

Postman Configuration

ThreatConnect offers a v3 API collection that you can fork or import into Postman™. This document details how to fork and import the ThreatConnect v3 API collection, configure the collection's variables, and make an API request using the collection.

Step 1: Fork or Import the ThreatConnect v3 API Collection

Click the **Run in Postman** button: . The **Fork collection into your workspace** screen will be displayed (Figure 1).

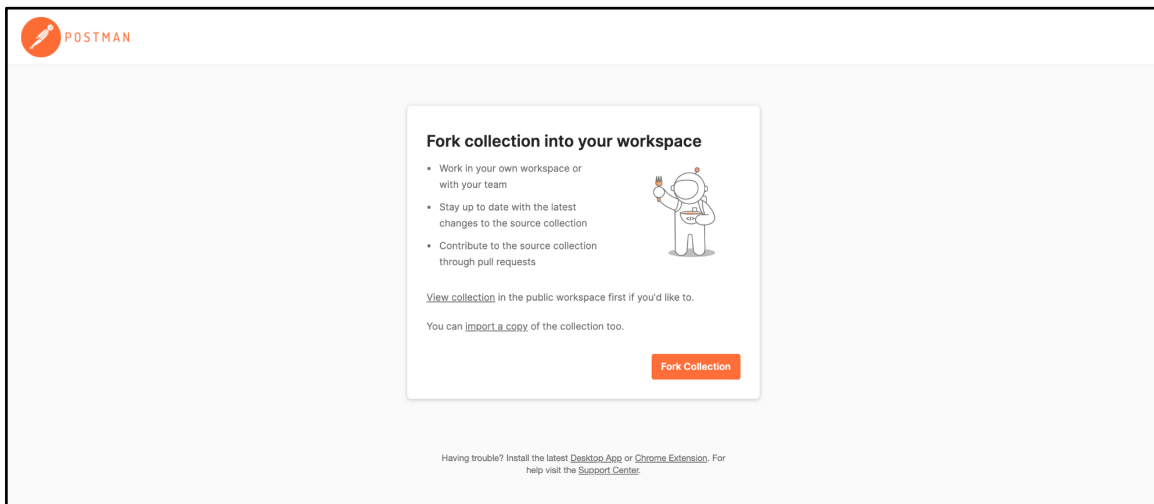



Figure 1

 **IMPORTANT:** You cannot create a workspace when prompted to select one on the **Fork collection** screen (Figure 2) and **Import collection** window of the Postman desktop app (Figure 3). Therefore, before forking or importing the v3 API collection, make sure to [create the workspace](#) into which the collection will be forked or imported.

On the **Fork collection into your workspace** screen, select one of the following options:

- Click the **Fork Collection** button to fork the collection into your Postman workspace. Your Postman profile must be public to fork a collection in a public workspace.
- Click the [import a copy](#) link to import a copy of the collection into your workspace. You must use the [Postman desktop app](#) to import a collection into your workspace.

Fork the Collection

After clicking the **Fork Collection** button, the **Fork collection** screen will be displayed (Figure 2).

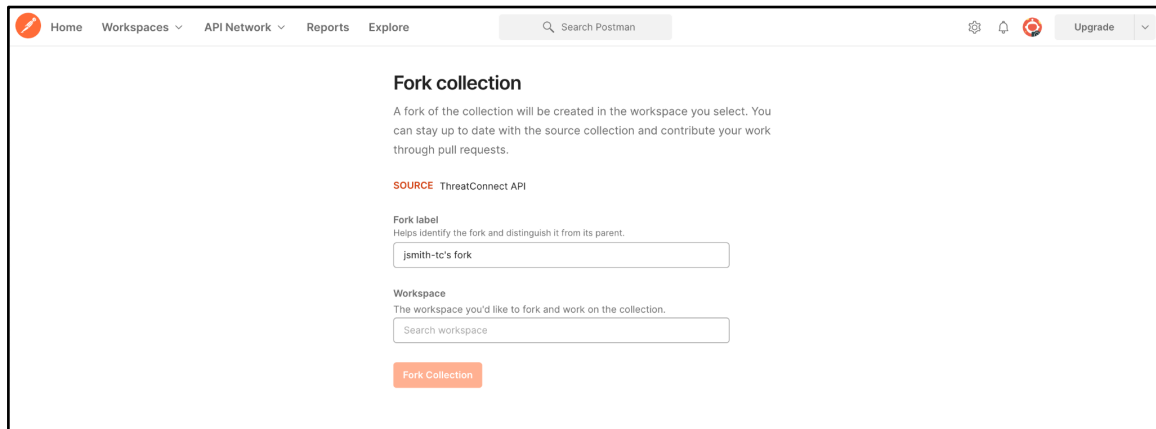



Figure 2

- **Fork label:** This field is automatically populated with your Postman username, followed by 's fork' (e.g., **jsmith-tc's fork**). Edit the fork label, if desired.
- **Workspace:** Search for and select a workspace into which a fork of the collection will be created.
- Click the **Fork Collection** button. A collection named **ThreatConnect API**, followed by the fork label, will be displayed under the **Collections** tab of the side navigation bar.

