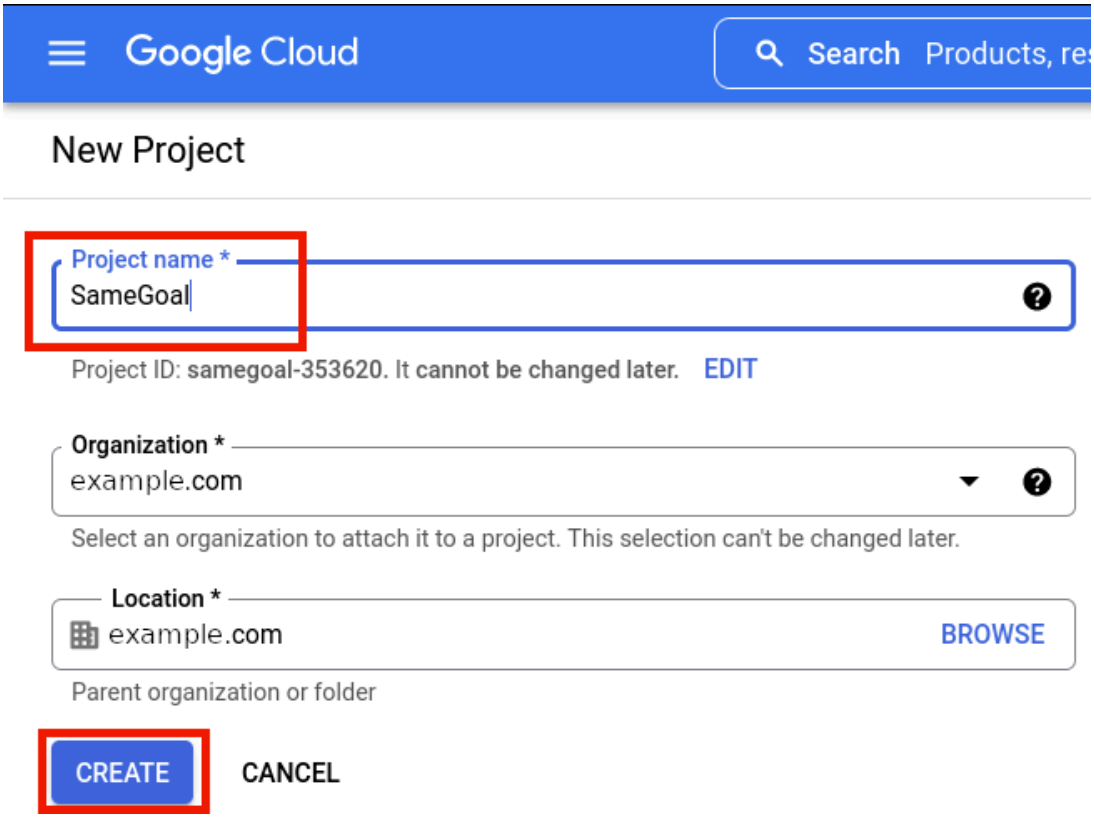
Steps *To create a new Google API project:*

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

- Log in to 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.



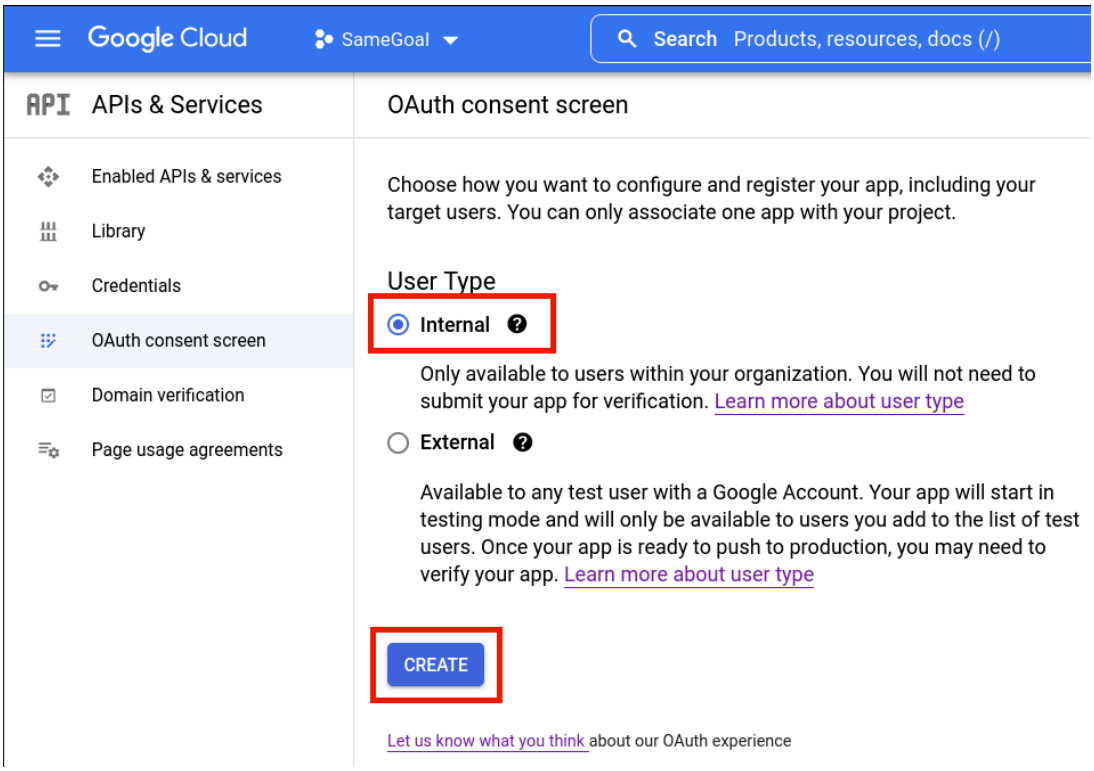
- When the activity completes, continue below.

