

# Exportar uma lista de bloqueio de aplicativos do portal AMP com APIs

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Processo](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve o procedimento para exportar informações da lista de bloqueio de aplicativos AMP (Advanced Malware Protection, Proteção avançada contra malware) para endpoints com APIs.

Contribuído por Uriel Montero e Yeraldin Sánchez, Engenheiros do TAC da Cisco.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao painel do Cisco AMP para endpoints
- Credenciais de API no portal AMP: ID do cliente API de terceiros e chave de API, este link mostra as etapas para obtê-las: [Como gerar uma credencial de API a partir do portal AMP](#)
- Um manipulador de API, neste documento, é usado na ferramenta Postman

## Componentes Utilizados

As informações neste documento são baseadas no software:

- Cisco AMP para endpoints para endpoints console versão 5.4.20190709
- ferramenta 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Produtos Relacionados

Este documento também pode ser usado com a versão da API:

- [api.amp.cisco.com](https://api.amp.cisco.com), v1

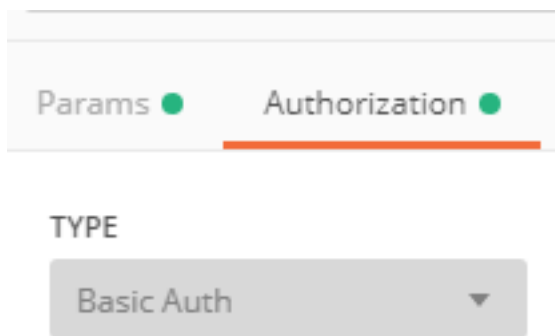
## Informações de Apoio

A Cisco não oferece suporte à ferramenta Postman. Se você tiver alguma dúvida, entre em contato com o suporte do Postman.

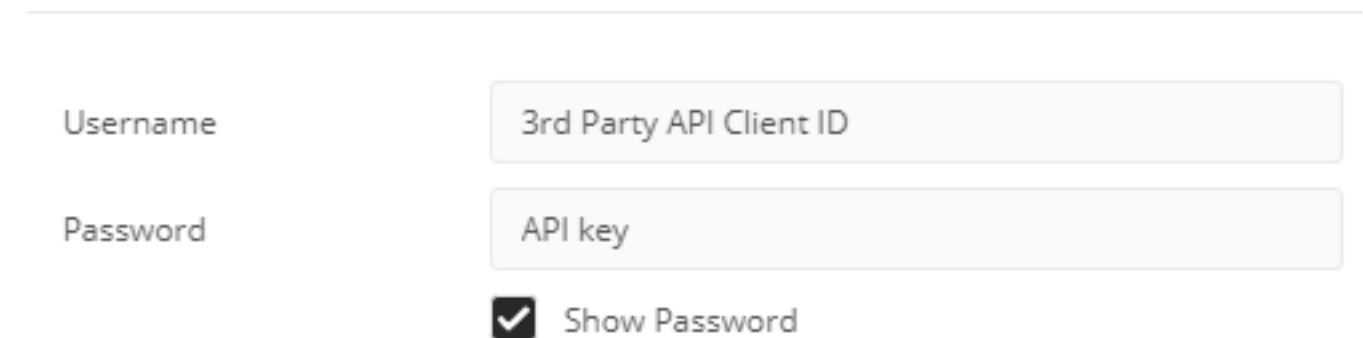
## Processo

Esse é o processo para coletar as listas de bloqueio de aplicativos da AMP e a lista SHA-256 da lista selecionada com APIs e a ferramenta Postman.

Etapa 1. Na ferramenta Postman, navegue até **Authorization > Basic Auth**, como mostrado na imagem.



Etapa 2. Adicione a **ID do cliente API de terceiros** na seção Nome de usuário e a **chave API** na opção Senha, como mostrado na imagem.



Etapa 3. Dentro do manipulador de API, selecione a solicitação **GET** e cole o comando: [https://api.amp.cisco.com/v1/file\\_lists/application\\_blocking?limit=100&offset=0](https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0).

- Limite: número de itens que a ferramenta exibe
- Deslocamento: de onde as informações começam a exibir os itens

Neste exemplo, o valor limite é 20 e o índice é 60, as informações começam a mostrar a lista 61 e o limite é 80, como mostrado nas imagens.

GET [https://api.amp.cisco.com/v1/file\\_lists/application\\_blocking?limit=20&offset=60](https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=20&offset=60)

Params Authorization Headers (8) Body Pre-request Script Tests

Query Params

KEY	VALUE
<input checked="" type="checkbox"/> limit	20
<input checked="" type="checkbox"/> offset	60
Key	Value

Body Cookies Headers (20) Test Results

Pretty Raw Preview JSON

O comando exibe toda a lista de bloqueio de aplicativos configurada no portal AMP se você quiser ter a lista dos códigos SHA-256 de uma lista específica, navegue até a próxima etapa.

Etapa 4. Na lista de bloqueio de aplicativos selecionada anteriormente, copie a **guid** e execute o comando: [https://api.amp.cisco.com/v1/file\\_lists/guid/files](https://api.amp.cisco.com/v1/file_lists/guid/files), neste exemplo a guid é 221f6ebd-1245-4d56-ab31-e6997f5779ea para a lista leisanch\_blocking2, como mostrado na imagem.

```
543 {
544   "name": "leisanch_blocking2",
545   "guid": "221f6ebd-1245-4d56-ab31-e6997f5779ea",
546   "type": "application_blocking",
547   "links": {
548     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
549   }
}
```

No portal AMP, a lista de bloqueio de aplicativos mostra 8 códigos SHA-256 adicionados, como mostrado na imagem.

**leisanch\_blocking2**

8 files Created by Yeraldin Sanchez Mendoza • 2019-03-26 18:48:02 CST

Used in policies: WIN POLICY LEISANCH

Used in groups: leisanch\_group2, leisanch\_RE-renamed\_1

[View Changes](#) [Edit](#) [Delete](#)

Com o comando: [https://api.amp.cisco.com/v1/file\\_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea](https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea), a lista deve exibir 8 códigos SHA-256, como mostrado na imagem.

```

1 {
2   "version": "v1.2.0",
3   "metadata": {
4     "links": {
5       "self": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea/files"
6     },
7     "results": {
8       "total": 8,
9       "current_item_count": 8,
10      "index": 0,
11      "items_per_page": 500
12    }
13  },
14  "data": {
15    "name": "leisanch_blocking2",
16    "guid": "221f6ebd-1245-4d56-ab31-e6997f5779ea",
17    "policies": [
18      {
19        "name": "WIN POLICY LEISANCH",
20        "guid": "768cdd65-dc8b-4301-82ae-60cb9bcbc57f",
21        "links": {
22          "policy": "https://api.amp.cisco.com/v1/policies/768cdd65-dc8b-4301-82ae-60cb9bcbc57f"
23        }
24      }
25    ],
26    "items": [
27      {
28        "sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c5",
29        "description": "first sha",
30        "source": "Created from SHAs in shasyeral.txt from [REDACTED]",
31        "links": {
32          "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
33        }
34      },
35      {
36        "sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c2",
37        "description": "first sha",
38        "source": "Created from SHAs in shasyeral.txt from [REDACTED]",
39        "links": {
40          "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
41        }
42      },
43      {
44        "sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c3",
45        "description": "first sha",
46        "source": "Created from SHAs in shasyeral.txt from [REDACTED]",
47        "links": {
48          "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
49        }
50      }
51    ]
52  }
53 }

```

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- [API da Cisco AMP para endpoints](#)
- [Cisco AMP para endpoints - Guia do usuário](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)