# Tutorial 9. OAuth2

Discuss in group

1. Why do we need a token based authorization? What is the problem of traditional session-based approach?
2. What is grant\_type? What are different grant\_type supported by Spring?
3. What is Resource Server and Authorization Server?
4. Where is the generated token stored?

Practice 1:

1. Clone the following project: <https://github.com/thanhnew2001/SpringOAuth2JWTCORS>
2. Examine 3 classes: AuthorizationServerConfig and ResourceServerConfig and SecurityConfig
3. Run the project using **mvn: jetty:run**
4. Now use Postman to test

Step 1) Obtain an access\_token:

Create a post to localhost:8080/oauth/token?grant\_type=password&username=admin&password=admin

Authorization header: select BasicAuth with client-id/secret

You will get an access\_token

Step 2) Use that access\_token to GET a resource:

localhost:8080/students/?access\_token=[access\_token]

Step 3) Try to get a new token using refresh\_token by creating a POST to

localhost:8080/oauth/token?grant\_type=refresh\_token&refresh\_token=[refresh\_token]

# Exercises

1. Update the clients with different validity, resource id and secret and try

clients.inMemory()  
 .withClient("client-id")  
 .authorizedGrantTypes("client\_credentials", "password", "refresh\_token")  
 .authorities("ROLE\_TRUSTED\_CLIENT")  
 .scopes("read", "write")  
 .resourceIds("resource-id")  
 .accessTokenValiditySeconds(1200)  
 .secret("secret");

2. Separate resource server and authorization server