

# Setting Up Google Auth for xela

These are the steps for your Google Auth setup

## Getting Started

Start at [https://developers.google.com/identity/sign-in/web/sign-in#before\\_you\\_begin](https://developers.google.com/identity/sign-in/web/sign-in#before_you_begin)

### Integrating Google Sign-In into your web app



Google Sign-In manages the OAuth 2.0 flow and token lifecycle, simplifying your integration with Google APIs. A user always has the option to [revoke access](#) to an application at any time.

This document describes how to complete a basic Google Sign-In integration.



#### Before you begin

Before you can integrate Google Sign-In into your website, you must create a client ID, which you need to call the sign-in API.

To create a Google API Console project and client ID, click the following button:

CONFIGURE A PROJECT



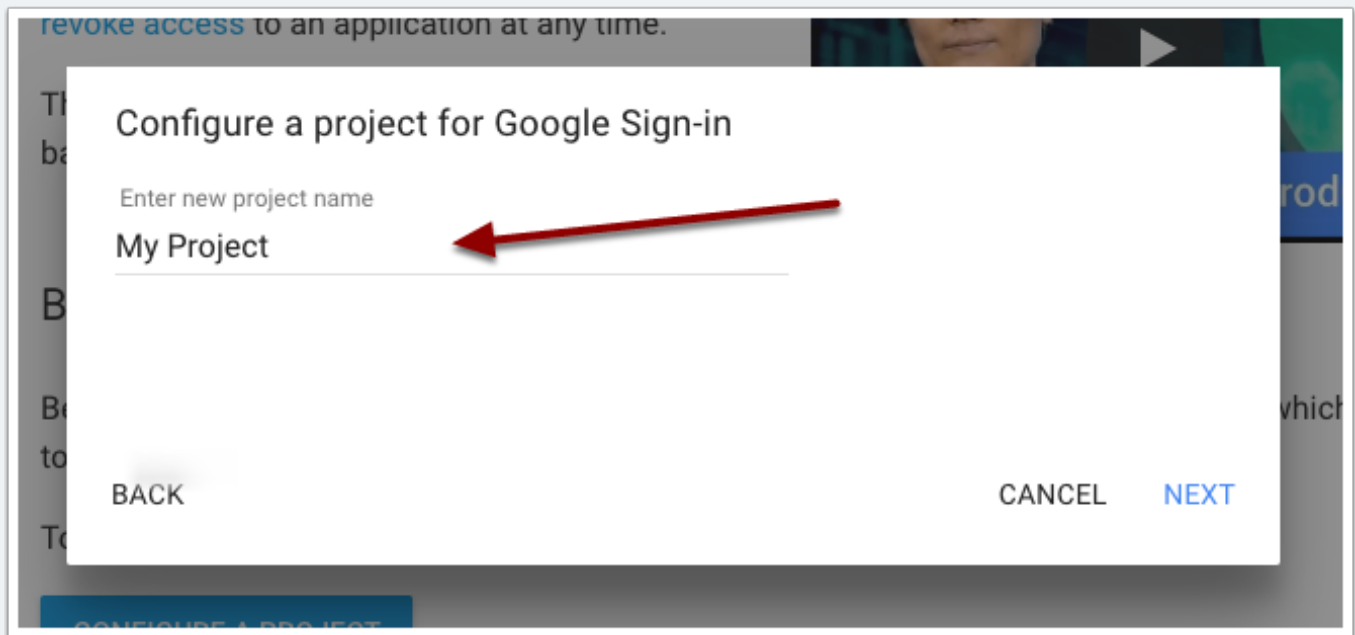
Configure a Project

When you configure the project, select the **Web browser** client type and specify the origin URI of your

