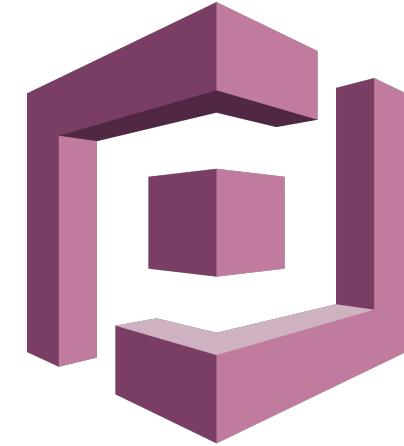


Cognito Primer

Cheng-Hao Ho

What?



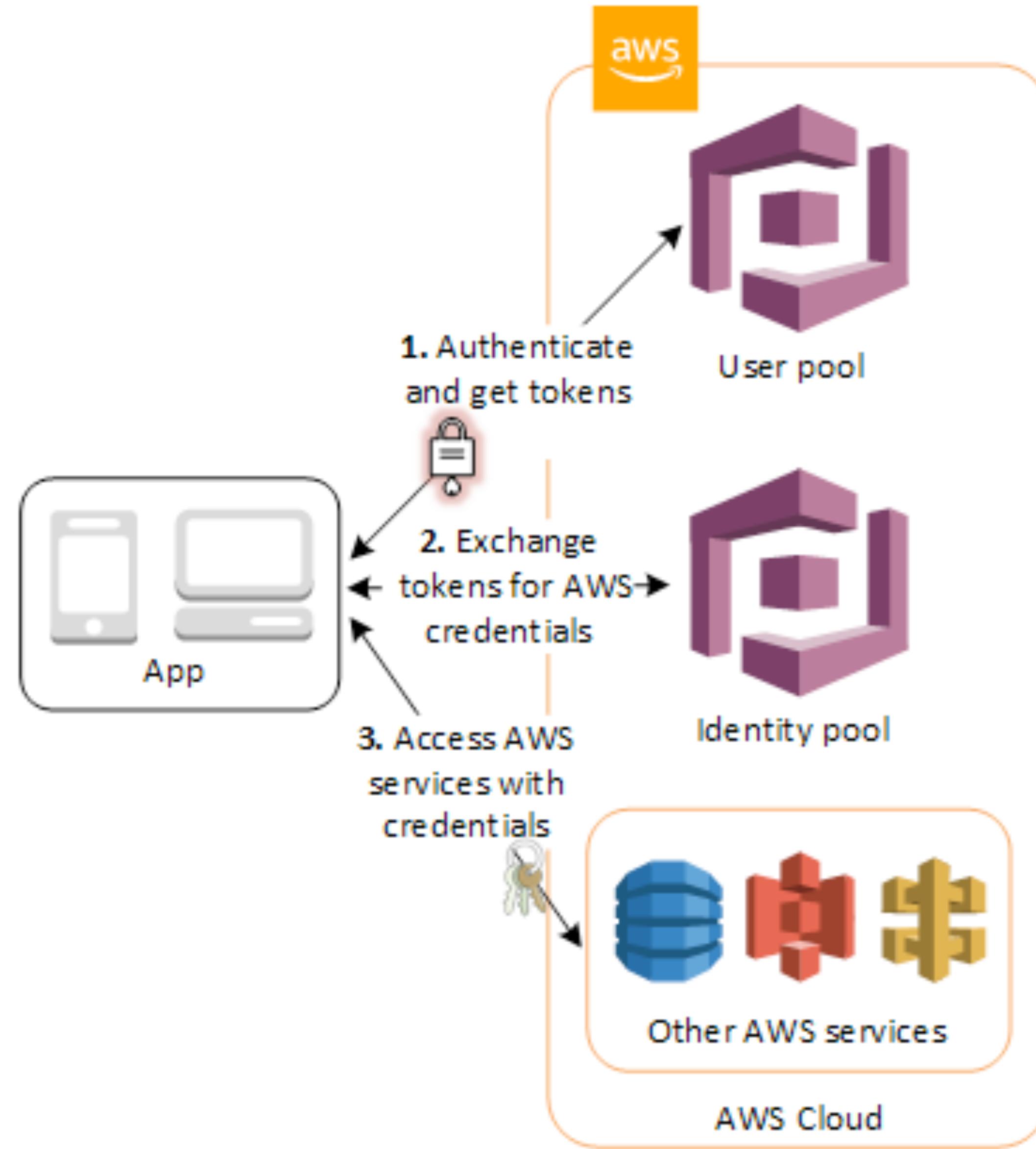
Authentication, Authorization, and User Management



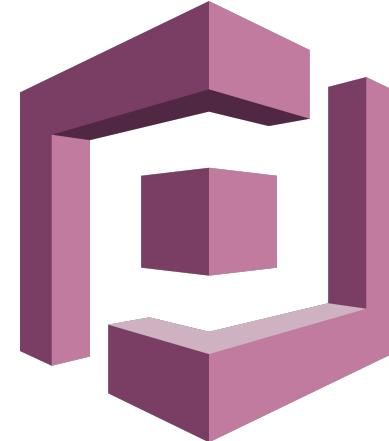
Add Sign-up and Sign-in



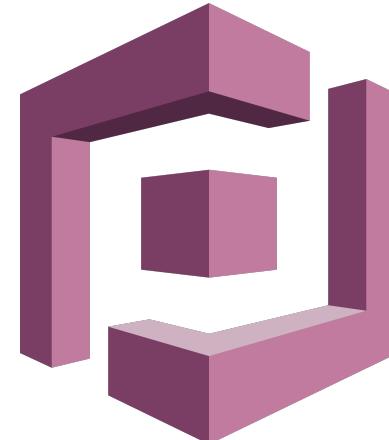
Grant your users access to AWS services



Components



User Pools: a user directory in Amazon Cognito;
With a user pool, users can sign in to your application



