ADP Federated Single Sign On Integration Guide v1.4







Table of Contents

Overview of Federation with ADP	4
Security Information	4
Methods of Access	4
Unique Identifier for Federated SSO Access	4
Federated Access	5
Direct Access	5
Dual Access	5
Terminated Employee Access	5
Federated Access on ADP Mobile	6
Configuration Steps	7
Protocols supported	7
OAuth/OIDC Federation Setup	7
OAuth/OIDC Identity Providers1	1
OKTA Setup	1
Microsoft Entra ID Setup	3
Ping Federate Setup	9
Finish Setup in ADP Federation Dashboard	4
SAML Federated Setup2	5
User Provisioning for Federated SSO Access2	7
User Deprovisioning for Federated SSO Access	8
Changing PID for Federated SSO Access2	9
Certificate management	0
Enabling Multiple ADP Services to Your SSO Connection	1
ОКТА	1
SAML – Assemble the ADP service Okta URL	1
Create the Additional App in Okta	1



Microsoft Entra ID	32
OIDC – Web Destination link	32
SAML – Mount the ADP service Entra ID URL	32
Create an Additional Application in MS Entra ID	33
Next Steps	5
User Rollout for Mobile and Web	35
Transition from SAML to OAuth/OIDC	35
Enabling Administrative Access for Your Users	35
Enabling Users to Use Federated Only Access	35
Employee Experience	6
Appendix – Options on Syncing Unique Identifier3	7
Appendix – Configuring personId as User Identifier in Okta	9
Appendix – Dashboard Errors	0
Appendix – Authentication Errors	4





Overview of Federation with ADP

In this guide, the term "Federation" denotes the establishment of a trusted and legal relationship between your organization and ADP 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 an 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 steps to protect your information. ADP uses OpenID Connect Authorization Code Flow, to secure a unique identifier 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).

Methods of Access

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 which one meets your organization's requirements.

Unique Identifier for Federated SSO Access

Determine the 'Unique Identifier' that will uniquely identify the user.

- The unique identifier is designated to uniquely recognize each employee in your organization's authentication server/system. ADP recommends using the employee ID/global personnel number/WFN associate ID as the identifier. **Note:** NAS (Nationals) clients must use the employee ID/WFN associate ID as the identifier.
- Your organization must not reuse this value for other employees. This value must be between 1 and 36 ASCII characters and contain English letters and/or numbers.





Unique Identifier Synchronization Options

After determining the value of the unique identifier, decide on an integration method. ADP offers four options to synchronize the unique identifier from ADP to the client identity provider:

- 1. Download the unique identifier using custom reports
- 2. Use ADP Marketplace worker API
- 3. Use ADP Marketplace partner Aquera
- 4. ADP Data bridge sync run a scheduled custom report to pull data and feed into the IDP system via SFTP delivery (Contact your ADP representative for additional information.)

Please reference the <u>Appendix</u> for additional information.

Federated Access

Federated access will allow your employees and administrators to access the ADP web and mobile applications using your IDP credentials.

Federated users do not have a password for their ADP user ID. They should only login via Federation. Any attempt to login to an ADP website using their ADP user ID will fail, and will eventually lock the user account. Users who wish to access ADP sites outside of Federation need to register for a full user ID/password, and will become Dual Access users (noted below).

Direct Access

Direct access allows your employees to access your ADP service website with ADP-issued credentials.

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. Alternatively, your administrator can provision employees with direct access to set up federated access.

Terminated Employee Access

For ADP Americas, 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.

For more information on terminated employee access to pay statements and W2s, please visit Login & Support | ADP iPay | View & Print Pay Stubs, W2, & 1099 Tax Statements.

For ADP International organizations, please contact your ADP representative for available options.





Federated Access on ADP Mobile

ADP enables the Federated SSO process to offer simplified access to your employees on the ADP Mobile App. Your employees use the ADP Mobile App to sign on with your organization's login user ID and password to access their ADP services, if supported by your OIDC-compliant Identity Provider. Please see the Mobile Federation SSO <u>Getting Started Guide for Employees</u> after the federated SSO has been configured.

Disclaimer:

The Screenshots and processes described in this guide are subject to change.





Configuration Steps

Please only proceed once your unique identifier has been decided. If undecided, please review the <u>Federated Unique Identifier</u> section.

Protocols supported

- OAuth/OIDC (Web and Mobile supported with single trust)
- SAML 2.0 (Web only with single trust)

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.

For ADP International organizations, please contact your ADP representative for available options presented in this guide.

OAuth/OIDC Federation Setup

Home VN 1 **Federation Setup** Resources 202 Useful resources to help you View your progress! ew and manage your federation tup progress in one place. Federation Integration Guide User Setur > for administrators Sample Letter to launch easy access to employees >

Below are the configuration steps to complete the OAuth/OIDC federation setup:





1. Sign into the ADP Federated SSO site with your ADP issued credentials

(https://identityfederation.adp.com/)

- 2. Select your Identity Provider.
- 3. Enable OIDC Federation by selecting Enable OIDC Setup.

