# Terminology

**Client** is the application that is making the request on behalf of the user.

Eg) Browser, App etc

**User** is the user who wishes to be authenticated.

Eg) The human user trying to login

**Authority**: It just means permission. The user can define his own authorities.

Eg) Homepage\_view, add\_friend

**Role**: It is also an authority. Just a specialized authority. It starts with ROLE\_ prefix. Here also the user can name it whatever he wants.

Eg) ROLE\_ADMIN, ROLE\_USER

**Scope**:

Just like Users have authorities, scope is the authority of the Client

# Eg) This is also user defined like “Share\_post\_to\_instagram”

# Authorization Server

Authorization Server is running on port 8081

*Header* passes the Client information

The *Body* passes the user information

1. **The “Token” Endpoint** to get an access token

<http://localhost:8081/oauth/token>

Headers:

* + Basic ZmFjZWJvb2tfYXBwOnNlY3JldA==
  + This above is base64 of “facebook\_app:secret” (which is the client’s id and secret)
  + Obviously, the token endpoint must be open to everyone without authentication. Hence the permitAll() in AuthServerConfiguration.java
  + Also note that the client details like authorities, token duration etc are also configured in AuthServerConfiguration.java
  + User details like password and roles are present in the UserDetailsService.java

Body (User’s credentials)

{

“grant\_type”:”password”,

“username”:”admin”,

“password”:”password”

}

Response

{

"access\_token": "eba6daa6-78df-4790-bf01-685664850ff4",

"token\_type": "bearer",

"refresh\_token": "7ac7b4e5-9ad3-4260-942d-b1d6124c2b84",

"expires\_in": 1199,

"scope": "get\_token access\_to\_facebook"

}

1. The “Check Token” Endpoint is used by the resource server to check whether the access token given to it is valid and get the details of the user like what all roles he has.

Ideally, we don’t need to hit this endpoint as it is done internally.

But to debug, this endpoint can be helpful.

<http://localhost:8081/oauth/check_token?token=e7c8c7ff-91ae-4ffd-9f9c-841c7d5bf335>

Response

{

"aud": [

"resource-server-rest-api"

],

"user\_name": "admin",

"scope": [ //The client’s permissions

"get\_token",

"access\_to\_facebook"

],

"active": true,

"exp": 1541009202,

"authorities": [ //The user’s permissions

"VIEW\_PROTECTED",

"VIEW\_REGULAR"

],

"client\_id": "facebook\_app"

}