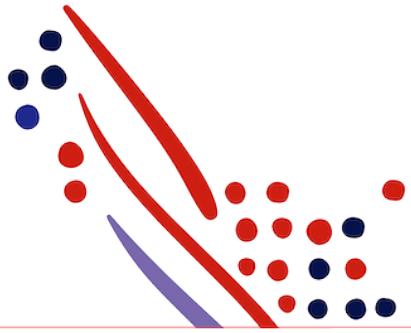
Guide

ADP Marketplace ESI - Getting started

Published on
Mar 22, 2022, 09:18 AM

Last modified
Jul 15, 2025, 02:47 PM

Always Designing for People™



ADP Copyright Information

Published on
Mar 22, 2022, 09:18 AM

Published on
Jul 15, 2025, 02:47 PM

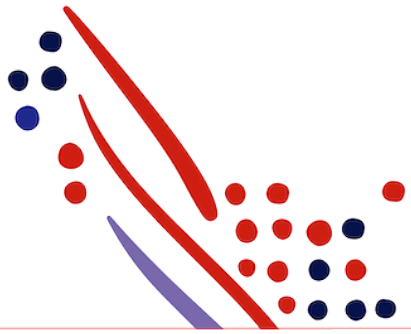


Table of Contents

Chapter 1

Introduction

In 2020 ADP launched ADP Marketplace in Europe. ADP Marketplace is the standard gateway for all APIs.
It offers extras like:

- an app store with partner products which certified interfaces
- a web app for the client showing which APIs are used by whom with the possibility to block the access when the client uses partners
- technical documentation on **http://developers.adp.com**

To be clear: one of the requirements for introducing ADP Marketplace in Europe is that all client data must stay and be stored in Europe. To meet this requirement we have deployed the related infrastructure in our data centers in Europe. In addition we have specific API endpoints for European customers.

This document provides basic information about the following subjects;

- Generating a Certificate Signing Request (ADP will provide the certificate)
- Requesting an Access Token (Bearer)
- Retrieving resources using the ADP Restful APIs

> **Note**
>
> Additional API Guides will be provided for each ADP HR Product.

Intended audience

This document is intended for:

- Architects
- Developers

Chapter 2

Certificate Signing Request

A private key and matching Web Services (WS) Certificate are required to access the ADP Marketplace web services. The WS Certificate provides client information to ADP and the matching private key confirms the authenticity of the client. To generate the WS Certificate a Certificate Signing Request (CSR) needs to be generated by the client. During the CSR generation the private key and matching public key are created. The CSR is submitted to the ADP Web Services Certificate Authority *(currently run by Sectigo)* and they return the WS Certificate.

Many software tools store the private key and the WS Certificate in one Personal Information Exchange Format (PFX) file, also known as P12- file.

Disclosure

Open Secure Sockets Layer (OpenSSL) is an open source tool. Although ADP has tested the commands, based on the OS and version configuration settings and other environmental factors as well as the commands and configuration may have to be adjusted. ADP does not support OpenSSL tool itself. For questions and support please reach out to your IT department and/or third party.

Other tools (such as Java Keytool), that can be used to generate a CSR, are not covered in this document. If another tool is used, please make sure the CSR is PEM format (base64 encoded with additional header and footer lines).

Clients need to ensure that every time new private and public keys are created, they are managed properly. If they are generated more than once, each key pair must be stored (possibly in different directories) so there is no confusion. In addition, the returned Web Services Certificate (which also contains the public key) must be managed properly (stored in the directory that has the matching private key).

Install OpenSSL Light for Windows

1. Download **OpenSSL Light for Windows** at: http://slproweb.com/products/Win32OpenSSL.html. Mac users can open *Terminal* and jump to the OpenSSL commands in step 3.
2. Follow the instructions in the Install Wizard. All options can be left default.

CSR for a new connection

1. Open **cmd.exe.**
2. Go to the location where you installed OpenSSL and set the current directory to the **bin** directory, for example **cd C:\Program Files\OpenSSL-Win64\bin**.
3. Using the commands below to generate the CSR and private key to a folder of choice, for example **C:\Temp**. Replace companyname_auth by the value you want to use.