Æ			
Home	Federation Setup		VN ~
Federation Setup	NAF-1216-1	Client ID:	
User Setup	Identity Provider		~
	OIDC Setup SAML Setup		
	Relying Party Redirect	t URI	
	https://mobifed.adp.com/oauth	/client/v2/bac448e6-3b66-4c7b-a3e4-100000	Pa COPY
	Well-known URL 🕄		
	https://fffffffadmin.o	kta.com/.well-known/openid-configuration	RETRIEVE

- a. Copy the **Relying Party Redirect URI** (to paste this on your identity provider website for the ADP Mobile application).
- b. Create the OAuth/OIDC application at your identity provider.
- c. Enter the **Well-known URL** from your identity provider and select **Retrieve**.
 - i) The Endpoints will be populated from the well-known endpoints.
 - ii) If the Well-known URL is not provided by your identity provider, you must manually enter

your endpoints from your identity provider.





d. Application Details

i) Application Client ID, Audience, Application Client Secret will come from your identity

provider.

ii) The User Identifier should be the name of the attribute of your unique identifier which is

synchronized between ADP and the identity provider.

e. Select Save and Activate Connection

Status of Conr	nection	
ACTIVE	Modified by: GPSPAIMMM2@PSPAIMMM	Date (mm/dd/yyyy): 1/23/2024
		SAVE ACTIVATE CONNECTION
Web Destinati	on Links	
A By using admin	istrator links for user access to ADP products, you if you have further questions.	u are responsible for setting up administrators using multi-factor authentication set at your identity provider. Contact your ADP
	. ,	
ADP Federated Sir	gle Sign On - Admin 🏻 🛍	
ADP Workforce No	w ^a	
ADP Workforce No	w - Admin 🗳	
ADP Workforce No	w Next Generation 🖉	
MyADP 🖄		
- Disable/Enabl	e OIDC Setup	
Disable/Enable	OIDC Setup	
-		

- i) During activate connection a federation provisioned user is required.
 - (1) If a provisioned user doesn't exist yet, then just select Save, then contact your ADP

Representative to provision the Federation Admin or a test user for federation, then

Activate the connection once that provisioning is confirmed.

(2) If the provisioned user is not the Federated Admin, Save and then copy the Activation

Link and provide it to the provisioned user.





- f. Once the connection has been verified, enable the OIDC setup.
- g. Navigate to **Web Destination Links** for user access.
- h. Please see the appendix for identity provider specific setup.
- i. For each service your organization has assigned, there will be a Web Destination Link. Copy this link to setup a bookmark app or embed it in your company's Portal for users to access this ADP

service. Please see the Enabling Multiple ADP Services section.

Note: ADP recommends that you setup a reminder for your organization to renew your secret before the expiration date. Without a valid secret, your employees will not be able to access ADP services.





OAuth/OIDC Identity Providers

ADP has listed identity provider setups. There are additional identity providers not listed and ADP can support any identity provider that supports OAuth 2.0 Authorization Grant Type. Outside these identity providers please check with your ADP representative. ADP is not responsible for the identity provider configurations.

OKTA Setup

- 1. On your identity provider environment, complete the steps below:
 - a. Select Create New App application:
 - a. Sign-in method: OIDC OpenID Connect
 - b. Application type: Web Application
 - b. Select Refresh Token under Grant type.
 - c. Paste Relying Party Redirect URI in Sign-in redirect URIs.
- 2. Copy the following information from your identity provider web site:
 - a. Well known URL for OKTA is the OKTA base URL plus '/.well-known/openid-configuration'.
 - b. Enter either the OKTA base URL, or well-known URL in the Well-known URL field and select

Retrieve.

- i) The Endpoints will be populated from the well-known endpoints.
- ii) Please confirm this is correct.
- iii) ID Token Issuer is from the well- known issuer value.
- c. Application Detail:
 - i) Client ID, Client Secret.
 - ii) Audience

Note: Audience is the labeled Audience in the Okta OIDC App.

iii) User Identifier - personId

Note: User Identifier is the attribute containing the unique identifier that was defined in the ADP Web SSO setup.

d. Additional Information:





- i) Make any adjustments needed for Scopes Requested, Response Type, Response Code.
- 3. Click Save.
- 4. Skip to <u>Finish Setup in ADP Federation Dashboard</u> section.





Microsoft Entra ID Setup

1. Please refer to the Microsoft Entra Tutorial: Microsoft Entra single sign-on (SSO) integration with ADP (OIDC)

Note: You will need to use this document to set up a valid User Info Endpoint and User Identifier on the Federation Dashboard page.

- 2. On your Microsoft Entra Identity provider environment, complete the following steps:
- Home > ADP ADP | App registrations 🛷 10 + New registration 🌐 Endpoints 🤌 Troubleshooting 🖒 Refresh 🞍 Download 💀 Preview features | 🖗 Got feedback? Manage Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more 🚨 Users 🚨 Groups External Identities All applications Owned applications Deleted applications 2. Roles and administrators Administrative units Delegated admin partners 4 applications found III. Enterprise applications Application (client) ID Created on 1 Certificates & secrets Display name 1 Devices III. App registrations Identity Governance
- a. Select App Registrations, then New registration.

