Google

This page is a step-by-step guide for the process of opening and setting up an external Google application as part of the Gigya Setup process.

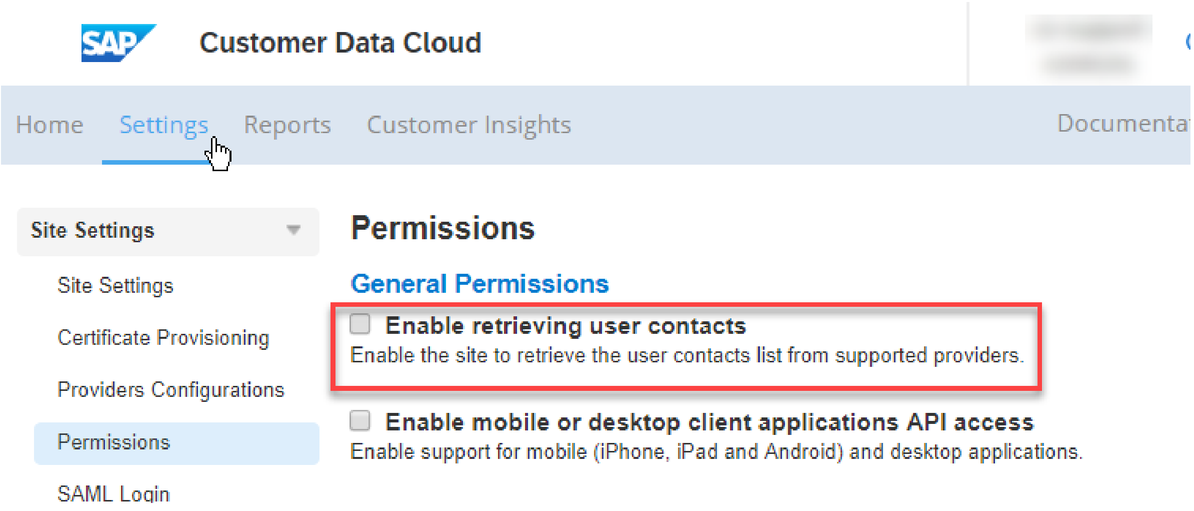
> **Note:** If your site is defined under one of Gigya's non-US data centers, replace domain references to "*socialize.gigya.com*" (or "*socialize.us1.gigya.com*") with **https://socialize.<data_center>/**
>
> Where <Data_Center> is:
>
> - **`us1.gigya.com`** - For the US data center.
> - **`eu1.gigya.com`** - For the European data center.
> - **`au1.gigya.com`** - For the Australian data center.
> - **`ru1.gigya.com`** - For the Russian data center.
> - **`cn1.gigya-api.cn`** - For the Chinese data center.
>
> If you are not sure of your site's data center, see Finding Your Data Center.
>
> Domain references are defined in Gigya's dashboard, externally in social network app definition pages, and when using Gigya's SDKs to set the domain (in particular the *APIDomain* field in class GSRequest).

Google Plus Deprecation FAQ

Google has announced they are accelerating the deprecation of all their G+ APIs. This begins on January 28, 2019 and will complete on March 7, 2019.

- Does the deprecation of Google Plus affect me?
  - Yes, if you are using Google as a login provider then you will need to take some action for Google to continue to function properly, as detailed below. We expect the transition to go smoothly, thanks to the following:
    - The OIDC login flow has been supported for some time, meaning users should continue to be able to log in using their Google identities.
    - Our tests show that the providerUID returned from Google is the same for Google Plus and Google Sign-In, so user records will update seamlessly after the change.

- What do I need to do to ensure the Google login option will work smoothly?
  - After your Provider Configuration is updated, if you are using the **General Permission** of **Enable retrieving user contacts** you will need to stop requesting that permission by unchecking the box and re-saving your site's Permissions.



Permissions

General Permissions

☐ **Enable retrieving user contacts**
Enable the site to retrieve the user contacts list from supported providers.

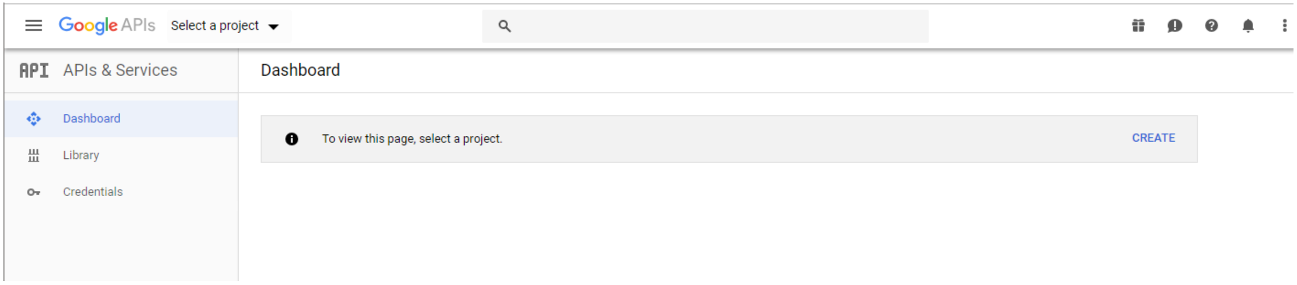
☐ **Enable mobile or desktop client applications API access**
Enable support for mobile (iPhone, iPad and Android) and desktop applications.

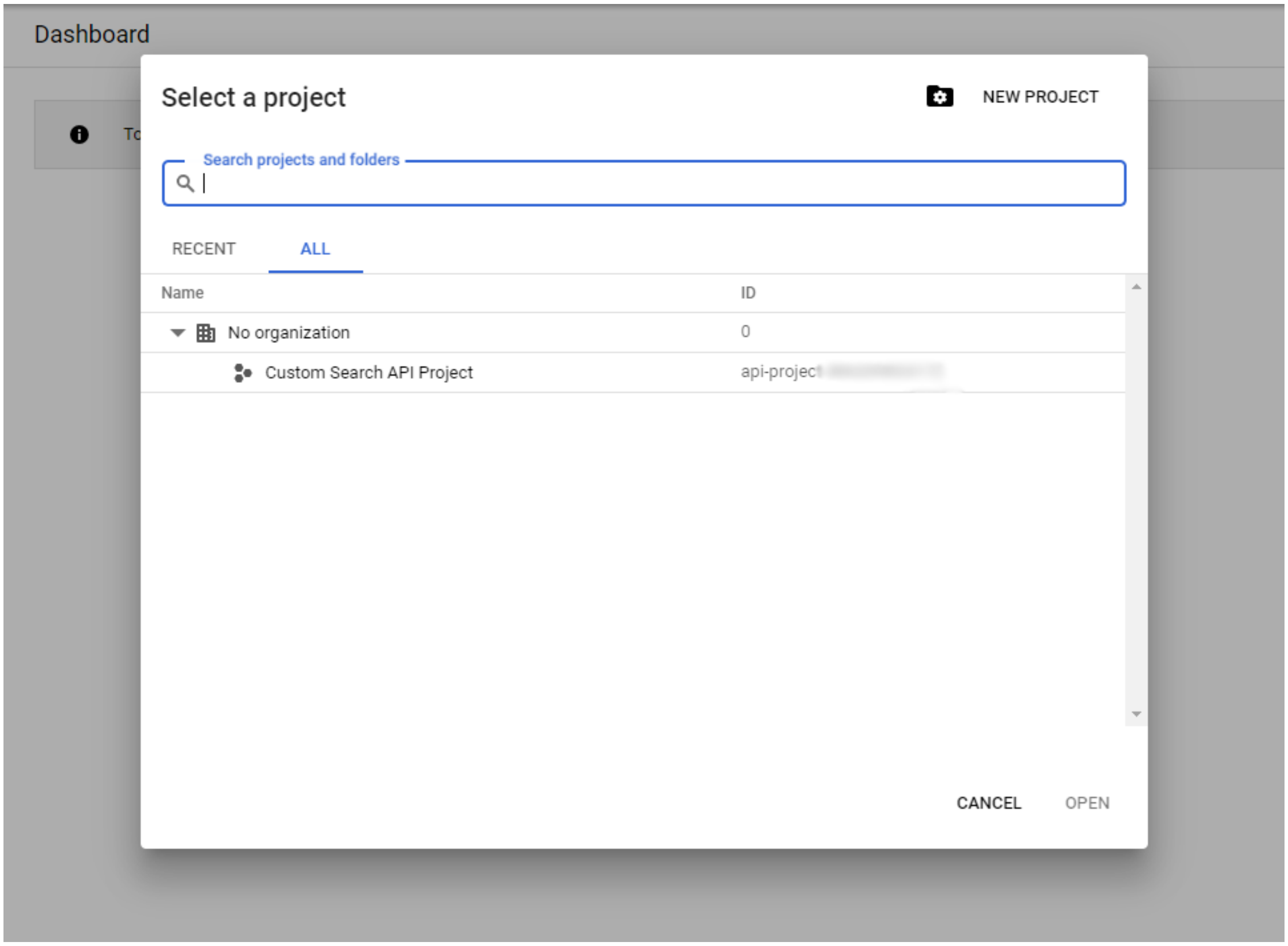
- Does the deprecation affect my mobile apps?
  - Yes, any mobile apps that are using Google as a login provider via our Android SDK need to be updated and recompiled with the latest SDK to support the Google Plus deprecation. Download the latest Android SDK (v3.3.28 or above): Gigya Developer Downloads