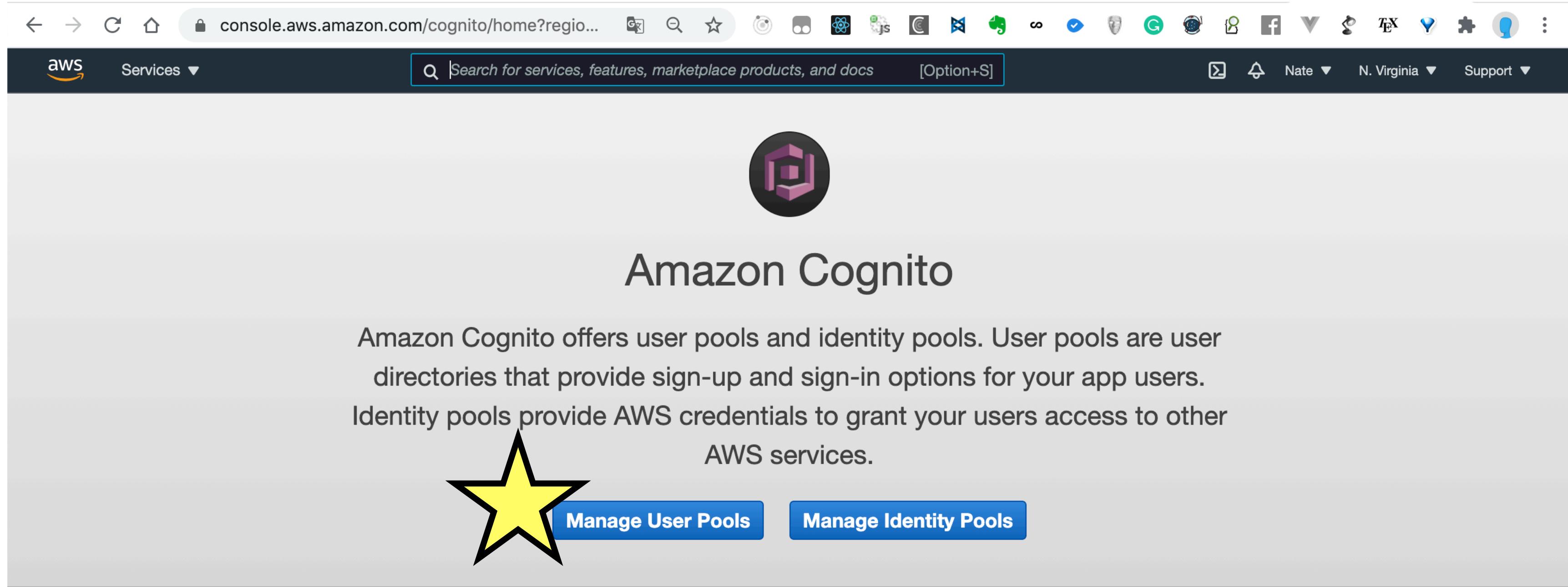
Identity Pools: With an identity pool, your users can obtain temporary AWS credentials to access AWS services

Sign in with Cognito

Username
/
Password

Third Party:
Facebook,
Google,
...

Create User pool



The screenshot shows the Amazon Cognito landing page. At the top, there's a navigation bar with icons for back, forward, search, and other AWS services. The URL is console.aws.amazon.com/cognito/home?region=. Below the navigation is a search bar with placeholder text "Search for services, features, marketplace products, and docs [Option+S]" and a dropdown menu for "Services". On the right of the search bar are links for "Nate", "N. Virginia", and "Support". The main header "Amazon Cognito" is centered above a purple hexagonal logo. A descriptive text block explains that Cognito offers user pools and identity pools for sign-up and sign-in options and AWS access. Below this are two blue buttons: "Manage User Pools" and "Manage Identity Pools", with a yellow star icon to the left of the first button.



Add Sign-up and Sign-in

With Cognito User Pools, you can easily and securely add sign-up and sign-in functionality to your mobile and web apps with a fully managed service that scales to support hundreds of



Grant your users access to AWS services

With Cognito Identity Pools, your app can get temporary credentials to access AWS services for anonymous guest users or for users who have signed in

Create User pool

← → ⌂ ⌂ console.aws.amazon.com/cognito/users/?region=N. Virginia Services ▾ Search for services, features, marketplace products, and docs [Option+S] ⌂ ⌂ Nate ▾ N. Virginia ▾ Support ▾

User Pools | Federated Identities

Create a user pool

Name

Attributes

Policies

MFA and verifications

Message customizations

Tags

Devices

App clients

Triggers

Review

Pool name

What do you want to name your user pool?

Give your user pool a descriptive name so you can easily identify it in the future.

Login

How do you want to create your user pool?

Review defaults

Start by reviewing the defaults and then customize as desired

Step through settings

Step through each setting to make your choices

Feedback English (US) ▾ © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Create Api Client

The screenshot shows the AWS Cognito User Pools configuration interface. The top navigation bar includes the AWS logo, a search bar, and various service icons. The main content area is titled "Review" and contains several configuration sections:

- Custom attributes**: Choose custom attributes...
- Minimum password length**: 8
- Password policy**: uppercase letters, lowercase letters, special characters, numbers
- User sign ups allowed?**: Users can sign themselves up
- FROM email address**: Default
- Email Delivery through Amazon SES**: Yes
- MFA**: Enable MFA...
- Verifications**: Email
- Tags**: Choose tags for your user pool
- App clients**: Add app client... (highlighted with a yellow star)
- Triggers**: Add triggers...

A blue "Create pool" button is located at the bottom right of the review section.

Create Api Client

The screenshot shows the AWS Cognito User Pools interface. The left sidebar has a navigation menu with several sections: General settings (Users and groups, Attributes, Policies, MFA and verifications, Advanced security, Message customizations, Tags, Devices, App clients, Triggers, Analytics), App integration (App client settings, Domain name, UI customization, Resource servers), and Federation (Identity providers, Attribute mapping). The 'App clients' item is highlighted with a yellow star. The main content area is titled 'Which app clients will have access to this user pool?' and contains a sub-instruction: 'The app clients that you add below will be given a unique ID and an optional secret key to access this user pool.' A large yellow star is overlaid on the 'Add an app client' button.

console.aws.amazon.com/cognito/users/?region=us-east-1

aws Services ▾

User Pools | Federated Identities

Login

General settings

- Users and groups
- Attributes
- Policies
- MFA and verifications
- Advanced security
- Message customizations
- Tags
- Devices
- App clients**
- Triggers
- Analytics

Add an app client

Which app clients will have access to this user pool?

The app clients that you add below will be given a unique ID and an optional secret key to access this user pool.

Return to pool details

Create Api Client

The screenshot shows the AWS User Pools 'Login' configuration page. The 'App clients' tab is selected. A yellow star highlights the 'App client name' field, which contains 'Login'. Below it, 'Refresh token expiration' is set to '30 days and 0 minutes'. Under 'Access token expiration', it says 'Must be between 60 minutes and 3650 days'. In the 'Security configuration' section, 'Enabled (Recommended)' is selected. A yellow star highlights the 'Create app client' button. At the bottom right, there is a 'Return to pool details' link.

aws Services ▾

User Pools | Federated Identities

Search for services, features, marketplace products, and docs [Option+S]

Logout Bell Nate ▾ N. Virginia ▾ Support ▾

Login

General settings

Users and groups

Attributes

Policies

MFA and verifications

Advanced security

Message customizations

Tags

Devices

App clients

Triggers

Analytics

App integration

Which app clients will have access to this user pool?

The app clients that you add below will be given a unique ID and an optional secret key to access this user pool.