Set up the consent screen

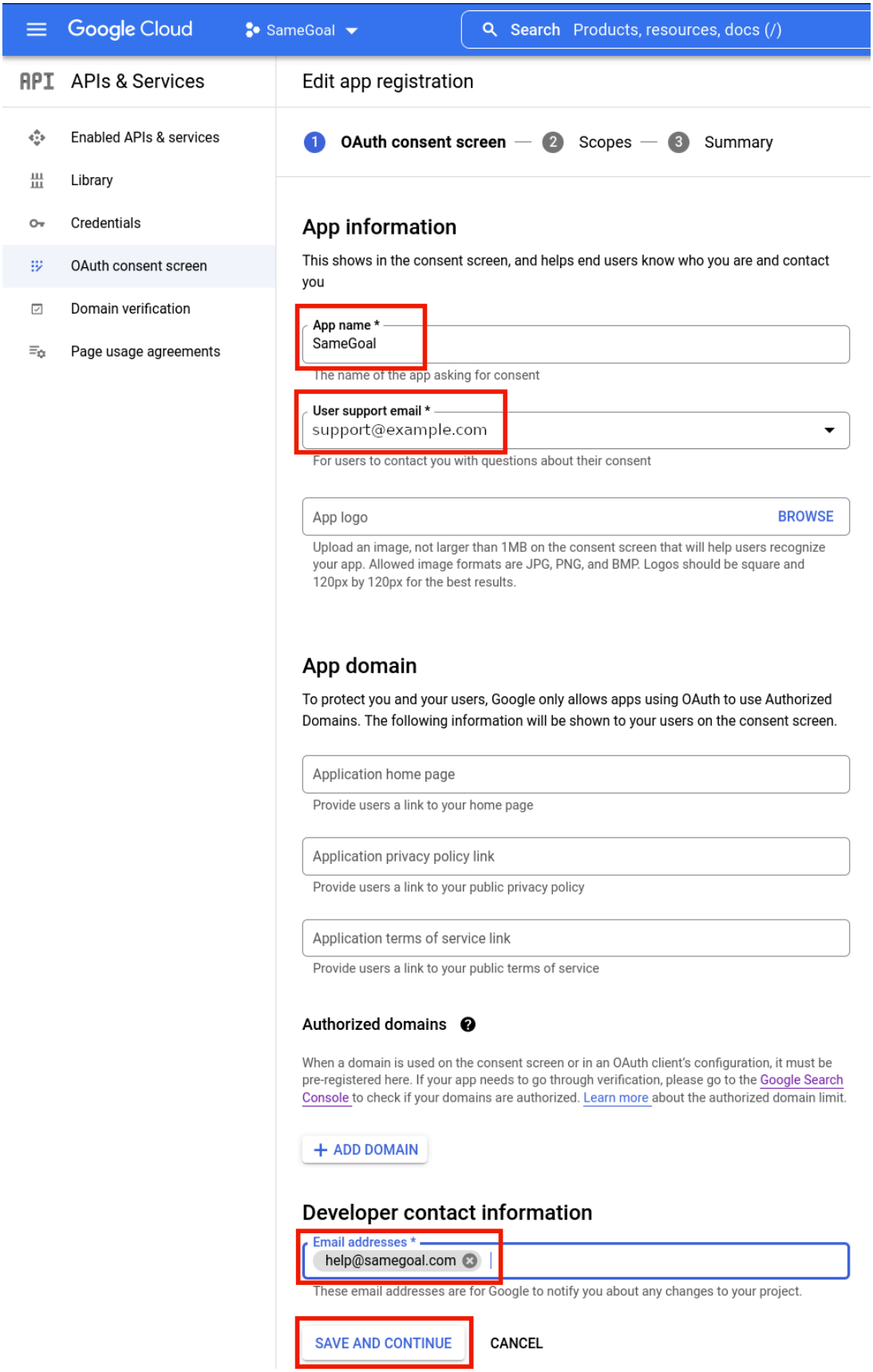
Steps *To setup the consent screen:*

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".



- 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".

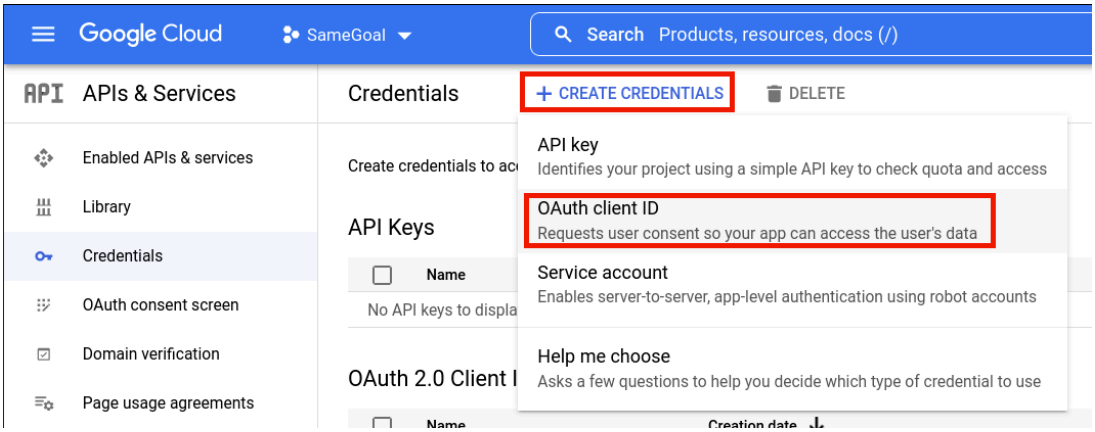


- On the scopes screen, leave the scopes unchanged and click "SAVE AND CONTINUE".
- On the summary screen, click "BACK TO DASHBOARD".

