文件信誉过滤和文件分析：

本章包含以下部分：

文件信誉过滤和文件分析概述

思科高级恶意软件保护 通过如下方式防范 邮件附件 中的零日威胁和基于文件的针对性威胁：

- 获取已知文件的信誉。
- 分析尚不为信誉服务所知的某些文件行为。
- 在获得新信息时持续评估新出现的威胁，并在确定为威胁的文件进入您的网络后通知您。

此功能可用于传入邮件和传出邮件。

文件信誉和文件分析服务提供适用于公共云或私有云（内部部署）的选项。

- 私有云文件信誉服务由思科 AMP 虚拟私有云设备提供，在“代理”或“air-gap”（本地）模式下运行。请参阅配置本地文件信誉服务器, on page 6。
- 私有云文件分析服务由本地思科 AMP 恶意软件分析设备提供。请参阅配置本地文件分析服务器 , on page 6。

文件威胁判定更新

随着新信息的出现可更改威胁判定。文件最初可能会被评定为未知或正常，然后，因此，文件可能会被发送至收件人。如果获得新信息时威胁判定更改，您会收到警报，且文件及其新判定将出现在 AMP 判定更新报告中。可以调查进入点，作为补救任何威胁影响的起点。

也可以将判定从恶意更改为正常。

当文件分析后在文件中找不到动态内容时，所得判决是低风险。文件未送交文件分析，邮件将通过邮件管道传递。

当设备处理同一文件的后续实例时，系统将立即应用已更新的判定。

有关判定更新的定时信息包括在文件信誉和分析服务所支持的文件 , on page 3中引用的文件条件文档中。

相关主题

- 文件信誉和文件分析报告与跟踪 , on page 22
- 在文件威胁判定更改时采取操作 , on page 25

文件处理概述

除非已对邮件采取最终操作，否则无论来自先前扫描引擎的判定如何，在防病毒扫描后都将立即评估文件信誉和发送文件进行分析。

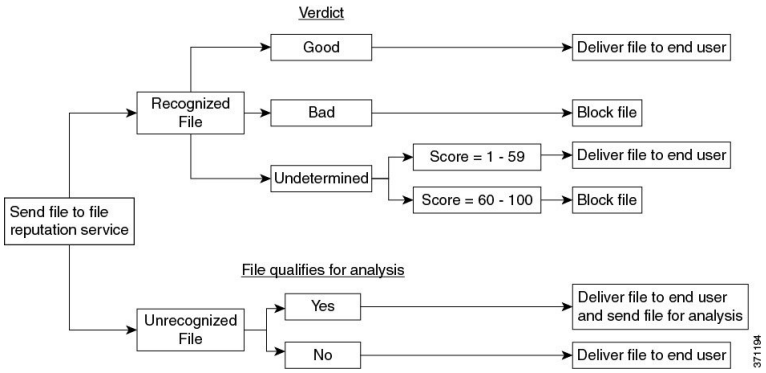
Note 默认情况下，如果邮件的 MIME 信头格式不正确，文件信誉服务将返回“不可扫描”的判定。设备还将尝试从该邮件中提取附件。如果设备无法提取附件，判定将保留为“不可扫描”(unscannable)。如果设备能够提取附件，则评估附件的文件信誉。如果附件是恶意的，判定将从“不可扫描”(unscannable) 更改为“恶意”(malicious)。

设备和文件信誉服务之间的通信已加密并已防止篡改。

评估文件的信誉后：

- 如果邮件不包含任何附件，则文件信誉服务将返回“已跳过”的判定。
- 如果文件为文件信誉服务所熟知且被确定为正常， 邮件继续通过工作队列。
- 对于邮件中的任何附件，，如果文件信誉服务返回恶意判定，则设备应用您在适用邮件策略中。
- 如果文件为信誉服务所知但信息不足以作出最后判定，则信誉服务基于文件特征（例如威胁指纹和行为分析）返回信誉得分。如果此分数达到或超过所配置的信誉阈值，则设备将应用您在邮件策略中为包含恶意软件的文件所配置的操作。
- 如果信誉服务没有文件相关信息，且文件不符合分析标准（请参阅文件信誉和分析服务所支持的文件 , on page 3），则将文件视为正常并且邮件继续通过工作队列。
- 如果启用了文件分析服务，信誉服务没有关于文件的信息，并且文件满足可以分析的文件的标准（请参阅文件信誉和分析服务所支持的文件 , on page 3），则可以隔离邮件（请参阅隔离附件送交分析的邮件, on page 18）并将文件送交分析。如果在发送附件以供分析时尚未将设备配置为隔离邮件或者不发送文件以供分析，则系统会向该用户释放邮件。
- 对于具备本地文件分析的部署，信誉评估和文件分析同时进行。如果信誉服务返回判定，则会使用该判定，因为信誉服务包括来自各种来源的输入。如果文件对于信誉服务来说是未知的，则会使用文件分析判定。
- 如果因为与服务器的连接超时而导致文件信誉判定信息不可用，则将该文件视为“不可扫描”(unscannable)，并应用配置的操作。

Figure 1: 面向公共云文件分析部署的思科高级恶意软件保护 工作流程



如果将文件送交分析：

- 如果将文件发送到云进行分析：文件将通过 HTTPS 发送。
- 分析通常需要数分钟，但可能更长。
- 在文件分析后标记为恶意的文件可能不会被信誉服务识别为恶意文件。文件信誉由一段时间内的多种因素确定，而不一定由单一的文件分析判定来确定。
- 使用本地 Cisco Secure Endpoint 恶意软件分析设备分析文件的结果将缓存在本地。

有关判定更新的信息，请参阅文件威胁判定更新 , on page 1。

文件信誉和分析服务所支持的文件

信誉服务评估大多数文件类型。文件类型标识由文件内容确定，而不是取决于文件名扩展名。

可以对信誉未知的某些文件进行威胁特征分析。在配置文件分析功能时，选择要分析的文件类型。可以动态添加新类型；当可上传的文件类型列表变化时，则会收到警报，并可以选择添加的文件类型进行上传。

有关信誉及分析服务支持哪些文件的详细信息只向注册思科客户提供。有关评估和分析哪些文件的信息，请参阅可从以下网址获取的《思科内容安全产品高级恶意软件保护服务的文件条件：https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html。评估文件信誉和文件送交分析的标准可能随时变更。

要访问此文档，您必须拥有一个含有支持合同的思科客户账户。要注册账户，请访问 https://tools.cisco.com/RPF/register/register.do。

您应将策略配置为阻止 传送 不是由 思科高级恶意软件保护处理的文件。

Note 已从源上传以进行分析的文件（传入邮件或传出邮件中的文件）不会再次上传。要查看此类文件的分析结果，请在“文件分析”(File Analysis) 报告页面中搜索 SHA-256。

