

# 文件分析在内容安全工具(ESA, SMA, WSA)和DC/FMC上的客户端ID

## Contents

[Introduction](#)

[文件分析在内容安全工具上的客户端ID](#)

[ESA GUI](#)

[SMA GUI](#)

[WSA GUI](#)

[FMC/DC GUI](#)

[Related Information](#)

## Introduction

本文描述如何查找或修建从Cisco防御中心(DC)或Firepower管理中心的与Cisco内容安全工具、电子邮件安全工具(ESA), 安全管理工具(SMA)和Web安全工具(WSA)相关联, 或者65个字符文件分析客户端ID (FMC)。

## 文件分析在内容安全工具上的客户端ID

### ESA GUI

1. 安全服务>文件名誉和分析
2. 点击编辑整体设置...
3. 扩展文件分析的先进的设置

列出得文件分析客户端ID这里。

运行AsyncOS 10.0.0-203电子邮件安全示例的vESA :

#### Edit File Reputation and Analysis Settings

Advanced Malware Protection	
Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.	
File Reputation Filtering:	<input checked="" type="checkbox"/> Enable File Reputation
File Analysis: ?	<input checked="" type="checkbox"/> Enable File Analysis
	File Types:
	<input checked="" type="checkbox"/> Adobe Portable Document Format (PDF)
	<input checked="" type="checkbox"/> Microsoft Office 2007+ (Open XML)
	<input checked="" type="checkbox"/> Microsoft Office 97-2004 (OLE)
	<input checked="" type="checkbox"/> Microsoft Windows / DOS Executable
	<input checked="" type="checkbox"/> Other potentially malicious file types
Advanced Settings for File Reputation	Advanced settings for File Reputation
Advanced Settings for File Analysis	File Analysis Server URL: AMERICAS (https://panacea.threatgrid.com)
	File Analysis Client ID: 01_VLNESA000132_4239CEE15FF3A9F9B804-0EDD2CF4F9D9_C100V_00000000

**Note:**有在文件分析客户端ID上的一个区别虚拟工具的与硬件工具。

文件分析客户端ID根据以下65字符串格式 :

值	说明
01_	ESA
VLNESAXXXYYY_	如果这是一种虚拟工具，使用VLN许可证# (从与showlicense的CLI被找到)。 如果这是工具，没有字段。
SERIAL_	这将是与版本的CLI被找到)的FULL序列工具(。
CX00V_	这是工具型号(再，从在CLI的版本)。 如果它是一种虚拟工具与硬件工具，这再将变
00000000	落后的零。 这些根据早先字段将变化，为了完成65个字符的字段。

## SMA GUI

### 1. 集中管理> Security工具

在底下部分，文件分析客户端ID列出得文件分析这里。

运行AsyncOS 9.6.0-051安全管理示例的vSMA :

File Analysis	
File Analysis Client ID:	06_VLNSMA20434706_564D6D7D1766E1C23D6E-D7CAE05515F5_M100V_000000
Appliance Group ID/Name:	File Analysis Server URL: AMERICAS:https://panacea.threatgrid.com
Group Name:	<input type="text"/> <input type="button" value="Group Now"/>
	<ul style="list-style-type: none"> <li>Typically, this value will be your Cisco Connection Online ID (CCO ID).</li> <li>This Group Name is case-sensitive.</li> <li>It must be configured identically on each appliance. An appliance can belong to only one group per server.</li> </ul>
	<b>This change will take effect immediately, without Commit. Once grouped, this value can only be reset by Cisco support.</b>
Grouping Details:	Not part of any group yet.