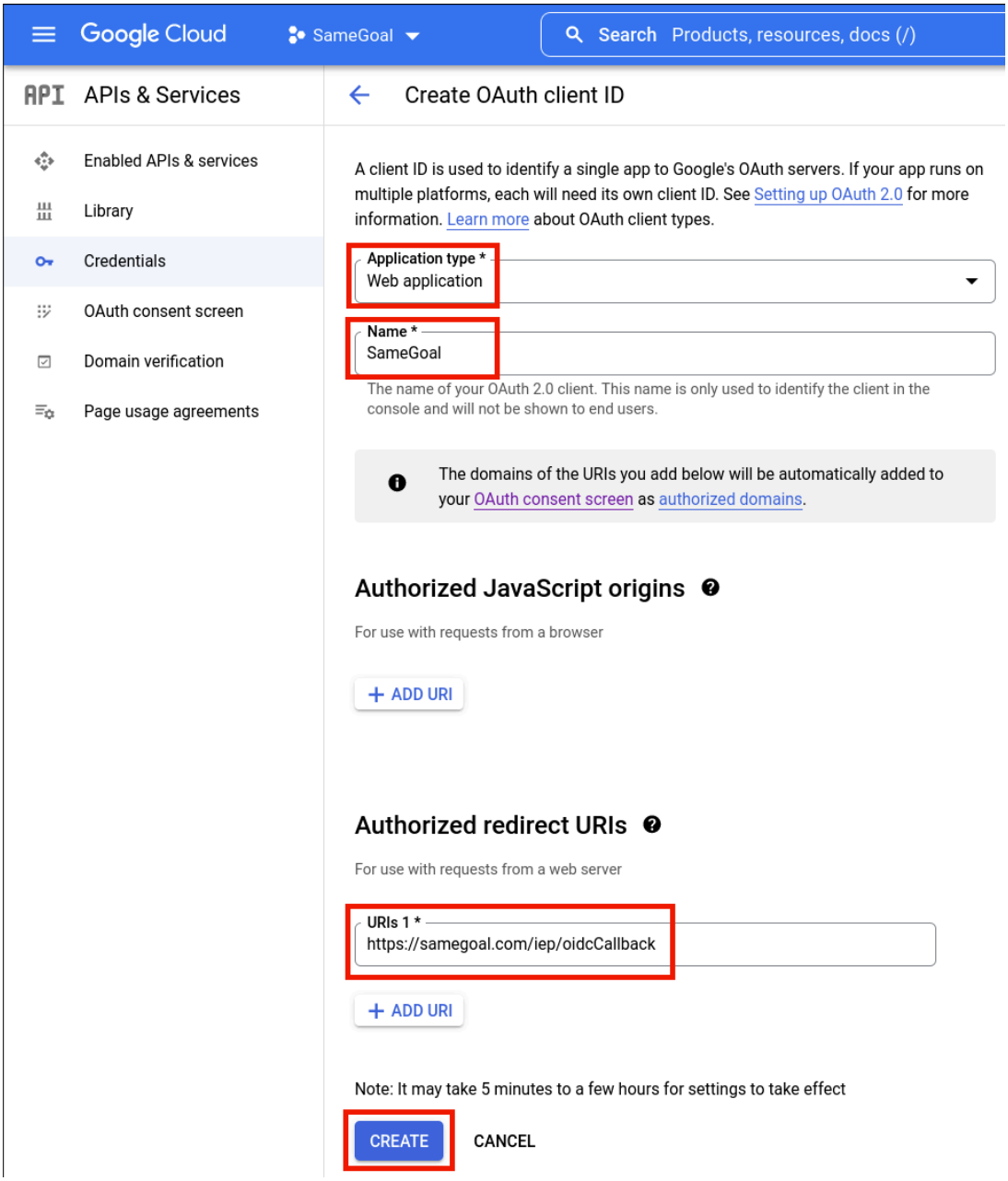
Create an OAuth 2.0 Client ID

Steps *To create an OAuth 2.0 Client ID:*

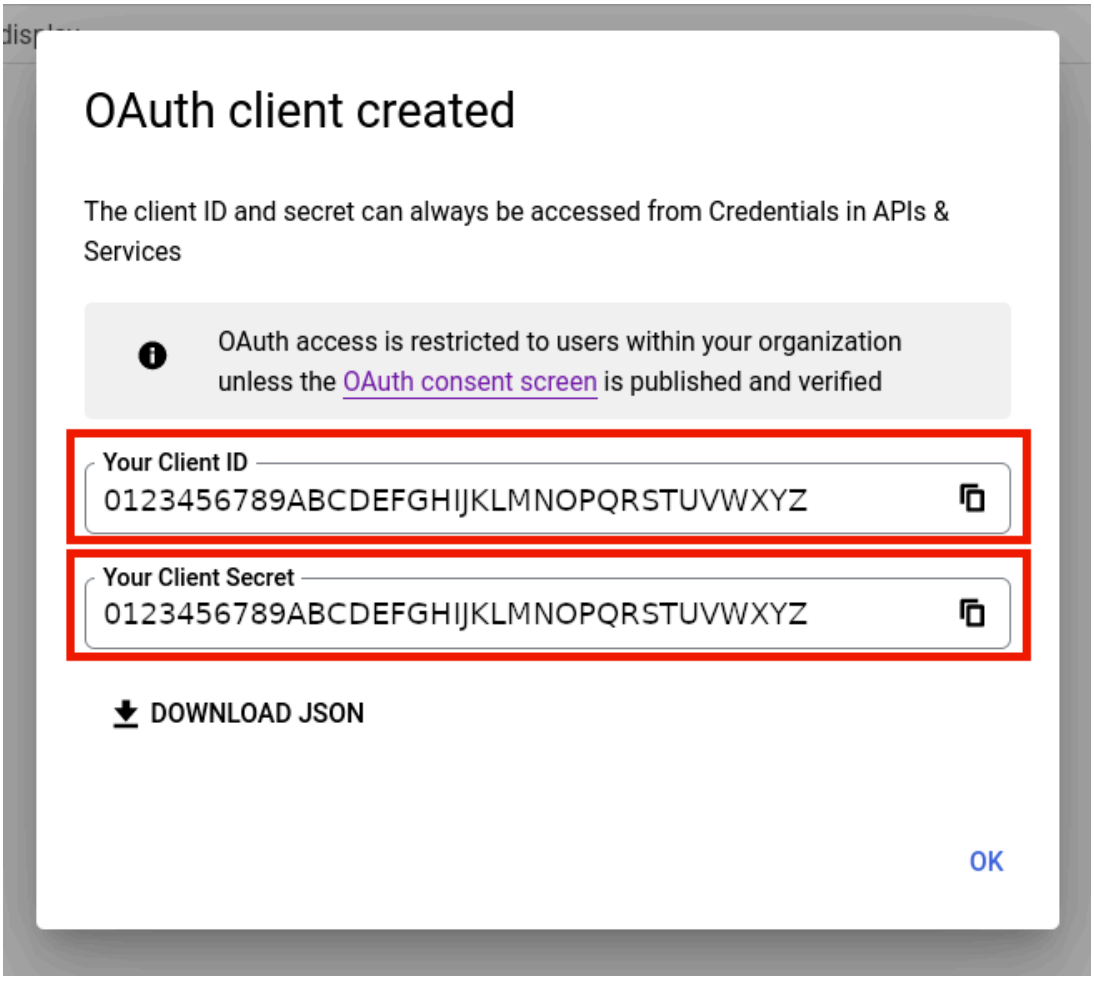
- On the Google Credentials Screen, select "CREATE CREDENTIALS" then "OAuth client ID".



- 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.



- 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