App client name

Refresh token expiration
30 days and 0 minutes
Must be between 60 minutes and 3650 days

Access token expiration

Security configuration

Prevent User Existence Errors [Learn more.](#)

Legacy

Enabled (Recommended)

[Set attribute read and write permissions](#)

[Cancel](#) [Create app client](#)

[Return to pool details](#)

Create Api Client

The screenshot shows the AWS User Pools 'Create a user pool' interface. The 'App clients' tab is selected, highlighted with an orange background and a yellow star icon. The left sidebar lists other tabs: Name, Attributes, Policies, MFA and verifications, Message customizations, Tags, Devices, App clients (selected), Triggers, and Review. The main content area is titled 'Which app clients will have access to this user pool?' and contains a sub-section for 'Login'. A note states: 'The app clients that you add below will be given a unique ID and an optional secret key to access this user pool.' Below this is a list of clients, with 'Login' being the only one shown. An 'Add an app client' button is at the bottom of the list. A 'Return to pool details' link is also present. The top navigation bar includes the AWS logo, a search bar, and various account and support links.

aws Services ▾

Search for services, features, marketplace products, and docs [Option+S]

User Pools | Federated Identities

Create a user pool

Name

Attributes

Policies

MFA and verifications

Message customizations

Tags

Devices

App clients

Triggers

Review

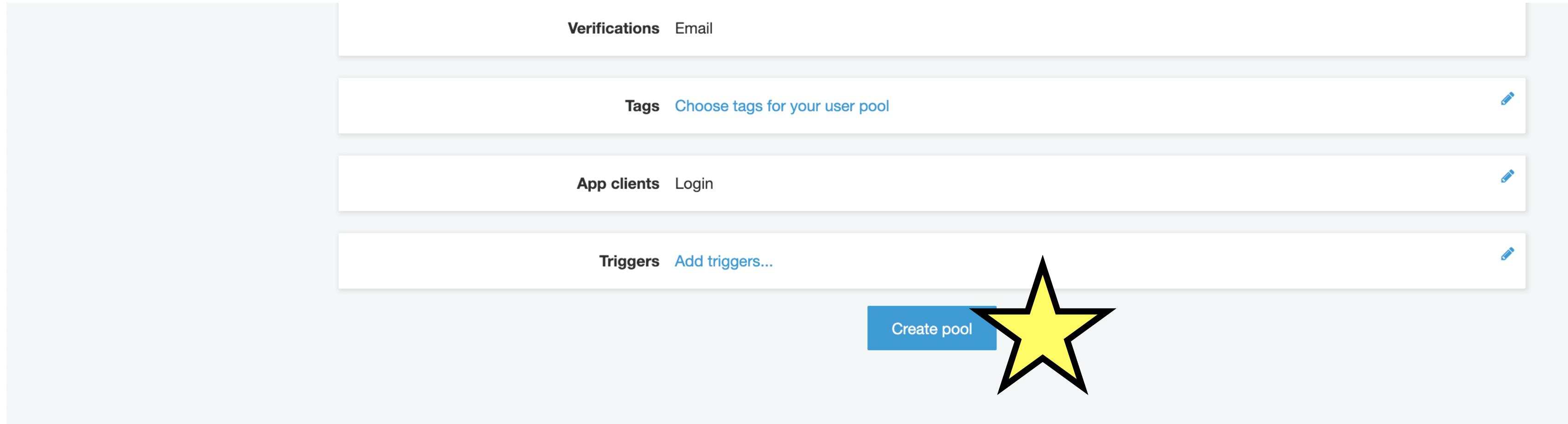
Login

The app client id and secret will be available after you save this user pool.

Add an app client

Return to pool details

Create Api Client



Get Cognito Domain

The screenshot shows the AWS Cognito User Pools 'Login' configuration page. On the left, there's a sidebar with various settings like General settings, App integration (with 'Domain name' highlighted), and Federation. The main area is titled 'What domain would you like to use?' and contains fields for 'Domain prefix' (with 'https://mylogin123' entered) and a 'Check availability' button. Below this, there's a section for 'Your own domain' with a note about needing an ACM certificate and a 'Use your domain' button. At the bottom right are 'Cancel' and 'Save changes' buttons.

console.aws.amazon.com/cognito/users/?regio...

aws Services ▾ [Option+S]

User Pools | Federated Identities

Login

General settings

- Users and groups
- Attributes
- Policies
- MFA and verifications
- Advanced security
- Message customizations
- Tags
- Devices
- App clients
- Triggers
- Analytics

App integration

- App client settings
- Domain name
- UI customization
- Resource servers

Federation

- Identity providers
- Attribute mapping

Amazon Cognito domain
Prefixed domain names can only contain lower-case letters, numbers, and hyphens. [Learn more about domain prefixes.](#)

Domain prefix

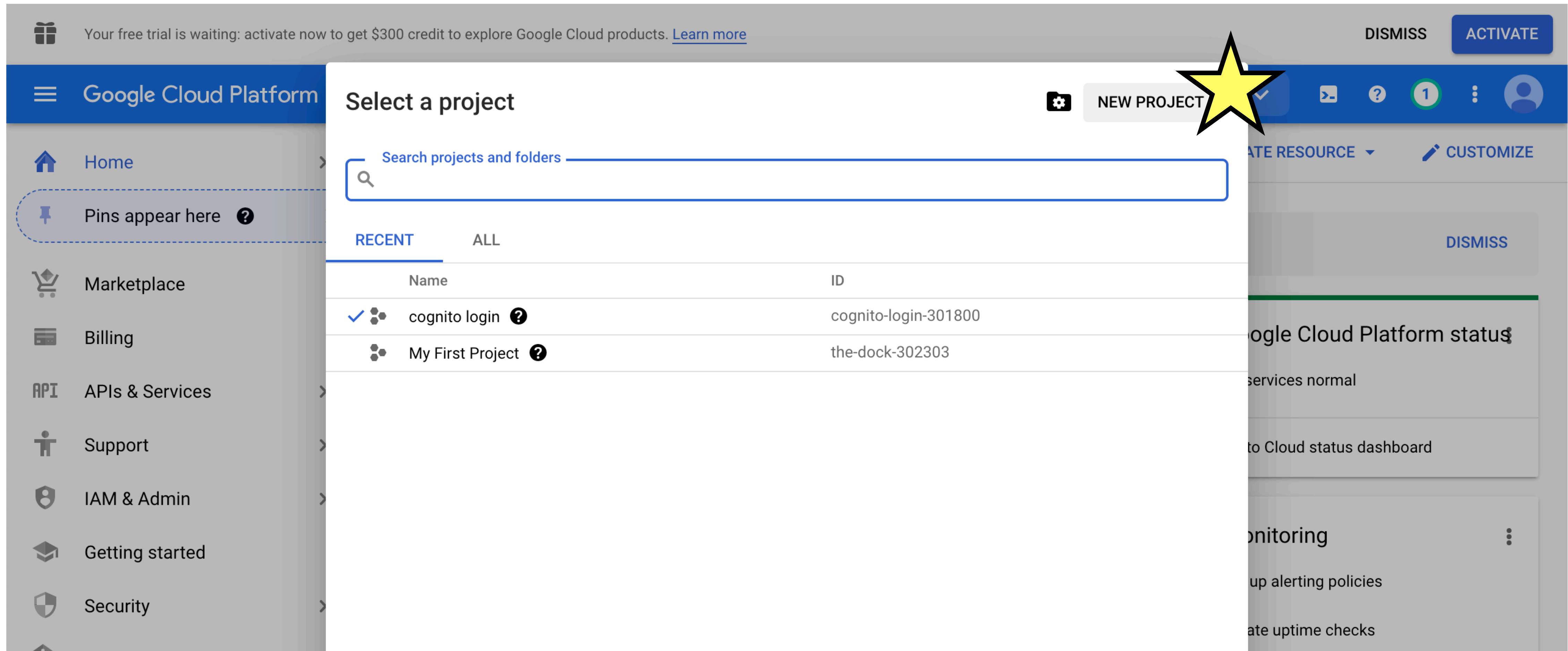
.auth.us-east-1.amazoncognito.com [Check availability](#)

