Chapter 1

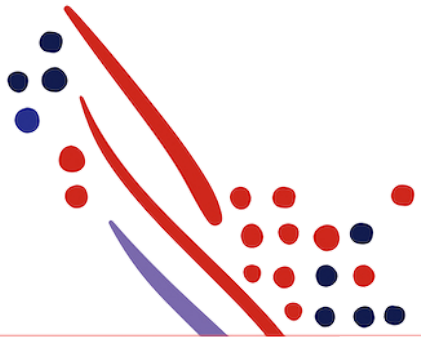
# Introduction

## from Single Sign-On Integration (SSO) Guide

Published on
Jun 14, 2021 10:54AM

Last modified
Feb 17, 2022 10:40AM

Always Designing for People™

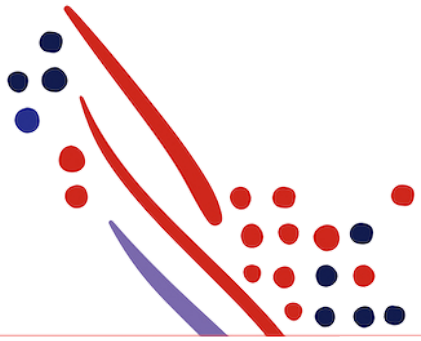


# ADP Copyright Information



Published on
Jun 14, 2021 10:54AM

Last modified
Feb 17, 2022 10:40AM



# Chapter Contents

Chapter 1

# Introduction

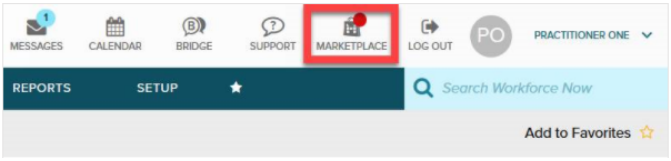
## Overview

Integrating ADP Marketplace partner applications with ADP® single sign-on (SSO) is **required** for both **data connector and core applications**, as it helps clients get seamless activation and instant access to applications immediately upon subscribing. In this approach, ADP is the openID provider for partner applications.

ADP clients expect SSO integration between ADP and partner applications. SSO helps them switch back and forth between their ADP platform (e.g., ADP Workforce Now®, RUN Powered by ADP® or ADP Vantage HCM®) and partners' applications. When clients have more than one solution from ADP Marketplace, SSO integration enables them to use multiple applications with one set of credentials.

When clients are logged into their ADP application, they can access their purchased partner applications through SSO by clicking the shopping bag icon as shown below.

**ADP Workforce Now, ADP Vantage HCM and RUN Powered by ADP (RUN)**




There are many use cases — like employee scheduling, adding a new worker to ADP, time and labor management, or general deductions integrations — in which clients will have to switch back and forth between ADP and partner applications. In these scenarios, clients expect SSO, so they do not have to maintain multiple credentials or continuously sign into different applications.

1. 
   - **In the case of work schedules:** A client makes job, time-off or other changes in their ADP application and would like to run the scheduling from the partner application while they are in session with the ADP application as well.
   - **In the case of time and labor management:** A partner's application will send the time and rate from their application for payroll processing. Then, the client will have to sign into their ADP platform for payroll processing. If there are errors in the payroll processing, they will have to switch back and forth between the applications. There could also be cases where the client has to process multiple batches of payroll, which require sending data back and forth between ADP and the partner's application. Some of the situations where practitioners will need to switch between a partner application and ADP as it relates to time partners include:
     - If payroll is rejected.
     - If out-of-sync information causes errors when importing time information into ADP.
       - An employee's pay cycle can change and cause an error in the timesheet import (e.g., weekly to biweekly)
       - Department changes
     - Processing off-cycle payroll.
     - Processing payroll in batches.
     - Other errors or exceptions.
       - It is not possible for partners to account for all exceptions and typically only a generic error message is displayed. Practitioners will need to go into their ADP application for further details.

