Contents

Overview of Federation with ADP ........................................................................................................ 3
Security Information .......................................................................................................................... 3
Accessing Your ADP Service ............................................................................................................ 3
  Direct Access ................................................................................................................................ 3
  Federated Access .......................................................................................................................... 4
  Dual Access ................................................................................................................................... 4
Implementation Process .................................................................................................................. 4
Information Your Organization Provides to ADP ............................................................................. 5
Information ADP Provides to Your Organization ............................................................................. 5
Configure Your Federation .............................................................................................................. 5
  Get Signed Certificate .................................................................................................................. 6
  Determine the Person Immutable ID (PID) ...................................................................................... 6
  Upload Your Certificate ................................................................................................................ 6
  Test Handshake (Using Test Data) ................................................................................................ 6
  Configure Live Environment ........................................................................................................ 7
User Provisioning .......................................................................................................................... 7
Employee Logon ............................................................................................................................ 8
Test Federated Access .................................................................................................................... 8
Go Live ........................................................................................................................................... 8
Frequently Asked Questions ........................................................................................................... 9
  User Maintenance ......................................................................................................................... 9
  Security ....................................................................................................................................... 9
  Signing Certificate ....................................................................................................................... 10
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 Security Assertions Markup Language (SAML 2.0), an XML-based framework, 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.

Accessing Your ADP Service

Your organization must determine the method your employees use to access your ADP services i.e., use 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.

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 using any device – work computer, home computer, or a kiosk with an internet connection. Using their Internet browser, your employees access your ADP service website and logon with their ADP-issued user ID and password.

Your administrators/practitioners logon with their ADP-issued user ID, password, and administrator access to perform administrative tasks.
Federated Access

Federated access allows employees logged on to your organization’s network or identity system to use the federated ADP service link on your portal to access their ADP service account.

Your employee authenticates first in your system using your organization’s logon/authentication scheme. Then your organization certifies that authentication and the user identity by sending a signed SAML assertion to ADP. ADP validates that the assertion is from your organization (identity provider) by validating your signature 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.

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.

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 submission of required information to ADP. Your ADP representative will assist as needed.

1. Your ADP representative provides this federation integration guide and the federation integration questionnaire to your administrator.

2. Your administrator provides the completed federation integration questionnaire to your ADP representative. See “Information Your Organization Provides to ADP”.

3. ADP works with your organization to prepare the ADP Federated Single Sign On agreement.

4. Your organization reviews, signs, and returns the ADP Federated Single Sign On agreement to your ADP representative.

5. Your ADP representative sets up your organization to use federated ADP services. This process may take a few days.

6. Your administrator receives an email to access ADP Federated Single Sign On. See “Information ADP Provides to Your Organization”.

ADP Federated Single Sign On Integration Guide

Federated Access

Dual Access

Implementation Process
Important: Your organization must sign the ADP Federated Single Sign On agreement to receive this information from ADP.

7. Your administrator configures federated access for your organization and secures the exchange with a signed certificate. See “Configure Your Federation”.

8. Your administrator performs a handshake test using test data. See “Test Handshake”.

   Note: If you use an ADP supported third party identity provider, handshake test does not apply.

9. Your ADP representative configures your organization to use federated access. This process may take a few days.

   Note: Your administrator receives an email to begin using federated access for your organization.

10. Your administrator completes user provisioning to verify your employee’s information to allow federated access. See “User Provisioning”.

Congratulations! You are ready to make the federated ADP service available to your employees.

Information Your Organization Provides to ADP

Before ADP sets up access to the federation environment, your organization must provide the following documents:

1. Completed Federation Integration Questionnaire.

2. Signed ADP Sales Order and/or ADP Federated Single Sign On agreement.

Information ADP Provides to Your Organization

Upon receipt of the completed federation integration questionnaire, ADP sets up your organization for federated access and notifies your administrator. Your administrator receives an email to access ADP Federated Single Sign On website. The Home page> Get Started section provides information to your administrator to configure federation with ADP.

Configure Your Federation

Your administrator receives an email to begin using the ADP Federated Single Sign On website to complete the federation setup.
Get Signed Certificate

Your organization requires a Secure Socket Layer (SSL) certificate to secure your federation with ADP. Your organization can get your certificate signed by a third party certificate authority such as Entrust, Symantec (Verisign), DigiCert, etc. ADP does not recommend or endorse any third party certificate authority.

Note: To use a signed certificate issued by an ADP-supported third party identity provider, contact your ADP representative. ADP does not allow self-signed certificates in the live environment.

Determine the Person Immutable ID (PID)

ADP requires that you designate a Person Immutable ID to uniquely recognize each employee in your organization’s authentication server/system. Your organization should not reuse this value for other employees. Many ADP solutions store a unique Employee ID/Associate ID; if you are using one of those solutions and you select to use the EmployeeID/AssociateID as the source of the Person Immutable ID (PID), you can automatically provide federated access to your employees (see Automated Provisioning below).

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

Upload Your Certificate

Your administrator logs on to the ADP Federated Single Sign On website and uploads your public/distribution certificate (base-64 encoded X.509 public key certificate) in the plain text format. ADP does not require your organization’s private key.

ADP verifies your setup information and configures your organization to test handshake. This process may take a few days.

Test Handshake (Using Test Data)

After ADP sets up your organization in the federation integration environment, your administrator configures your handshake environment with the target URL displayed on the ADP Federated Single Sign On website. Your organization must initiate a handshake test to ensure that your assertions are correct and pass the expected data to ADP. Your administrator completes a handshake test with the test data available on the ADP Federated Single Sign On website.

Note: This step is not required when using a supported third party identity provider.
Configure Live Environment

After testing handshake on ADP’s verification site, your administrator receives an email notification to begin using federation in the live environment. Your administrator then completes user provisioning to set up your employees for federated access.