Your own domain
This domain name needs to have an associated certificate in [AWS Certificate Manager \(ACM\)](#). You also need the ability to add an alias record to the domain's hosted zone after it's associated with this user pool. [Learn more about using your own domain.](#)

[Use your domain](#)

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

Create Google Project



Your free trial is waiting: activate now to get \$300 credit to explore Google Cloud products. [Learn more](#)

DISMISS ACTIVATE

Google Cloud Platform

Home

Pins appear here ?

Marketplace

Billing

APIs & Services

Support

IAM & Admin

Getting started

Security

Select a project

NEW PROJECT

RECENT ALL

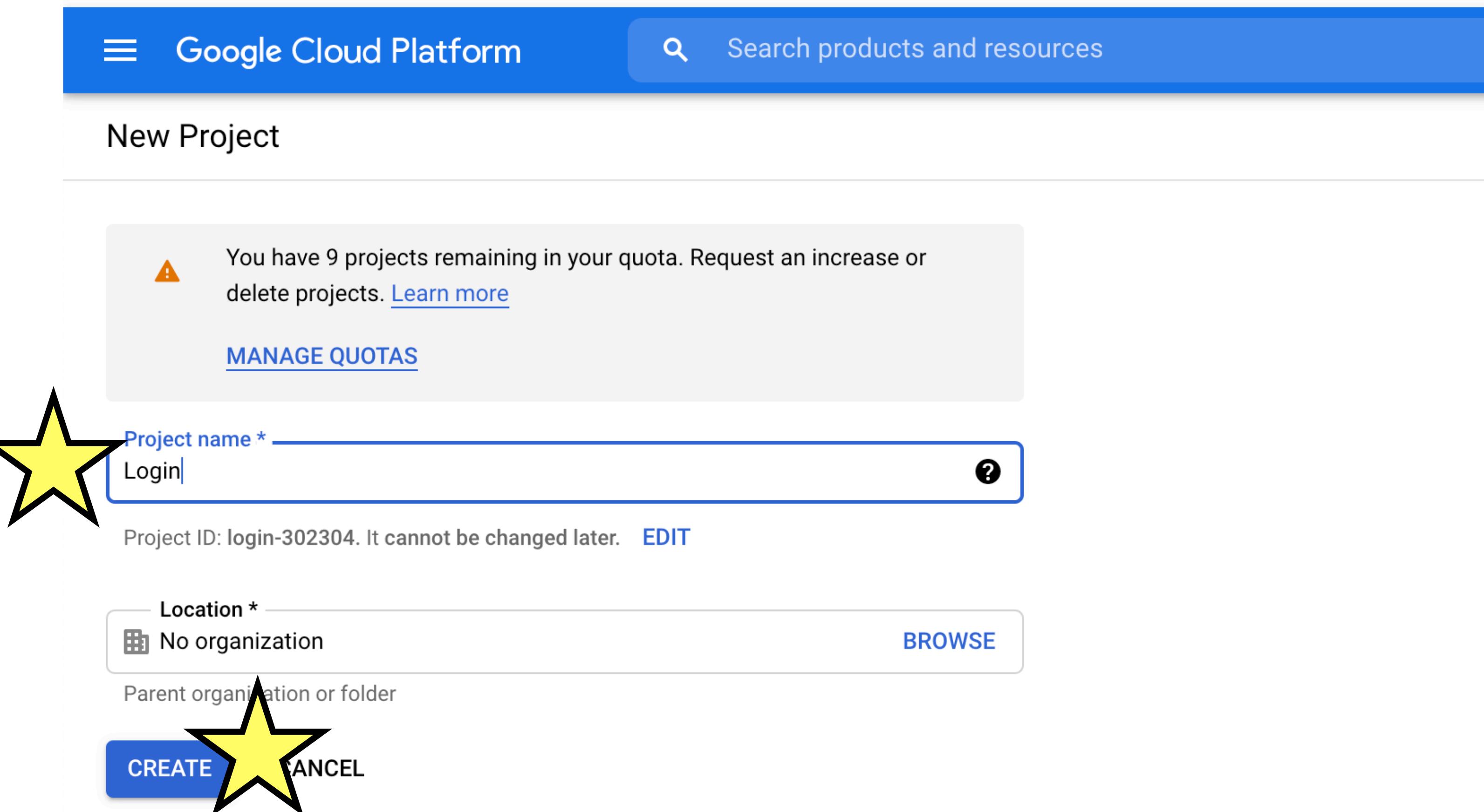
Name	ID
cognito login ?	cognito-login-301800
My First Project ?	the-dock-302303

CREATE RESOURCE CUSTOMIZE DISMISS

Google Cloud Platform status services normal
to Cloud status dashboard

Monitoring up alerting policies
Create uptime checks

Create Google Project



Google Cloud Platform Search products and resources

New Project

⚠ You have 9 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name * Login ?

Project ID: login-302304. It cannot be changed later. [EDIT](#)

Location * No organization [BROWSE](#)

