Make Your First API Call Using Postman

FOR ADP AUTHORIZED USERS ONLY

Contents

- Overview
- Prerequisite
- Installing and Preparing Postman
- Making Your First Call
  - Requesting a Bearer Token
  - Making an API Call with Your Bearer Token
- Frequently Encountered Errors and Resolutions
  - Received an HTTP 401 Error When Trying to Authenticate with ADP’s Security Token Service
  - Received an HTTP 401 Error From Other APIs
  - Received an HTTP 403 Error

Overview

This guide provides an overview of using Postman to make your first Application Programming Interface (API) call to ADP®. if you are already familiar with Postman then you can skip this document.

Prerequisite

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

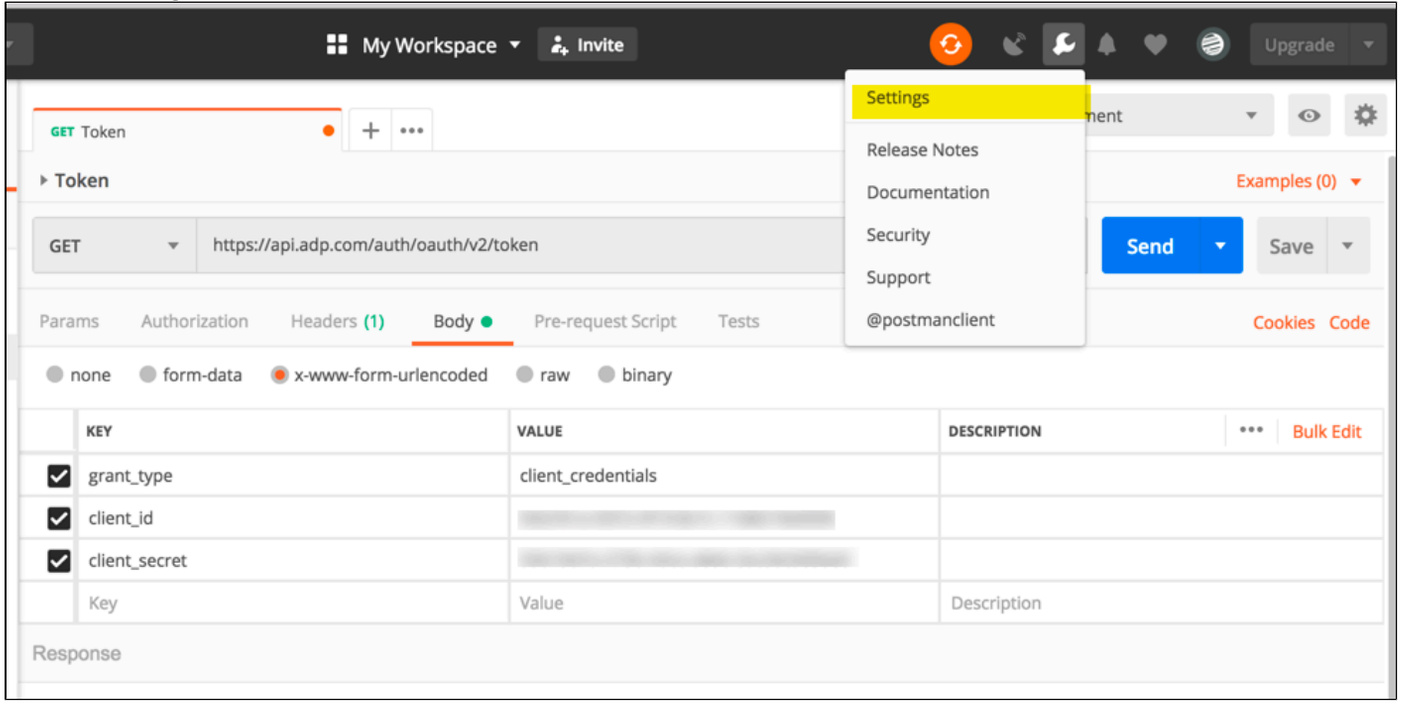
- Client ID and Client Secret. If you don't have this information, contact your client representative.
- A Certificate Signing Request (CSR). For more detailed information, see the Certificate Signing Request Guide.

