文件/恶意软件事件和网络文件轨迹

以下主题提供文件和恶意软件事件的概述、本地恶意软件分析、动态分析、捕获文件和网络文件轨迹。

关于文件/恶意软件事件和网络文件轨迹

文件策略会自动为匹配的流量生成文件和恶意软件事件，并记录捕获的文件信息。当文件策略生成文件或恶意软件事件或者捕获文件时，系统还会自动将关联连接的结尾记录到 Cisco Secure Firewall Management Center数据库。您可分析此数据以解决任何不利影响及阻止未来攻击的事件。

根据文件分析结果，您可以使用“分析”>“文件”菜单下提供的页面上的表格查看捕获的文件以及生成的恶意软件和文件事件。您可以仔细查阅文件的构成、处置情况、威胁评分和动态分析摘要报告（如果有这些信息），从而进一步了解恶意软件分析。

要使分析更具针对性，您可以使用恶意软件文件的网络文件轨迹（显示该文件如何遍历您的网络、如何在主机之间传输以及各种文件属性的图）来跟踪个别威胁随时间推移跨主机进行的传播，从而在最有用的方面集中开展爆发控制和防御工作。

如果您在文件规则中配置本地恶意软件分析或动态分析，则系统会对与规则匹配的文件进行预分类并生成文件处置情况报告。

如果您的组织已部署 *Cisco Secure Endpoint* 并将该部署与 Cisco Secure Firewall Management Center 进行了集成，您还可以导入扫描记录、恶意软件检测和隔离，以及该产品识别的危害表现 (IOC)。此数据与 Cisco Secure Firewall 收集的事件数据一起显示，以便更全面地了解网络上的恶意软件。

情景管理器、控制面板和报告功能也有助于更深入地了解检测、捕获和阻止的文件及恶意软件。您也可以使用事件触发关联策略违规或者通过邮件、SMTP 或系统日志向您发出警报。

注释 要配置系统以检测恶意软件并生成文件和恶意软件事件，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的 网络恶意软件保护和文件策略 。

文件和恶意软件事件

Cisco Secure Firewall Management Center可以记录各种类型的文件和恶意软件事件。可用于任何单个事件的信息可能会根据该事件的生成方式和原因而异：

- 文件事件表示文件，包括系统（恶意软件防护）检测到的恶意软件。文件事件不包含Cisco Secure Endpoint 相关字段。
- 恶意软件事件表示 恶意软件防护 或 Cisco Secure Endpoint 检测到的恶意软件；恶意软件事件还可以记录除来自 Cisco Secure Endpoint 部署的威胁以外的数据，例如扫描和隔离。
- 追溯性恶意软件事件表示恶意软件防护 检测到的其处置情况（文件是否为恶意软件）已更改的文件。

注释

- 由恶意软件防护 识别为恶意软件的文件同时生成文件事件和恶意软件事件。由 Cisco Secure Endpoint 生成的恶意软件事件没有对应的文件事件。
- 未识别为恶意软件的文件（安全和中性文件）会生成文件事件。无论文件下载了多少次，系统都会为每个文件创建一个文件事件。但是，会为正在下载的每个文件实例生成连接事件。
- 检查 NetBIOS-ssn (SMB) 流量所生成的文件事件不会立即生成连接事件，因为客户端和服务器构建一个持久连接。系统在客户端或服务器结束会话之后生成连接事件。
- 系统支持显示和输入使用 Unicode (UTF-8) 字符的文件名。但是，Unicode 文件名在 PDF 报告中以转译形式显示。此外，SMB 协议将文件名中不可打印的字符替换为英文句号。

文件和恶意软件事件类型

文件事件

系统将按照当前部署的文件策略记录当受管设备在网络流量中检测或阻止文件时生成的文件事件。

系统生成文件事件时，无论调用访问控制规则采用何种日志记录配置，系统都会将关联连接的结束事件记录到 Cisco Secure Firewall Management Center数据库中。

恶意软件事件

Firepower 系统（特别是恶意软件防护 功能）在网络流量中检测到恶意软件时会生成恶意软件事件，这是整个访问控制配置的一部分。恶意软件事件包含生成事件的处置情况，以及有关检测该恶意软件的方式、位置和时间的情景数据。

表 *1:* 恶意软件事件生成情景

当系统检测到文件并且...	处理结果
成功查询 AMP 云（执行恶意软件云查找）以了解文件的处置情况	恶意软件、干净或未知
查询 AMP 云，但无法建立连接或云因其他原因而不可用	不可用 您可能看到很少一部分事件为此处置；这是预期行为。
与文件关联的威胁评分超过检测到该文件的文件策略中定义的恶意软件威胁评分阈值，或者本地恶意软件分析识别恶意软件	恶意软件
它包含在自定义检测列表中（手动标记为恶意软件）	自定义检测
它包含在干净的列表中（手动标记为干净）	正常

恶意软件事件中的文件处置和文件操作

每个文件规则都有用于确定系统如何处理与规则条件匹配的流量的关联操作。如果选择 阻止恶意软件 或 恶意软件云查询 作为文件规则操作，系统将查询 AMP 云以确定通过网络传输的文件是否包含恶意软件，然后阻止存在威胁的文件。云查找允许您根据文件的 SHA-256 散列值获取并记录文件的处置情况。

下表介绍与 AMP 云返回的文件处置情况相关联的文件操作：

表 *2:* 恶意软件事件中的文件处置和文件操作

已选的文件规则操作	文件处置	恶意软件事件中的文件操作
• 阻止恶意软件 • 恶意软件云查找	恶意软件	阻止
	• 正常 • 未知 • 不可用 • 不适用	云查找 **注释** 在文件策略编辑器高级设置下，您可以为 **如果 AMP 云处置情况为未知，根据威胁评分覆盖处置情况** 选项设置阈值威胁评分。如果设置了阈值威胁评分，则 AMP 云判定为“未知”的文件如果其动态分析评分等于或低于阈值，则会被视为恶意软件。

追溯性恶意软件事件

对于在网络流量中检测到的恶意软件文件，处置情况可以更改。例如，AMP 云可以确定先前被视为干净的文件现在被识别为恶意软件，或者正好相反，以前被识别为恶意软件的文件实际上是干净的。当上周查询的文件的处置情况发生更改时，AMP 云会通知系统。然后将发生两件事情：

- Cisco Secure Firewall Management Center产生新追溯性恶意软件事件。

  新追溯性恶意软件事件代表上一周检测到的具备相同 SHA-256 哈希值的所有文件的性质发生变更。因此，这些事件包含限定信息：Cisco Secure Firewall Management Center接到性质变更通知的日期和时间、新性质、文件 SHA-256 哈希值以及威胁名称。它们不包含 IP 地址或其他上下文信息。

