# 目录



# 简介

本文描述如何确定通过先进的恶意软件保护的文件(安培)处理在思科电子邮件安全工具(ESA)是否为文件分析发送，并且什么相关的日志文件提供。

# 确定文件是否为分析上传

当文件分析启用时，文件也许通过安培自动地发送到进一步分析的Cloud。这提供最高水平保护零天和被瞄准的威胁。当文件名誉过滤启用时，文件分析只是可用的。

请使用文件类型选项为了限制也许发送到Cloud文件的种类。发送的特定文件根据从文件分析服务Cloud的请求总是，瞄准那些文件另外的分析是需要的。当文件分析服务Cloud到达产能时，特定的文件类型的文件分析也许临时地禁用。

> **注意**：参考先进的恶意软件保护业务的文件标准思科内容安全产品Cisco文档的其他信息。

> **注意**： 查看版本注释和用户指南在您的设备运行AsyncOS的特定版本的，因为文件分析文件类型将变化基于版本。

可以为文件分析发送的文件类型：

- 支持文件分析和Windows可执行的所有版本，例如：**.exe**、**.dll**、**.sys**和**.scr**文件。
- 您为在Settings页的反恶意软件的加载选择和的名誉的文件类型(Web安全)或Settings页文件的名誉和的分析(电子邮件安全)。初始支持包含PDF和微软办公软件文件。