 **NOTE:** You must make your Postman profile public to fork a collection from a public workspace. If your Postman profile is private, you will be prompted to make it public after clicking the **Fork Collection** button. If you do not want to make your Postman profile public, [import a copy of the collection into your workspace via the Postman desktop app](#) instead.

Import a Copy of the Collection

After clicking the [import a copy](#) link, you will be prompted to open the [Postman desktop app](#) (or download the app if it is not installed on your computer). After the Postman desktop app opens, the **Import collection** window will be displayed (Figure 3).

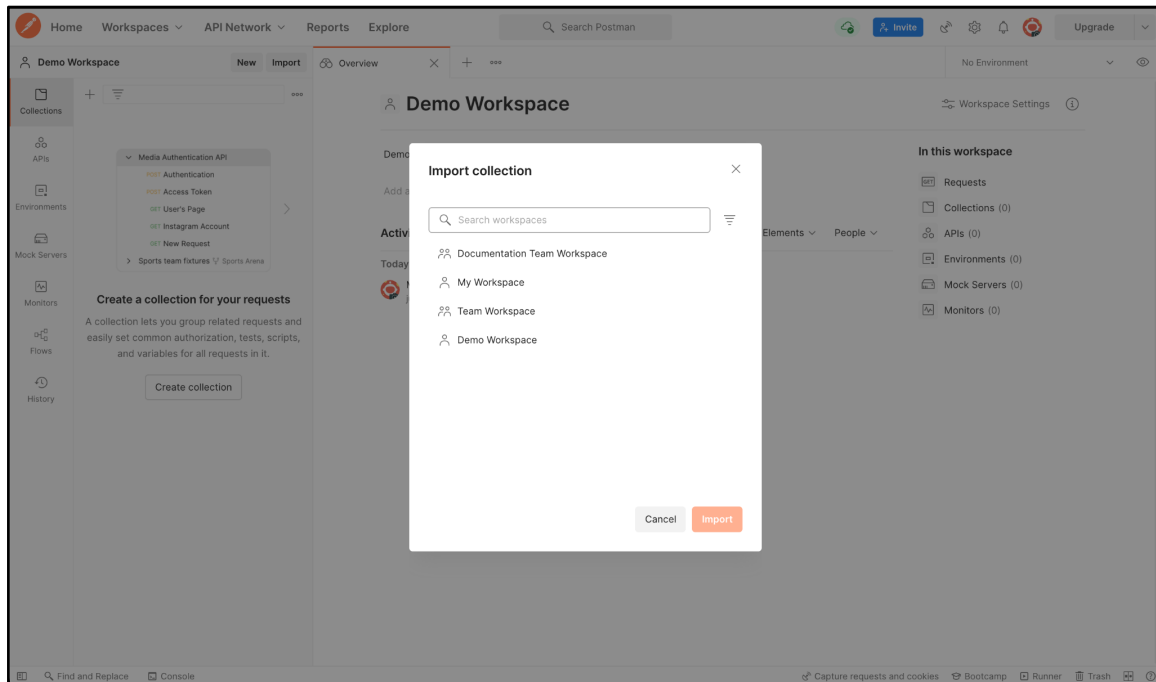


Figure 3

- Select the workspace into which the collection will be imported.
- Click the **Import** button. A collection named **ThreatConnect API** will be displayed under the **Collections** tab of the side navigation bar.

Step 2: Configure the ThreatConnect v3 API Collection

On the **Collections** tab, select the **ThreatConnect API** collection that was either forked or imported into your workspace. A **ThreatConnect API** tab will open with the **Authentication** subtab selected (Figure 4).