Parent organization or folder

CREATE **CANCEL**

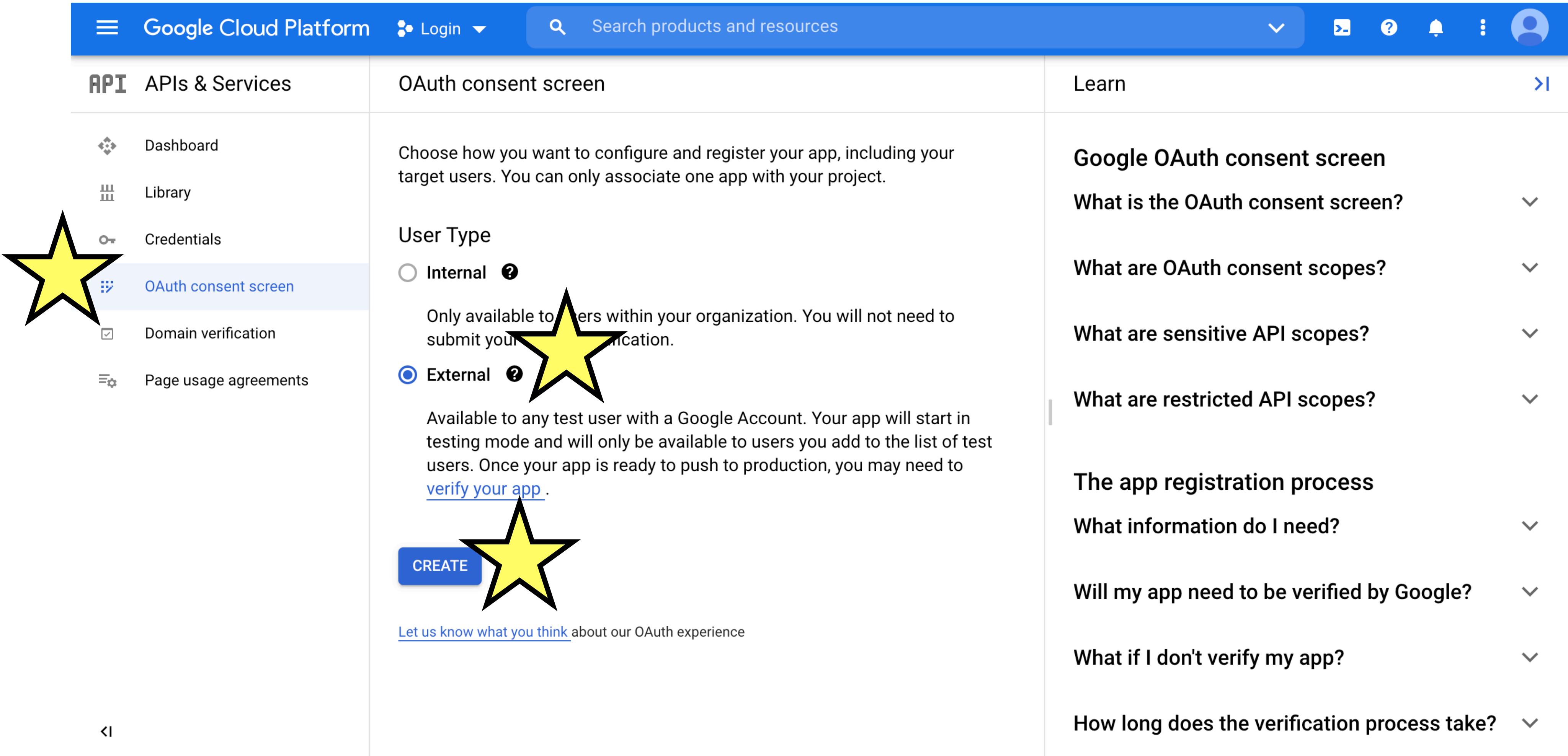
Create OAuth Client

The image shows the Google Cloud Platform (GCP) dashboard. At the top, there's a blue header bar with the GCP logo, a search bar, and various navigation icons. Below the header is a navigation menu on the left containing links like Home, Marketplace, Billing, APIs & Services, Support, IAM & Admin, Getting started, Security, Compliance, and Anthos. The main area of the dashboard is divided into several cards:

- Project info:** Shows Project name (Login), Login, Project ID (login-302304), and Project number (378412114539). It also has a "ADD PEOPLE TO THIS PROJECT" button and a "Go to project settings" link.
- API APIs:** A chart showing Requests (requests/sec) over time. The chart indicates "No data is available for the selected time frame." It has a "Go to APIs overview" link at the bottom.
- Google Cloud Platform status:** Shows "All services normal" and a link to "Go to Cloud status dashboard".
- Monitoring:** Links for "Set up alerting policies" and "Create uptime checks". It also has a "View all dashboards" link and a "Go to Monitoring" link.

A large yellow star is overlaid on the "Go to APIs overview" link in the API card.

Create OAuth Client

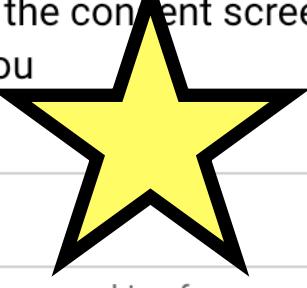
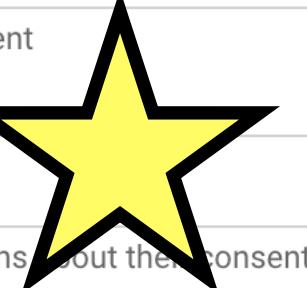
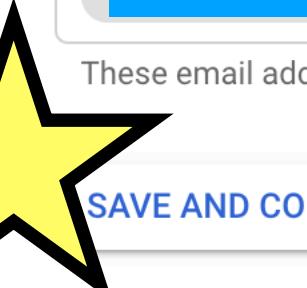
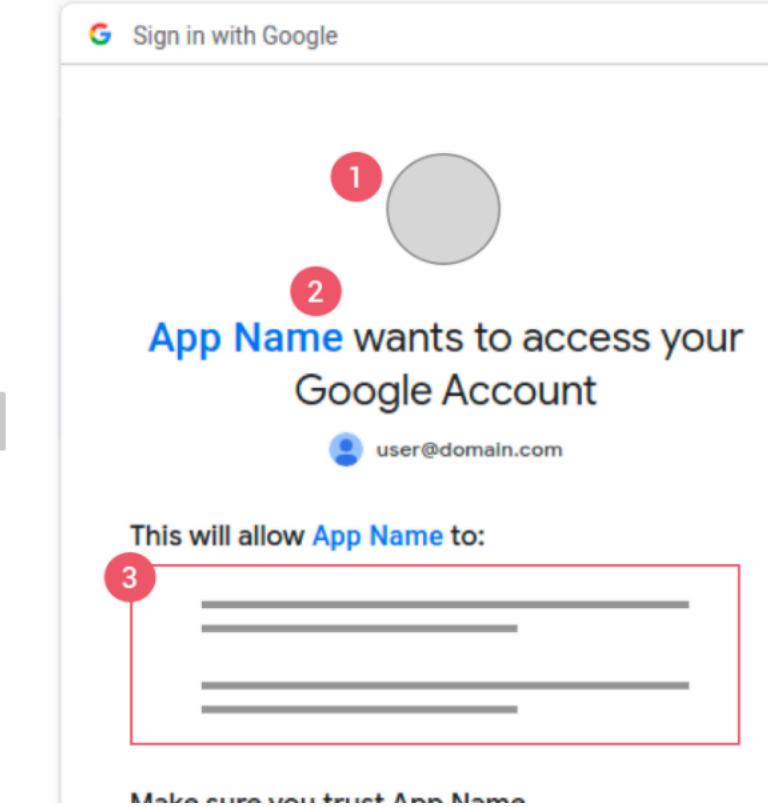


The screenshot shows the Google Cloud Platform interface for creating an OAuth client. The left sidebar is titled "APIs & Services" and includes links for Dashboard, Library, Credentials, **OAuth consent screen**, Domain verification, and Page usage agreements. The "OAuth consent screen" link is highlighted with a yellow star. The main content area is titled "OAuth consent screen" and describes how to configure and register an app. It offers two "User Type" options: "Internal" (disabled) and "External" (selected). The "External" option is described as being available to any test user with a Google Account. A "CREATE" button is at the bottom. The right sidebar contains a "Learn" section with links to Google OAuth consent screen documentation and other API-related topics, each with a yellow star.