- Cisco Secure Firewall Management Center变更此前检测到的具有追溯事件相关 SHA-256 哈希值的文件的文件性质。

  如果文件性质变更为 Malware，Cisco Secure Firewall Management Center在其数据库内记录新恶意软件事件。除了新性质，新恶意软件事件信息与最初检测到文件时生成的文件事件中的信息都相同。

  如果文件的处置情况更改为“安全”，则 Cisco Secure Firewall Management Center不会删除恶意软件事件。相反，该事件反映处置情况更改。这表示文件性质为安全的文件能够出现在恶意软件表中，前提是它们最初被视为恶意软件。从未识别为恶意软件的文件只会出现在文件表中。

由面向终端的 AMP 生成的恶意软件事件

如果您的组织使用面向终端的 AMP，则个人用户可以在终端（计算机和移动设备）上安装轻量级连接器。连接器可在进行上传、下载、执行、打开、复制、移动等操作后检查文件。这些连接器与 AMP 云进行通信，以确定检查的文件是否包含恶意软件。

文件被确定为恶意软件后，AMP 云会向 Cisco Secure Firewall Management Center发送威胁识别。AMP 云还可以向 Cisco Secure Firewall Management Center发送其他类型的信息，包括有关扫描、隔离、受阻执行和云召回的数据。Cisco Secure Firewall Management Center将这些信息记录为恶意软件事件。

注释 面向终端的 AMP 生成的恶意软件事件中所报告的 IP 地址可能不在网络映射中 - 甚至可能根本不在监控的网络中。根据部署、合规级别以及其他因素，您的组织中由面向终端的AMP监控的终端可能与恶意软件防护 监控的终端不是相同的主机。

使用 Cisco Secure Endpoint 的恶意软件事件分析

如果您的组织已部署 Cisco Cisco Secure Endpoint：

- 您可以将系统配置以在 防火墙管理中心 事件页面上显示由 Cisco Secure Endpoint 检测的恶意软件事件， 旁边显示 恶意软件防护检测到的事件。
- 如果您使用 AMP 公共云，可以在 Cisco Secure Endpoint中查看文件轨迹和有关特定 SHA 的其他信息。只需在事件页面上的表中右键点击文件的 SHA 散列值。

要配置上述功能，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 集成 *DeviceUUID (*仅限系统日志*)Cisco Secure Firewall* 和*Cisco Secure Endpoint*。

来自 Cisco Secure Endpoint 的事件数据

如果您的组织已部署 Cisco Secure Endpoint 以进行恶意软件防护，则您可以将系统配置为允许在 防火墙管理中心 中处理来自 Cisco Secure Endpoint的文件和恶意软件数据。

但是，您应了解来自 Cisco Secure Endpoint 的文件和恶意软件数据与来自系统的 恶意软件防护 功能的文件和恶意软件数据之间的差异。

由于Cisco Secure Endpoint 恶意软件检测是在下载或执行时于终端处执行，而受管设备在网络流量中检测恶意软件，因此两种类型的恶意软件事件中的信息不同。例如， Cisco Secure Endpoint 检测到的恶意软件事件（“基于终端的恶意软件”）包含有关文件路径、调用客户端应用等等的信息，而网络流量中的恶意软件检测则包含有关用于传输文件的连接的端口、应用协议和始发 IP 地址信息。

再例如，恶意软件防护 检测到的恶意软件事件（“基于网络的恶意软件事件”）中，用户信息向用户展示此用户最近登录的主机是恶意软件的攻击目标，并且恶意软件是由网络发现功能确定的。但是， Cisco Secure Endpoint-报告的用户是指当前登录其中检测到恶意软件的终端的用户。

注释 根据您的部署，由 Cisco Secure Endpoint 监控的终端可能不是与由 恶意软件防护监控的终端相同的主机。因此， Cisco Secure Endpoint 生成的恶意软件事件不将主机添加到网络映射。但是，系统会使用 IP 和 MAC 地址数据标记具有从 Cisco Secure Endpoint 部署获取的危害表现的受监控主机。如果不同恶意软件解决方案监控的两个不同主机具有相同的 IP 和 MAC 地址，则系统可能会错误地标记具有 Cisco Secure Endpoint IOC 的受监控主机。

下表汇总了 Firepower 使用 恶意软件防御 许可证时生成的事件数据与 Cisco Secure Endpoint生成的事件数据之间的差异。

表 *3: AMP* 产品之间的数据差异汇总

功能	恶意软件防护	Cisco Secure Endpoint
生成的事件	文件事件、捕获文件、恶意软件事件及追溯性恶意软件事件	恶意软件事件
恶意软件事件中的信息	基本的恶意软件事件信息，以及连接数据（IP 地址、端口和应用协议）	深入的恶意软件事件信息；无连接数据
网络文件轨迹	基于防火墙管理中心	防火墙管理中心 和 Cisco Secure Endpoint 管理控制台均具有网络文件轨迹。两者均很有用。

相关主题

在 《Cisco Secure Firewall Management Center 设备配置指南》中集成 *Firepower* 和 *Cisco Secure Endpoint*

使用文件和恶意软件事件工作流程

通过此过程可查看表中的文件和恶意软件事件，并根据与分析相关的信息操作事件视图。在访问事件时看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以从广泛视图移动到更加突出重点的视图，使用这些页面评估事件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

您必须是管理员或安全分析师用户才能执行此任务。

过程

选择以下其中一个选项：

- **分析** > **文件 (File Events Analysis Files** > **)**
- **分析** > **文件** > **恶意软件事件**

提示
事件表视图中的一些字段在默认情况下处于隐藏状态。要显示事件视图的隐藏字段，请展开搜索限制，然后点击 **Disabled Columns** 下的字段名称。

提示
要快速查看检测到特定文件的连接，请使用表中的复选框选择文件，然后从**跳转至**下拉列表中选择**连接事件**。

提示
右键点击表中的项目以查看选项。（并非每个列都提供选项。）

相关主题

文件和恶意软件事件字段，第 7 页
预定义文件工作流程
预定义恶意软件工作流程
配置事件视图设置

文件和恶意软件事件字段

文件和恶意软件事件（您可以通过工作流程查看和搜索文件和恶意软件事件）包含此部分中列出的字段。请记住，可用于任何单个事件的信息可能会根据该事件的生成方式和原因而异。

注释 由恶意软件防护识别为恶意软件的文件同时生成文件事件和恶意软件事件。由 Cisco Secure Endpoint 生成的恶意软件事件没有对应的文件事件，并且文件事件没有与 Cisco Secure Endpoint相关的字段。

