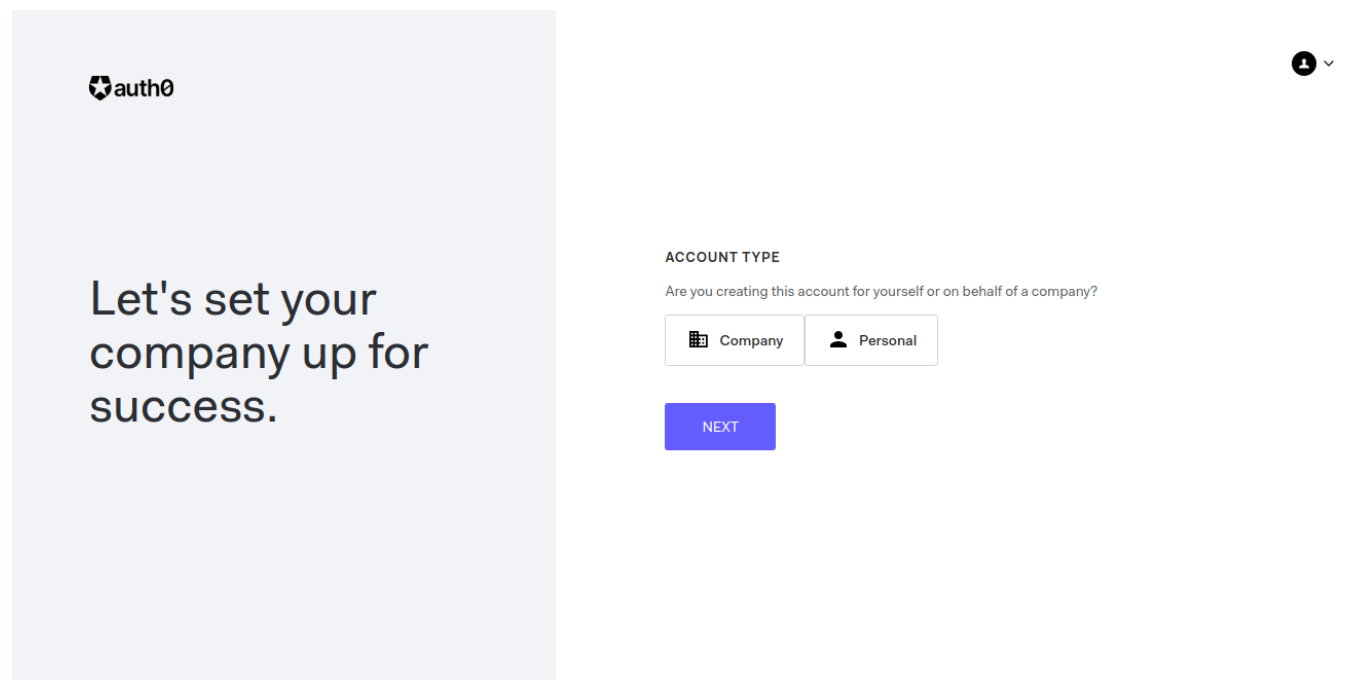


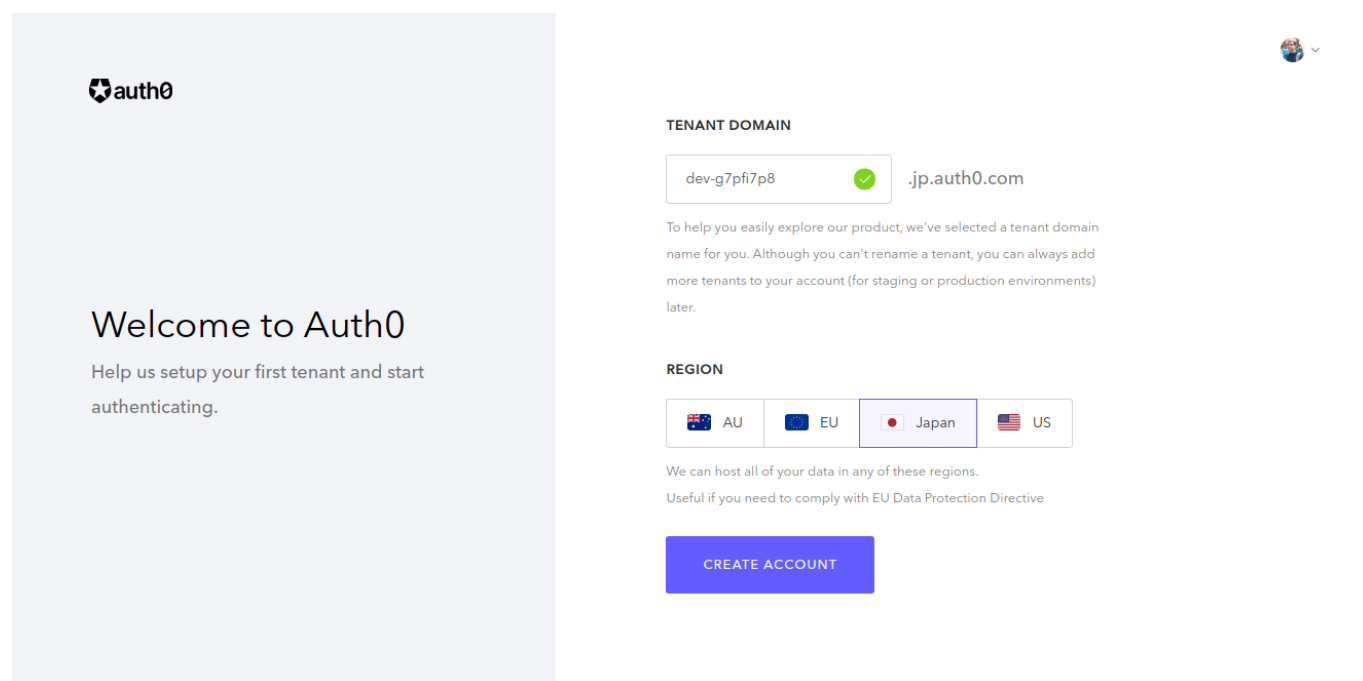
Auth0 Set-up

How to create an account