Installing and Preparing Postman

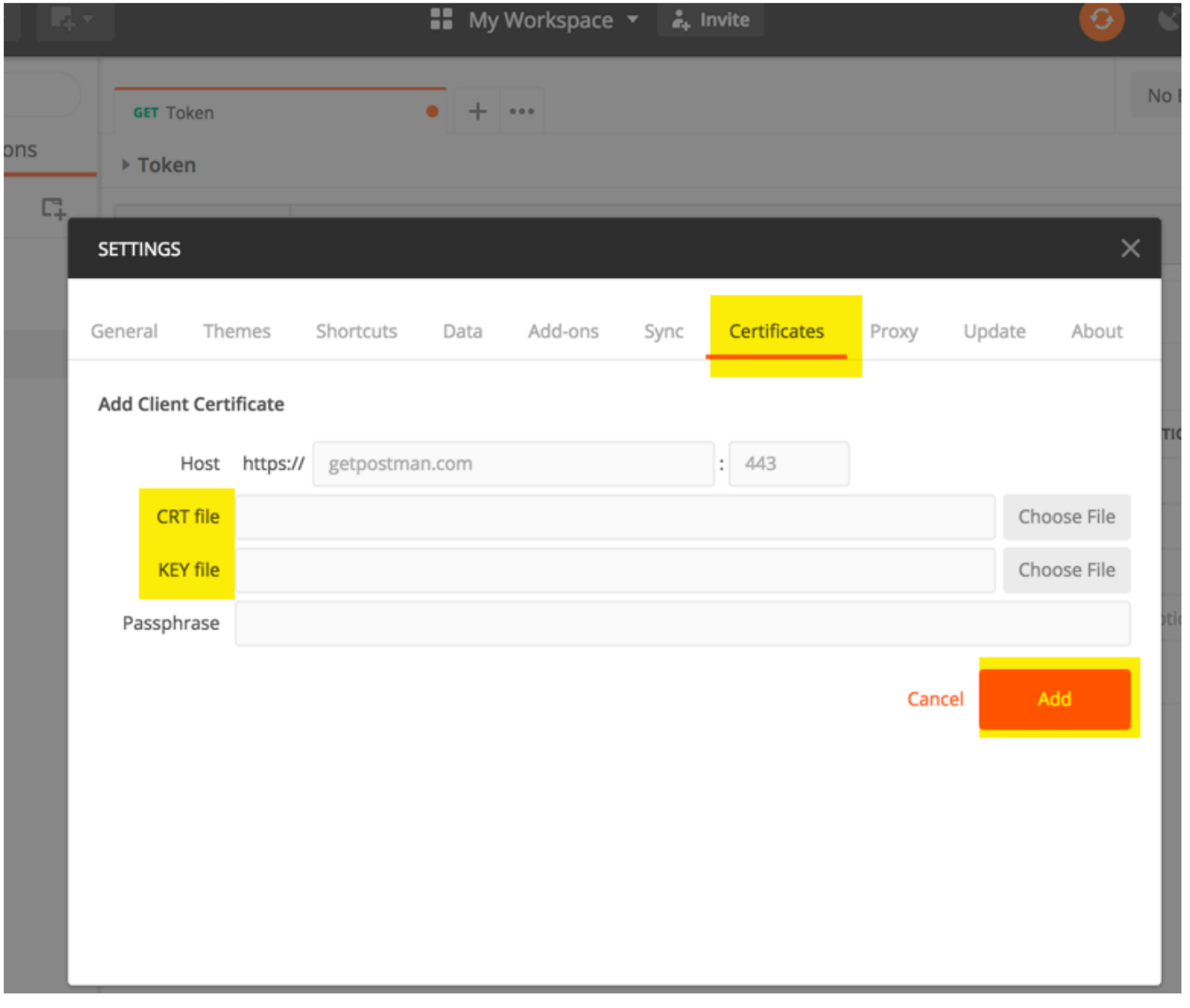
1. Install Postman from https://www.getpostman.com/apps .