- b. Enter Name (such as ADP Mobile Solutions)
- c. For **Redirect URI select 'Web' and paste the Relying Party Redirect URI** copied from the ADP <u>OIDC Setup</u> section into the **Redirect URL** field on your Entra ID.
- d. Select Register.





Register an application

		
Supported accou	nt types	
Who can use this an	plication or acce	ss this ADI?
Accounts in this	organizational di	irectory only (ADP only - Single tenant)
Accounts in any	organizational di	irectory (Any Azure AD directory - Multitenant)
Accounts in any	organizational di	irectory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skyp
Personal Microso	- oft accounts only	
changed later, but a v	alue is required	ise to this UKI after successfully authenticating the user. Providing this now is optional and for most authentication scenarios.
Web	· ·	eig. https://inyapp.com/auti
Web		

- 3. On your new registered app:
 - a. Select **Certificates & Secrets** section under **Manage** and click + **New client secret**.
 - b. Add a description under Add a client secret (optional).
 - c. Select expiration period of your client secret and then click Add.
 - d. Copy the client secret right away to a text document.

Note: Once this client secret expires, you will be required to create a new one and update the ADP Federated SSO website to continue using Mobile SSO.

vays Designing for People*				
Search (Ctrl+/) Search (Ctrl+/) Overview Quickstart Integration assistant (preview) Manage Searchize	Got feedback? Credentials enable confidential applications to identify themselves to the authentication scheme). For a higher level of assurance, we recommend using a certificate (instead of a Certificates Certificates Certificates can be used as secrets to prove the application's identity when requesting a	Add a client secret	Enter a description for this client secret Recommended: 180 days (6 months) Recommended: 180 days (6 months) 90 days (3 months)	×
Branding Authentication Certificates & secrets Token configuration	T Upload certificate Thumbprint Start date		365 days (12 months) 545 days (18 months) 730 days @4 months) Custom	
 API permissions Expose an API Owners Roles and administrators (Preview) Manifest 	Client secrets A secret string that the application uses to prove its identity when requesting a token. A How client secret Description Expires	lsi		
Support + Troubleshooting Image: Troubleshooting New support request	No client secrets have been created for this application.	Add Cancel		
Description	Expires Value ① 2/14/2025 HIBBO~ Apdianation	Secret ID	1-4r41-855a-d00406a6aerr	

e. Click Endpoints in the Overview section.

Home > Enterprise applications Overv ADP Mobile Solution	ew > Enterprise applications > Add an application > Add your own application > App registration	ns >
✓ Search (Ctrl+/) «	🗊 Delete 🌐 Endpoints	
Sverview	Display name : ADP Mobile Solutions - Roberto	
🗳 Quickstart	Application (client) ID : dd1c390f-a398-415f-b144-b9c505a45d67	
🚀 Integration assistant (preview)	Directory (tenant) ID : 91cbb937-bc44-4d89-988e-2f7e9192cb15	
	Object ID : 05f12a18-e411-4004-9bca-945a58dbe1f8	
Manage		*

f. Copy the link under **Open ID Connect metadata document** and paste it in the **Well Known URL** field on the ADP Federation Dashboard.





Endpoints	×
OAuth 2.0 authorization endpoint (v2)	Copy to clipboard
OAuth 2.0 token endpoint (v2)	
	ľ.
OAuth 2.0 authorization endpoint (v1)	
and a second	D
OAuth 2.0 token endpoint (v1)	
OpenID Connect metadata document	
https://login.microsoftonline.com/91cbb937-bc44-4d89-988e-2f7e9192cb15/v2.0/.well-known/openid	configuration
Microsoft Graph API endpoint	
	D
Federation metadata document	
	D
WS-Federation sign-on endpoint	
	D
SAML-P sign-on endpoint	
	Ď
SAML-P sign-out endpoint	
	Ď

- 4. Paste the Well-known URL from your identity provider and select Retrieve.
 - a. The Endpoints will be populated from the well-known endpoints.
 - b. *Please confirm this is correct.*
 - c. ID Token Issuer is from the well-known issuer value.
- 5. Client ID: copy the Application ID from Entra ID

