# 使用API從AMP門戶匯出應用阻止清單

## 目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[流程](#)
[驗證](#)
[疑難排解](#)
[相關資訊](#)

### 簡介

本文檔介紹使用API從面向終端的高級惡意軟體防護(AMP)應用阻止清單匯出資訊的過程。

作者：Uriel Montero和Yeraldin Sánchez，思科TAC工程師。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 訪問面向終端的思科AMP控制面板
- 來自AMP門戶的API憑證：第三方API客戶端ID和API金鑰，此連結顯示獲取這些證書的步驟：如何從AMP門戶生成API憑據
- 本文檔中的API處理程式使用Postman工具

### 採用元件

本檔案中的資訊是根據以下軟體：

- 適用於終端的思科AMP終端控制檯版本5.4.20190709
- 郵遞員工具

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

### 相關產品

本檔案也適用於以下API版本：

- api.amp.cisco.com,v1

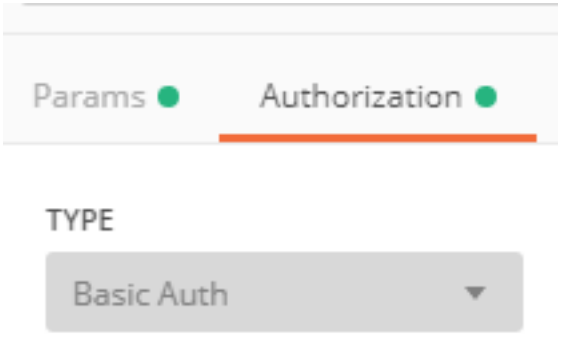
### 背景資訊

思科不支援Postman工具，如果您對此有疑問，請與Postman支援部門聯絡。

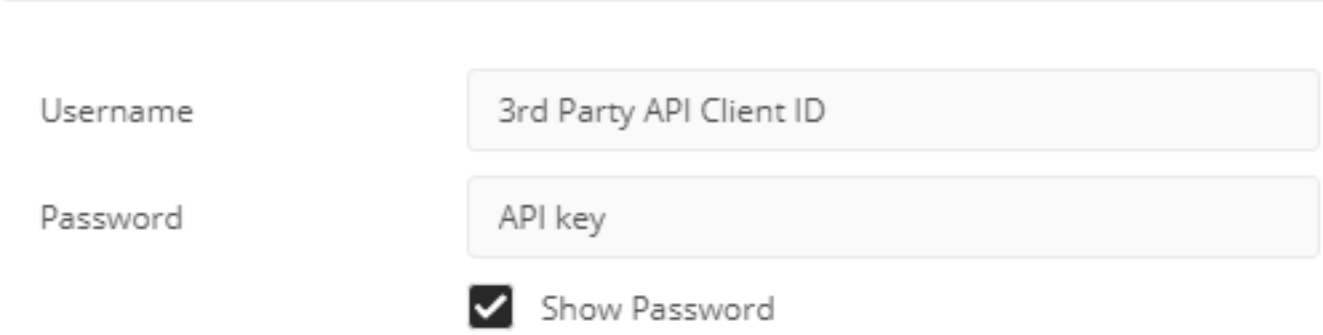
## 流程

這是使用API和Postman工具從選定清單中收集AMP應用程式阻止清單和SHA-256清單的過程。

步驟1。在Postman工具上，導覽至**Authorization > Basic Auth**，如下圖所示。



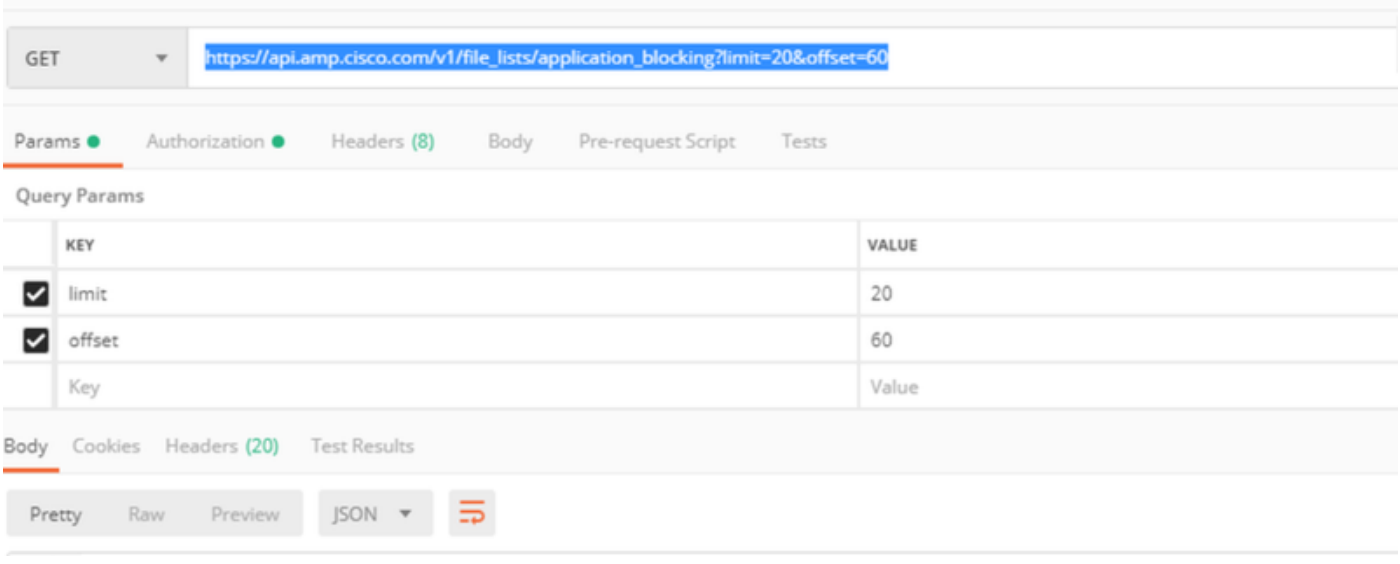

步驟2.在「**Username**」部分新增第三方API客戶端ID，並在「**Password**」選項上新增API金鑰，如下圖所示。




步驟3.在API處理程式中，選擇**GET**請求並貼上命令:https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0。

