# 使用API从AMP门户导出应用阻止列表

### 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> <u>Process</u> <u>验</u> <u>啦</u> 排除</u> 相关信息

#### 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:<u>如何从AMP门户生成API凭据</u>
- 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。

Params 🔵	Authorization
TYPE	
Basic Auth	Ŧ

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。

Username	3rd Party API Client ID
Password	API key
	Show Password

步骤3.在API处理程序内,选择GET请求并粘贴命令:<u>https://api.amp.cisco.com/v1/file\_lists/application\_blocking?limit=100&offset=0</u>。

- 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。

GET	г	https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=20&offset=60							
Para	ms 🔵	Auth	orization 🖲	Headers (8)	Body	Pre-request Script	Tests		
Que	ry Param	s							
	KEY							VALUE	
~	limit							20	
$\checkmark$	offset							60	
	Key							Value	
Body	Cookies	; He	aders (20)	Test Results					
Pre	etty F	law	Preview	JSON 🔻	Ð				

步骤4.在之前选择的应用阻止列表上,复制guid并运行命令<u>https://api.amp.cisco.com/v1/file\_lists/guid/files</u>,在本例中,guid为221f6ebd-1245-4d56-ab31e6997f5779ea,用于lisanch\_blocking2,如图所示。

"name": "leisanch blocking2".
"guid": "221f6ebd-1245-4d56-ab31-e6997f5779ea",
"type": "application_blocking",
"links": {
"file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
}

### 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。

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					
O View Changes	🕑 Edit 🔟 Delete				

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

1 -	{		
2	"ve	rsion": "v1.2.0",	
3 🔻	"me	tadata": {	
4 -		"links": {	
5		"self": "https://api.amp.cisco.com/v1/file lists/221f6ebd-1245-4d56-ab31-e6997f5779ea/files"	
6		3	
7 -		"results": {	
0		· · · · · · · · · · · · · · · · · · ·	
0		Utar . o,	
9		Current_Item_count : 8,	
10		index : 0,	
11		"items_per_page": 500	
12		}	
13	},		
14 🔻	"da	ta": {	
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		v	
24			
24			
20		Ja Néteore R. F	
20 *		items: [	
2/ -			
28		"sna256": "380962c/98aDd2Dd/2/+Dc5062dae86ddc2Dae86393/902158D003/686+9821c5",	
29		"description": "first sha",	
30		"source": "Created from SHAs in shasyeral.txt from	
31 🔻		"links": {	
32		"file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea	e
33		}	
34		},	
35 🔻		{	
36		"sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c2",	
37		"description": "first sha",	
38		"source": "Created from SHAs in shasyeral.txt from ".	
30 -			
JJ		"links": {	
40		<pre>"links": {     "file list": "https://api.amp.cisco.com/v1/file lists/221f6ebd-1245-4d56-ab31-e6997f5779ea</pre>	
40 41		<pre>"links": {     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea }</pre>	
40 41 42		<pre>"links": {     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea   } }</pre>	
40 41 42 43 -		<pre>"links": {     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea     } },</pre>	
40 41 42 43 <del>-</del>		<pre>"links": {     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea     },     {</pre>	
40 41 42 43 <del>•</del> 44		<pre>"links": {     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea     } }, {     sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c3".</pre>	
40 41 42 43 <del>-</del> 44 45		<pre>"links": {     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea     }     ,     {</pre>	
40 41 42 43 <del>-</del> 44 45 46		<pre>"links": {     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea     } }, {     'sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c3"]     "description": "first sna",     "source": "Created from SHAs in shasyeral.txt from", </pre>	-
40 41 42 43 <del>-</del> 44 45 46 47 <del>-</del>		<pre>"links": {     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea }, {     sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c3"     "description": "first sna",     "source": "Created from SHAs in shasyeral.txt from",     "links": {     "links": {     " "     " "     " "     " "     " "     " "     " "     " "     " "     " "     " "     " "     " "     " "     " "     " "     " "     "</pre>	-
40 41 42 43 <del>▼</del> 44 45 46 47 <del>▼</del> 48		<pre>"links": {     "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea }, {     sha256": "3a0962c79aabd2bd727fbc50e2dae8ddc2bae863937902158b0037e86f9a21c3"]     "description": "first sna",     "source": "Created from SHAs in shasyeral.txt from</pre>	

# 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

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