    - openssl genrsa -out C:\Temp\companyname_auth.key 2048
    - openssl req -new -key C:\Temp\companyname_auth.key -out C:\Temp\companyname_auth.csr

    > **Note**
    >
    > Your CSR must not request S/MIME capabilities.

4. Enter the information below into your CSR. Other fields can be left empty.

    - Country Name
    - State or Province Name
    - Locality Name
    - Organization Name
    - Common Name
    - Leave Challenge password blank *(i.e. no password)*

    > **Note**
    >
    > - Please contact your ADP Representative for the values to be used for **Organization Name** and **Common Name**.
    > - For Country Name use the ISO compliant 2 letter code, for example NL.
    > - If you enter an e-mail address, please make sure it is an existing group e-mail address we can use to send notifications to on certificate expiration.

5. Attach the CSR to the ADP eService ticket. Please also a provide a **group e-mail address** to be automatically notified when the generated certificate is approaching its two-year expiration date.

> **Important**
>
> - Please make sure to store the generated private key in a safe location. It is needed to setup a connection to ADP Marketplace. Never give the private key to unauthorized parties and never send it via unsecure connections.
> - The private key should **not** be send to ADP.
> - Please make sure the values used for **Organization Name** and **Common Name** are stored. You will need them when the current certificate is going to expire to generate a new CSR.

6. After receiving the e-mail from ADP with download links for your certificate. Please download and save the signed certificate. The downloaded certificate together with the private key are needed to connect to the ADP web services.

> **Tip**
>
> If you are using Windows/IIS you can use the following command to combine the private key and certificate in PKCS12 format file (.pfx):
>
> openssl pkcs12 -export -out *companyname_auth*.pfx -name "*Company Name Mutual SSL*" -inkey *companyname_auth*.key -in *companyname_auth*.pem.

If needed replace *companyname_auth* with the correct name. The resulting .pfx file can be used for mutual SSL authentication.

CSR for certificate renewal

1. Create the CSR, see *Certificate Signing Request for a new connection*.

> **Important**
>
> Make sure the values for **Organization Name** and **Common Name** match the values used for the initial CSR and current certificate ***exactly***. When in doubt contact your ADP Representative to check the values. Using the wrong values will result in loss of connection.

2. After you have created your CSR, you have two options for submitting it to ADP for signing:
    1. Mail the CSR to marketplace esi client support@adp.com for processing or,
    2. Submit your request directly to ADP security Services:
        - Open the ADP Certificate Signing Tool.
        - Enter your e-mail address and click [Submit].
        - Click [Enroll Certificate].
        - For Certificate Profile choose **Authentication and Transaction Signing**.
        - Upload the CSR via the button [Upload CSR] or paste the complete contents including the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines of your CSR into the CSR text box.
        - Enter the following information in the Custom Fields:
            - Company name

> **Note**
>
> This value has to be an exact match of the value of the Organization you chose when creating the CSR.

            - Your ADP Client ID

> **Note**
>
> Please contact your ADP Representative for your ADP Client ID.

            - Your technical contact's first and last name.
            - Your technical contact's e-mail address. The certificate will be sent to this address.

> **Tip**
>
> Please use group distribution list or group e-mail address as this address will also be used to automatically notify you when the generated certificate is approaching its two-year expiration date.

            - Click 'Submit'.

> **Note**
>
> It might take up to a week for you to receive the certificate.

Important

Make sure you safeguard the .key, .pfx and .jks files. Anyone that possesses these confidential files can potentially access to the web service.

Chapter 3

Access Token

As part of the OpenID Connect and Open Authorization (OAuth) 2.0 flows, Access Tokens are provided by ADP and used for secure calls to protect ADP APIs. This document outlines how Access Tokens are used as well as some limitations and security considerations.

Request an Access Token from ADP

Your application can request an access token by sending an HTTPS POST request to the token endpoint:
https://accounts.eu.adp.com/auth/oauth/v2/token

The request must include the following parameters:

Parameter	Description
grant_type	REQUIRED. Must be set to the value "client_credentials".
client_id	REQUIRED. The consumer application's account identifier, assigned during account registration or at secret reset.
client_secret	REQUIRED. The consumer application's account password, assigned during account registration or at secret reset.