DOWNLOAD JSON
OK

Microsoft Entra OpenID Connect Configuration (Entra SSO)

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

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

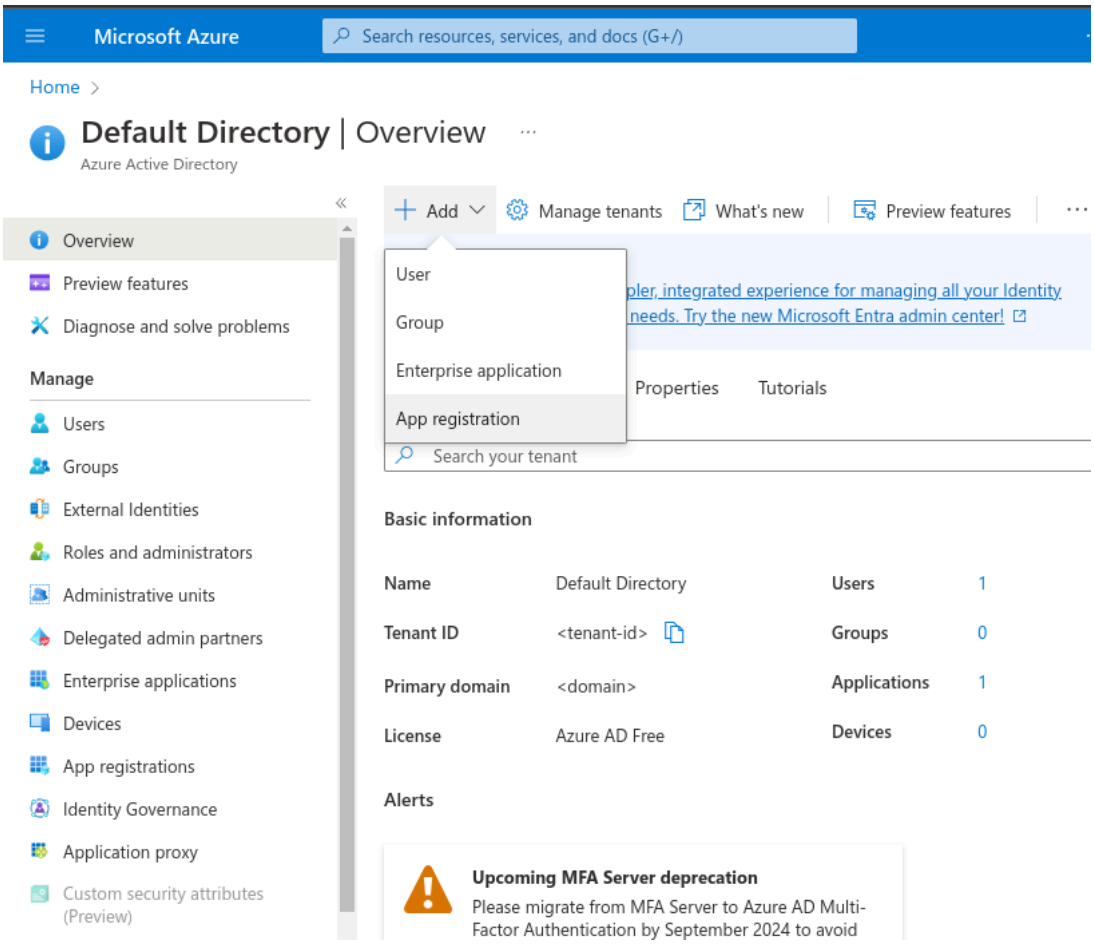
Tip Microsoft Entra frequently changes their user interfaces; directions may not fully match the current Microsoft Entra interface.

