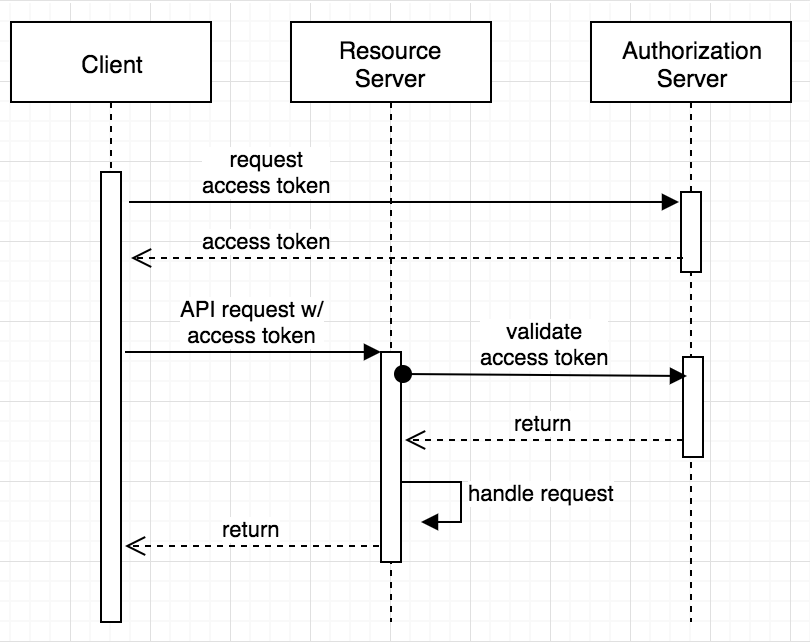
**Okta Client Credentials Flow Setup for YSN Application**

[**What Is the Client Credentials Grant Flow?**](https://developer.okta.com/blog/2021/05/05/client-credentials-spring-security#what-is-the-client-credentials-grant-flow)

The goal of the OAuth 2.0 client credentials grant is to allow two automated services to interact securely. It does this primarily by replacing the old scheme, HTTP Basic, with a token-based authentication scheme that greatly reduces the number of requests that expose sensitive access credentials.