相关主题

- 启用和配置文件信誉和分析服务 , on page 7
- 确保您收到关于 思科高级恶意软件保护 问题的警报, on page 22
- 存档或压缩文件处理, on page 4

存档或压缩文件处理

如果文件已压缩或存档，

- 则系统会评估压缩或存档文件的信誉。

有关检查哪些存档和压缩文件的信息（包括文件格式），请参阅文件信誉和分析服务所支持的文件 , on page 3链接的信息。

在此情景中，

- 如果提取的其中一个文件是恶意的，则文件信誉服务会针对压缩或存档文件返回“恶意”判定。
- 如果压缩或存档文件是恶意的，并且所有已提取文件都是干净的，则文件信誉服务会针对压缩或存档文件返回“恶意”判定。
- 如果判定任何提取的文件为未知文件，则可以选择将提取的文件送交分析（如果已配置该功能且文件分析支持该文件类型）。
- 如果将提取的任何文件或附件判定为低风险，则不将该文件送交分析。
- 如果在对压缩或存档文件进行解压缩时提取文件失败请记住，在此场景中，如果其中一个提取的文件是恶意文件，那么文件信誉服务会针对压缩或存档文件返回“恶意”(Malicious) 判定（“恶意”(Malicious) 判定优先于“不可扫描”(Unscannable) 判定）。
- 在以下情况下，压缩文件或存档文件将被视为不可扫描文件：
  - 数据压缩比大于 20。
  - 存档文件包含五个以上的嵌套级别。
  - 存档文件包含的子文件超过 200 个。
  - 存档文件大小超过 50 MB。
  - 存档文件受密码保护或不可读。

Note 系统不会评估具有安全 MIME 类型（例如文本/纯文本）的已提取文件的信誉。

发送到云端的信息的隐私性

- 只有唯一标识文件的 SHA 才会发送到云端的信誉服务。不会发送文件本身。
- 如果使用云端的文件分析服务，并且文件符合分析条件，则该文件本身将发送到云端。

- 有关每个发送到云端进行分析并且判定为“恶意”的文件的信息将添加到信誉数据库中。此信息与其他数据共同用于确定信誉分数。

  有关本地 Cisco Secure Endpoint 恶意软件分析设备所分析文件的信息不会与信誉服务共享。

配置文件信誉和分析功能

与文件信誉和分析服务通信的要求

- 所有使用这些服务的邮件安全设备都必须能通过互联网直接与其连接（不包括配置为使用本地的 Cisco Secure Endpoint 恶意软件分析设备的文件分析服务）。
- 默认情况下，与文件信誉和分析服务的通信 。
- 默认情况下，通过与默认网关相关联的接口来路由与文件信誉分析服务和基于云的分析服务的通信。要通过其他接口路由此流量，请在“安全服务”(Security Services) >“文件信誉和分析”(File Reputation and Analysis) 页面的“高级”(Advanced) 部分中为每个地址创建静态路由。
- 必须打开以下防火墙端口：

防火墙端口	说明	协议	输入/输出	主机名	设备接口
32137（默认）或 443	访问云服务获取文件信誉。	TCP	输出	如在“安全服务”(Security Services) > “防恶意软件和信誉”(Anti-Malware and Reputation)，“高级”(Advanced) 部分的云服务器池参数中所配置的一样。	管理，除非将静态路由配置为通过数据端口路由该流量。
443	访问云服务以进行文件分析。	TCP	输出	如在“安全服务”(Security Services) > “防恶意软件和信誉”(Anti-Malware and Reputation)，“高级”(Advanced) 部分中所配置的一样。	

配置本地文件信誉服务器

如果您将思科 AMP 虚拟私有云设备用作私有云文件分析服务器：

- 您可以从以下位置获得思科 思科高级恶意软件保护 虚拟私有云设备文档，包括安装和配置 FireAMP 私有云指南：
  http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html

  使用此文档执行本主题中介绍的任务。

  其他文件可从 AMP 虚拟私有云设备的“帮助”链接获取。
- 在“代理”或“空隙”（本地部署）模式中设置和配置思科 AMP 虚拟私有云设备。
- 确保思科 AMP 虚拟私有云设备软件版本为 2.2，该版本可与思科邮件安全设备集成。
- 在该设备上下载 AMP 虚拟私有云证书和密钥，以便上传到此邮件安全设备
- 当邮件安全设备信任的根颁发机构未对隧道代理服务器证书签名时，请使用**根证书**选项跳过标准验证。

注释 设置现场文件信誉服务器之后，您将从此邮件安全设备配置与该服务器的连接；请参阅启用和配置文件信誉和分析服务 ，第 7 页的步骤 6

配置本地文件分析服务器

如果您将 Cisco Secure Endpoint 恶意软件分析设备用作私有云文件分析服务器：

- 获取《 Cisco Secure Endpoint 恶意软件分析设备设置和配置指南》和《 Cisco Secure Endpoint 恶意软件分析设备管理指南》。Cisco Secure Endpoint 恶意软件分析设备文档可从

https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html 获取。

使用此文档可执行本主题中描述的任务。

使用 Cisco Secure Endpoint 恶意软件分析设备中的“帮助”链接可获取其他文档。

在《管理指南》中，搜索下列内容的相关信息：与其他思科设备的集成、CSA、Cisco Sandbox API、ESA 和邮件安全设备、 。

- 设置和配置 Cisco Secure Endpoint 恶意软件分析设备。
- 如果需要，请将 Cisco Secure Endpoint 恶意软件分析设备软件更新为版本 1.2.1，该版本支持与思科 邮件安全设备的集成。

  有关确定版本号和执行更新的说明，请参阅 AMP 恶意软件分析文件。
- 请确保您的设备可通过网络彼此通信。思科 邮件安全设备 必须能够连接到 Cisco Secure Endpoint 恶意软件分析设备的正常接口。
- 如果您要部署自签名证书：从 Cisco Secure Endpoint 恶意软件分析设备生成要在您的 邮件安全设备 上使用的自签名 SSL 证书。请参阅 Cisco Secure Endpoint 恶意软件分析设备管理员指南中有关下载 SSL 证书和密钥的说明。请务必生成一个将 Cisco Secure Endpoint 恶意软件分析设备主机名作为 CN 的证书。来自 Cisco Secure Endpoint 恶意软件分析设备的默认证书不起作用。
- 当您提交用于文件分析的配置时，系统将自动向恶意软件分析设备注册您的邮件安全设备，如启用和配置文件信誉和分析服务 中所述。但是，您必须按照同一程序中所述激活注册。