  > **注意**： 如果在文件分析服务的负载超出产能，也许不分析一些文件，即使文件类型为分析选择。当服务临时地无法处理特定类型的文件时，您收到警报。

这是一些重要提示：

- 文件大小标准由根据当前威胁趋势的文件分析服务动态地设立，并且它能在任何时间更改。标

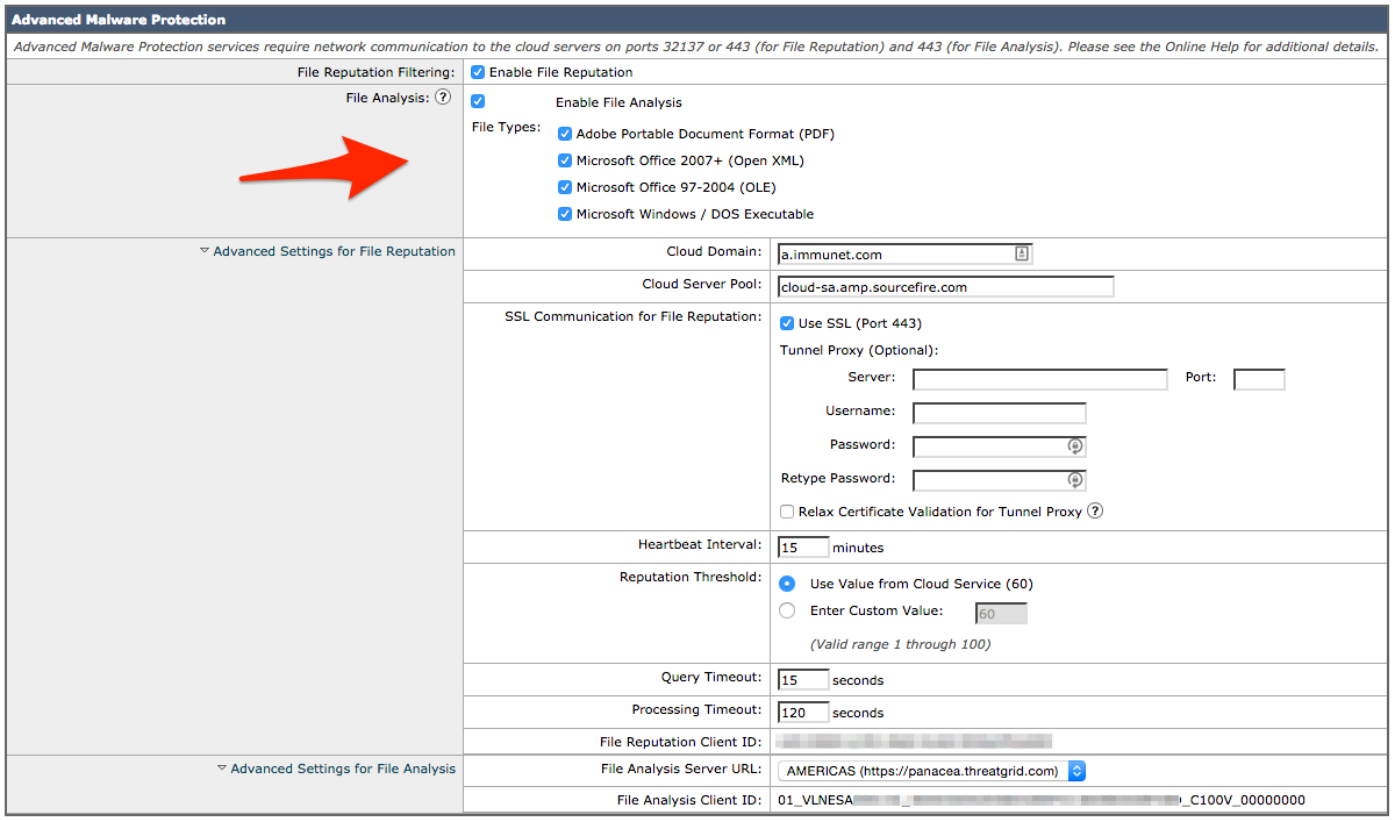
准更改自动地生效，因此您没有要求采取任何行动。

- 如果文件从任何来源最近上传，文件再没有上传。为了从报告页的文件分析得到此文件的文件分析结果， **SHA-256的**搜索。

- 设备尝试一次上传文件;如果加载不是成功的(例如，由于连接问题)，文件也许不上传。如果失败归结于文件分析服务器超载，加载更加尝试。

# 配置文件分析的安培

为了通过GUI配置文件分析的安培，请导航对**安全服务>文件名誉和分析> Edit全局设置...** ：




为了通过CLI配置文件分析的安培，请输入**ampconfig > setup命令**并且通过答复向导移动。当您提交与此问题时，您必须选择**Y** ： **是否要修改文件分析的文件类型？**

凭此配置，启用的文件类型为分析被扫描并且发送，如可适用。

# 复核文件分析的安培日志

当可适用的文件由安培时扫描，他们在安培日志被记录。为了检查所有安培操作的此日志，请输入**尾标安培**命令到CLI或者通过或者**尾标的**答复向导移动或**grep命令**。 **grep命令**是有用的，如果认识您在安培日志希望搜索的特定文件或其他详细信息。

示例如下：

**amp_watchdog.txt**文件显示在日志的每十分钟。此文件是一部分的keep-alive AMP.的。

使用为名誉处理的文件，他们有**upload_action**被标记在文件名誉查询结束时。有加载操作的三答复

：

此答复指明文件是否为分析发送。再次，它必须满足已配置的文件类型的标准为了顺利地提交。

### 加载操作"0"的说明与加载操作"2"

对于"0,"这意味着文件“没有必要为加载发送”。或者，一个更加好的方式查看它是，文件*可以*为加载*如果必须*发送到文件分析。 然而，如果文件然后没有要求文件没有发送。

对于"2,"这的严格“请勿发送”加载的文件。 此操作最终和果断，并且文件分析处理完成。

## 示例情景

此部分描述文件为分析适当地上传的三个可能的情况，或者不上传的归结于一个特定原因。

### 为分析上传的文件

此示例显示满足标准和用**upload_action**标记**= 1.的**DOCX文件**。**在下一条，**为分析**安全哈希算法(SHA)**上传的文件**被记录对安培日志。

### 为分析没上传的文件由于文件类型

此示例显示由安培扫描并且用**upload_action**标记**= 1**被添附对文件名誉日志的压缩文件，但是安培文件分析不支持压缩文件。所以，没有SHA被记录对此文件的安培日志。

### 为分析没上传的文件，由于文件已经知道

由与**upload_action的**安培扫描**= 2**被添附对文件名誉日志的此示例显示PDF文件。此文件已经为Cloud所知和没有要求为分析上传，因此再没有上传。

## 相关信息

- AsyncOS用户指南
- 先进的恶意软件保护业务的文件标准思科内容安全产品的
- ESA提前的恶意软件保护(安培)测验
- 技术支持和文档 - Cisco Systems