



aqua

Aqua Postman Collections

Overview

This guide serves as a reference for both SaaS and Self-Hosted environments

The purpose of this document is to provide guidance on how to leverage the Aqua Postman Collections within your organization to perform API requests to the targeted endpoints. The guide will cover creating API Keys, assigning roles to keys, API payload, generating tokens, importing the environments and collections, and finally how to leverage the imports for multiple Aqua environments. This guide assumes that permission sets and roles are already created in the environment and will not cover those topics, it is included in the [references](#) section if more information is required. If there are any questions or concerns, please contact Aqua Support

Prerequisites

An Aqua Admin must perform the following steps on either SaaS or Self-Hosted

For either SaaS or Self-Hosted, the workload protection module requires a **role** to be created which is dependent on a **permission set** also being created. The roles and permissions provide the following:

- what the token will have access to
- what the token can do with the resources it has access to

Both roles and permission sets will not be covered in this guide, but referenced in the [references](#) section below

SaaS

It is recommended to create either 2 or 3 API Keys. One specifically for the CWPP module and either a shared one for both CSPM/SSCS or one per module

An **API Key** must be generated to leverage the API automation, each section will describe the **different permissions** each API Key needs while this section provides guidance on how to create them.

Steps to generate an API Key:

Do not select a **group** for the API Key when editing the key to perform the task, ensure group remains blank. **Save** the API Keys as soon as they are generated

1. Navigate to **Account Management**



Aqua Hub

Context aware risk management of cloud and Kubernetes resources

Supply Chain Security

Protect your software supply chain and source code

CSPM

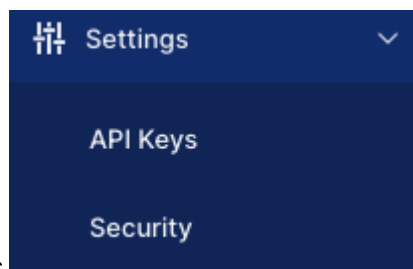
Monitor cloud infrastructure security and compliance risks

Workload Protection

Runtime protection for cloud native applications

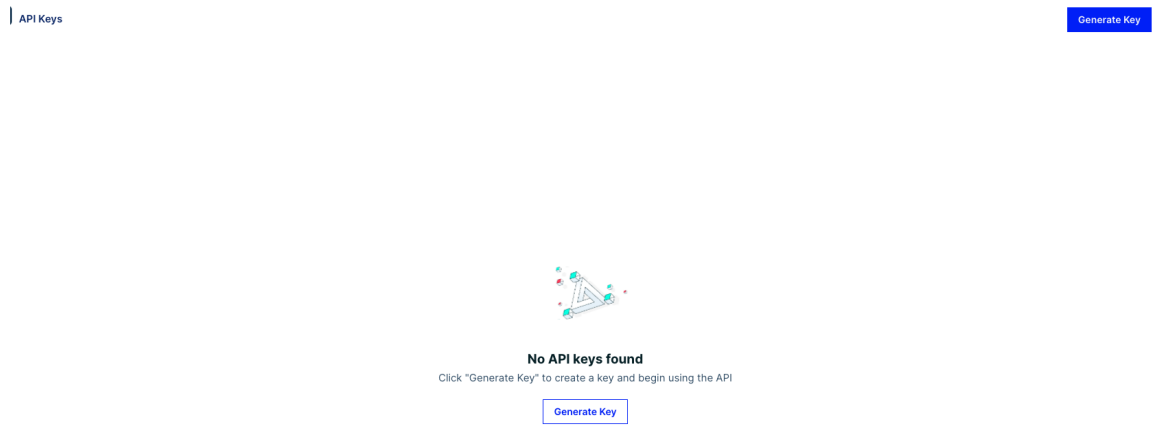
Account Management

Manage users, roles, permissions, and billing



2. Click on **Settings**

3. Click on **Generate Key**



4. Upon clicking **Generate Key**, the API Key and Secret will display. **Save** them immediately.

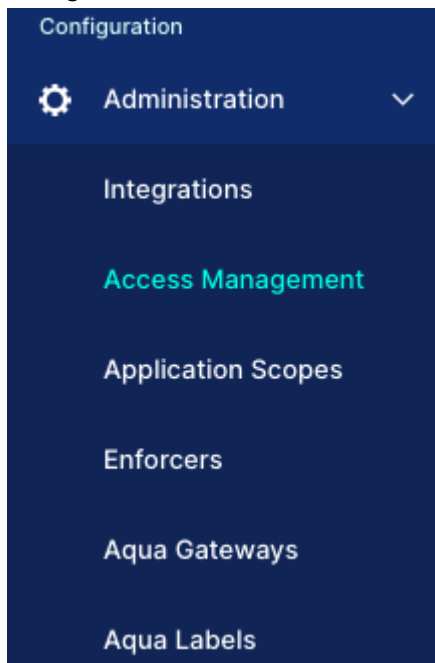
The generation of API Keys is not completed, refer to each section as to what permissions are required for the Postman Collections to work! **Happy Automating!**

Self-Hosted

Self-Hosted is not dependent on API Keys, it is dependent on a user with sufficient access to generate a token to perform the API capabilities. This section will guide on how to create a user and assign an existing role to it.