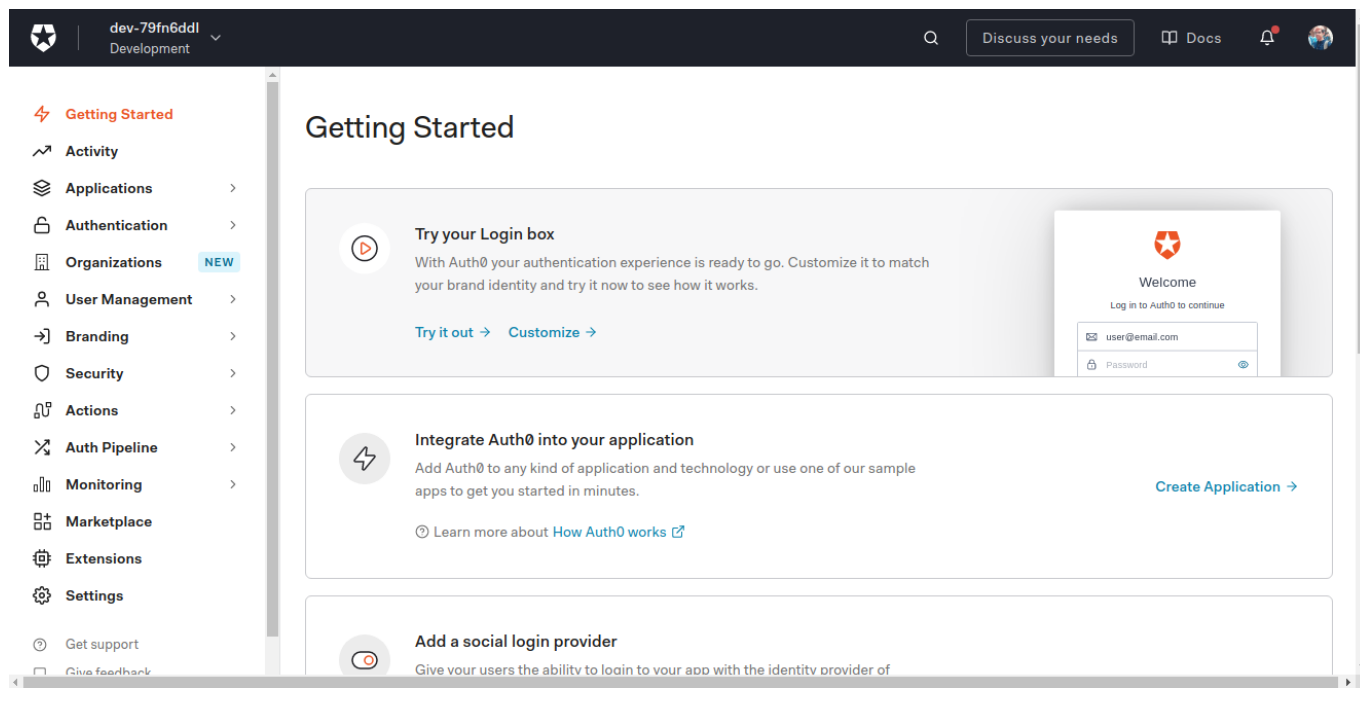
Selecciona el tipo de cuenta "Personal" y le da siguiente.



