API를 사용하여 AMP 포털에서 애플리케이션 차단 목록 내보내기

목차

소개

이 문서에서는 API와 함께 AMP(Advanced Malware Protection) for Endpoints 애플리케이션 차단 목록에서 정보를 내보내는 절차에 대해 설명합니다.

기고자: Uriel Montero 및 Yeraldin Sánchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AMP for Endpoints 대시보드 액세스
- AMP 포털의 API 자격 증명:서드파티 API 클라이언트 ID 및 API 키, 이 링크에서는 이를 얻기 위한 단계를 보여줍니다. AMP 포털에서 API 자격 증명을 생성하는 방법
- 이 문서에서 API 처리기는 Postman 도구로 사용됩니다

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어를 기반으로 합니다.

- Cisco AMP for Endpoints for Endpoints 콘솔 버전 5.4.20190709
- Postman 툴

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

관련 제품

이 문서는 API 버전과 함께 사용할 수도 있습니다.

- api.amp.cisco.com, v1

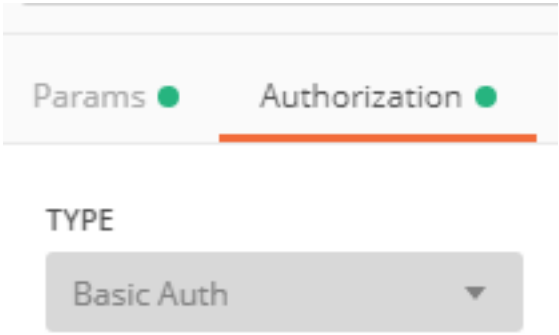
배경 정보

Cisco는 Postman 툴을 지원하지 않습니다. 이에 대한 질문이 있는 경우 Postman 지원에 문의하십시오.

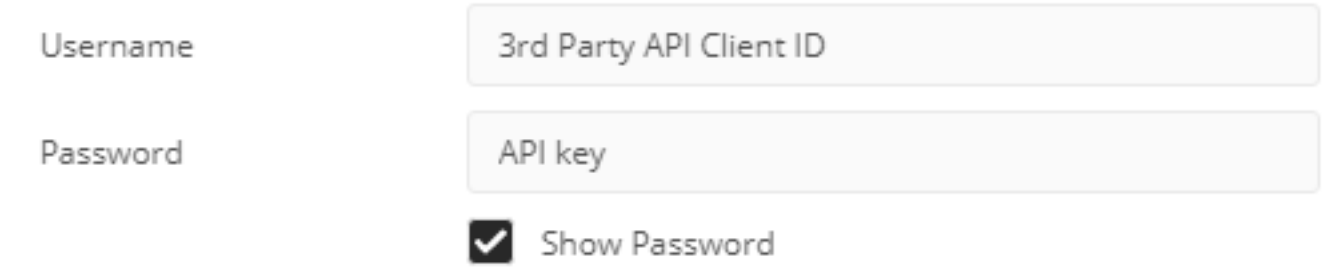
프로세스

API 및 Postman 툴을 사용하여 선택한 목록에서 AMP 애플리케이션 차단 목록 및 SHA-256 목록을 수집하는 프로세스입니다.

1단계. Postman 툴에서 이미지에 표시된 대로 **Authorization(권한 부여) > Basic Auth(기본 인증)**로 이동합니다.



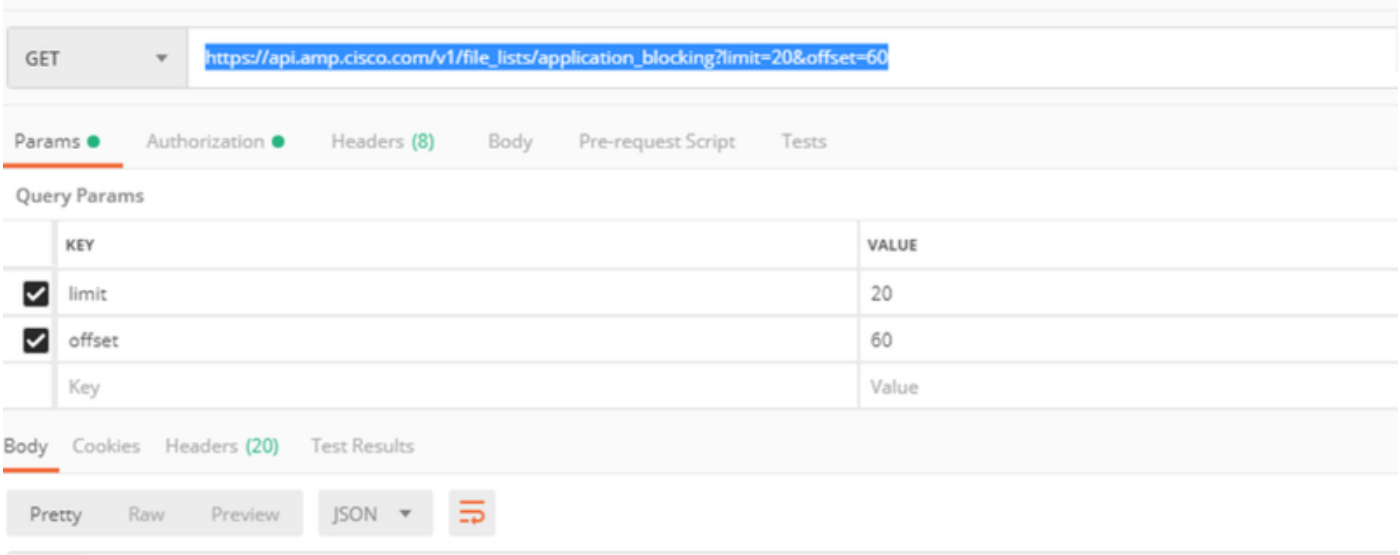
2단계. 사용자 이름 섹션에 **서드파티 API 클라이언트 ID**를 추가하고 이미지에 표시된 대로 비밀번호 옵션에 **API 키**를 추가합니다.