Phase 1 - Setting up a Google Application

Creating a project

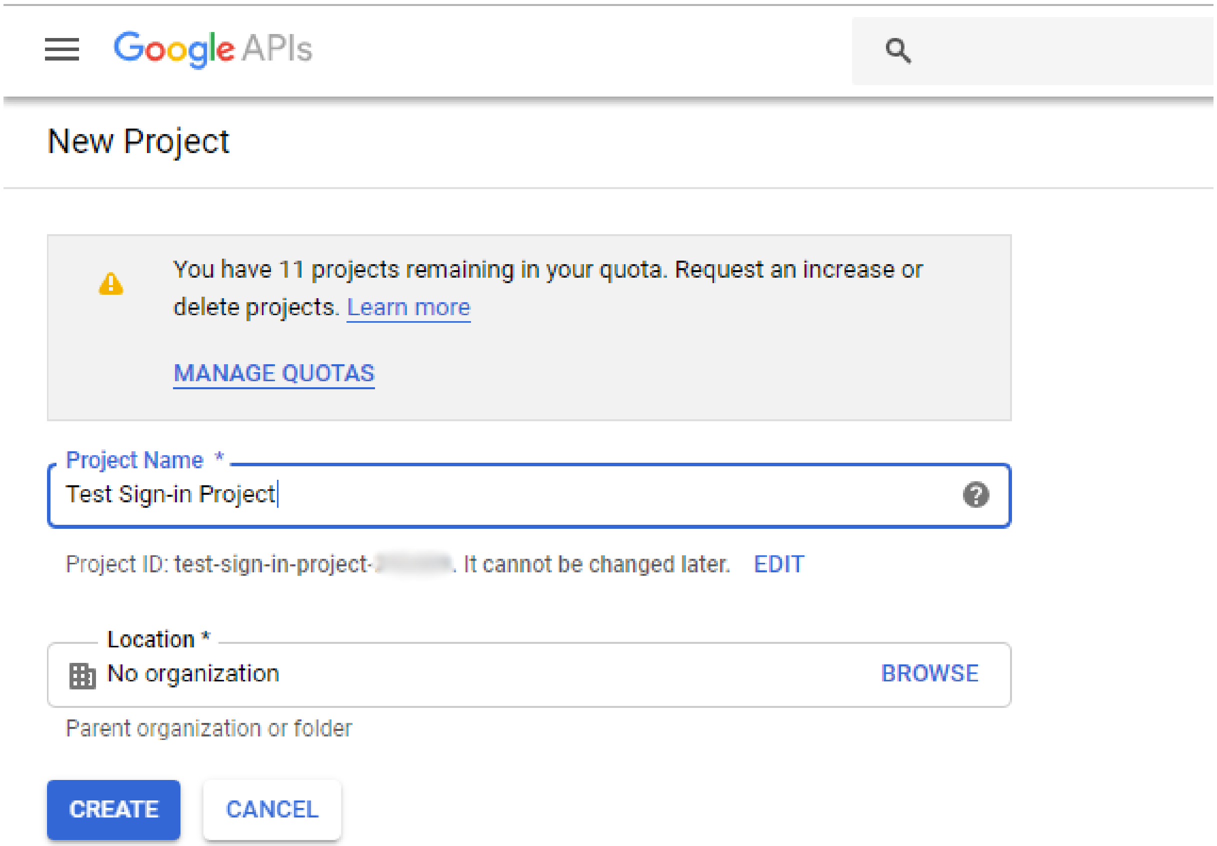
1. Go to the Google Developers Console at https://console.developers.google.com.
2. Click the **Select a project** menu to open the Projects screen, then press the **NEW PROJECT** button add a new project.





3. In the "New Project" box:

   - Enter a Project Name.
   - Define whether or not to attach the new project to an organization.
   - Click **Create**.
   - You will then arrive at the projects Dashboard.



New Project

You have 11 projects remaining in your quota. Request an increase or delete projects. Learn more

