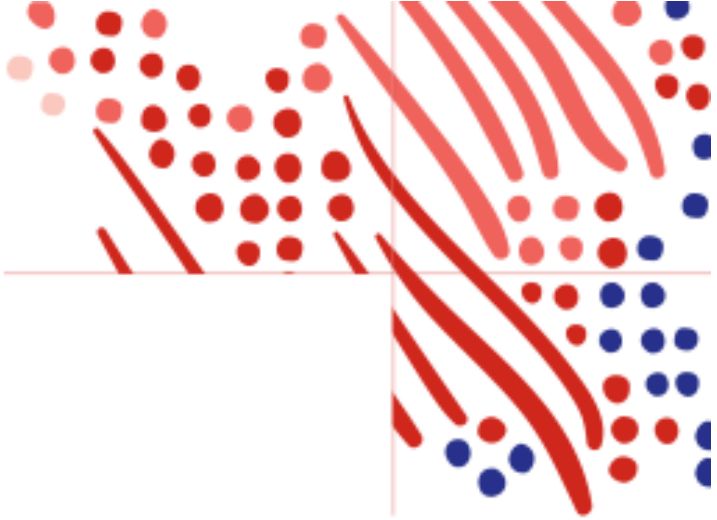


ADP Federated Single Sign On

Web Integration Guide v3.3.2

Always Designing for People™

Contents

Overview of Federation with ADP

In this guide, the term "Federation" 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 employees have in fact authenticated and do not require their ADP-issued user ID and password to access the ADP services your organization has purchased.

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

Security Information

ADP takes the security of your organization's data very seriously and takes adequate steps to protect your information. ADP uses the Security Assertions Markup Language (SAML 2.0), an XML-based framework, to secure the Person Immutable ID (PID) 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. Your organization is the identity provider (IdP), and ADP is the service provider (SP).

Accessing Your ADP Service

Your organization must determine the method your employees use to access your ADP services (for example, direct, federated, or dual - both direct and federated access). Use the information in this section to select the access that meets your organization's requirements.

Federated Access

Federated web access is an IdP-initiated sign in, and only allows your employees to access the ADP web from your identity provider.

Federated mobile access is an SP-initiated sign in from within the ADP Mobile application.

Direct Access

Direct access allows your employees to access your ADP service website from any location (inside or outside of your **organization's** network) and from any device, such as a work computer, home computer, or a kiosk with an internet connection. Using an Internet browser, your employees can access your ADP service website and sign on with their ADP-issued user ID and password. Your administrators and practitioners can sign on with their ADP-issued user ID and password and can perform administrative tasks.

Dual Access

Dual access is the combination of direct and federated access. Your federated employees can register for an ADP service account to establish their direct access. Alternately, your administrator can provision employees with direct access to set up federated access.

Terminated Employees

Terminated employees can be issued a personal registration code. This enables them to connect with ADP after their termination using an ADP-issued user ID and password. Alternatively, there is a verification process to access pay and W2 information without having ADP issued credentials.

User Provisioning

Before going thru the configuration guide please determine your approach for provisioning users. ADP requires a 'Person Immutable ID (PID)' to identify the user.

