Esportazione di elenchi di blocco applicazioni dal portale AMP con le API

Sommario

Introduzione

In questo documento viene descritta la procedura per esportare informazioni dall'elenco di blocco dell'applicazione Advanced Malware Protection (AMP) for Endpoints con le API.

Contributo di Uriel Montero e Yeraldin Sánchez, tecnici Cisco TAC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso al dashboard di Cisco AMP for Endpoints
- Credenziali API dal portale AMP: ID client API di terze parti e chiave API, questo collegamento mostra i passaggi per ottenerli: Come generare una credenziale API dal portale AMP
- In questo documento viene utilizzato un gestore API per lo strumento Postman

Componenti usati

Le informazioni di questo documento si basano sul software:

- Cisco AMP for Endpoints console versione 5.4.20190709
- strumento Postman

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questo documento può essere usato anche con la versione API:

- api.amp.cisco.com, v1

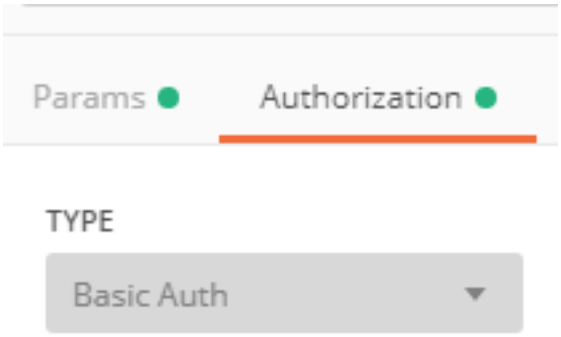
Premesse

Cisco non supporta lo strumento Postman. Per qualsiasi domanda, contattare il servizio di assistenza Postman.

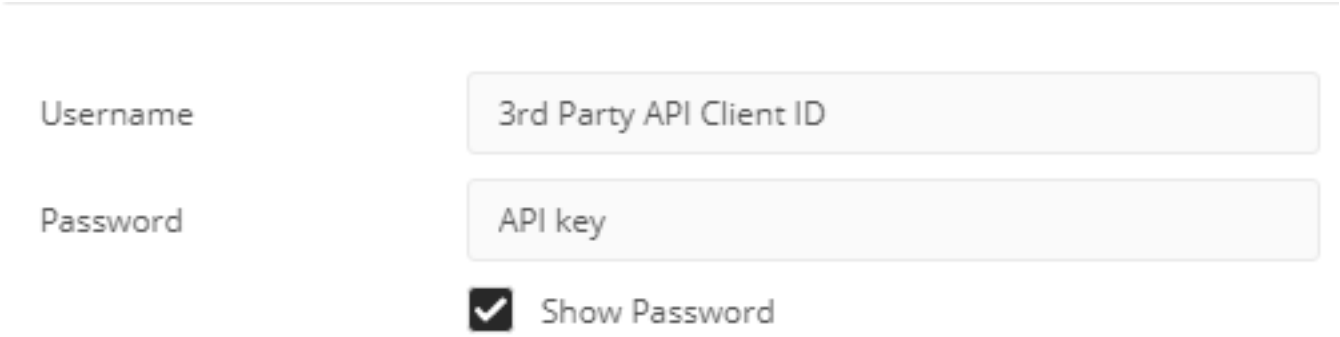
Processo

Questo è il processo per raccogliere gli elenchi di blocco delle applicazioni AMP e l'elenco SHA-256 dall'elenco selezionato con le API e lo strumento Postman.

Passaggio 1. Nello strumento Postman, passare ad **Autorizzazione > Autenticazione di base**, come mostrato nell'immagine.



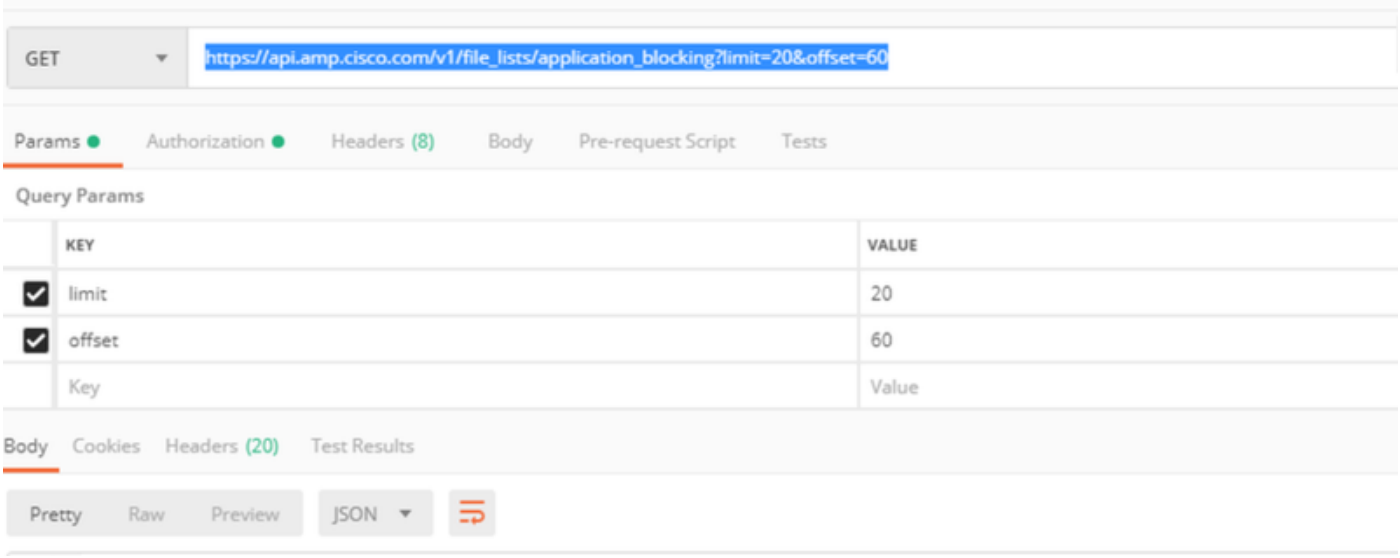
Passaggio 2. Aggiungere l'**ID del client API di terze parti** nella sezione Nome utente e la **chiave API** sull'opzione Password, come mostrato nell'immagine.