To create a User:

1. Navigate to **Administration** and click on **Access Management**



2. Click create **Add User**

Access Management 🔄

[Users](#) [Roles](#) [Permission Sets](#)

Search by user name

[Add User](#)

<input type="checkbox"/>	Display Name ↕	User Name ↕	Status ↕	Email ↕	Password reset ↕	Roles
<input type="checkbox"/>	🔗 administrator	administrator	Active		No	Administrator

3. Provide a desired **username** and **password**, select the **role**, optionally enter a **Display Name**, and **email** to indicate an owner or shared mailbox to send password resets to. Once completed click **Save**

[Users](#) > New User [Save](#) [Cancel](#)

* Username

0/100

This is the name used for authentication.

* Password

* Confirm Password

* Roles

▼

Display Name (optional)

0/100

Email (optional)

☐ User must change password at next login

A new user with automation privileges has been created! **Happy Automating!**

Aqua Container Workload Protection Platform (CWPP)

The CWPP module for both SaaS and Self-Hosted rely on a **Bearer Token** to be generated for the API Automation.

SaaS and Self-hosted create the **Bearer Token** in distinct ways in order to use them in the api calls. Below are the details as to how each generate the token:

- **SaaS** utilizes API Keys and roles to generate the token.
- **Self-Hosted** leverages username/password with an assigned role to generate one.

This section will break down the permissions for the API key needed for SaaS

To ensure the API Key created in the [prerequisites](#) section works for the CWPP module, the following **must** be completed:

1. Navigate to **Account Management**



Aqua Hub

Context aware risk management of cloud and Kubernetes resources

Supply Chain Security

Protect your software supply chain and source code

CSPM

Monitor cloud infrastructure security and compliance risks

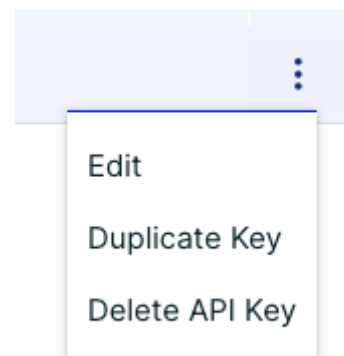
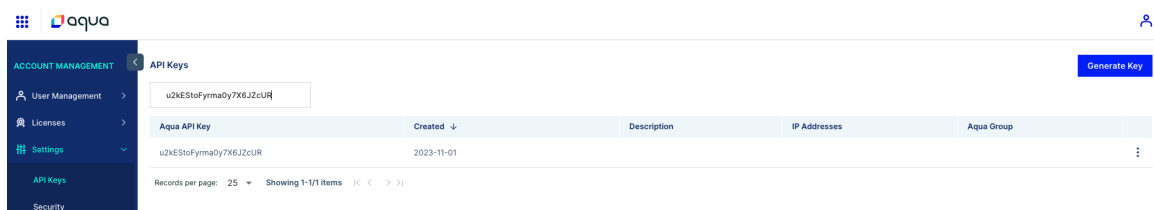
Workload Protection

Runtime protection for cloud native applications

Account Management

Manage users, roles, permissions, and billing

2. Click on **Settings** followed by **API Keys** and search for your **API Key** created in the prerequisites section



3. Click on the ellipses on the far right of the key and select **Edit**

4. Once the menu pops up, enter a description to identify the key usage and disable the **Global Admin** slider

Edit API Key



Description

CWPP Postman Key

IP Addresses

Note: Allowed IP(s) come in the form of comma delimited IP sequence. Leaving this field empty, removes IP restriction on API apiKey.

Aqua Group

Select a Group



Selecting an Aqua Group limits this API key to access resources belonging only to this group. An empty group makes the API key an account admin with access to all groups only for CSPM endpoints.

Global Permissions

Selecting an Aqua Group limits this API key to access resources belonging only to this group. An empty group makes the API key an account admin with access to all groups.



Enable global admin permission

5. Scroll all the way down to the bottom of the page and enable **roles:assign** and **tokens:readwrite** then select the role from the drop down and click **Save**



roles:assign - Assign roles to tokens. (Account Admin Only)



tokens:readwrite - View and create tokens for use with CLI scanning and other tools

demo_developer_role



Cancel

Save

The API Key is now configured to generate tokens and scope them to the assigned roles!

Aqua CSPM & Software Supply Chain Security (SaaS Only)

The API Key created for CSPM and Supply Chain require the API Key to have **Global Admin** enabled as those two modules are Admin Only modules. The option here is whether to create a single API Key to share between both modules or an API Key per module. Consult your internal security team for the best practice on how to proceed forward

Below are the steps to generate the key but leave **Global Admin** enabled per the [prerequisite](#) section:

1. Navigate to **Account Management**



Aqua Hub

Context aware risk management of cloud and Kubernetes resources

Supply Chain Security

Protect your software supply chain and source code

CSPM

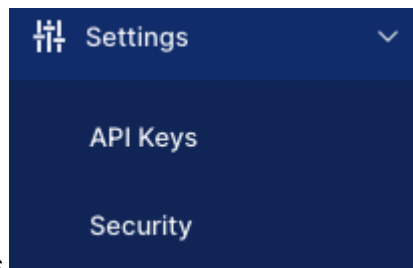
Monitor cloud infrastructure security and compliance risks

