Exporter des listes de blocage d'applications à partir du portail AMP avec des API

Contenu

Introduction

Ce document décrit la procédure à suivre pour exporter des informations à partir de la liste de blocage des applications AMP (Advanced Malware Protection) for Endpoints avec des API.

Contribué par Uriel Montero et Yeraldin Sánchez, ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès au tableau de bord Cisco AMP for Endpoints
- Informations d'identification de l'API à partir du portail AMP : ID de client et clé d'API d'API tiers, ce lien indique les étapes à suivre pour les obtenir : Comment générer des informations d'identification d'API à partir du portail AMP
- Un gestionnaire d'API, dans ce document, est utilisé dans l'outil Postman

Components Used

Les informations de ce document sont basées sur le logiciel :

- Cisco AMP for Endpoints for Endpoints version 5.4.20190709
- Outil 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

Ce document peut également être utilisé avec la version de l'API :

- api.amp.cisco.com, v1

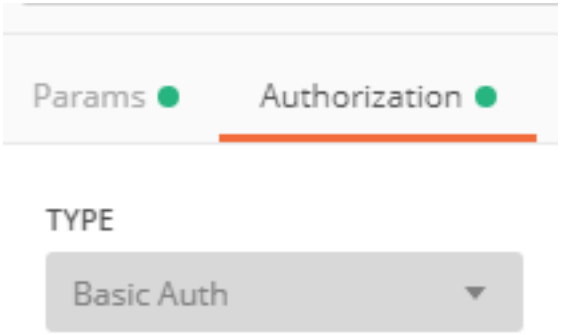
Informations générales

Cisco ne prend pas en charge l'outil Postman. Si vous avez des questions à ce sujet, contactez le support de Postman.

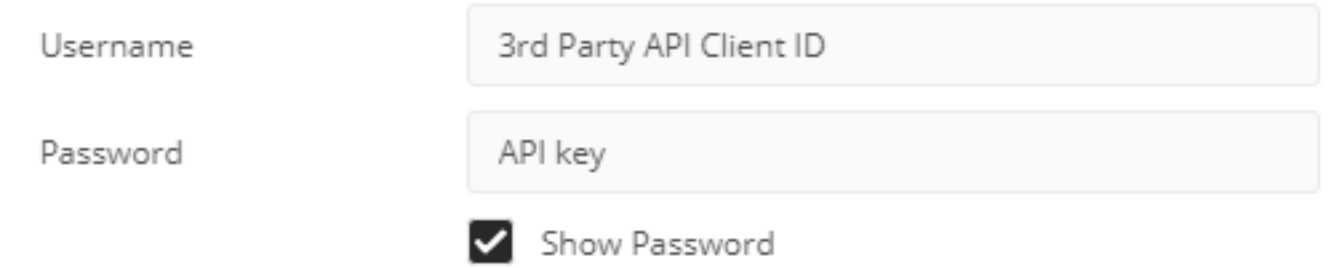
Process

Il s'agit du processus de collecte des listes de blocage des applications AMP et de la liste SHA-256 de la liste sélectionnée avec les API et l'outil Postman.

Étape 1. Dans l'outil Postman, naviguez jusqu'à **Autorisation > Authentification de base**, comme illustré dans l'image.



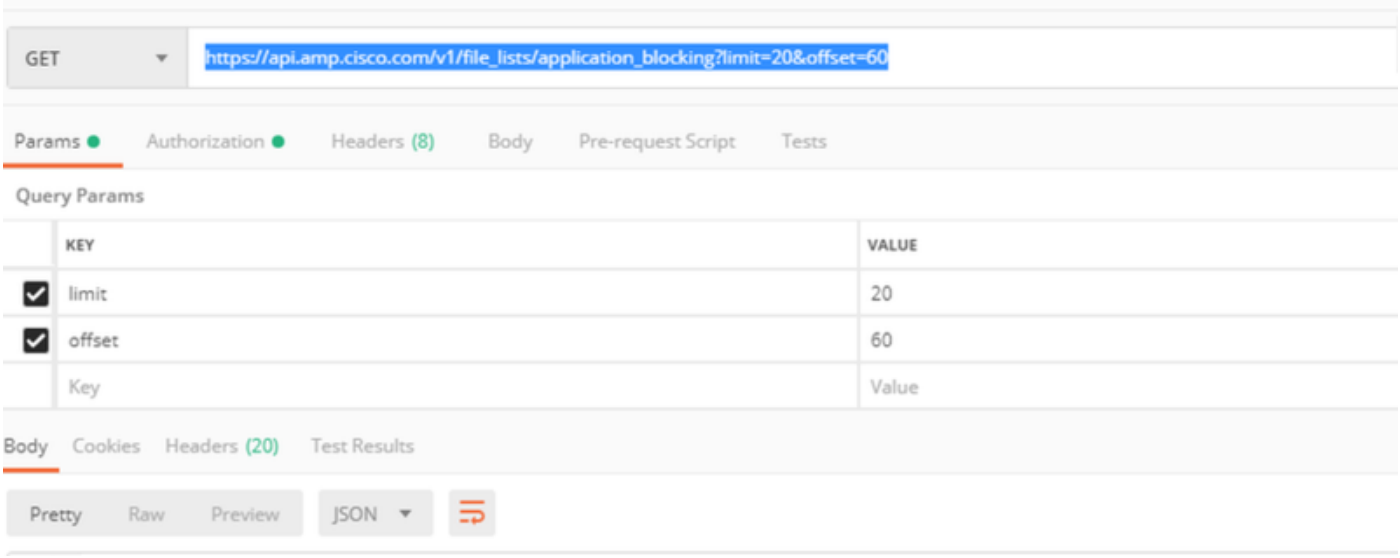
Étape 2. Ajoutez l'**ID client de l'API tierce** dans la section Nom d'utilisateur et la **clé API** dans l'option Mot de passe, comme illustré dans l'image.



