

Chapter 2

Prerequisites

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.

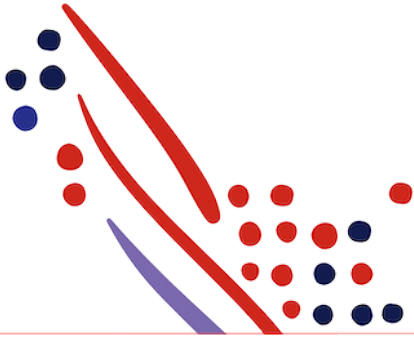
All other trademarks are the property of their respective owners.

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 2

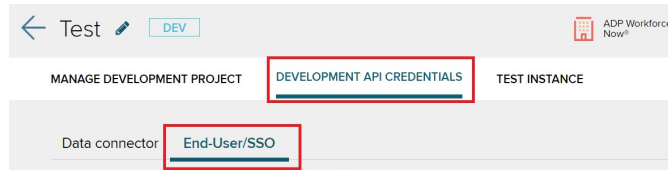
Prerequisites

Chapter 2

Prerequisites

You must obtain the following from [ADP Self Service tool](#) in order to implement OpenID Connect with ADP:

- Signed Certificate
The [ADP Self Service tool](#) allows partners to request a Mutual SSL certificate, that is required for **all calls exchanged with ADP API Gateway - [api.adp.com](#) OR [accounts.adp.com](#)**
- Partner SSO Credentials (End User/SSO Credentials) which can be found by going to:
 1. [ADP Self Service Tool](#) and logging in with your partner credentials
 2. Click on your project
 3. Click on "Development API Credentials" then click on "End-User app/SSO"



4. Under Step 2 "Obtain your access token" You will see the Client ID and Client Secret that will need to be used when integrating with SSO.

Obtain access token

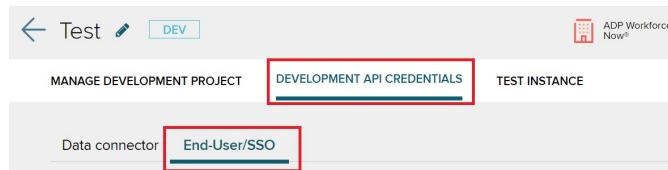
Use these credentials to exchange authorization code from step 1 for access token

1. Your credentials SHOW SECRET

✓ Client ID
a891 COPY

✓ Client Secret COPY REGENERATE

- SSO Redirect URL which can both be found and updated by going to:
 1. [ADP Self Service Tool](#) and logging in with your partner credentials
 2. Click on your project
 3. Click on "Development API Credentials" then click on "End-user app/SSO"



4. Under Step 1 "Provided redirect URI for you app" you can view and update your Redirect URI (Note only "https" is supported)

Provide redirect URI of your app.

End-user logs in to ADP from your app and provides one-time consent, and ADP will send the user back to your supplied app redirect URI (see below) with an authorization code.

Since ADP is the identity provider for your end-user consumer application, please provide an app redirect URI to indicate where to send user after successful login.

⚠ You must update the app redirect URI when you switch environments prior to going live

App redirect URI

UPDATE REDIRECT

Using localhost is acceptable while app is in development.

If you are targeting more than one SOR/ADP platform you will need to add a product identifier so your application knows which partner SSO credentials to use when calling the **userinfo** API

- **Example:** <https://adppartner.com/adp/callback?productId=RUN>