User Provisioning

User provisioning can be accomplished through the following methods:

Automated Provisioning

- Many ADP Services create or generate Employee ID/Associate IDs for your employees during the new hire process. ADP ensures the uniqueness of these values and they are a good option to use as the Person Immutable ID (PID). If you do use Employee ID/Associate ID as the PID, ADP provides an automatic provisioning capability which, when enabled, will automatically create federated accounts for your employees.

- Your administrator needs to ensure that this field is correctly populated on your identity provider and is sent accurately in the SAML assertion to ADP. This capability is only available when the Employee ID/Associate ID field is used as the PID.

Note: This process cannot be enabled via the ADP Federated SSO website – you must contact your ADP representative to get this process enabled.

Manual File-Based Provisioning

- ADP also provides a manual provisioning option on the ADP Federated Single Sign on website. It requires creating a Comma Separated Value (.CSV) provisioning file which can be uploaded by your administrator.

- The provisioning file must include the Person Immutable ID, Employee ID/Associate ID, First Name, Last Name, and Date of Birth (mm/dd/yyyy) of each employee and should only include the employees who require federated identity access to your ADP solution.

- The provisioning file must not exceed 1,000 employee records or 2MB in size. Multiple files may be used to provision additional employees as needed for federated identity access.
Direct Text Entry

- You may also enter individual employee provisioning data as text directly on the ADP Federated SSO website. The website prompts the user for the required information and verifies the completeness of the provisioning data entered.

Employee Logon

Once your employees are successfully provisioned, they are ready to log on. Your employee logs onto your company website or Identity Provider application and clicks the federated ADP service link to access their information.

Note: ADP does not support federated access with service provider-initiated logins.

Test Federated Access

Identify a limited number of employees to test federated access. Select employees who currently access your ADP service. Your organization includes the link to the federated ADP service on your portal for easy access or in the sample letter to notify your employees. The sample letter is also available on the ADP Federated Single Sign On website.

Important: Do not test your implementation in the live environment until you receive confirmation from ADP.

Go Live

After you successfully complete your test for federated access with a limited number of employees, you are ready to make the federated ADP service available to your employees.

ADP recommends that your organization pilot the federated ADP service with a limited number of employees and gradually rollout the federated ADP service.
Frequently Asked Questions

User Maintenance

Q: Do you allow administrators/practitioners to have federated access?
A: No. Administrators/practitioners must use direct access two factor authentication with ADP. However, they can use federated single sign on for the self-service access to their account.

Q: Does ADP support federated access for employees using kiosks to log in to their ADP service?
A: No. Employees using kiosks must use direct access to log in to their ADP service website.

Q: How can administrators view federated user information?
A: Your administrators can view this information by logging on and accessing ADP Security Management Service.
Go to Reports > Run & View Reports. Click Associate Information report and select the user information to be included in your report.
After submitting the request for your report, go to Reports > Run & View Reports > Current to view your report results in Portable Document Format (.PDF) or Comma Separated Value (.CSV) output.

Q: Can administrators make changes to or delete the information of federated employees?
A: This change cannot be initiated from the ADP Federated SSO website. If you have changes or need to delete a provisioned employee, please contact your ADP representative.

Security

Q: Does ADP support W3C XML encryption of SAML assertions?
A: Yes. ADP supports W3C XML encryption for OASIS SAML 2.0 protocol.

Q: How can my organization secure the data transmitted to ADP?
A: ADP recommends the use of SAML 2.0 transport with Secure Sockets Layer (SSL). Strong Secure Sockets Layer (SSL) secures the information exchanged between your organization and ADP.

Q: Should I sign the SAML assertions and the SAML response?
A: No. You should make your selection and sign only one of the two options. The overhead and message size significantly increases if you use both the options.
Q: What is Time Synchronization?
A: SAML assertion validation is dependent on the time stamp information. This makes it critical to synchronize the clocks of your identity provider server and ADP service provider server against a definitive source. SAML assertions require synchronization of the server clocks.

The Network Time Protocol (NTP) is available for time synchronization of servers. NTP is capable of synchronizing your organization’s clocks within milliseconds on Local Area Networks (LAN) and tens of milliseconds over Wide Area Networks (WAN).

For information and listing of Network Time Protocol (NTP) public timeservers, refer to the following resources:
- National Institute of Standards and Technology - [http://tf.nist.gov/service/its.htm](http://tf.nist.gov/service/its.htm)
- NTP Public Services Project - [http://support.ntp.org/bin/view/Servers/WebHome](http://support.ntp.org/bin/view/Servers/WebHome)

Q: Does ADP utilize the SAML "Name Identifier"?
A: No, however, your organization must include the “NameID” element.

Q: Is my organization required to send subject confirmation?
A: Yes. Your organization must use the bearer method to provide the subject confirmation. If your organization is using SAML 2.0, include the following in your assertion:

```
<subjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"
<saml:SubjectConfirmation>
  <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
</saml:SubjectConfirmation>
```

**Signing Certificate**

Q: How can my organization get a third party signed certificate?
A: Complete the following steps before you contact the third party certificate authority such as Entrust, Thawte, and Verisign:

1. Generate a private key. You can generate this key by using one of many free industry tools such as: OpenSSL, Java Key tool, and .NET. You select the tool based on the SAML vendor you use. You must use the RSA algorithm and generate a private key valid for at least two years.
2. Do not share the private key with any other organization.
3. Generate a Certificate Signing Request (CSR) using the same tool.
4. Use the CSR to create a file based on the private key.
5. Provide the file to the third party certificate authority when you request for a Signing Certificate.
**Note:** To use a wild card certificate, your organization must have a PFX or JKS keystore file that contains the wild card information.