Exportar listas de bloqueo de aplicaciones desde el portal de AMP con API

Contenido

Introducción

Este documento describe el procedimiento para exportar información de la lista de bloqueo de aplicaciones de protección frente a malware avanzado (AMP) para terminales con API.

Colaborado por Uriel Montero y Yeraldin Sánchez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso al panel de Cisco AMP para terminales
- Credenciales de API del portal de AMP: ID de cliente API y clave de API de terceros, este enlace muestra los pasos para obtenerlos: Cómo generar una credencial de API desde el portal de AMP
- En este documento, se utiliza un controlador API para la herramienta Postman

Componentes Utilizados

La información de este documento se basa en el software:

- Cisco AMP para terminales, consola 5.4.20190709
- herramienta Postman

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también se puede utilizar con la versión de la API:

- api.amp.cisco.com, v1

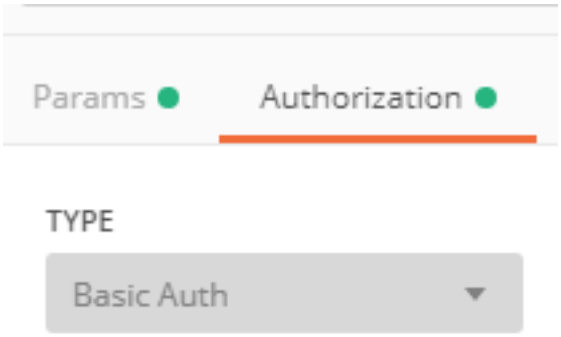
Antecedentes

Cisco no admite la herramienta Postman; si tiene alguna pregunta al respecto, póngase en contacto con el servicio de asistencia técnica de Postman.

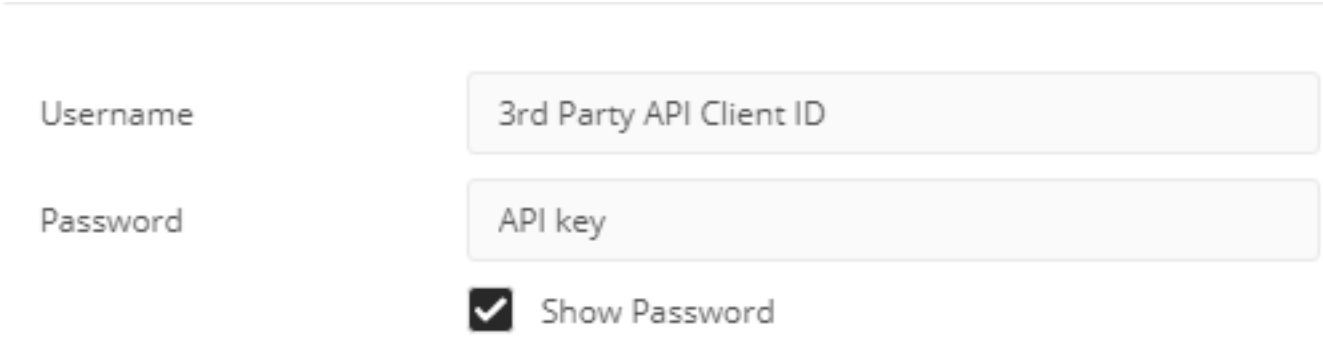
Proceso

Este es el proceso para recopilar las listas de bloqueo de aplicaciones de AMP y la lista SHA-256 de la lista seleccionada con las API y la herramienta Postman.

Paso 1. En la herramienta Postman, navegue hasta **Autorización > Autenticación básica**, como se muestra en la imagen.



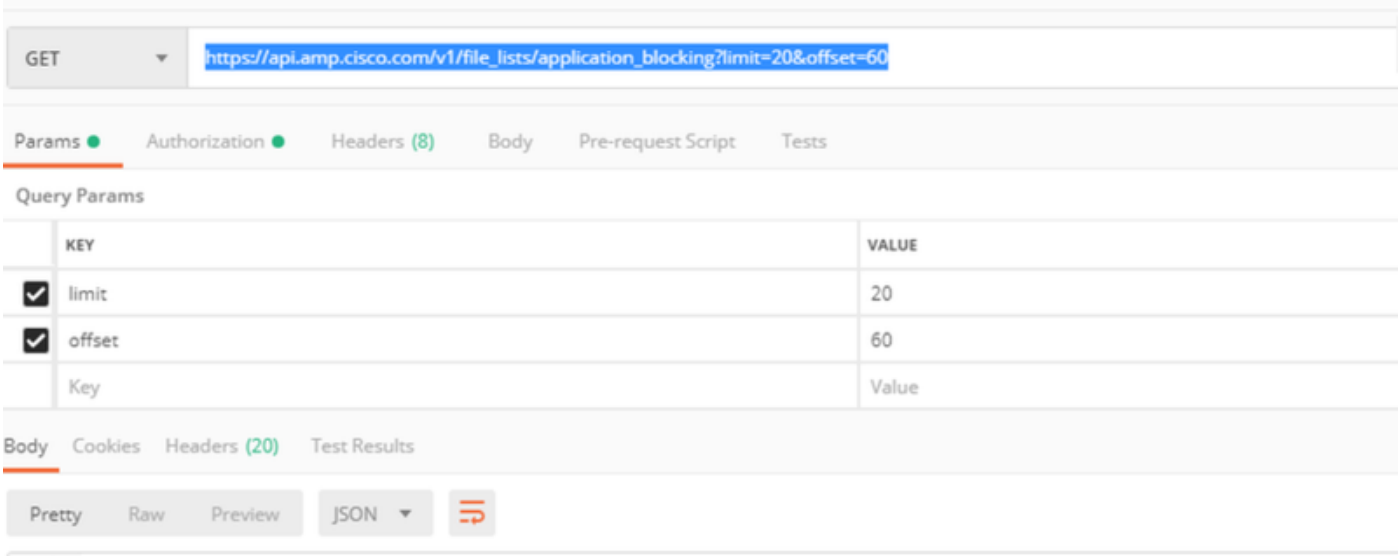
Paso 2. Agregue la **ID de cliente de API de terceros** en la sección Nombre de usuario y la **clave API** en la opción Contraseña, como se muestra en la imagen.