There are two options to send the required parameters. Your consumer application should pass the client_id and client_secret parameters in the HTTP Authorization header using the HTTP Basic authentication scheme or as a form POST. Examples of both options are documented below. The client_id and client_secret must be separated by a single colon (":") character and encoded within a base64-encoded string, as required by IETF RFC 2617.

Your consumer application must:

- Send the request with the X.509 certificate provided during registration.
- Pass all parameters in a URL-encoded format with UTF-8 character encoding as specified by the HTTP header *Content-Type: application/x-www-form-urlencoded*.

Example (Curl) – Basic Auth Headers

A Curl example of how to perform a request for a Access Token from ADP

```
curl
  --request POST
  --url 'https://accounts.eu.adp.com/auth/oauth/v2/token' --cert '/path/to/cert.crt'
  --key '/path/to/key.key'
  --user ': '
  --header 'Content-Type: application/x-www-form-urlencoded'
  --data-urlencode 'grant_type=client_credentials'
```

Example (Curl) – Form POST

A Curl example of how to perform a request for a Access Token from ADP

```
curl
  --request POST
  --url 'https://accounts.eu.adp.com/auth/oauth/v2/token' --cert '/path/to/cert.crt'
  --key '/path/to/key.key'
  --header 'Content-Type: application/x-www-form-urlencoded'
```

```
  --data-urlencode 'client_id='
  --data-urlencode 'client_secret='
  --data-urlencode 'grant_type=client_credentials'
```

Response

```
{
  "access_token": "27b16f3c-e4f3-44c2-b800-b571424c4e88",
  "token_type": "Bearer",
  "expires_in": 3600
}
```

Parameter	
access_token	The access_token parameter is set to the value of the access token issued by the ADP authorization service in exchange for the authorization code.
token_type	Identifies the type of token returned. At this time, this field always has the value Bearer.
expires_in	The expires_in parameter is set to the time remaining in the token's life (in seconds). For example, the value "3600" indicates that the access token will expire in one hour.

How to use an access token

After your application obtains an Access Token, it can use it to request multiple Web APIs for as long as the Access Token is valid.
Your application must follow these guidelines to request a protected Web API:

- Use the Transport Client Authentication in all Web API requests with the X.509 certificate provided during the registration of your application. For example, mutual Secure Sockets Layer (SSL)/Transport Layer Security (TLS).
- Use the HTTP Authorization header with the Bearer authentication scheme and a valid access token.

The following is an example of a Web API request with a bearer token:

GET /hr/v2/workers HTTP/ 1.1 Host : api.eu.adp.com Authorization : Bearer 024ded5f831d4483a9c606710026b09b

Your application must be able to process the errors as defined in Internet Engineering Taskforce (IETF) Request for Comment (RFC) 6750. Your application must be able to handle the errors in the following table.

HTTP Status	Error code	Deescription
400 Bad Request	invalid_request	Specifies that the Web API request is missing a required parameter or includes an invalid or distorted parameter value.
401 Unauthorized	invalid_token	Indicates the Web API request contained an expired, revoked, or invalid Access Token. Additional information about the error might be provided in the WWW- Authenticate header.
403 Forbidden	insufficient scope	Specifies that the Web API request requires higher privileges than provided by the Access Token.
500 Internal Server Error		Indicates the Web API cannot be processed due to a runtime error.
503 Service		Indicates the Web API cannot be processed because the service is unavailable.

HTTP Status	Error code	Deescription
Unavailable		

The following is an example of an error:

HTTP/ 1.1 401 Unauthorized WWW- Authenticate : Bearer realm="oauth", error="invalid_token", error_description=" Access token expired"

For other errors, the authorization server might provide the error code and error_description in the body as a JavaScript Object Notation (JSON) object.

The following is another example of an error:
HTTP/ 1.1 403 Forbidden Content-Type : application/json;charset=UTF- 8 { "error":"insufficient_scope", "error_description":" Unauthorized Web API"

For other errors, the authorization server might provide the error code and error description in the body as a JSON object.