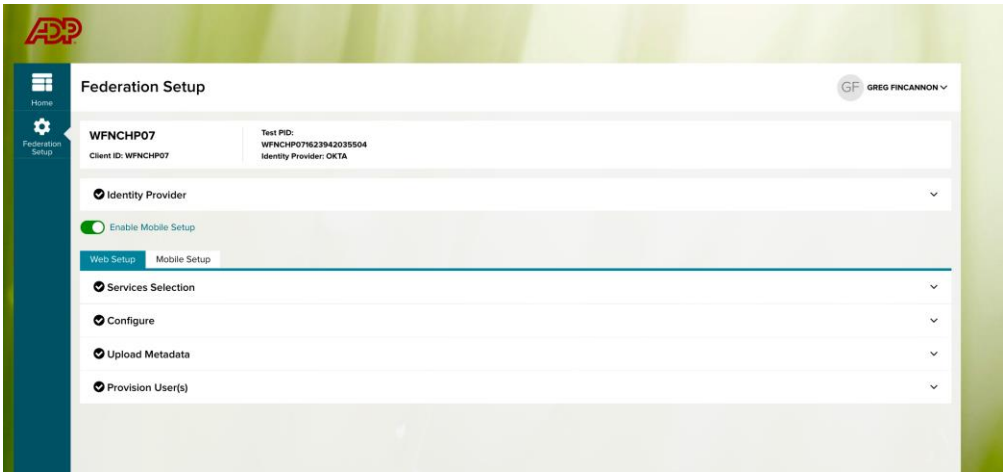
- **EMEA clients**, please setup the PID using the ADP application that manages the users. (e.g. Global MyView Admin Console.)
- *For MAS (Majors) clients, the preference is to use the Associate ID as the PID. Alternatively, you can assign a PID that uniquely recognizes each* employee *in your organization's authentication server/system. Your organization should not reuse this value for other employees.*
- *For NAS (Nationals) clients, the only option is to use the Employee/Associate ID as the PID.*
- All others please *contact ADP Support for other options.*

Configuration Steps

Your organization and ADP will work together to complete the implementation process. The timeframe to complete the process will vary depending on your organization's setup and the submission of required information to ADP. Your ADP representative will assist you as needed.

You, or someone on behalf of your organization, must have administrative access to your Identity Provider to perform some of the steps on this guide.

Below are the configuration steps to complete a new client web federation setup:



1. Contact your ADP representative so they can perform the initial setup, including granting you access to the ADP Federated SSO site.

2. Sign into the ADP Federated SSO site (https://identityfederation.adp.com/)
3. Select your Identity Provider. ADP supports preconfigured setups for selected IdP partners.
   Notes:
   - *For NAS clients, you can select "Other not listed identity provider" if your IdP is not displayed.*
   - *The "Other not listed identity provider" option is not supported in MAS.*
   - *For EMEA clients there will be one option "Standard Identity Provider".*

4. Select the ADP Services that you want to configure for SSO.

5. Complete the information in the **Configure** section. The steps in this section will vary depending on your selections in steps 3 and 4.

6. After completing your IdP setup, click **Next**.
   Note: most IdPs have an ADP application listed in their catalog. Please search for this application and follow the IDP's setup instructions.

7. On the **Upload Certificate** tab, click **Browse** and select your IdP's metadata file.
   Note: When your certificate expires in the future, use the Upload Certificate feature to renew it.

8. Click **Upload.** When the upload is completed, the **Federated Issuer Key** field will be updated, and the new certificate appears in the **Latest Uploaded Certificate** list with status **Active**.
   Notes:
   - *Your certificate will be immediately available in the ADP production servers.*
   - *You will not be able to make further changes to the* ***Federated Issuer Key*** *(AKA "Issuer URL"). However, you can update a certificate as many times as needed.*

9. Handshake step: Handshake is verification process to help verify that your IdP setup is configured as per ADP requirements.
   Notes:
   - *Handshake will only appear if you are using "Other not listed identity provider", ADFS, or "Standard Identity Provider" for EMEA clients.*
   - *Please update the Test PersonImmutableID to match the account of the test user.*

10. You can now test with a few employee users in your company. To begin the test, click **Provision User(s)**.

    For *NAS (Nationals) clients* please contact your implementation representation to complete this step.

11. Provision Users:
    - **EMEA clients**, please setup the PID using the ADP application that manages the users. (e.g. Global MyView Admin Console.)
    - ***All others****, ADP can assign a unique PID to a federation account using the Employee ID/Associate ID as the PID.*

    Notes:
    - *For MAS (Majors) clients, the preference is to use the Associate ID as the PID. Alternatively, you can assign a PID that uniquely recognizes each* employee *in your*

organization's authentication server/system. Your organization should not reuse this value for other employees.