3단계. API 처리기 내에서 **GET** 요청을 선택하고 명령:https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0을 **붙여넣습니다**.

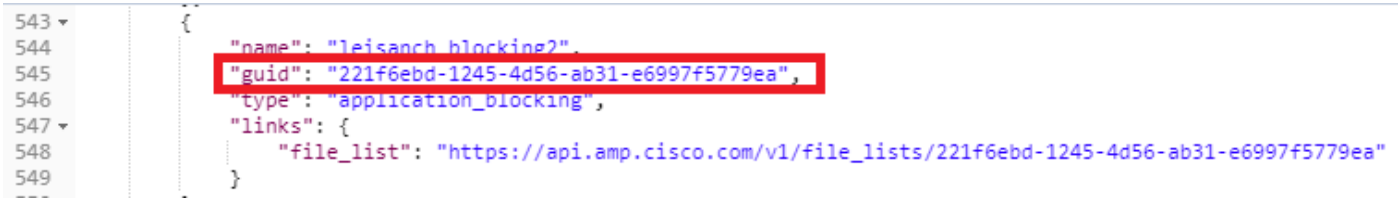
- 제한:도구에 표시되는 항목 수
- 오프셋:정보가 항목을 표시하기 시작하는 위치

이 예에서 제한 값은 20이고 오프셋은 60이고, 정보는 목록 61을 표시하기 시작하며, 제한 값은 이미지에 표시된 대로 80입니다.

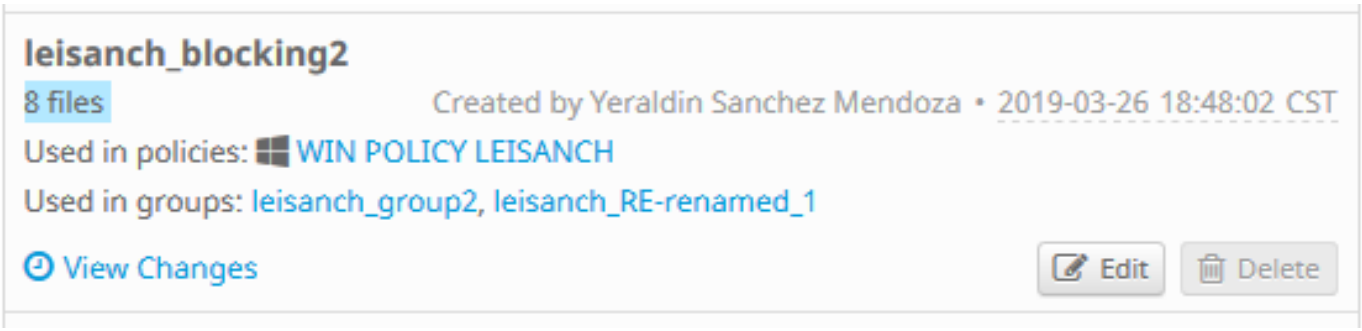


특정 목록의 SHA-256 코드 목록을 원하는 경우 이 명령은 AMP 포털에 구성된 모든 애플리케이션 차단 목록을 표시하고 다음 단계로 이동합니다.

4단계. 이전에 선택한 애플리케이션 차단 목록에서 guid를 **복사하고** https://api.amp.cisco.com/v1/file_lists/guid/files 명령을 실행합니다. 이 예에서 guid는 이미지의 leisanch_blocking2 목록에 대해 221f6ebd-1245-4d56-ab31-e699f5779ea입니다.



AMP 포털에서 애플리케이션 차단 목록에는 이미지에 표시된 대로 8개의 SHA-256 코드가 추가되었습니다.



명령:https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea를 사용하면 목록에 이미지에 표시된 대로 8개의 SHA-256 코드가 표시되어야 합니다.

```
{
    "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"
```


다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco AMP for Endpoints API
- Cisco AMP for Endpoints - 사용 설명서
- 기술 지원 및 문서 – Cisco Systems