# Setting Up Google Auth for xela

## Give it a name

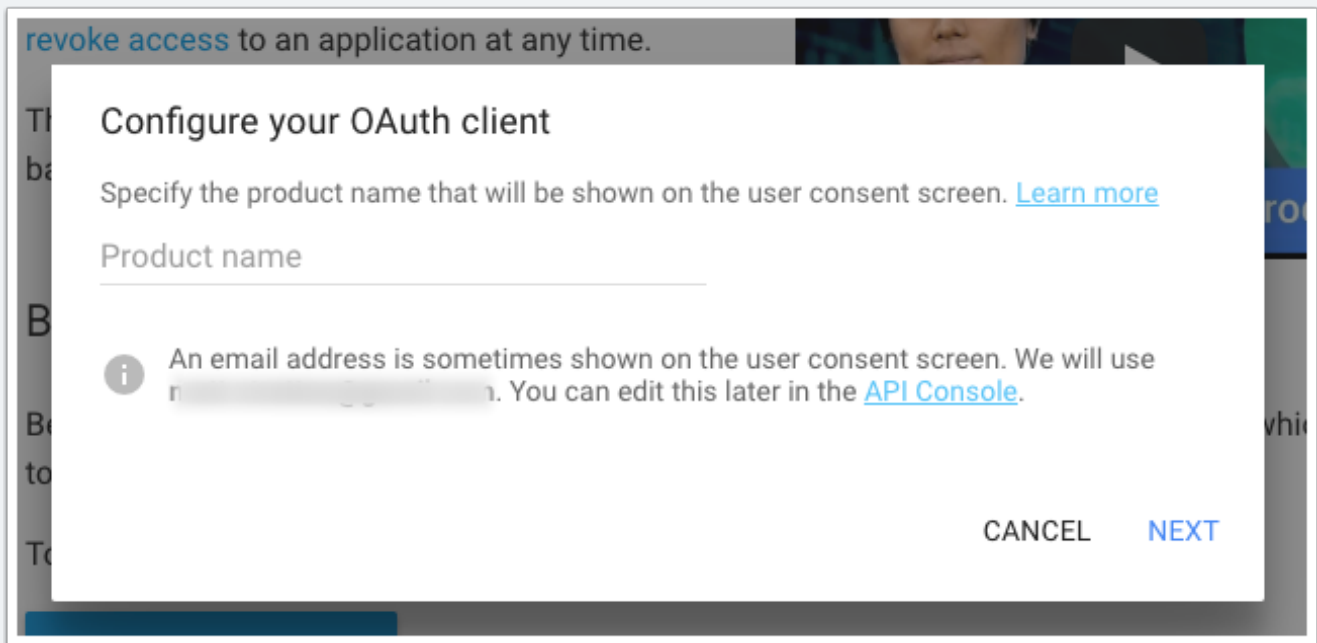
On the previous screen, make sure you selected "new project"



# Setting Up Google Auth for xela

## Name the application/product

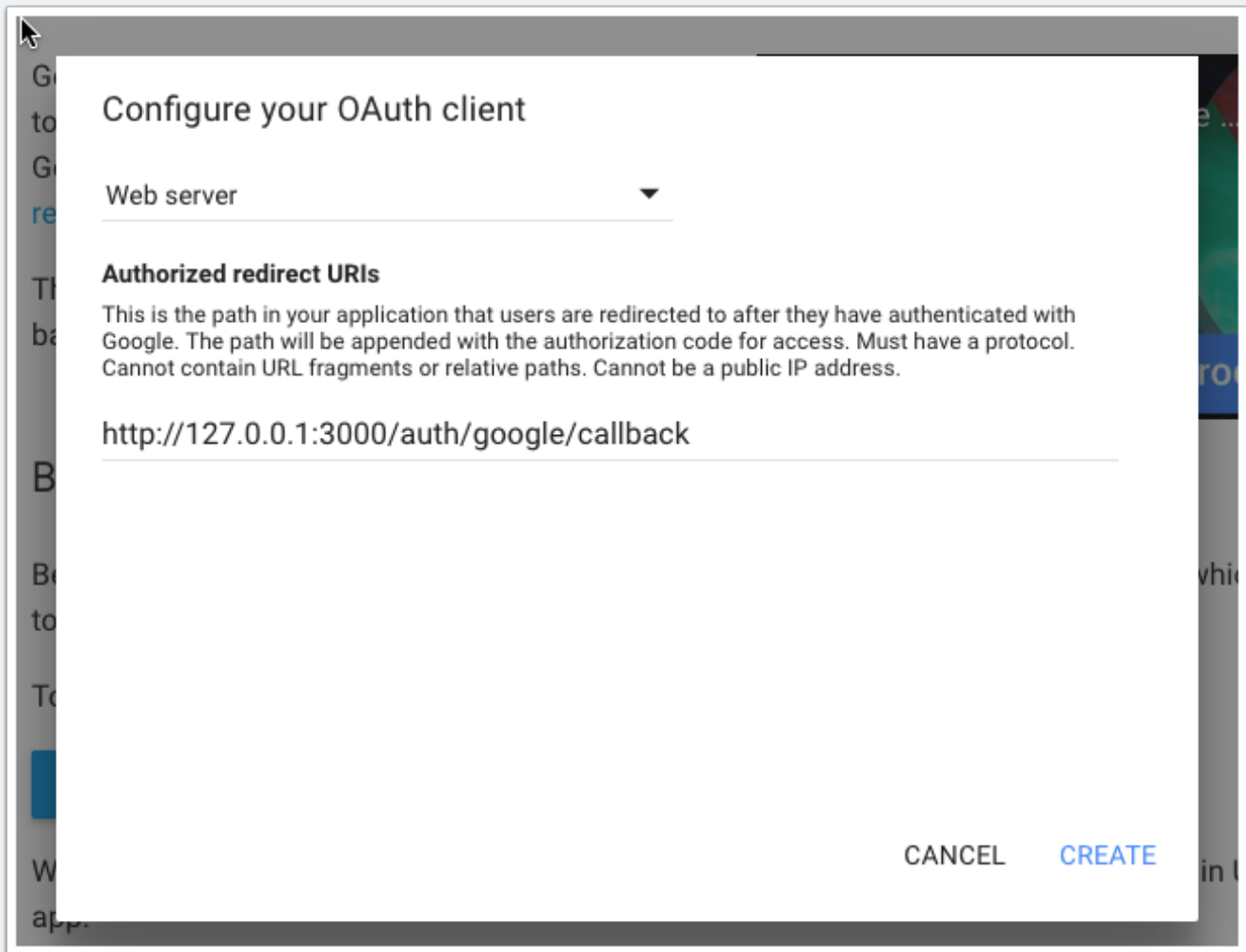
You can call this whatever you want, but I recommend "XELA"



