Export an Application Blocklists from the AMP Portal with APIs

Contents

Introduction

This document describes the procedure to export information from the Advanced Malware Protection (AMP) for Endpoints application blocklist with APIs.

Contributed by Uriel Montero and Yeraldin Sánchez, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to the Cisco AMP for Endpoints dashboard
- API Credentials from the AMP portal: 3rd Party API Client ID and API key, this link shows the steps to obtain them: How to Generate an API Credential from the AMP Portal
- An API handler, in this document, is used the Postman tool

Components Used

The information in this document is based on thede software:

- Cisco AMP for Endpoints for Endpoints console version 5.4.20190709
- Postman tool

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Related Products

This document can also be used with the API version:

- api.amp.cisco.com, v1

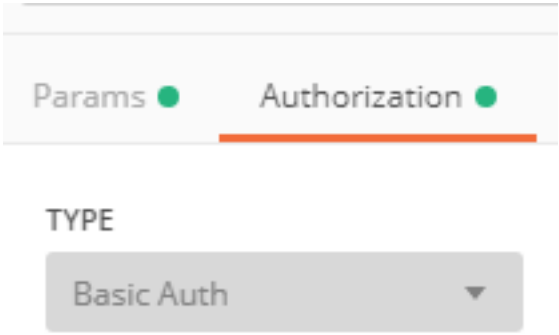
Background Information

Cisco does not support the Postman tool, if you have a question about it, please contact the Postman support.

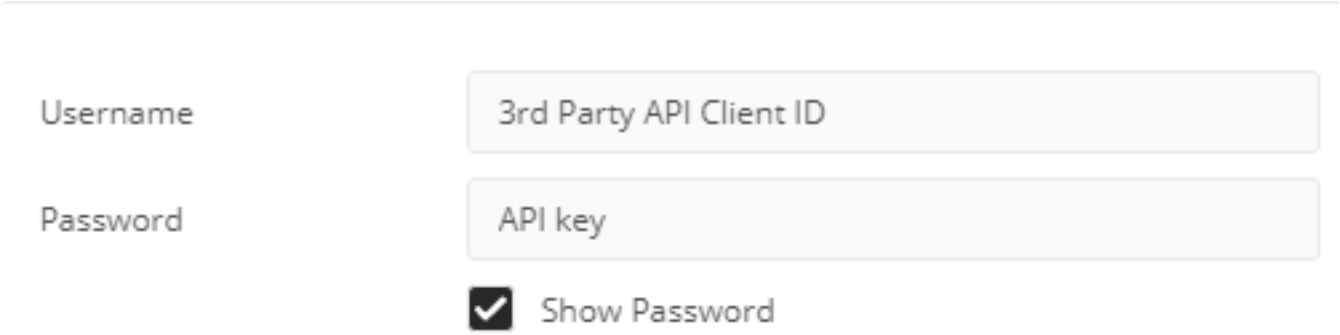
Process

This is the process to collect the AMP application blocklists and the SHA-256 list from the selected list with APIs and the Postman tool.

Step 1. On the Postman tool, navigate to **Authorization > Basic Auth**, as shown in the image.



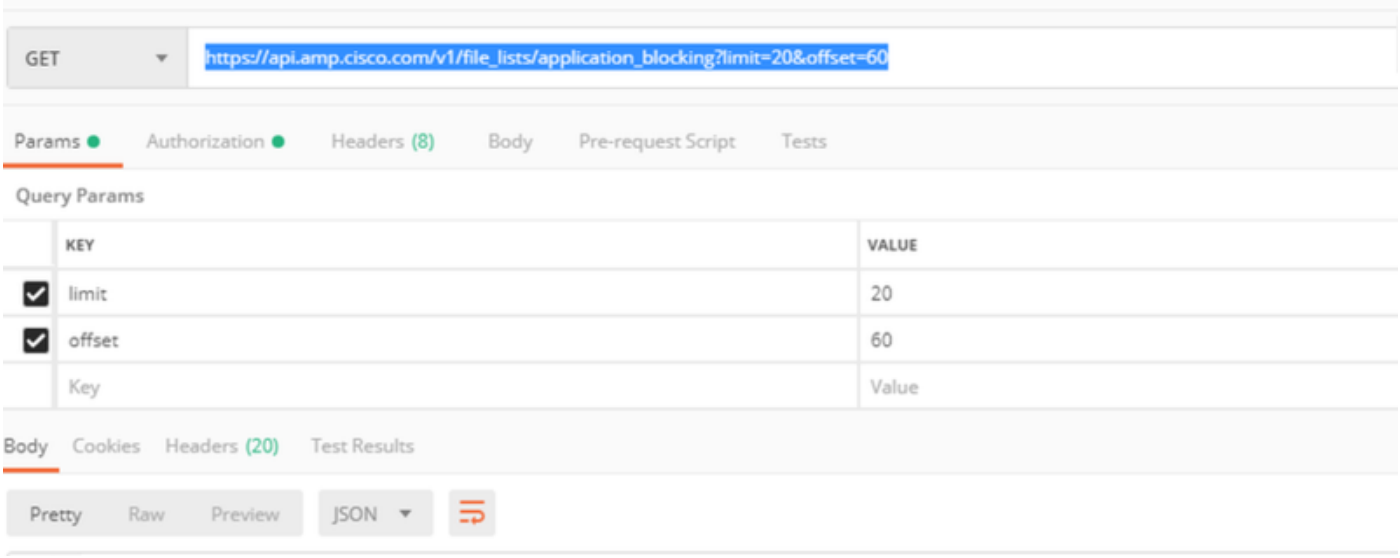
Step 2. Add the **3rd Party API Client ID** on the Username section, and the **API key** on the Password option, as shown in the image.



