

[View Section](#)

[Setup & Installation](#)

[Getting Started](#) <

[React & React Native](#) <

[Angular & Ionic](#) <

[Vue](#) <

[Quickstart](#) <

[Usage](#) <

[GraphQL Transform](#) <

[Plugins & Extensions](#) <

[Analytics](#) <

[API](#) <

[Authentication](#) <

[Interactions](#) <

[Predictions](#) <

[PubSub](#) <

[Push Notifications](#) <

[Storage](#) <

[XR](#) <

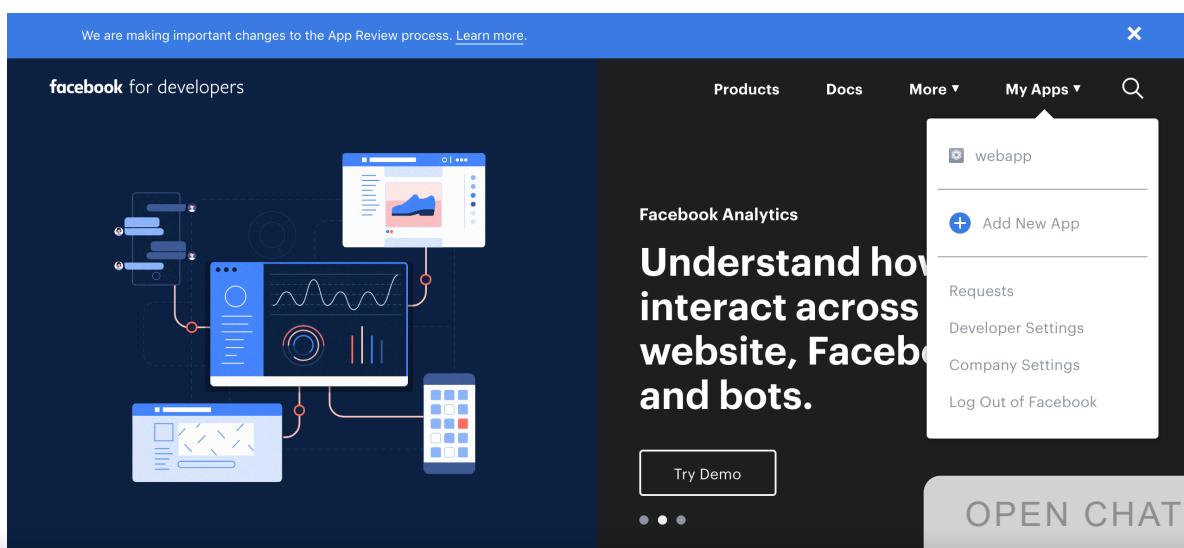
[OPEN CHAT](#)

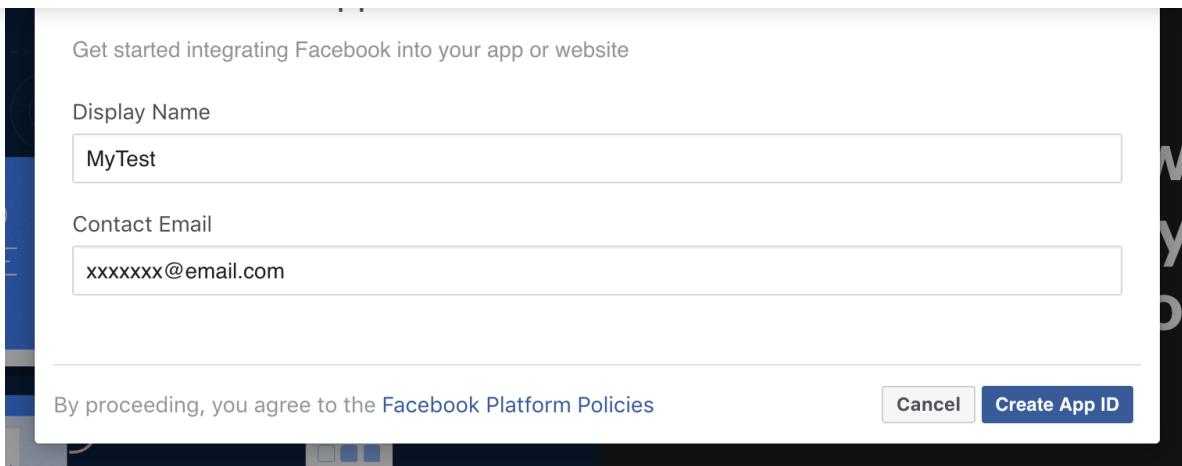
## Social Provider Setup

Before adding a social provider to an Amplify project, you must first create go to that provider and configure an application identifier as outlined below.