启用和配置文件信誉和分析服务

Before you begin

- 获取文件信誉服务和文件分析服务的功能密钥，并将其传输到此设备。
- 满足与文件信誉和分析服务通信的要求 , on page 5。
- 验证与配置升级和服务更新设置中“更新”(Updates) 页面上。
- 如果您将思科 AMP 虚拟私有云设备用作私有云文件信誉服务器，请参阅 配置本地文件信誉服务器, on page 6。
- 如果您将 Cisco Secure Endpoint 恶意软件分析设备用作私有云文件分析服务器，请参阅 配置本地文件分析服务器 , on page 6。

Procedure

步骤 1 选择**安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 点击**启用文件信誉过滤 (Enable File Reputation Filtering)**和可选的**启用文件分析 (Enable File Analysis)**。

- 如果选中**启用文件信誉过滤 (Enable File Reputation Filtering)**，则必须配置**文件信誉服务器 (File Reputation Server)** 部分（在**步骤 6** 中），方法如下：选择外部公共信誉云服务器的URL，或提供私有信誉云服务器连接信息。
- 同样，如果选中**启用文件分析 (Enable File Analysis)**，则必须配置**文件分析服务器 URL (File Analysis Server URL)** 部分（在**步骤 7** 中），方法如下：提供外部云服务器的 URL，或提供私有分析云连接信息。

Note 升级后可能添加新的文件类型，并且默认情况下不启用。如果已启用文件分析，并且需要在分析中包含新的文件类型，则必须启用这些文件类型。

步骤 4 接受许可协议（如果存在）。

步骤 5 在**文件分析 (File Analysis)** 部分中，从相应文件组中选择所需文件类型（例如“Microsoft 文档”）以发送进行文件分析。

有关支持的文件类型的信息，请参阅所介绍的文档。文件信誉和分析服务所支持的文件 , on page 3

Note 思科会定期检查潜在的恶意文件类型，以防止零日威胁。如果识别到新威胁，此类文件类型的详细信息将通过更新程序服务器发送到您的设备。选择**其他潜在恶意文件类型 (Other potentially malicious file types)** 选项以启用此功能。如果启用此功能，除了您已选择的文件类型，您的设备还会发送此类文件类型进行分析。

步骤 6 展开**文件信誉的高级设置 (Advanced Settings for File Reputation)** 面板，并根据需要调整下列选项：

选项	说明
云域 (Cloud Domain)	用于文件信誉查询的域的名称。
文件信誉服务器 (File Reputation Server)	选择公共信誉云服务器的主机名，或私有信誉云。 如果选择私有信誉云，请提供以下内容： • **服务器** - 思科 AMP 虚拟私有云设备的主机名或 IP 地址。 • **公钥 (Public Key)** - 为此设备与您的私有云设备之间的加密通信提供有效的公钥。此公钥必须与私有云服务器使用的密钥相同：找到此设备上的密钥文件，然后点击**上传文件 (Upload File)**。 **Note** 您必须已将此密钥文件从服务器下载到此设备。
面向终端的高级恶意软件防护 控制台集成	点击 **向面向终端的高级恶意软件防护** 注册设备，将您的设备与 面向终端的高级恶意软件防护 控制台集成。有关详细说明，请参阅将设备与 面向终端的高级恶意软件防护控制台集成, on page 11。

选项	说明
文件信誉的 SSL 通信 (SSL Communication for File Reputation)	选中**使用 SSL (端口 443）(Use SSL [Port 443])** 以在端口 443 而不是默认端口 32137 上进行通信。有关启用对服务器的 SSH 访问的信息，请参阅《思科 AMP 虚拟私有云设备用户指南》。 **Note** 通过端口 32137 的 SSL 通信可能需要您在防火墙中打开该端口。 通过此选项，您还可配置上游代理来与文件信誉服务进行通信。如果选中此选项，请提供相应的**服务器 (Server)**、**用户名 (Username)** 和**密码 (Passphrase)** 信息。 选中**使用 SSL (端口 443) (Use SSL (Port 443))** 时，如果隧道代理服务器的证书未由受信任的根颁发机构签名，还可以选中**放宽证书验证 (Relax Certificate Validation)** 以跳过标准证书验证。例如，如果在受信任的内部隧道代理服务器上使用自签名证书，则选择此选项。 **Note** 如果在“文件信誉的高级设置”的“文件信誉的SSL通信”部分选中 **使用 SSL (端口 443)**，则必须使用 CLI 命令 certconfig > CERTAUTHORITY > CUSTOM 或 Web 界面中的”网络“ >“证书”（自定义证书颁发机构）将内部部署信誉服务器 CA 证书上的 AMP 添加到此设备上的证书存储库。从服务器获得此证书（“配置”(Configuration) >“SSL”>“云服务器”(Cloud server) >“下载”(download)）。
心跳间隔 (Heartbeat Interval)	以分钟为单位的 ping 追溯事件频率。
查询超时 (Query Timeout)	信誉查询超时前经过的秒数。
处理超时 (Processing Timeout)	文件处理超时前经过的秒数。
文件信誉客户端 ID (File Reputation Client ID)	文件信誉服务器上此设备的客户端 ID（只读）。
文件追溯 (File Retrospective)	选中**抑制追溯性判定警报 (Suppress the retrospective verdict alerts)**，以面向未传送至邮件收件人、丢弃或隔离的邮件抑制追溯性判定警报。

Note 在无思科支持指导的情况下，请勿更改本部分中的任何其他设置。

步骤 7 如果要使用云服务进行文件分析，请展开“文件分析的高级设置”面板并根据需要调整以下选项：

选项	说明
文件分析服务器 URL (File Analysis Server URL)	选择外部云服务器的名称 (URL) 或**私有分析云 (Private analysis cloud)**。 如果指定外部云服务器，请选择与您的设备物理距离最近的服务器。系统将使用标准更新流程定期将新的可用服务器添加到该列表中。 选择私有分析云以使用内部部署的 Cisco Secure Endpoint 恶意软件分析设备进行文件分析，并提供以下内容： • **TG 服务器** - 输入独立或集群 Cisco Secure Endpoint 恶意软件分析设备的 IPv4 地址或主机名。您最多可以添加七个 Cisco Secure Endpoint 恶意软件分析设备。 **Note** 序列号表示您添加独立或集群 Cisco Secure Endpoint 恶意软件分析设备的顺序。而不是这些设备的优先级。 **Note** 不能在一个实例中同时添加独立服务器和集群服务器。它必须是独立服务器或集群服务器。 您只能在一个实例中添加一个独立服务器。如果是集群模式，则最多可以添加 7 个服务器，且所有服务器均必须属于同一个集群。不能添加多个集群。 • **证书颁发机构 (Certificate Authority)** - 选择**使用思科默认的证书颁发机构 (Use Cisco Default Certificate Authority)** 或**使用上传的证书颁发机构 (Use Uploaded Certificate Authority)**。 如果选择**使用上传的证书颁发机构 (Uploaded Certificate Authority)**，请点击**浏览 (Browse)** 来为此设备与私有云设备间的加密通信上传有效证书文件。此证书必须与私有云服务器使用的证书相同。 **Note** 如果您在设备上为文件分析配置了 Cisco Secure Endpoint 恶意软件分析网格门户，则可以访问 Cisco Secure Endpoint 恶意软件分析门户（例如https://panacea.threatgrid.eu），以查看和跟踪提交进行文件分析的文件。有关如何访问 Cisco Secure Endpoint 恶意软件分析门户的详细信息，请联系 Cisco TAC。
代理设置 (Proxy Settings)	选中**使用文件信誉代理 (Use File Reputation Proxy)** 复选框，以使用您已配置的同一个文件信誉隧道代理，作为文件分析的上游代理。 如果要配置不同的上游代理，请取消选中 **使用文件信誉代理 (Use File Reputation Proxy)** 复选框，然后输入合适的**服务器 (Server)**、**端口 (Port)**、**用户名 (Username)** 和**Passphrase (密码)** 信息。
文件分析客户端 ID (File Analysis Client ID)	文件分析服务器上此设备的客户端 ID（只读）。