# Setting Up Google Auth for xela

## Configure OAuth client

Choose "Web Server" and make sure that the redirect URL is exactly as specified



**Configure your OAuth client**

Web server ▼

**Authorized redirect URIs**

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.

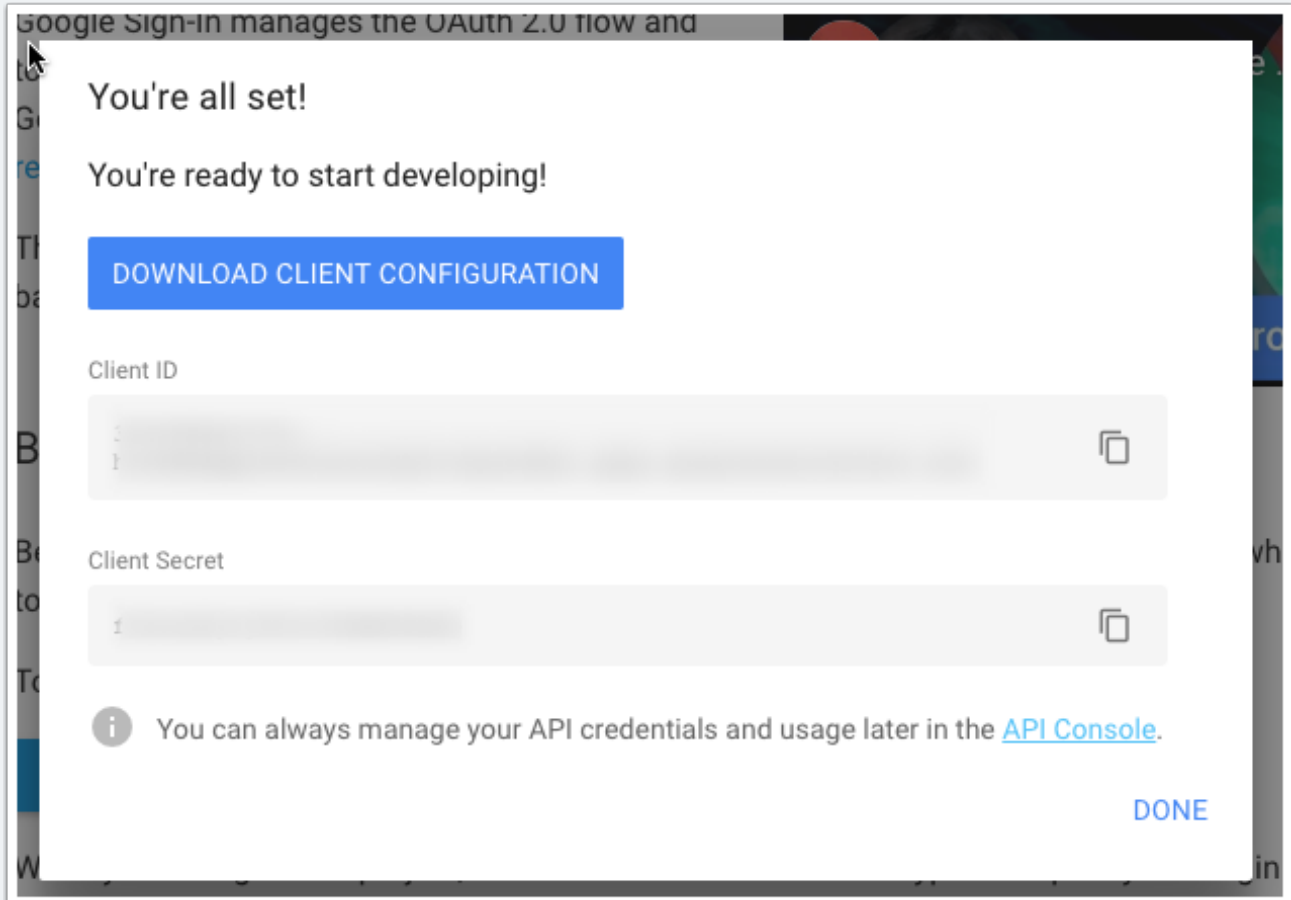
http://127.0.0.1:3000/auth/google/callback