## Facebook Instructions

1. Create a [developer account with Facebook](#)
2. [Sign In](#) with your Facebook credentials.
3. From the *My Apps* menu, choose *Add New App*.



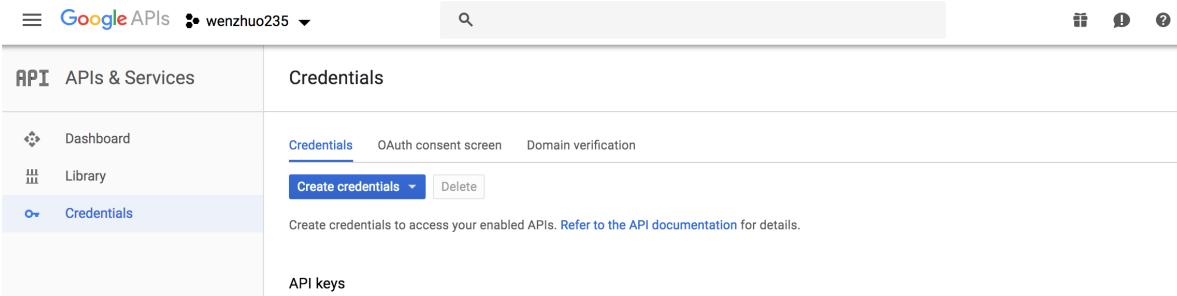


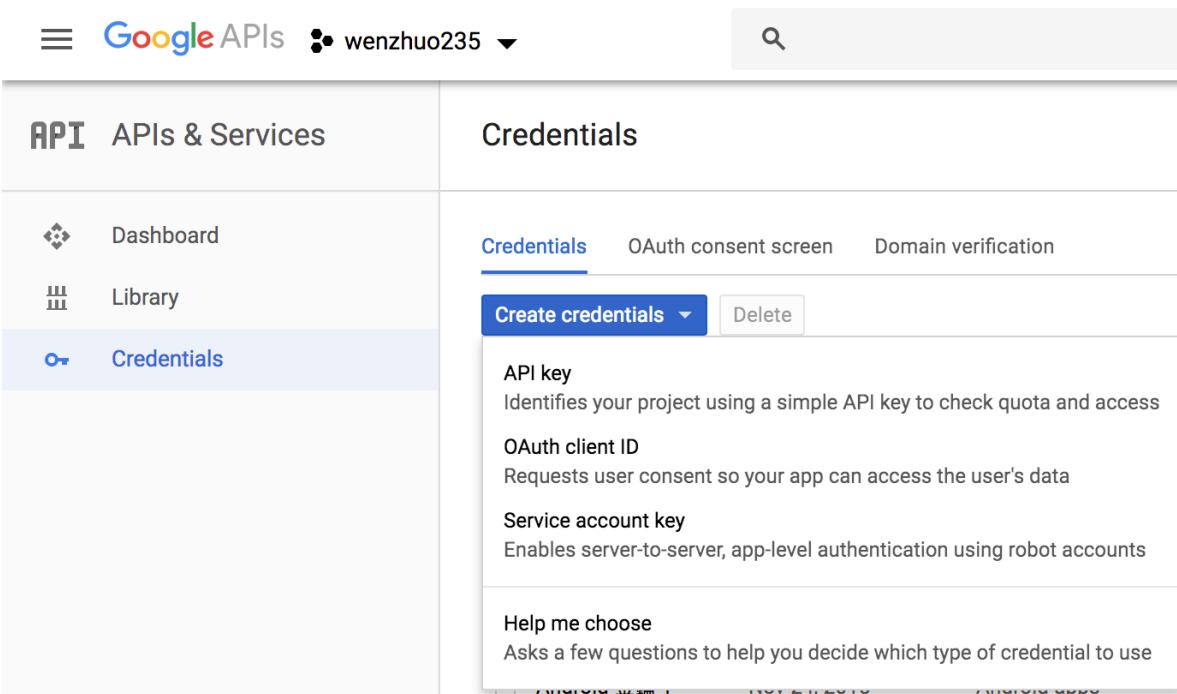
5. On the left navigation bar, choose *Settings* and then *Basic*.