ADP Web API Limitations

For security reasons ADP places limits on the usage of Access Tokens and Web APIs. You may want to consider the following limitations in your application:

- Access Tokens are tied to your application. You cannot use one Access Token in another application.
- Access Tokens may be tied to the computing environment used by your application during the authorization process. For example, restricted to a certain IP address. Access might not be allowed from a different computing environment.
- Access Tokens have a short life span. By default, Access Tokens expire in 60 minutes. If your application and security requirements require a smaller expiration time, indicate your requirements during application registration.

Tip

Since tokens expire after 60 minutes, your application should only request a different token when the current one is about to expire. Do not call a new token for every API request.

If your application and security requirements require a different setting, indicate your requirements during application registration.

Security Considerations

ADP recommends your organization considers keeping application credentials under strict control to prevent leakage and misuse . This includes the following:

- Account identifier
- Account secret
- X.509 certificate

Your application should never store or pass Access Tokens in cookies or parameters. They are transient and stored temporarily in your application's memory. You should do the following:

- Discard Access Tokens when your application finishes its processing with ADP.
- Consider limiting the access scope requested in authorization requests. This limits the capabilities associated with Access Tokens produced by these authorization requests.

Chapter 4

ADP Restful APIs

ADP APIs are designed using REST for resource management. This pattern separates the act of retrieving resources and modifying them into separate activities along with providing event notifications that indicate changes to a resource.

Retrieving Resources

The most common method to retrieve resources through the ADP REST APIs is to do a GET against the resource endpoint. By default, this request returns all resources of a given type, but supports several query parameters to control what is returned.
For example, the resource you are interested in is Worker v2. The request to get all workers is: **GET https://api.eu.adp.com/hr/v2/workers**. You can control the results returned by using the following query parameters:

- **$top**: Specifies the upper limit on the number of items to return.
- **$skip**: Specifies the number of items to skip from the beginning of the list.
- **$filter**: Specifies an expression that an item must match to be included in a response.

Another example is that you can do the following:

- Request only the first 10 workers:
  GET https://api.eu.adp.com/hr/v2/workers?$top=10

Example (Curl)

A Curl example of how to perform a request for a worker call from ADP

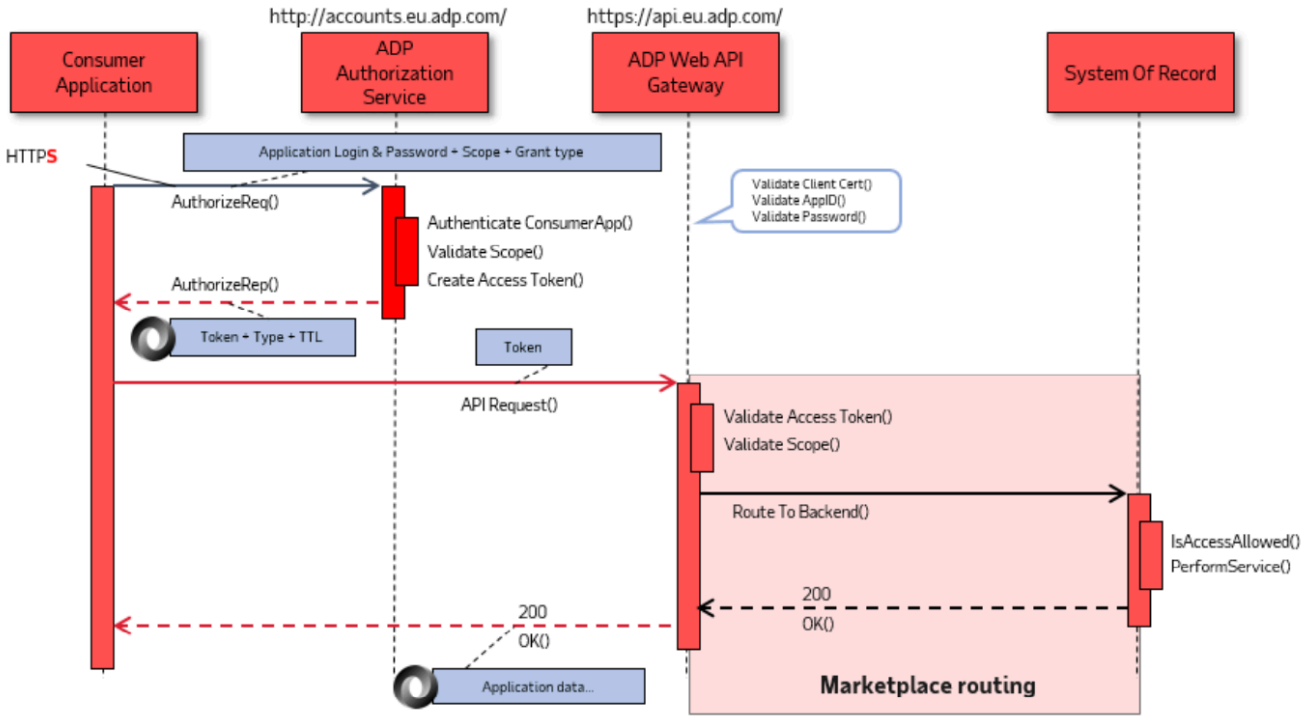
```
curl
  --location --request GET 'https://api.eu.adp.com/hr/v2/workers'
  --header 'Authorization: Bearer 024ded5f831d4483a9c606710026b09b'
```