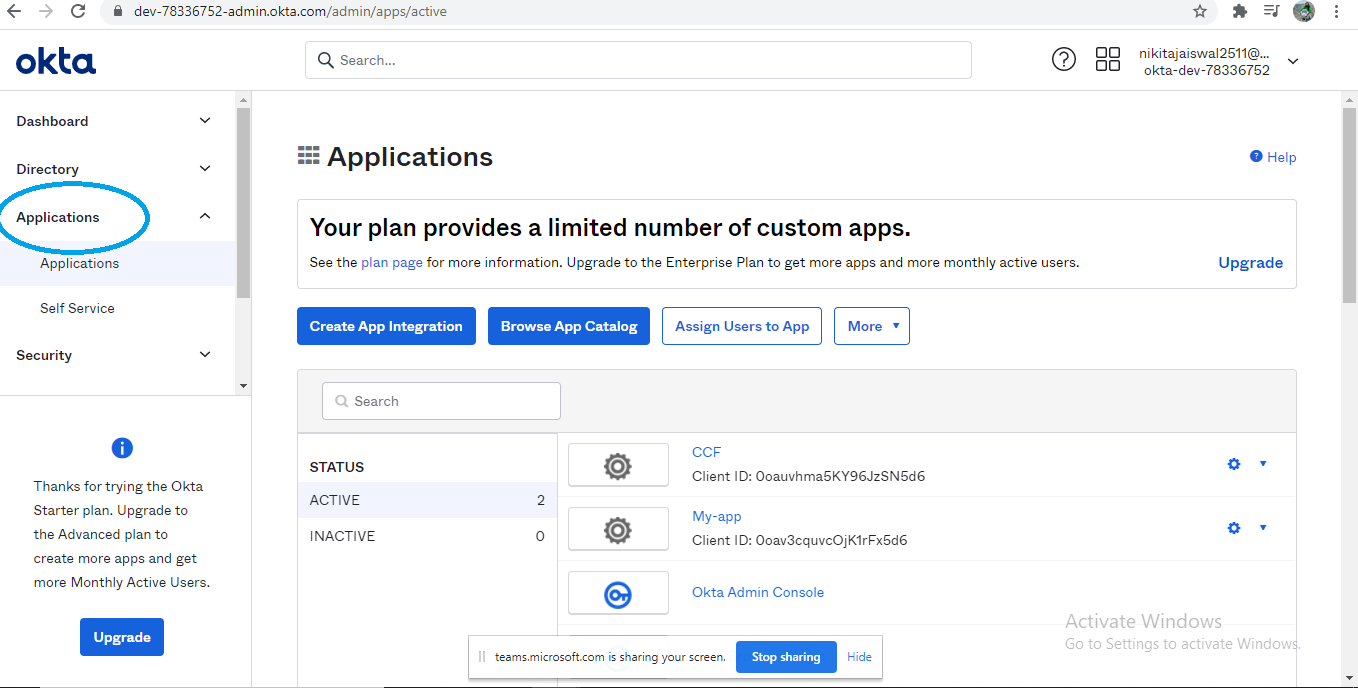


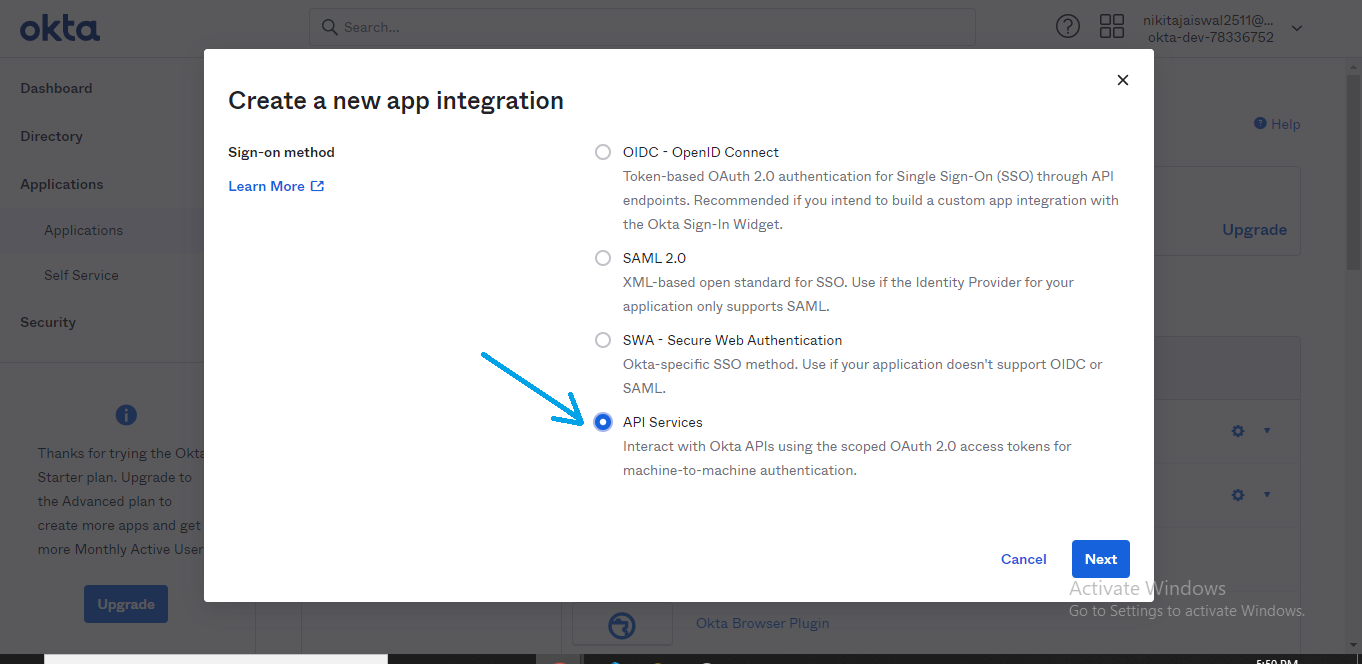
Setup Okta

Log in to your Okta Developer account (or [sign up](https://developer.okta.com/signup/) if you don’t have an account) and navigate to **Applications** > **Add Application**. Click **Single-Page App**, click **Next**, and give the app a name you’ll remember. Click **Done**.