Elige un nombre para el dominio y la region donde se hospedaran los datos, y finalmente le da en crear cuenta.

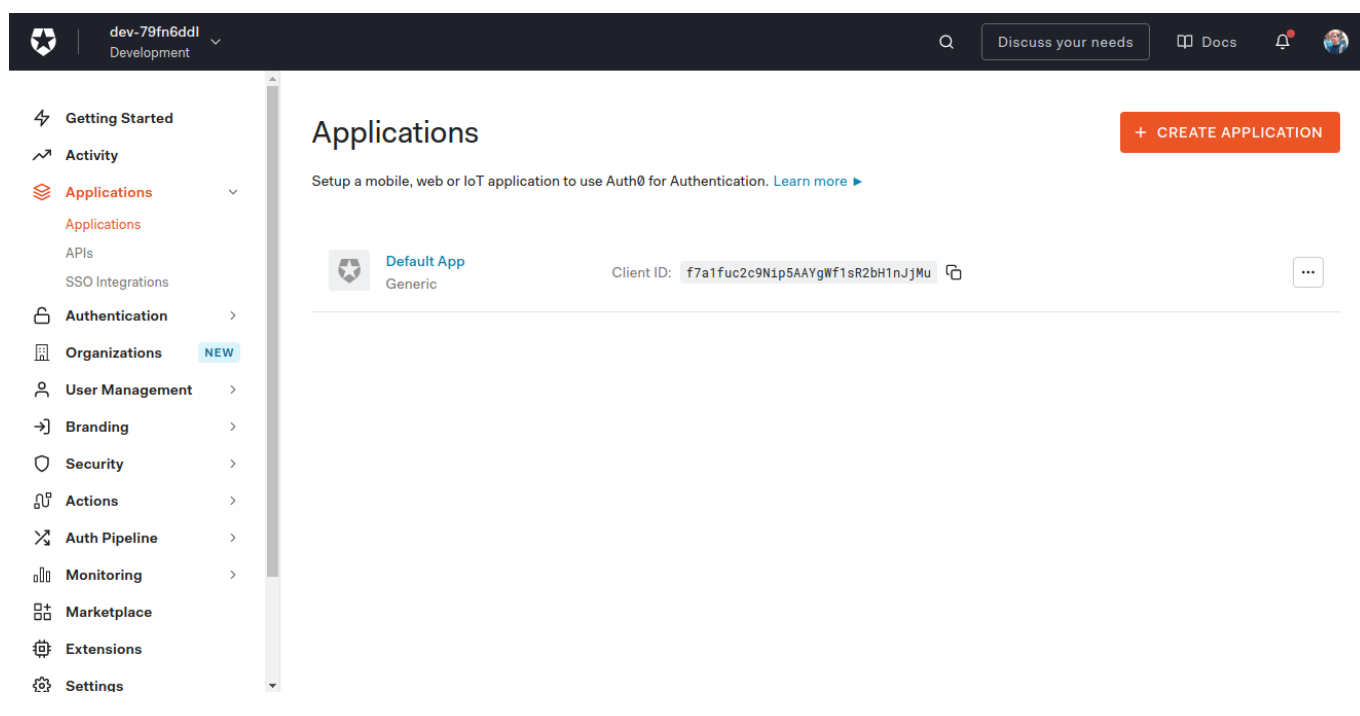


Y listo, lo mandara al dashboard de Auth0.