步骤 8 （可选）如果要为文件信誉处置值配置缓存到期期限，请展开“缓存设置”(Cache Settings) 面板。

步骤 9 如果要设置可接受文件分析分数的上限，请展开“阈值设置”(Threshold Settings) 面板。高于此阈值的分数表示文件被感染。选择以下任一选项：

- 使用来自云服务的值 (95)
- 输入自定义值 - 默认值为 95

步骤 10 提交并确认更改。

步骤 11 如果您使用的是本地 Cisco Secure Endpoint 恶意软件分析设备，请在 Cisco Secure Endpoint 恶意软件分析设备上激活此设备的帐户。

激活“用户”账户的完整说明在 Cisco Secure Endpoint 恶意软件分析文档中提供。

a) 请记下页面部分底部显示的文件分析客户端 ID。此 ID 标识您将要激活的“用户”。
b) 登录 Cisco Secure Endpoint 恶意软件分析设备。
c) 选择 **欢迎... > 管理用户**，并浏览到“用户详细信息”。
d) 根据邮件安全设备的文件分析客户端 ID 找到“用户”帐户。
e) 为设备激活该“user”账户。

将设备与 面向终端的高级恶意软件防护控制台集成

您可以将您的设备与 面向终端的高级恶意软件防护控制台集成，并在 面向终端的高级恶意软件防护控制台中执行以下操作：

- 创建一个简单的自定义检测列表。
- 将新的恶意文件 SHA 添加到简单的自定义检测列表中。
- 创建应用允许列表。
- 将新文件 SHA 添加到应用允许列表。
- 创建自定义策略。
- 将简单的自定义检测列表和应用允许列表附加到自定义策略中。
- 创建自定义组。
- 将自定义策略附加到自定义组。
- 将已注册的设备从默认组移动到自定义组。
- 查看特定文件 SHA 的文件轨迹详细信息。

要将您的设备与 面向终端的高级恶意软件防护控制台集成，您需要使用控制台注册您的设备。

集成后，当文件 SHA 发送到文件信誉服务器时，从文件信誉服务器获得的文件 SHA 判决被 面向终端的高级恶意软件防护控制台中已用于同一文件 SHA 的判决覆盖。

如果文件 SHA 已标记为全局恶意，并且如果您将同一文件添加到 Cisco Secure Endpoint 控制台中的阻止列表中，则文件处置是恶意的。

思科高级恶意软件保护报告页中包括新按类别划分的**传入恶意软件文件 (Incoming Malware Files by Category) 部分**，以查看从 面向终端的高级恶意软件防护控制台收到的列入阻止列表的文件 SHA 比例，这些文件 SHA 显示为**自定义检测**。在报告的“传入恶意软件威胁文件”(Incoming Malware Threat Files) 部分中，被列入阻止列表的文件 SHA 的威胁名称显示为**简单自定义检测 (Simple Custom Detection)**。您可以点击报告的“更多详细信息”部分中的链接，以查看在 面向终端的高级恶意软件防护控制台中已列入阻止列表的文件 SHA 的文件轨迹详细信息。

开始之前

确保您在 面向终端的高级恶意软件防护控制台中拥有具有管理访问权限的用户账户。有关如何创建面向终端的高级恶意软件防护控制台用户账户的更多详细信息，请联系 Cisco TAC。

[对于集群配置]在集群配置中，只能向 面向终端的高级恶意软件防护控制台注册已登录的设备。如果您已在单机模式下向 面向终端的高级恶意软件防护控制台注册设备，请确保手动取消该设备的注册，然后您才能将其加入集群。

请确保已启用和配置文件信誉过滤。请参阅启用和配置文件信誉和分析服务，了解如何启用和配置文件信誉过滤。

过程

步骤 1 依次选择**安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)**。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 在 Web 界面的“文件信誉和文件分析”(File Reputation and File Analysis) 页面中文件信誉的“高级设置”(Advanced Settings) 面板中，点击**向** 面向终端的高级恶意软件防护 注册设备 。

点击向 面向终端的高级恶意软件防护注册设备后， 面向终端的高级恶意软件防护 控制台登录页面将显示。

步骤 4 使用用户凭证登录到 面向终端的高级恶意软件防护 控制台。

步骤 5 点击面向终端的高级恶意软件防护 (AMP for Endpoints) 授权页面中的**允许 (Allow)** 以注册您的设备。

下一步做什么

后续步骤：

- 您可以转至 面向端点的 AMP 控制台页面的“账户”>“应用程序”部分，以验证是否向 面向端点的 AMP 注册了您的设备。您的设备名称将显示在 面向终端的高级恶意软件防护 控制台页面的“应用程序”部分。
- 注册后，您的设备将被添加到默认组（审核组）中，该组被附加了默认策略（网络策略）。默认策略包含添加到阻止列表或允许列表的文件SHA。如果要自定义设备的面向终端的高级恶意软件防护 设置，并添加自己的阻止列表或允许列表文件SHA，请参阅 https://console.amp.cisco.com/docs中 面向终端的高级恶意软件防护 用户文档。