Create Application

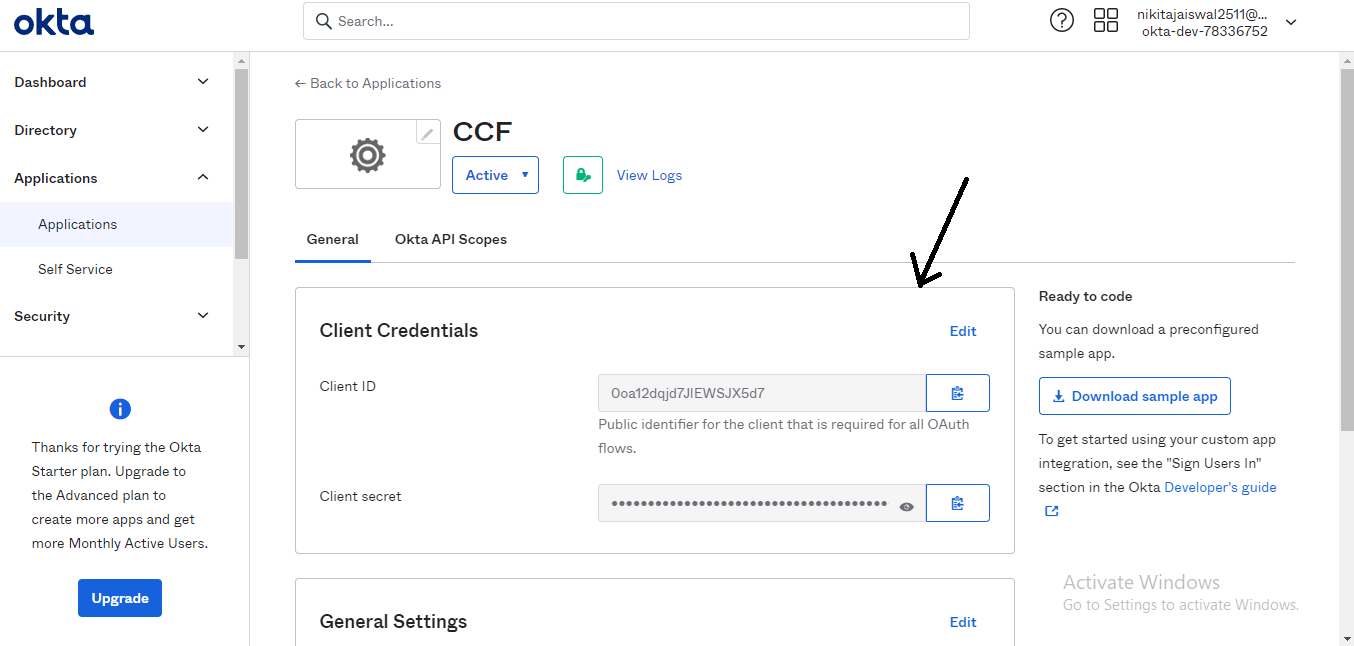
In your Okta dashboard, click on **Applications** in the top header. Applications are also known as clients, so this is where you can create a test client. Click **Add Application** and choose **Service** (Machine-to-Machine). The only information it needs is a name, so you can use something like Test Client. This will give you the credentials for your client (in this testing case, that would be you).

