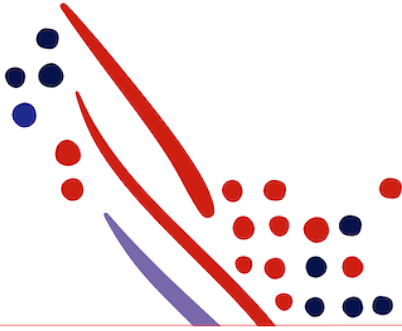Guide

ADP Marketplace ESI - Making your first API call using Postman

Published on
Mar 31, 2022, 09:50 AM

Last modified
Aug 08, 2024, 02:09 PM

ADP Copyright Information

Published on
Mar 31, 2022, 09:50 AM

Published on
Aug 08, 2024, 02:09 PM
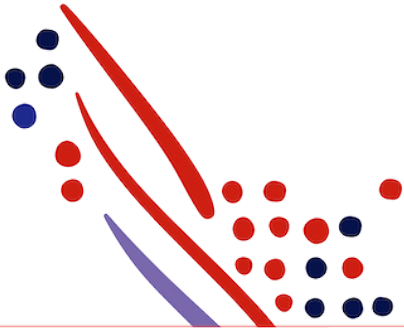
Table of Contents

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.

- Allowed access to ADP API Gateway IP addresses
  - 195.200.255.231
    195.200.255.232

Endpoints

The endpoints for ADP Marketplace International are:

- Token call: https://accounts.**eu**.adp.com/auth/oauth/v2/token
- Feature call: https://api.**eu**.adp.com/{URI}

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).

- Click *Settings.*
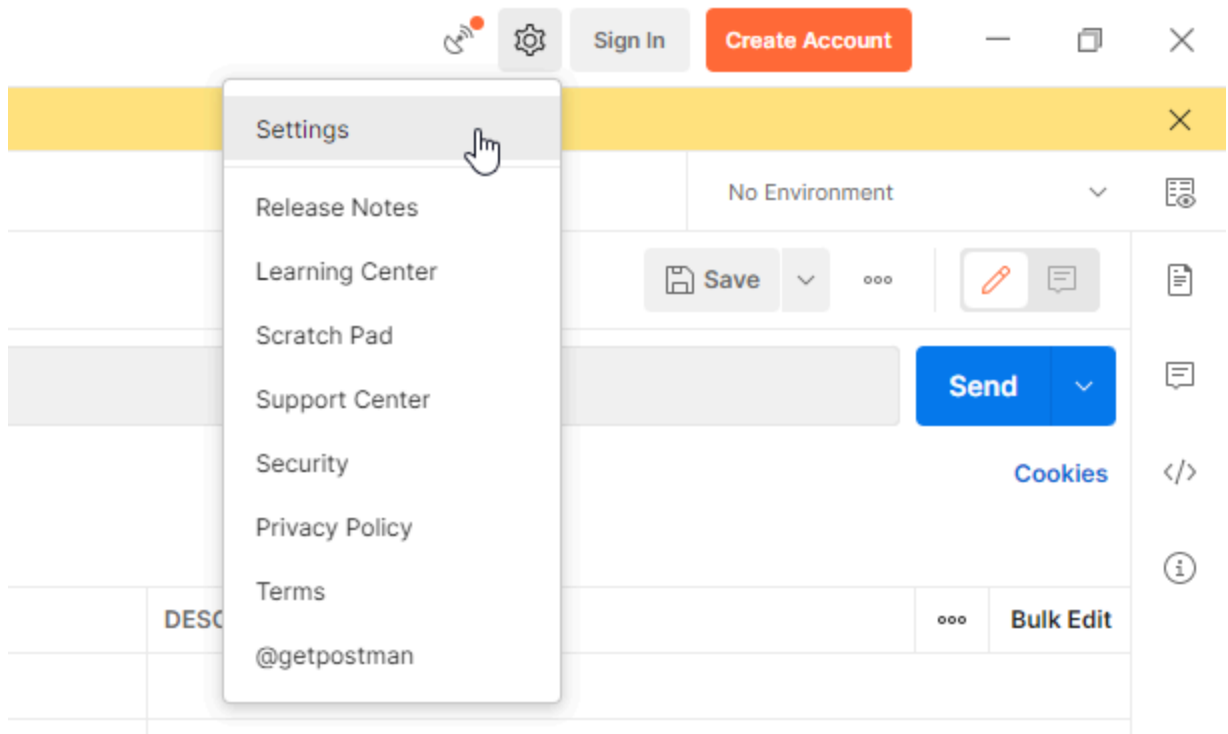
- Click *Certificates, Add Certificates.*

- For Host enter the value **accounts.eu.adp.com**

- Next to *CRT file* click [Select file], browse to your ADP issued certificate (.CER file) and click [Open].

