



Thank you for signing up for Auth0! You have 12 days left in your trial to experiment with [features that are not in the Free plan](#). Like what you're seeing? Please enter your [billing information here](#).

[View Plans](#)[← Back to Applications](#)

## Cuattro

Single Page Application

Client ID pXRkdIHA6F3v1sGSB15H8RGmSaZgpY5I

[Quickstart](#)[Settings](#)[Addons](#)[Connections](#)[Organizations](#)

### Basic Information

Name \*

Cuattro



Domain

dev-p0emhjwrs2yxtq75.us.auth0.com



Client ID

pXRkdIHA6F3v1sGSB15H8RGmSaZgpY5I



Client Secret

.....



The Client Secret is not base64 encoded.

Description

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

Add a description in less than 140 characters

### Application Properties

Add text description of the application. Max character count is 140.

### Application Logo



 [https://path.to/my\\_logo.png](https://path.to/my_logo.png)

The URL of the logo to display for the application, if none is set the default badge for this type of application will be shown. Recommended size is 150×150 pixels.

### Application Type


Single Page Application ▼

The type of application will determine which settings you can configure from the dashboard.

## Application URIs

### Application Login URI

<https://myapp.org/login>

In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's `/authorize` endpoint. [Learn more](#) 

### Allowed Callback URLs

<http://localhost:3000>, [http://localhost:3000/\\*](http://localhost:3000/*), <https://api.cuatro.4lumen.com/>

After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like

in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol `https://`. You can use [Organization URL](#) parameters in these URLs.

### Allowed Logout URLs

Comma-separated list of allowed logout URLs for redirecting users post-logout. You can use wildcards at the subdomain level ( `*.google.com` ). Query strings and hash information are not taken into account when validating these URLs. [Learn more about logout](#)

### Allowed Web Origins

http://localhost:3000, http://localhost:3000/\*, http://api.cuatro.4lumen.com

Comma-separated list of allowed origins for use with [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`. You can use wildcards at the subdomain level (e.g.: `https://*.contoso.com`). Query strings and hash information are not taken into account when validating these URLs.

## OpenID Connect Back-Channel Logout

**ENTERPRISE** [Learn more about OpenID Connect Back-Channel Logout](#)

### Back-Channel Logout URI

https://myapp.org/backchannel-logout ⓧ

Logout URI that will receive a `logout_token` when selected Back-Channel Logout initiators occur. URIs with a querystring will be re-encoded properly.

### Back-Channel Logout Initiators

☐ Selected initiators only

☐ All supported initiators

Send a `logout_token` on selected Back-Channel Logout initiators only.

- ☐ RP-Logout ? **REQUIRED**
- ☐ Password Changed ?
- ☐ Session Expired ?
- ☐ Account Deleted ?
- ☐ Email Changed ?
- ☐ Session Revoked ?
- ☐ Account Deactivated ?

## Cross-Origin Authentication

### Allow Cross-Origin Authentication



When allowed, [cross-origin authentication](#) ↗ allows applications to make authentication requests when the Lock widget or custom HTML is used.

### Allowed Origins (CORS)

List additional origins allowed to make [cross-origin resource sharing \(CORS\)](#) ↗ requests. Allowed callback URLs are already included in this list.

- URLs can be comma-separated or added line-by-line
- Use wildcards (\*) at the subdomain level (e.g. [https://\\*:contoso.com](#))
- Query strings and hash information are ignored
- [Organization URL](#) ↗ placeholders are supported

### Cross-Origin Verification Fallback URL

Fallback URL when third-party cookies are not enabled in the browser. URL must use https and be in the same domain as the embedded login widget.

## ID Token Expiration

36000

seconds

Time until an `id_token` expires regardless of activity.

## Refresh Token Expiration

### Set Idle Refresh Token Lifetime



Require `refresh tokens` to expire after a set period of inactivity.

[Learn more about refresh token expiration](#) 


### Idle Refresh Token Lifetime \*

1296000

seconds

### Set Maximum Refresh Token Lifetime



Require `refresh tokens` to expire after a set period regardless of activity. Required for refresh token rotation. [Learn more about refresh token expiration](#) 

### Maximum Refresh Token Lifetime \*

2592000

seconds

## Refresh Token Rotation

### Allow Refresh Token Rotation



When allowed, `refresh tokens` will automatically be invalidated after use and exchanged for new tokens to prevent replay attacks. Requires a maximum refresh token lifetime.

[Learn more about refresh token rotation](#) 

### Rotation Overlap Period \*

0

seconds

Period of time the most recently-used `refresh token` can be reused without triggering breach detection.



## Token Sender-Constraining

### Require Token Sender-Constraining ADD-ON



When required, `access tokens` must be constrained to this application to prevent unauthorized use of leaked or stolen tokens. [Learn more about token sender-constraining](#)

## Authorization Requests

### Require Pushed Authorization Requests (PAR) ADD-ON



When required, authorization request parameters must be sent using back-channel communication for confidentiality and integrity protection. Requires tenant to allow PAR.

[Learn more about Pushed Authorizarion Requests \(PAR\)](#)

### Require JWT-Secured Authorization Requests (JAR) ADD-ON



When required, authorization request parameters must be wrapped in a signed JSON Web Token (JWT) for cryptographically confirmed non-repudiation.

[Learn more about JWT-Secured Authorizarion Requests \(JAR\)](#)

Advanced Settings



## Danger Zone

### Delete this application

All your apps using this client will stop working.

Delete

### Rotate secret