系统日志消息使用初始值填充并且不会更新。即使防火墙管理中心 Web 接口中的等效字段使用追溯性判定等进行了更新，系统日志消息也不会更新。

操作（系统日志： **FileAction**）

检测文件的文件策略规则的相关操作以及任何相关文件规则操作选项。

AMP 云

产生面向终端的 AMP 事件的 AMP 云名称。

应用文件名

检测面向终端的 AMP 期间访问恶意软件文件的客户端应用。这些应用与网络发现或应用控制无关联。

应用文件 **SHA256**

检测面向终端的 AMP 期间访问被检测或隔离文件的父文件的 SHA-256 散列值。

在统一事件查看器中，此字段显示为 **应用文件 SHA-256**。

应用协议（系统日志：**ApplicationProtocol**）

受管设备检测到文件的流量所用应用协议。

应用协议类别或标记

展示应用特征的条件，协助您了解应用功能。

应用风险

与连接中检测到的应用流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。

存档深度（系统日志： **ArchiveDepth**）

文件嵌入存档文件的层级（如有）。

存档名称（系统日志： **ArchiveFileName**）

包含恶意软件文件的存档文件名称（如有）。

要查看存档文件的内容，请在**分析 (Analysis) > 文件 (Files)**下打开列出该存档文件的任意表，右键点击该存档文件的表行来打开情景菜单，然后点击**查看存档内容 (View Archive Contents)**。

存档 **SHA256**（系统日志： **ArchiveSHA256**）

包含恶意软件文件的存档文件的 SHA-256 散列值（如有）。

要查看存档文件的内容，请在“分析”(Analysis)>“文件”(Files)下打开列出该存档文件的任意表，右键点击该文档文件的表行来打开情景菜单，然后点击**查看存档内容 (View Archive Contents)**。

ArchiveFileStatus（仅限系统日志）

正在被检测的存档的状态。可能会有以下值：

- 待处理 - 正在检测存档
- 已提取 - 已成功检测，且无任何问题
- 失败 - 检测失败，系统资源不足
- 超出深度 - 检测成功，但存档超出嵌套检测深度
- 已加密 - 部分检测成功，存档已加密或包含加密存档
- 不可检测 - 部分检测成功，文件可能格式有误或损坏

业务相关性

与连接中检测到的应用流量关联的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。

类别/文件类型类别

一般类别文件类型，例如：Office 文档、存档、多媒体、可执行文件、PDF 文件、编码文件、图形或系统文件。

客户端（系统日志：**Client**）

在一台主机上运行并依靠服务器发送文件的客户端应用。

客户端类别或标记

展示应用特征的条件，协助您了解应用功能。

连接计数器 （仅限系统日志）

区分一个连接与另一个同时连接的计数器。此字段本身没有意义。

以下字段共同唯一地标识与特定文件或恶意软件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

连接实例 ID （仅限系统日志）

处理连接事件的 Snort 实例。此字段本身没有意义。

以下字段共同唯一地标识与特定文件或恶意软件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

计数

应用创建两个或多个相同行的限制条件后，与每行中的信息匹配的事件数。

检测名称

被测恶意软件名称。

检测器

识别恶意软件的面向终端的 AMP 检测器，例如 ClamAV、Spero 或 SHA。

设备

对于文件事件和 防火墙 设备生成的恶意软件事件，显示检测到文件的设备的名称。

对于面向终端的 AMP 生成的恶意软件事件和 AMP 云生成的追溯性恶意软件事件，显示 防火墙管理中心的名称。

DeviceUUID （仅限系统日志）

生成事件的 防火墙 设备的唯一标识符。

以下字段共同唯一地标识与特定文件或恶意软件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

处置情况/文件处置情况（系统日志： SHA_Disposition）

文件的处置情况：

恶意软件

表示 AMP 云将文件归类为恶意软件，本地恶意软件分析识别的恶意软件或文件威胁评分超过文件策略中定义的恶意软件阈值。

干净

表示AMP云将文件分类为干净，或用户将文件添加到干净列表。干净的文件仅在变更为干净后才会显示在恶意软件表中。

未知

表示系统已查询 AMP 云，但文件尚未被分配处置情况；换句话说，AMP 云尚未对文件进行分类。

自定义检测

表示用户将文件添加到自定义检测列表。

不可用

表示系统无法查询 AMP 云。您可能看到很少一部分事件为此处置；这是预期行为。

不适用

表示“检测文件”或“阻止文件”规则已处理文件，Cisco Secure Firewall Management Center未查询 AMP 云。

只有系统为之查询 AMP 云的文件才会显示文件处置情况。

系统日志字段仅反映初始处置情况；它们不会进行更新以反映追溯裁定。

域

对于文件事件和 防火墙 设备生成的恶意软件事件，显示检测到文件的设备的域。对于面向终端的 AMP 生成的恶意软件事件和 AMP 云生成的追溯性恶意软件事件，显示与报告事件的 AMP 云连接关联的域。

仅当曾经配置 防火墙管理中心以实现多租户时，此字段才存在。

DstIP（仅限系统日志）

对连接作出响应的主机的IP地址。这可能是文件发送方或接收方的IP地址，具体取决于FileDirection字段中的值：

如果 FileDirection 字段中的值为 **Upload**，则为文件接收方的 IP 地址。

如果 FileDirection 字段中的值为 **Download**，则为文件发送方的 IP 地址。

另请参阅 **SrcIP**。

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明。

DstPort（仅限系统日志）

DstIP 所述在连接中使用的端口。

出口虚拟路由器

在使用虚拟路由的网络中，用于流量离开网络的虚拟路由器的名称。

事件子类型

导致恶意软件检测的面向终端的 AMP 操作，例如，“创建”(Create)、“执行”(Execute)、“移动”(Move) 或“扫描”(Scan)。

事件类型

恶意软件事件的子类型。

文件名（系统日志： **FileName**）

文件名称。

文件路径

面向终端的 AMP 检测到的恶意软件文件的文件路径，不包括文件名。

文件策略（系统日志： **FilePolicy**）

检测文件的文件策略。

文件存储/已存储（系统日志： **FileStorageStatus**）

与事件关联的文件的存储状态：

已存储

返回当前存储相关文件的所有事件。

已在连接中存储 (Stored in connection)