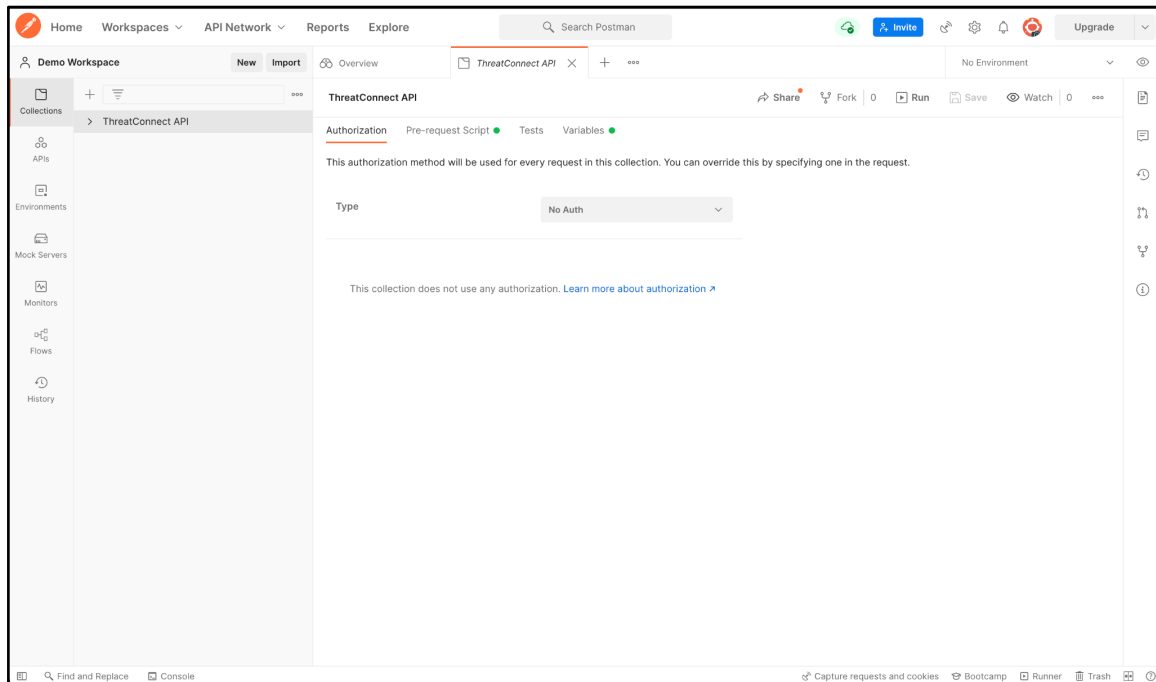


Figure 4

Leave the authentication type set to **No Auth**, as the pre-request script included in the collection will perform all steps necessary for the authentication process.

Select the **Variables** subtab to display the variables in the **ThreatConnect API** collection. The ThreatConnect API supports [hash-based message authentication code \(HMAC\)](#) and [token-based authentication](#). Based on the type of authentication you will be using, fill out the corresponding variables as detailed in the following sections.

IMPORTANT: If you enter an API token in addition to your ThreatConnect Access ID and Secret Key, token-based authentication will be used instead of HMAC authentication. However, if your token expires and you do not update the value for the **tcToken** variable, or clear its checkbox, token-based authentication will still be used instead of HMAC authentication. Therefore, **it is recommended to use one authentication method only**.


HMAC Authentication

- **baseUrl:** By default, this variable is set to the API URL for ThreatConnect's Public Cloud instance. If you are using an On-Premise or Dedicated Cloud ThreatConnect instance, enter the API URL for your instance (e.g., `https://companyabc.threatconnect.com/api`).
- **tcAccessId:** Enter the Access ID for your [ThreatConnect API user account](#) in the **CURRENT VALUE** column.
- **tcSecretKey:** Enter the Secret Key for your ThreatConnect API user account in the **CURRENT VALUE** column.

- **tcToken**: Clear the checkbox for this variable.
- Click the **Save** button in the top toolbar of the **ThreatConnect API** tab.

Token-based Authentication

- **baseUrl**: By default, this variable is set to the API URL for ThreatConnect's Public Cloud instance. If you are using an On-Premise or Dedicated Cloud ThreatConnect instance, enter the API URL for your instance (e.g., `https://companyabc.threatconnect.com/api`).
- **tcAccessId**: Clear the checkbox for this variable.
- **tcSecretKey**: Clear the checkbox for this variable.
- **tcToken**: Enter a ThreatConnect API token created by your Organization Administrator in the **CURRENT VALUE** column.
- Click the **Save** button in the top toolbar of the **ThreatConnect API** tab.

 **IMPORTANT**: ThreatConnect API tokens **expire automatically after four hours**. To obtain a new API token, contact your Organization Administrator. Instructions for creating an API token are available in the "API Token" section of *ThreatConnect Organization Administration Guide*.

Step 3: Make a ThreatConnect API Request in Postman

1. Expand the **ThreatConnect API** collection on the **Collections** tab to display a **v3** folder.
2. Expand the **v3** folder to view folders for each endpoint in v3 of ThreatConnect's API.
3. Expand an endpoint's folder (**indicators** in this example) to view available requests for the endpoint.
4. Select an API request from the endpoint's folder (**GET Retrieve Indicators** in this example). A new tab will be opened for the selected API request.
5. Click the **Send** button to the right of the request URL. If you connected successfully to the ThreatConnect API, response data will be displayed in the lower pane of the tab for the API request.

You're now ready to use the ThreatConnect API collection in Postman. To learn more about each endpoint in v3 of the ThreatConnect API, select an endpoint under the **THREATCONNECT API** section of the [API Reference documentation](#).

Optional: Create Environments in Postman

If you use multiple ThreatConnect instances, it can be helpful to [create an environment](#) for each instance with the [variables included in this collection](#) via the **Environments** tab on the side navigation bar. Once you have created environments for each ThreatConnect instance you access, [select the environment](#) from the **Environment** dropdown when [making API requests in Postman](#).