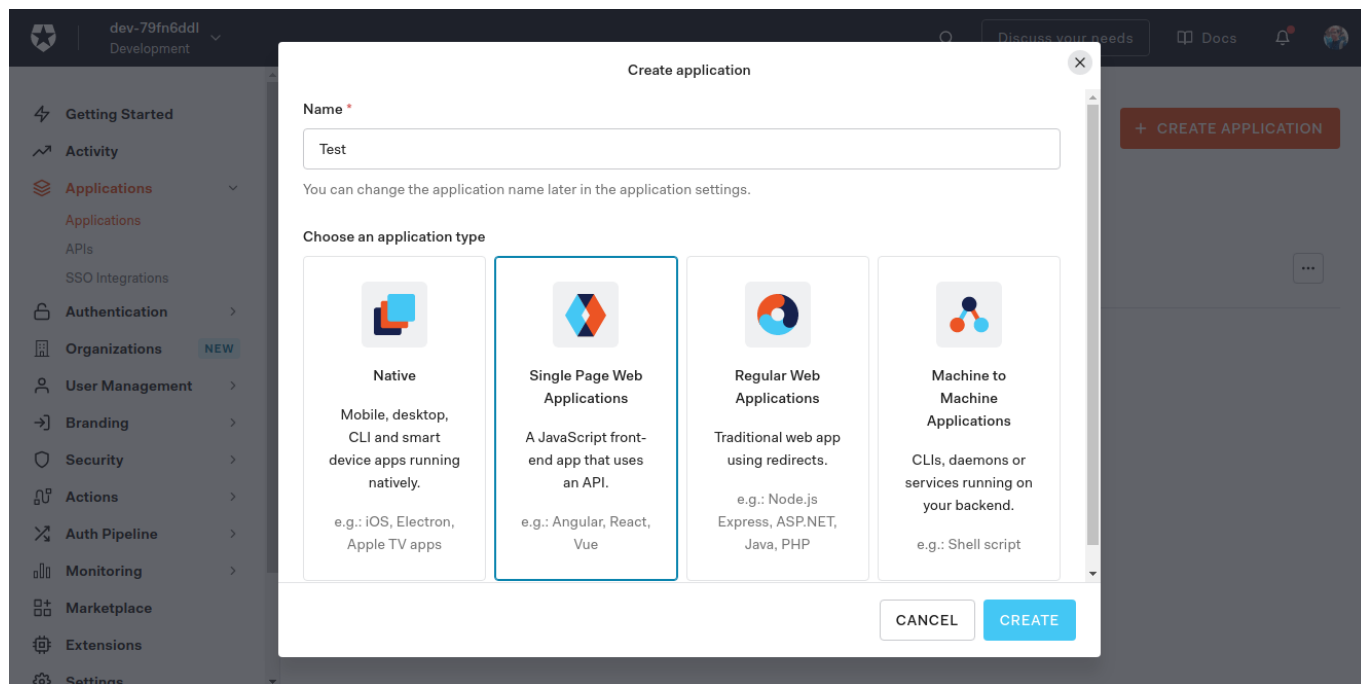


Configure your first Auth0 application

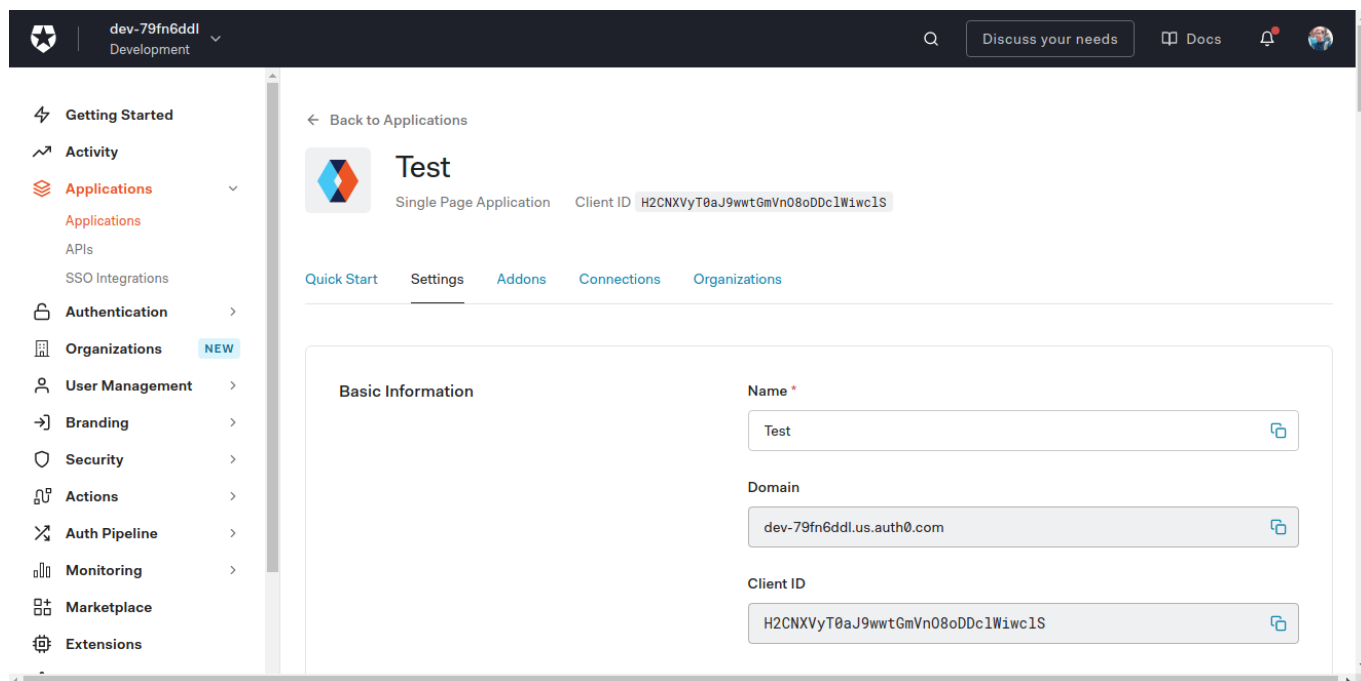
Primero se dirige a la barra lateral y selecciona "Applications->Applications" y se mostrara esto.



Despues selecciona en donde dice "Create application" y le mostrara un campo para elegir el nombre de la aplicacion y de que tipo es su aplicacion. Lo anterior se podra cambiar una vez se cree su aplicacion.



Despues lo que se cree su aplicacion lo mandaran a este panel, en donde podra consultar todo los secretos necesarios para conectarlo con sus otras aplicaciones exteriores.



Bajando hasta el apartado de "Application URIs" encontrara los campos de "Allowed Callback URLs", "Allowed Logout URLs", "Allowed Web Origins" y "Allowed Origins (CORS)".

The screenshot shows the Auth0 dashboard for a development environment (dev-79fn6ddl). The left sidebar contains navigation links: Getting Started, Activity, Applications (selected), APIs, SSO Integrations, Authentication, Organizations (marked as NEW), User Management, Branding, Security, Actions, Auth Pipeline, Monitoring, Marketplace, and Extensions. The main content area is titled 'Application URIs'. It includes three sections: 'Application Login URI' with a text input field containing 'https://myapp.org/login'; 'Allowed Callback URLs' with an empty text input field; and 'Allowed Logout URLs' with an empty text input field. A paragraph explains that the callback URL must point to a route in the application that redirects to the tenant's /authorize endpoint, with a link to 'Learn more'.