返回系统捕获并存储相关文件的所有事件，无论当前是否已存储相关文件。

失败

返回系统无法存储相关文件的所有事件。

系统日志字段仅包含初始状态；它们不会进行更新以反映更改的状态。

文件时间戳

面向终端的 AMP 检测到恶意软件文件创建的时间和日期。

FileDirection（仅限系统日志）

文件在连接期间是否进行过下载或上传。可能的值包括：

- 下载 - 文件由 DstIP 传输至 SrcIP。
- 上传 - 文件由 SrcIP 传输至 DstIP。

FileSandboxStatus（仅限系统日志）

表示是否已发送文件以进行动态分析，若已发送则表示状态。

第一个数据包时间 （仅限系统日志）

系统遇到第一个数据包的时间。

以下字段共同唯一地标识与特定文件或恶意软件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

FirstPacketSecond（仅限系统日志）

文件下载或上传流程开始的时间。

消息报头时间戳中捕获有事件发生的时间。

HTTP 响应代码

传输文件时，系统响应客户端的 HTTP 请求发送的 HTTP 状态代码。

入口虚拟路由器

在使用虚拟路由的网络中，用于流量进入网络的虚拟路由器的名称。

IOC

对于连接涉及的主机，恶意软件事件是否触发危害表现 (IOC)。当面向终端的 AMP 数据触发 IOC 规则时，将生成 AMP IOC 类型的完整恶意软件事件。

消息

恶意软件事件相关的其他信息。对于文件事件和防火墙 设备生成的恶意软件事件，系统仅对处置情况发生变更的文件（即具有关联追溯性事件的文件）填充此字段。

MITRE

您可以点击以显示 MITRE 战术和层次结构中的技术的完整列表的模式计数。

协议（仅限系统日志）

用于连接的协议，例如 TCP 或 UDP。

接收大洲

接收文件的主机所在大洲。

接收国家/地区

接收文件的主机所在国家/地区。

接收 IP

在 防火墙管理中心 Web 界面，对于文件事件和 防火墙 设备生成的恶意软件事件，显示接收文件的主机的 IP 地址。另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明。

对于面向终端的 AMP 生成的恶意软件事件，显示连接器报告事件的终端的 IP 地址。

有关系统日志等效项（仅 防火墙 设备生成的事件），请参阅 **DstIP** 和 **SrcIP**。

接收端口

在 防火墙管理中心 web 接口，检测到文件的流量所用目标端口。

对于系统日志等效项，请参阅 **DstIP** 和 **SrcIP** 以及 **DstPort** 和 **SrcPort**。

发送大洲

发送文件的主机所在大洲。

发送国家/地区

发送文件的主机所在国家/地区。

发送 IP

在 防火墙管理中心 Web 接口，发送文件的主机的 IP 地址。另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明。

对于系统日志等效项，请参阅 **DstIP** 和 **SrcIP**。

发送端口

在 防火墙管理中心 web 接口，检测到文件的流量所用源端口。

对于系统日志等效项，请参阅 **DstIP** 和 **SrcIP** 以及 **DstPort** 和 **SrcPort**。

SHA256/文件 SHA256 （系统日志： FileSHA256）

文件的 SHA-256 散列值。

要具有 SHA256 值，文件必须已经过以下任一文件规则处理：

- 启用了**存储文件**的“检测文件”文件规则
- 启用了**存储文件**的“阻止文件”文件规则
- “恶意软件云查找”(Malware Cloud Lookup) 文件规则
- “阻止恶意软件”(Block Malware) 文件规则
- 面向终端的 AMP

此列还会显示代表最近检测到的文件事件和文件处置情况且链接到网络文件轨迹的网络文件轨迹图标。

大小 (KB)/文件大小 (KB) （系统日志： FileSize）

在 防火墙管理中心 Web 接口，文件大小（千字节）。

在系统日志消息中：文件大小（字节）。

请注意，如果系统在完全接收某个文件前确定了该文件的文件类型，则可能不会计算该文件的大小。在这种情况下，此字段为空。

SperoDisposition（仅限系统日志）

表示文件分析中是否使用了 SPERO 签名。可能的值：

- 已对文件执行 Spero 检测
- 未对文件执行 Spero 检测

SrcIP（仅限系统日志）

发起连接的主机的 IP 地址。这可能是文件发送方或接收方的 IP 地址，具体取决于 FileDirection 字段中的值：

如果 FileDirection 字段中的值为 **`Upload`**，此为文件发送方的 IP 地址。

如果 FileDirection 字段中的值为 **`Download`**，此为文件接收方的 IP 地址。

另请参阅 **DstIP**。

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明。

SrcPort（仅限系统日志）

SrcIP 所述在连接中使用的端口。

SSL 实际操作（系统日志：SSLActualAction）

系统应用于已加密流量的操作：

阻止或通过重置阻止

表示阻止的加密连接。

解密（重新签名）

表示使用重新签名的服务器证书解密的传出连接。

解密（替换密钥）

表示使用具有替代公钥的自签名服务器证书解密的传出连接。

解密（已知密钥）

表示使用已知私钥解密的传入连接。

默认操作

表示连接采用默认操作处理。

不解密

表示系统未解密的连接。

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 证书信息

用于加密流量的公钥证书上存储的信息，包括：

- 使用者/颁发者公用名称
- 使用者/颁发者组织
- 使用者/颁发者单位
- 无效时间
- 序列号、证书指纹
- 公钥指纹

有关系统日志，请参阅 **SSLCertificate**。

SSL 失败原因（系统日志： SSLFlowStatus）

系统无法解密已加密流量的原因：

- 未知
- 不匹配
- 成功
- 未缓存的会话
- 未知密码套件
- 不支持的密码套件
- 不支持的 SSL 版本
- 使用了 SSL 压缩
- 会话在被动模式下无法解密
- 握手错误
- 解密错误
- 挂起的服务器名称类别查找
- 挂起的公用名类别查找
- 内部错误 (Internal Error)
- 网络参数不可用
- 服务器证书处理无效
- 服务器证书指纹不可用

- 无法缓存使用者 DN
- 无法缓存颁发者 DN
- 未知的 SSL 版本
- 外部证书列表不可用
- 外部证书指纹不可用
- 内部证书列表无效
- 内部证书列表不可用
- 内部证书不可用
- 内部证书指纹不可用
- 服务器证书验证不可用
- 服务器证书验证失败
- 无效操作

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 状态

与记录加密连接的 **SSL 实际操作** （解密规则、默认操作或无法解密的流量操作）关联的操作。 **锁定图标** 指向 TLS/SSL 证书详细信息。如果证书不可用（例如，对于因 TLS/SSL 握手错误而受阻的连接），锁定图标会灰显。

如果系统无法解密已加密连接，则其会显示所采取的 **SSL 实际操作 (SSL Actual Action)**（无法解密的流量操作）以及 **SSL 失败原因 (SSL Failure Reason)**。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查即允许了该流量，则此字段显示 `Do Not Decrypt (Unknown Cipher Suite)`。

当搜索该字段时，请键入一个或多个 **SSL 实际操作 (SSL Actual Action)** 和 **SSL 失败原因 (SSL Failure Reason)** 值以查看系统处理或无法解密的已加密流量。

