

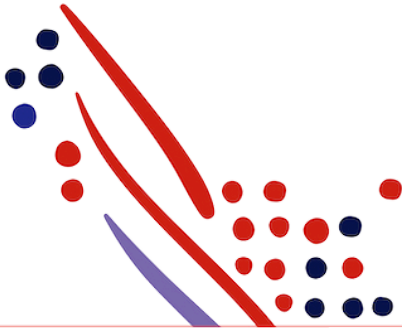
## Chapter 2

# Request an Access Token from ADP

from Understanding the Data Connector App Authorization Process

Published on  
Nov 08, 2019, 04:07 AM

Last modified  
Oct 07, 2024, 03:26 PM



## 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.

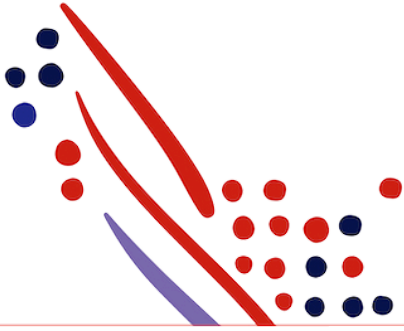
All other trademarks are the property of their respective owners.

Copyright © 2024 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  
Nov 08, 2019, 04:07 AM

Published on  
Oct 07, 2024, 03:26 PM



## Chapter Contents

### Chapter 2

Understanding the Data Connector App Authorization Process

# Request an Access Token from ADP

Your application can request an access token by sending an HTTPS POST request to the token endpoint:  
<https://accounts.adp.com/auth/oauth/v2/token>

The request must include the following parameters in the POST body:

Parameter	Description
grant_type	REQUIRED. Must be set to the value "client_credentials".
client_id	REQUIRED. The consumer application's account identifier, assigned during account registration or at secret reset.
client_secret	REQUIRED. The consumer application's account password, assigned during account registration or at secret reset.

In general, your consumer application should pass the `client_id` and `client_secret` parameters in the HTTP Authorization header using the HTTP Basic authentication scheme (or other designated scheme). The `client_id` and `client_secret` must be separated by a single colon (":") character and encoded within a base64-encoded string, as required by IETF RFC 2617.

Your consumer application must:

- Send the request with the X.509 certificate provided during registration.
- Pass all parameters in a 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:

```
POST /auth/oauth/v2/token HTTP/1.1
Host: accounts.adp.com
Authorization: Basic QURQVGFiGV0OnRoZXRhYmxldHBhc3N3b3Jk
Content-Type: application/x-www-form-urlencoded
grant_type=client_credentials
```

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

Parameter	Description
access_token	The <code>access_token</code> 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 <code>expires_in</code> 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.