ADP Federated Single Sign On Mobile Integration Guide

Contents

Overview of Federation with ADP

The term federation in this guide denotes the establishment of a trusted and legal relationship between ADP and your organization to exchange identity and authentication information between the two organizations. Federated single sign-on with ADP is a mechanism by which your organization conveys to ADP that the employee has in fact authenticated and does not require their ADP-issued user ID and password to access the ADP services your organization has purchased.

Security Information

ADP takes the security of your organization's data very seriously and takes adequate steps to protect your information. ADP uses the OpenID Connect federation method to secure the person immutable ID exchange between your organization and ADP to allow federated access.

Your organization is responsible for authenticating and asserting the authentication and identity of your users. ADP is responsible for providing access to ADP's protected resources for your authorized users. Using the OASIS SAML terminology, your organization is the identity provider (IDP) and ADP is the service provider (SP).

Note: The term "your organization" includes any third-party provider that you may engage in the federation with ADP.

Federated Access on ADP Mobile

ADP will soon be piloting the Federated SSO process to offer simplified access to your employees on the ADP Mobile App. Your employees use their ADP Mobile App to sign on with your organization's login user ID and password to access their ADP services.

Your organization's identity system (Okta®) certifies that authentication and the user identity by sending a signed Oauth assertion to ADP. ADP validates that the assertion is from your organization (identity provider) and, on this basis, authorizes the user to access the requested ADP service. The key here is that your organization – not ADP – authenticates and certifies the identity of the user (your employee).

Note: ADP does not support federated access for administrators/practitioners.

Implementation Process

Your organization and ADP will work together to complete the implementation process. The timeframe to complete the implementation process will vary depending on your organization's set up and time to update the configuration information on ADP Federated SSO website. Your ADP representative will assist as needed.

Before You Begin: Your ADP representative provides this mobile federation integration guide to your administrator.

1. Your administrator logs on to ADP Federated SSO website to configure the setup – Enable Mobile Federation and copy the ADP Mobile Federation URL.
2. Your administrator logs on to your identity provider environment and configures the ADP Mobile Federation URL to allow federated access on the ADP Mobile App.
3. Your administrator logs on to ADP Federated SSO website, updates the identity provider information, and completes ADP setup.
4. Your ADP representative verifies your setup and notifies your administrator to test federated access for your organization on ADP Mobile App.
5. On your identity provider environment, your administrator assigns the federated ADP mobile application to few employees to test federated access.
6. Your employees access the ADP mobile app and sign on with our organization's credentials to access their ADP service. This confirms a successful test.
7. On confirmation of a successful test, your administrator assigns the federated ADP mobile application to your employees to roll out this feature.

Configure Your Federation

Determine the Person Immutable ID (PID)

ADP requires that you designate a Person Immutable ID (PID) to uniquely recognize each employee in your organization's authentication server/system. Your organization should not reuse this value for other employees. This value must be between 1 and 36 ASCII characters and contain English letters and numbers.

Note: If you want to use Employee ID, employees' names, phone numbers or email addresses as part of the Person immutable ID, you must ensure that the resulting PIDs are immutable.

Configure OpenID

Your administrator configures your OpenID setup for the federation with ADP:

1. Setup your OpenID configuration (instancebaseurl/.well-known/openid-configuration) to include the following values:
   - "scopes_supported":["openid,"profile","offline_access"]
   - "response_types_supported":["code"]
   - "response_modes_supported":["query"]
2. Configure your ADP Mobile App on Okta to include the following values:

   "grant_types_supported":["authorization_code","refresh_token"]

Configure Your Identity Provider- Okta

Your administrator configures your Identity Provider environment:

1. Log on to your identity provider environment as an administrator.
2. Select Add Applications. See Step.
3. Select Create New App. See Step.
   1. Select "Web" Platform & "OpenID Connect" Sign on method. See Step.
   2. Enters the login redirect URIs available on the site. See Step.
   3. Click Edit, Select the Refresh Token, and Save. See Step.
   4. Copy the Client ID and Client Secret and include it in the Federation integration Questionnaire. See Step.

5. Go to the Sign On Tab. Copy the Audience and Issuer information and include it in the Federation Integration Questionnaire. See Step.

4. Go to Directory > Profile Editor and select the ADP Mobile Access User profile editor and configure the ADP App profile for the PersonID attribute.
Note: Select Add Attribute to add the PersonID attribute, if not included in the App profile. See Step.

5. Select the Map Attributes option and complete the mapping:
    1. Map the Employee Number to the PersonID attribute. See Step.
    2. On the Okta to ADP Mobile Access tab, complete the mapping. See Step.

6. Assign few users to the ADP Mobile App to test federated access. See Step.
Upon successful test, complete user/group assignment to the ADP Mobile Access application on Okta. See Step.

Configure Your Identity Provider- Microsoft® Azure

Your administrator configures your Identity Provider environment:

1. Log on to your identity provider environment as an administrator.

2. Select App Registrations and add a new application registration. See Step.

3. Select Create New App.
    1. Select "Web app/ API". See Step.
    2. Enters the login redirect URIs available on the site. See Step.
    3. Create client secret. Copy the client secret right away. See Step.
    4. Copy the Client ID and App ID URL (also audience). See Step.
    5. Enter the well known API open ID configuration URL.
    6. Enter the PersonImmutableID attribute.

4. Assign few users to the ADP Mobile App to test federated access.
Upon successful test, complete user/group assignment to the ADP Mobile Access application on Microsoft® Azure.

Employee Experience

Once your employees are successfully assigned to the ADP Mobile Access application in your identity provider, your organization can rollout mobile federated experience to your employees.

Employees download the free app from the Apple® App Store, or Google® Play. Your employees use their ADP Mobile App to sign on with your organization's network login user ID and password to access their ADP services.

View the Employee experience video.