dev-kp18twnv
Development

Discuss your needs | Docs

Thank you for signing up for Auth0! You have 5 days left in your trial to experiment with features that are not in the Starter plan. Like what you're seeing? Please enter your billing information here.

View Plans

← Back to Applications

Udagram-Lesson5

Single Page Application Client ID `mxd2CVi6z8yBgKQRDmdUZ5Vaj0Y9zp1l`

Quick Start | Settings | Addons | Connections | Organizations

Basic Information

Name *

Udagram-Lesson5

Domain

dev-kp18twnv.us.auth0.com

Client ID

mxd2CVi6z8yBgKQRDmdUZ5Vaj0Y9zp1l

Client Secret

••

The Client Secret is not base64 encoded.

Description

Add a description in less than 140 characters

Add a description in less than 140 characters

A free text description of the application. Max character count is 140.

Application Properties

Application Logo

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 150x150 pixels.

Application Type

Single Page Application

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

Token Endpoint Authentication Method

None

Defines the requested authentication method for the token endpoint. Possible values are 'None' (public application without a client secret), 'Post' (application uses HTTP POST parameters) or 'Basic' (application uses HTTP Basic).

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/callback

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 QA or testing). Make sure to specify the protocol (`https://`) otherwise the callback may fail 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

A set of URLs that are valid to redirect to after logout from Auth0. After a user logs out from Auth0 you can redirect them with the `returnTo` query parameter. The URL that you use in `returnTo` must be listed here. You can specify multiple valid URLs by comma-separating them. You can use the star symbol as a wildcard for subdomains (`*.google.com`). Query strings and hash information are not taken into account when validating these URLs. Read more about this at https://auth0.com/docs/login/logout

Allowed Web Origins

http://localhost:3000

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.

Allowed Origins (CORS)

Allowed Origins are URLs that will be allowed to make requests from JavaScript to Auth0 API (typically used with CORS). By default, all your callback URLs will be allowed. This field allows you to enter other origins if you need to. You can specify multiple valid URLs by comma-separating them or one by line, and also 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.. You can use Organization URL placeholders in these URLs.

ID Token

ID Token Expiration

36000 seconds

This setting allows you to set the lifetime of the `id_token` (in seconds)

Refresh Token Rotation

Rotation

When enabled, as a result of exchanging a refresh token, a new refresh token will be issued and the existing token will be invalidated. This allows for automatic detection of token reuse if the token is leaked. In addition, an absolute expiration lifetime must be set. Learn more

Reuse Interval

0 seconds

The allowable leeway time that the same `refresh_token` can be used to request an `access_token` without triggering automatic reuse detection.

Refresh Token Expiration

Absolute Expiration

When enabled, a `refresh_token` will expire based on an absolute lifetime, after which the token can no longer be used. If rotation is enabled, an expiration lifetime must be set. Learn More

Absolute Lifetime

2592000 seconds

Sets the absolute lifetime of a `refresh_token` (in seconds).

Inactivity Expiration

When enabled, a `refresh_token` will expire based on a specified inactivity lifetime, after which the token can no longer be used.

Inactivity Lifetime

1296000 seconds

Sets the inactivity lifetime of a `refresh_token` (in seconds).

Advanced Settings

Application Metadata | Device Settings | OAuth | Grant Types

Allowed APPs / APIs

Allowed Applications / APIs are applications that will be allowed to make delegation request. By default, all your applications will be allowed. This field allows you to enter specific client ids. You can specify multiple IDs by comma-separating them or one by line.

JSON Web Token (JWT) Signature Algorithm

RS256

Specify the algorithm used to sign the JSON Web Token: HS256: JWT will be signed with your client secret. RS256: JWT will be signed with your private signing key and they can be verified using your public signing key (see Certificates - Signing Certificate section).

OIDC Conformant

Applications flagged as OIDC Conformant will strictly follow the OIDC specification. Turning on this flag can introduce breaking changes to this application. If you have any questions you can contact support.

Cross-Origin Verification Fallback

https://domain.tld/path

Location URL for the page that will be rendered inside an iframe to perform the token verification when third party cookies are not enabled in the browser. Must be in the same domain where the embedded login form is hosted and must have a https scheme.

Save Changes

Danger Zone

Delete this application

All your apps using this client will stop working.

Delete

Rotate secret

All authorized apps will need to be updated with the new client secret.

Rotate