

# Google as OpenID Connect server for translate5 - example with Google's OAuth 2.0 API

Before your translate5 application can use Google's OAuth 2.0 authentication system for user login, you must set up a project in the [Google API Console](#) to obtain OAuth 2.0 credentials, set a redirect URI, and (optionally) customize the branding information that your users see on the user-consent screen.

## Obtain OAuth 2.0 credentials

You need OAuth 2.0 credentials, including a client ID and client secret, to authenticate users and gain access to Google's APIs.

To find your project's client ID and client secret, do the following:

1. Select an existing OAuth 2.0 credential or open the [Credentials page](#). (see image1)
2. If you haven't done so already, create your project's OAuth 2.0 credentials by clicking **Create credentials > OAuth client ID**, and providing the information needed to create the credentials.
  - a. click on Create credentials dropdown and select OAuth client ID and fill in the requested data
  - b. on the next window
    - i. select Web application in the radio button options
    - ii. give a name to your OAuth client ID (this is not the display name of your app) and click create
  - c. now the new created client id should be listed in the credentials tab (see image2)
3. the next step is to set up Authorized domain
  - a. navigate to the OAuth consent screen
  - b. in the Authorized domains field add you current translate5 domain without protocol (see image4)
  - c. click on save in the page below
4. the next step is to add redirect UrIs
  - a. click on the credentials tab, and click on the openid client
  - b. in the field Authorized redirect URIs add your translate5 instacne domain folowed by /login (image3) and click on save
5. Look for the **Client ID** in the **OAuth 2.0 client IDs** section. For details, click the client ID.

The screenshot shows the 'Create credentials' dialog box. It has a title bar 'APIs & Services' and 'Credentials'. Below the title bar, there are tabs for 'Credentials', 'OAuth consent screen', and 'Domain verification'. A large central area contains the text: 'You need credentials to access APIs. Enable the APIs you plan to use and then create credentials. You may need to enable the APIs if you need an API key, a service account key, or an OAuth 2.0 client ID. For more information, see the authentication documentation.' At the bottom of this area is a blue 'Create credentials' button.

The screenshot shows the 'OAuth 2.0 client IDs' list. The left sidebar shows 'APIs & Services' and 'Credentials'. The main area has tabs for 'Credentials', 'OAuth consent screen', and 'Domain verification'. Below the tabs, there is a message: 'Create credentials to access your enabled APIs. For more information, see the authentication documentation.' Underneath this message, there is a table titled 'OAuth 2.0 client IDs'. The table has columns: 'Name', 'Creation date', 'Type', and 'Client ID'. There is one entry: 'Translated Web application' with 'Mar 1, 2019' in the creation date column, 'Web application' in the type column, and a redacted Client ID.

Google APIs OpenID Project

[Client ID for Web application](#) [DOWNLOAD JSON](#) [RESET SECRET](#) [DELETE](#)

Client ID	[REDACTED]
Client secret	[REDACTED]
Creation date	Mar 1, 2019, 10:31:31 AM
Name	Translated Web application

**Restrictions**  
 An origin, port, origin, redirect URLs, or both. Learn More

**Authorized JavaScript origins**  
 For user auth requests from your browser. This is the origin URL of the client application. It can contain a wildcard (\*). For example, https://example.com/\* or a path (https://example.com/submit). If you're using a nonstandard port, you must include it in the origin URL.  
 Type in the domain and press Enter to add it

**Authorized redirect**  
 For user auth requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. For example, https://www.example.com/auth. Cannot be a public IP address.  
 Type in the domain and press Enter to add it

**Save** **Cancel**

**APIs & Services**

**Credentials**

An image on the consent screen that will help users recognize your app <input type="file" value="Local file for upload"/> <a href="#">Browse</a>	Logo <ul style="list-style-type: none"> <li>Your app displays an icon on its OAuth consent screen</li> <li>Your app has a large number of authorized domains</li> <li>You have made changes to a previously-verified OAuth consent screen</li> </ul>
Support email <input type="text" value=""/> Show on the consent screen for user support	The verification process may take up to several weeks, and you will receive email updates as it progresses. Learn more about verification.
<b>Scopes for Google APIs</b> Scopes allow your application to access your user's private data. Learn more If you add a sensitive scope, such as scopes that give you full access to Gmail or Drive, Google will verify your consent interface is published.	Let us know what you think about our OAuth experience
email profile <input type="text" value="((item.getDeveloperCode())&amp;shortFormDeveloperCode)"/>	
<b>Add scope</b> <b>Authorized domains</b> To protect you and your users, Google only allows applications that authenticate using OAuth to use authorized domains. Your application's links must be hosted on Authorized domains. Learn more <input type="text" value="translated-openid.com"/> <a href="#">Verify</a>	
<b>Application Homepage link</b> Shown on the consent screen. Must be hosted on an Authorized Domain. <input type="text" value="https://url.com"/> <a href="#">Verify</a>	
<b>Application Privacy Policy link</b> Shown on the consent screen. Must be hosted on an Authorized Domain. <input type="text" value="https://url.com"/> <a href="#">Verify</a>	
<b>Application Terms of Service link</b> (Optional) Shown on the consent screen. Must be hosted on an Authorized Domain. <input type="text" value="https://url.com"/> <a href="#">Verify</a>	
<b>Save</b> <b>Submit for verification</b> <b>Cancel</b>	