ADP Mobile	\$
	📋 Delete Endpoints
R Overview	↑ Essentials
🗳 Quickstart	Display name : ADP Mobile
🚀 Integration assistant (preview)	Application (client) ID : 1
	Directory (tenant) ID :
Manage	Object ID :





instance base one.		User Info Endpoint: *	
https://login.microsoftonline.com	m/91cbb937-bc44-4d89-988e-2f7e9192cb15/v2.0/.well-known	https://graph.microsoft.com/v1.0/me/?\$select=emplo	byeeld
Authorization Endpoint: *		JWKS Endpoint: *	
https://login.microsoftonline.com/91cbb937-bc44-4d89-988e-2f7e9192cb15/oauth2/v2.0/auth		https://login.microsoftonline.com/91cbb937-bc44-4d89-988e-2f7e9192cb15/discovery/v2.0/ku	
Token Endpoint: *		Revocation Endpoint: *	
https://login.microsoftonline.com	m/91cbb937-bc44-4d89-988e-2f7e9192cb15/oauth2/v2.0/toke	https://login.microsoftonline.com/91cbb937-bc44-4d	189-988e-2f7e9192cb15/oauth2/v2.0/log
id loken issuer.			
https://login.microsoftonline.com	m/91cbb937-bc44-4d89-988e-2f7e9192cb15/v2.0		
https://login.microsoftonline.com	m/91cbb937-bc44-4d89-988e-2f7e9192cb15/v2.0		
https://login.microsoftonline.cor Application Detail Application Client ID: *	n/91cbb937-bc44-4d89-988e-2f7e9192cb15/v2.0	Audience: *	
https://login.microsoftonline.com Application Detail Application Client ID: * fcd4cf02-b397-427c-aa10-bc8e	m/91cbb937-bc44-4d89-988e-2f7e9192cb15/v2.0	Audience: * fcd4cf02-b397-427c-aa10-bc8e25f1c15c	
https://login.microsoftonline.com Application Detail Application Client ID: * fcd4cf02-b397-427c-aa10-bc8e Application Client Secret: *	n/91cbb937-bc44-4d89-988e-2f7e9192cb15/v2.0	Audience: * fcd4cf02-b397-427c-aa10-bc8e25f1c15c User Identifier: *	
https://login.microsoftonline.com Application Detail Application Client ID: * fcd4cf02-b397-427c-aa10-bc8e Application Client Secret: *	m/91cbb937-bc44-4d89-988e-277e9192cb15/v2.0	Audience: * fcd4cf02-b397-427c-aa10-bc8e25ffc15c User Identifier: * employeeld	
https://login.microsoftonline.com Application Detail Application Client ID: * fcd4cf02-b397-427c-aa10-bc8e Application Client Secret: *	m/91cbb937-bc44-4d89-988e-277e9192cb15/v2.0	Audience: * fcd4cf02-b397-427c-aa10-bc8e25f1c15c User Identifier: * employeeld Response Type:	Response Mode:

- a. Audience: Copy the Application ID from Entra ID.
- b. Client Secret: Paste it from step 2d.
- c. Enter a **User Identifier**. This should reference an Entra attribute (such as employeeld or employeeNumber or an Extension Attribute) that contains the Federation Identifier you have chosen.
- d. For the **User Info Endpoint**, construct it based on the user identifier (Unique Identifier) which needs to be used:

User Identifier	User Info Endpoint
userPrincipalName	https://graph.microsoft.com/v1.0/me/?\$select=userPrincipalName
employeeld	https://graph.microsoft.com/v1.0/me/?\$select=employeeId
mail	https://graph.microsoft.com/v1.0/me/?\$select=mail
extensionAttributex	https://graph.microsoft.com/v1.0/me/?\$select=extension_ <applicationid></applicationid>
	_extensionAttributex

Note: If you are using an OnPrem Extension Attribute, your User Info Endpoint should be

<u>http://graph.microsoft.com/v1.0/me/onPremisesExtensionAttributes/extensionAttributex</u> and your User Identifier should be "value".

e. Visit <u>https://developer.microsoft.com/en-us/graph/graph-explorer</u>





- f. Click Sign in to Graph Explorer and enter your credentials
- g. To discover all available attributes that can be mapped as unique identifier, run the following query: <u>https://graph.microsoft.com/v1.0/me/?\$select=*</u>:
- h. Add the following API permission in Entra ID:

API Permissions > Add a permission > Microsoft Graph > Delegated permissions > Expand User >

Select..

User.Read User Read.All User. ReadBasicAll

Once the permissions are added, click on Grant Admin Consent for your tenant button.

Skip to Finish Setup in ADP Federation Dashboard section





Ping Federate Setup

- 1. On your PingFederate identity provider environment, complete below steps:
 - a. Under oAuth server, create one Access Token Management

Ping Federate	
MAIN	AUTHORIZATION SERVER Authorization Server Settings
ි Identity Provider	Scope Management Client Settings
E Service Provider	Client Registration Policies
OAuth Server	GRANT MAPPING IdP Adapter Mapping
SETTINGS	Authentication Policy Contract Mapping Resource Owner Credentials Mapping
	TOKEN MAPPING
le Security	Access Token Management Access Token Mapping
≟ System	OpenID Connect Policy Management
	CIBA
	Authenticators Request Policies

- b. Create Access Token Mapping for the Access Token Management created at step a.
- c. Create an OpenID Connect Policy for the Access Token Management created at step a.
- d. personId should be part of attribute mapping and map Employee number with personId.
- e. Create oAuth client:
 - Enter client id, client name, generate client secret.
 - Enter redirect uri provided by ADP
 - Check the Restrict for Restrict Common Scopes