- Next to *KEY file* click [Select file], browse to your private key (.KEY file generated as part of the CSR process) and click [Open].

- Click [Add].
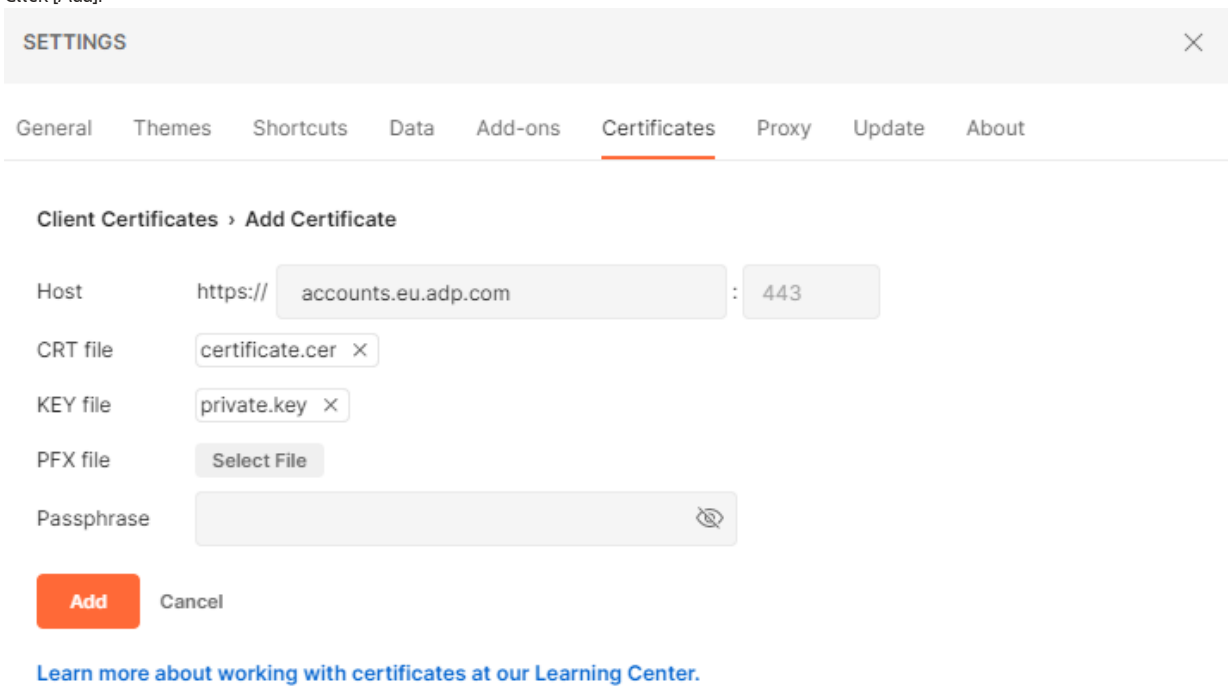
- Repeat the steps above for the host **api.eu.adp.com**

SETTINGS   ✕

General   Themes   Shortcuts   Data   Add-ons   Certificates   Proxy   Update   About

CA Certificates   ⬤ OFF

The file should consist of one or more trusted certificates in PEM format.

PEM file   Select File

Client Certificates   **Add Certificate**

Add and manage SSL certificates on a per domain basis.