Workload Protection

Runtime protection for cloud native applications

Account Management

Manage users, roles, permissions, and billing



2. Click on **Settings**

3. Click on **Generate Key**

API Keys

Generate Key



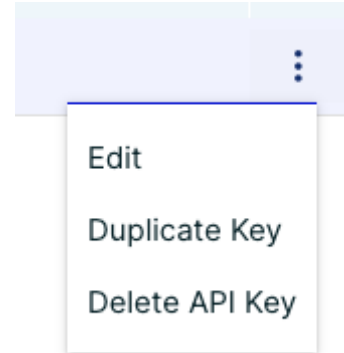
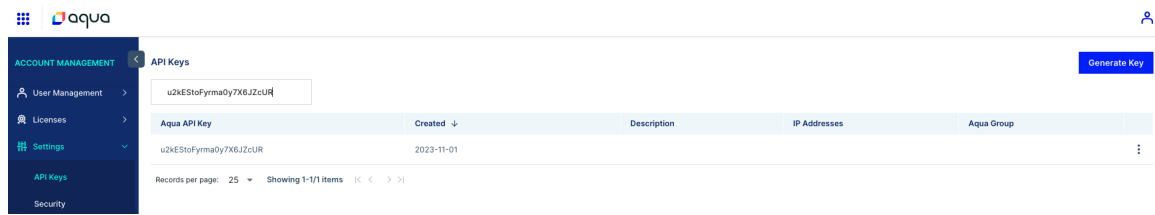
No API keys found

Click "Generate Key" to create a key and begin using the API

Generate Key

4. Upon clicking **Generate Key**, the API Key and Secret will display. **Save** them immediately.

5. Click on **Settings** followed by **API Keys** and search for your **API Key** created in the [prerequisites](#) section



6. Click on the ellipses on the far right of the key and select **Edit**
7. Enter a description for the API Key and ensure **Global Admin** is enabled, scroll down and click **Save**

Edit API Key



Description

CSPM & Supply Chain Postman Key

IP Addresses

Note: Allowed IP(s) come in the form of comma delimited IP sequence. Leaving this field empty, removes IP restriction on API apiKey.

Aqua Group

Select a Group



Selecting an Aqua Group limits this API key to access resources belonging only to this group. An empty group makes the API key an account admin with access to all groups only for CSPM endpoints.

Global Permissions

Selecting an Aqua Group limits this API key to access resources belonging only to this group. An empty group makes the API key an account admin with access to all groups.



Enable global admin permission

Granular Permissions

Selecting an Aqua Group limits this API key to access resources belonging only to this group. An empty group makes the API key an account admin with access to all groups.



accounts:read - View the account information



alerts:read - View all alerts for the account



alerts:readwrite - View, create, modify, and delete alerts



apikeys:read - View the API keys and usage data

Cancel

Save

This completes configuring CSPM & Software Supply Chain Security API Keys for Postman usage

Postman

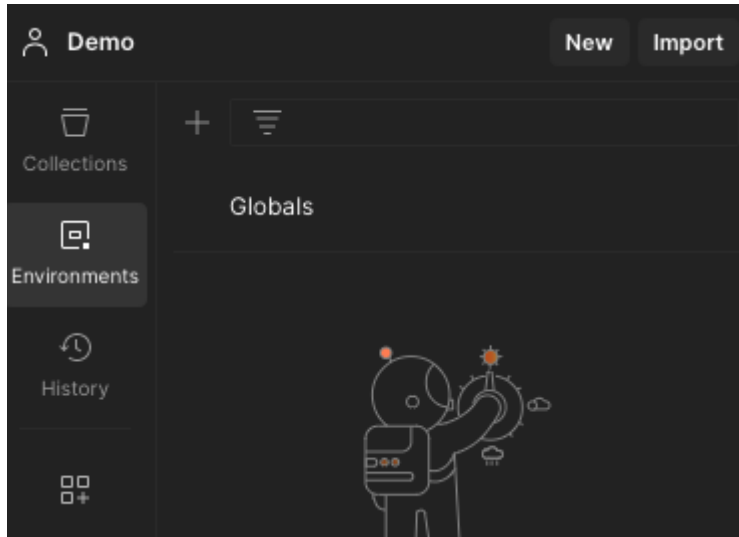
This section will cover how the **API Keys** and **Bearer Tokens** are utilized within Postman as well as importing the required files from the following GitHub Repository [aquaseclabs/api-postman](https://github.com/aquaseclabs/api-postman)