Throttling

To prevent high load on ADP infrastructure ADP Marketplace ESI supports throttling. Throttling in this context means ADP Marketplace ESI will respond with error codes (429) once a certain requests threshold has been reached. The response contains a retry-after header that you can use to wait for the next request. The value is in seconds. When ADP Marketplace ESI responds with a http 429 error, the request is not passed to the systems of records preventing overload on these systems. ADP Marketplace ESI allows you to perform up to 10 concurrent api calls per second with some burst allowance (150% within a minute). Everything beyond this threshold will result in a 429 error.

Global Sequence

The following drawing provides some details of requesting a token call and performing a call to retrieve workers from the SOR.



Chapter 5

OData

ADP APIs support the following options defined in Open Data Protocol (OData):

- $filter
- $top
- $skip

These options allow a client device to control the representation it gets back from the server. Multiple query parameters may be used together by separating each option with the & character.

About OData

OData is a standardized protocol built over existing Hypertext Transfer Protocol (HTTP) and Representational State Transfer (REST) protocols supporting CRUD (Create, Read, Update, Delete) operations for creating and consuming data APIs.

For more information, see: https://www.odata.org/getting-started/understand-odata-in-6-steps/.
For URL conventions, see: https://www.odata.org/documentation/odata-version-3-0/url-conventions/.

OData Parameter Types

About the $filter Parameter

The **$filter** option filters a collection of resources addressed by a request URL. The expression specified with **$filter** is evaluated for each resource in the collection, and only items where the expression evaluates to true are included in the response.

To Get	Use the following query
Only workers from specific department:	GET https://api.eu.adp.com/hr/v2/workers? $filter=/workers/workAssignments/homeOrganizationalUnits/nameCode/codeValue eq '000040'
Both workers from specific department and started in 2020:	GET https://api.eu.adp.com/hr/v2/workers? $filter=/workers/workAssignments/homeOrganizationalUnits/nameCode/codeValue eq '000040' and /workers/workAssignments/actualStartDate ge '20200101'

The **$filter** parameter supports field values in single quotes only.

Info

Supported **$filter** resource paths will vary by ADP product.

About the $top Parameter

The **$top** option requests the number of items in the queried collection to be included in the result. The following request returns the first ten workers of the workers collection:
GET https://api.eu.adp.com/hr/v2/workers?$top=10

About the $skip Parameter

The **$skip** option specifies the number of items in the queried collection to be skipped and not included in the result.
GET https://api.eu.adp.com/hr/v2/workers?$skip=18

Pagination Using $top and $skip for Large Collections

The following request returns 20 workers, starting with the 51st worker of the workers collection while using the HR V2 Workers API and pagination using $top and $skip for large collections:

GET https://api.eu.adp.com/hr/v2/workers?$top=20&$skip=50

> **Note**
>
> While using Pagination, when you reach the end of all the records, a 204 response code with No Content will be returned or a 200 response code with an empty array.