A screenshot of the Facebook Developers dashboard for the app 'MyTest'. The left sidebar shows 'Dashboard', 'Settings' (with 'Basic' selected), 'Advanced', 'Roles', 'Alerts', and 'App Review'. Below this is a 'PRODUCTS' section with a plus sign. The main content area is titled 'Add a Product' and features a 'Account Kit' section with a blue circular icon containing a user profile and a plus sign. Text below it says 'Seamless account creation. No more passwords.' with 'Read Docs' and 'Set Up' buttons.

6. Note the *App ID* and the *App Secret*. You will use them in the next section in the CLI flow.

OPEN CHAT

1. Go to the [Google developer console](#).
  2. On the left navigation bar, choose *Credentials*.
- 
- The screenshot shows the Google Developer Console interface. The top navigation bar includes the Google APIs logo, a user dropdown (wenzhuo235), and a search bar. The left sidebar has sections for Dashboard, Library, and Credentials, with 'Credentials' currently selected. The main content area is titled 'Credentials' and contains tabs for 'Credentials', 'OAuth consent screen', and 'Domain verification'. A prominent blue button labeled 'Create credentials' with a dropdown arrow is centered. Below it, a note says 'Create credentials to access your enabled APIs. Refer to the API documentation for details.' At the bottom of the main area, there's a link to 'API keys'.
3. Create your OAuth2.0 credentials by choosing *OAuth client ID* from the *Create credentials* drop-down list.



4. Choose *Web application*.
5. Click *Create* twice.
6. Note the *OAuth client ID* and *client secret*. You will need them for the next section in the CLI flow.
7. Choose *OK*.

OPEN CHAT

1. Create a developer account with Amazon.
2. Sign in with your Amazon credentials.
3. You need to create an Amazon security profile to receive the Amazon client ID and client secret. Choose Create a Security Profile.

You haven't set up Login with Amazon yet. Start now.

Login with Amazon allows users to login to third party websites or apps ('clients') using their Amazon username and password. Clients may ask the user to share some personal information from their Amazon profile, including name, email address, and zip code.

Login with Amazon features are linked to the Security Profile you create for your websites and apps. To get started, click [Create a New Security Profile](#).

[Create a New Security Profile](#)

**Login with Amazon**  
Securely connect with apps and websites with millions of Amazon customers and personalize their experience.

4. Type in a Security Profile Name, a Security Profile Description, and a Consent Privacy Notice URL.

**Name your new Security Profile**

Choose a name for this security profile. You can create multiple security profiles. You will associate a security profile with one or more apps. Apps that use the same security profile can share some types of data (for example, a "My App - Free" and a "My App - HD" could share data). For a shared security profile, choose a name that applies to all the apps that will use it (for example, "My App profile"). [Learn More](#)

\* Indicates a required field

Security Profile Name *	<input type="text" value="mynewapp"/>
Security Profile Description *	<input type="text" value="Security profile for my new app"/>
Consent Privacy Notice URL *	<input type="text" value="https://mynewapp.com"/>
Consent Logo Image	<input type="file" value="UPLOAD IMAGE"/>

[Save](#) [Cancel](#)

5. Choose Save.

OPEN CHAT

The screenshot shows the AWS Amplify Console interface. At the top, there are navigation links: Home, Documentation, and Login with Amazon Console. Below these, a section titled "Login with Amazon" is displayed. It includes a note about enabling Login with Amazon for a Security Profile, a "Create a New Security Profile" button, and a success message: "Login with Amazon successfully enabled for Security Profile. Click ⚙ to manage Security Profile." A table titled "Login with Amazon Configurations" lists one entry: "mynewapp" under "Security Profile Name" and "OAuth2 Credentials" under "Show Client ID and Client Secret". There is also a "Manage" button with a gear icon.

