



Chapter 5

Exchange Authorization Code for Access Token

from Single Sign-On Integration (SSO) Guide

Published on
Jun 14, 2021 10:54AM

Last modified
Feb 17, 2022 10:40AM



ADP Copyright Information

ADP, the ADP logo, and Always Designing for People are trademarks of ADP, Inc.

Windows is a registered trademark of the Microsoft Corporation.

All other trademarks are the property of their respective owners.

Copyright © 2022 ADP, Inc. ADP Proprietary and Confidential - All Rights Reserved. These materials may not be reproduced in any format without the express written permission of ADP, Inc.

These materials may not be reproduced in any format without the express written permission of ADP, Inc. ADP provides this publication "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. ADP is not responsible for any technical inaccuracies or typographical errors which may be contained in this publication. Changes are periodically made to the information herein, and such changes will be incorporated in new editions of this publication. ADP may make improvements and/or changes in the product and/or the programmes described in this publication.

Published on
Jun 14, 2021 10:54AM

Last modified
Feb 17, 2022 10:40AM



Chapter Contents

Chapter 5

Exchange Authorization Code for Access Token

Exchange Authorization Code for Access Token

The response to your authentication request includes a code parameter, a one-time authorization code that your server can exchange for an access token. Your server makes this exchange by sending an HTTPS POST request. The POST request is sent to the token endpoint.

The request must include the following body within the POST request for the ADP access_token:

Header	Query Parameter	Description
	grant_type	REQUIRED. The grant_type parameter must be set to the value "authorization_code".
	code	REQUIRED. The code parameter must be set to the value returned by the ADP Authorization Service in the authorization response.
	redirect_uri	REQUIRED. The redirect_uri parameter must be set to value provided during the registration of the consumer application. This value must be provided in URL encoded format and use the HTTPS protocol.
client_id		REQUIRED. The client_id parameter is the consumer application's account identifier. In general, the consumer application should use the HTTP Authorization header to pass the client_id and the client_secret parameters via Basic Authentication.
client_secret		REQUIRED. The client_secret parameter is the consumer application's account secret. In general, the consumer application should use the HTTP Authorization header to pass the client_id and the client_secret parameters via Basic Authentication.

Your consumer application must send the request with the X.509 certificate provided during registration.

In general, your consumer application should provide the authentication credentials using the HTTP Basic authentication scheme (or other designated scheme) and provide the HTTP Authorization header in the access token request. The consumer application's client_id and client_secret must be provided as required by IETF RFC 2617 - the string : encoded in base 64 where client_id and client_secret are the values assigned to the consumer application during registration (or secret reset).

Your consumer application must pass all parameters in an URL encoded format with UTF-8 character encoding as specified by the HTTP header:

```
Content-Type: application/x-www-form-urlencoded
```

The actual request might look like the following example

(line breaks and spaces added for readability):

```
POST /auth/oauth/v2/token HTTP/1.1
Host: accounts.adp.com
Authorization: Basic QURQVGFiGV0OnRoZXRhYmxldHBhc3N3b3Jk
Content-Type: application/x-www-form-urlencoded
Body: code=d7289a844107481dbf6a6555de2052e2
&redirect_uri=https%3A%2F%2Fconsumerapp%2Ecom%2Fcallback
&grant_type=authorization_code
```

A successful response to this request contains the following fields in a JSON array:

Parameter	Description
access_token	The access_token parameter is set to the value of the access token issued by the ADP authorization service in exchange for the authorization

	code.
token_type	Identifies the type of token returned. At this time, this field always has the value Bearer.
expires_in	The expires_in parameter is set to the time remaining in the token's life (in seconds). For example, the value "3600" indicates that the access token will expire in one hour.
id_token	A JWT that contains identity information about the user that is digitally signed by ADP.

```
{
  "access_token": "314ec73f-7eb5-4eff-b0d6-6fc2d5508f65"
  "token_type": "Bearer"
  "expires_in": 3600
  "refresh_token": ""
  "scope": "openid"
  "id_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ewogInN1YiI6IChodHRwczovL2FjY291bnRzLmFkcC5jb20vdXNlci9HM1haQUpZSFhFVjZESDFOL0czQjcyQjgxSEdZM0VZ"
  "id_token_type": "urn:ietf:params:oauth:grant-type:jwt-bearer"
}
```