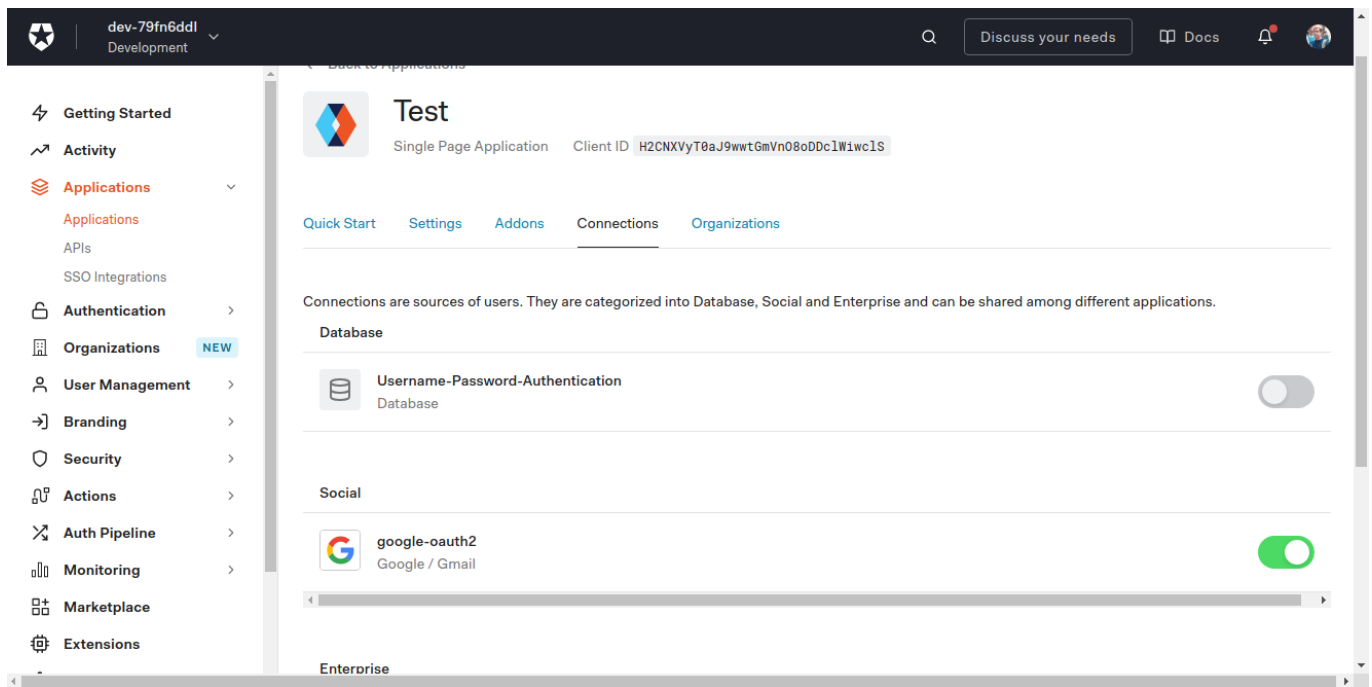
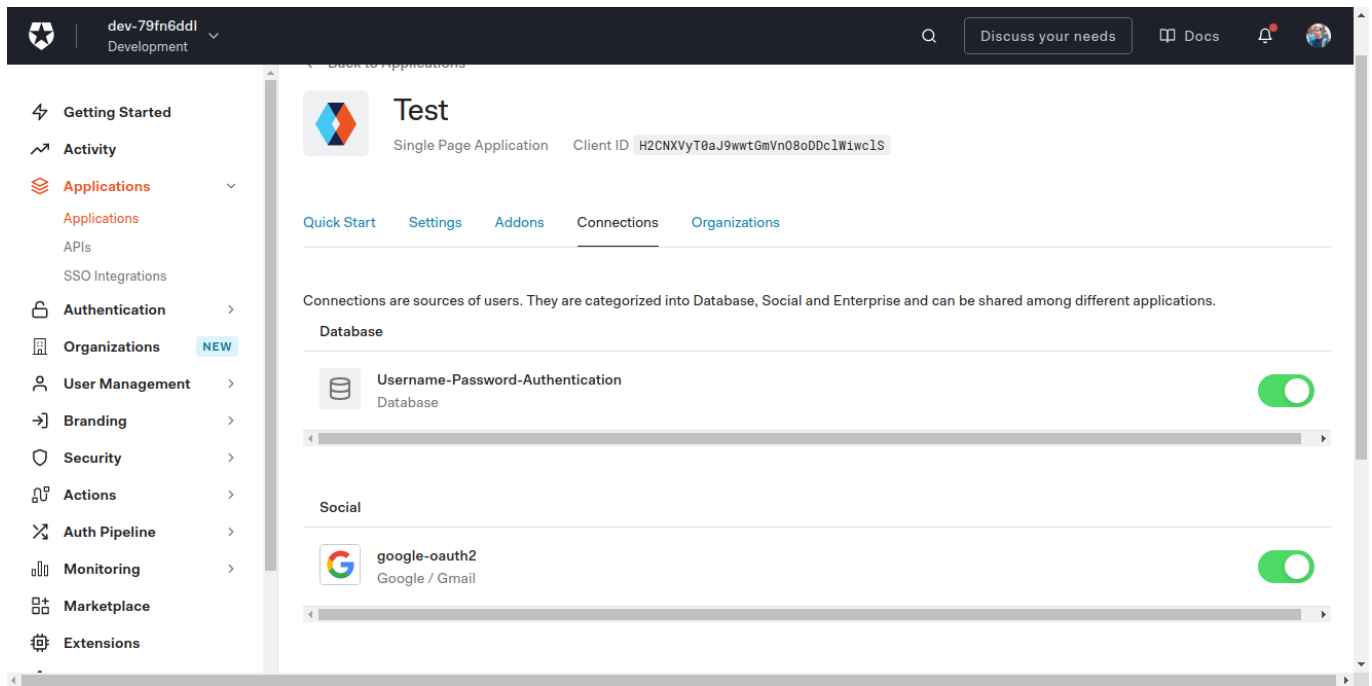
The screenshot shows the 'Allowed Web Origins' and 'Allowed Origins (CORS)' configuration pages in the Auth0 dashboard. The left sidebar is identical to the previous screenshot. The main content area has two sections: 'Allowed Web Origins' with an empty text input field, and 'Allowed Origins (CORS)' with an empty text input field. A paragraph explains that the allowed origins are used for Cross-Origin Authentication, Device Flow, and web message response mode, in the form of <scheme> "://" <host> [":" <port>], such as https://login.mydomain.com or http://localhost:3000. It also mentions that query strings and hash information are not taken into account when validating these URLs.