# Finish Social Setup

After adding your Social provider information into the Amplify project setup, the domain that was created must be added into the Social provider configuration to complete the process.

## Facebook Instructions

1. [Sign In](#) with your Facebook credentials.
2. From the *My Apps* menu, choose *Your App*.

The screenshot shows the Facebook Developers website. At the top, there is a banner about changes to the App Review process. The main header includes "facebook for developers" and navigation links: Products, Docs, More ▾, My Apps ▾, and a search bar. A prominent graphic on the left illustrates various devices and data integration. On the right, there is a callout for "Facebook Analytics" with the text: "Understand how users interact across your website, Facebook and bots." Below this are buttons for "Try Demo" and "OPEN CHAT". The "My Apps" menu is open, showing a list with "webapp" selected, followed by "Add New App", "Requests", "Developer Settings", and "Company Settings". There is also a "Log Out of Facebook" option.

The screenshot shows the Facebook Business Manager interface. At the top left, there's a logo and the text "MyTest". To its right, the text "APP ID: 194071554866010" is displayed. On the left side, a sidebar menu is visible with the following items:

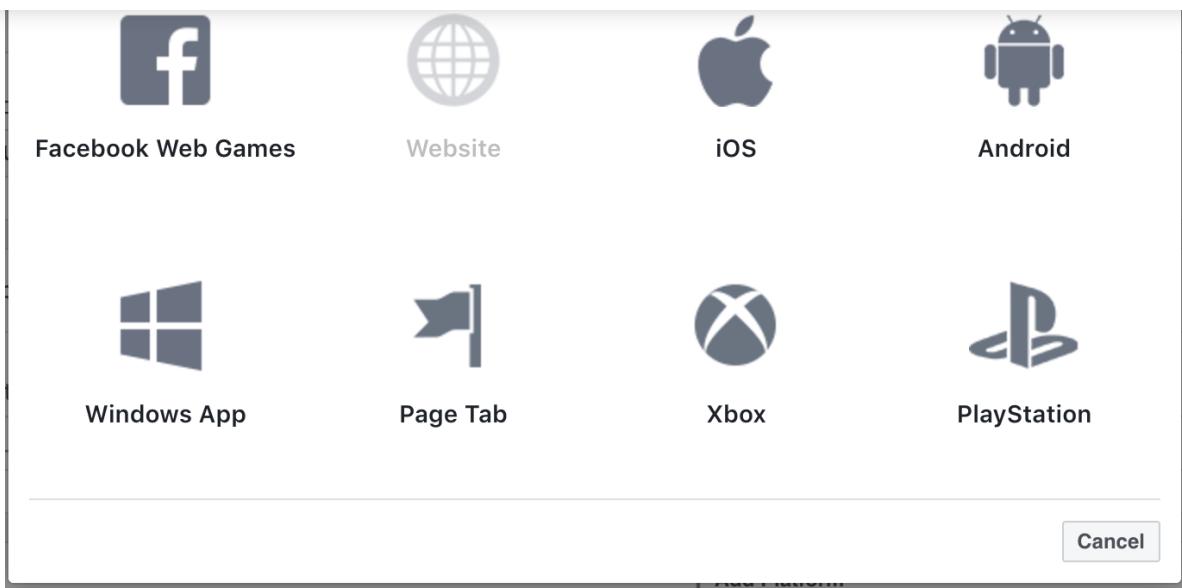
- Dashboard**
- Settings** (selected, indicated by a highlighted box)
  - Basic
  - Advanced
- Roles**
- Alerts**
- App Review**

Below the sidebar, the text "PRODUCTS" is followed by a blue circular button with a white plus sign.