Google Cloud Platform Search products and resources

API	APIs & Services	OAuth consent screen	Learn
Dashboard	Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.		
Library			
Credentials	User Type		
OAuth consent screen	<input type="radio"/> Internal Only available to users within your organization. You will not need to submit your application.		
Domain verification	<input checked="" type="radio"/> External Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app .		
Page usage agreements	CREATE		
	Let us know what you think about our OAuth experience		
	Google OAuth consent screen		
	What is the OAuth consent screen?		
	What are OAuth consent scopes?		
	What are sensitive API scopes?		
	What are restricted API scopes?		
	The app registration process		
	What information do I need?		
	Will my app need to be verified by Google?		
	What if I don't verify my app?		
	How long does the verification process take?		

Create OAuth Client

API APIs & Services	Edit app registration	Learn
<ul style="list-style-type: none">❖ Dashboard☰ Library❖ Credentials❖ OAuth consent screen☒ Domain verification☒ Page usage agreements	<p>1 OAuth consent screen — 2 Scopes — 3 Test users — 4 Summary</p> <p>App information</p> <p>This shows in the consent screen, and helps end users know who you are and contact you</p> <p>App name * Login </p> <p>The name of the app asking for consent</p> <p>User support email * </p> <p>For users to contact you with questions about the consent</p> <p>Developer contact information</p> <p>Email addresses * </p> <p>These email addresses are for Google to notify you about any changes to your project.</p> <p>SAVE AND CONTINUE CANCEL</p>	<p>How is this info presented to users?</p> <p>This is the consent screen that users see</p>  <p>Sign in with Google</p> <p>1 App Name wants to access your Google Account user@domain.com</p> <p>This will allow App Name to:</p> <p>3</p> <p>Make sure you trust App Name</p> <p>Make sure you trust App Name</p> <p>4</p> <p>Learn about the risks</p> <p>Cancel Allow</p>

Create OAuth Client

The screenshot shows the Google Cloud Platform interface for creating credentials. The left sidebar has 'APIs & Services' selected, with 'Credentials' highlighted. The main area shows a 'CREATE CREDENTIALS' button and a 'DELETE' button. A modal window is open, listing four credential types: 'API key', 'OAuth client ID', 'Service account', and 'Help me choose'. The 'OAuth client ID' option is highlighted with a large yellow star. The modal also contains descriptive text for each type.

Name	Creation date	Type
No API keys to display		
No OAuth clients to display		

Create OAuth Client

API APIs & Services [← Create OAuth client ID](#)

❖ Dashboard	A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See Setting up OAuth 2.0 for more information.
☰ Library	
🔑 Credentials	
☷ OAuth consent screen	
☑ Domain verification	
≡⚙️ Page usage agreements	

Application type *

- Web application 
- Android
- Chrome app
- iOS
- TVs and Limited Input devices
- Desktop app
- Universal Windows Platform (UWP)

Create OAuth Client

≡ Google Cloud Platform Login ▾ Search products and resources

API APIs & Services ← Create OAuth client ID

❖ Dashboard

☰ Library

🔑 Credentials

❖ OAuth consent screen

☒ Domain verification

⚙️ Page usage agreements

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information.

Application type * Web application

[Learn more about OAuth client types](#)

Name *  login

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Create OAuth Client

The screenshot shows the Google Cloud Platform interface for creating an OAuth client ID. The left sidebar is titled "APIs & Services" and has a "Credentials" section selected. The main page title is "Create OAuth client ID".

Authorized JavaScript origins: `https://mylogin123.auth.us-east-1.amazoncognito.com` (highlighted with a yellow star)

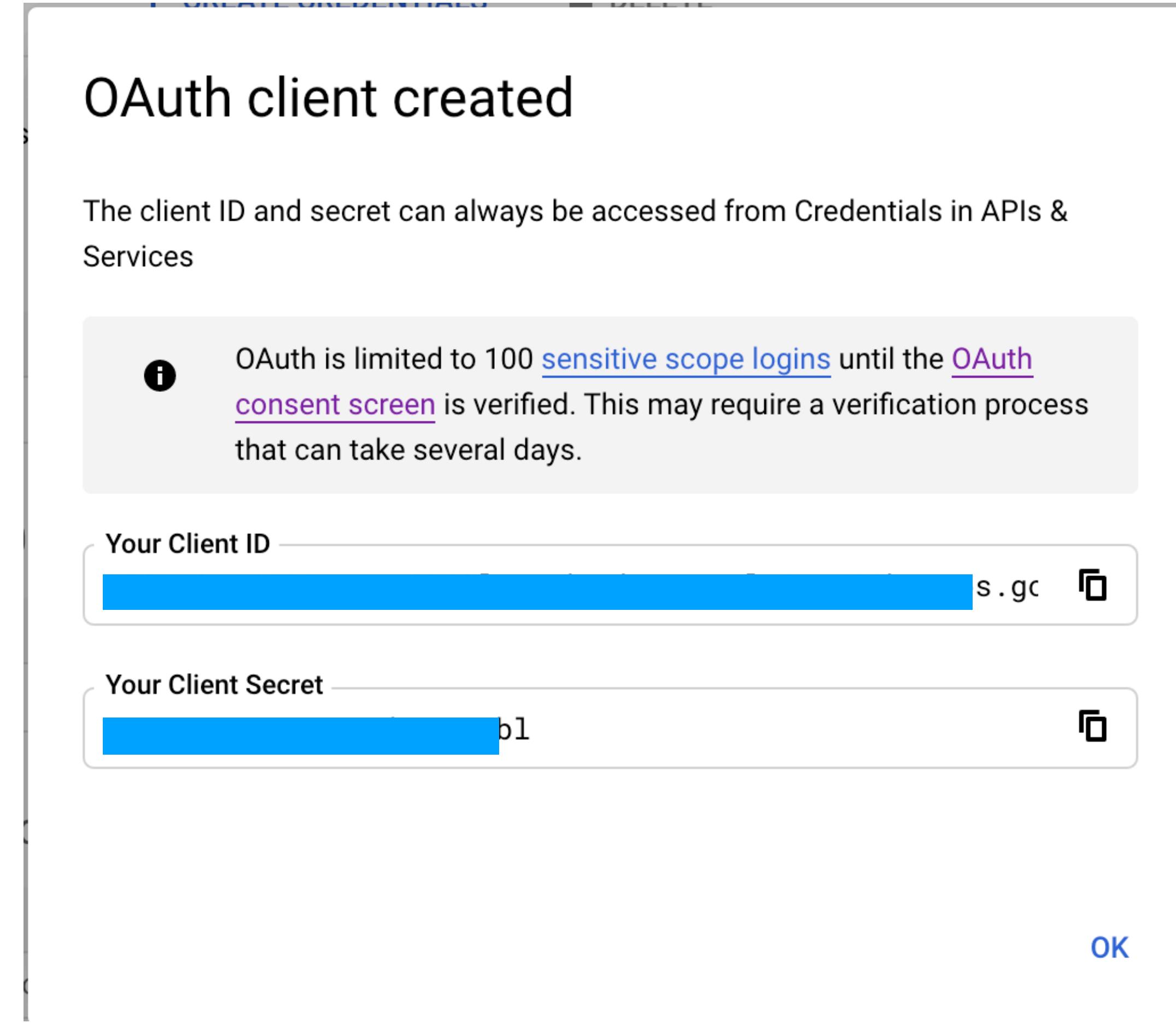
Authorized redirect URIs: `https://mylogin123.auth.us-east-1.amazoncognito.com/oauth2/idresponse` (highlighted with a yellow star)

Buttons at the bottom: "CREATE" (highlighted with a yellow star) and "CANCEL".