Import Environments and Collections

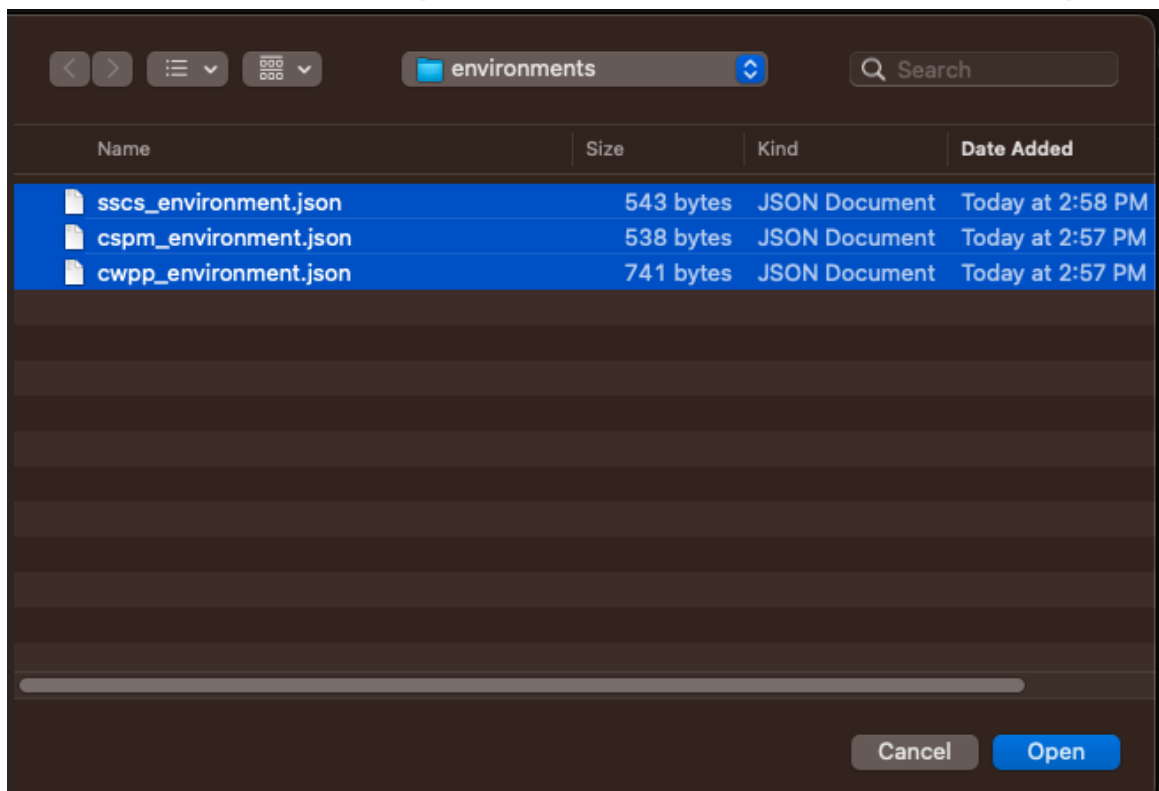
Once the repository is downloaded or cloned, open Postman. We will start by importing the **environments** since this is where we have to enter the **API Key** or **Username/Password** for the required **requests**

Import Environments

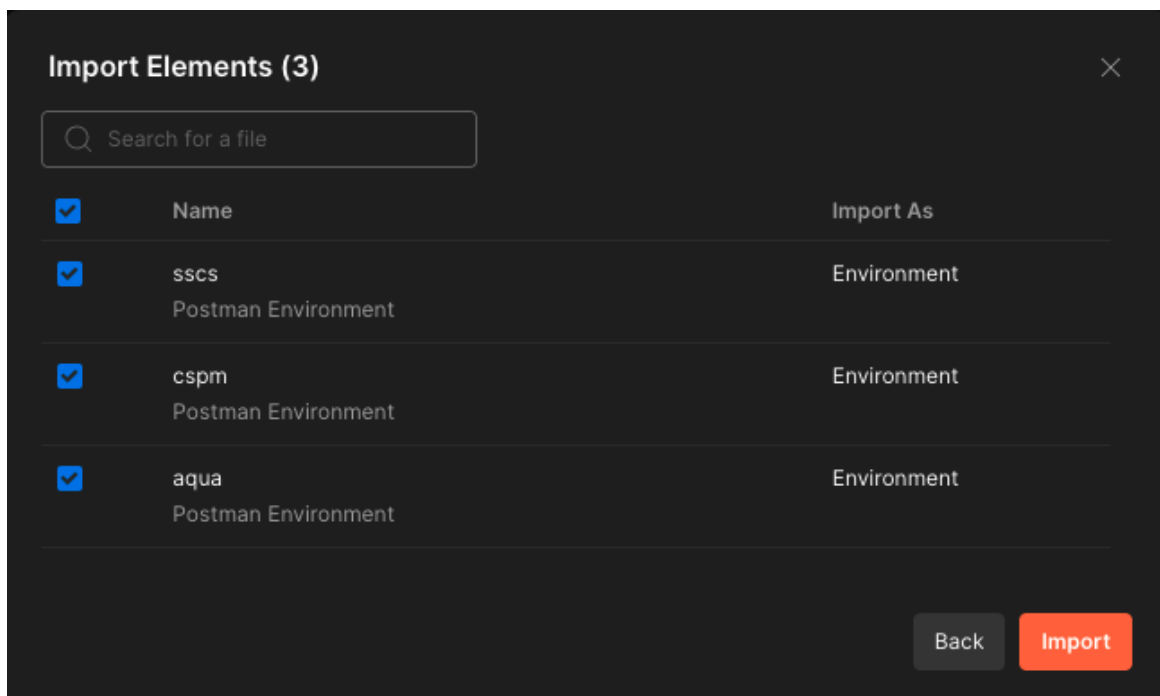
1. Click on the **Environment** tab on the left side