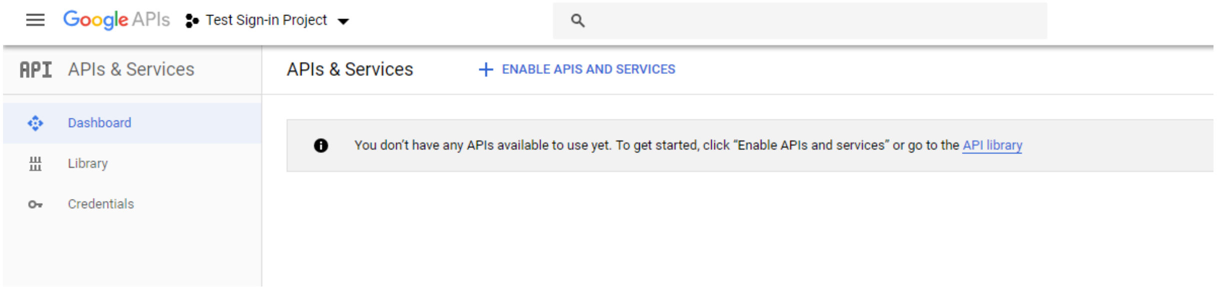
MANAGE QUOTAS

Project Name *
Test Sign-in Project

Project ID: test-sign-in-project-[redacted]. It cannot be changed later. EDIT

Location *
No organization BROWSE

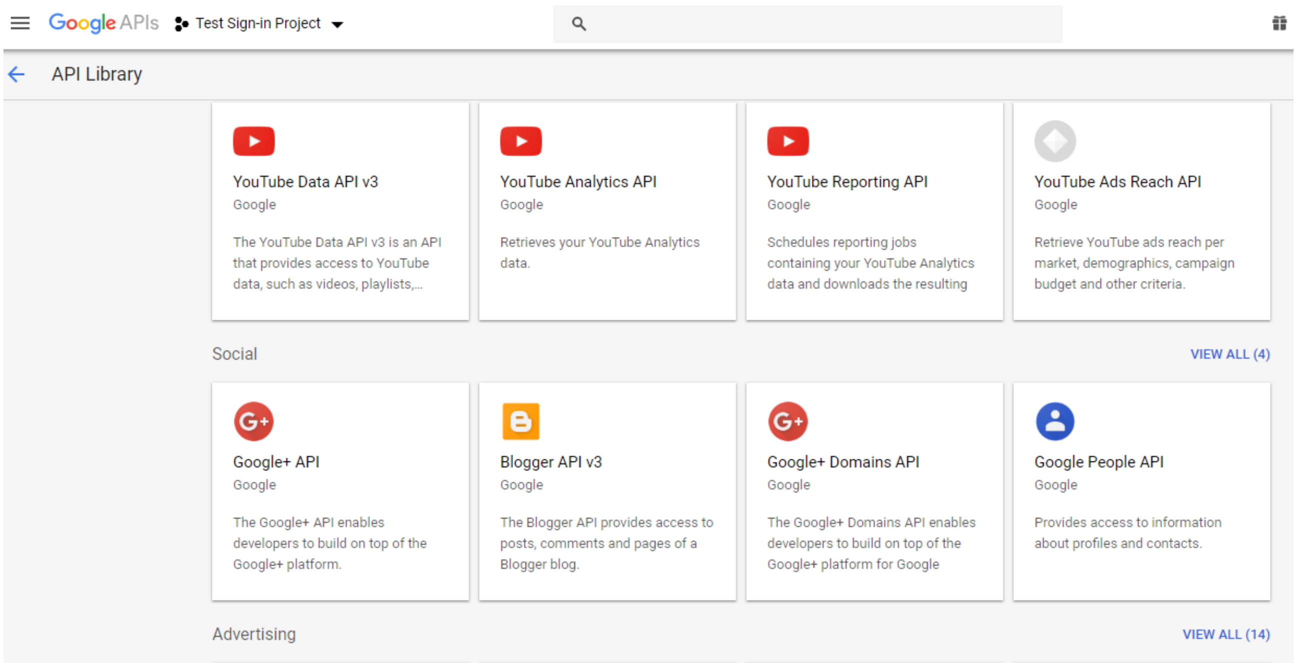
Parent organization or folder



You don't have any APIs available to use yet. To get started, click "Enable APIs and services" or go to the API library

Selecting your APIs for use with Gigya

1. Click ENABLE APIS AND SERVICES (above), scroll-down and select "Google People API" (under 'Social APIs').



YouTube Data API v3
Google
The YouTube Data API v3 is an API that provides access to YouTube data, such as videos, playlists,...

YouTube Analytics API
Google
Retrieves your YouTube Analytics data.

YouTube Reporting API
Google
Schedules reporting jobs containing your YouTube Analytics data and downloads the resulting

YouTube Ads Reach API
Google
Retrieve YouTube ads reach per market, demographics, campaign budget and other criteria.

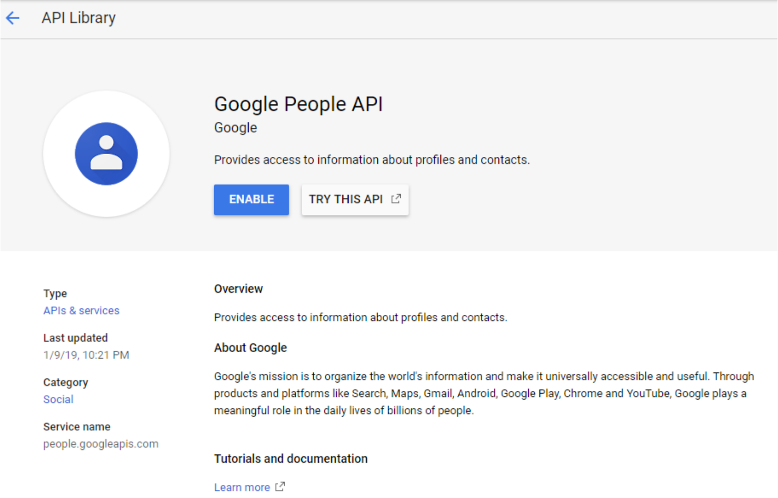
Google+ API
Google
The Google+ API enables developers to build on top of the Google+ platform.

Blogger API v3
Google
The Blogger API provides access to posts, comments and pages of a Blogger blog.

Google+ Domains API
Google
The Google+ Domains API enables developers to build on top of the Google+ platform for Google

Google People API
Google
Provides access to information about profiles and contacts.

2. On the following page press the ENABLE button.



Google People API
Google
Provides access to information about profiles and contacts.

Type
APIs & services

Last updated
1/9/19, 10:21 PM

Category
Social

Service name
people.googleapis.com

Overview

Provides access to information about profiles and contacts.

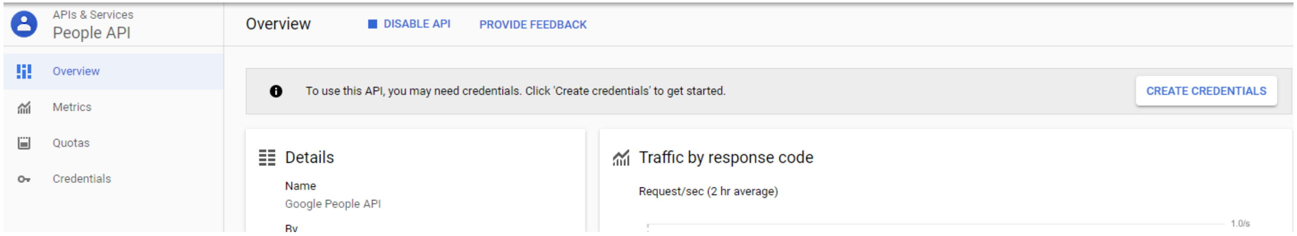
About Google

Google's mission is to organize the world's information and make it universally accessible and useful. Through products and platforms like Search, Maps, Gmail, Android, Google Play, Chrome and YouTube, Google plays a meaningful role in the daily lives of billions of people.