Register a new Microsoft Entra application

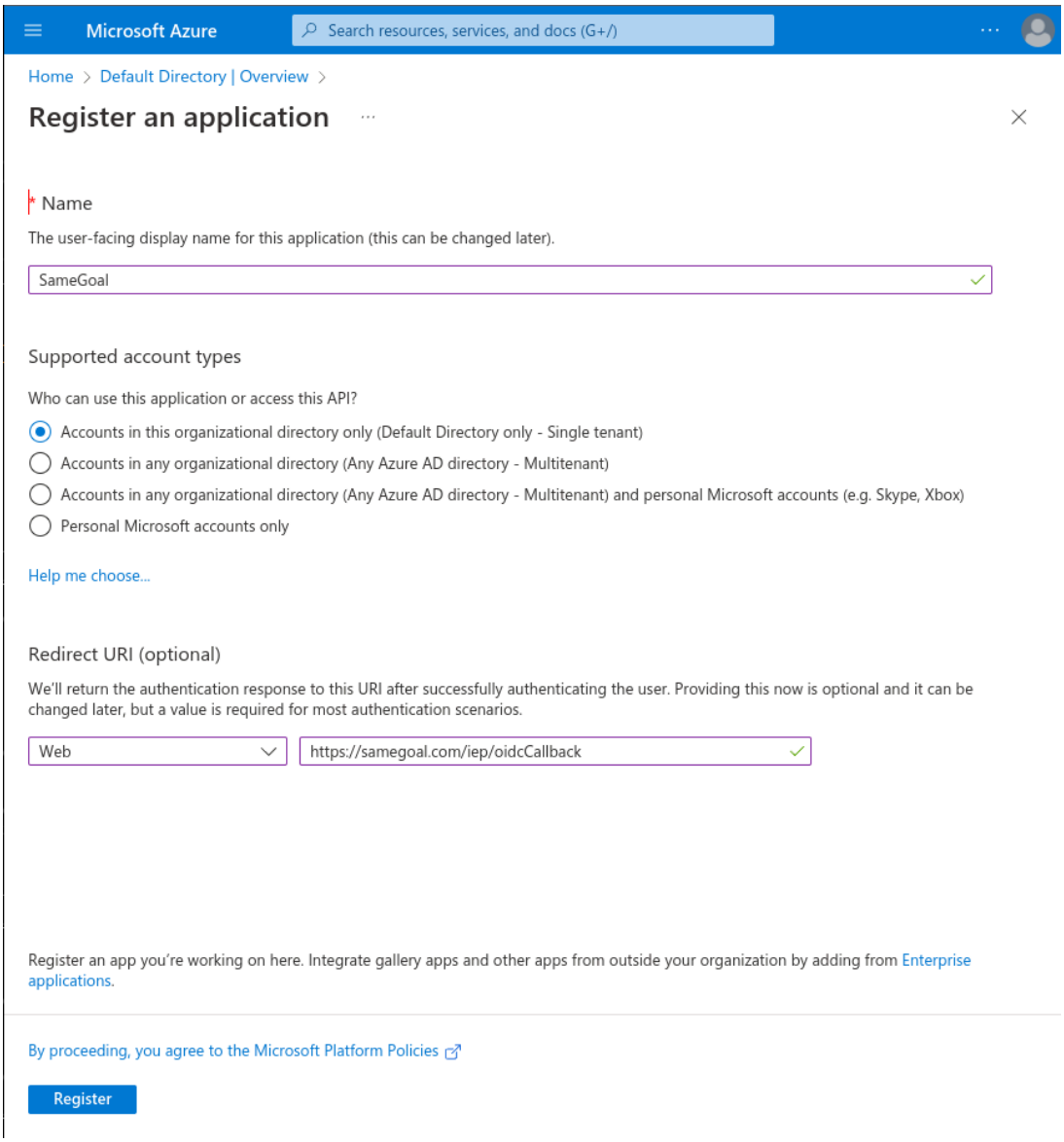
Steps *To register a new Microsoft Entra application:*

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

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



- 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.

