Try Authorization Code Grant

The Authorization Code Grant is one of the grant types in the OAuth 2.0 specification. For more information about this grant type, see Authorization Code Grant.

⚠️ Before you begin, you must first set up the sample webapp.

This section demonstrates the Authorization Code Grant with PKCE and without PKCE.

The Proof Key for Code Exchange (PKCE) is a specification supported by WSO2 Identity Server to mitigate code interception attacks. See Mitigating Authorization Code Interception Attacks to configure PKCE for an OAuth application.

- Running the application (without PKCE)
- Running the application (with PKCE)

Running the application (without PKCE)

1. Visit the URL http://wso2is.local:8080/playground2/oauth2.jsp to start the application.
2. Enter the following details and click Authorize. For information on how to obtain these authorization details, see Configuring OAuth2-OpenID Connect.

Authorization Grant Type: Authorization Code
Client ID: (the client id received at the application registration)
Callback URL: http://wso2is.local:8080/playground2/oauth2client
Authorize Endpoint: https://localhost:9443/oauth2/authorize
3. Log in with the user credentials.
4. Select Approve Once or Approve Always in Access to profile information section. Also, select the attributes you agree to share. Click Continue.

5. Provide the following details and click on Get Access Token.

   - **Callback URL:** [http://wso2is.local:8080/playground2/oauth2client](http://wso2is.local:8080/playground2/oauth2client)
   - **Access Token Endpoint:** [https://localhost:9443/oauth2/token](https://localhost:9443/oauth2/token)
   - **Client Secret:** (client secret received at the application registration)

   If you have configured the service provider in a tenant, you have to add the tenant domain as a query parameter to the access token endpoint.

   If the tenant domain is **wso2.com**, access token endpoint will be as follows.

At this point, the application receives the Access Token. Enter the introspection endpoint (i.e., `https://localhost:9443/oauth2/introspect`) and click **Get TokenInfo** to get the token information.

OAuth 2.0 Token Introspection defines a protocol that allows authorized protected resources to query the authorization server to determine the set of metadata for a given token that was presented to them by an OAuth Client. This metadata includes whether or not the token is currently active (or if it has expired or otherwise been revoked), what rights of access the token carries (usually conveyed through OAuth 2.0 scopes), and the authorization context in which the token was granted (including who authorized the token and which client it was issued to). Token introspection allows a protected resource to query this information regardless of whether or not it is carried in the token itself, allowing this method to be used along with or independently of structured token values.
6. Now you should be able to see the access token information as seen below, as long as the provided access token is valid.

![WSO2 OAuth2 Playground ~ Token Info]

Running the application (with PKCE)

1. Visit the URL `http://wso2is.local:8080/playground2/oauth2.jsp` to start the application.
2. Enter the following details and click **Authorize**.

   - **Authorization Grant Type**: Authorization Code
   - **Client ID**: (the client id received at the application registration)
   - **Callback URL**: `http://wso2is.local:8080/playground2/oauth2client`
   - **Authorize Endpoint**: `https://localhost:9443/oauth2/authorize`
   - **Use PKCE**: Yes
   - **PKCE Challenge Method**:

![WSO2 OAuth2 Playground](Image)
3. Log in with the user credentials.

![Sign In Form]

4. Click Approve to consent to this action.

![Authorize Form]

5. Provide the following details and click on Get Access Token.

   Callback URL: http://wso2is.local:8080/playground2/oauth2client
   Access Token Endpoint: https://localhost:9443/oauth2/token
   Client Secret: (client secret received at the application registration)
   PKCE Verifier: (this will be populated using the value generated in step 1)

   ! If you have configured the service provider in a tenant, you have to add the tenant domain as a query parameter to the access token endpoint.

   If the tenant domain is wso2.com, access token endpoint will be as follows.

6. At this point, the application receives the Access Token. Enter the introspection endpoint (i.e., https://localhost:9443/oauth2/introspect) and click Get TokenInfo to get the token information.

OAuth 2.0 Token Introspection defines a protocol that allows authorized protected resources to query the authorization server to determine the set of metadata for a given token that was presented to them by an OAuth Client. This metadata includes whether or not the token is currently active (or if it has expired or otherwise been revoked), what rights of access the token carries (usually conveyed through OAuth 2.0 scopes), and the authorization context in which the token was granted (including who authorized the token and which client it was issued to). Token introspection allows a protected resource to query this information regardless of whether or not it is carried in the token itself, allowing this method to be used along with or independently of structured token values.
7. Now you should be able to see the access token information as seen below, as long as the provided access token is valid.

![WSO2 OAuth2 Playground ~ Token Info](image)

**Related Topics**

- See [Invoke the OAuth Introspection Endpoint](#) to invoke the OAuth introspection endpoint using cURL commands.
- See [Mitigating Authorization Code Interception Attacks](#) for more information about using PKCE with an OAuth application.