The main content area has a light gray background. At the top, the text "Add a Product" is centered. Below it is a large rectangular box containing a teal circular icon with a white user profile symbol and a plus sign. To the right of the icon, the text "Account Kit" is displayed. Underneath, the text "Seamless account creation. No more passwords." is shown. At the bottom of this box are two buttons: "Read Docs" on the left and "Set Up" on the right.

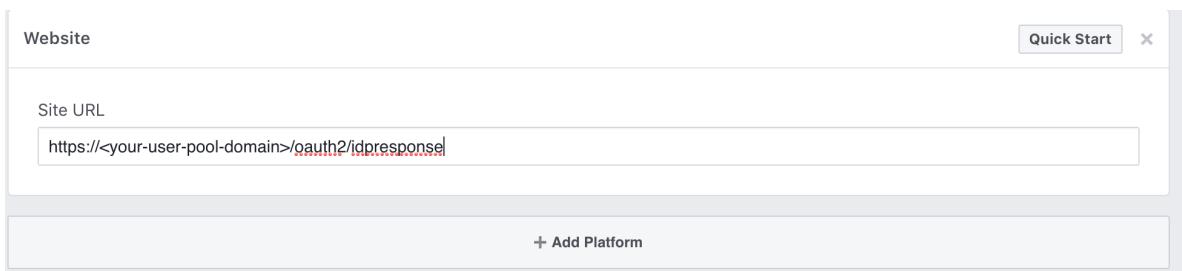
4. Choose *+ Add Platform* from the bottom of the page and then choose *Website*.