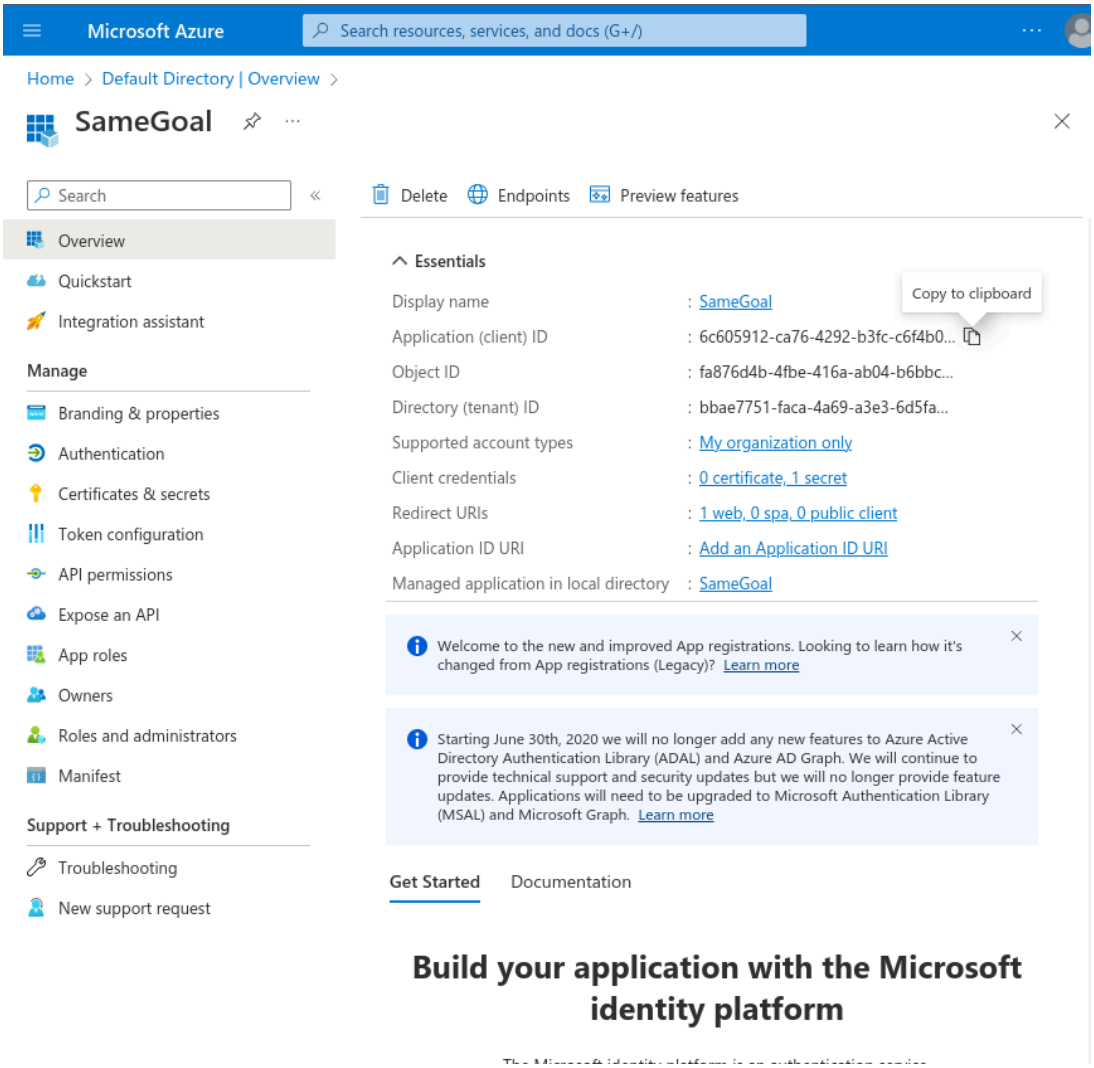


- When the activity completes, continue below.

