OAuth2 Client credentials for API Clients

To use the API's provided by GOPACS, your application needs to identify itself and use an OAuth2 Bearer token.

This manual describes all the steps needed to set up client credentials and retrieve an OAuth2 Bearer Token. For general information on OAuth2, see for instance https://oauth.net/2/.

There are two steps:

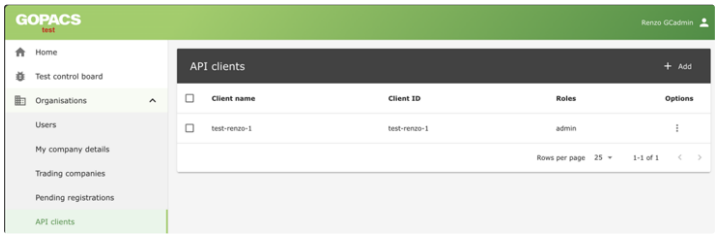
1. Your API Client needs to be registered within GOPACS, resulting in a client id and a client secret.
2. With this client id and secret, you obtain the bearer token at the authorization server.

Below these two steps are further explained. For a video instruction (in Dutch), please check this explanation video.

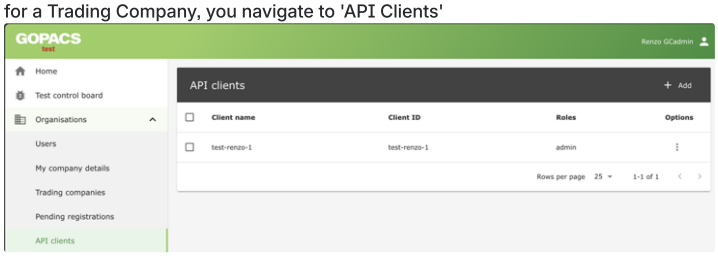
1. Set up client credentials

You need to set up once the client credentials for the application that uses one of the GOPACS APIs.

1. Log in to the GOPACS UI as a Grid Admin or Trading Company Admin
2. Now,
   a. for a Grid Admin, you have to navigate to 'Organisations > API Clients'



   b. for a Trading Company, you navigate to 'API Clients'



3. Press the '+ Add' button to create a new API client
4. Specify a unique name and the roles you want to attach to this client
   a. e.g. Depending on the role, you can restrict what an API client is capable off.
5. Once created, you will see a client key. For security reasons, ***this key is only shown once!***

2. Obtain bearer token

To obtain the Bearer Token, you need to authorize with our OAuth2 Authorization server using the client credentials you received in step 1. The URL of the authorization server is in the table below.

Environment	Authorization server URL
Acceptance	https://auth.acc.gopacs-services.eu/realms/gopacs/protocol/openid-connect/token
Production	https://auth.gopacs-services.eu/realms/gopacs/protocol/openid-connect/token

This endpoint expects a *POST* request with content-type *application/x-www-form-urlencoded.* It will respons with a JSON object.

```
curl -X POST "https://auth.acc.gopacs-services.eu/realms/gopacs/protocol/openid-connect/token" \
-H "Content-Type: application/x-www-form-urlencoded" \
-d "client_id=xxxxxx" \
-d "client_secret=xxxxxxxx" \
-d "grant_type=client_credentials"
```

In the response you'll find an access token. This token can be used as authentication for the service

```
{
 "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSl...",
 "expires_in": 300,
 "refresh_expires_in": 1800,
 "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSl...",
 "token_type": "bearer",
 "not-before-policy": 0,
 "session_state": "a856fb91-eabc-460e-a54b-808c93acdc29"
}
```

Now, you need to read the access_token from this object and add it to the *Authorization* header of any subsequent request to any GOPACS API.

```
Authorization: Bearer <token>
Accept: application/json
```