使用API从AMP门户导出应用阻止列表

目录

简介

本文档介绍使用API从面向终端的高级恶意软件防护(AMP)应用阻止列表导出信息的过程。

作者：Uriel Montero和Yeraldin Sánchez，Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 访问面向终端的思科AMP控制面板
- 来自AMP门户的API凭证：第3方API客户端ID和API密钥，此链接显示获取这些密钥的步骤：如何从AMP门户生成API凭据
- 本文档中使用的API处理程序是Postman工具

使用的组件

本文档中的信息基于以下软件：

- 面向终端的思科AMP面向终端的终端控制台版本5.4.20190709
- 邮递员工具

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

相关产品

本文档还可与API版本一起使用：

- api.amp.cisco.com, v1

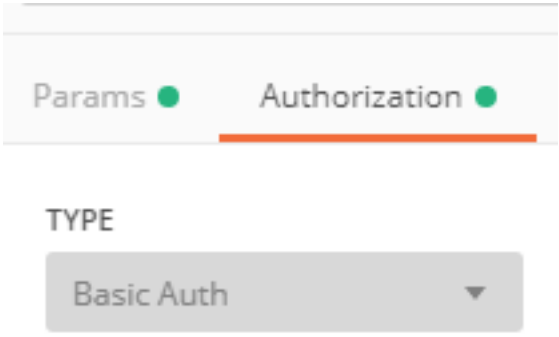
背景信息

思科不支持邮递员工具，如果您对此有疑问，请联系邮递员支持。

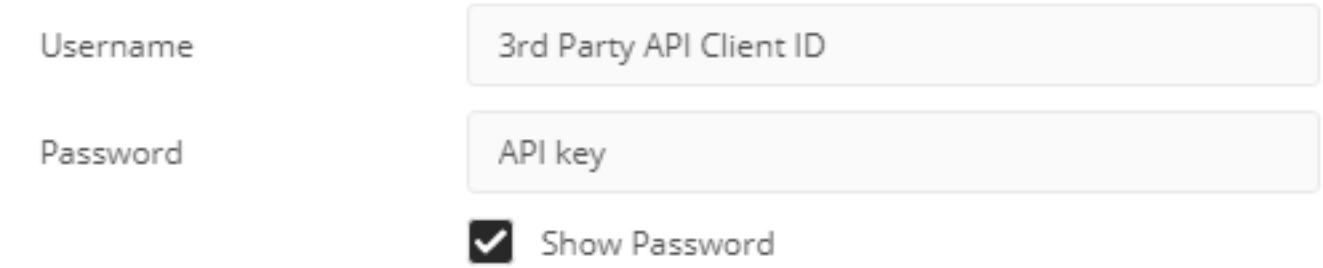
Process

这是从使用API和Postman工具的选定列表收集AMP应用阻止列表和SHA-256列表的过程。

步骤1.在Postman工具上，导航到**Authorization > Basic Auth**，如图所示。



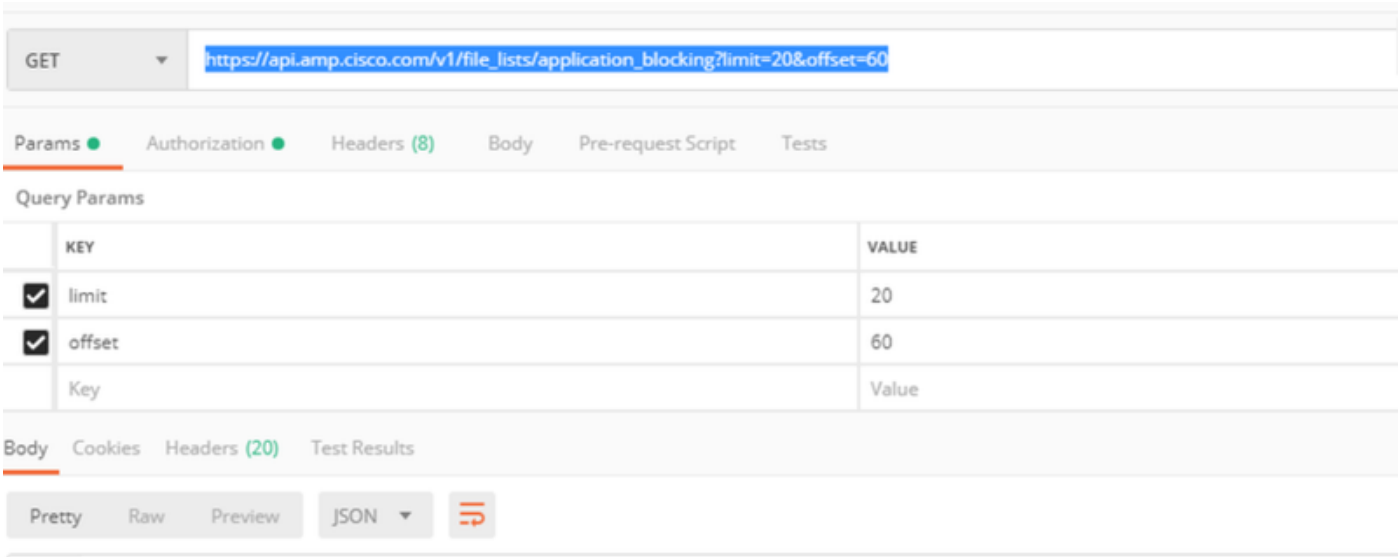
步骤2.在Username**部分添加第**三方API客户端ID，在**Password**选项上添加API密钥，如图所示。