Tutorials and documentation

Learn more

3. Press the **Create Credentials** button on the next page to create your credentials, on the right.

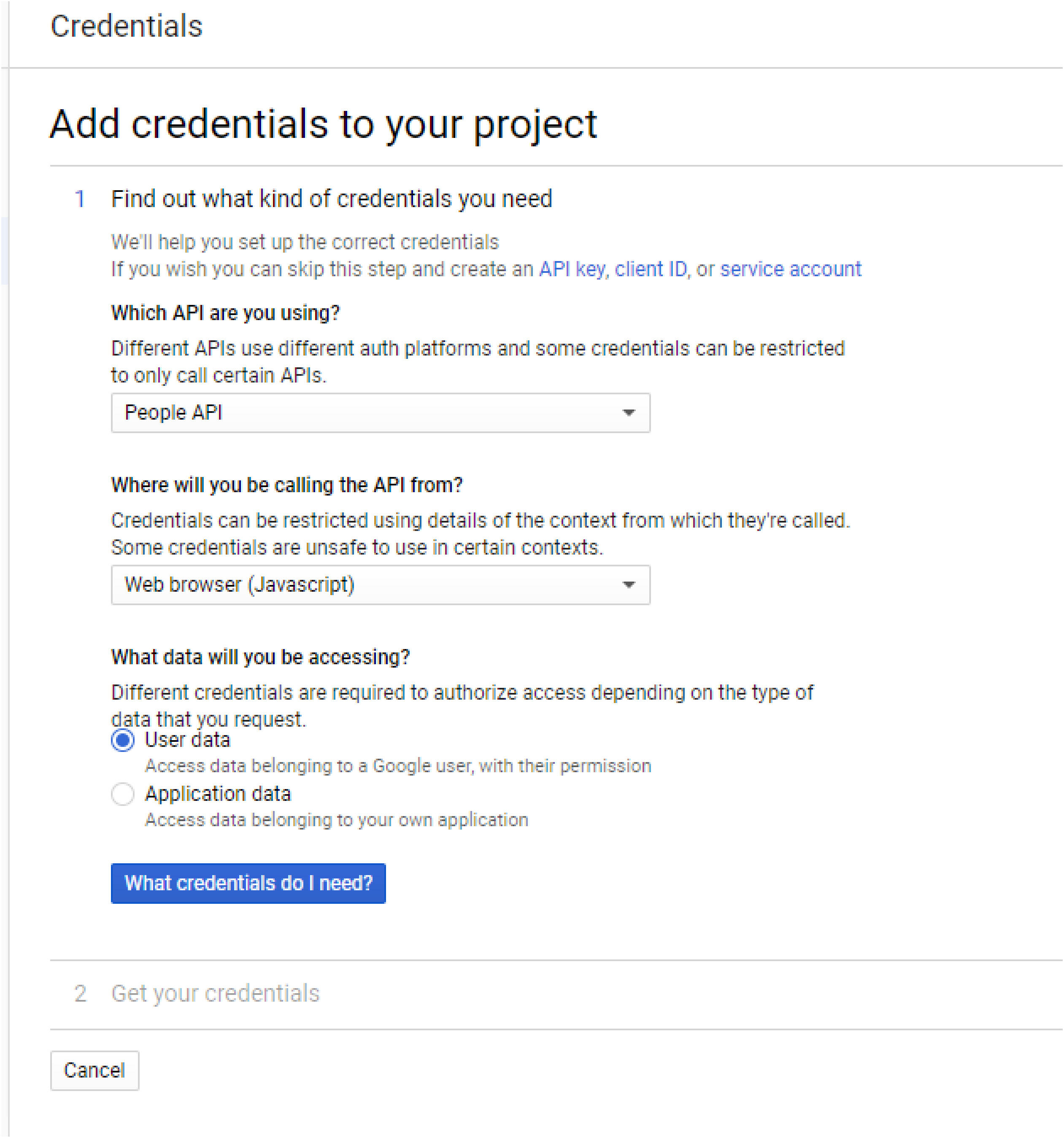


To use this API, you may need credentials. Click 'Create credentials' to get started.

Name
Google People API
By

Get your Google credentials

1. Google supplies a brief questionnaire to help you configure your app. Simply answer the questions and it will direct you to the proper credential type for your app. Since we are using the **People API** for the **web**, we will choose those and select **User data** as what we will be accessing. When finished, click **What credentials do I need?**.



Credentials

Add credentials to your project

1 Find out what kind of credentials you need

We'll help you set up the correct credentials
If you wish you can skip this step and create an API key, client ID, or service account

Which API are you using?

Different APIs use different auth platforms and some credentials can be restricted to only call certain APIs.

People API

Where will you be calling the API from?

Credentials can be restricted using details of the context from which they're called. Some credentials are unsafe to use in certain contexts.

Web browser (Javascript)

What data will you be accessing?

Different credentials are required to authorize access depending on the type of data that you request.

● User data
Access data belonging to a Google user, with their permission

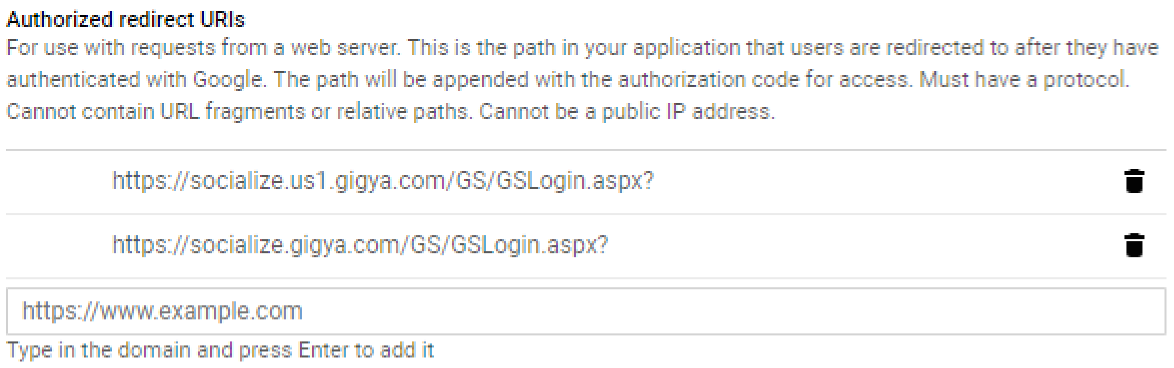
○ Application data
Access data belonging to your own application

2. The system should now direct you to Create an OAuth 2.0 client ID. Give your app a name and enter your **Authorized redirect URIs** in the respective fields. If you are not using a Cname, these will be:

```
https://<DataCenter>/GS/GSLogin.aspx?
```

Finding Your Data Center

The URIs **must** include the trailing "**?**".



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.

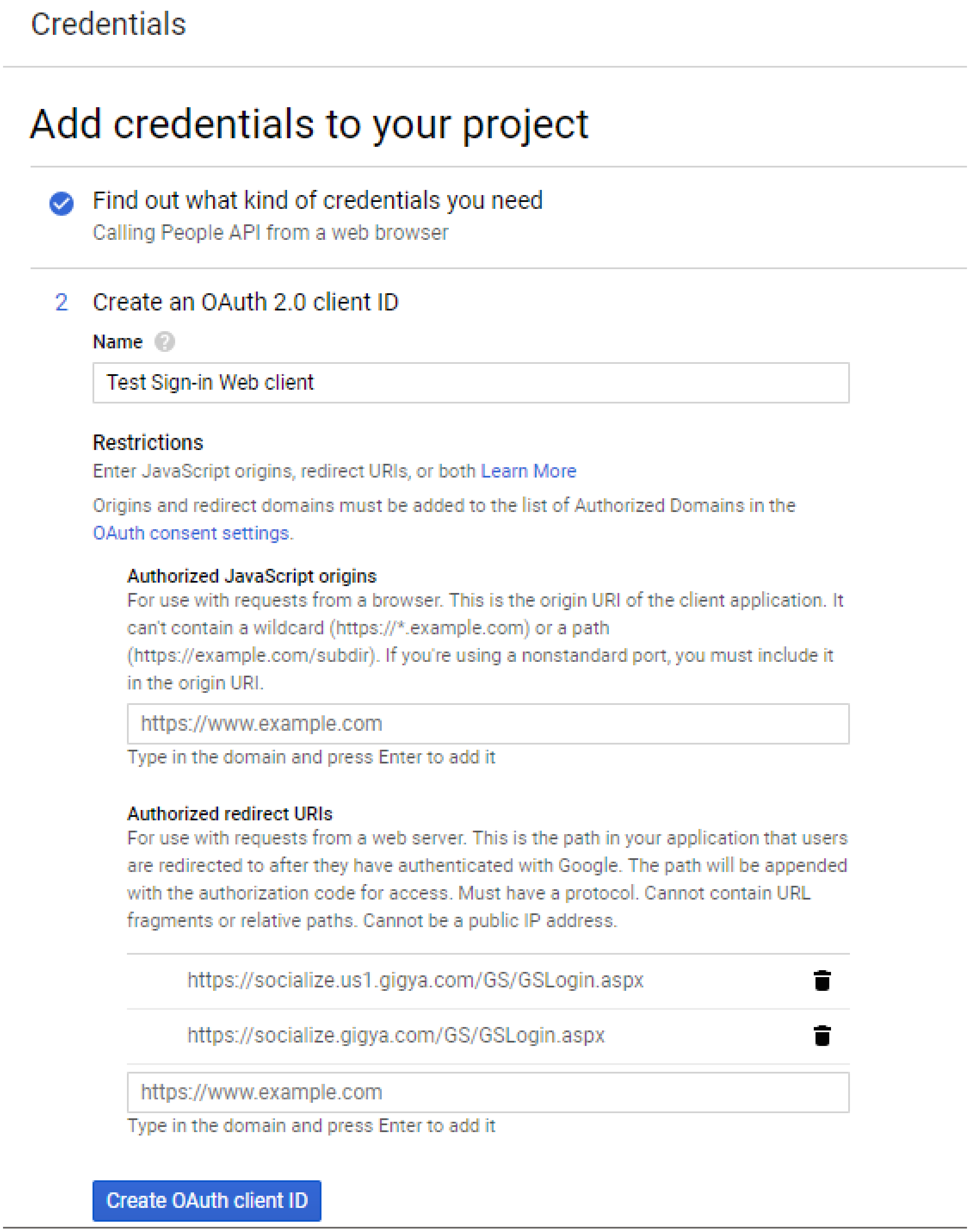
https://socialize.us1.gigya.com/GS/GSLogin.aspx?

https://socialize.gigya.com/GS/GSLogin.aspx?

https://www.example.com

Type in the domain and press Enter to add it

When complete, press **Create OAuth client ID**.