Ding Eodorato	_	_	
	NAME	ADPMobileclient	
Identity Provider	DESCRIPTION		
Service Provider			.i.
OAuth Server	CLIENT AUTHENTICATION	O NONE	
TTINGS			
Security			
System	CLIENT SECRET	Control Second	
		CHANGE SECRET	
	ALGORITHM	Allow Any	~
OAuth Server	JWKS URL		
ETTINGS			
Security	JWKS		
System	REDIRECT URIS	Redirection URIs 1/client/v2/134767543532432432432432421421	Action Update Cancel
			Add
	LOGO URL		
	BYPASS AUTHORIZATION APPROVAL RESTRICT COMMON SCOPES	Bypass Sestrict	
yright © 2003-2019		Nestrict	

f. Check the openid and profile scope.





- g. Check the following for Allowed Grant Types:
 - Authorization Code
 - Refresh Token
 - Access Token Validation (Client is a Resource Server)
- h. Select Access Token Manager created from step A for the Default Access Token Manager
- i. Select openid connection policy created from step c.

ିଅ Identity Provider	REFRESH TOKEN ROLLING POLICY	Use Global Setting ODon't F	Roll 🔵 Roll
Service Provider	OPENID CONNECT	ID Token Signing Algorithm	
OAuth Server			
	/	ID Token Key Management Encryption A	gorithm
SETTINGS		No Encryption	~
Security		Policy	
⇒ System		····· ·	

- j. Save the client.
- 2. Copy the following information from your identity provider web site:
 - a. Instance Base URL (You can find PingFederate Base URL under Server Configuration -> System settings -> Server Settings -> Roles & Protocols: Enable OpenID Connect as shown below).





Federation Into				
My Base URL				
SAML 2.0 Entity ID				

Select the role(s) and protocol(s) that you intend to use with your federation partners.



Note: Well known URL for Ping is the Ping base URL plus '/.well-known/openidconfiguration'.

- i. Enter either the ping well known URL in the Well-known URL field and select Retrieve.
 - i) The Endpoints will be populated from the well-known endpoints.
 - ii) Please confirm this is correct.
 - iii) ID Token Issuer is from the well-known issuer value.
- j. Application Detail:
 - i) Client ID, Client Secret.
 - ii) Audience
 - iii) User Identifier personId

Note: User Identifier is the attribute containing the unique identifier that was defined in the ADP Web SSO setup.

- k. Additional Information:
 - i) Make any adjustments needed for Scopes Requested, Response Type, Response Code.
 - b. Client ID, Client Secret.
 - c. Audience, ID Token Issuer

Note: Audience is the Client ID of the app in Ping federate. ID Token Issuer is the "Issuer" of Ping IDP.

 Paste the above copied information on the ADP Federated SSO web site -> Mobile Setup -> OIDC Setup section





- On the ADP Federated SSO web site -> Mobile Federation section, complete the remaining steps:
 - a. Enter the type value personId in the User Identifier field. This value is case-sensitive.
 - b. Click Save.
 - c. Click Synchronize to save the configuration information to your production environment.

Note: You will not be able to synchronize until Web setup is complete.

5. Upon successful synchronization, your administrator performs any other pending configs on your identity provider environment to allow federated access on the ADP Mobile App.





Finish Setup in ADP Federation Dashboard

1. Configure the Additional Information section to match this graphic:

Allowed Grant Types:	Scopes Requested:	Response Type:	Response Mode:
Authorization code	OpenID Profile Offline Access	Code ID token	Query O Form post

- 2. Click **Save** to save the configuration.
- 3. Provision one user to create a federation account with the unique identifier.
- 4. Click Activate Connection to verify the connection.
 - a. A new tab will present a sign in with your provider using the provisioned user.
 - b. A confirmation message will be shown.
- 5. Upon successful activation, your administrator configures your identity provider environment to allow federated access to the ADP Mobile App.
- 6. On your identity provider environment, your administrator assigns the federated ADP mobile application to a few employees to test federated access.
- 7. Select the slider button to Enable OID Setup.
 - a. Your employees can now access the ADP mobile app and sign on with our organization's credentials to access their ADP service. This confirms a successful test.
 - b. On confirmation of a successful test, your administrator assigns the federated ADP mobile application to the balance of your employees to roll out this feature.

Note: ADP recommends that you setup a reminder for your organization to renew your certificate before the expiration date. Without a valid certificate, your employees will not be able to access ADP services.





SAML Federated Setup

Please only proceed once your provisioning approach has been decided. If undecided, please review the provisioning users section.

Below are the configuration steps to complete a SAML federated setup.