   Add your ADP issued .PEM file and your .KEY file (as part of the CSR process) into Postman for the domains using the following steps (you can use the instructions found at https://www.getpostman.com/docs/postman/sending_api_requests/certificates):

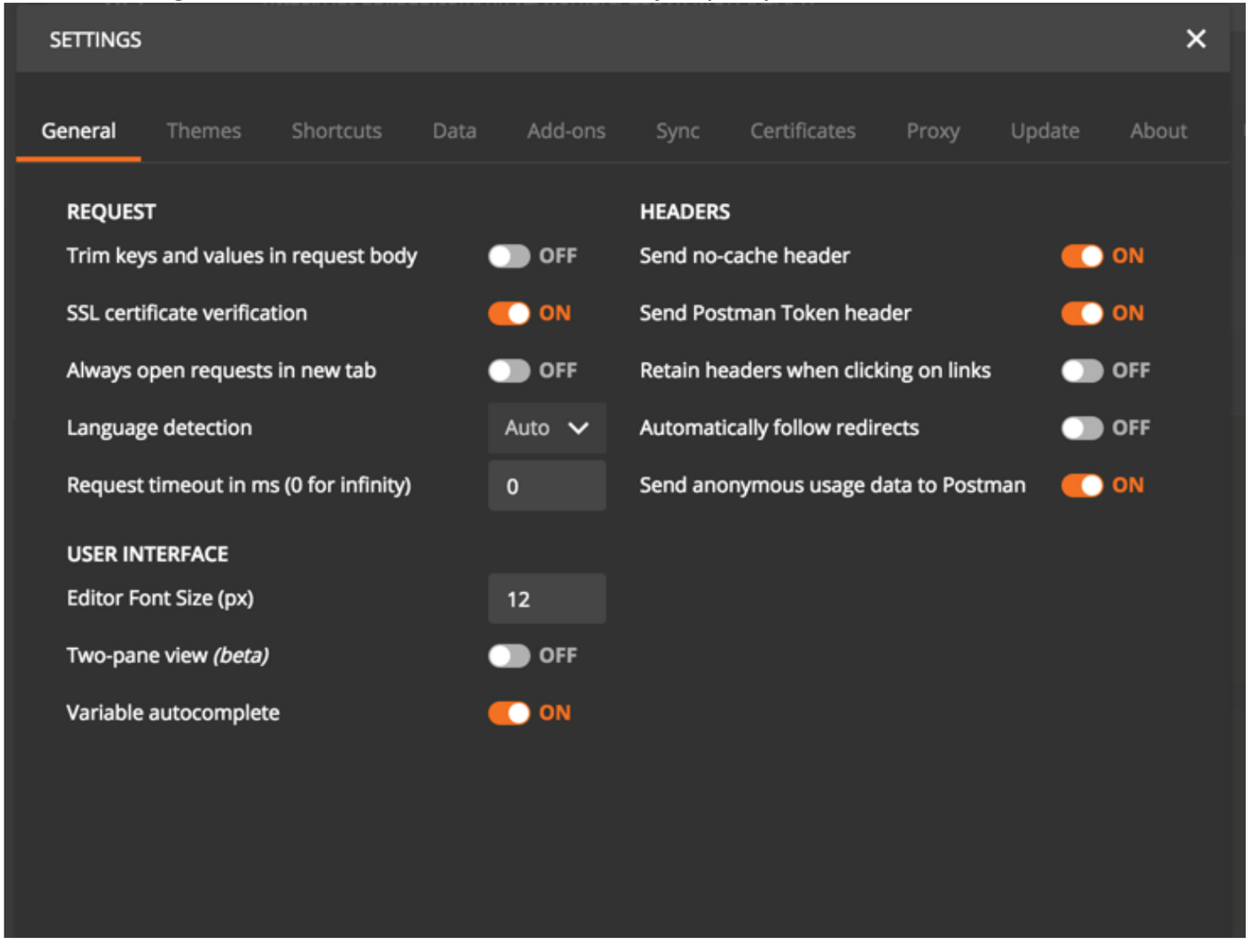
   a. Click **Settings**.



b. Click **Certificates** , select the certificate and KEY files. Then, click **Add** .