- 确保“文件信誉设置”(File Reputation Settings) 页面中的“文件信誉客户端 ID”(File Reputation Client ID) 值与 面向终端的高级恶意软件防护 控制台门户中注册设备的“设备 GUID”(Device GUID) 相同。如果值不同，则设备与面向终端的高级恶意软件防护 的集成将无法在计算机或集群级别正常工作。您需要注销并重新注册设备，才能使用面向终端的高级恶意软件防护 功能。
- 要从面向终端的高级恶意软件防护 (AMP for Endpoints) 控制台中注销设备连接，可以在设备的“文件信誉”(File Reputation) 部分的“高级设置”(Advanced Settings) 中点击**取消注册 (Deregister)**，或者您需要转到https://console.amp.cisco.com/中的 面向终端的高级恶意软件防护 (AMP for Endpoints) 控制台页面。有关更多信息，请参阅 https://console.amp.cisco.com/docs中的 面向终端的高级恶意软件防护 用户文档。

注释 将文件信誉服务器更改为其他数据中心时，您的设备将自动从面向终端的高级恶意软件防护注销。使用为文件信誉服务器选定的相同数据中心，使用面向终端的高级恶意软件防护控制台重新注册设备。

注释 如果您在集群级别更改了文件信誉服务器，则登录的设备将自动从面向终端的高级恶意软件防护控制台取消注册。确保取消注册集群中的所有其他计算机。使用为文件信誉服务器选定的相同数据中心，使用 面向终端的高级恶意软件防护 控制台重新注册设备。

注释 如果恶意文件 SHA 得到了一个安全的判决，请验证相同的文件 SHA 是否列入了 面向终端的高级恶意软件防护 控制台的允许列表中。

重要提示！文件分析设置所需的更改

如果计划使用新的公共云文件分析服务，请务必阅读以下说明以保持数据中心隔离：

- 新文件分析服务器中不保留现有的设备分组信息。您必须在新文件分析服务器上对设备重新分组。
- 隔离到文件分析隔离区的邮件将会被保留到保留期。隔离区保留期过后，邮件将从文件分析隔离区中删除，并由 AMP 引擎重新扫描。然后，将该文件上传到新的文件分析服务器以进行分析，但不会再次将该邮件发送到文件分析隔离区。

有关更多详细信息，请参阅https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html中的思科 AMP 恶意软件分析文档。

（仅公共云文件分析服务）配置设备组

对于发自组织内任意设备的待分析文件，为了允许组织内的所有内容安全设备可以在云中查看这些文件的文件分析结果详细信息，您需要将所有设备加入到同一设备组。可以在计算机或集群级别配置设备组。

准备工作：

- 确保集群中的所有计算机都正常工作。
- 确保您已连接到您所在区域的已配置文件分析服务器，并且该服务器正在运行。

Note 如果您在本地虚拟邮件网关中加载的许可证密钥文件不包含“云管理员功能”密钥，您仍然可以使用智能许可证账户 ID 执行威胁组文件分析的自动注册。

Procedure

步骤 1 选择**安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)**。

步骤 2 点击**点击此处分组或查看邮件网关文件分析报告 (Click here to group or view Email Gateway for File Analysis reporting)** 选项来创建设备分组。

步骤 3 [如果在邮件网关上禁用智能许可，则适用] 在**设备 ID /名称 (Appliance ID/Name)** 字段中手动输入组 ID，然后点击 **立即分组 (Group Now)**。

或

[如果在邮件网关上启用智能许可，则适用] 系统自动将智能账户 ID 注册为组 ID，并将其显示在 **设备组 ID /名称** 字段中。

说明：

- 一台设备只能属于一个组。
- 您可以随时将设备添加到组。
- 您可以在计算机和集群级别配置设备组。
- 如果这是要添加到组中的第一个设备，请为该组提供有用的标识符。此ID区分大小写并且不能包含空格。
- 提供的设备组ID在将要共享有关上传以供分析的文件的数据的所有设备上必须相同。但在后续组中设备上，不会验证该 ID。
- 如果更新设备组 ID，则更改会立即生效，并且不需要提交。
- 您必须为该组中的所有设备配置以在云中使用相同的文件分析服务器。
- 如果启用智能许可，则使用智能帐户 ID 对设备进行分组。

更新文件分析报告的设备组名称

Procedure

步骤 1 选择 **安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)**。

步骤 2 点击**点击此处分组或查看邮件网关文件分析报告 (Click here to group or view Email Gateway for File Analysis reporting)** 选项。

步骤 3 点击设备中的**更改分组 (Change Group)** 文件分析报告页面。

Note 您还可以在 CLI 中使用 *ampconfig> setgroup* 子命令更改组 ID。

步骤 4 在**设备组 ID /名称 (Appliance Group ID/Name)** 字段中输入名称或 ID，然后点击**立即分组 (Group Now)**。

Note 您必须单独更新特定组中所有设备的组名称。

哪些设备在分析组中？

Procedure

步骤 1 选择**安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)**。

步骤 2 点击**点击此处分组或查看邮件网关文件分析报告 (Click here to group or view Email Gateway for File Analysis reporting)** 选项。

步骤 3 点击**查看设备 (View Appliances)** 以查看在特定文件分析组中添加的设备。

查看文件分析分组的警报

下表包含为设备分组生成的用于文件分析的系统警报列表，包括对警报和警报严重性的说明。

组件/警报名称	邮件和描述	参数
AMP.ENGINE.ALERT.WARN	警报文本：未能向 Cisco Secure Malware Analytics (Threat Grid) 服务器注册文件分析组名称。如需帮助，请与 Cisco TAC 联系。 警报级别：WARNING。 说明：当邮件网关无法使用智能账户 ID 向 Cisco Secure Malware Analytics (Threat Grid) 服务器注册设备组名称时发送警报。	参数：失败原因

配置用于文件信誉扫描和文件分析的邮件策略

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)** 或**邮件策略 (Mail Policies) > 传出邮件策略 (Outgoing Mail Policies)**（如果适用）。

步骤 2 点击邮件策略的**高级恶意软件保护 (Advanced Malware Protection)** 列中的链接进行修改。

步骤 3 选择选项。

- 如果没有本地思科 Cisco Secure Malware Analytics (Threat Grid) 设备，并且不希望将文件发送至云（例如出于机密性原因），请取消选中**启用文件分析 (Enable File Analysis)**。
- 如果附件被视为“不可扫描”，则选择设备必须执行的操作。当设备因以下原因不可扫描文件时，附件被视为“不可扫描”：
  - **邮件错误**：
    - 受密码保护的存档或压缩文件
    - 存在 RFC 违规的邮件。
    - 包含 200 个以上子文件的邮件
    - 包含五个以上嵌套级别的子文件的邮件
    - 提取失败的邮件
  - **速率限制** - 文件分析服务器未扫描文件，因为设备已达到文件上传限制。
  - **AMP 服务不可用**：
    - 文件信誉服务不可用。
    - 文件分析服务不可用。
    - 文件信誉查询超时
    - 文件上传查询超时
- 您可以对 AMP 引擎未扫描的邮件配置下列任一邮件处理操作：
  - 删除邮件
  - 原样传送邮件
  - 将邮件发送到策略隔离区
- 如果选择传递邮件，请选择以下附加操作：
  - 是否将原始邮件存档。存档消息作为 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (amparchive) 日志订用。