ÆP					
Home Home				GG	9
Federation Setup	Setup	Resources			
User Setup	our progress! Id manage your federation rogress in one place.	Useful resources to help you Bederation Integration Guide for administrators	>		
	HECK PROGRESS	Sample Letter to launch easy access to employees	>		

- 1. Sign into the ADP Federated SSO site (<u>https://identityfederation.adp.com/</u>)
- 2. Select your Identity Provider. ADP supports preconfigured setups for selected IDP partners.
- 3. Complete the information in the **Configure** section within the **SAML Setup** tab. The steps in this section will vary depending on your selections in steps 3 and 4.
- After completing your IDP setup, click Next.
 Note: Most IDPs have an ADP application listed in their catalog. Please search for the ADP application at the IDP and follow the IDP's setup instructions.
- On the Upload Certificate tab, click Browse and select your IDP's metadata file (this must be an .XML file, not just a certificate).
 Note: When your certificate expires in the future, use the Upload Certificate feature to renew it.
- 6. 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**.





Note: 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.

7. 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.
- 8. You can now test with a few employee users in your company. To begin the test, click **Provision User(s)** under the **User Setup** on the left navigation bar.
 - For NAS (Nationals) clients please contact your implementation representation to complete this step.





User Provisioning for Federated SSO Access

Provision User(s)

Home	User Setup	GF GREG FINCANNON ~
Federation Setup	Gregs SSO client Client ID: gregssofit Identity Provider: OKTA	
**	Provision User(s) Deprovision User(s)	
User Setup	Upload your unique identifier via: O Use employee ID/WFN Associate ID as Person Immutable ID	

- Upload your unique identifier via CSV (may not be available to all clients). CSV is also a good choice if client wishes to limit SSO to a subset of employees.
- It is normal to see some errors on this process. This usually happens for orphan records or some other invalid entry that should not be provisioned. Note: Clients who use Employee ID/WFN Associate ID for provisioning cannot see the error log.
- ADP preferred option: Using Employee ID/WFN Associate ID as Person Immutable ID Automatic setup
 - This configuration will apply to all associates created having an Employee ID/WFN Associate ID.
 - Automatic setup will most likely happen overnight to avoid performance impacts.
 Depending on the number of users to be provisioned, the process may take several hours to complete.
 - Once the process finishes, you will see the provisioning results, with an end time, total users processed, and number of successes and failures.

Note: You can safely close the app and return later to view the status.

Note: This option is available for Americas only.





User Deprovisioning for Federated SSO Access

Deprovision User(s)

Home	User Setup				IC
Federation Setup		Client ID:	ICROSOFT ENTRA ID		
	Provision User(s) Deprovision	User(s) Change PID			
User Setup	Provisioned users are displaye	d and are eligible for deprovision	ning. Non-provisioned users cann	ot be removed.	
	First Name	Last Name	Employee ID/Ass	ociate ID	
	Enter full first name	Enter full last name	Enter complete	ID	Q SEARCH ALL
	DEPROVISION				
	First Name	Last Name	Person Immutable ID	Employee ID/Asso	. Status
	CSVTest	Victor	victor.h_i	1324858	Provisioned

- Provisioned users and not provisioned users will be shown on this page, however only provisioned users can be deprovisioned.
- Users can be deprovisioned at will and as needed.
- The number of users that can be deprovisioned in one go is the amount of users shown on the screen.

Note: This option is available for Americas only.





Changing PID for Federated SSO Access

Change PID

Home	User Setup			VN
Federation Setup	NATULE AND	Client ID:	ID	
*	Provision User(s) Deprovision User(s)	Change PID		
User Setup	First Name * Enter full first name	Last Name * Enter full last name	Employee ID/Associate ID * Enter complete ID	Q SEARCH
	CHANGE PID			
	First Name	Last Name	Person Immutable ID	Employee ID/Associate ID

- The ability to change PIDs (Person Immutable ID) has been recently introduced.
- Since it's not something that should happen often, PIDs can only be updated one by one.
- Bulk action is not supported.
- Characters supported in the change operation are the same as the supported in the provision operations.

Note: This option is available for Americas only.

Note: This option is not available for NAS clients.





Certificate management

Clients using federated SSO will need to maintain their x.509 public key certificate. Typically it will need to be renewed every 1 to 2 years. If the certificate is not renewed before expiration, their employees' federated access will be disabled.

- The client admin with Federated SSO dashboard access will receive an email notification from <u>SecurityServices noreply@adp.com</u> in advance of the expiration.
- To check for any of their public certificates that are set to expire in 30 days, the client admin can review at <u>https://identityfederation.adp.com</u> (Reports > Expired Certificates).
- The client will upload the certificate by uploading a Metadata file, which contains both the Federated Issuer Key and Certificate (XML file).





Enabling Multiple ADP Services to Your SSO Connection

ΟΚΤΑ

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

OIDC – Web Destination link



Copy the web destination link

SAML – 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:<u>https://abc.okta.com/app/adp/exk58v1rvvmmFB47G5d7/sso/saml?RelayState=https</u> ://fed.adp.com/saml/fedlanding.html?REDBOX

Create the Additional App in Okta

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

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 Entra ID

Please follow the Microsoft Entra ID setup instructions for the ADP SSO application.

OIDC – Web Destination link



Copy the web destination link for use below.

SAML – Mount the ADP service Entra ID URL

- 1. Log into your MS Entra ID 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: You must create one URL per extra ADP service selected during the setup process.