Text overlays:

- your_AWS_Cognito_api_client_domain** (overlaps the first yellow star)
- your_AWS_Cognito_api_client_domain/oauth2/idresponse** (overlaps the second yellow star)

Create OAuth Client



Set ID provider in Cognito

The screenshot shows the AWS Cognito console interface. On the left, the navigation menu includes options like MFA and verifications, Advanced security, Message customizations, Tags, Devices, App clients, Triggers, Analytics, App integration, App client settings, Domain name, UI customization, Resource servers, Federation, Identity providers (which is selected and highlighted with a yellow star), and Attribute mapping.

In the main area, there are several identity provider icons: Facebook, Google, Login with Amazon, Sign in with Apple, SAML, and OpenID Connect. The Google icon is highlighted with a yellow star. A modal window for Google sign-in configuration is open, showing fields for Google app ID (value: 3), App secret (value: Z), and Authorize scope (value: profile email openid). The 'Enable Google' button is at the bottom of the modal, also highlighted with a yellow star.

Set ID provider in Cognito

The screenshot shows the AWS Cognito Attribute Mapping configuration page. On the left, there's a sidebar with options like App integration, Federation, Identity providers, and Attribute mapping, with Attribute mapping selected. The main area lists various attributes with checkboxes:

- phoneNumbers
- access_token
- token_type
- expires_in
- refresh_token
- email Email ▼
- email_verified
- name
- picture
- given_name
- family_name
- sub Username ▼

At the bottom, there are "Add Google attribute" and "Save changes" buttons.

Set ID provider in Cognito

AWS Services ▾ Search for services, features, marketplace products, and docs [Option+S] Nate ▾ N. Virginia ▾ Support ▾

Advanced security
Message customizations
Tags
Devices
App clients
Triggers
Analytics

App integration
App client settings **Enabled Identity Providers** Select all Google Cognito User Pool

Sign in and sign out URLs
Enter your callback URLs below that you will include in your sign in and sign out requests. Each field can contain multiple URLs by entering a comma after each URL.

Callback URL(s) **wanted url redirect after login**
https://www.example.com

Sign out URL(s)

OAuth 2.0
Select the OAuth flows and scopes enabled for this app. [Learn more about flows and scopes.](#)

Allowed OAuth Flows
 Authorization code grant Implicit grant Client credentials

Allowed OAuth Scopes
 phone email openid aws.cognito.signin.user.admin profile

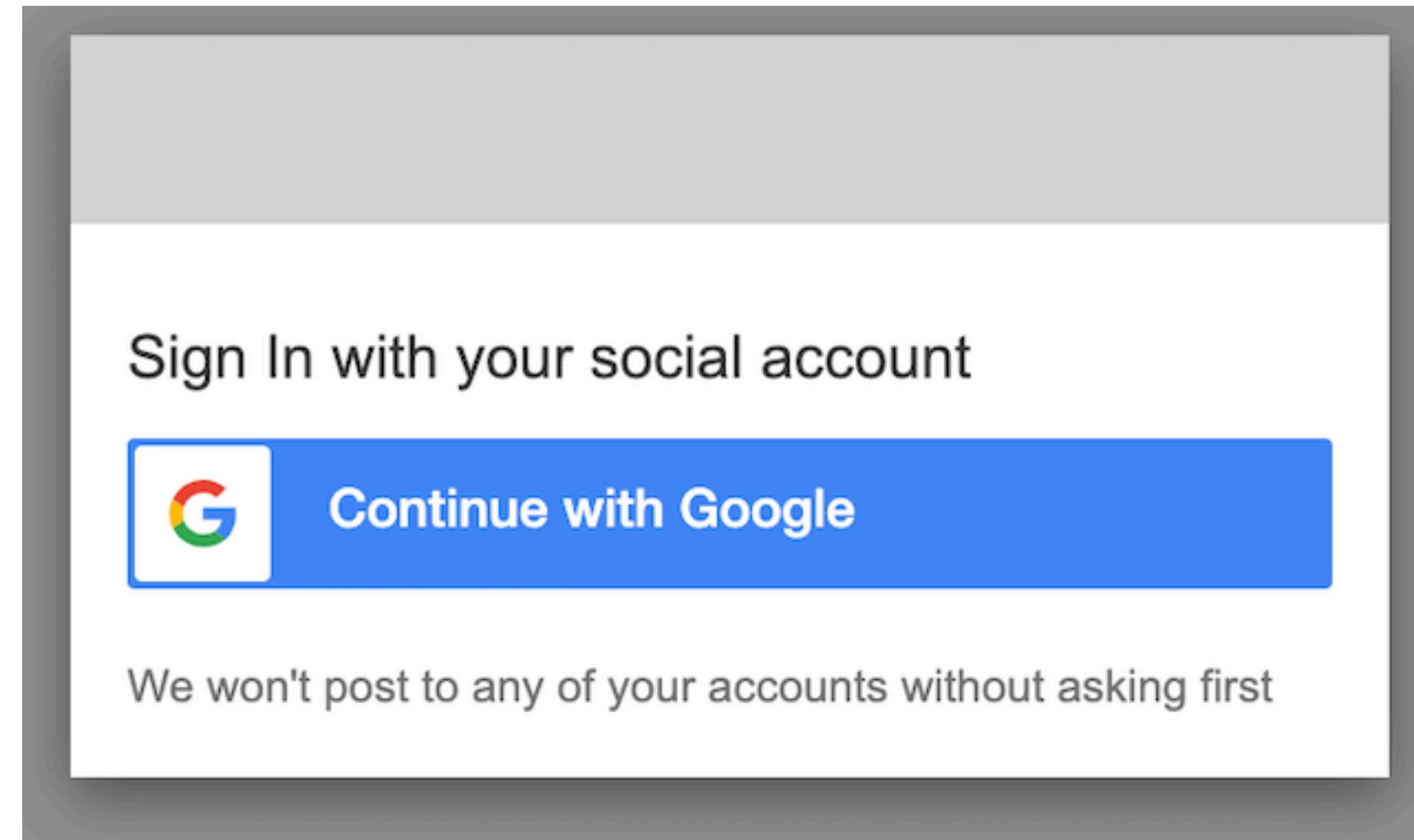
Cancel Save changes

Login with Google Email

The screenshot shows the AWS Cognito App Client Settings page for a Google app client. A yellow star highlights the 'App client settings' section in the left sidebar. The main area shows the following configuration:

