



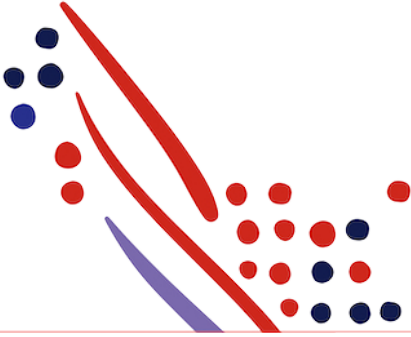
Guide

# ADP Marketplace ESI - Making your first api call using Postman

Published on  
Mar 31, 2022 5:50AM

Last modified  
Mar 22, 2023 11:23AM





## ADP Copyright Information

ADP, the ADP logo, and Always Designing for People are trademarks of ADP, Inc.

Windows is a registered trademark of the Microsoft Corporation.

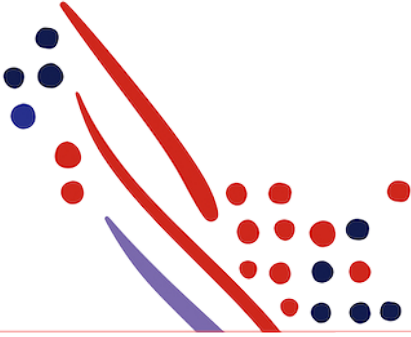
All other trademarks are the property of their respective owners.

Copyright © 2023 ADP, Inc. ADP Proprietary and Confidential - All Rights Reserved. These materials may not be reproduced in any format without the express written permission of ADP, Inc.

These materials may not be reproduced in any format without the express written permission of ADP, Inc. ADP provides this publication "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. ADP is not responsible for any technical inaccuracies or typographical errors which may be contained in this publication. Changes are periodically made to the information herein, and such changes will be incorporated in new editions of this publication. ADP may make improvements and/or changes in the product and/or the programs described in this publication.

Published on  
Mar 31, 2022 5:50AM

Last modified  
Mar 22, 2023 11:23AM



# Table of Contents

## Chapter 1

### Prerequisites

- Overview
- Intended audience
- Prerequisites
- Installing and preparing postman
- Import the Postman collection

## Chapter 2

### Making your first call

- Requesting a bearer token
- Making an API Call with Your Bearer Token

## Chapter 3

### Frequently Encountered Errors and Resolutions

- Contacting your ADP representative
- HTTP 401 - invalid\_client
- HTTP 401 - invalid\_request
- HTTP 401 - Unauthorized
- HTTP 403 - Invalid scope
- HTTP 404 - Canonical URI not found

## Chapter 4

### Terminology and Acronyms

# Prerequisites

## Overview

This guide provides an overview of using Postman to make your first application programming interface (API) call to ADP.



### Important

Depending on the version of Postman you use screens and options may differ from the images in this document.

## Intended audience

This document is intended for:

- Architects
- Developers

This document is intended for ADP Marketplace ESI, meaning countries outside North America and Canada.

## Prerequisites

You need to have the following ready before making your first API call:

- Client ID and Client Secret: If you don't have this information, contact your ADP representative
- Certificate: If you don't have this information, contact your ADP representative
- Private key

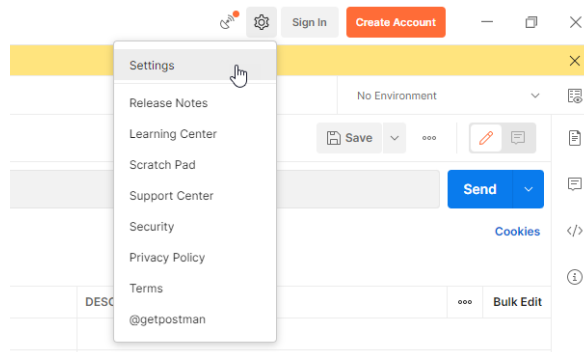


### Note

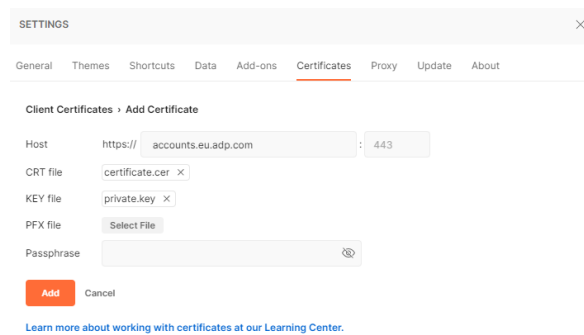
These are all a result of the process as described in the [ADP Marketplace ESI - Getting started](#) document.