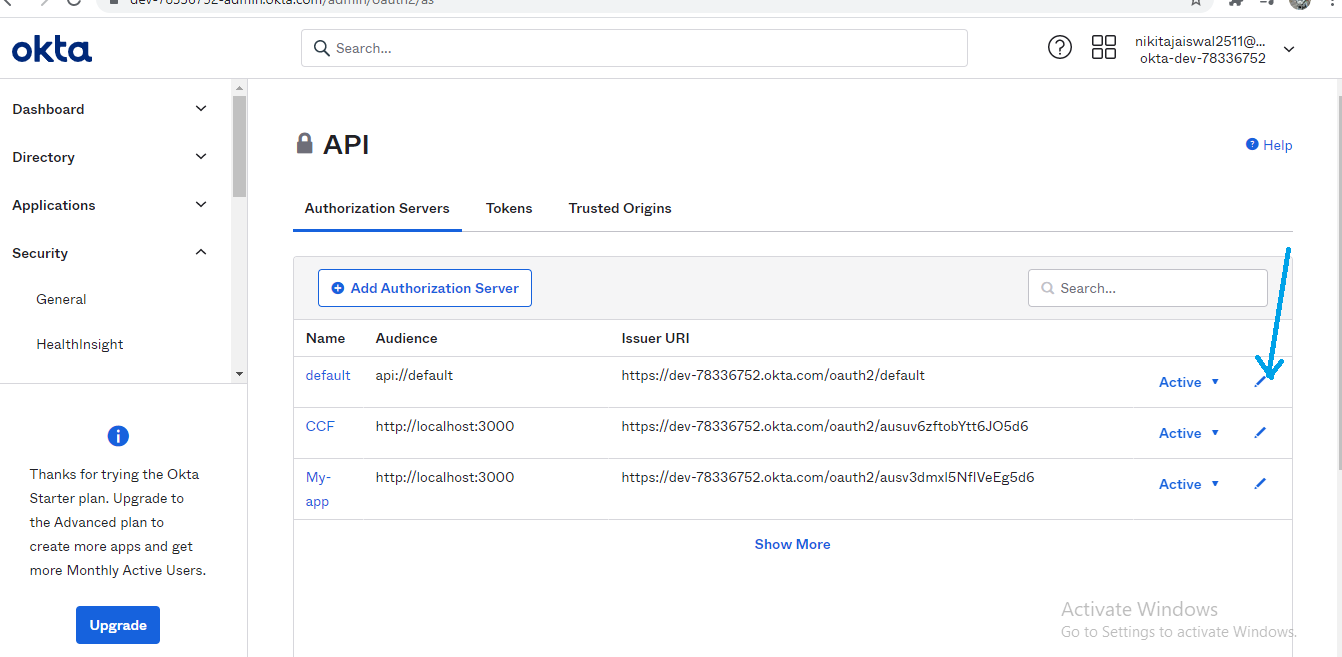




Create Authorization Server

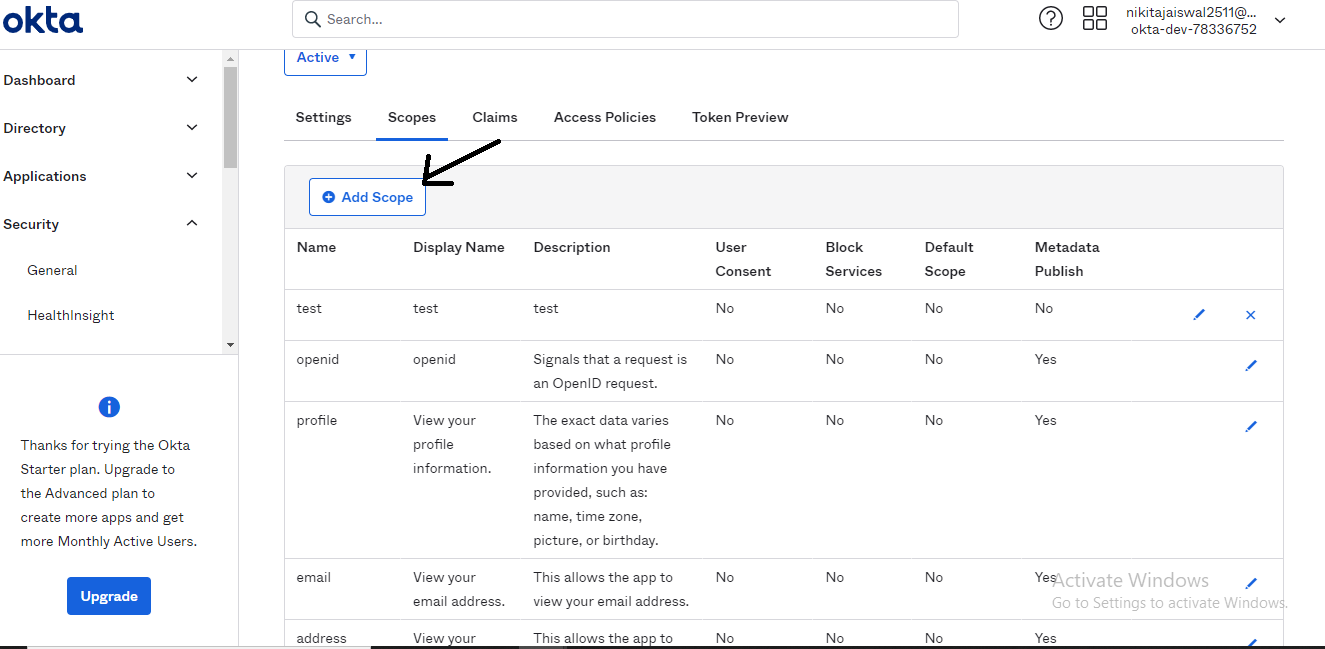
The authorization server is where clients can request a token to use on your API server. Inside the Okta dashboard, click on the **API** tab in the header, then select the **Authorization Servers** tab. Click **Add Authorization Server**, then give your server a useful name and description. The Audience should be an absolute path for the server that will be consuming the tokens.





