APIを使用したAMPポータルからのアプリケーションブロックリストのエクスポート

内容

概要

このドキュメントでは、APIを使用してAdvanced Malware Protection(AMP)for Endpointsアプリケーションブロックリストから情報をエクスポートする手順について説明します。

著者：Cisco TACエンジニア、Uriel MonteroおよびYeraldin Sanchez

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco AMP for Endpointsダッシュボードへのアクセス
- AMPポータルからのAPIクレデンシャル：サードパーティAPIクライアントIDとAPIキーを取得する手順を示します。AMPポータルからAPIクレデンシャルを生成する方法
- このドキュメントでは、APIハンドラをPostmanツールで使用します

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアに基づいています。

- Cisco AMP for Endpoints for Endpointsコンソールバージョン5.4.20190709
- Postmanツール

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、APIバージョンでも使用できます。

- api.amp.cisco.com、v1

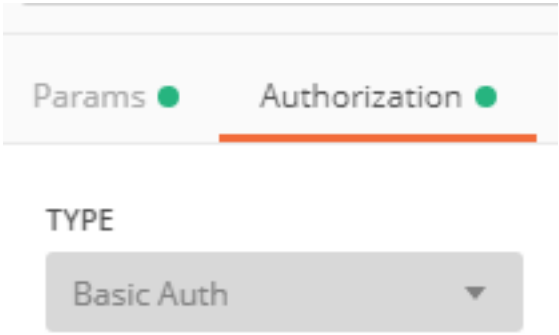
背景説明

シスコはPostmanツールをサポートしていません。ご質問がございましたら、Postmanサポートにお問い合わせください。

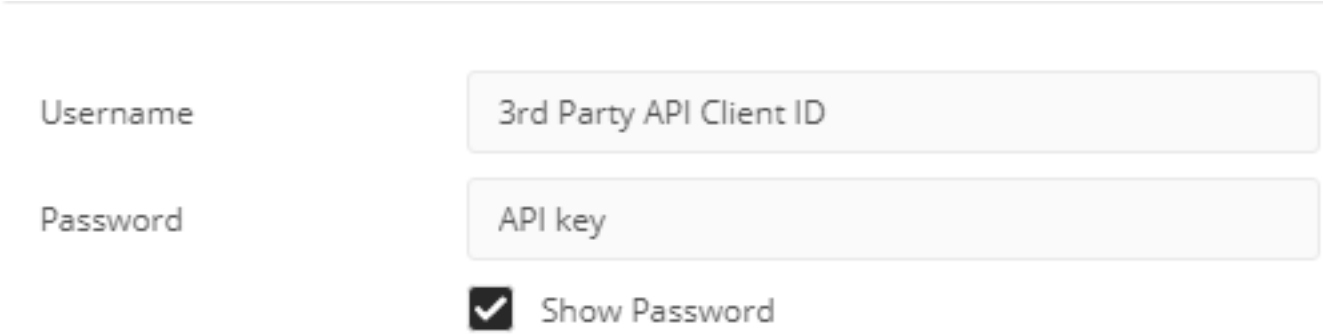
プロセス

これは、AMPアプリケーションブロックリストとSHA-256リストを、APIとPostmanツールを使用して選択したリストから収集するプロセスです。

ステップ1：図に示すように、Postmanツールで[**Authorization**] > [**Basic Auth**]に移動します。



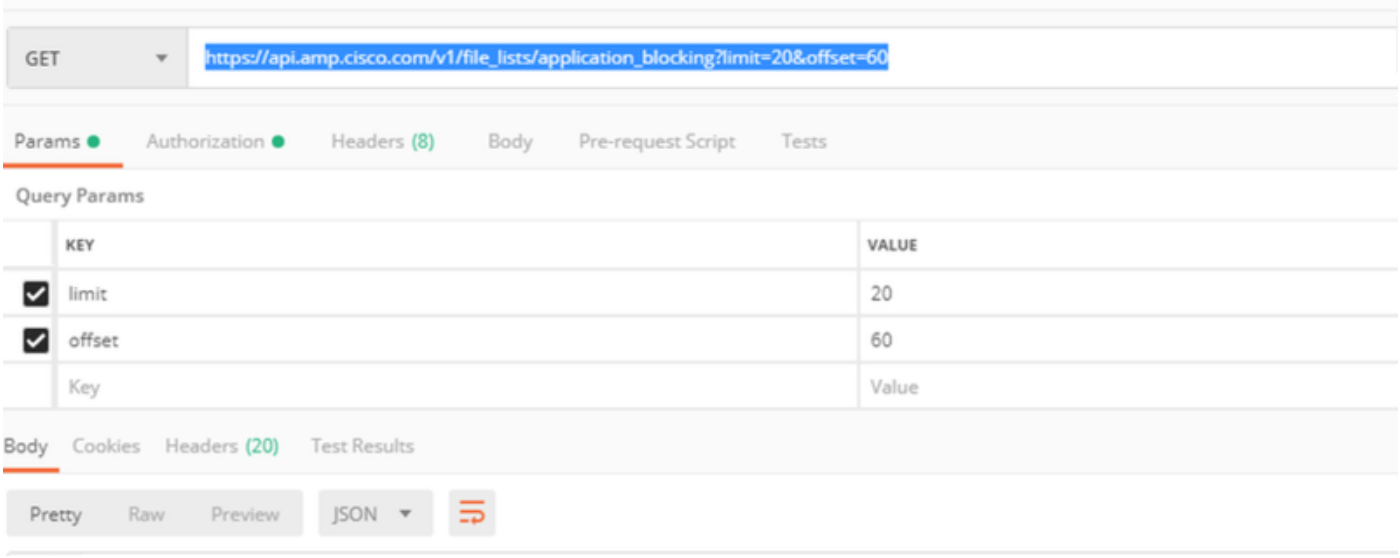
ステップ2：図に示すように、[ユー**ザー名]セクションにサード**パーティAPIクライアントIDを追加し、**[パスワ**ード]オプションにAPIキーを追加します。