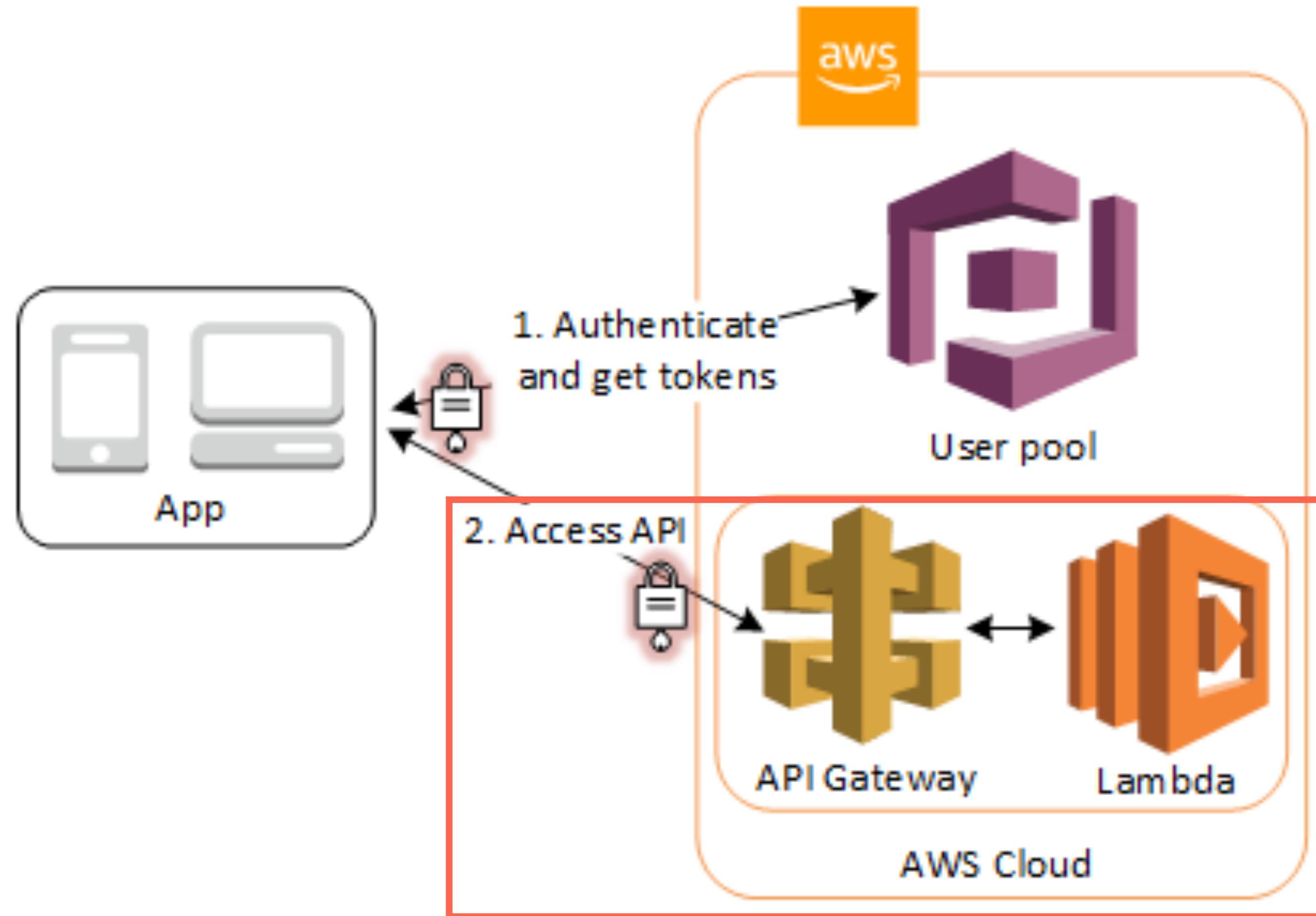
- Sign in and sign out URLs:** Entered as `https://www.example.com`.
- OAuth 2.0:**
 - Allowed OAuth Flows:** Authorization code grant, Implicit grant, Client credentials.
 - Allowed OAuth Scopes:** phone, email, openid, aws.cognito.signin.user.admin, profile.
- Hosted UI:** A button labeled "Launch Hosted UI" is shown, with a yellow star highlighting it.

Login with Google Email



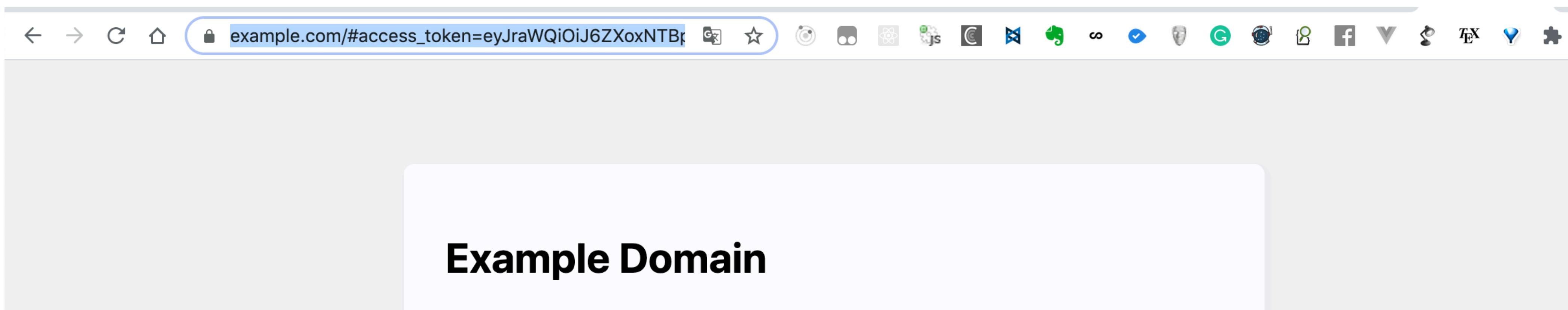
More Resources

API Authorization



API Authorization

get bearer **access token** after login



Some resources

- Blog: <https://aws.amazon.com/tw/blogs/mobile/integrating-amazon-cognito-user-pools-with-api-gateway/>
- Integrate a REST API with an Amazon Cognito user pool: <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-enable-cognito-user-pool.html>
- Set COGNITO_USER_POOLS at Api Gateway -> Method Request -> End Point -> Settings -> Authorization: <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-create-cognito-user-pool.html>
- Defining Resource Servers for Your User Pool: <https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-define-resource-servers.html>