Step 3. Inside the API handler, select the **GET** request and paste the command:**https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0**.

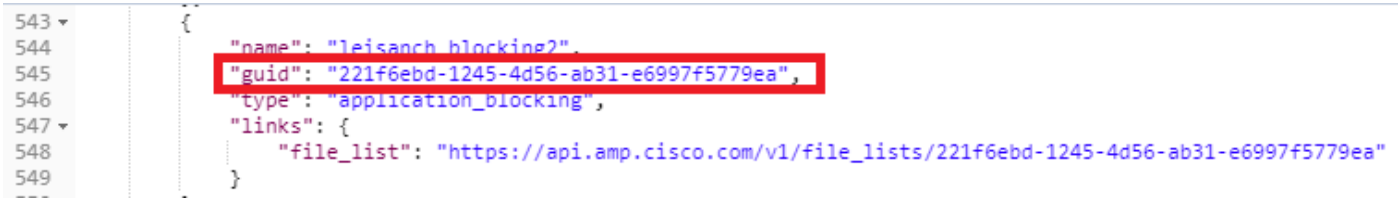
- Limit: number of items the tool displays
- Offset: from where the information starts to display the items

In this example, the limit value is 20 and the offset is 60, the information starts to show the list 61 and the limit is 80, as shown in the images.

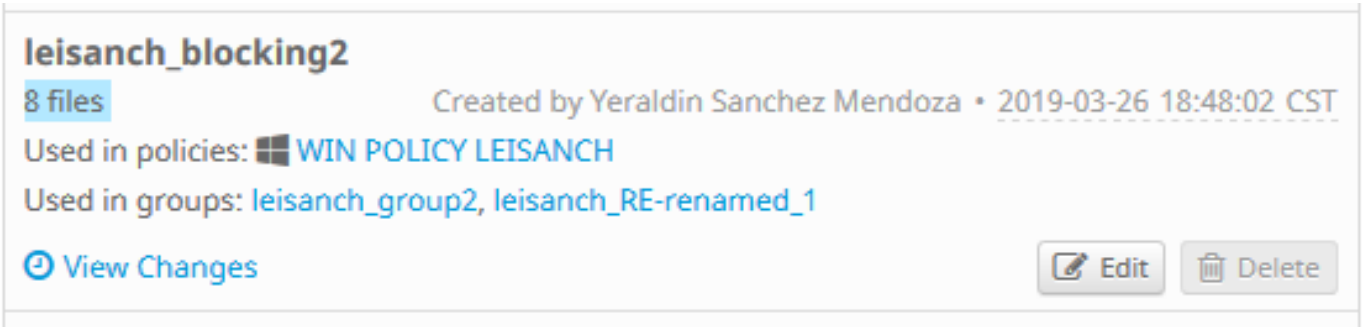


The command displays all the application blocklist configured on the AMP portal if you want to have the list of the SHA-256 codes of a specific list, navigate to the next step.

Step 4. On the application blocklist previously selected, copy the **guid** and run the command: **https://api.amp.cisco.com/v1/file_lists/guid/files,** in this example the guid is 221f6ebd-1245-4d56-ab31-e6997f5779ea for the list leisanch_blocking2, as shown in the image.



On the AMP portal, the application blocklist shows 8 SHA-256 codes added, as shown in the image.



With the command:**https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea**, the list must display 8 SHA-256 codes, as shown in the image.

```
{
    "version": "v1.2.0",
    "metadata": {
        "links": {
            "self": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea/files"
        },
        "results": {
            "total": 8,
            "current_item_count": 8,
            "index": 0,
            "items_per_page": 500
        }
    },
    "data": {
        "name": "leisanch_blocking2",
        "guid": "221f6ebd-1245-4d56-ab31-e6997f5779ea",
        "policies": [
            {
                "name": "WIN POLICY LEISANCH",
                "guid": "768cdd65-dc8b-4301-82ae-60cb9bcbc57f",
                "links": {
                    "policy": "https://api.amp.cisco.com/v1/policies/768cdd65-dc8b-4301-82ae-60cb9bcbc57f"
                }
            }
        ],
        "items": [
            {
                "sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c5",
                "description": "first sha",
                "source": "Created from SHAs in shasyeral.txt from [redacted] ",
                "links": {
                    "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
                }
            },
            {
                "sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c2",
                "description": "first sha",
                "source": "Created from SHAs in shasyeral.txt from [redacted] ",
                "links": {
                    "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
                }
            },
            {
                "sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c3",
                "description": "first sha",
                "source": "Created from SHAs in shasyeral.txt from [redacted] ",
                "links": {
                    "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
```


Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Cisco AMP for Endpoints API**
- **Cisco AMP for Endpoints - User Guide**
- **Technical Support & Documentation - Cisco Systems**