Credentials

Add credentials to your project

✓ Find out what kind of credentials you need

Calling People API from a web browser

2 Create an OAuth 2.0 client ID

Name

Test Sign-in Web client

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.

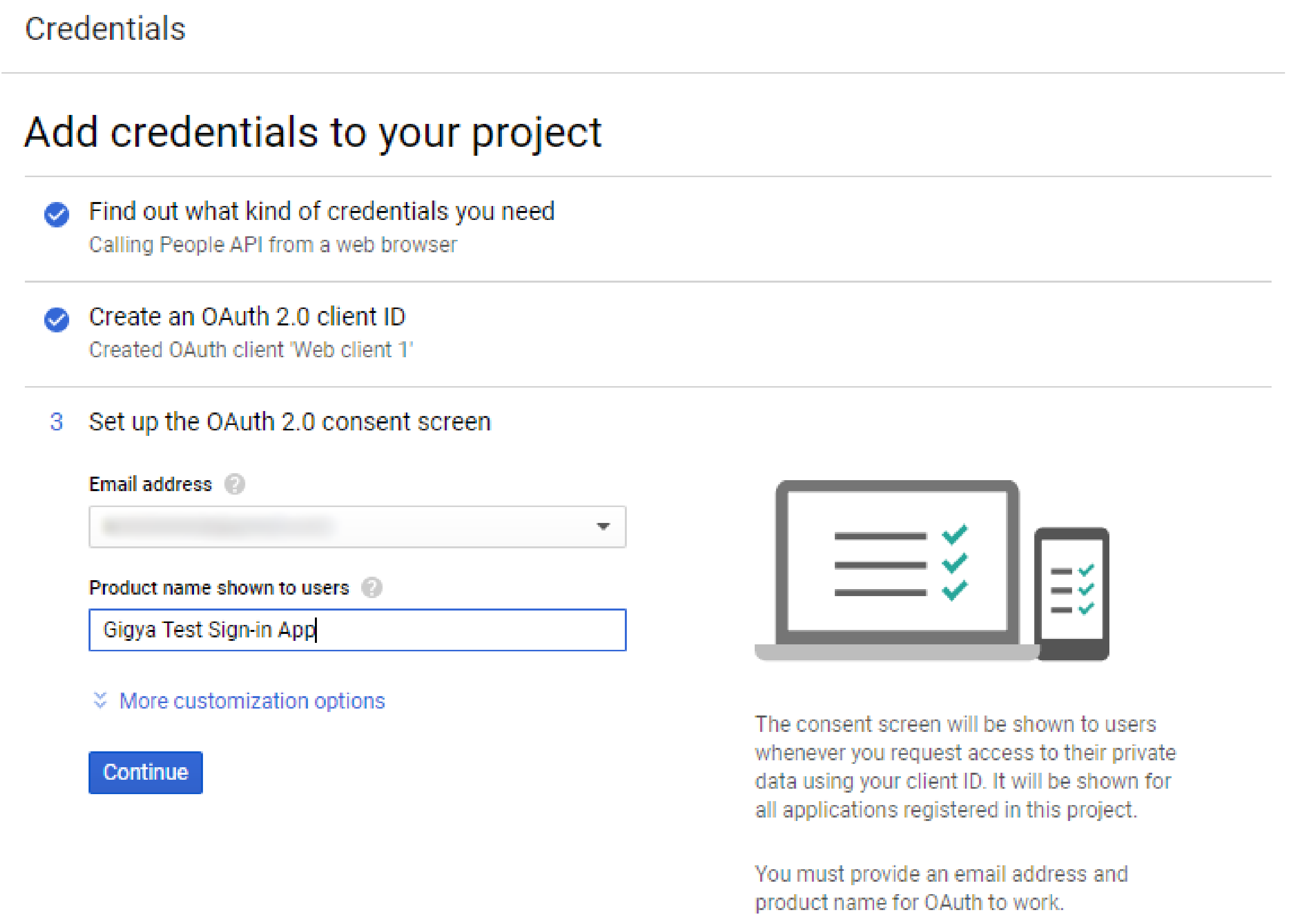
https://socialize.us1.gigya.com/GS/GSLogin.aspx

https://socialize.gigya.com/GS/GSLogin.aspx

https://www.example.com

Type in the domain and press Enter to add it

3. Next, you will need to configure your Consent screen. You must input a valid email address and name your app as you would like it displayed to users. Then click **Continue**.



Credentials

Add credentials to your project

✓ Find out what kind of credentials you need
Calling People API from a web browser

✓ Create an OAuth 2.0 client ID
Created OAuth client 'Web client 1'