OPEN CHAT



5. Under Website, type your user pool domain with the /oauth2/idpresponse endpoint into *Site URL*

`https://<your-user-pool-domain>/oauth2/idpresponse`



6. Save changes.
7. Type your user pool domain into *App Domains*:

`https://<your-user-pool-domain>`

Display Name

MyTest

App Domains

<https://<your-user-pool-domain>> 

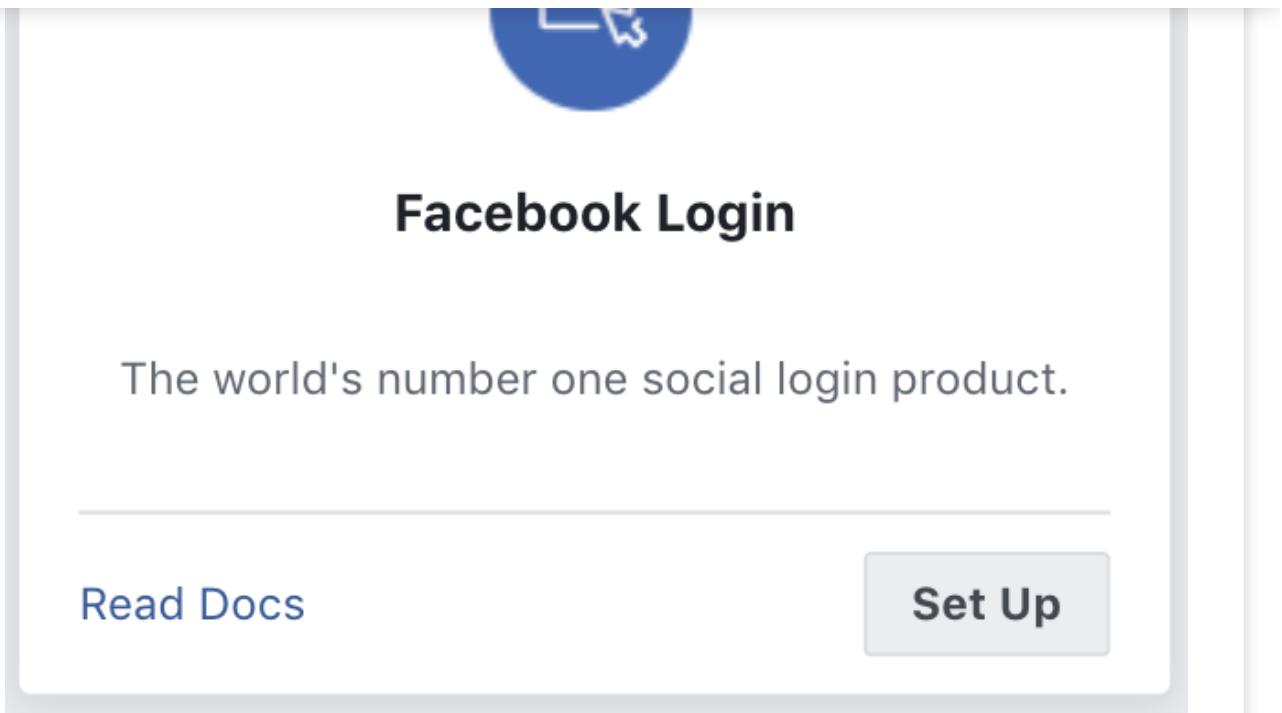
Privacy Policy URL

Privacy policy for Login dialog and App Details

App Icon (1024 x 1024)

8. Save changes.
9. From the navigation bar choose *Products* and then *Set up* from *Facebook Login*.

OPEN CHAT



10. From the navigation bar choose *Facebook Login* and then *Settings*.
11. Type your redirect URL into *Valid OAuth Redirect URIs*. It will consist of your user pool domain with the /oauth2/idpresponse endpoint.

**https://<your-user-pool-domain>/oauth2/idpresponse**

Client OAuth Settings

Client OAuth Login  
Enables the standard OAuth client token flow. Secure your application and prevent abuse by locking down which token redirect URLs are allowed with the options below. Disable globally if not used. [?]

Web OAuth Login  
Enables web-based Client OAuth Login. [?]

Enforce HTTPS  
Enforce the use of HTTPS for Redirect URLs and the JavaScript SDK. Strongly recommended. [?]

Force Web OAuth Reauthentication  
When on, prompts people to enter their Facebook password in order to log in on the web. [?]

Embedded Browser OAuth Login  
Enable webview Redirect URLs for Client OAuth Login. [?]

Use Strict Mode for Redirect URIs  
Only allow redirects that use the Facebook SDK or that exactly match the Valid OAuth Redirect URIs. Strongly recommended. [?]

Valid OAuth Redirect URIs  
https://<your-user-pool-domain>/oauth2/idpresponse

12. Save changes.

OPEN CHAT

1. Go to [Google Developer Console](#).

2. Click **CONFIGURE A PROJECT**

The screenshot shows the Google Sign-In for Websites documentation. The left sidebar has sections for Basics (Integrate Google Sign-In, Get Profile Information, Authenticate with a Backend Server), Additional Capabilities (Customize the Sign-In Button, Monitor the User's Session State, Request Additional Permissions, Integrate Sign-In Using Listeners, Google Sign-In for Server-Side Apps, Disconnect and Revoke Scopes), Cross-Platform Integration (Over-the-Air Android App Installation, Cross-Platform Single Sign-In), and Troubleshooting (Migrate from Google+ Sign-In). The main content area is titled "Integrating Google Sign-In into your web app". It includes a video thumbnail for "Google Sign-In: Introduction" and a "Before you begin" section. The right sidebar contains links to Contents, Before you begin, Load the Google Platform Library, Specify your app's client ID, Add a Google Sign-In button, Get profile information, and Sign out a user.

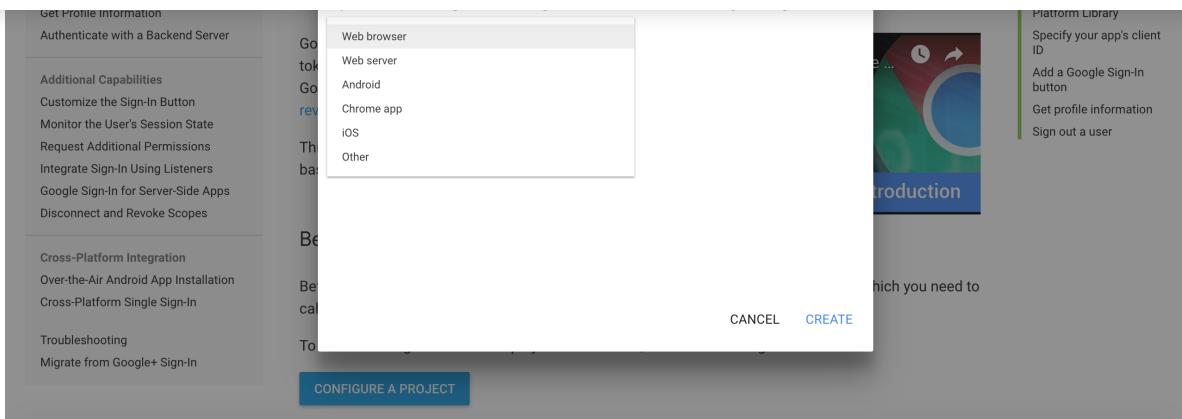
3. Type in a project name and choose **NEXT**.