Create an Additional Application in MS Entra ID

ADP - Mobifed	Linl	ked Sign-on	X
 Overview Deployment Plan Diagnose and solve problems 	«	Change single sign-on modes Linked sign-on lets you configure the target on to the application. Choose linked sign-on	location when a user selects the app in your organization's My Apps or Office 365 portal. This option does not add single sign- when the application is configured for single sign-on in another identity provider service. Learn more [2]
Manage		Configure Sign-on URL	
Properties		Provide the URL your users will use to navig	ate to ADP - Mobifed FIT
A Owners			
Roles and administrators		Sign on URL ①	nt/v2/a8106e933bcdc136f9a7fe9d6ebb8675cd65009e34cd79cc9c66e2cdebac6601?run=true & adpwf=true & appid=WFN
Users and groups			
Single sign-on			
Provisioning			
Self-service			
 Custom security attributes (preview) 			
Security			
e Conditional Access		Save Discard	

- 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.
- For OIDC, add the Web Destination link copied from the ADP Federation dashboard to the "Sign on URL" and save.
- For SAML, add the ADP service Entra ID URL mounted in the process above to the "Sign on URL" and save.
- 10. Set up user and app configs as needed.
- 11. MS Entra ID takes a few minutes to refresh the apps. After this, go to your app dashboard and the newly created app should be available.





Note: You can test the Entra ID URLs 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, the user will not be found in the process.





Next Steps

User Rollout for Mobile and Web

ADP provides a sample email template, a web and <u>mobile federated SSO user experience guide</u> to help you craft your own process to move to federated SSO.

While in transition the users will become dual users (with both ADP-issued credentials and a federated account). Once employees and administrators are using federated SSO to access ADP services, please contact ADP to make the users direct, which will only use federated access to ADP.

Transition from SAML to OAuth/OIDC

If you have a current SAML connection and successfully have setup an OAuth/OIDC connection, you can begin to transition your users to use the OAuth/OIDC connection. Determine how your users currently access ADP thru the SAML relay states links. This could be an internal portal, your IDP might host the access, etc. This process needs to be replaced with the links from above.

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** organization has successfully completed the setup, please protect the administrator relay state or the OIDC web destination link with Multi-factor Authentication (MFA). Your administrators will use this link to access the ADP services.

Enabling Users to Use Federated Only Access

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. There are configurations that need to be done on the client settings to alter the functionality.

Note: This option will **not** remove existing dual accounts (please contact your ADP representative to remove the existing password accounts). Terminated users have the option of receiving a direct account.





Employee Experience

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

View the <u>Mobile Federation SSO Getting Started Guide for Employees</u> and <u>Web Federation SSO Getting</u> <u>Started Guide for Employees</u> for additional information.

Your employees can download the free ADP Mobile Solutions app and use your company login credentials to sign-in to ADP services.







Appendix – Options on Syncing Unique Identifier

To sync your federation identity directory to your ADP system you will need to sync the unique identifier, also referred to as Person Immutable ID (PID), with your internal systems (LDAP, active directory, etc). There are 3 ways to get the data into the IDP system: **Manual**, **Automated**, and **Real-time**.

- **Manual** Manually type in PID (contact your IT team in charge of federation for instructions) after reviewing ADP system.
 - EV5 PID is ID From Portal.adp.com go to Human Resources -> launch Enterprise ->
 People -> Personal Actions -> Change Job/Position information -> Change Job Position
 - EV6 People -> Personnel Actions -> Change Job/Position information -> Change Job/Position. (PID is to the left of Name)
 - WFN PID is Associate ID People -> Employment -> Employment Profile (Select card icon next to Employee Name)
 - **Vantage** PID is Employee # People -> Employee Profile -> Personal Information
 - **Netsecure** PID is Employee/Associate ID People -> Manage users
- Automated/Batch Run a scheduled report to pull that data and feed into the IDP system. May require ADP project services
 - **EV5** ADP DataCloud Advanced Reporting (ADPR)
 - **EV6** ADP DataCloud Advanced Reporting (ADPR)
 - WFN Reports & Analytics > Reports Dashboard > Additional Reporting Links > Custom reports
 - Vantage Reports & Analytics > Custom Reporting > Custom Reporting Home
- **Real-time** Use the available APIs for your ADP SOR to pull this data. May require ADP project services or 3rd party contractor.



0

- Search for existing 3rd party applications <u>https://apps.adp.com</u> Search for "Data Connectors"
 - Example Aquera Identity Directory Sync Bridge
- Create your own application using ADP APIs -Speak to your Service Representative or CSE to set up an API Onboarding Call.