3 Set up the OAuth 2.0 consent screen

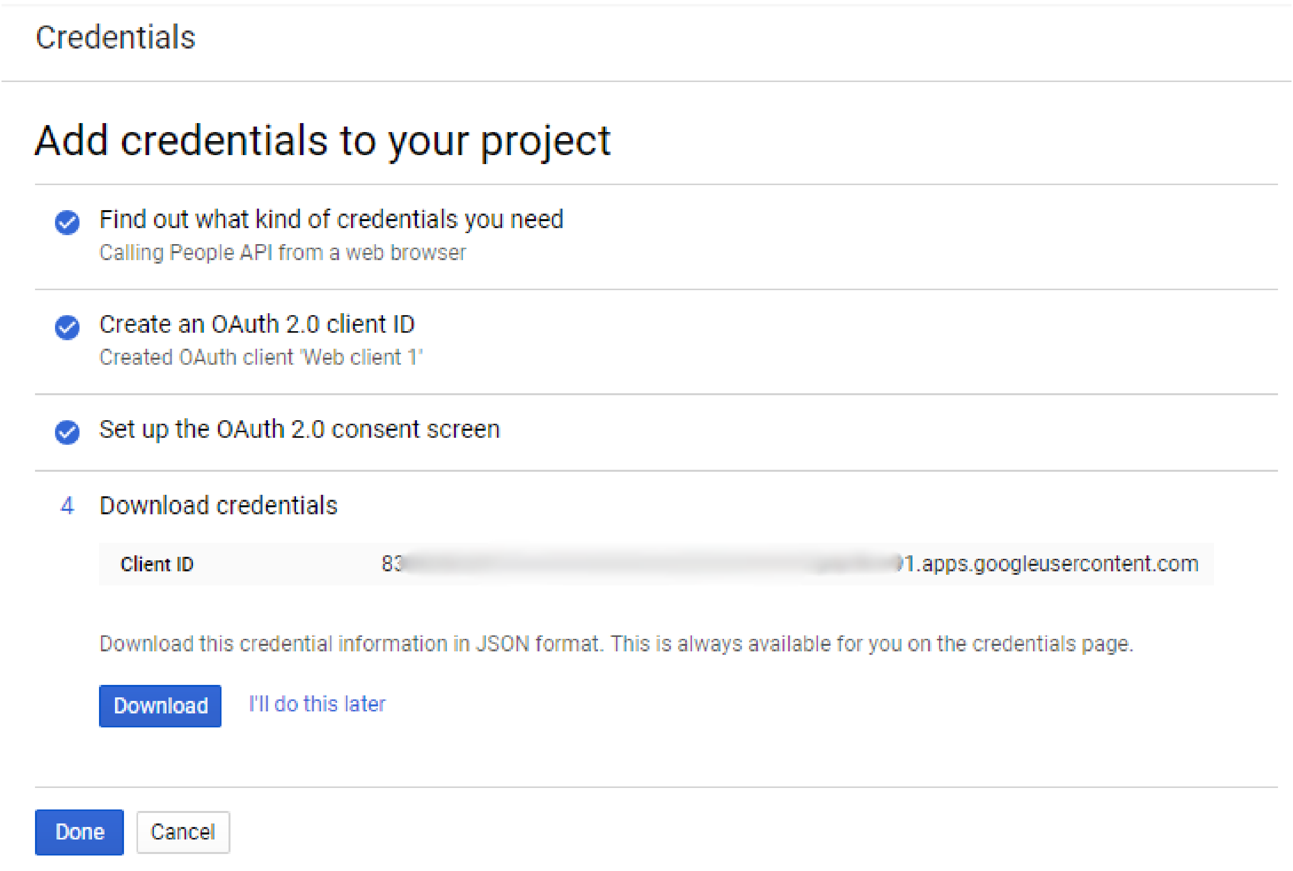
Email address ?
[redacted] ▾

Product name shown to users ?
Gigya Test Sign-in App

The consent screen will be shown to users whenever you request access to their private data using your client ID. It will be shown for all applications registered in this project.

You must provide an email address and product name for OAuth to work.

4. You will now be presented with your Client ID. You can download it as a JSON file or copy it, and then click **Done**.



Credentials

Add credentials to your project

✓ Find out what kind of credentials you need
Calling People API from a web browser

✓ Create an OAuth 2.0 client ID
Created OAuth client 'Web client 1'

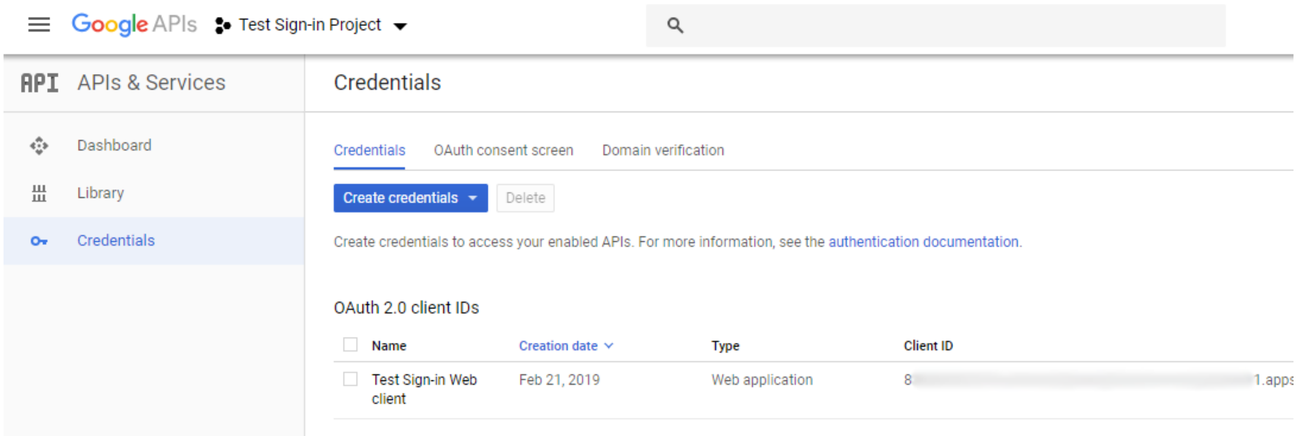
✓ Set up the OAuth 2.0 consent screen

4 Download credentials

Client ID	83[redacted]1.apps.googleusercontent.com

Download this credential information in JSON format. This is always available for you on the credentials page.

5. You will be taken back to the Credentials tab of your project. To view the it's configuration, click on the app name on the left.

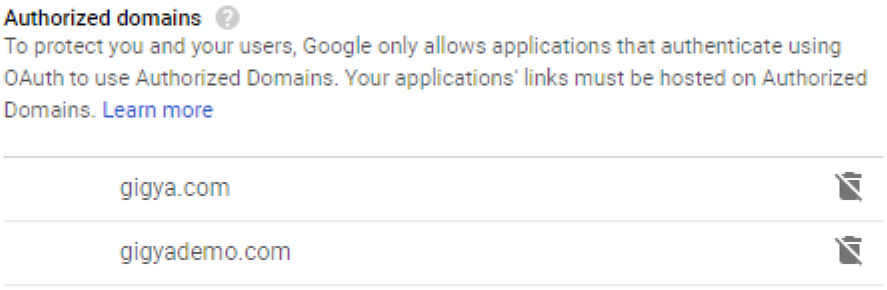


Create credentials to access your enabled APIs. For more information, see the authentication documentation.

OAuth 2.0 client IDs

□	Name	Creation date	Type	Client ID
□	Test Sign-in Web client	Feb 21, 2019	Web application	8[redacted]1.apps

6. Before you can add your Authorized JavaScript origins, you must add your site(s) to the Authorized domains by going to the **OAuth consent screen** section. Enter any domains that will be hosting the app.



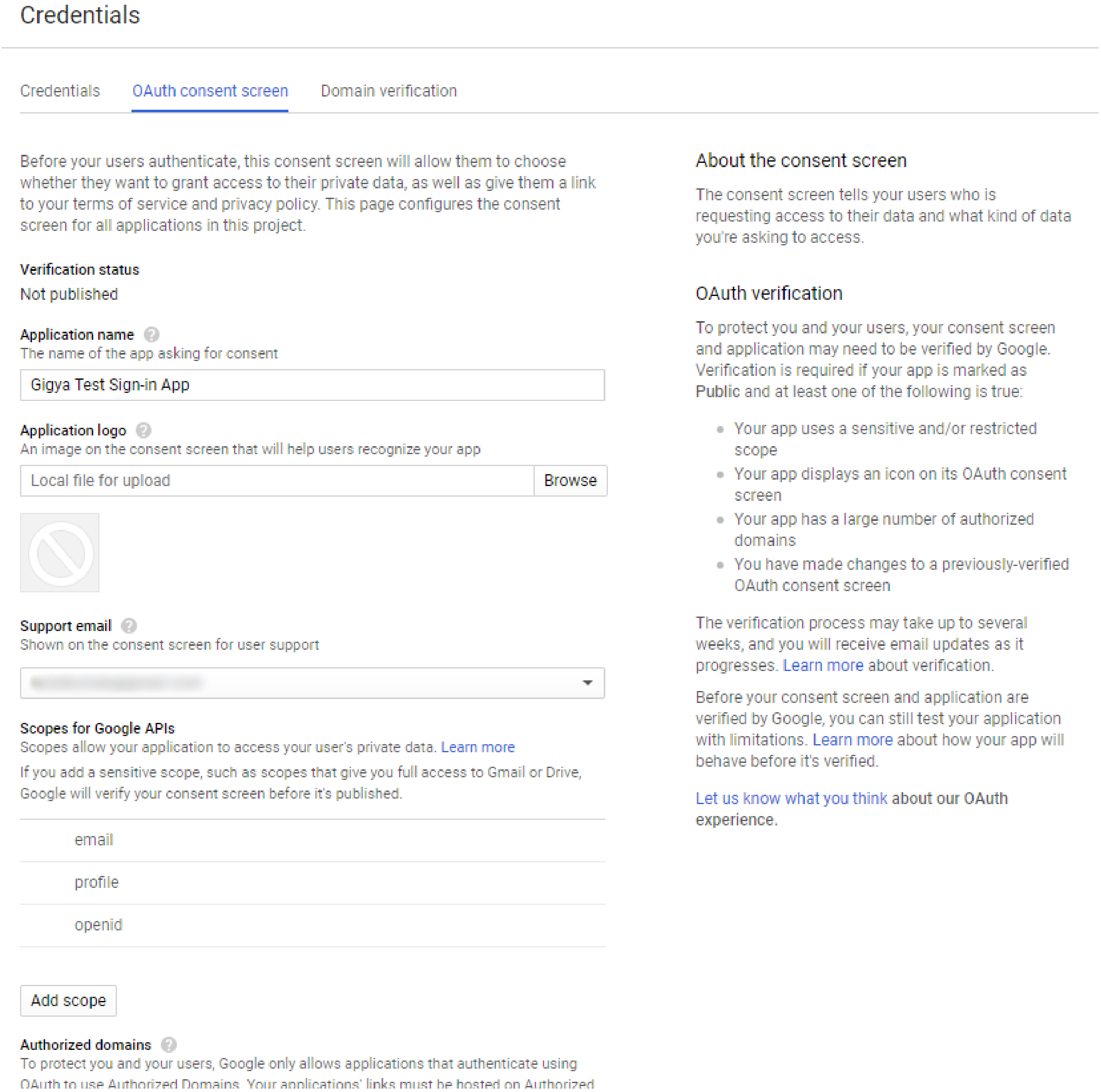
Authorized domains
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. Learn more