SSL 使用者/颁发者所在国家/地区

与加密证书关联的使用者或颁发者所在国家/地区的双字符 ISO 3166-1 alpha-2 国家/地区代码。

SSLCertificate（仅限系统日志）

TLS/SSL 服务器的证书指纹。

威胁名称（系统日志： ThreatName）

被测恶意软件名称。

威胁评分（系统日志： ThreatScore）

与此文件相关的最新威胁评分。此为 0 至 100 之间的数值，该数值基于动态分析期间观察到的潜在恶意行为。

威胁评分图标可连接到“动态分析摘要”(Dynamic Analysis Summary) 报告。

时间

事件生成的日期和时间。此字段不可搜索。

在系统日志消息中，请参阅 **FirstPacketSecond**。

类型/文件类型（系统日志： FileType）

文件类型，例如 HTML 或 MSEXE。

URI/文件 URI（系统日志： URI）

与文件事务关联的连接的 URI，例如，用户下载文件所使用的 URL。

用户（系统日志： User）

发起连接的主机的 IP 地址相关的用户名。如果此 IP 地址在您的网络外部，则关联的用户名通常是未知的。

如果适用，用户名前面会附加 <区域>\。

对于文件事件和 防火墙 设备生成的恶意软件事件，此字段显示由身份策略或授权登录确定的用户名。如果没有身份策略，则显示“无需身份验证”。

对于面向终端的 AMP 生成的恶意软件事件，用户名由面向终端的 AMP 确定。这些用户不受用户发现或控制束缚。他们不会出现在用户表中，您也无法查看这些用户详细信息。

Web 应用（系统日志：WebApplication）

代表连接内被检测 HTTP 流量内容或所请求 URL 的应用。

Web 应用类别或标记

展示了应用特征的条件，以帮助您了解应用功能。

恶意软件事件子类型

下表列出了恶意软件事件子类型、是面向网络的AMP生成的恶意软件事件（“基于网络的恶意软件事件”）还是面向终端的AMP生成的恶意软件事件（“基于终端的恶意软件事件”）可具有该子类型，以及系统是否使用该子类型来建立网络文件轨迹。

表 *4:* 恶意软件事件类型

恶意软件事件子类型/搜索值	恶意软件防护	面向终端的 **AMP**	文件轨迹
网络文件传送中检出威胁	是	否	是
网络文件传送（回溯）中检出威胁	是	否	是
检测出威胁	否	是	是
排除部分检出威胁	否	是	是
隔离威胁	否	是	是
AMP IOC（危害表现）	否	是	否
执行受阻	否	是	否
云召回隔离	否	是	否
云召回隔离尝试失败	否	是	否
开始云召回隔离	否	是	否
从隔离中恢复云召回	否	是	否
从隔离中恢复云召回失败	否	是	否
从隔离中恢复云召回启动	否	是	否
隔离失败	否	是	否
恢复隔离项目	否	是	否
恢复隔离失败	否	是	否
开始恢复隔离	否	是	否
扫描完成，未检出	否	是	否
扫描完成，检出	否	是	否
扫描失败	否	是	否
开始扫描	否	是	否

文件和恶意软件事件字段中的可用信息

下表列出系统是否显示每个文件和恶意软件事件字段的信息。

如果您的组织已部署 Cisco Secure Endpoint，您可以选择将该产品与 Cisco Secure Firewall 部署进行集成：

- 从 Cisco Secure Endpoint 部署导入的恶意软件事件和危害表现 (IOC) 不包含情景连接信息，但其确实包含在下载或执行时获取的信息，例如文件路径、调用客户端应用等等。
- 文件事件表视图不显示与 Cisco Secure Endpoint 相关的字段。

表 *5:* 文件和恶意软件事件字段中的可用信息

字段	文件事件	系统检测到的恶意软件事件	系统检测到的追溯性事件	以下项检测到的恶意软件事件：**Cisco Secure Endpoint**
操作	是	是	是	否
AMP 云	否	否	否	是
应用文件名	否	否	否	是
应用文件 SHA256	否	否	否	是
应用协议	是	是	否	否
应用协议类别或标记	是	是	是	否
应用风险	是	是	是	否
存档深度	是	是	否	是
存档名称	是	是	否	是
存档 SHA256	是	是	否	是
业务相关性	是	是	是	否
类别/文件类型类别	是	是	否	是
客户端	是	是	是	否
客户端类别或标记	是	是	是	否
计数	是	是	是	是
检测名称	否	是	否	否
检测器	否	否	否	是
设备	是	是	是	是
处置情况/文件处置情况	是	是	是	否
域	是	是	是	是

字段	文件事件	系统检测到的恶意软件事件	系统检测到的追溯性事件	以下项检测到的恶意软件事件：**Cisco Secure Endpoint**
事件子类型	否	否	否	是
事件类型	否	是	是	是
文件名	是	是	否	是
文件路径	否	否	否	是
文件策略	是	否	否	否
文件时间戳	否	否	否	是
HTTP 响应代码	是	是	否	否
IOC（危害表现）	否	是	是	是
消息	是	是	否	是
接收大洲	是	是	是	否
接收国家/地区	是	是	否	否
接收 IP	是	是	否	是
接收端口	是	是	否	否
安全情景	是	是	是	是
发送大洲	是	是	是	否
发送国家/地区	是	是	否	否
发送 IP	是	是	否	否
发送端口	是	是	否	否
SHA256/文件 SHA256	是	是	是	是
大小 (KB)/文件大小 (KB)	是	是	否	是
SSL 实际操作（仅限搜索）	是	是	否	否
SSL 证书信息 (SSL Certificate Information)（仅限搜索）	是	是	否	否
SSL 失败原因 （仅限搜索）	是	是	否	否

字段	文件事件	系统检测到的恶意软件事件	系统检测到的追溯性事件	以下项检测到的恶意软件事件：**Cisco Secure Endpoint**
SSL 状态	是	是	否	否
SSL 使用者/颁发者所在国家/地区（仅限搜索）	是	是	否	否
文件存储/已存储（仅限搜索）	是	是	否	否
威胁名称	否	是	是	是
威胁评分	是	是	否	否
时间	是	是	是	是
类型/文件类型	是	是	否	是
URI/文件 URI	是	是	否	否
用户	是	是	否	是
Web 应用	是	是	是	否
Web 应用类别或标记	是	是	是	否

查看有关已分析文件的详细信息

提示 要查看其他选项，请右键点击事件页面上的表中的文件SHA。有关信息，请参阅使用基于Web的资源的事件调查。

文件构成报告

如果配置本地恶意软件分析或动态分析，则系统会在分析文件后会生成文件构成报告。您可以通过此报告进一步分析文件，并确定它们是否可能携带嵌入式恶意软件。

文件构成报告列出文件属性、文件中嵌入的任何对象以及任何检测到的病毒。文件构成报告还可能列出特定于该文件类型的其他信息。当系统删除存储的文件时，也会删除相关联的文件构成报告。

