Exportieren einer Anwendungs-Blockliste aus dem AMP-Portal mit APIs

Inhalt

Einführung

Dieses Dokument beschreibt das Verfahren zum Exportieren von Informationen aus der Anwendungsblockliste für AMP (Advanced Malware Protection) für Endgeräte mit APIs.

Unterstützt von Uriel Montero und Yeraldin Sánchez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zugriff auf das Dashboard von Cisco AMP für Endgeräte
- API-Anmeldeinformationen des AMP-Portals: API-Client-ID und API-Schlüssel von Drittanbietern. Dieser Link zeigt die Schritte, um diese zu erhalten: Erstellen einer API-Anmeldeinformationen vom AMP-Portal
- Ein API-Handler wird in diesem Dokument mit dem Postman-Tool verwendet.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Software:

- Cisco AMP für Endgeräte Konsolenversion 5.4.20190709
- Postman-Tool

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Dieses Dokument kann auch mit der API-Version verwendet werden:

- api.amp.cisco.com, v1

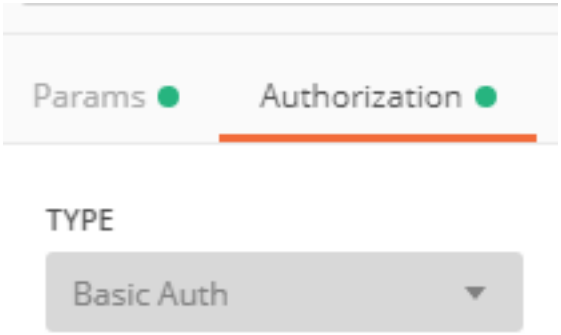
Hintergrundinformationen

Cisco unterstützt das Postman-Tool nicht. Wenn Sie Fragen dazu haben, wenden Sie sich bitte an den Postman-Support.

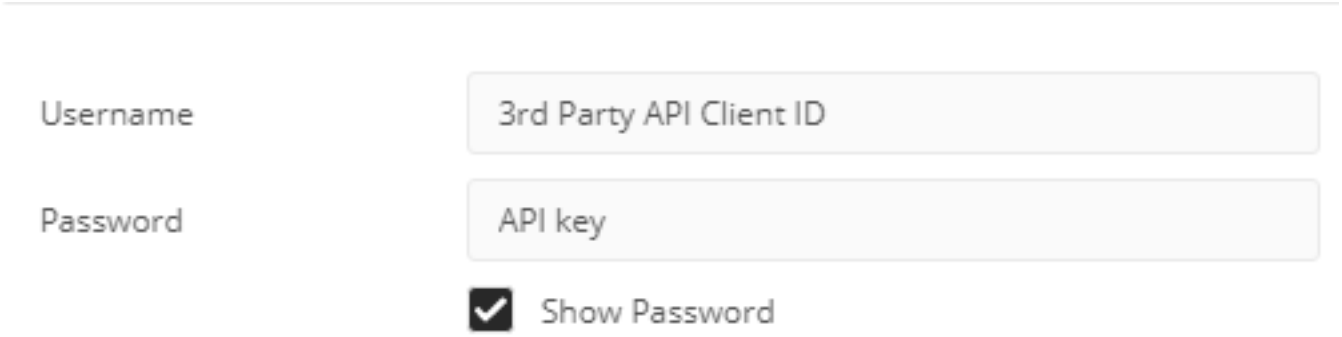
Prozess

Dabei werden die AMP-Anwendungsblocklisten und die SHA-256-Liste aus der ausgewählten Liste mit APIs und dem Postman-Tool erfasst.

Schritt 1: Navigieren Sie im Postman-Tool zu **Authorization > Basic Auth**, wie im Bild gezeigt.



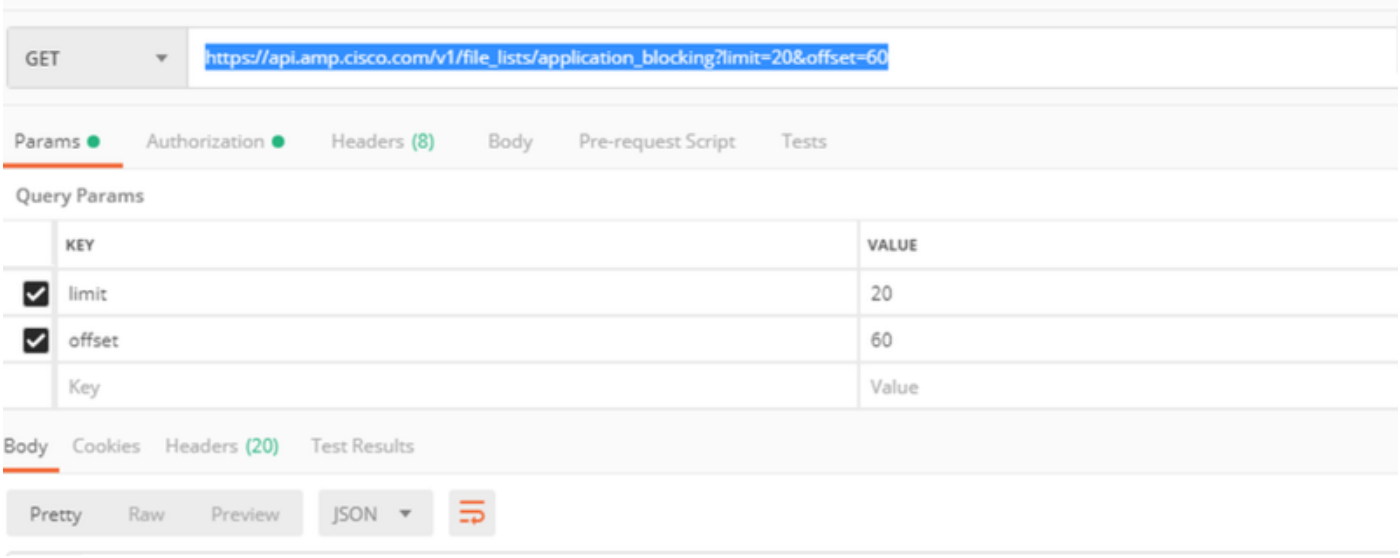
Schritt 2: Fügen Sie die **Drittanbieter-API-Client-ID** im Bereich Username (Benutzername) und den **API-Schlüssel** in der Option Password (Kennwort) hinzu, wie im Bild gezeigt.