Learn more about working with certificates at our Learning Center ↗

Host   accounts.eu.adp.com   **Remove**
CRT file
KEY file

Host   api.eu.adp.com   **Remove**
CRT file
KEY file

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

SETTINGS   ✕

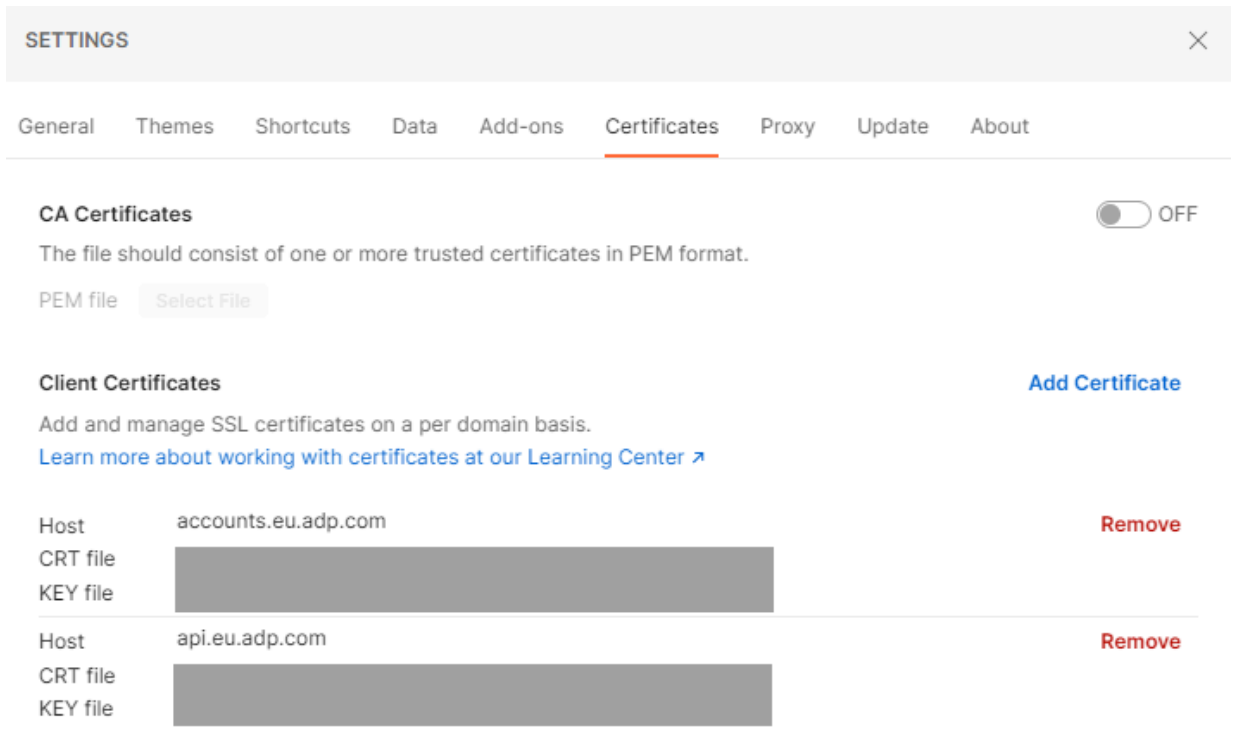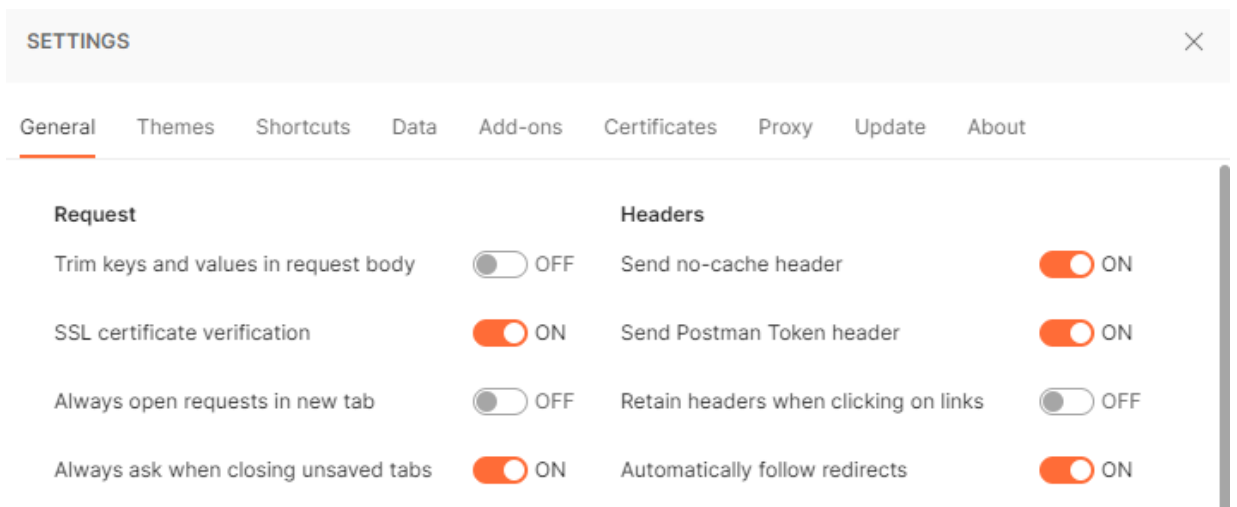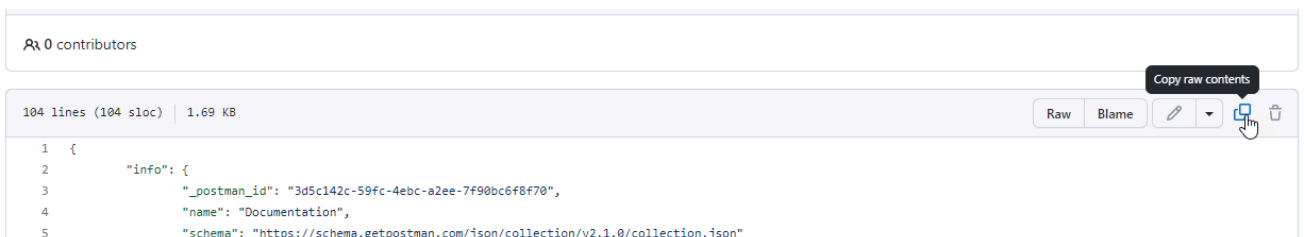General   Themes   Shortcuts   Data   Add-ons   Certificates   Proxy   Update   About