要查看文件组成信息，请参阅 使用网络文件轨迹，第 32 页。

在 AMP 私有云中查看文件详细信息

如果您已部署 AMP 私有云，则可以查看有关私有云中已分析文件的其他详细信息。

有关详细信息，请参阅私有云的文档。

过程

直接登录 AMP 私有云控制台。

威胁评分和动态分析摘要报告

威胁评分

表 *6:* 威胁评分等级

威胁评分	数字分数	图标
Low	0-24	低
Medium	25-69	中等
High	70-94	高
Very High	95-100	很高

Cisco Secure Firewall Management Center对文件威胁评分进行缓存的时间与对文件处置情况进行缓存的时间相同。如果系统之后检测到这些文件，则会显示缓存威胁评分而不是重新查询 Secure Secure Malware Analytics 云或 Secure Secure Malware Analytics 设备。您可以自动向威胁评分超过已定义的恶意软件阈值威胁评分的文件分配恶意软件文件处置情况。

动态分析总结

如有动态分析总结，您可以点击威胁评分图标进行查看。如果存在多份报告，该总结应当基于与精确威胁评分匹配的最新报告。如果没有报告与精确威胁评分匹配，则会显示威胁评分最高的报告。如果存在多份报告，您可以选择一个威胁评分查看各份报告。

总结将列明构成威胁评分的各部分威胁。每个组件威胁都可以扩展至列出 AMP 云查找结果，以及与此组件威胁相关的任何进程。

进程树显示 Secure Secure Malware Analytics 云尝试运行该文件时启动的进程。这有助于识别包含恶意软件的文件是否在尝试访问超出预期的进程和系统资源（例如，运行 Word 文档打开 Microsoft Word，接着启动 Internet Explorer，然后运行 Java 运行时环境）。

列出的每个进程都包含可用于验证实际进程的进程标识符。进程树中的子节点表示由于父进程而启动的进程。

从动态分析摘要中，您可以点击**查看完整报告 (View Full Report)** 以查看完整分析报告，其中详述 AMP 云的完整分析，包括常规文件信息、对检测到的所有进程的更深入审核、文件分析明细以及其他相关信息。

查看思科 Secure Secure Malware Analytics 云中的动态分析结果

Secure Secure Malware Analytics 提供的有关已分析文件的报告比 防火墙管理中心提供的要详细。如果您的组织有 Secure Secure Malware Analytics 云账户，则您可以直接访问 Secure Secure Malware Analytics 门户，查看有关从托管设备发出的进行分析的文件的其他详细信息。

开始之前

- 将您的 防火墙管理中心 与您的 Secure Secure Malware Analytics 云账户关联。请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 启用对公共云中动态分析结果的访问权限
- 许可证要求：恶意软件
- 您必须在全局域中才能执行此任务。
- 您必须具有以下用户角色之一：管理员、访问管理员、网络管理员

过程

步骤 1 通过 Secure Secure Malware Analytics 文档中提供的地址访问 Secure Secure Malware Analytics 云门户。

步骤 2 使用您在此任务的前提条件中创建关联时使用的帐户凭证登录。

步骤 3 查看组织提交的文件，或使用其 SHA 搜索特定文件。

如有问题，请参阅 Secure Secure Malware Analytics 文档。

使用已捕获文件工作流程

当受管设备捕获在网络流量中检测到的文件时，它会记录一个事件。

注释 如果设备捕获包含恶意软件的文件，设备会生成两个事件：其检测文件时的文件事件，以及其识别恶意软件时的恶意软件事件。

通过此过程可查看表中已捕获文件的列表，并根据与分析相关的信息操作事件视图。在访问捕获的文件时看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以使用这些页面从较宽泛的视图移动至更精细化的视图来评估事件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

如果系统在配置更改后重新捕获文件（如更新的文件策略），则会更新该文件的现有信息。

例如，如果您将文件策略配制为通过**恶意软件云查找 (Malware Cloud Lookup)** 操作捕获文件，则系统会连同文件一起存储文件处置情况和威胁评分。然后，如果您更新文件策略，且系统因新的**检测文件 (Detect Files)** 操作重新捕获同一文件，则系统会更新该文件的**上次更改时间 (Last Changed)** 值。但系统不会删除现有处置情况和威胁评分，即使您没有再次执行恶意软件云查找。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

开始之前

您必须是管理员或安全分析师用户才能执行此任务。

过程

选择**分析** > **文件** > 、**捕获的文件**。

提示
事件表视图中的一些字段在默认情况下处于隐藏状态。要显示事件视图的隐藏字段，请展开搜索限制，然后点击 **Disabled Columns** 下的字段名称。

相关主题

捕获文件字段，第 24 页
预定义捕获文件工作流程
配置事件视图设置

捕获文件字段

捕获文件表视图是预定义捕获文件工作流程的最终页面，也可以添加到自定义工作流程中，且该视图为捕获文件表中的每个字段都准备了对应的列。

搜索此表时，请记住搜索结果取决于所搜索事件的可用数据；根据可用数据，搜索限制可能并不适用。例如，如果文件从未被提交用于动态分析，可能没有与其关联的威胁评分。

表 7: 捕获文件字段

字段	说明
存档检查状态	对于存档文件，存档检查状态如下： • “待定”(Pending) 表示系统仍在检查存档文件及其内容。如果文件再次通过您的系统，就可以提供完整的信息。 • “已提取”(Extracted) 表示系统能够提取和检查存档内容。 • 在极少数情况下，如果系统无法处理提取内容，会出现“失败”(Failed) 状态。 • “超出深度”(Depth Exceeded) 表示存档包含超出最大允许深度的进一步嵌套存档文件。 • “已加密”(Encrypted) 表示存档文件内容已加密，无法进行检查。 • “不可检查”(Not Inspectable) 表示系统未提取和检查存档内容。策略规则操作、策略配置和损坏文件是出现此状态的三个主要原因。 要查看某个存档文件的内容，请右键点击其在表中所在的行，打开上下文菜单，然后选择**查看存档内容 (View Archive Contents)**。
类别	一般类别文件类型，例如：Office 文档、存档、多媒体、可执行文件、PDF 文件、编码文件、图形或系统文件。
检测名称	被测恶意软件名称。
处理结果	文件的 恶意软件防护处置情况： • “恶意软件”(Malware) 表示本地恶意软件分析识别出恶意软件，AMP 云将文件归类为恶意软件，或文件威胁评分超过文件策略中定义的恶意软件阈值。 • “干净”(Clean) 表示 AMP 云将文件归类为干净，或者用户将该文件添加到干净列表。 • “未知”(Unknown) 表示系统查询了 AMP 云，但是尚未为文件分配处置情况；换句话说，AMP 云尚未将文件分类。 • “自定义检测”(Custom Detection) 表示用户将文件添加到自定义检测列表。 • “不可用”(Unavailable) 表示系统无法查询 AMP 云。您可能看到很少一部分事件为此处置；这是预期行为。 • “不适用”表示“检测文件”或“阻止文件”规则处理了文件，Cisco Secure Firewall Management Center未查询 AMP 云。
域	检测到捕获文件的域。 仅当曾经配置 防火墙管理中心以实现多租户时，此字段才存在。