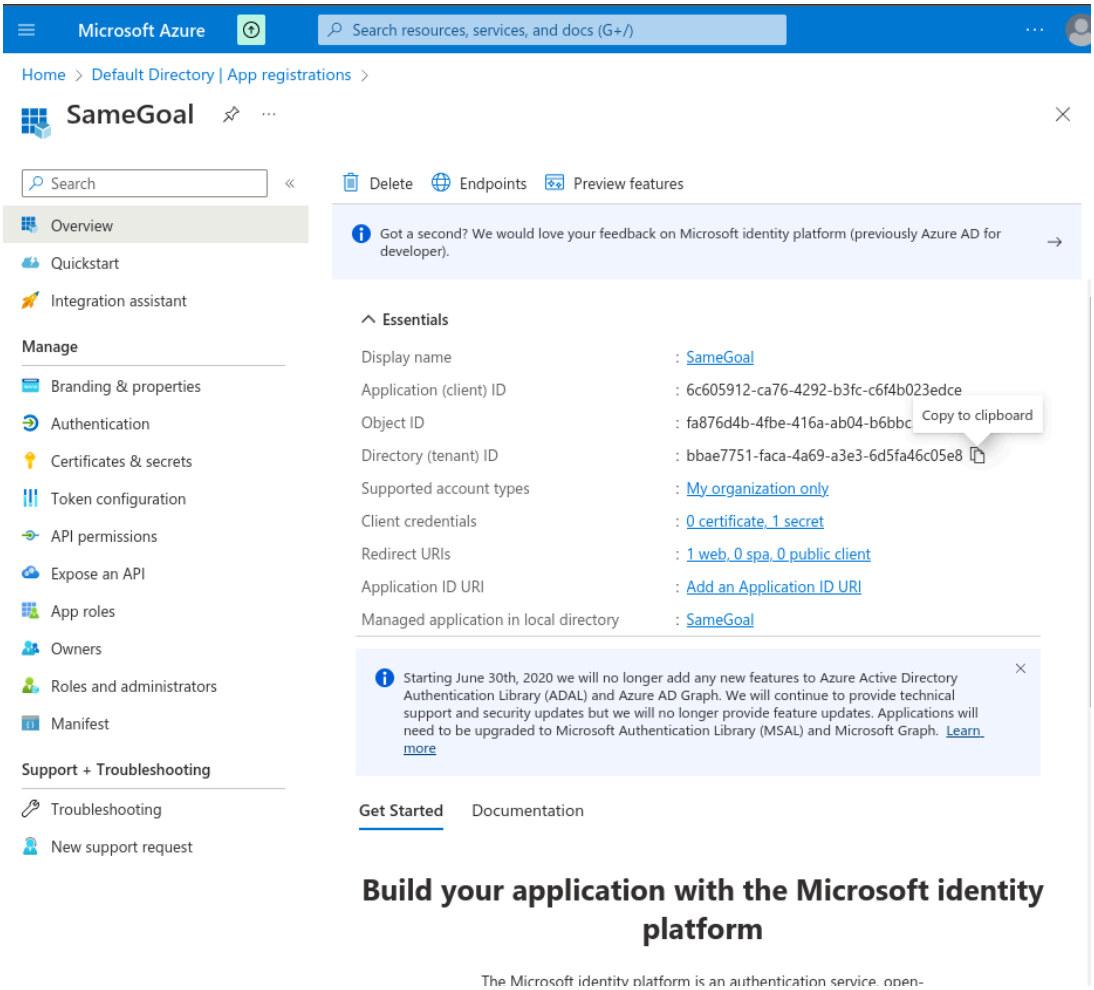
Copy the OAuth 2.0 Client ID

Steps *To copy the OAuth 2.0 Client ID:*

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



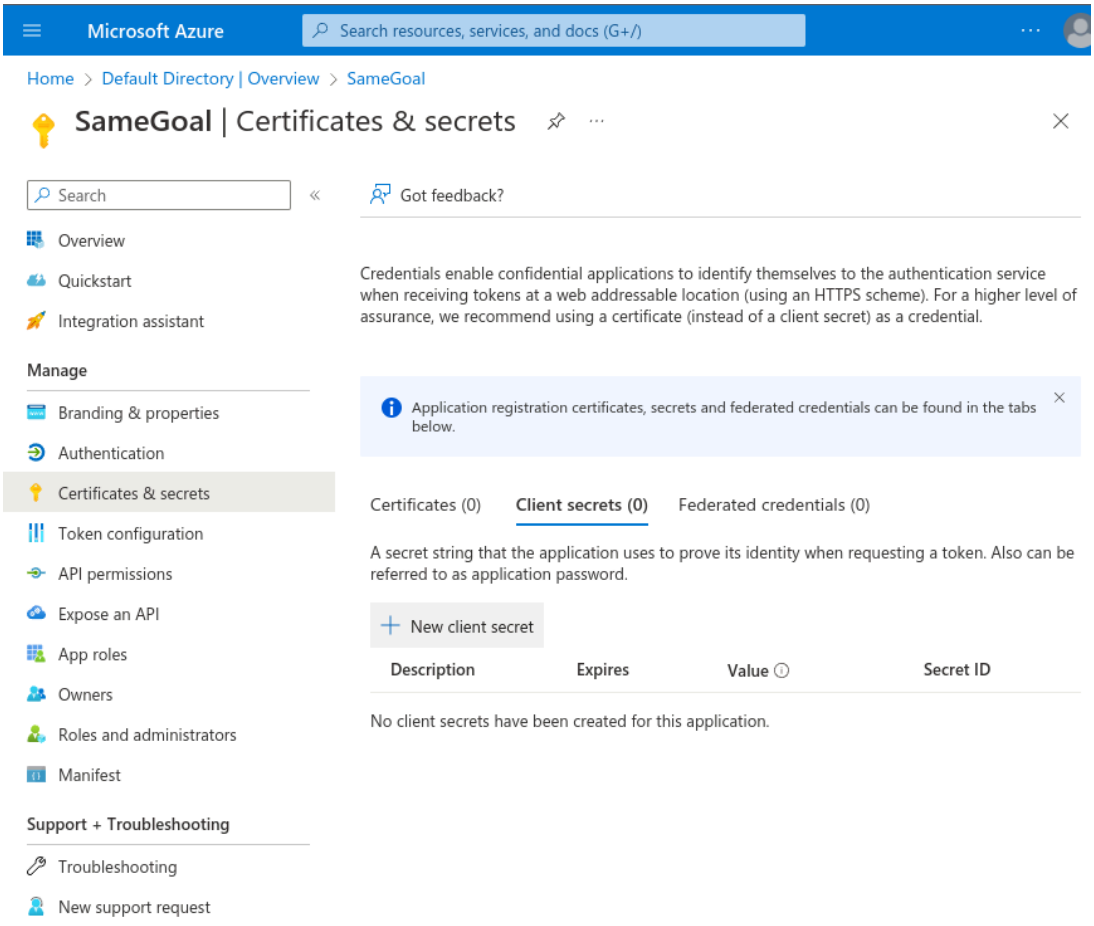
- On the Microsoft Entra Default Directory - SameGoal Overview Screen, copy the "Directory (tenant) ID".
- This Tenant ID will later be pasted into SameGoal as the "Issuer URL" formatted as **https://login.microsoftonline.com/{directory tenant id}/v2.0**.