Add Scope

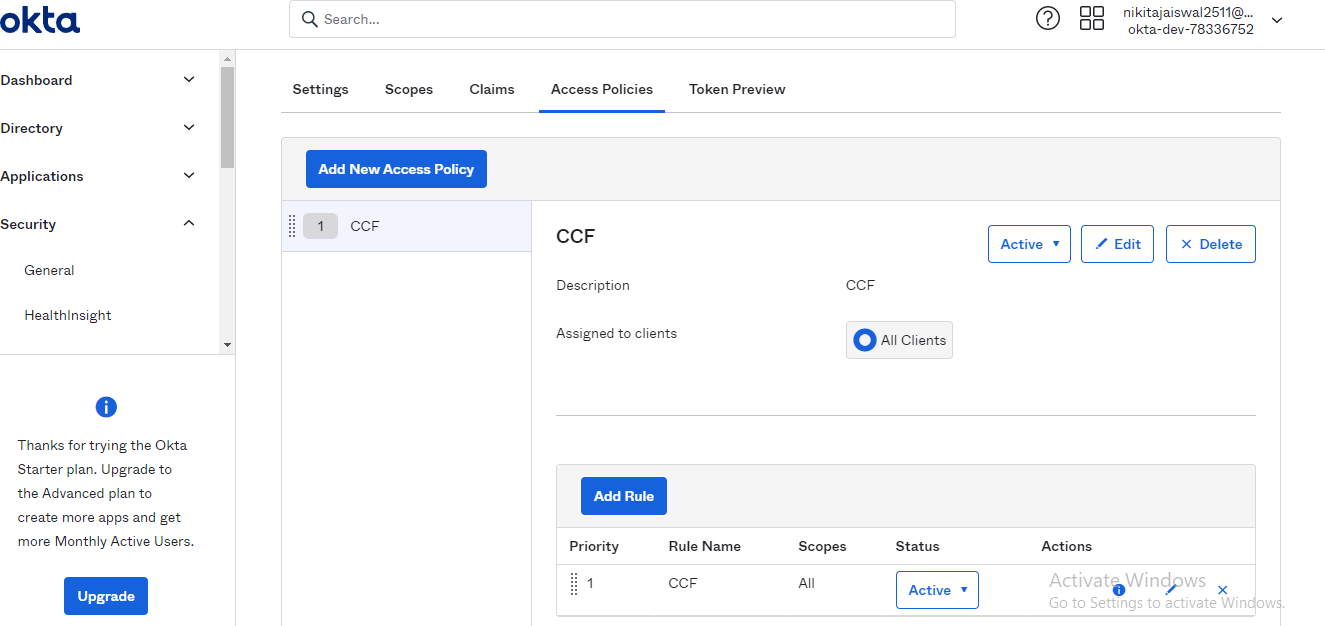
Once you create the authorization server, you will need a scope for your clients to access. Click the **Scopes** tab and add a scope. You can have many of these, which can help define what parts of the API are being used, or even who is using it.