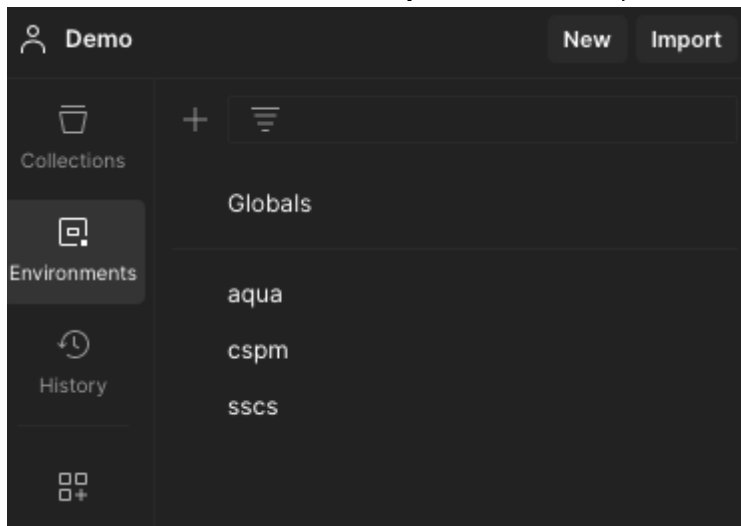
2. Once in environment click on **import** and select the **environment files** and click **open**



3. Postman will evaluate these files and load them if valid, click on **Import** to complete the import



4. The **Postman Environment import** is now completed!

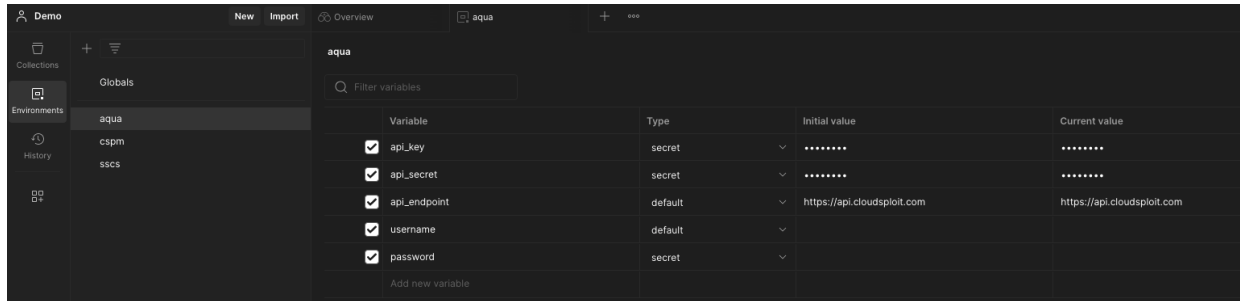


Update Environment Values

The values for each environment will need the API Key/Secret or Username/Password update for each applicable environment or environment created

Once the **environments** are imported, click on one of them. Update the **api_key** and **api_secret** if you are a SaaS customer, otherwise update **username** and **password** for Self-Hosted customers. Ensure both Initial value and Current value are populated when entering

values

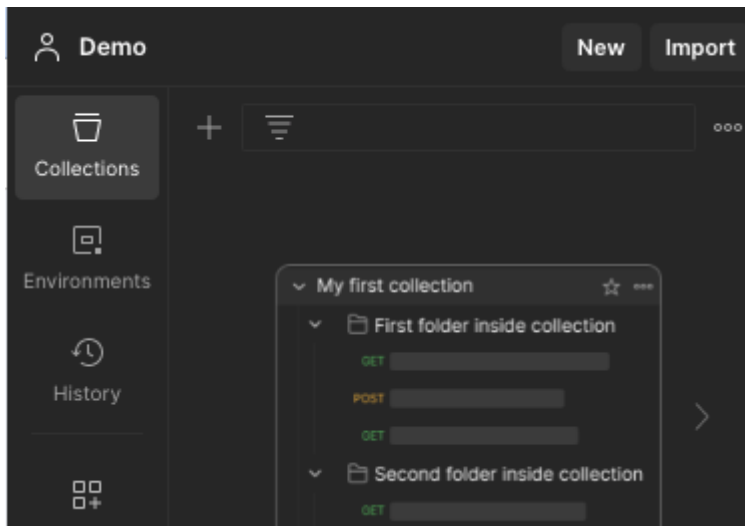


Variable	Type	Initial value	Current value
<input checked="" type="checkbox"/> api_key	secret	▼
<input checked="" type="checkbox"/> api_secret	secret	▼
<input checked="" type="checkbox"/> api_endpoint	default	▼ https://api.cloudsploit.com	https://api.cloudsploit.com
<input checked="" type="checkbox"/> username	default	▼	
<input checked="" type="checkbox"/> password	secret	▼	
Add new variable			

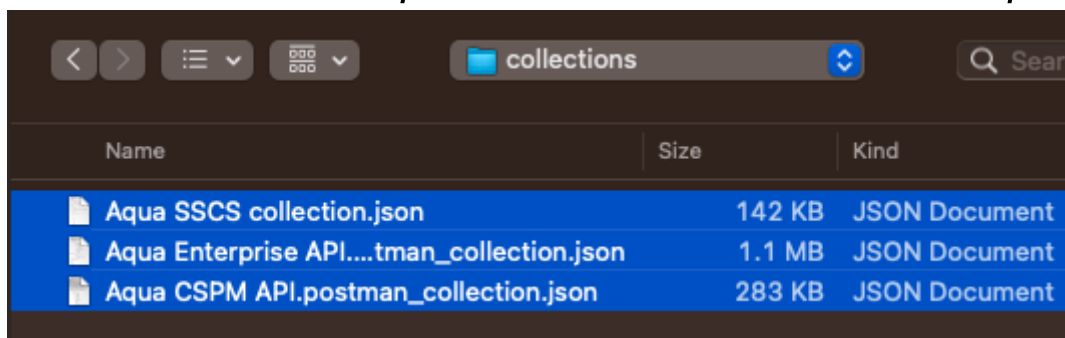
For Self-Hosted customers, the **aqua** environment is the only one applicable, update the **username**, **password**, and **aqua_url** fields. Optionally, re-name the environment if you choose to