- *For NAS (Nationals) clients, the only option is to use the Employee/Associate ID as the PID.*

1. **Using Employee ID/WFN Associate ID as Person Immutable ID – Automatic setup**
   - Depending on the number of users to be provisioned, automatic setup may happen overnight to avoid performance impacts. If your organization has less than 1000 users to be provisioned, the process will start immediately.
     Note: Please be aware that the process may take several hours to complete. You can safely close the app and return later to view the status.
   - Once the process finishes, you will see the provisioning results, with an end time, total users processed, and number of successes and failures.

Next Steps

Enabling Mobile SSO for your client

If your Identity Provider is Okta or Azure, you can also enable Mobile SSO using OIDC which will allow access your company credentials.

ADP offers detailed steps for you to complete your Mobile SSO configuration.

Enabling administrative access for your users

Important: as mandated by the ADP Global Security Office (GSO), organizations requiring federated access to administrators at the ADP services must support Multi-factor Authentication (MFA) on the Identity Provider side and every administrator must be authenticated via MFA prior to the federation connection.

After **your** client has successfully completed the setup and your users need administrative access to at least one of the assigned ADP services please reach out to your ADP representative.

Enabling users to use federated only access

In order to restrict your users from accessing ADP systems with a password account and require federated single sign on please reach out to your ADP representative.

Note, this option will not remove existing password accounts (Please contact your ADP representative for to remove the existing password accounts). Terminated users have the option of receiving a direct account.

Appendix

Enabling multiple ADP services to your SSO connection

Okta

To configure more than one ADP service with Okta, in case the service needed is not pre-configured, follow the steps below.

Assemble the ADP service Okta URL

1. View the ADP connection meta data and select the 'HTTP-POST' location.
    a. Ex: <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://abc.okta.com/app/adp/exk58v1rvvmmFB47G5d7/sso/saml"/>
2. Append the RelayState query parameter
    a. Ex: https://abc.okta.com/app/adp/exk58v1rvvmmFB47G5d7/sso/saml?RelayState=ADMWFN

Create the additional app in Okta

After creating the ADP service Okta URL, follow and complete the steps available in this document: https://support.okta.com/help/s/article/How-do-you-create-a-bookmark-app?language=en_US

In step #2, in which the **URL** is required, use the ADP service Okta URL mounted in the step above.

Steps to test the connection in Okta are also available in the document linked above.

Microsoft Azure

Mount the ADP service Azure URL

1. Log into your MS Azure instance and select the ADP app.
2. In the ADP app, click the "**Get started"** link in the **"2. Set up single sign on"**.

3. On the left side menu, click "**Properties"** and copy the "**User access URL"** to a text file.
    a. **Important**: this is going to be the base of the access URL for the ADP services we need access to.
4. Append to the copied URL **"&relaystate=" plus the value of the ADP URL** provided in the instructions step during setup or by the ADP rep.
    a. Note the "**&"** (and sign) and the "**r"** and "**s"** in lower case.

Important: note you need to create one URL per extra ADP service selected during the setup process.

Create the additional app in MS Azure

1. In the header menu, click on "**Enterprise applications"**
2. In Enterprise applications, click "**New application"**
3. Search for the ADP app and click on the ADP app returned.
4. In the side panel, add the name of the new app (e.g.: ADP WFN (Workforce Now) admin) and click **"Create".**
5. Select the newly created app and select "**Properties"** in the left side menu.
6. Click the "**Get started"** link in the **"2. Set up single sign on"**.
7. In the new view, click the **"Linked"** tab.
8. Add the ADP service Azure URL mounted in the process above to the **"Sign on URL"** and save.
9. Set up user and app configs as needed.

10. MS Azure takes a few minutes to refresh the apps. After this, go to your app dashboard and the newly created app should be available.

Please note that you can test the Azure URL's by hitting them directly using any browser. You should see the ADP page with an error message, indicating that ADP was reached, but since the SAML is missing the user, user will not be found in the process.