- 限制：工具顯示的項數
- Offset:資訊開始顯示專案的位置

在此示例中，限制值為20，偏移量為60，資訊開始顯示清單61，限制值為80，如圖所示。

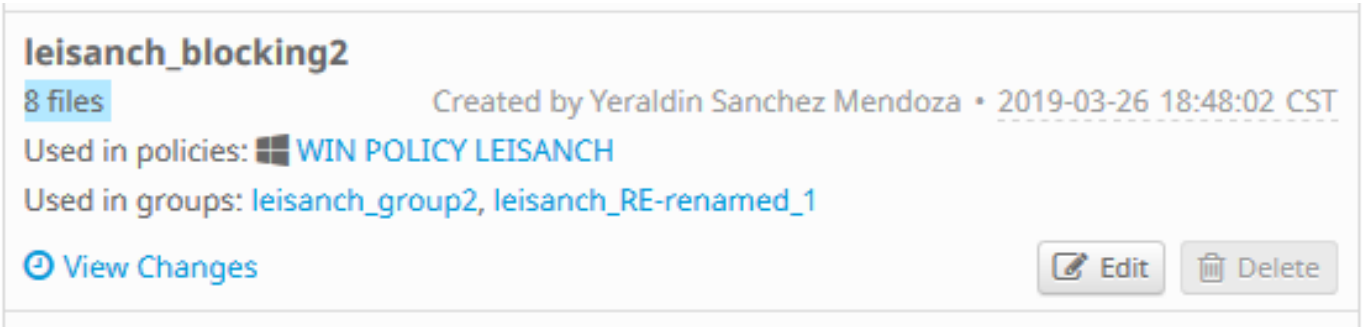



如果您希望獲得特定清單的SHA-256代碼清單，該命令會顯示在AMP門戶上配置的所有應用程式阻止清單，導航到下一步。

步驟4.在先前選定的應用程式阻止清單中，複製**guid**，然後運行命令：https://api.amp.cisco.com/v1/file_lists/guid/files，在此示例中，清單leisanch_blocking2的guid為221f6ebd-1245-4d56-ab31-e6997f5779ea，如下圖所示。


```
543 {
544     "name": "leisanch_blocking2",
545     "guid": "221f6ebd-1245-4d56-ab31-e6997f5779ea",
546     "type": "application_blocking",
547     "links": {
548         "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
549     }
```


在AMP門戶上，應用阻止清單顯示新增的8個SHA-256代碼，如下圖所示。




使用命令https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea時，清單必須顯示8個SHA-256代碼，如下圖所示。


```
{
    "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"
                }
```

## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

## 相關資訊

- 思科終端進階惡意軟體防護API
- 面向終端的思科AMP — 使用手冊
- 技術支援與文件 - Cisco Systems