## Installing and preparing postman

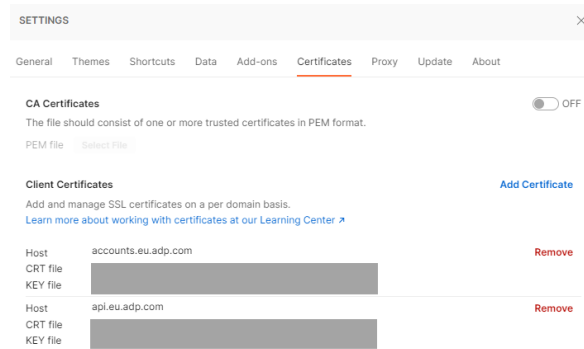
1. Install Postman from <https://www.getpostman.com/apps>.
2. Using the following steps, add your ADP issued certificate (.CER file) and your private key (.KEY file generated as part of the CSR process) into Postman. You can also use the instructions found at <https://www.getpostman.com/docs/postman/sending.api.requests/certificates>.
  - o Click **Settings**.



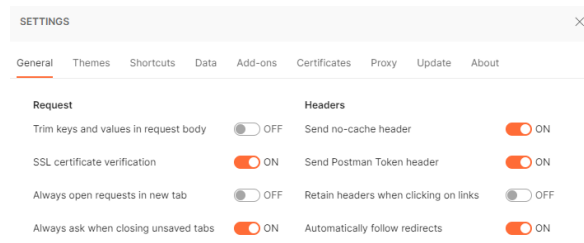
- o Click **Certificates, Add Certificates**.
- o For Host enter the value **accounts.eu.adp.com**
- o Next to **CRT file** click [Select file], browse to your ADP issued certificate (.CER file) and click [Open].
- o Next to **KEY file** click [Select file], browse to your private key (.KEY file generated as part of the CSR process) and click [Open].
- o Click [Add].



- o Repeat the steps above for the host **api.eu.adp.com**



- o On the **Settings** page enable **SSL certificate verification**.



## Import the Postman collection

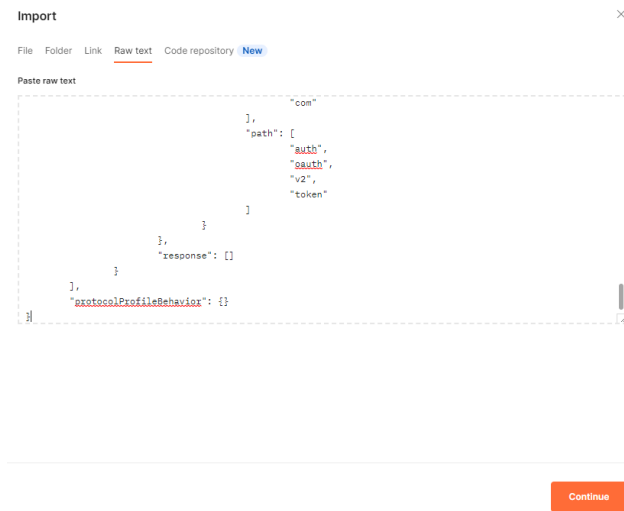
Postman allows you to store a collection of APIs and share them with others. In this document we use examples from a collection you can download [here](#). Import this collection in Postman.

- Download the collection from the website by clicking *Copy raw contents*.

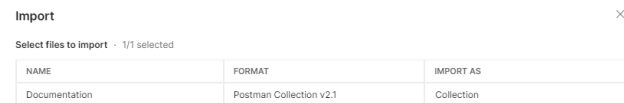


```
1 {
2   "info": {
3     "_postman_id": "5d1c44c1-99fc-465c-a2ae-7f96c0d9970c",
4     "name": "Documentation",
5     "schema": "https://schema.getpostman.com/json/collection/v2.1.0/collection.json"
6   }
7 }
```

- Postman click [Import], go to the tab *Raw text* and paste the code that was copied in the previous step.

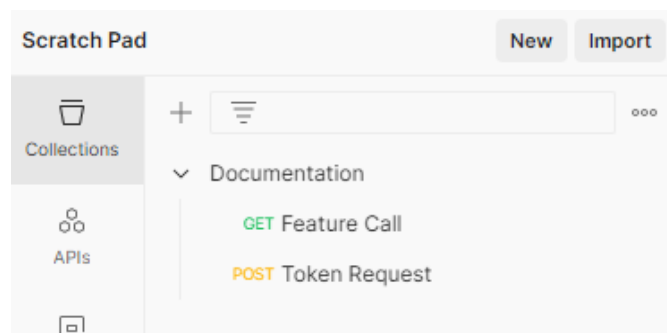


- Click [Continue] and [Import].



NAME	FORMAT	IMPORT AS
Documentation	Postman Collection v2.1	Collection

The collection with a Token Request and a Feature Call is now available in Postman.



## Requesting a bearer token



### Info

This example is based on the Postman collection downloaded and imported in the previous chapter.