CANCEL CREATE

# Setting Up Google Auth for xela

## Download or copy settings

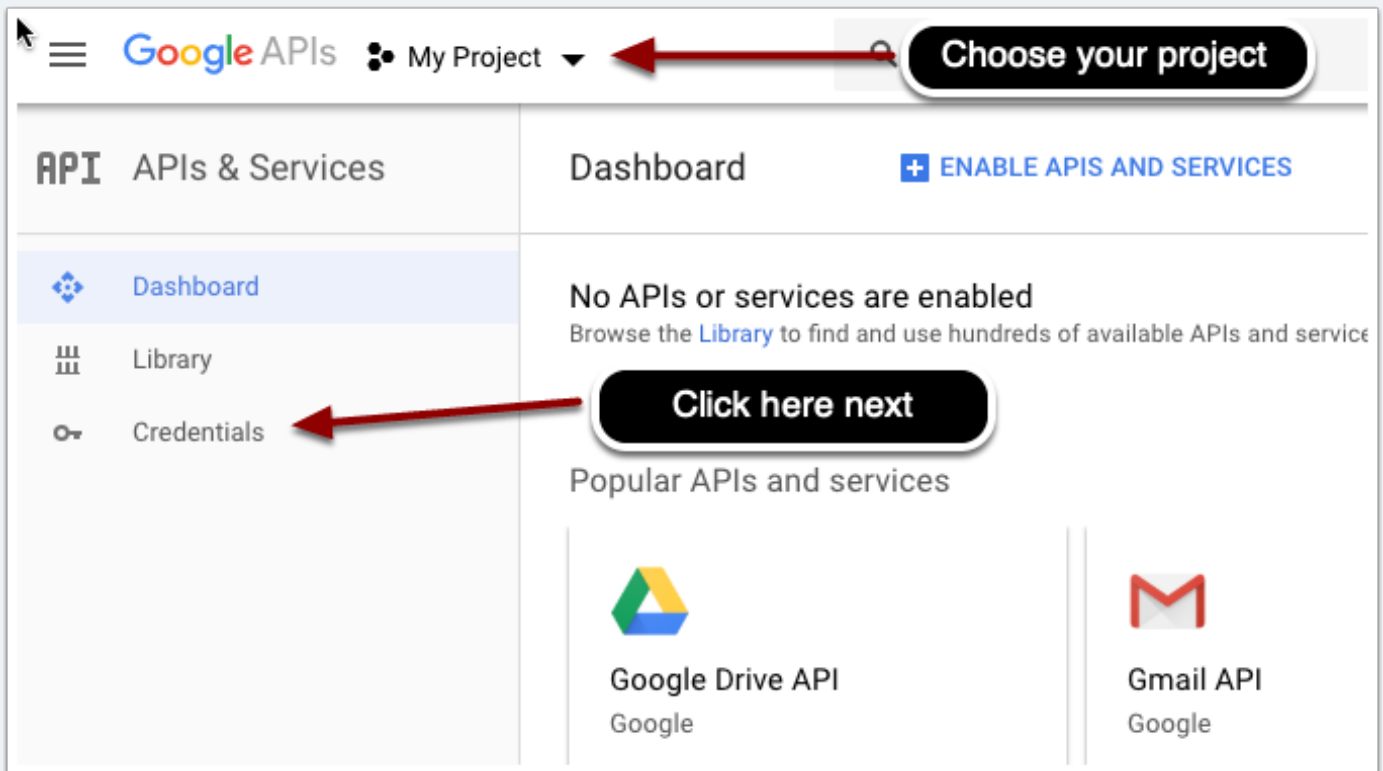
This is the only chance you get. You will need these settings later for your environment variables.



