Exporteren en toepassingsblocklisten van de AMP Portal met API's

Inhoud

Inleiding

Dit document beschrijft de procedure om informatie van de Advanced Malware Protection (AMP) voor Endpoints te exporteren met API's.

Bijgedragen door Uriel Montero en Yeraldin Sánchez, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot de Cisco Advanced Malware Protection voor endpoints
- API-credits van het AMP-portaal: Clientid en API voor gebruik door derden, toont deze link de stappen om deze te verkrijgen: Hoe kan er een API-krediet worden gegenereerd van de AMP-portal
- Een API-geleider, in dit document, wordt gebruikt als postgereedschap

Gebruikte componenten

De informatie in dit document is gebaseerd op de software:

- Cisco Advanced Malware Protection voor endpoints voor endpoints, versie 5.4.2019
- Postgereedschap

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Verwante producten

Dit document kan ook worden gebruikt met de API-versie:

- api.amp.cisco.com, v1

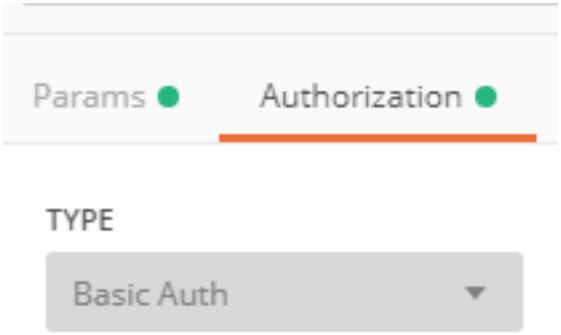
Achtergrondinformatie

Cisco ondersteunt het Postman gereedschap niet. Als u een vraag hebt over dit, neem dan contact op met de Postman ondersteuning.

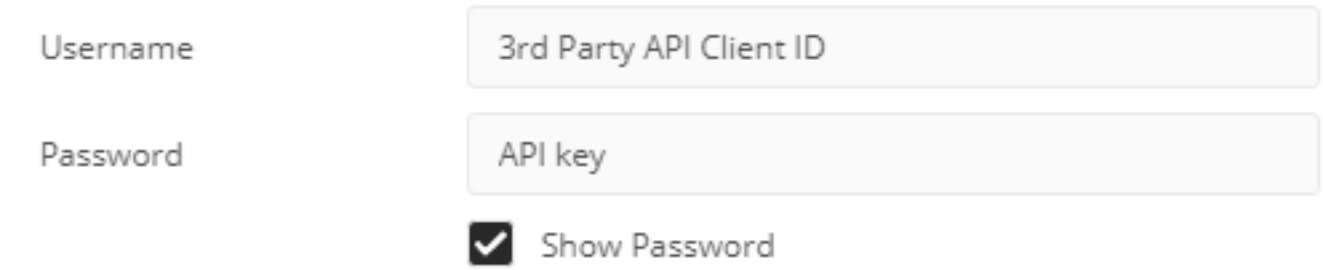
verwerken

Dit is het proces om de AMP-toepassingsblokkades en de SHA-256-lijst van de geselecteerde lijst te verzamelen met API's en het Post-gereedschap.

Stap 1. navigeer in het gereedschap Postman naar **Auteur > Basic Auth**, zoals in de afbeelding.



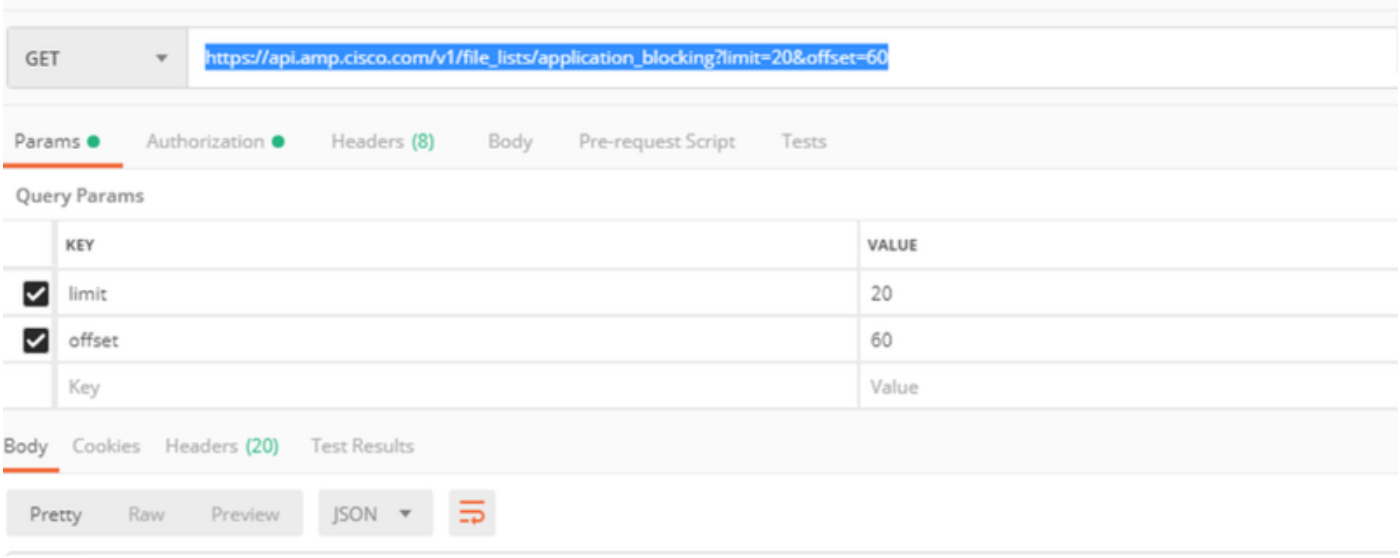
Stap 2. Voeg de **client-ID** van **derden** toe aan de sectie Gebruikersnaam en de **API-toets** voor de optie Wachtwoord, zoals in de afbeelding weergegeven.