字段	说明
动态分析状态	以下一个或多个值表示是否已提交文件以供动态分析： • “分析完成”(Analysis Complete) - 已提交文件以供动态分析且收到威胁评分和动态分析摘要报告 • “容量已处理”(Capacity Handled) - 已存储文件，因为当前无法提交文件 • “容量已处理（网络问题）”(Capacity Handled [Network Issue]) - 已存储文件，因为由于网络连接问题而无法提交文件 • “容量已处理（速率限制）”(Capacity Handled [Rate Limit]) - 已存储文件，因为已达到最大提交数量而无法提交文件 • 设备未激活 - 未提交文件，因为未在内部 Secure Secure Malware Analytics 设备上激活设备。如果看到此状态，请联系支持部门。 • “失败（分析超时）”(Failure [Analysis Timeout]) - 文件已提交，但 AMP 云尚未为其返回结果 • “失败（无法运行文件）”(Failure [Cannot Run File]) - 文件已提交，但 AMP 无法在测试环境中运行文件 • “失败（网络问题）”(Failure [Network Issue]) - 文件由于网络连接失败而未提交 • “未发送以供分析”(Not Sent for Analysis) - 文件未提交 • “不可疑（未发送以供分析）”(Not Suspicious [Not Sent For Analysis]) - 文件预先分类为非恶意软件 • 之前已分析 - 具有缓存威胁评分的文件，表示之前已发送 • 拒绝分析 - 根据静态分析，文件不太可能构成风险，例如，因为它不包含动态元素。 • “已发送以供分析”(Sent for Analysis) - 文件被预先分类为恶意软件，并排队等待动态分析
动态分析状态已更改	上一次文件分析状态发生变化的时间。
文件名	最近检测到的与文件 SHA-256 散列值相关的文件名。
上次更改时间	上一次更新与该文件有关信息的时间。
上次发送时间	最近一次向 AMP 云提交文件以供动态分析的时间。

字段	说明
本地恶意软件分析状态	下列值之一表示系统是否对文件执行本地恶意软件分析： • “分析完成”(Analysis Complete) - 系统使用本地恶意软件分析检查文件，并对文件预先分类。 • “分析失败”(Analysis Failed) - 系统尝试使用本地恶意软件分析检查文件但已失败。 • “手动请求已提交”(Manual Request Submitted) - 用户提交文件以供本地恶意软件分析 • “未分析”(Not Analyzed) - 系统未使用本地恶意软件分析检查文件
SHA256	文件的 SHA-256 散列值以及显示最近检测文件事件和文件处置情况的网络文件轨迹图标。要查看网络文件轨迹，请点击轨迹图标。
存储状态	表示文件是否存储于受管设备： • 已存储文件 • 未存储（处置情况待定）(Not Stored [Disposition Was Pending])
威胁评分	与此文件相关的最新威胁评分。 要查看动态分析总结报告，请点击威胁评分图标。
类型	文件类型；例如 HTML 或 MSEXE。

存储的文件下载

设备存储文件后，只要 Cisco Secure Firewall Management Center可以与该设备保持通信并且未删除文件，就可以将文件下载本地主机以供长期存储和分析，并手动分析文件。您可以从相关文件事件、恶意软件事件、捕获文件视图或文件轨迹中下载文件。

由于恶意软件有害，默认情况下，您必须在每次下载文件时进行确认。但是，可以在“用户首选项”(User Preferences) 中禁用确认。

因为性质为Unknown的文件可能包含恶意软件，当您下载文件时，系统会首先将该文件存档至 `.zip` 压缩包。`.zip` 文件名包含文件处置情况和文件类型（如有）以及 SHA-256 散列值。您可以对 `.zip` 文件采用密码保护以防意外解压缩。可以在“用户首选项”(User Preferences) 中编辑或删除默认 `.zip` 文件密码。

注意 思科强烈建议**不要**下载恶意软件，因为其可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

手动提交文件以供分析

手动提交文件以进行分析时，系统会运行本地分析，然后将这些文件提交到云以进行动态分析。但是，如果文件策略中未启用本地分析，您需要手动提交文件进行分析，则系统仅发送文件进行动态分析。

除了可执行文件，您也可以提交不适合自动提交的文件类型，例如 .swf、.jar 和其他类型。这样，您可以更快速地分析多种文件（而不管处置情况为何），并准确确定事故具体成因。

注释 系统会检查 AMP 云，确定动态分析合格文件类型列表是否更新（不超过一日一次）以及可提交的最小和最大文件大小。

根据具体情况，有两种方法可以提交文件进行分析：

开始之前

为了手动提交捕获的文件以进行分析，必须配置一个或多个文件规则来存储文件。有关信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 网络恶意软件保护和文件策略 一章。

过程

步骤 1 要提交单个文件进行分析，请执行以下操作：

a) 选择以下一个选项：

- **分析 > 文件 (File Events Analysis Files >)**
- **分析 > 文件 > 恶意软件事件**
- **分析 > 文件 > 、捕获的文件**

b) 点击 **<事件类型或文件> 的表视图**。

c) 右键点击表中的文件，然后选择**分析文件 (Analyze File)**。

步骤 2 要提交多个捕获的文件以进行分析（一次最多 25 个），请执行以下操作：

a) 选择 **分析 > 文件 > 、捕获的文件**

b) 选中每个要分析的文件旁边的复选框。

c) 点击**分析**。

网络文件轨迹

网络文件轨迹功能映射出主机怎样在网络中传送文件，包括恶意软件文件。轨迹以图表形式展示文件传输数据、文件处置情况以及是否阻止文件传送或是否隔离文件。您可以确定哪些主机和用户可能已传送恶意软件、哪些主机存在风险，并观察文件传送趋势。

您可以跟踪具有 AMP 云分配处置情况的所有文件。系统可以使用与检测和阻止来自恶意软件防护和面向终端的 AMP 的恶意软件相关的信息来建立轨迹。

最近检测到的恶意软件和分析的轨迹

“网络文件轨迹列表”(Network File Trajectory List) 页面显示网络上最近检测到的恶意软件，以及最近查看过轨迹映射的文件。从这些列表中，可以查看最近在网络上查看每个文件的时间，该文件的 SHA-256 散列值、名称、类型、当前文件处置情况、内容（对于存档文件），以及与该文件相关联的事件的数量。