The screenshot shows a modal dialog box titled "Configure a project for Google Sign-in". It has a text input field labeled "Enter new project name" containing the text "Test". At the bottom right of the dialog are "CANCEL" and "NEXT" buttons. The background of the page shows the same "Integrating Google Sign-In into your web app" guide as the previous screenshot.

4. Type in your product name and choose **NEXT**.

5. Choose *Web browser* from the *Where are you calling from?* drop-down list.

OPEN CHAT



6. Click ***CREATE***. You will NOT use the *Client ID* and *Client Secret* from this step.

7. Click Done.

8. Go to the [Google developer console](#).

9. On the left navigation bar, choose *Credentials*.

10. Select the client you created in the first step and choose the edit option

11. Type your user pool domain into Authorized Javascript origins.

12. Type your user pool domain with the `/oauth2/idpresponse` endpoint into *Authorized Redirect URLs*.

Web application

Android [Learn more](#)

Chrome App [Learn more](#)

iOS [Learn more](#)

Other

Name [?](#)  
Web client 2

**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.

Invalid Redirect: must end with a public top-level domain (such as .com or .org).  
Invalid Redirect: domain must be added to the authorized domains list before submitting.

**Note:** If you saw an error message **Invalid Redirect: domain must be added to the authorized domains list before submitting.** when adding the endpoint, please go to the *authorized domains list* and add the domain.

13. Click Save.

## Amazon Login Instructions

1. [Sign in](#) with your Amazon credentials.
2. Hover over the gear and choose Web Settings associated with the security profile you created in the previous step, and then choose

OPEN CHAT

Login with Amazon allows users to login to registered third party websites or apps (clients) using their Amazon user name and password. Clients may ask the user to share some personal information from their Amazon profile, including name, email address, and zip code. To get started, select an existing Security Profile or create a new Security Profile. [Learn More](#)

Create a New Security Profile

✓ Login with Amazon successfully enabled for Security Profile. Click ⚙ to manage Security Profile.

Login with Amazon Configurations

Security Profile Name	OAuth2 Credentials	Manage
mynewapp	Show Client ID and Client Secret	<ul style="list-style-type: none"><li>Security Profile</li><li>Web Settings</li><li>Kindle/Android Settings</li><li>iOS Settings</li><li>TVs and Other Devices Settings</li></ul>

3. Type your user pool domain into Allowed Origins and type your user pool domain with the /oauth2/idresponse endpoint into Allowed Return URLs.

amazondeveloper

Dashboard Apps & Services Alexa Login with Amazon Dash Services Reporting Settings

My Account Company Profile Payment Information Tax Identity User Permissions Mobile Ads Identity Security Profiles

KG ?

### Security Profile Management

#### mynewapp - Security Profile

General Web Settings Android/Kindle Settings iOS Settings TVs and Other Devices Settings

To use Login with Amazon with a website, you must specify either an allowed JavaScript origin (for the Implicit grant) or an allowed return URL (for the Authorization Code grant). [Learn More](#)

**Client ID**

**Client Secret**

**Allowed Origins** [?](#) https://<your-user-pool-domain>  
Add Another

**Allowed Return URLs** [?](#) https://<your-user-pool-domain>/oauth2/idresponse  
Add Another

Save Cancel

4. Choose Save.

OPEN CHAT

AWS Amplify is supported by Amazon Web Services

© 2018-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.



[OPEN CHAT](#)