Chapter 6

Request Response APIs vs Event Notifications

Request Response APIs

Request Response APIs retrieve the actual status of an entity in the HR System, which you can compare to your own data and perform the necessary actions. Examples of entities are workers, departments or time-off requests. Consider scheduling these type of requests daily for the purpose of synchronizing data.

> **Note**
>
> Request Response APIs are not intended to be used for synchronization in real-time. Processing all data might require a high load of CPU cycles.

Example: Retrieve all workers over night and sync the changes with your system.

Event notifications

Event Notifications are messages, containing only the changed entities (events) in the HR system. An event can be an approved Time-Off request, a hired worker or a name change of a department.

> **Note**
>
> Event Notifications are intended for near real-time processing. This requires an implementation effort by the consumer.

Example: Push information about new hires directly into other systems to start a workflow.

Event Notifications allow your application to be notified of data changes. They can be used to retrieve the latest data, to sync your system with ADP products and applications. When data is updated in an ADP application, ADP generates an Event Notification message. This message is sent to a subscriber's message queue.

Examples:

- Creating/disabling a user in the facilities ticketing system when the employee is joining or leaving the company
- Update the name of supervisor registered in a purchasing system when the employee transfers to another department
- Register a vacation day in a time sheet application when the request for leave is approved

Event notifications give you the opportunity to work with small amounts of transaction data
without the need to use batch processing

About Event Notifications

ADP Representational State Transfer (REST) APIs use an event-based pattern for resource modification. Clients or partners need to know if there are any changes in the System of Record (SOR) at ADP to act upon or keep themselves aware . Events mark every change made in the system. Partners or clients will get to know about the changes after they subscribe to the specific changes for which they want to be notified. Event Notifications provide the details about the changes to partners. This prompts action by the partners and keeps their records updated.

Note

Event notifications are used in near real-time scenarios and it's recommended to check the event notification list on scheduled basis with at least a maximum of one hour.

Process overview

When data is updated in an ADP application, ADP generates an Event Notification message. Then, the message is sent to a subscriber's message queue. To regularly check and retrieve, event notification messages subscribe your application to data change events. For example, you can subscribe to the Worker Hire event to be notified when a new hire is added to an ADP product. This is so you can do some work with the new hire's data.

	Actor	Description
1	A human user or a system	Makes a change to a record. For example, an employee updates a worker's email address in an ADP product.
2	ADP product	Generates an Event Notification message and sends copies to a subscriber's message queue. Messages are queued based on the first in, first out (FIFO) method
3	Consumer application	On scheduled time, retrieves one Event Notification message from its message queue and acts as needed.
4	Consumer application	Deletes the Event Notification message from its message queue and repeats steps 3 and 4 until there are no more messages in the queue.

Required Setup Steps

To subscribe to an Event Notification, contact your ADP Representative.

Note

Detailed information regarding event notifications can be found in the Event Notification Manual

Chapter 7

Terminology and Acronyms

API	(Application Programming Interface) A system of tools and resources in an operating system created by ADP, enabling developers to create software applications.

Canonical ID	Unique IDs that ADP assigns to API end points to manage API access and authorization. Application developers need to request API access using canonical IDs.
CSR	(Certificate Signing Request) Required for accessing ADP APIs and authenticating users with SSO.
OAuth	(Open Authorization) Framework for token-based authentication and authorization for web-based applications.
Private Key	A text file used initially to generate a CSR, and later to secure and verify connections using the certificate created per that request. The client is the owner for this key and the server is not aware of the key.
Public Key	Distributed by the vendor and is included as part of the SSL certificate. It works together with a private key to make sure that data is encrypted, not tampered with, and verified.
SOR	(System of Records) Refers to the ADP HCM solution.
SSL	(Secure Sockets Layer) A global standard security technology that enables encrypted communication between a web browser and a web server.
SSO	(Single Sign-On) Authentication process that allows a user to access multiple applications with one set of login credentials.