

导出从AMP门户的一应用程序Blocklists有API的

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[Process](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述步骤导出从先进的恶意软件保护(AMP)的信息终端与API的应用程序blocklist的。

贡献用Uriel蒙特罗和Yeraldin Sánchez，Cisco TAC工程师。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

- 对Cisco AMP的访问终端控制板的
- 从AMP门户的API凭证：第三方Api client ID和API密钥，此链路显示步骤获取他们：[如何生成从AMP门户的一API凭证](#)
- 本文的，使用一个API处理程序邮差工具

[使用的组件](#)

本文档中的信息根据thede软件：

- 终端的Cisco AMP终端控制台版本5.4.20190709的
- 邮差工具

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](#)

本文可能也与API版本一起使用：

- api.amp.cisco.com，v1

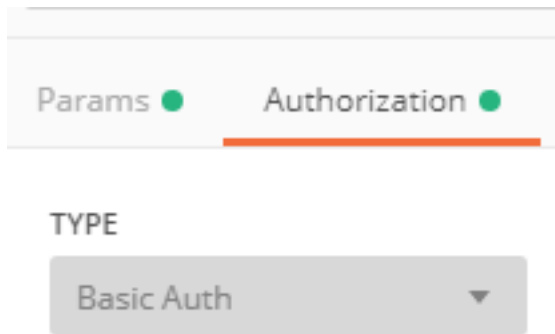
[背景信息](#)