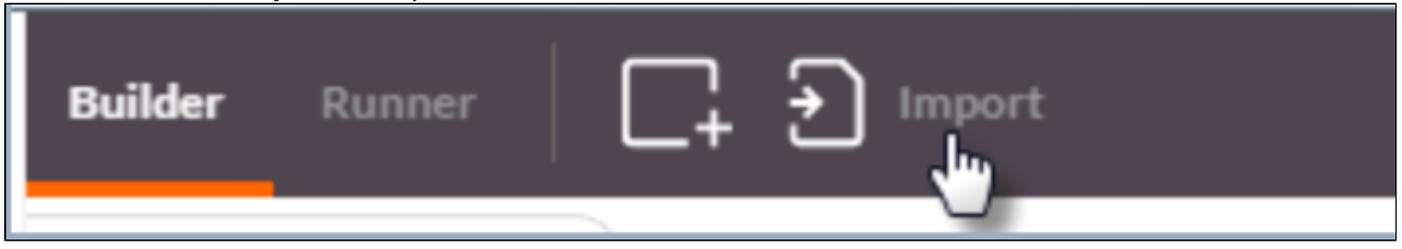


c. On the **Settings** screen, turn the Secure Sockets Layer (SSL) Certificate on.



HINTS: If you're not prompted to select an SSL certificate and this is your first request in this Postman session, you should check to make sure your SSL certificate is installed correctly. Once you have selected the proper certificate, you will not be prompted for a certificate again until you start a new Postman session. If you know your SSL certificate is installed correctly, close Postman and open the Google Chrome browser instances and try your request again.

2. (Optional) Import the ADP APIs.
   RESULT: Postman allows you to store a collection of APIs and share with others. ADP will continue to share sample collections on GITHUB. For example, you can find the ADP Workforce Now (WFN)® collection by clicking on this link. When at the location, download the file and click **Import** to import the list file.

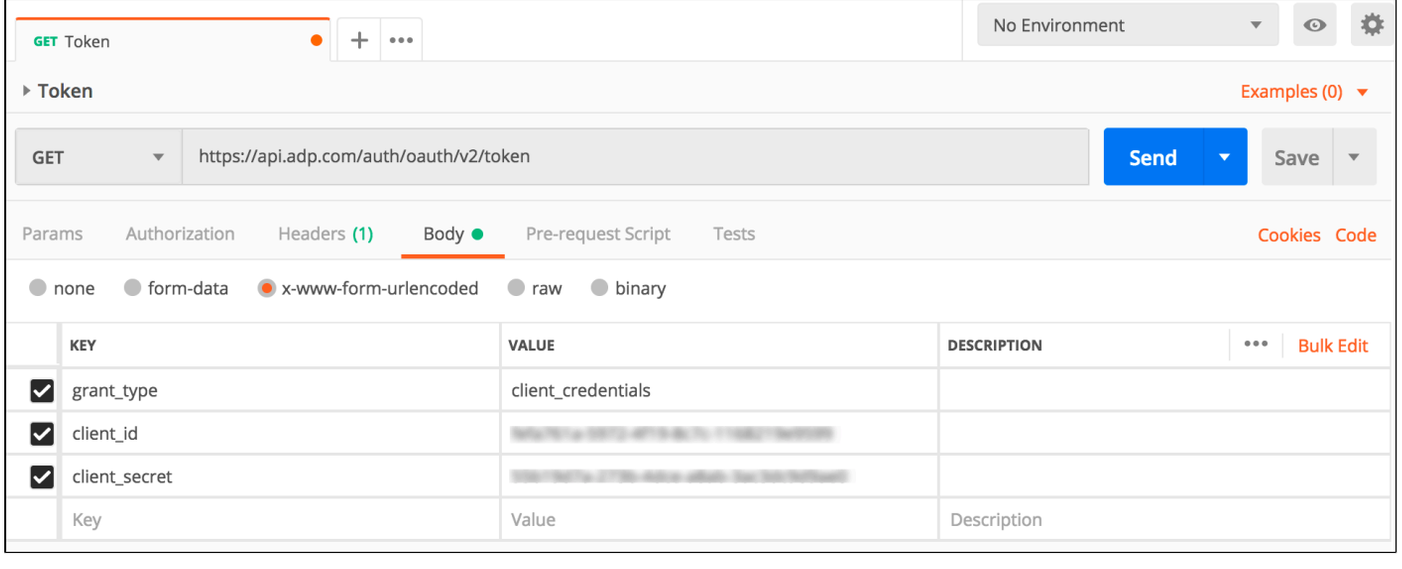


Making Your First Call

Requesting a Bearer Token

Each request to one of ADP's APIs needs to be accompanied by an Authorization header containing a bearer token issued by ADP Security Token Service.