Appendix – Configuring personId as User Identifier in Okta

If personId is not already configured as an attribute, it will need to be set up for your ADP OIDC connection. Please follow the steps below:

- 1. Open Directory -> Profile editor
- 2. Find your ADP app
- 3. Select 'Add attribute'
- 4. Add a new attribute with 'personId' for Display Name and Variable Name
- 5. Go to Mappings
- 6. Select the 'Okta User to (appname)' option
- 7. Find 'personId' in the righthand column
- 8. On the left hand column, select the attribute you are mapping to 'personId'. This attribute should contain the Federation ID chosen for your users.
- 9. Change the mapping to 'Apply mapping on user create and update' as shown below and save.

okta	okta User User Profile user			Æ	SG Lottery AD appuser
Username	is set by SG Lottery ADP			userName	
user.emp	loyeeNumber		<mark>↔</mark> •	personId	
			-> Apply update	mapping on use	r create and
Preview	Enter an Okta user to preview their mapp		O+ Apply	mapping on use	r create only
			-/-> Do not	map	0

10. Remove users from the ADP app and reassign them to engage the mapping.

You may need to also set up the personId as a Token. An additional "claim" may need to be added in Okta Authorization server.

In Okta, Security -> API -> Authorization Servers Under Claims -> Add Claim

Value in this claim can vary but in should retrieve the value equal to Federation ID.





Appendix – Dashboard Errors

To enhance the usability of the Federation Dashboard, documented below are the most frequent errors:

Area	Error message	Action
Federation Setup (SAML)	Invalid X.509 certificate format.	Check if metadata file XML
	Please confirm if your metadata	which contains certificate is
	file is correct.	correct. There's usually some
		typo.
	An error happened on SAML	Contact ADP representative for
	Setup process.	assistance.
	Federation Issuer Key is already	Check if the value of the entity
	setup and cannot be changed.	ID within the metadata file is
		the same that already exists for
		this setup on the Dashboard. If
		there are any federated users
		created with this federation
		setup, then the issuer key
		cannot be updated. Contact
		ADP representative for
		assistance.
Provision Users (CSV option)	User information could not be	Review CSV file as it might
	found: first name is incorrect.	contain: blank spaces or invalid
	OR	characters. CSV file must follow
	User information could not be	headers order as shown in
	found: last name is incorrect.	sample CSV.
	OR	



	User information could not be	
	found: date of birth is incorrect.	
	User is already provisioned with	The Person Immutable ID (PID)
	a different Person Immutable	is taken by some user already
	ID.	provisioned.
	User information could not be	Given employee ID could not be
	found: employee ID is incorrect.	found. The associate may not
		have been provisioned or may
		just be incorrect/different from
		associate created.
	User information could not be	Provisioning terminated users is
	found. The associate status is	not allowed. Check status of the
	terminated.	employment in case user is not
		supposed to be terminated.
Provision Users (Auto provision)	The request to set up federated	Misconfiguration in Netsecure.
	access with automatic	Multiple federation URLs could
	provisioning cannot be	be set up for the client, or user
	processed for your company.	has both employee ID and WFN
		ID. Contact ADP representative
		for assistance.
	Before selecting employee	System of Record is missing or
	ID/WFN Associate ID as Person	not found. System of Record
	Immutable ID option, make sure	must be added and associates
	the client has at least one	provisioned by the SOR. Contact
	employee record provisioned	ADP representative for
	with this information.	assistance.

•



Deprovision Users	You may not deprovision	Federation setup is not
	employees for Federated Single	completed. Functionality will
	Sign On if have not yet	only be displayed once the
	completed the Federation	setup is done and there are
	Setup.	users to be deprovisioned.
	More than one Identity Provider	Two or more Identity Providers
	found for given client.	were configured. Contact ADP
		representative for assistance.
Generic Error	Error. Contact your ADP	Common error after session
	representative for assistance.	timeout expires. Log out and log
	(no error code)	back in, or refresh page to login
		again.
Federation Setup (OIDC) –	06-3027	User not found. Account is likely
Activate Connection		not created yet.
	01-3001	Session failure. Token might be
		expired.
	03-3013	The user identifier defined on
		ADP side is not coming in the
		user info response from the
		Identity Provider.
	03-3007	Client secret or client ID doesn't
		match with what ADP has.
		Generate secret again and set
		the value on the Dashboard.
		Changes might take a few mins
		to reflect.



	03-3004	Token endpoint is not reachable
		or token endpoint did not
		respond.
	03-3006	Grant type is wrong.
Change PID	The Person Immutable ID is	PID is already assigned to the
	already in use.	same user or to another user.
	The update could not be	Account may have been deleted
	completed because the account	while user was updating the
	was not found.	PID. Please reload page to
		update with valid accounts.





Appendix – Authentication Errors

Documented below are the most frequent errors upon user authentication from federated session:

Area	Error message	Action
Authentication	3027	User not found. Account is likely
		not created yet.
	3001	Session failure. Token might be
		expired.
	3013	Make sure the client is sending
		the Userldentifier in the
		UserInfo response.
	3007	Client secret or client ID doesn't
		match with what is configured
		in ADP. Make sure Refresh flow
		is setup on client side.
	3004	Token endpoint is not reachable
		or token endpoint did not
		respond.





Did you find this guide helpful? We'd love to hear your feedback! Send us an email at:

AIM.productowners@ADP.com.