步骤3.在API处理程序内，选择**GET请**求并粘贴命令：https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0。

- 限制:工具显示的项目数
- 偏移：信息开始显示项目的位置

在本例中，限制值为20，偏移量为60，信息开始显示列表61，限制为80，如图所示。

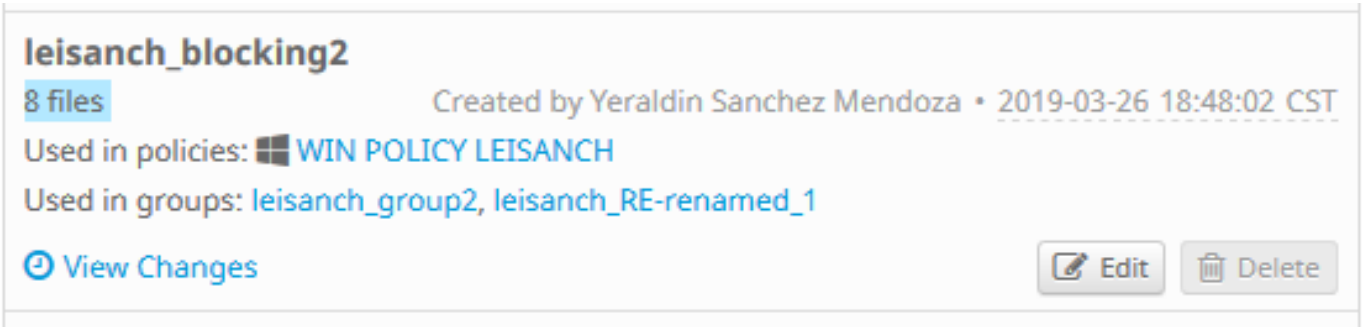


如果要拥有特定列表的SHA-256代码列表，请导航至下一步，该命令将显示在AMP门户上配置的所有应用阻止列表。

步骤4.在之前选择的应用阻止列表上，复制**guid**并运行命令https://api.amp.cisco.com/v1/file_lists/guid/files，在本例中，**guid为221f6ebd-1245-4d56-ab31-e6997f5779ea，用于lisanch_blocking2，如图所示。**


```
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             }
```


在AMP门户上，应用阻止列表显示8个添加的SHA-256代码，如图所示。



使用命令https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea时，列表必须显示8个SHA-256代码，如图所示。


```
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                  }
```

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 面向终端的思科AMP API
- 面向终端的思科AMP — 用户指南
- 技术支持和文档 - Cisco Systems