ステップ3:APIハンドラ内でGET要求を選択**し、コ**マンドhttps://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0を貼り付けます。

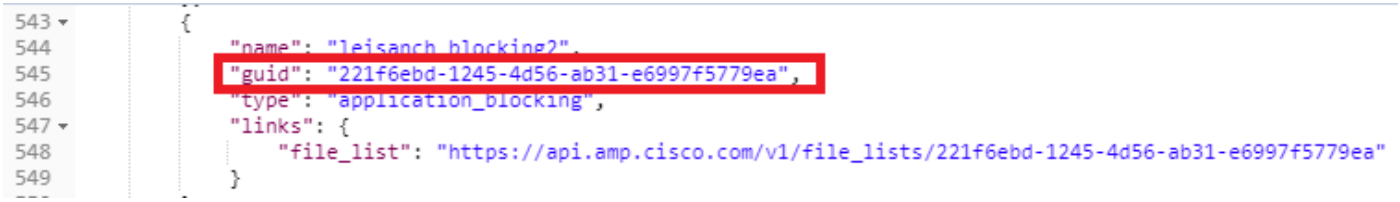
- 上限：ツールに表示される項目数
- Offset:情報が表示される場所から

この例では、リミット値が20、オフセットが60で、情報はリスト61を表示し始め、リミットは80です（図を参照）。

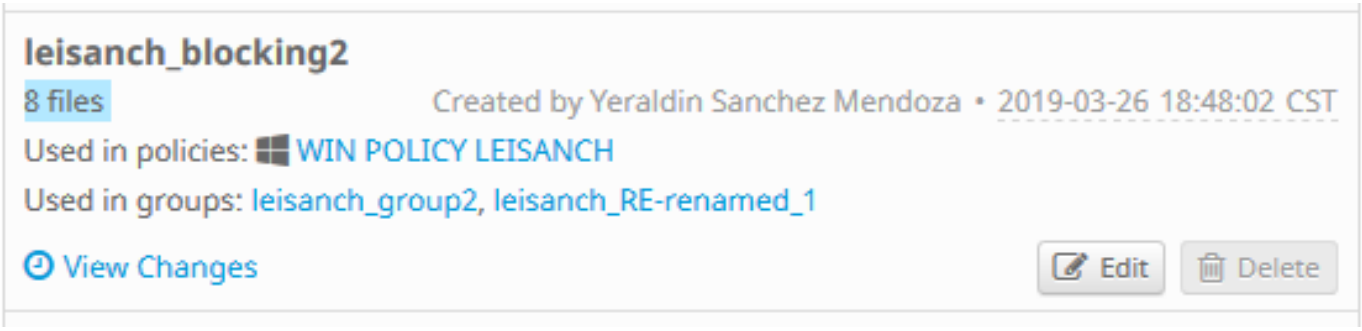


特定のリストのSHA-256コードのリストを取得する場合は、AMPポータルで設定されているすべてのアプリケーションブロックリストを表示し、次の手順に移動します。

ステップ4：前に選択したアプリケーションのブロックリストで**guid**をコピーし、コマンドhttps://api.amp.cisco.com/v1/file_lists/guid/filesを実行します。この例では、guidは221f6ebd-1245-4d56-ab31-e6997f577799992です。図に示すように



AMPポータルでは、図に示すように、追加された8つのSHA-256コードがアプリケーションブロックリストに表示されます。



https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779eaコマンドを使用すると、リストに8つのSHA-256コードが表示されます（図を参照）。

```
{
    "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"
                }
```


確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco AMP for Endpoints API
- エンドポイント向けCisco AMP – ユーザガイド
- テクニカル サポートとドキュメント – Cisco Systems