## Approach

**Minimum requirement:** Clients should be able to access your application via SSO by logging into ADP Marketplace and clicking the app listing from the My apps section of their account. This is best suited for partners who are listing only the data connector (+ referral listing) in the storefront.

If you are listing your core solution (+ integration) on ADP Marketplace, adding the following optional items to your solutions will enhance users' experience:

- Introducing ADP sign-in button and SSO in your application's login page.
- Enabling ADP SSO in your solution's mobile apps.

## SSO Technologies

In ADP's SSO, the **authentication** aspect deals with validating the client's employee credentials and establishing their identity with ADP. The **authorization** aspect deals with access restrictions with respect to which APIs the user can access. ADP's SSO uses OpenID Connect for authentication and oAuth 2.0 for authorization.

**IMPORTANT:** ADP requires, at a minimum, TLS v1.2 for all secure and encrypted communication. Please ensure your application has been configured to use this if you encounter issues around establishing a connection.

## ADP Libraries

ADP provides software libraries for SSO integration for technologies such as Java, Python, PHP, Ruby, Node.js and.NET. ADP recommends using software libraries to help you quickly ramp up your SSO integration and keep up with future changes.

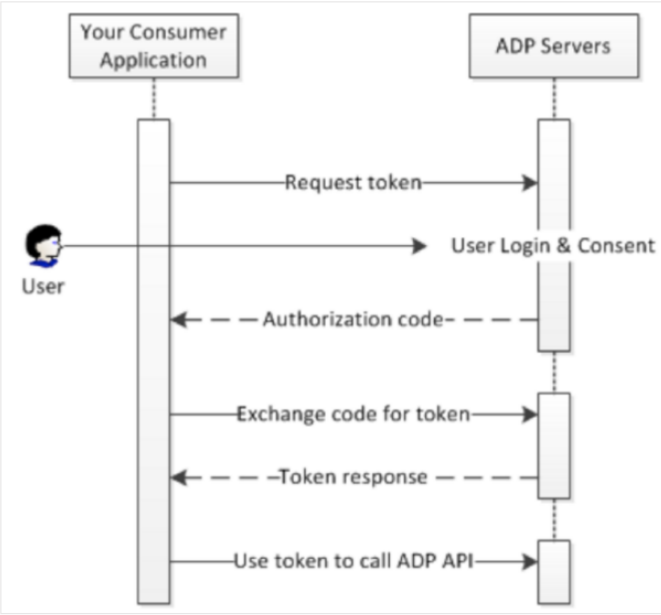
Here is the URL for software libraries: https://developers.adp.com/articles/guides/all/devlib/devlib

You should select only the library for **End User Application** for your relevant technology from the above URL. Note that the software libraries already contain test credentials, test certificates and SSO endpoints to the test environment, which will help you quickly develop and test your integrations. But, you will have to change credentials, certificates and SSO endpoints in the software libraries for the production environment.

Details about the production environment endpoints are included in the documentation for End User App Authorization. You should use the consumer application credentials and SSL certificates from ADP to implement the code with the production endpoints.

## Single Sign-On Flow

The below diagram illustrates the flow of steps between the user, partner application (consumer application) and ADP servers.




**Note:** *SSO tokens are unique per user and should be stored separately.*

## OpenID Connect Endpoints

The ADP endpoints involved in the OpenID Connect protocol are described below.

| Endpoint | URI |
| --- | --- |
| Authorization endpoint | https://accounts.adp.com/auth/oauth/v2/authorize |
| Token endpoint | https://accounts.adp.com/auth/oauth/v2/token |
| Userinfo endpoint | https://api.adp.com/core/v1/userinfo |
| Logout endpoint | https://accounts.adp.com/auth/oauth/v2/logout |

## Info

**Postman Collection**
To accompany this document is a Postman Collection to use when Testing SSO as outlined in Chapter 10. Click on **SSO Test Postman Collection** to download the collection.