Cisco不支持工具的邮差，如果有问题对此，请与邮差支持联系。

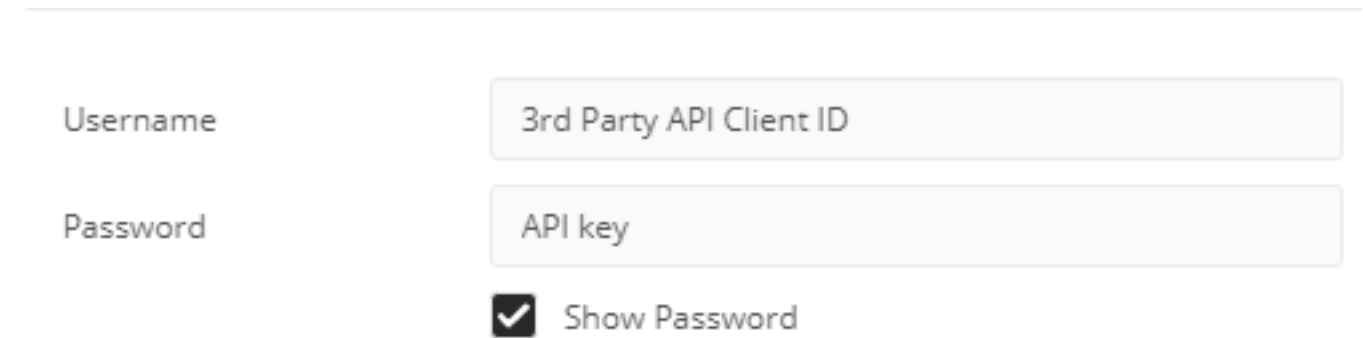
Process

这是收集AMP应用程序blocklists和SHA-256列表的进程从选定列表用API和邮差工具。

第 1 步：如镜像所显示，在邮差工具上，请导航对**授权>基本验证**。



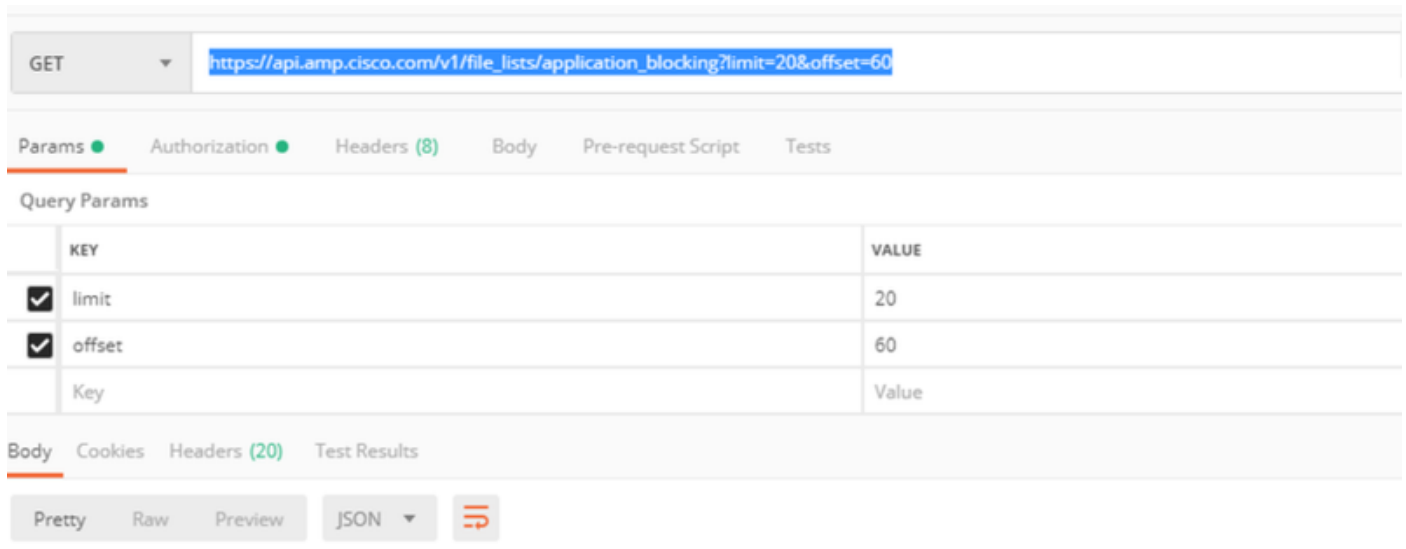
步骤2.如镜像所显示，添加在用户名部分的**第三方Api client ID**和在Password选项的**API密钥**。



步骤3.在API处理程序里面，请选择**GET**请求并且粘贴命令：https://api.amp.cisco.com/v1/file_lists/application_blocking?limit=100&offset=0。

- 限制：项目编号工具显示
- 偏移量：从信息开始显示项目的地方

在本例中，极限值是20，并且偏移量是60，信息开始显示列表61如镜像所显示，并且限制是80。



命令显示在AMP门户配置的所有应用程序blocklist，如果要有一特定列表的SHA-256代码的列表，导航对下一步。

第 4 步：在以前选择的应用程序blocklist，请复制guid并且运行命令：如镜像所显示， https://api.amp.cisco.com/v1/file_lists/guid/files，在本例中guid是列表的leisanch_blocking2 221f6ebd-1245-4d56-ab31-e6997f5779ea。

```
543 {
544   {
545     "name": "leisanch_blocking2",
546     "guid": "221f6ebd-1245-4d56-ab31-e6997f5779ea",
547     "type": "application_blocking",
548     "links": {
549       "file_list": "https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea"
550     }
551   }
552 }
```

在AMP门户，应用程序blocklist显示8个SHA-256代码被添加，如镜像所显示。

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

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

用命令：如镜像所显示， https://api.amp.cisco.com/v1/file_lists/221f6ebd-1245-4d56-ab31-e6997f5779ea，列表必须显示8个SHA-256代码。

```
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-60cb9bcb57f",
21        "links": {
22          "policy": "https://api.amp.cisco.com/v1/policies/768cdd65-dc8b-4301-82ae-60cb9bcb57f"
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 }
```

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

- [终端API的Cisco AMP](#)
- [终端的Cisco AMP -用户指南](#)
- [技术支持和文档 - Cisco Systems](#)