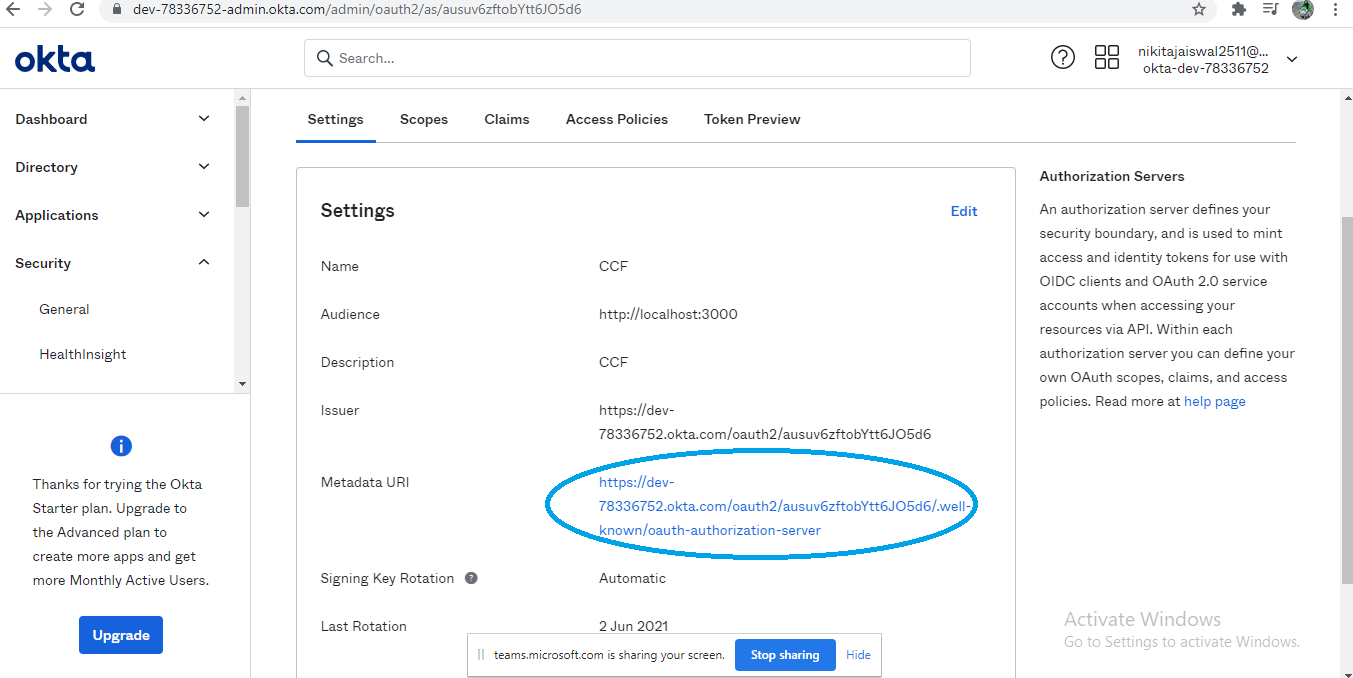
Add Rule

Now that you have a scope, you also need to specify some rules to say who has access to it. Click the **Access Policies** tab and create a new policy. For now, just allow access to All clients. Then click **Add Rule** and give it a name. Since this is only for client credentials, remove the other grant types for acting on behalf of a user (Authorization Code, Implicit, and Resource Owner Password) so the only grant type is Client Credentials. Aside from that, just use the default settings for now.

Back on the **Settings** tab, take note of the **Issuer**. This is the address clients will use to request a token, and what your API server will use to verify that those tokens are valid.



Configure Settings



Modify .env to use the settings you specified above.

ISSUER=https://{yourOktaDomain}/oauth2/abcdefg1234567

DEFAULT\_SCOPE=such\_scope

TEST\_CLIENT\_ID={yourClientId}

TEST\_CLIENT\_SECRET={yourClientSecret}

**NOTE:** The value of {yourOktaDomain} should be something like dev-123456.oktapreview.com. Make sure you don't include -admin in the value!