Passaggio 3. All'interno del gestore API, selezionare la richiesta **GET** e incollare il comando:https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0.

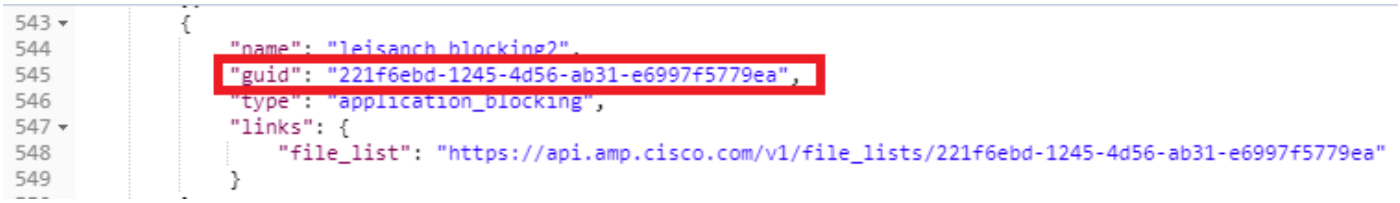
- Limite: numero di elementi visualizzati dallo strumento
- Scostamento: dal punto in cui le informazioni iniziano a visualizzare gli elementi

In questo esempio, il valore limite è 20 e l'offset è 60, le informazioni iniziano a mostrare l'elenco 61 e il limite è 80, come mostrato nelle immagini.

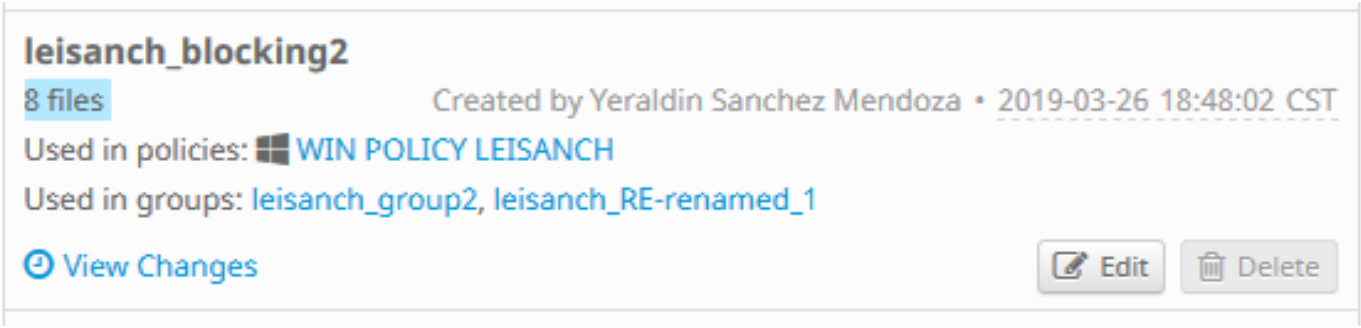


Il comando visualizza tutti gli elenchi di blocco delle applicazioni configurati sul portale AMP. Se si desidera visualizzare l'elenco dei codici SHA-256 di un elenco specifico, passare al passaggio successivo.

Passaggio 4. Nell'elenco delle applicazioni bloccate precedentemente selezionato, copiare il **GUID** ed eseguire il comando https://api.amp.cisco.com/v1/file_lists/guid/files, in questo esempio il GUID è 221f6ebd-1245-4d56-ab31-e6997f5779ea per l'elenco leisanch_blocking2, come mostrato nell'immagine.



Sul portale AMP, l'elenco di blocco delle applicazioni mostra 8 codici SHA-256 aggiunti, come mostrato nell'immagine.



Con il comando:https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea, l'elenco deve visualizzare 8 codici SHA-256, come mostrato nell'immagine.

```
{
    "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"
                }
```


Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- API Cisco AMP for Endpoints
- Cisco AMP for Endpoints - Guida per l'utente
- Documentazione e supporto tecnico – Cisco Systems