- 是否通过修改消息主题警告最终用户，例如 [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]。
- 是否添加自定义报头，以向管理员提供精细控制。
- 是否修改邮件收件人，使邮件传送至其他地址。点击“是”，并输入新的收件人地址。
- 是否将不可扫描的邮件发送到备用目标主机。点击“是”(Yes)，并输入备用IP地址或主机名。

- 如果选择将邮件发送到策略隔离区，请选择以下附加操作：
  - 是否从下拉列表中选择策略隔离区。当标记为隔离时，邮件到达邮件管道的末尾时，将放置在隔离区中，并由邮件管道中的所有其他引擎进行扫描。
  - 是否将原始邮件存档。存档消息作为 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (`amparchive`) 日志订用。
  - 是否通过修改消息主题警告最终用户，例如 [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]。
  - 是否添加自定义报头，以向管理员提供精细控制。
- 如果附件被视为“恶意”(Malicious)，则选择 AsyncOS 必须执行的操作。以下选项
  - 是发送还是丢弃消息。
  - 是否将原始邮件存档。存档消息作为 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (amparchive) 日志订用。
  - 删除恶意软件附件后是否发送消息。
  - 是否通过修改邮件主题来警告最终用户，例如，[警告：在附件中检测到恶意软件]。
  - 是否添加自定义报头，以向管理员提供精细控制。
  - 是否修改邮件收件人，使邮件传送至其他地址。点击**是 (Yes)**，并输入新的收件人地址。
  - 是否将恶意邮件发送到备用目标主机。点击**是 (Yes)**，并输入备用 IP 地址或主机名。
- 选择附件被发送进行文件分析时 AsyncOS 必须执行的操作。以下选项
  - 传送还是隔离邮件。
  - 是否将原始邮件存档。存档消息作为 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (amparchive) 日志订用。
  - 是否通过修改邮件主题来警告最终用户，例如，“[警告：附件可能包含恶意软件]”。
  - 是否添加自定义报头，以向管理员提供精细控制。
  - 是否修改邮件收件人，使邮件传送至其他地址。点击**是 (Yes)**，并输入新的收件人地址。

- 是否将发送进行文件分析的邮件发送到备用目标主机。点击**是 (Yes)**，并输入备用 IP 地址或主机名。

- （仅用于传入邮件策略）配置当威胁判决更改为恶意时，对发送给最终用户的邮件将执行的补救操作。选择“启用邮箱自动补救”(Enable Mailbox Auto Remediation)并选择下列操作之一：
  - 转发到某个邮件地址。选择此选项可将包含恶意附件的邮件转发给指定用户，例如邮件管理员。
  - 删除邮件。选择此选项可从最终用户的邮箱中永久删除包含恶意附件的邮件。
  - 转发到邮件地址并删除该邮件。选择此选项可将包含恶意附件的邮件转发给指定用户（例如邮件管理员），并从最终用户的邮箱中永久删除该邮件。

  Note 由于 Office 365 服务不支持删除这些文件夹中的邮件，因此无法删除来自某些文件夹（例如，已删除邮件）的邮件。

  Important 在配置“邮箱自动补救”设置之前，请查看 补救邮箱中的邮件

步骤 4 提交并确认更改。

隔离附件送交分析的邮件

您可以将设备配置为隔离送交分析的文件，而不是立即将它们释放至工作队列。从隔离区释放后，重新扫描隔离的邮件及其附件。如果在文件分析结果可用于信誉扫描程序后释放邮件，将在重新扫描过程中捕获任何已识别的威胁。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)** 或**邮件策略 (Mail Policies) > 传出邮件策略 (Outgoing Mail Policies)**（如果适用）。

步骤 2 点击邮件策略的**高级恶意软件保护 (Advanced Malware Protection)** 列中的链接进行修改。

步骤 3 在“文件分析待定的邮件”(Messsages with File Analysis Pending) 部分下面，从“应用于邮件的操作”(Action Applied to Message) 下拉列表中选择**隔离**。

隔离的邮件存储在文件分析隔离区中。请参阅使用文件分析隔离区, on page 19。

步骤 4 （可选）在“文件分析待处理的邮件”(Messages with File Analysis Pending) 部分下，选择以下选项：

- 是否将原始邮件存档。存档消息作为 mbox 格式日志文件存储在设备上的 amparchive 目录中。需要预配置的 AMP 存档 (amparchive) 日志订用。
- 是否通过修改邮件主题来警告最终用户，例如，“[警告：附件可能包含恶意软件]”。
- 在从设备传送最终邮件时，是否丢弃文件分析判定为待处理的附件。默认选项为“否”(No)

- 是否添加自定义报头，以向管理员提供精细控制。

Note 仅当从隔离区释放邮件而非将该邮件发送到隔离区时，步骤 4 中提到的上述操作才会适用：

- 存档原始邮件。
- 修改邮件主题。
- 添加自定义信头。

步骤 5 提交并确认更改。

What to do next

相关主题

使用文件分析隔离区, on page 19

使用文件分析隔离区

编辑文件分析隔离区设置

Procedure

步骤 1 选择**监控 (Monitoring) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 2 点击**文件分析 (File Analysis)** 隔离区链接。

步骤 3 指定保留期。

不建议更改为有别于默认值（1 小时）的值。

步骤 4 请指定保留期经过后 AsyncOS 必须采取的默认操作。

步骤 5 如果您不希望在指定的保留期结束之前处理此隔离区中的邮件，即使隔离区磁盘空间已满也如此，请取消选择**通过在空间溢出后对邮件应用默认操作来释放空间 (Free up space by applying default action on messages upon space overflow)**。

步骤 6 如果选择**释放**作为默认操作，则可以根据情况指定要应用于在保留期之前释放的邮件的其他操作：

选项	信息
修改主题 (Modify Subject)	键入文本，以添加和指定是否将其添加到原始邮件主题的开头或结尾。 例如，您可能希望警告收件人邮件可能包含恶意附件。 **Note** 要正常显示使用非 ASCII 字符的主题，必须根据 RFC 2047 进行表示。
添加 X 报头 (Add X-Header)	X 报头可提供对邮件采取的操作的记录。这可能会非常有用，例如在处理有关传送特定邮件的原因的查询时。 输入名称和值。 示例： 名称 = Inappropriate-release-early 值 = True
拆离附件 (Strip Attachments)	删除附件可防御邮件中包含的恶意软件附件。