Each request to one of ADP's APIs needs to be accompanied by an Authorization header containing a bearer token issued by the ADP Security Token Service. Please verify if you are granted the permission by your IT department to execute the process below.

1. In Postman open the **Token Request**. To expose the body click **Body**. Fill in the `client_id` and `client_secret` that have been provided by ADP and click [Send].

The screenshot shows a Postman interface for a POST request named 'Token Request' at the URL `https://api.eu.adp.com/auth/oauth/v2/token`. The 'Body' tab is selected, and the body type is set to 'x-www-form-urlencoded'. The form contains the following fields:

KEY	VALUE
<input checked="" type="checkbox"/> <code>client_id</code>	[Redacted]
<input checked="" type="checkbox"/> <code>client_secret</code>	[Redacted]
<input checked="" type="checkbox"/> <code>grant_type</code>	<code>client_credentials</code>
Key	Value

2. If your POST request is successful you will receive an HTTP 200 from the server with your token in the body of the response. Copy the **access\_token** value.

The screenshot shows the response body of the token request, which is a JSON object. The status is 200 OK, and the response is displayed in 'Pretty' format:

```
1 {
2   "access_token": "[Redacted]",
3   "token_type": "Bearer",
4   "expires_in": 3600,
5   "scope": "api"
6 }
```

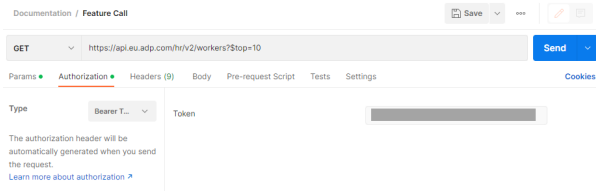
3. You will receive an Access Token in response, which is valid for 1 hour. The token can be used to make API calls by adding the following header:

**Authorization: Bearer {accessToken}**

## Making an API Call with Your Bearer Token

The following sample shows selecting the GET HR - Worker (List) API and making the first call.

1. In Postman open the **Feature Call** request.
2. Paste your bearer token into the Token field and click [Send].



If your request was successful you will receive an HTTP 200 message from the server within a few records. The following sample shows a response of the GET HR - Worker (List) API request:



### Chapter 3

## Frequently Encountered Errors and Resolutions

### Contacting your ADP representative

Before contacting your ADP representative for support first, please:

- Confirm that you have followed all the necessary steps to make calls to the ADP APIs.
- Check the errors outlined on this page to see if any of them match the error you get.

When contacting your ADP representative via ADP eService, please:

- Provide the **API call** you are executing. For example `GET https://api.eu.adp.com/hr/v2/workers?$top=10`.
- Provide the **error code** (status) and **message** you are getting.
- Provide the **ADP-CorrelationID** from the response headers.

KEY	VALUE
ADP-CorrelationID	492a5f78-6523-496b-bf60-b3a796fa8655

### HTTP 401 - invalid\_client

<b>Status</b>	401 Unauthorized
<b>Error</b>	invalid_client
<b>Error description</b>	The given client credentials were not valid

An HTTP 401 error is returned from the ADP Security Token Service when you do a token request call and fail to provide valid credentials in the request header.



```

Body Cookies Headers (8) Test Results Status: 401 Unauthorized Time: 37 ms Size: 374 B Save Response
Pretty Raw Preview Visualize JSON
1 {
2   "error": "invalid_client",
3   "error_description": "The given client credentials were not valid"
4 }

```

**Resolution**

Make sure you have the `client_id`, `client_secret` and `grant_type` in the authorization headers. Make sure you use the correct values for the `client_id` and `client_secret`. See [the previous chapter](#).

## HTTP 401 - invalid\_request

<b>Status</b>	401 Unauthorized
<b>Error</b>	invalid_request
<b>Error description</b>	proper client ssl certificate was not presented

An HTTP 401 error is returned from the ADP Security Token Service when you do a token request call and fail to provide the correct certificate. The certificate can be either missing or incorrect.

```

Body Cookies Headers (7) Test Results Status: 401 Unauthorized Time: 41 ms Size: 386 B Save Response
Pretty Raw Preview Visualize JSON
1 {
2   "error": "invalid_request",
3   "error_description": "proper client ssl certificate was not presented"
4 }

```

**Resolution**

Make sure you are including your ADP-issued SSL Certificate in the request. See [the previous chapter](#).