Import Collections

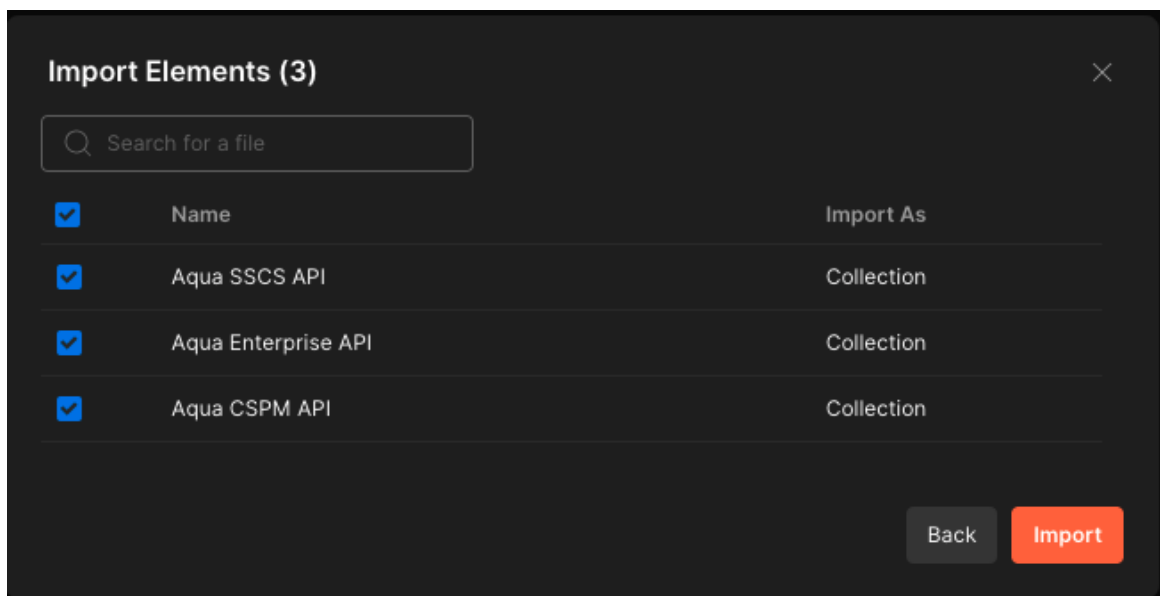
1. Click on the **Collections** tab on the left side



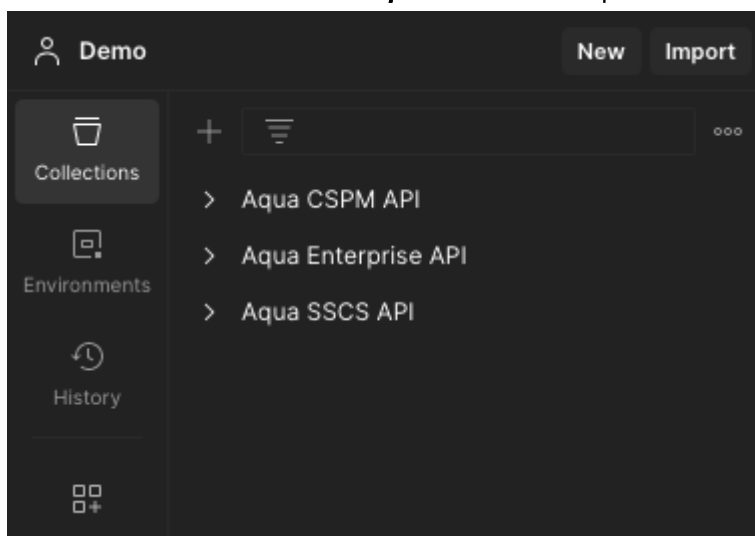
2. Once in collections click on **import** and select the **collection files** and click **open**



3. Postman will evaluate these files and load them if valid, click on **Import** to complete the import



4. The **Postman Collections import** is now completed!



The imports for both Postman **Environments** and **Collections** are now completed!

Postman Scripts and Requests

This section will provide guidance on the scripts used for CSPM and the token generation for Workload Protection/Supply Chain Security for both SaaS and Self-Hosted customers

Scripts

All of the modules requires a signature to be passed through along with the request, we have added the signature script to cover a wide range if not all of the API requests for these modules. Below is the signature located in the collection under **Pre-request Script**. This script will assign global variables for **signature** and **timestamp** to be utilized in the headers of the requests

Pre-request Script

Aqua CSPM API

Aqua CSPM API

OverviewAuthorizationPre-request ScriptTestsVariablesRuns

This script will execute before every request in this collection. Learn more about [Postman's execution order](#)

```
1 var crypto = require('crypto-js');
2 var moment = require('moment');
3
4 var secret = pm.environment.get("api_secret");
5 //console.log(secret)
6
7 var timestamp = (moment.unix(new Date())/1000);
8 let path = '/v2' + pm.request.url.getPath();
9 // console.log(path)
10
11 let method = pm.request.method.toUpperCase();
12 // console.log(method)
13
14 if (pm.request.body.raw == null) {
15   var body = "";
16 }else{
17   var body = JSON.parse(pm.request.body.raw);
18 }
19
20 // console.log(body)
21
22 var string = timestamp + method + path + (body && Object.keys(body).length > 0 ? JSON.stringify(body) : '');
23
24 console.log(string)
25
26 var hmac = crypto.HmacSHA256(string, secret);
27 var signature = hmac.toString();
28 // console.log(signature)
29
30
31 pm.globals.set("signature", signature);
32 pm.globals.set("timestamp", timestamp);
```