1. In Postman, open the **Token Request** and to expose the headers, click **Headers** .



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 same can be used to make api calls by adding the following header:

   Authorization: Bearer {accessToken}

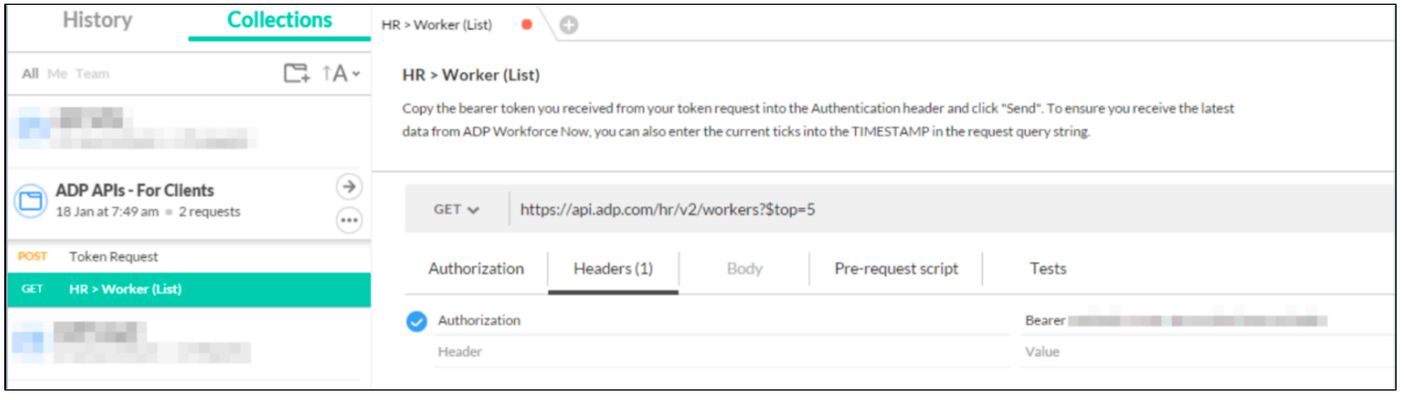
   NOTE: Postman allows you to store a collection of APIs and share with others. ADP will continue to share sample collections on GITHUB. For example, you can find the ADP Workforce Now (WFN)® collection by clicking on this link. When at the location, download the file and click **Import** to import the list file.

Making an API Call with Your Bearer Token

If you already have an API collection, you can select an API from a collection. The sample below shows the steps of pick the GET HR - Worker (List) API and make the first call.