## HTTP 401 - Unauthorized

**Error**

An HTTP 401 Unauthorized error is returned when doing a feature call and you fail to provide a valid bearer token in the request header. Or the token you used, is expired.

```

Body Cookies Headers (9) Test Results Status: 401 Unauthorized Time: 173 ms Size: 805 B Save Response
Pretty Raw Preview Visualize JSON
1 {
2   "response": {
3     "responseCode": 401,
4     "methodCode": "GET",
5     "resourceUri": {
6       "href": "/hr/v2/workers"
7     }
8   },
9   "serverRequestDateTime": "2023-02-03T10:17:26.281Z",
10  "applicationCode": {
11    "code": 401,
12    "typeCode": "error",
13    "message": "Unauthorized"
14  },
15  "client_ip_address": "29.136.23.126",
16  "adp-correlationID": "eddccac7-e501-466a-87a5-57b090d2544"
17 }

```

**Resolution**

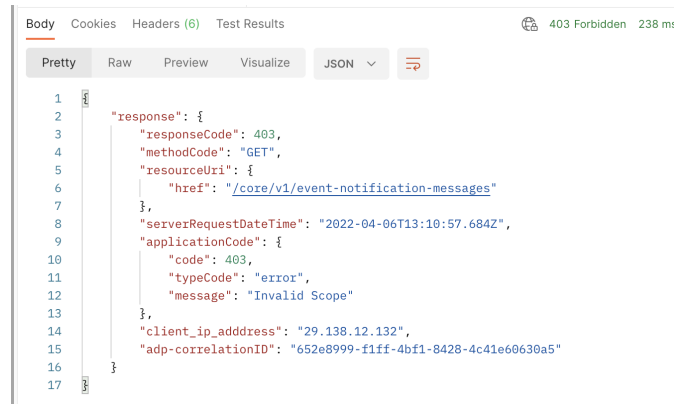
Make sure you have added an Authorization header to your request along with a valid bearer token you fetched from the ADP Security Token Service. The Header `WWW-Authenticate` will provide the value `Bearer error="Invalid request"` when this occurs.

KEY	VALUE
ADP-CorrelationID	09b7bbb2-d448-4e3e-b61f-892aab40778
WWW-Authenticate	Bearer error="Invalid request"

## HTTP 403 - Invalid scope

### Error

An HTTP 403 Invalid scope error is returned from the server when the bearer token you provided is valid, but you are not authorized to access the resource you have requested.



```
Body Cookies Headers (6) Test Results 403 Forbidden 238 ms
Pretty Raw Preview Visualize JSON
1
2 "response": {
3   "responseCode": 403,
4   "methodCode": "GET",
5   "resourceUri": {
6     "href": "/core/v1/event-notification-messages"
7   },
8   "serverRequestDateTime": "2022-04-06T13:10:57.684Z",
9   "applicationCode": {
10    "code": 403,
11    "typeCode": "error",
12    "message": "Invalid Scope"
13  },
14  "client_ip_address": "29.138.12.132",
15  "adp-correlationID": "652e8999-f1ff-4bf1-8428-4c41e60630a5"
16 }
17
```

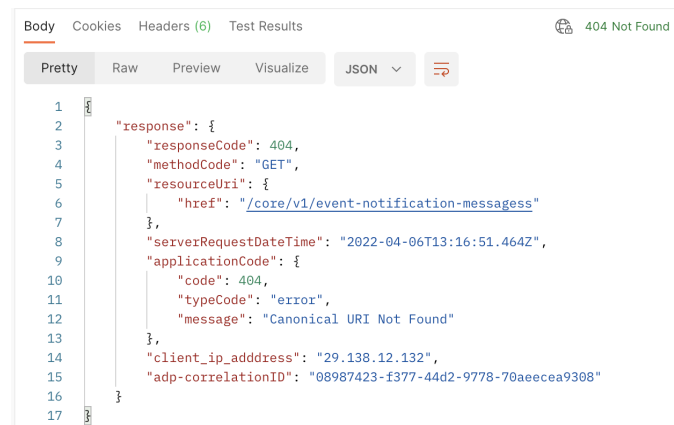
### Resolution

First confirm that you have not made a mistake in the request Uniform Resource Indicator (URI). If there quest URI is correct, contact your ADP Representative to request access to the URI in question.

## HTTP 404 - Canonical URI not found

### Error

An HTTP 404 error is returned from the server when the URL you provided is invalid.



```
Body Cookies Headers (6) Test Results 404 Not Found
Pretty Raw Preview Visualize JSON
1
2 "response": {
3   "responseCode": 404,
4   "methodCode": "GET",
5   "resourceUri": {
6     "href": "/core/v1/event-notification-messages"
7   },
8   "serverRequestDateTime": "2022-04-06T13:16:51.464Z",
9   "applicationCode": {
10    "code": 404,
11    "typeCode": "error",
12    "message": "Canonical URI Not Found"
13  },
14  "client_ip_address": "29.138.12.132",
15  "adp-correlationID": "08987423-f377-44d2-9778-70aeecea9308"
16 }
17
```

### Resolution

First confirm that you have not made a mistake in the requested URL. If the requested URL is correct, contact your ADP representative.

## Chapter 4

# 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.

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.