SaaS Body

HTTP Aqua API / CWPP / generate_tokens

POST

{{api_endpoint}}/v2/tokens

ParamsAuthorizationHeaders (13)BodyPre-request ScriptTestsSettings

none

form-data

x-www-form-urlencoded

raw

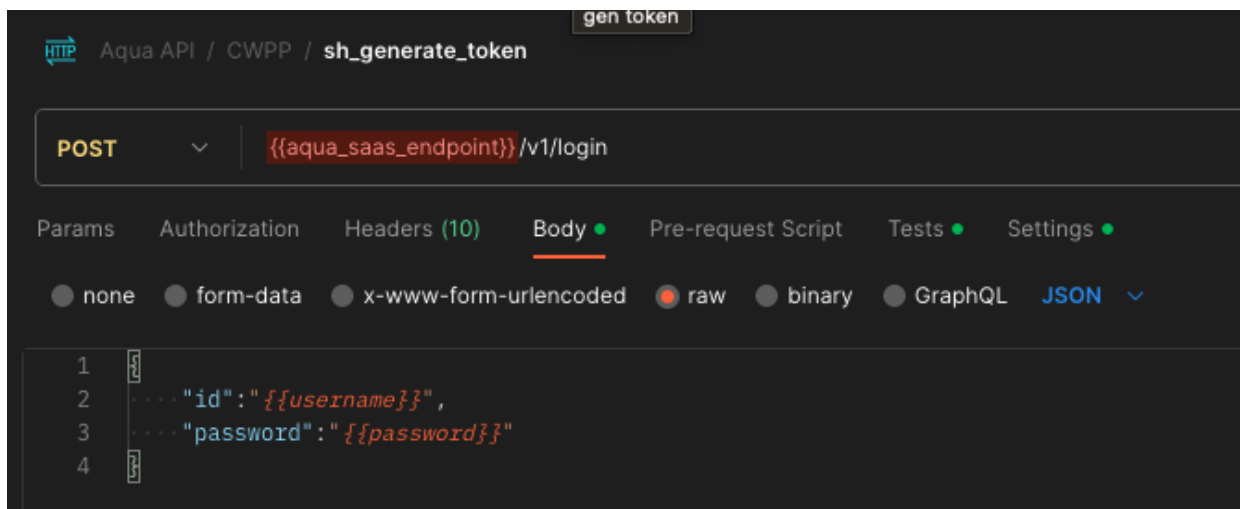
binary

GraphQL

JSON

```
1 {
2   ...."validity":240,
3   ...."allowed_endpoints":["ANY"]
4 }
```

Self-Hosted Body



Some endpoints will require additional information in the signature, if there are any issues reach out to your CSM/CSA/Aqua Support

Tokens

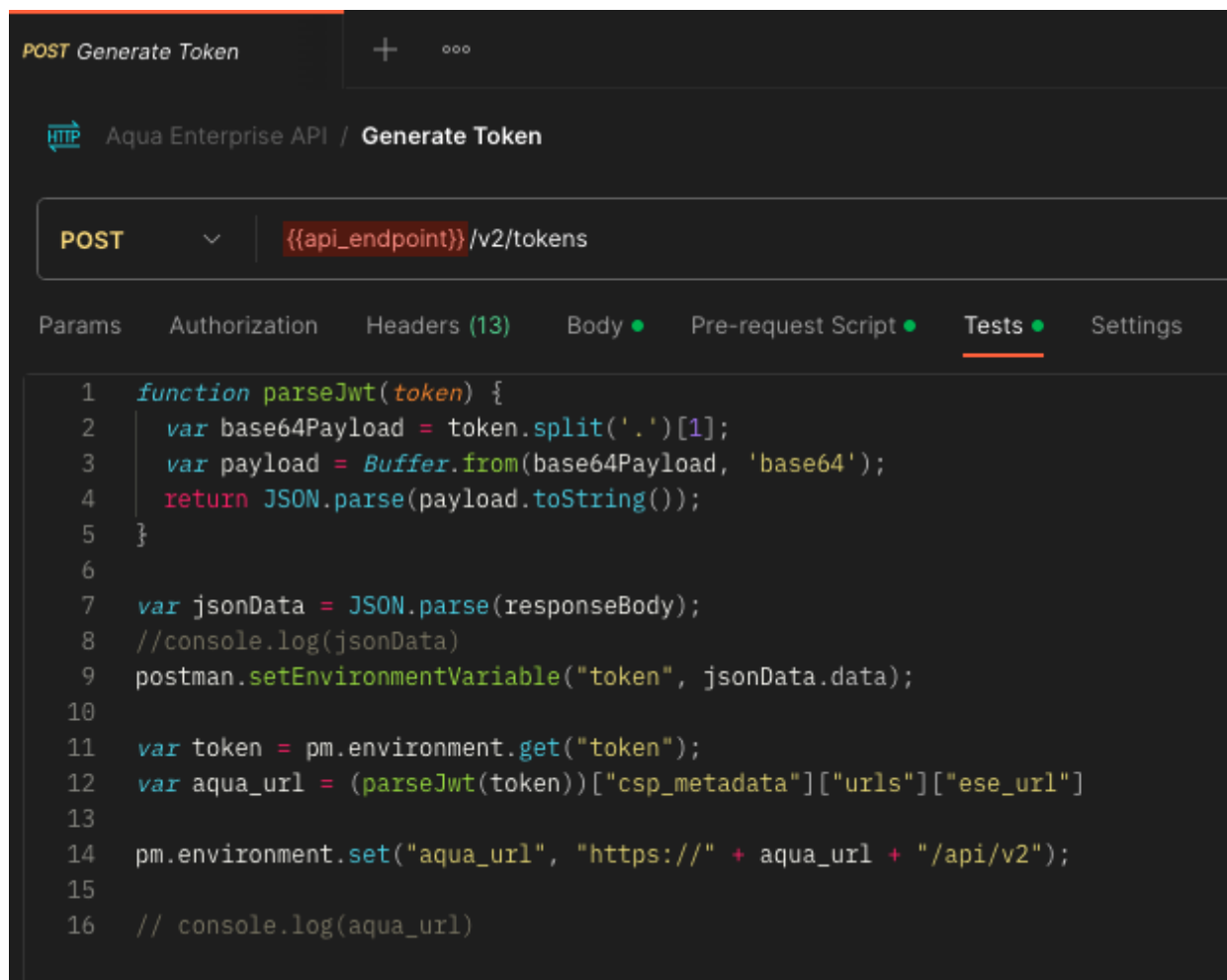
This section will cover the different login endpoints and scripts used within the Generate token requests within the Workload Protection collection called **Aqua Enterprise API**. The requests must be executed **first** before utilizing any of the other requests.