**Note:**有在文件分析客户端ID上的一个区别虚拟工具的与硬件工具。

文件分析客户端ID根据以下65字符串格式 :

值	说明
06_	SMA
VLNSMAXXXYYY_	如果这是一种虚拟工具，使用VLN许可证# (从与showlicense的CLI被找到)。 如果这是工具，没有字段。
SERIAL_	这将是与版本的CLI被找到)的FULL序列工具(。
MX00V_	这是工具型号(再，从在CLI的版本)。 如果它是一种虚拟工具与硬件工具，这再将变
000000	落后的零。 这些根据早先字段将变化，为了完成65个字符的字段。

## WSA GUI

### 1. 安全服务>反Malware和名誉

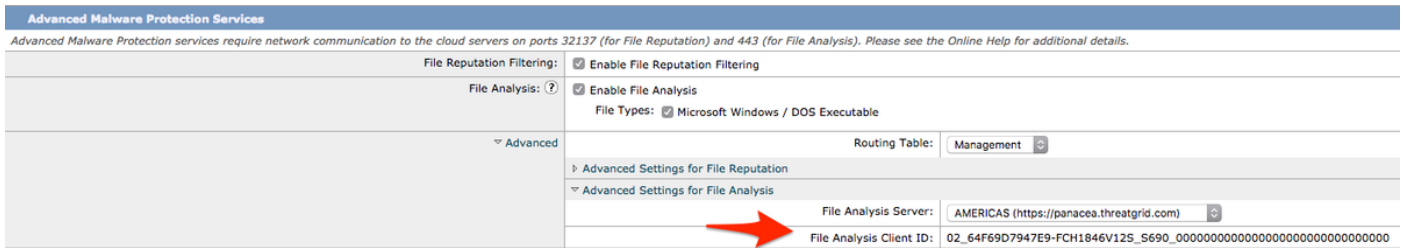
#### 2. 点击编辑整体设置...

#### 3. 在先进的Malware和保护业务区分，扩展先进

#### 4. 扩展文件分析的先进的设置

列出得文件分析客户端ID这里。

运行AsyncOS 9.1.1-041 Web安全示例的WSA :



**Note:** 有在文件分析客户端ID上的一个区别虚拟工具的与硬件工具。

文件分析客户端ID根据以下65字符串格式：

值	说明
02_	WSA
VLNWSAXXXYYY_	如果这是一种虚拟工具，使用VLN许可证# (从与showlicense的CLI被找到)。如果这是工具，没有字段。
SERIAL_	这将是与版本的CLI被找到)的FULL序列工具(。
SX00V_	这是工具型号(再，从在CLI的版本)。如果它是一种虚拟工具与硬件工具，这再将变
000000	落后的零。这些根据早先字段将变化，为了完成65个字符的字段。

## FMC/DC GUI

从运行的CLI获得API关键(文件分析ID)为FMC/DC，：

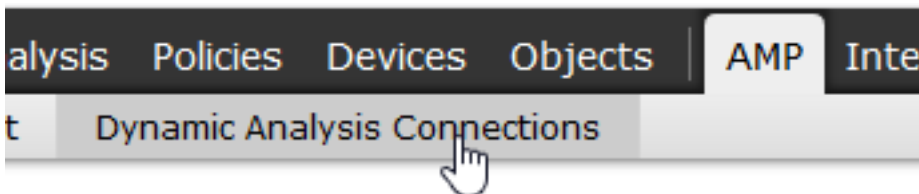
```
perl -MFlyLoader -e "print SF::Files::Analysis::get_apikey()"
```

**Note:** 在一些硬件上有Perl的多安装。管理Perl的默认安装可能不正确地执行命令。如果有被看到的输出错误，请指定以下，直接路径，当呼叫Perl时：`/ngfw/usr/bin/perl -MFlyLoader -e "打印SF :: 文件 :: 分析 :: get_apikey()"`

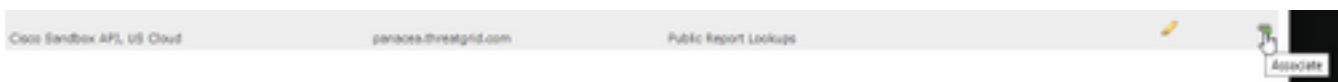
1. 连接对AMP >Dynamic分析连接
2. 在菜单项panacea.threatgrid.com的右边请点击关联图标。
3. 上推是将出现，点击完成关联。
4. 验证在URL的结尾文件分析客户端ID。ID在devices%3D以后开始对URL的结尾。

示例：

### 1.连接的菜单



### 2.关联FMC



### 3. 确认的关联