Ahora rellene los campos con la URL de donde se enviaran peticiones a Auth0. Ejemplo de dominio de app: `https://subdomain.my-page.com/` En "Allowed Callback URLs" el URL debe de se por protocolo https, en los demas pueden ser por http. Y al final guarda los cambios.

The screenshot shows the Auth0 console interface. On the left is a navigation sidebar with options: Getting Started, Activity, Applications (selected), APIs, SSO Integrations, Authentication, Organizations (marked NEW), User Management, Branding, Security, Actions, Auth Pipeline, Monitoring, Marketplace, and Extensions. The main content area is titled 'Application URIs'. It contains three sections: 'Application Login URI' with a text input field containing 'https://myapp.org/login'; 'Allowed Callback URLs' with a text input field containing 'https://subdomain.my-page.com/callback'; and 'Allowed Logout URLs' with a text input field containing 'https://subdomain.my-page.com/'. Each section includes explanatory text and links to learn more.

This block contains two screenshots of the Auth0 console. The top screenshot shows the 'Allowed Web Origins' configuration page. It features a text input field with 'https://subdomain.my-page.com/'. Below the field, text explains that this is a comma-separated list of allowed origins for use with Cross-Origin Authentication, Device Flow, and web message response mode, providing examples like 'https://login.mydomain.com' and 'http://localhost:3000'. The bottom screenshot shows the 'Allowed Origins (CORS)' configuration page. It has a text input field with 'https://subdomain.my-page.com/'. Below the field, text explains that these are URLs allowed to make requests from JavaScript to the Auth0 API, typically used with CORS, and provides examples of wildcard usage like 'https://*.contoso.com'.

Ahora nos vamos a la pestaña de "Connections" y quitamos la opción de "Username-Password-Authentication".



Listo, ya puede ser usada en app externas, solo tiene que copiar el "Domain", "Client ID" y "Client Secret" y configurarlo en su app.