SaaS Tokens

The request to generate tokens for SaaS customers is called **Generate Token**. This request includes the **Pre-request Script** and **Body** to call the **/v2/tokens** endpoint in order to generate a token. once the token is generated, the **Postman Tests** tab will set the following variables:

- **aqua_url** - The url for the appropriate api request for the correct tenant
- **token** - Bearer token to be used within the header request

For customers with multiple tenants, the test script will **decode** the JWT token and extract the **Aqua Tenant URL**, there is no need to enter it manually



Self-Hosted Tokens

The **aqua_url** variable needs to be predefined prior to executing the token request

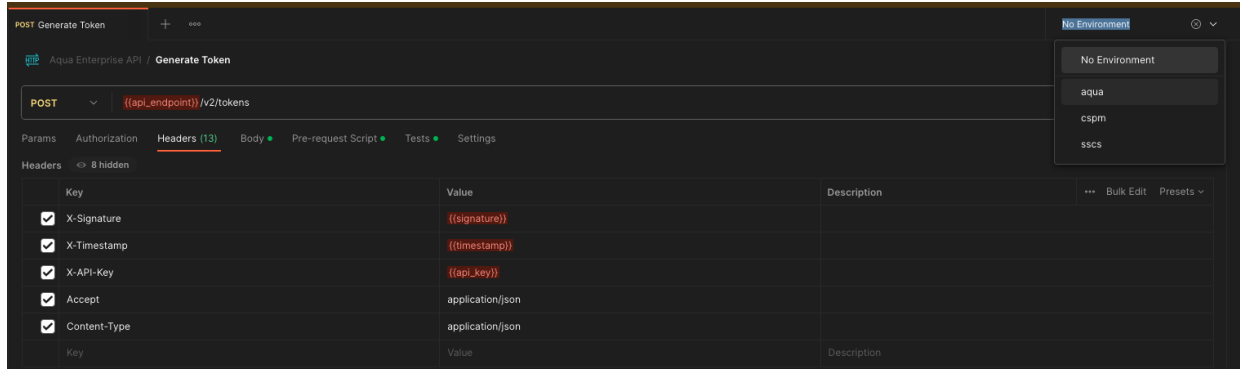
The request to generate tokens for SaaS customers is called **Self-Hosted Generate Token**. This request includes the **Pre-request Script** and **Body** to call the **/v1/login** endpoint in order to generate a token. once the token is generated, the **Postman Tests** tab will set the following variables:

- **token** - Bearer token to be used within the header request

Postman Usage

The use of environments will be crucial to segment API Keys/Secrets or Username/Password for different Aqua Tenants within your environment. The requests within the Postman Collections **do not need to change** Simply select the environment on the top right hand corner and send

the request



As long as all of the variables within the environment are defined correctly, you can execute the requests seamlessly and generate the outputs.

If the need arises to create additional environments, the recommendation is to do the following:

1. Duplicate the imported environment
2. Re-name the duplicate to the appropriate name
3. Update the variables with the appropriate values

If you encounter any issues please let your **CSM/CSA** know and **create a ticket** if problems persist. Happy Automating!

References

- [Permission Sets](#)
- [Aqua Role](#)
- [RBAC Overview](#)
- **Cloud Workload Protection Platform**
 - [SaaS API Authentication](#)
 - [SaaS API Reference](#)
 - [Self-Hosted Authentication](#)
 - [Self-Hosted API Reference](#)
- **CSPM**
 - [CSPM API Documentation](#)
 - [CSPM Code Examples](#)
- **Software Supply Chain Security**
 - [API Reference](#)