gigya.com

gigyademo.com

7. While still on the OAuth Consent screen page, enter all your links, i.e.:
   - Application Homepage link
   - Application Privacy Policy link
   - Application Terms of Service link

   On this tab you can also view the current permissions for your app in the **Scopes for Google APIs** section:



Credentials

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

Verification status
Not published

Application name
The name of the app asking for consent
Gigya Test Sign-in App

Application logo
An image on the consent screen that will help users recognize your app
Local file for upload

Support email
Shown on the consent screen for user support
[redacted]

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
openid

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

About the consent screen

The consent screen tells your users who is requesting access to their data and what kind of data you're asking to access.

OAuth verification

To protect you and your users, your consent screen and application may need to be verified by Google. Verification is required if your app is marked as Public and at least one of the following is true:

- Your app uses a sensitive and/or restricted 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

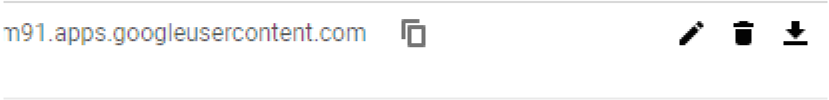
The verification process may take up to several weeks, and you will receive email updates as it progresses. Learn more about verification.

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.

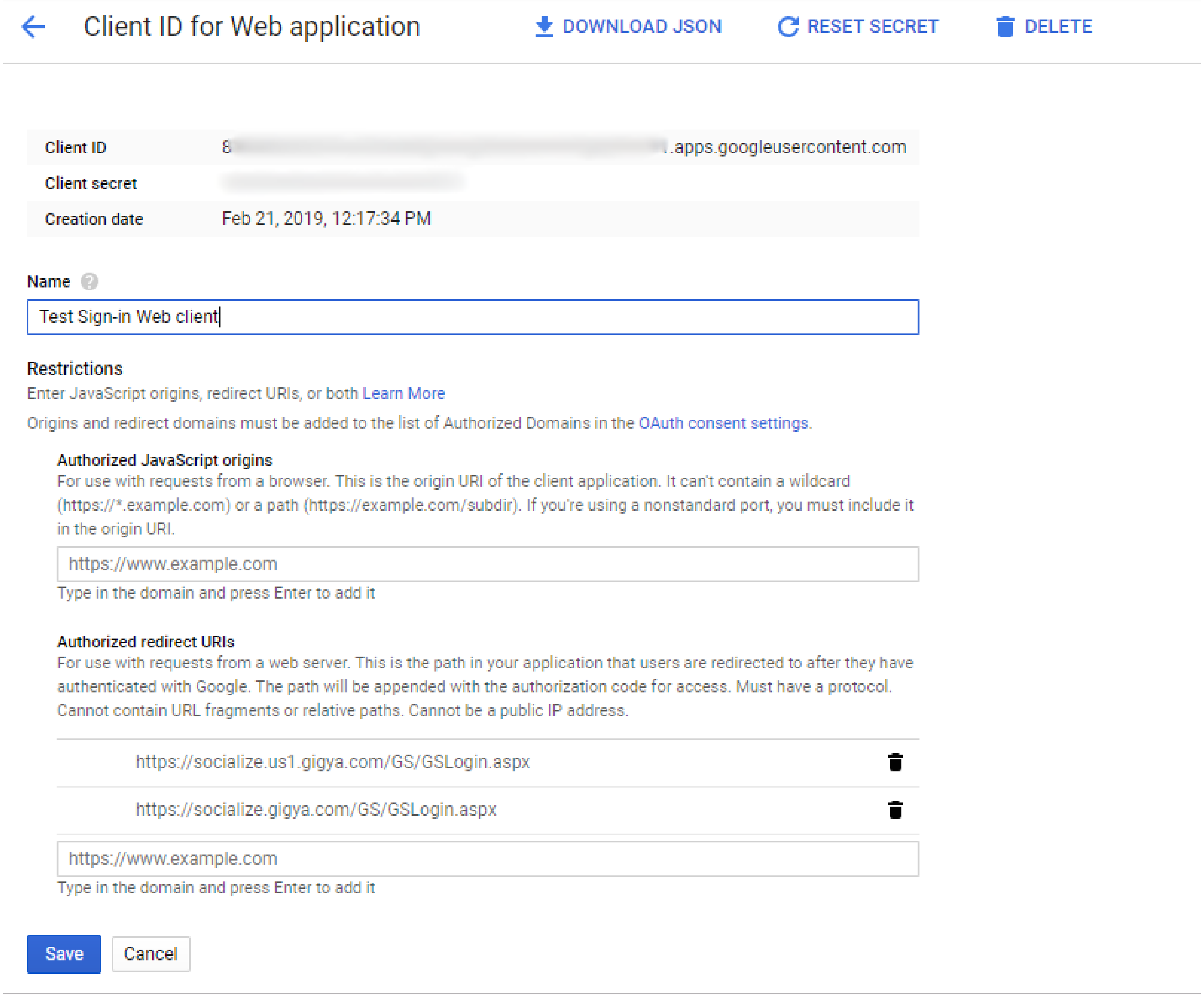
   When done, press **Save**.

8. The last thing still to do is to get your secret key. While on the Credentials page of your project, click the pencil icon to Edit the app.



ɱ91.apps.googleusercontent.com

Here you will be able to view or reset your secret key:



Client ID for Web application

Client ID	8[redacted].apps.googleusercontent.com
Client secret	[redacted]
Creation date	Feb 21, 2019, 12:17:34 PM

Name

Test Sign-in Web client

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.