# Setting Up Google Auth for xela

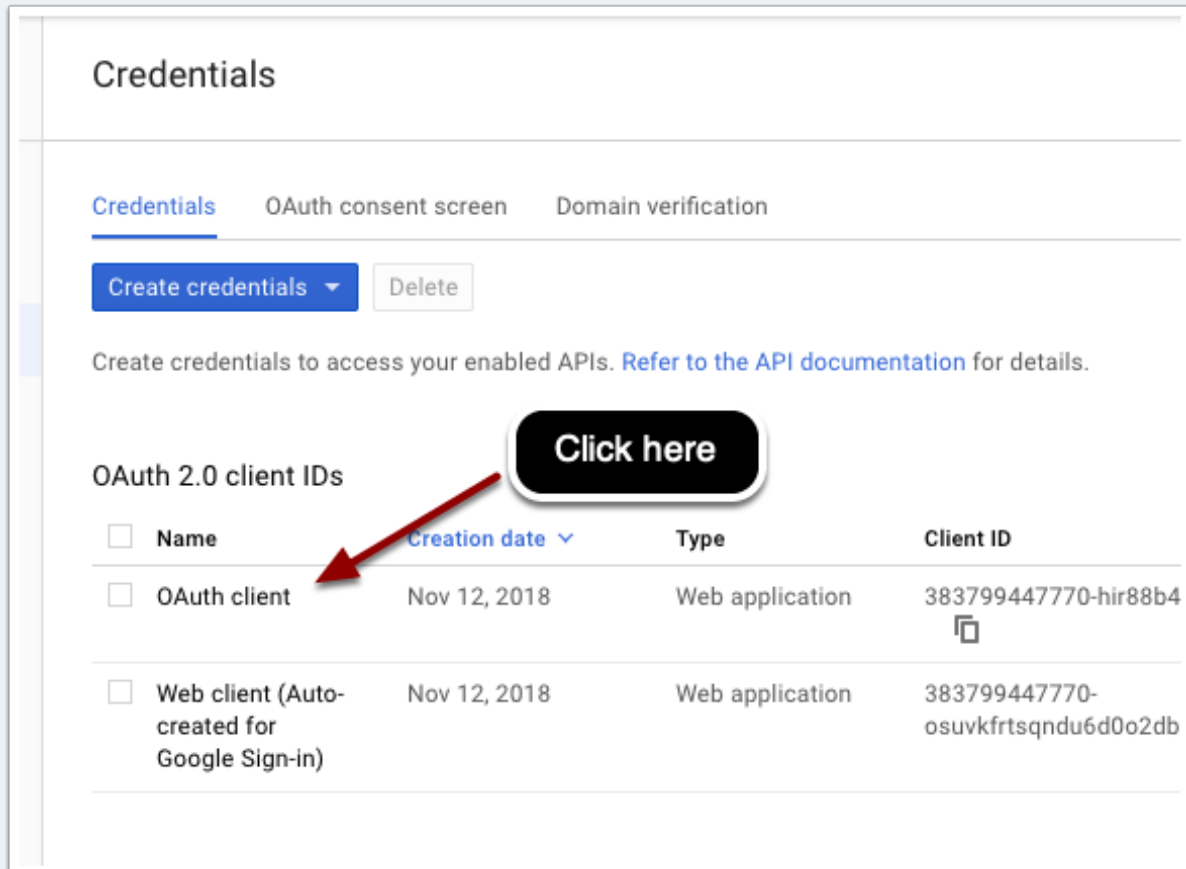
## Insert authorized domains

Visit <https://console.developers.google.com>



# Setting Up Google Auth for xela

## Configure OAuth Client




**Credentials**

[Credentials](#) [OAuth consent screen](#) [Domain verification](#)

[Create credentials](#) [Delete](#)

Create credentials to access your enabled APIs. [Refer to the API documentation](#) for details.

**OAuth 2.0 client IDs**

<input type="checkbox"/> Name	<a href="#">Creation date</a> ▼	Type	Client ID
<input type="checkbox"/> OAuth client	Nov 12, 2018	Web application	383799447770-hir88b4 
<input type="checkbox"/> Web client (Auto-created for Google Sign-in)	Nov 12, 2018	Web application	383799447770-osuvkfrtsqndu6d0o2db

# Setting Up Google Auth for xela


## Confirm localhost settings

Make sure your settings look like this exactly.

**Name** ?

**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.  



**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.  