Create a new OAuth 2.0 Client Secret ID

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

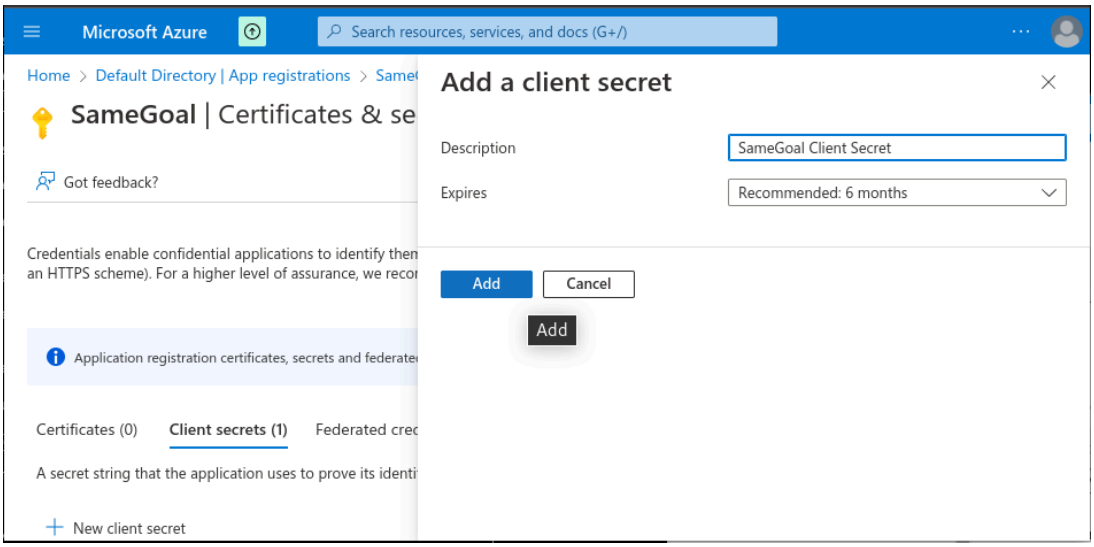
- On the Microsoft Entra Default Directory - SameGoal Overview Screen, select the "Certificates & secrets" option on the left side.
- On the "SameGoal | Certificates & secrets" page that opens, click the "+ New client secret" button.



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

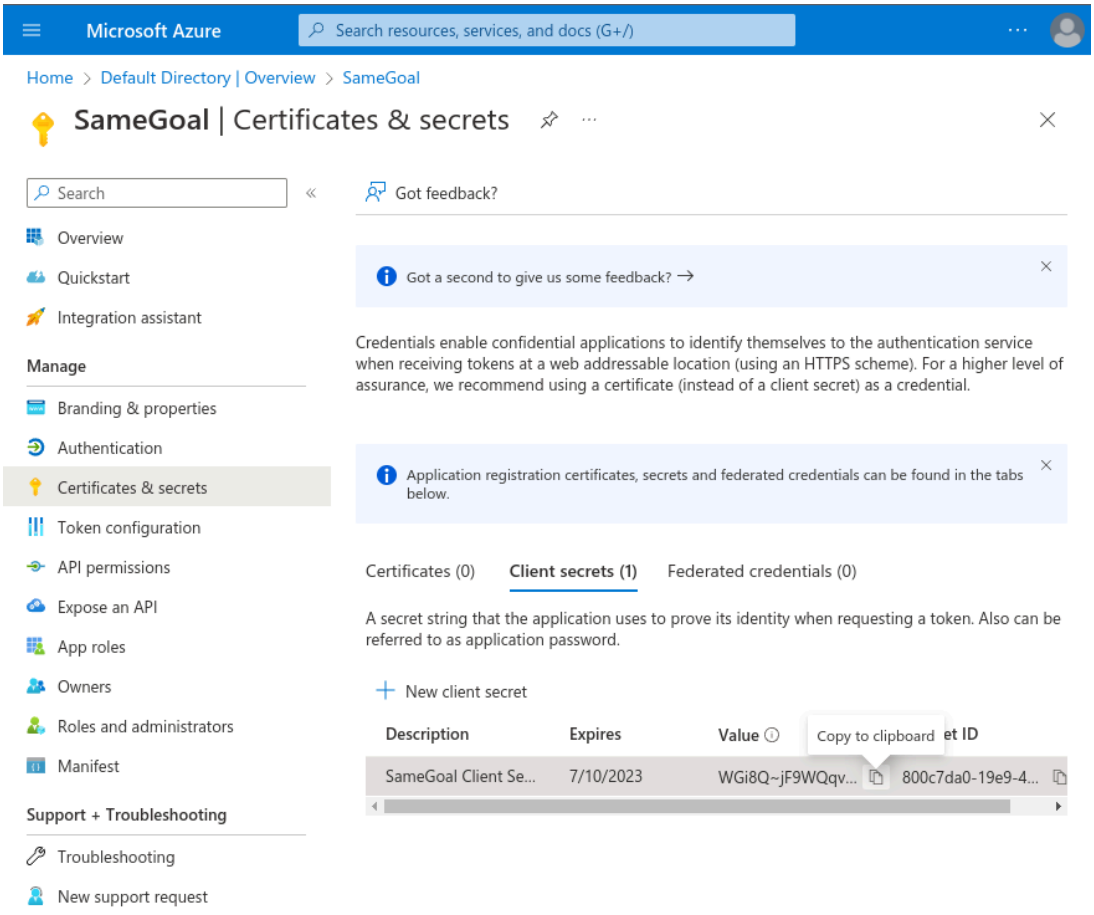
Tip The shorter the expiration, the more often this setup must occur.

- Click the "Add" button.



- Copy the "SameGoal Client Secret" value.

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



- Enter configuration information into SameGoal.

Enter configuration information into SameGoal

Steps *To enter configuration information into SameGoal:*

- Log in to 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).