步骤 7 指定可以访问此隔离区的用户：

用户	信息
本地用户 (Local Users)	本地用户列表仅包含具有可以访问隔离区的角色的用户。 该列表不包括具有管理员权限的用户，因为所有管理员都对隔离区具有完全访问权限。
以外部方式进行身份验证的用户 (Externally Authenticated Users)	您必须已配置外部身份验证。
自定义用户角色 (Custom User Roles)	仅当您已创建至少一个具有隔离区访问权限的自定义用户角色时，才会看到此选项。

步骤 8 提交并确认更改。

手动处理文件分析隔离区中的邮件

Procedure

步骤 1 选择**监控 (Monitoring) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 2 在文件分析隔离区的对应行中，点击表的“邮件” (Messages) 列中的蓝色数字。

步骤 3 根据要求，对邮件执行以下操作：

- 删除
- 释放
- 延迟从隔离区计划退出
- 将邮件副本发送到您指定的邮件地址

集中文件分析隔离区

有关集中文件分析隔离的信息, 请参阅 Cisco 电子邮件安全装置指南 中的 "集中策略、病毒和爆发隔离" 一章。

文件信誉和分析 X 报头

可以使用 X 报头标记具有消息处理步骤操作和结果的消息。可以在邮件策略中利用 X 报头对消息进行标记，然后使用内容过滤器选择这些消息的处理选项和最终操作。

值区分大小写。

信头名称	可能的值（区分大小写）	说明
X-Amp-Result	正常 恶意 (Malicious) 不可扫描 (Unscannable)	判定适用于文件信誉服务所处理的消息。
X-Amp-Original-Verdict	文件未知 判定未知	基于信誉阈值的调整前判定。仅当原始判定是其中一个可能的值时，此报头才存在。
X-Amp-File-Uploaded	true false	如果将附加至消息的任何文件送交分析，则该报头为“真”(true)。

向最终用户发送有关已丢弃消息或附件的通知

当基于文件信誉扫描丢弃可疑附件或其父消息时，要向最终用户发送通知，则使用 X 报头或自定义报头和内容过滤器。

高级恶意软件防护和集群

如果使用集中管理，则可以启用集群、组和计算机级别的高级恶意软件防护和邮件策略。

必须在计算机级别添加功能密钥。

不应在集群级别配置设备组。

确保您收到关于 思科高级恶意软件保护 问题的警报

确保设备配置为向您发送与 思科高级恶意软件保护 相关的警报。

当出现以下情况时，您将收到警报：

警报说明	类型	严重性
您正在建立与现场（私有云） Cisco Secure Endpoint 恶意软件分析设备的连接，并且需要激活帐户，如 启用和配置文件信誉和分析服务 中所述。	防恶意软件	警告
功能密钥过期	（作为所有功能的标准）	
不可访问文件信誉或文件分析服务。	防病毒和 AMP	警告
与云服务建立通信。	防病毒和 AMP	信息
信誉和分析引擎由监视程序服务重新启动	防病毒和 AMP	信息
文件信誉判定更改。	防病毒和 AMP	信息
可送交分析的文件类型已更改。可能希望启用上传新类型文件。	防病毒和 AMP	信息
暂时无法分析某些文件类型。	防病毒和 AMP	警告
临时性中断后恢复分析所有受支持文件类型。	防病毒和 AMP	信息
文件分析服务密钥无效。您需要联系思科 TAC 并提供文件分析 ID 详细信息，以修复该错误。	AMP	错误

相关主题

- 有关无法连接至文件信誉或文件分析服务器的若干警报 , on page 26
- 在文件威胁判定更改时采取操作 , on page 25

思科高级恶意软件保护 功能的配置集中报告

如果您将在安全管理设备上集中报告，请参阅管理设备的联机帮助或用户指南的邮件报告主题中 思科高级恶意软件保护 部分中的重要配置要求。

文件信誉和文件分析报告与跟踪

- 通过 SHA-256 散列标识文件 , on page 23

- 文件信誉和文件分析报告页面, on page 23
- 查看其他报告中的文件信誉过滤数据 , on page 24
- 关于 消息 跟踪和 思科高级恶意软件保护 功能 , on page 24

通过 SHA-256 散列标识文件

由于文件名很容易更改，因此设备会使用安全散列算法 (SHA-256) 为每个文件生成标识符。如果设备处理具有不同名称的同一文件，所有实例被识别为相同的 SHA-256。如果多个设备处理相同的文件，则该文件的所有实例都具有相同的 SHA-256 标识符。

在大多数报告中，文件按其 SHA-256 值列出（采用缩写格式

文件信誉和文件分析报告页面

报告	说明
思科高级恶意软件保护	显示由文件信誉服务识别的基于文件的威胁。 有关判定已更改的文件，请参阅 AMP 判定更新报告。这些判定不会反映在 思科高级恶意软件保护 报告中。 如果从某个已压缩或已存档的文件中提取的某个文件是恶意文件，则只有这个已压缩或已存档的文件的 SHA 值包括在 思科高级恶意软件保护 报告中。 **按类别划分的传入恶意软件文件** 部分显示了从面向终端的高级恶意软件防护控制台所接收、归类为 **自定义检测** 且已列入阻止列表的文件 SHA 百分比。 从面向终端的高级恶意软件防护控制台获取的阻止列表中的文件 SHA 威胁名称在报告的“传入恶意软件威胁文件”部分中显示为 **简单自定义检测** 。 您可以点击报告的“更多详细信息”部分中的链接，以查看在面向终端的高级恶意软件防护控制台中已列入阻止列表的文件 SHA 的文件轨迹详细信息。 您可以在报告的 AMP处理的传入文件部分查看**低风险**判定详细信息。

报告	说明
思科高级恶意软件保护 文件分析	显示送交分析的每个文件的时间和判定（或临时判定）。设备每 30 分钟检查一次分析结果。 要查看超过 1000 个文件分析结果，请将数据导出为 .csv 文件。 深入分析以查看详细的分析结果，包括每个文件的威胁特征。 您还可以搜索有关 SHA 的其他信息，或点击文件分析详细信息页面底部的链接以在分析了文件的服务器上查看其他详细信息。 **注释** 如果发送从某个压缩或存档文件中提取的文件以供分析，则文件分析报告中仅包含已提取的这些文件的 SHA 值。
思科高级恶意软件保护 信誉	由于 思科高级恶意软件保护 重点关注有针对性的威胁和零日威胁，因此威胁判定可以随着汇聚数据提供更多信息而发生变化。 AMP 信誉报告会列出此设备处理的其裁定自收到邮件以来已发生更改的文件。有关此情况的详细信息，请参阅文件威胁判定更新 ，第 1 页。 要查看超过 1000 个裁定更新，请将数据导出为 .csv 文件。 如果单个 SHA-256 的判定多次发生变化，此报告仅显示最新的判定，而不显示判定历史记录。 要查看特定 SHA - 256 在最大可用时间范围内的所有受影响的邮件（无论为报告选择的时间范围如何），请点击 SHA-256 链接。