Request   **Headers**

Trim keys and values in request body ⬤ OFF   Send no-cache header   ⬤ ON

SSL certificate verification   ⬤ ON   Send Postman Token header   ⬤ ON

Always open requests in new tab   ⬤ OFF   Retain headers when clicking on links ⬤ OFF

Always ask when closing unsaved tabs ⬤ ON   Automatically follow redirects   ⬤ ON

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*.

ጸ 0 contributors

104 lines (104 sloc) 1.69 KB   Raw   Blame   ✏ ▼   ⎘   🗑
                                                          Copy raw contents

1 {
2   "info": {
3   "_postman_id": "3d5c142c-59fc-4ebc-a2ee-7f90bc6f8f70",
4   "name": "Documentation",
5   "schema": "https://schema.getpostman.com/json/collection/v2.1.0/collection.json"

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

Import ✕

File   Folder   Link   **Raw text**   Code repository New

Paste raw text

```
                                        "com"
                                    ],
                                    "path": [
                                        "auth",
                                        "oauth",
                                        "v2",
                                        "token"
                                    ]
                                }
                            },
                            "response": []
                        }
                    ],
                    "protocolProfileBehavior": {}
                }
```
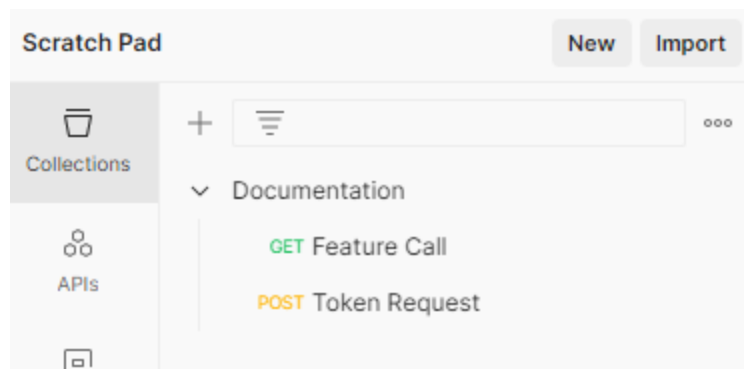
Continue

- Click [Continue] and [Import].

Import ✕

Select files to import · 1/1 selected

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.

Making your first call

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].

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.

