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

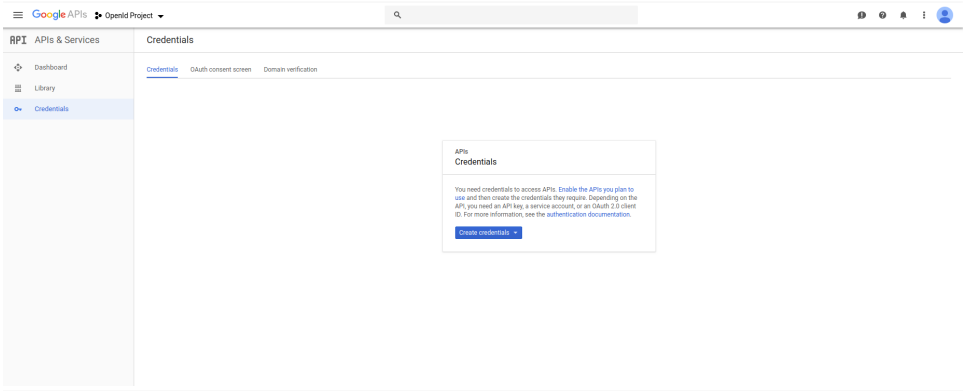
Before your translate5 application can use Google's OAuth 2.0 authentication system for user login, you must set up a project in the Google API Console to obtain OAuth 2.0 credentials, set a redirect URI, and (optionally) customize the branding information that your users see on the user-consent screen.

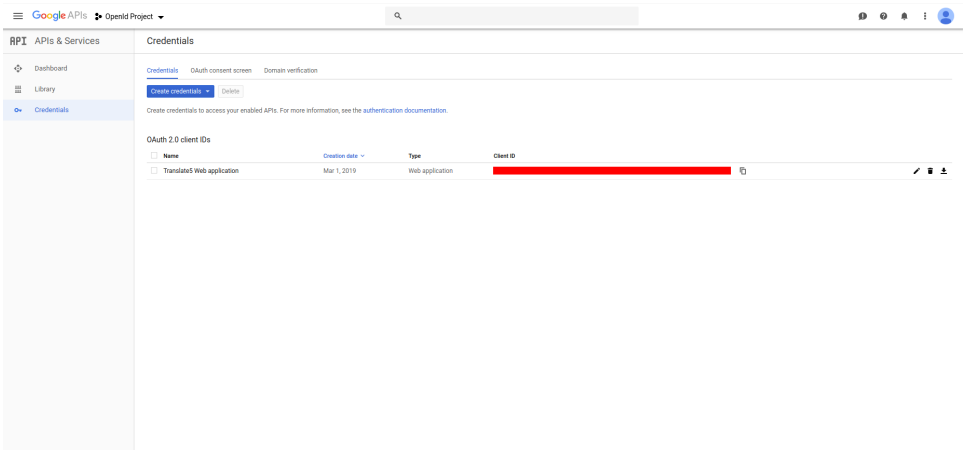
Obtain OAuth 2.0 credentials

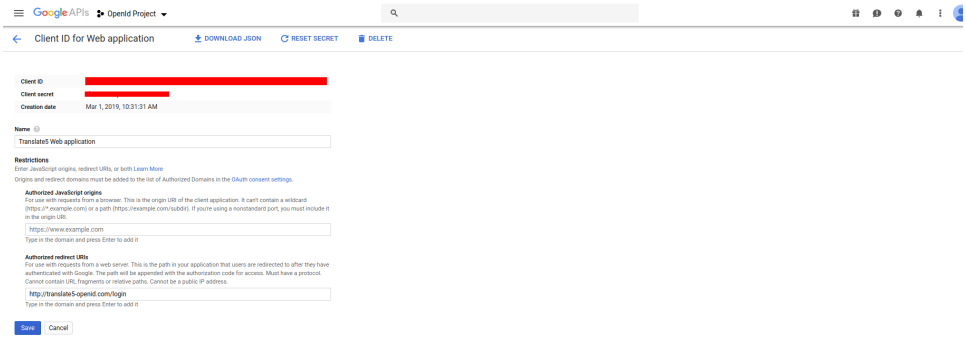
You need OAuth 2.0 credentials, including a client ID and client secret, to authenticate users and gain access to Google's APIs.

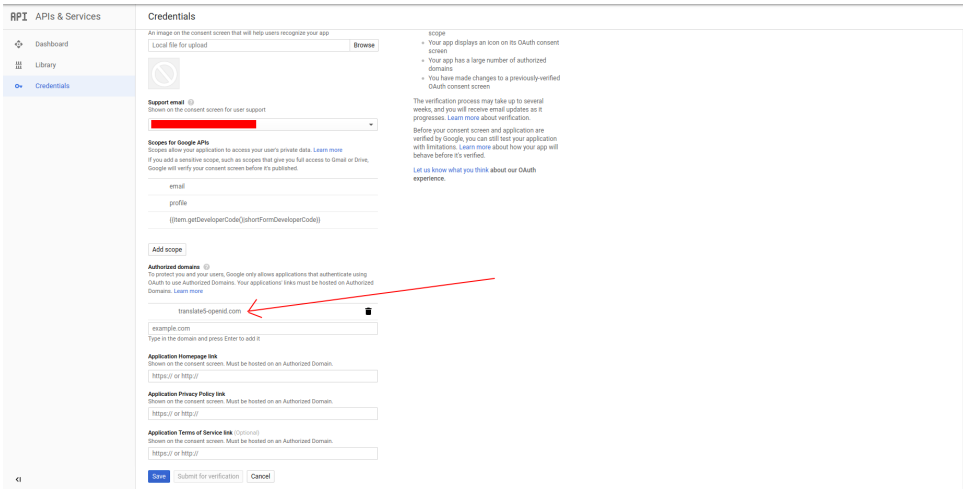
To find your project's client ID and client secret, do the following:

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 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 Urls
    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.






Google APIs
OpenId Project
Client ID for Web application
DOWNLOAD JSON
RESET SECRET
DELETE
Client ID
Client secret
Creation date
Mar 1, 2019, 10:31:31 AM
Name
Translate5 Web application
Restrictions
Enter JavaScript origins, redirect URIs, or both Learn More
Origins and redirect domains must be added to the list of Authorized Domains in the OAuth consent settings.
Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.
https://www.example.com
Type in the domain and press Enter to add it
Authorized redirect URIs
For use with 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. Cannot contain URL fragments or relative paths. Cannot be a public IP address.
http://translate5-openid.com/login
Type in the domain and press Enter to add it
Save
Cancel


APIs & Services
Dashboard
Library
Credentials
Credentials
An image on the consent screen that will help users recognize your app
Local file for upload
Browse
Support email
Shown on the consent screen for user support
Scopes for Google APIs
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 screen before it's published.
email
profile
{{item.getDeveloperCode()|shortFormDeveloperCode}}
Add scope
Authorized domains
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. Learn more
translate5-openid.com
example.com
Type in the domain and press Enter to add it
Application Homepage link
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://
Application Privacy Policy link
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://
Application Terms of Service link (Optional)
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://
Save
Submit for verification
Cancel
scope
Your app displays an icon on its OAuth consent screen
Your app has a large number of authorized domains
You have made changes to a previously-verified OAuth consent screen
The verification process may take up to several weeks, and you will receive email updates as it progresses. Learn more about verification.
Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified.
Let us know what you think about our OAuth experience.