Schritt 3: Wählen Sie im API-Handler die **GET-**Anforderung aus, und fügen Sie den Befehl https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0 ein.

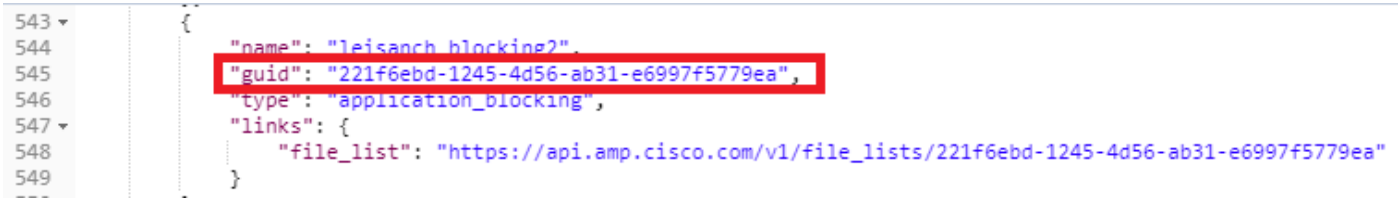
- Begrenzung: Anzahl der vom Tool angezeigten Artikel
- Offset: von wo aus die Informationen beginnen, die Elemente anzuzeigen

In diesem Beispiel ist der Grenzwert 20 und der Offset 60, die Informationen zeigen die Liste 61 an und der Grenzwert 80, wie in den Bildern gezeigt.

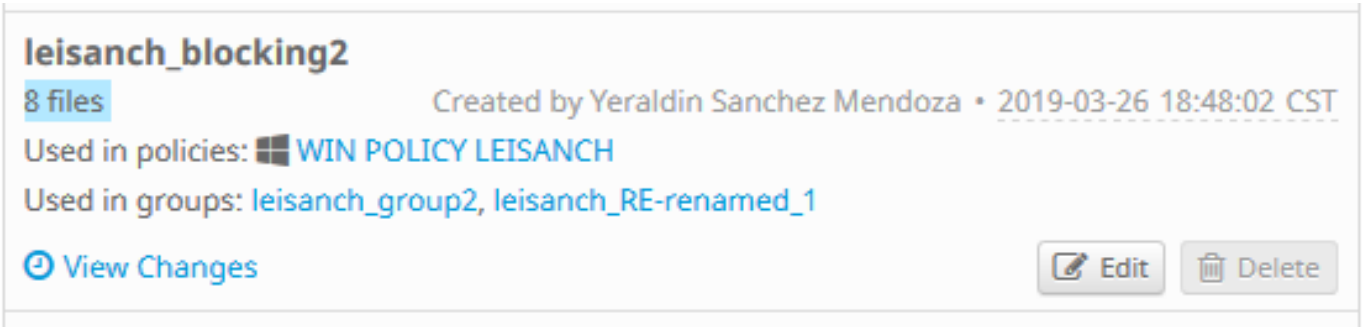


Der Befehl zeigt alle im AMP-Portal konfigurierten Anwendungsblocklisten an, wenn Sie eine Liste der SHA-256-Codes einer bestimmten Liste erhalten möchten. Navigieren Sie dann zum nächsten Schritt.

Schritt 4: Kopieren Sie in der zuvor ausgewählten Anwendungsblockliste die **GUID** und führen Sie den Befehl https://api.amp.cisco.com/v1/file_lists/guid/files, in diesem Beispiel lautet die GUID 221f6ebd-1245-4d56-ab31-e6997f5779ea für die Liste leisanch_locking2, wie dargestellt. im Bild.



Im AMP-Portal zeigt die Anwendungsblockliste 8 hinzugefügte SHA-256-Codes, wie im Bild gezeigt.



Mit dem Befehl https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea muss die Liste 8 SHA-256-Codes anzeigen, wie im Bild gezeigt.

```
{
    "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"
```


Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- API für Cisco AMP für Endgeräte
- Cisco AMP für Endgeräte - Benutzerhandbuch
- Technischer Support und Dokumentation - Cisco Systems