Paso 3. Dentro del controlador de API, seleccione la solicitud **GET** y pegue el comando:https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0.

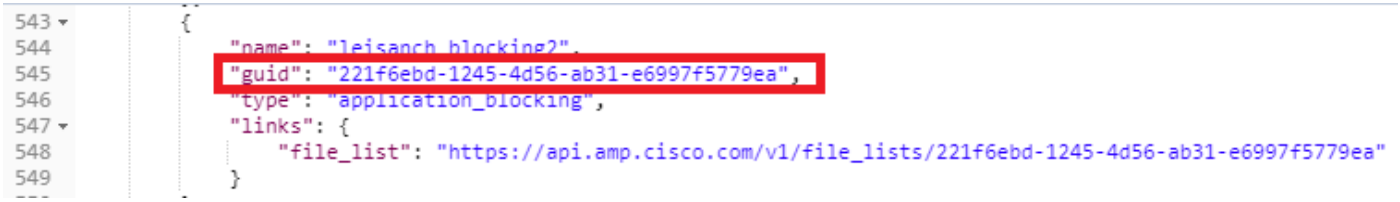
- Límite: número de elementos que muestra la herramienta
- Desplazamiento: desde donde la información comienza a mostrar los elementos

En este ejemplo, el valor límite es 20 y el desplazamiento es 60, la información comienza a mostrar la lista 61 y el límite es 80, como se muestra en las imágenes.

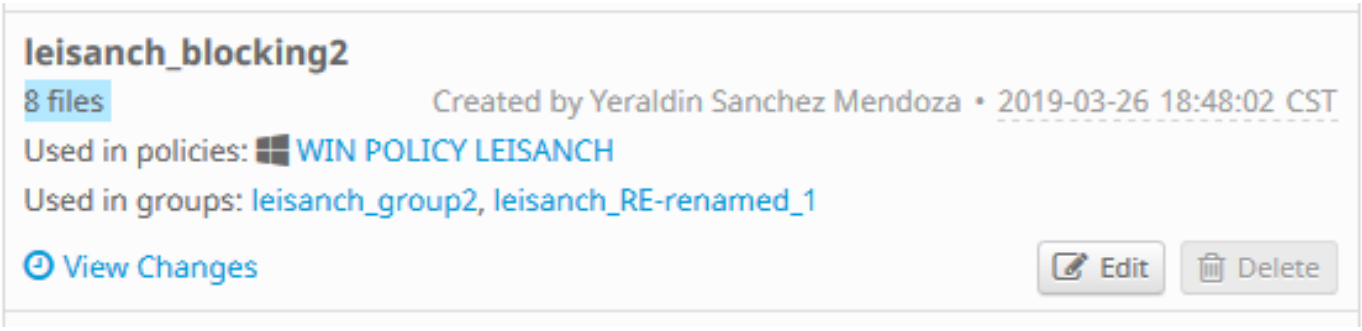


El comando muestra toda la lista de bloqueo de aplicaciones configurada en el portal de AMP si desea tener la lista de códigos SHA-256 de una lista específica, vaya al siguiente paso.

Paso 4. En la lista de bloqueo de la aplicación seleccionada previamente, copie el **guid** y ejecute el comando: https://api.amp.cisco.com/v1/file_lists/guid/files, en este ejemplo el guid es 221f6ebd-1245-4d56-ab31-e6997f5779ea para la lista leisanch_block2, se muestra en la imagen.



En el portal de AMP, la lista de bloqueo de la aplicación muestra 8 códigos SHA-256 agregados, como se muestra en la imagen.



Con el comando https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea, la lista debe mostrar 8 códigos SHA-256, como se muestra en la imagen.

```
{
    "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"
                }
```


Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- API de Cisco AMP para terminales
- Cisco AMP para terminales: guía del usuario
- Soporte Técnico y Documentación - Cisco Systems