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:
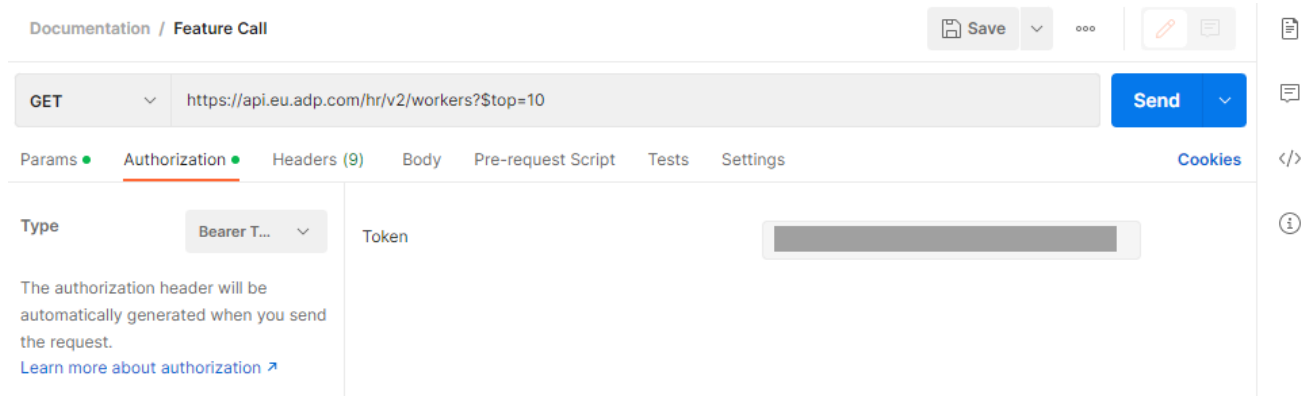
   Authorization: Bearer {accessToken}

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:
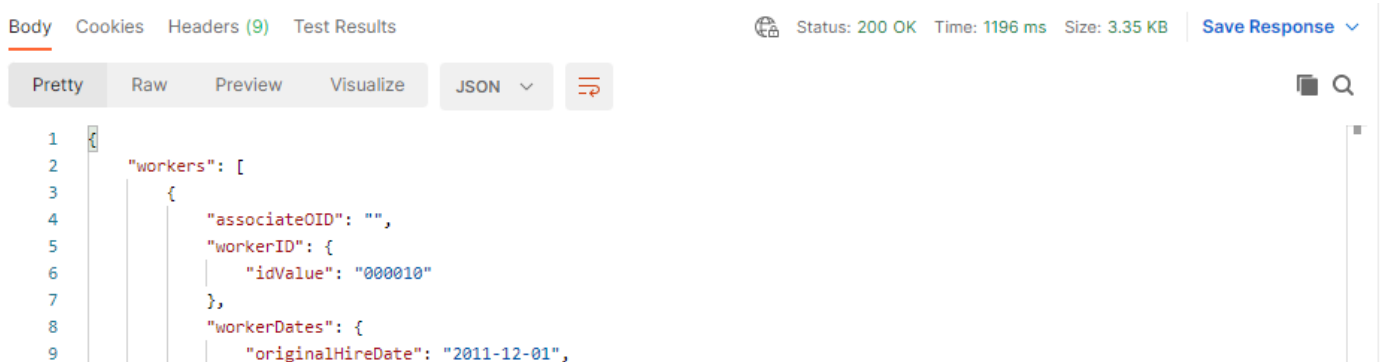
Frequently Encountered Errors and Resolutions

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 reponse headers.

HTTP 401 - invalid_client

Status	401 Unauthorized
Error	invalid_client
Error description	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.

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

Status	401 Unauthorized
Error	invalid_request
Error description	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.

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.

```json
{
    "response": {
        "responseCode": 401,
        "methodCode": "GET",
        "resourceUri": {
            "href": "/hr/v2/workers"
        },
        "serverRequestDateTime": "2023-02-03T10:17:26.281Z",
        "applicationCode": {
            "code": 401,
            "typeCode": "error",
            "message": "Unauthorized"
        },
        "client_ip_adddress": "29.136.23.126",
        "adp-correlationID": "eddcacd7-e501-4dda-87a5-57b8b90d2544"
    }
}
```

Body Cookies Headers (9) Test Results Status: 401 Unauthorized Time: 173 ms Size: 805 B Save Response ∨

Pretty Raw Preview Visualize JSON ∨

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.

Body Cookies Headers (9) Test Results Status: 401 Unauthorized Time: 142 ms Size: 805 B Save Response ∨

KEY	VALUE
ADP-CorrelationID ⓘ	09b7bbb2-dd48-4e3e-b61f-892aabf40778
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_adddress": "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 ⌄

```json
1  {
2      "response": {
3          "responseCode": 404,
4          "methodCode": "GET",
5          "resourceUri": {
6              "href": "/core/v1/event-notification-messagess"
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_adddress": "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.