查看其他报告中的文件信誉过滤数据

用于文件信誉和分析的数据会在其他相关的报告中提供。被思科高级恶意软件保护阻止检测列在适用报告中可能被隐藏。要显示其他列，请点击表格下方的“列“(Columns) 链接。

关于 消息 跟踪和 思科高级恶意软件保护 功能

在“邮件跟踪”(Web Message Tracking) 中搜索文件威胁信息时，请注意以下几点：

- 要搜索文件信誉服务找到的恶意文件，请在**积极的高级恶意软件保护 (Advanced Malware Protection Positive)**。
- “邮件跟踪”(Web Message Tracking) 仅包括处理事务邮件时返回的文件信誉处理和原始文件信誉判定的相关信息。例如，如果最初发现文件是干净的，然后判定更新发现文件是恶意的，则在跟踪结果中仅显示干净判定。

  在“邮件跟踪”(Message Tracking) 详细信息的“处理详细信息”(Processing Details) 部分显示：

  - 邮件中每个附件的 SHA-256；

- 邮件的整体最终 思科高级恶意软件保护 判定，以及
- 发现包含恶意软件的任何附件。

- 判定更新仅在 AMP 判定更新报告中可用。“邮件跟踪”(Web Message Tracking) 中的原始邮件详细信息不会随着判定变化而更新。要查看涉及特定文件邮件（具有特定附件）的事务，请点击判定更新报告中的 SHA-256。
- 有关文件分析的信息（包括分析结果以及是否发送文件进行分析）仅在文件分析报告中可用。

  有关所分析的文件的其他信息，可从云端或现场文件分析服务器获取。要查看文件的任何可用文件分析信息，请依次选择**报告 (Reporting) 监控 (Monitor) > 文件分析 (File Analysis)**，然后输入 SHA-256 搜索文件或。如果文件分析服务已分析任何源中的文件，则可以查看详细信息。系统仅会为已分析的文件的结果。

  如果设备处理了送交分析的某个文件的后续实例，这些实例将显示在“邮件跟踪”(Web Message Tracking) 搜索结果中。

在文件威胁判定更改时采取操作

Procedure

步骤 1 查看 AMP 判定更新报告。

步骤 2 点击相关的 SHA-256 链接查看所有事务的 Web 消息跟踪数据，这些事务涉及包含最终用户的文件。

步骤 3 使用跟踪数据标识可能已危及用户、违规中所涉及的文件名等信息以及文件发件人。

步骤 4 检查“文件分析”(File Analysis) 报告查看是否将该 SHA-256 送交分析，以更详细地了解文件威胁行为。

What to do next

相关主题

文件威胁判定更新 , on page 1

故障排除文件信誉和分析

日志文件

在日志中：

- `AMP` 和 `amp` 是指文件信誉服务或引擎。
- `Retrospective` 是指判定更新。
- `VRT` 和 `sandboxing` 是指文件分析服务。

有关思科高级恶意软件保护（包括文件分析）的信息会记录在或 AMP 引擎日志。

文件信誉过滤和分析事件记录在 AMP引擎日志和邮件日志中。

在日志消息“文件信誉查询收到的响应”中，“上传操作”的可能值为：

- 1：发送。在这种情况下，您必须发送文件进行文件分析。
- 2：不发送。在这种情况下，您不会发送文件进行文件分析。
- 3：仅发送元数据。在这种情况下，您只会发送元数据，而不会发送文件分析的整个文件。
- 0：无操作。在这种情况下，不需要进行任何其他操作。

对于邮件日志中的“Disposition”：

- 1: 未检测到恶意软件，或假定为正常（视为正常）
- 2：正常
- 3：恶意软件

Spyname 是威胁名称。

使用跟踪

跟踪不可用于文件信誉过滤和分析功能。相反，从贵组织外的账户发送测试邮件。

有关无法连接至文件信誉或文件分析服务器的若干警报

问题

您会收到有关在云中无法连接至文件信誉或分析服务的若干警报。（单个警报可能仅表示瞬态问题。）

解决方案

- 确保已满足与文件信誉和分析服务通信的要求 , on page 5中的要求。
- 检查可能阻止设备与云服务进行通信的网络问题。
- 增加查询超时值：

选择**安全服务 (Security Services)** > **文件信誉和分析 (File Reputation and Analysis)**。“查询超时”值出现在 “高级”设置区域中。

API 密钥错误（本地文件分析）

问题

您在尝试查看“文件分析”(File Analysis) 报告详细信息时收到 API 密钥警告，或者邮件安全设备 无法连接到 AMP 恶意软件分析服务器以上传要分析的文件。

解决方案

发生此错误的原因是您更改了 AMP 恶意软件分析服务器的主机名，并且正在使用来自 AMP 恶意软件分析服务器的自签证书，但在其他情况下也可能会发生此错误。解决问题：

- 从拥有新主机名的 AMP 恶意软件分析设备生成新证书。
- 将新证书上传到 邮件安全设备 。
- 重置 AMP 恶意软件分析设备上的 API 密钥。有关说明，请参阅 AMP 恶意分析设备的在线帮助。

相关主题

- 启用和配置文件信誉和分析服务

API 密钥错误（公共云文件分析）

问题

当试图查看或分组用于文件分析报告的设备时，或者当您的电子邮件网关无法连接至 Cisco Secure Malware Analytics (Threat Grid) 服务器以上传文件进行分析时，您会收到 API 密钥警报。

解决方案

如果无法访问 Cisco Secure Malware Analytics (Threat Grid) 服务器，可能会发生此错误。选中以下各项并尝试重新连接：

- 您已连接到您所在区域的正确 Cisco Secure Malware Analytics (Threat Grid) 服务器。
- Cisco Secure Malware Analytics (Threat Grid) 服务器当前正在运行。

相关主题

- （仅公共云文件分析服务）配置设备组 , on page 14

未按预期上传文件

问题

未按预期评估或分析文件。无警报或明显错误。

解决方案

请考虑以下方面：

- 该文件可能已由另一设备送交分析，因此已存在于文件分析服务器上，或存在于正在处理该文件的设备的缓存中。

有关可送交分析的文件类型警报

问题

您会收到有关可送交文件分析的文件类型严重性信息警报。

解决方案

受支持文件类型更改或检查设备以查看受支持的文件类型时，发送该警报。这可能会出现于：

- 您或其他管理员更改选作分析的文件类型时。
- 基于云服务可用性受支持文件类型暂时改变。在这种情况下，将尽快恢复设备上选定的文件类型支持。两个过程均是动态的，您无需进行任何操作。
- 设备重新启动，例如作为 AsyncOS 升级的一部分。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。