Étape 3. Dans le gestionnaire d'API, sélectionnez la requête **GET** et collez la commande : https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0.

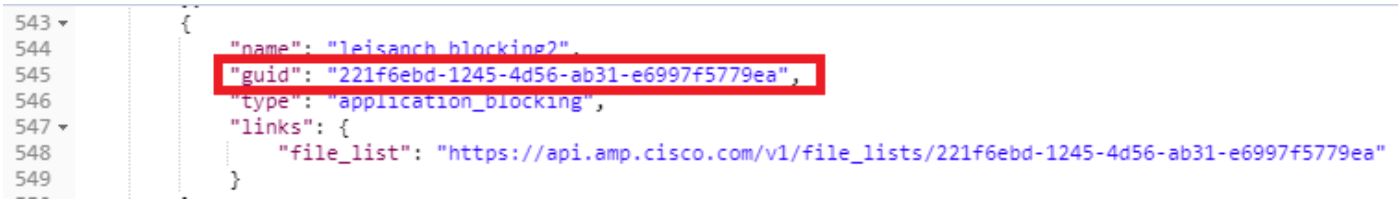
- Limite : nombre d'éléments affichés par l'outil
- Décalage : à partir de laquelle les informations commencent à afficher les éléments

Dans cet exemple, la valeur limite est 20 et le décalage est 60, les informations commencent à afficher la liste 61 et la limite est 80, comme le montrent les images.

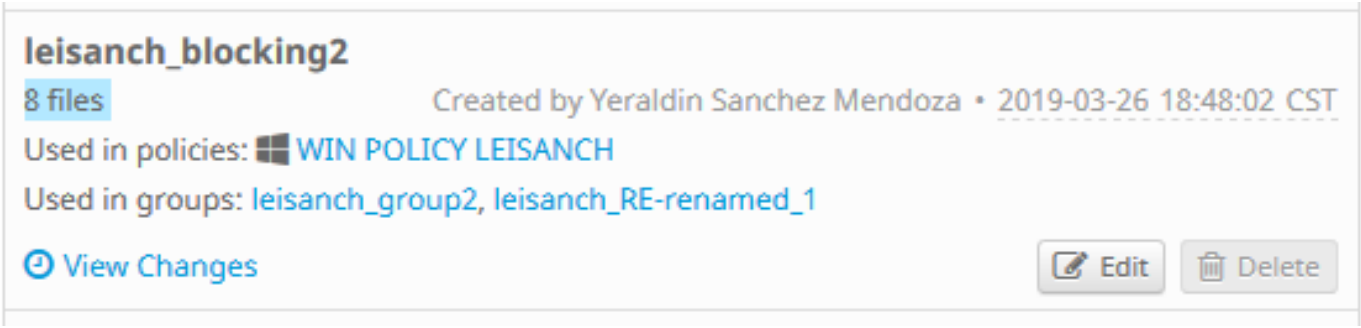


La commande affiche toutes les listes de blocage d'application configurées sur le portail AMP si vous voulez avoir la liste des codes SHA-256 d'une liste spécifique, accédez à l'étape suivante.

Étape 4. Dans la liste de blocage d'application précédemment sélectionnée, copiez le **GUID** et exécutez la commande https://api.amp.cisco.com/v1/file_lists/guid/files, dans cet exemple, le GUID est 221f6ebd-1245-4d56-ab31-e6997f5779ea pour la liste leisanch_block2, en tant, affiché dans l'image.



Sur le portail AMP, la liste de blocage des applications affiche 8 codes SHA-256 ajoutés, comme l'illustre l'image.



Avec la commande : https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea, la liste doit afficher 8 codes SHA-256, comme le montre l'image.

```
{
    "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"
                }
```


Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- API Cisco AMP for Endpoints
- Cisco AMP for Endpoints - Guide de l'utilisateur
- Support et documentation techniques - Cisco Systems