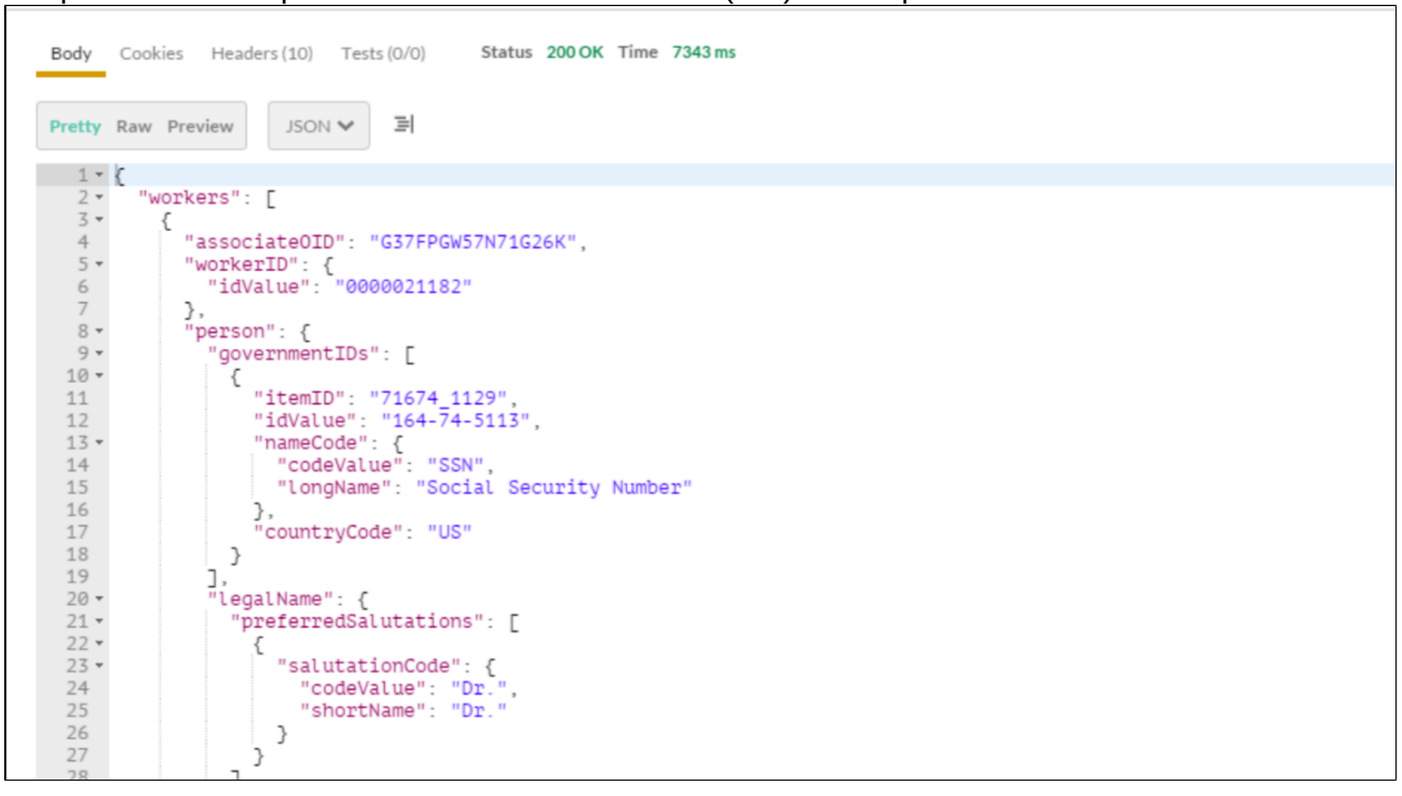
1. Open the **HR > Worker (List)** request and click **Headers** to expose the headers.

2. Paste your bearer token into the **Authorization** header and click **Send**.



NOTE: Remember to leave the **Bearer** and a space to the left of your token. Since Postman is a browser-based application, the browser caching mechanism will save responses to the cache. To ensure that changes you make in ADP applications are reflected in Postman, we recommend placing a cache-buster into the query string between each request. For example, **'preventCache=timestamp'**, where timestamp is a unique value such as the current time's ticks. You won't need to do this when you're building your application because browser-based caching won't come into play.

RESULT: If your request was successful, you'll 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

Received an HTTP 401 Error When Trying to Authenticate with ADP's Security Token Service

Error:

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

Resolution:

Take the following suggested troubleshooting steps before contacting your ADP Representative for assistance:

1. Make sure you have base-64 encoded in your OAuth2 Client ID and Client Secret before sending them to the Authorization header.
2. Make sure you are also base- 64 encoding the colon (":") between your OAuth2 Client ID and Client Secret.
3. Make sure there is a space between **Basic** and your base -64 encoded credentials.
4. Make sure you are including your ADP-issued SSL Certificate in the request.

Received an HTTP 401 Error From Other APIs

Error:

An HTTP 401 error is returned from APIs other than the ADP Security Token Service when you fail to provide a valid bearer token in the request header.

Resolution:

Take the following suggested troubleshooting steps before contacting your ADP Representative for assistance:

- Make sure you have added an Authorization header to your request along with the bearer token you fetched from the ADP Security Token Service.
- Make sure you have a space between **Bearer** and the token you are using in the Authorization header.
- Check the body of the response for an "expired token" message. If that message is present in the response, fetching a fresh bearer token and resubmitting your request should resolve the issue.

Received an HTTP 403 Error

Error:

An HTTP 403 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.

Resolution:

First, confirm that you have not made a mistake in the request URI. If the request URI is correct, contact your ADP Representative to request access to the URI in question.

Other Useful Links

API Common Exceptions and Tips for Handling