Stap 3. In de API-afvoerder selecteert u het **Get** request en paste de opdracht aan:https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0.

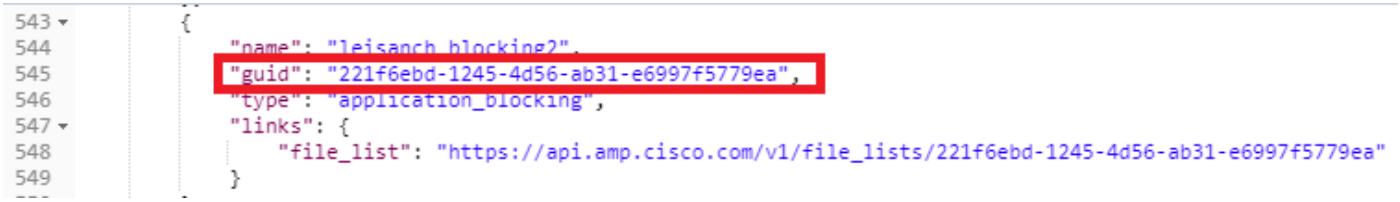
- Limiet: aantal items dat het gereedschap toont
- Offset: vanaf waar de informatie de items begint weer te geven

In dit voorbeeld is de grenswaarde 20 en de offset 60, de informatie begint de lijst 61 te tonen en de limiet is 80, zoals in de beelden wordt getoond.

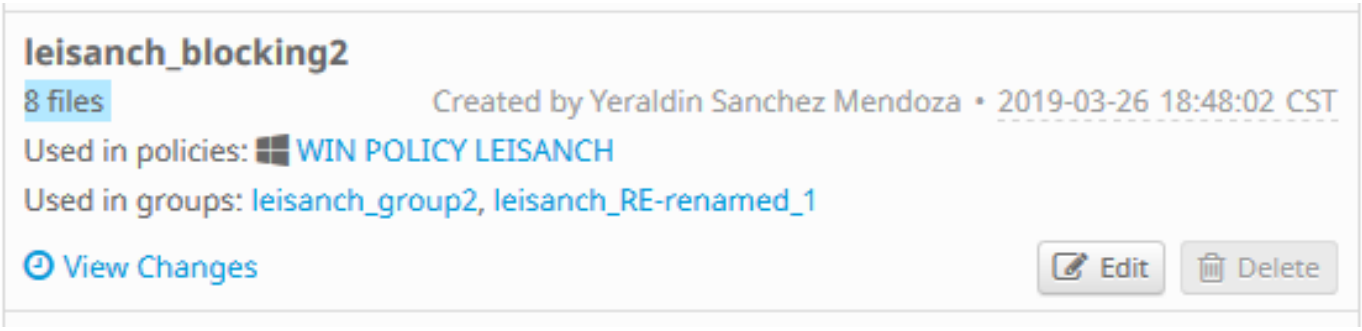


De opdracht geeft alle toepassingsblokkades weer die in het AMP-portal zijn ingesteld als u de lijst wilt hebben met de SHA-256-codes van een specifieke lijst en navigeer naar de volgende stap.

Stap 4. Op de eerder geselecteerde applicatieblokkeerlijst kopieert u de **gelid** en voert u de opdracht uit: https://api.amp.cisco.com/v1/file_lists/guid/files, in dit voorbeeld is de gids 221f6ebd-1245-4d56-ab31-e6997f579ea voor de lijst leisanea ch_block2, zoals getoond in de afbeelding.



Op het AMP-portaal toont de applicatie-blocklist 8 SHA-256-codes die toegevoegd worden, zoals in de afbeelding.



Met de opdracht:https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea moet de lijst 8 SHA-256-codes weergeven, zoals in de afbeelding.

```
{
    "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"
                }
```


Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco Advanced Malware Protection voor endpoints API
- Cisco Advanced Malware Protection voor endpoints - gebruikershandleiding
- Technische ondersteuning en documentatie – Cisco Systems