https://socialize.us1.gigya.com/GS/GSLogin.aspx

https://socialize.gigya.com/GS/GSLogin.aspx

https://www.example.com

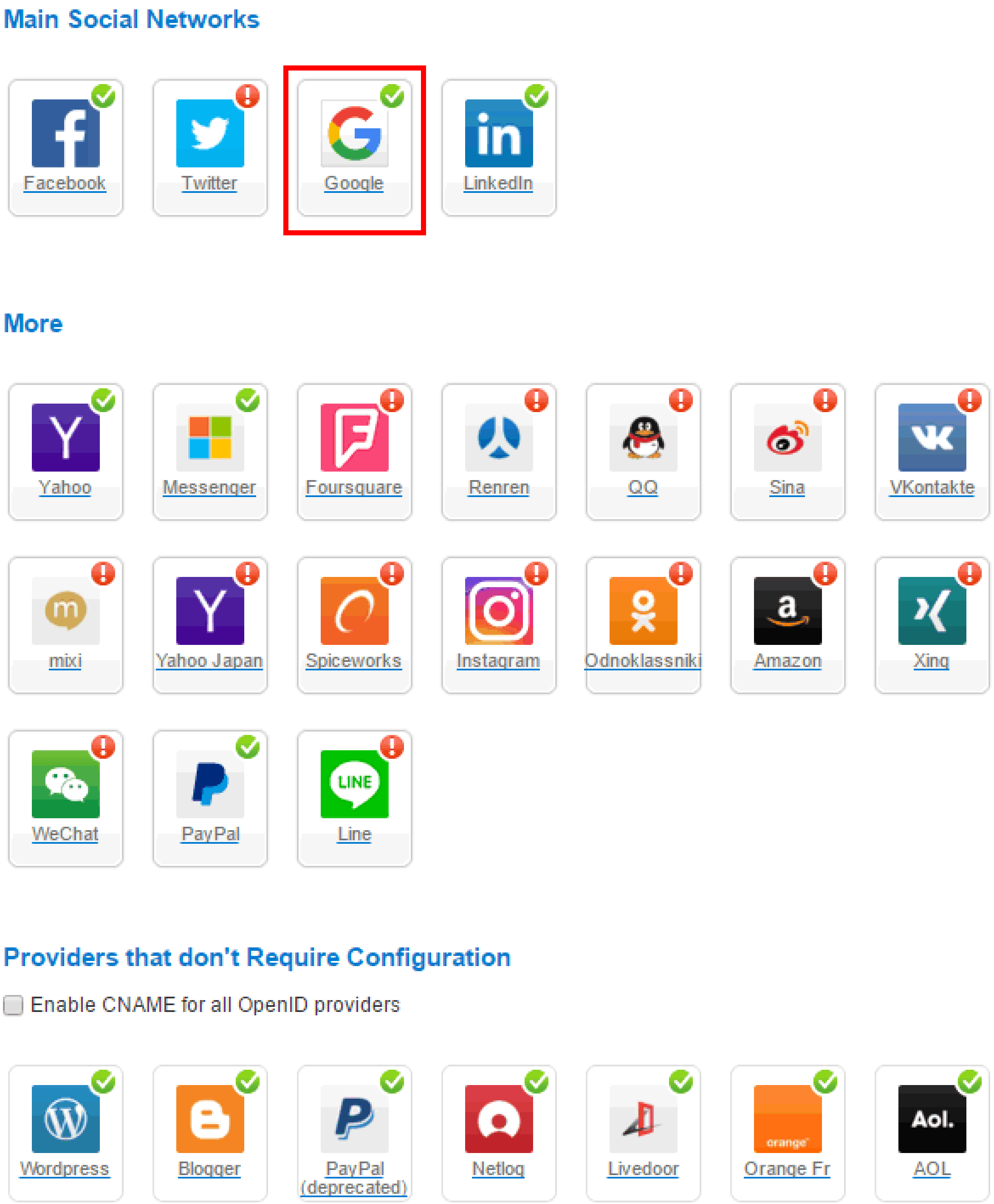
Type in the domain and press Enter to add it

9. That's it. Your app is now ready and you can proceed to Phase 2, below.

Phase 2 - Configuring Google Application Keys in Gigya's Website

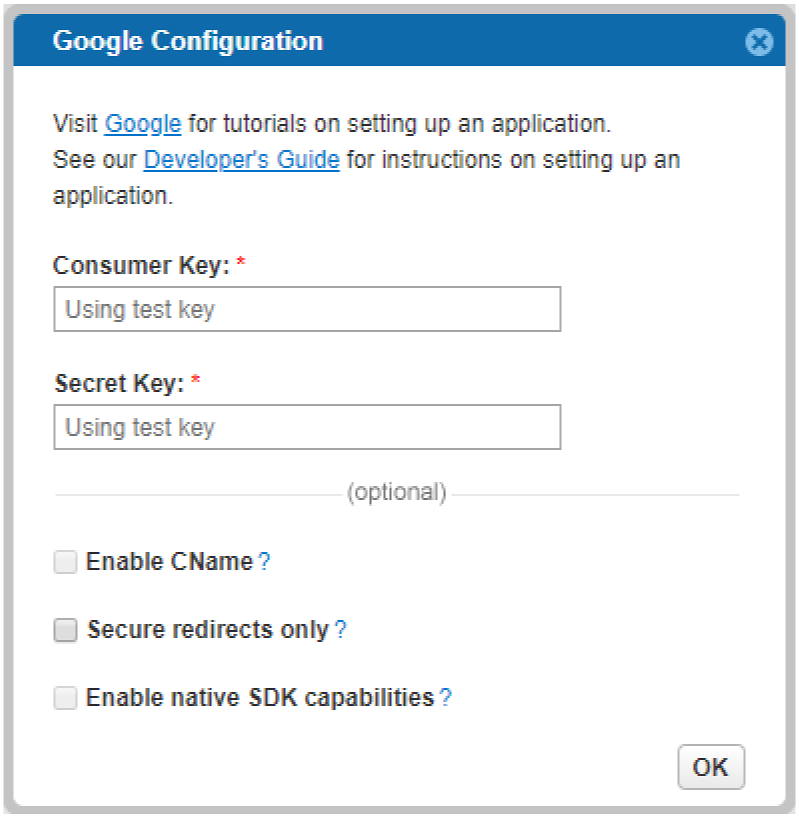
Setting your keys in the Google Configuration Editor

1. Log into your Gigya account and go to the Providers Configurations page of Gigya's Console.
2. Click on **Google** to open its configuration window.



☐ Enable CNAME for all OpenID providers

3. In the Google Configuration window enter:
   - Your "Client ID" from the Google Developers Dashboard into the "Consumer Key" field. (The entire string, including *.apps.googleusercontent.com*)
   - Your "Client Secret" into the "Secret Key" field.
   - If you are using a CNAME, be sure to select the "Enable CName" checkbox.
   - Select **Secure redirects only** to allow only HTTPS redirects from Google.
   - Selecting "Enable Native SDK Capabilities" is required to enable automatic login. For more information see Native SDK Capabilities.



Google Configuration

Visit Google for tutorials on setting up an application.
See our Developer's Guide for instructions on setting up an application.

Consumer Key: *

Using test key

Secret Key: *

Using test key

(optional)

□ Enable CName ?

□ Secure redirects only ?

□ Enable native SDK capabilities ?

OK

4. Click "OK".
5. Click "Save Settings" on the bottom right-hand corner.

That's it, Google configuration is complete! Please note that it might take up to 10 minutes for our system to become synchronized with Google.

Additional Information

App Verification

To ensure the best possible user experience when users engage your app, you will now need to get it verified by Google. The verification process can take between 3 and 7 business days and possibly longer, so should be started as soon as possible after creating and setting up your application. If you do not get your app verified, whenever users log in to your site using your Google App they will be presented with a warning screen stating **This app isn't verified** (it is important to note that the number of users able to use an unverified app via passing through the warning screen will be capped at an undisclosed number of users determined by Google. See https://developers.google.com/apps-script/guides/client-verification for more information).

The steps necessary to get your app verified are as follows:

- Your domain must be already verified in Google Webmaster Tools.
- Complete and submit the form located here.
  - The entire form must be completed. When defining the scopes your app requires, at a minimum you need to add all the scopes pertaining to:
    - https://www.googleapis.com/auth/plus.login
    - https://www.googleapis.com/auth/userinfo.email
    - https://www.google.com/m8/feeds - If you have checked the **Enable retrieving user contacts** from the Gigya Console Permissions page.
    - Any additional scopes your app will use beyond what Gigya natively supports listed above.
  - You must have a valid and public Privacy Policy on the domain the app resides defining exactly what data you are collecting and the purpose and use of the data.
- If at any time you change redirect URIs, home page URL, product name, or scopes, you will need to re-verify the app by submitting a new form with the changes.

For additional information, visit https://support.google.com/cloud/answer/7454865.

Unable to render {include} The included page could not be found.