OAuth 2.0 Client Registration for the Authorization Code Grant Type

Minimum requirements are `SAP_BASIS 7.40 SP02 & SAP_GWFND 7.40 SP02` for using OAuth 2.0 authorization code grant type.

For using OAuth 2.0 authorization code grant type, an OAuth 2.0 Client must be registered in the AS ABAP and configured with the corresponding authentication method. Two steps will be executed there. Firstly a service user needs to be created. It is required to execute e.g. Access Token requests. Secondly the required OAuth 2.0 Client data needs to be defined. In this example, how to configure one OAuth 2.0 client `LEAVEAPP` is demonstrated.

Table of Contents:

- Create a service user for the OAuth 2.0 Client
- Register the new OAuth 2.0 Client ID with the creation wizard

Create a service user for the OAuth 2.0 Client

The OAuth 2.0 Client ID must be identical with the username the OAuth 2.0 client uses for login when requesting an Access Token. Therefore as a prerequisite a user with the name `LEAVEAPP` must exist in the system that will be used by the Leave-Request-Application client.

1. Start transaction `SU01`
   Enter the user name for the OAuth 2.0 client's service user e.g. `LEAVEAPP`.
   Choose `Create` or press F8.

2. Make sure that the tab `Address` is selected and enter a last name, e.g. `LEAVEAPP`.

3. Switch to the tab `Logon Data` and choose `User Type System`.

4. In the `Password` section choose `Generate`.

5. The system will generate a password for the user and display it in the message section.
   Copy the displayed password and use it in the configuration of your Client Application.

6. As last step of the OAuth 2.0 Client's service user configuration choose `Save`.
   You can then leave transaction `SU01`.

As a result the OAuth 2.0 Client's service user is completely configured.

Register the new OAuth 2.0 Client ID with the creation wizard

To register a new OAuth 2.0 client start transaction `SOAUTH2`. The transaction will display an overview about the OAuth 2.0 clients that were already registered. Choose `Create` to start the wizard for the new leave request application client `LEAVEAPP`. 
1. On the first wizard screen enter LEAVEAPP
   P in the field OAuth 2.0 Client ID.

   This identifier must be identical to
   the name of the service user
   created in the prerequisite step.

2. Enter a short Description for this OAuth
   2.0 Client, e.g. Leave Request Application.
   If required adjust the value in the field Token
   Lifetime.

   The default Token Lifetime of
   issued Access Tokens is one hour
   (3600s). For security reasons you
   can shorten the Token Lifetime.

   Choose Next to switch to the Client
   Authentication Details screen.

3. Define the OAuth 2.0 Client Authentication
   Details
   Keep the selected default values.

   When you activate the option
   "Client User Id & Password", the
   requests to the AS ABAP's OAuth
   2.0 Token Endpoint must contain
   username and password. The
   server requires an HTTP
   Authorization Header containing
   the username LEAVEAPP and
   password.

   You can also allow that the OAuth
   2.0 Client authenticates with an
   SSL Client certificate during the
   SSL handshake.

   Choose Next to switch to the Resource
   Owner Authentication Details screen.
4. Define the Resource Owner Authentication Details
To allow Resource Owner authentication with authorization code grand, make sure that the checkbox “Grant Type Authorization Code Active” is selected.
Enter the redirect url of LEAVEAPP OAuth client in the Redirect URI input field. Choose Next to switch to the Scope Assignment screen.

5. Assign the following two scopes to the OAuth 2.0 Client LEAVEAPP:
- ZLEAVEREQUEST_0001
- ZLEAVEREQUESTAPPR_0001

You can get an overview about available OAuth 2.0 Scope IDs with the F4-Help.

During validation of the Access Token Request the AS ABAP will check if the requested scopes are assigned both to the client and to the resource owner. Access requests to any OAuth 2.0 Scope that is not assigned to both client and resource owner will be denied.

Choose Next to switch to the OAuth 2.0 Client Summary.

6. Check the OAuth 2.0 Client Summary once again and choose Finish.

As a result the OAuth 2.0 Client is completely configured for using authorization code grand type.