该页面还包含一个可让您定位文件的搜索框，可基于 SHA-256 哈希值、文件名或传送或接收文件主机的 IP 地址进行查找。定位一个文件后，您可以点击**文件 SHA256** 值，查看详细轨迹映射。

网络文件轨迹详细视图

您可以通过查看网络文件详细轨迹在网络中跟踪文件。搜索文件的 SHA 256 值或点击网络文件轨迹列表中的**文件 SHA 256 (File SHA 256)** 链接可查看该文件的详细信息。

“网络文件轨迹详细信息”(Network File Trajectory Details) 页面包含三个部分：

- 摘要信息 - 文件的轨迹页面显示文件的相关摘要信息，包括文件识别信息、首次及最近一次在网络上查看该文件的时间及查看该文件的用户、与该文件相关的事件和主机数量以及该文件的当前处置情况。从本节开始，如果受管设备已存储文件，您可以进行本地下载、提交文件进行动态分析或将文件添加至文件列表。
- 轨迹映射 - 文件的轨迹映射直观地跟踪从网络上第一次检测到文件至最近一次检测到该文件的情况。该映射显示出主机传送或接收文件的时间、传送文件频率和阻止或隔断文件的时间。数据点之间的垂直线代表文件在主机之间传送。连接数据点的水平线表示随时间推移的主机文件活动。

  该映射同时显示该文件生成文件事件的频率，以及系统为文件分配性质或回溯性质的时间。您可以在映射中选择数据点，并突出显示追溯至主机第一次传输该文件的实例的路径；此路径还将贯穿每次主机作为该文件接收方或发送方的事例，并识别所涉及的用户。
- 相关事件 -“事件”(Events) 表列出映射中各数据点的事件信息。使用该表和映射，您可以准确定位特定文件事件、网络上传送或接收该文件的主机和用户、映射中的相关事件以及表中受选定值限制的其他关联事件。

网络文件轨迹摘要信息

对于“网络文件轨迹”(Network File Trajectory) 列表中显示的文件，“详细信息”(Details) 页面顶部会显示以下摘要信息。

提示 要查看相关文件事件，请点击字段值链接。在新窗口中打开文件事件默认工作流程首页，显示包含选定值的所有文件事件。

表 *8:* 网络文件轨迹摘要信息字段

名称	说明
存档内容	对已检查存档文件，指存档文件包含的文件数量。
当前处置	可以为下列恶意软件防护 文件安全状态之一： • 恶意软件 (Malware) 表示 AMP 云将文件分类为恶意软件，本地恶意软件分析识别恶意软件，或者文件的威胁评分超过文件策略中定义的恶意软件阈值。 • 干净 (Clean) 表示 AMP 云将文件归类为干净，或者用户将该文件添加到干净列表。 • 未知 (Unknown) 表示系统查询了 AMP 云，但是尚未为文件分配处置情况；换句话说，AMP 云尚未将文件分类。 • Custom Detection 表示用户将文件添加到自定义检测列表。 • 不可用 (Unavailable) 表示系统无法查询 AMP 云。您可能看到很少一部分事件为此处置；这是预期行为。 • 不适用表示“检测文件”或“阻止文件”规则处理了文件，Cisco Secure Firewall Management Center未查询 AMP 云。
检测名称	本地恶意软件分析检测到的恶意软件的名称。
事件计数	网络上看到的与该文件相关事件的数量，以及如检测到超过250个事件时映射中显示的事件数量。
文件类别	文件类型的一般类别，例如 Office Documents 或 System Files。
文件名	事件关联文件的名称，如网络上所示。 如果一个SHA-256哈希值与多个文件名关联，列出最近检测到的文件名。您还可通过点击more将其展开以查看其余文件名。
文件 SHA256	文件的 SHA-256 散列值。 默认情况下以压缩格式显示哈希值。要查看完整哈希值，请将指针悬停在上方。如果一个文件名与多个 SHA-256 哈希值关联，将指针悬停在链接上方查看全部哈希值。
文件大小 (KB)	文件大小（千字节）。

名称	说明
文件类型	文件类型，例如 HTML 或 MSEXE。
首次查看时间	恶意软件防护 或Cisco Secure Endpoint 首次检测到文件以及主机（第一个上传该文件和相关用户的身份信息的主机）的 IP 地址的时间。
上次查看时间	恶意软件防护 或Cisco Secure Endpoint 最近一次检测到文件以及主机（最后一个下载该文件和相关用户的身份信息的主机）的 IP 地址的时间。
父应用	在Cisco Secure Endpoint 执行检测时访问恶意软件文件的客户端应用。这些应用与网络发现或应用控制**无**关联。
出现时间	发送或接收文件的主机数量。因为一台主机可以在不同时间上传和下载文件，在 Seen On Breakdown 字段中的主机总数可能与发送方总数加上接收方总数之和并不匹配。
中断时出现	发送文件的主机数量，然后紧接接收文件的主机数量。
威胁名称	通过Cisco Secure Endpoint 与检测到的恶意软件相关联的威胁的名称。
威胁评分	文件的威胁评分。

网络文件轨迹映射和相关事件列表

文件轨迹映射的 y 轴包含与该文件交互的所有主机 IP 地址的列表。IP 地址按照系统在主机上首次检测到该文件的时间降序排列。每行都包含与该 IP 地址相关的所有事件，无论是单一文件事件、文件传送还是回溯事件。x 轴包含系统检测到各个事件的日期和时间。时间戳按时间顺序排列。如果一分钟内发生了多个事件，则在同一栏中列出所有事件。您可以水平或垂直滚动映射，以查看其他事件和 IP 地址。

映射中显示多达 250 个与文件 SHA-256 散列值有关的事件。如有超过 250 个事件，则映射上只显示前十个，并用 **箭头**截略其他事件。然后映射再显示剩下的 240 个事件。

系统将在新窗口中显示“文件事件”默认工作流程的首页，同时显示基于文件类型受限的所有其他事件。如果未显示面向终端的 AMP 生成的恶意软件事件，您必须切换到“恶意软件事件”表进行查看。

每个数据点都表示一个事件及其文件处置情况，如映射下方图例中所述。例如，“恶意软件阻止”(Malware Block) 事件图标结合了“恶意处置情况”(Malicious Disposition) 图标和“阻止事件”(Block Event) 图标。

面向终端的 AMP 生成的恶意软件事件（“基于终端的恶意软件事件”）包括一个图标。回溯事件在栏中为检测到文件的各个主机显示一个图标。文件传送事件始终包括两个图标，一个文件发送图标和一个文件接收图标，两者之间用垂直线连接。箭头表示从发送方到接收方的文件传送方向。

要跟踪文件在网络中的历程，可以点击任意数据点突出显示一个轨迹，其中包括与选定数据点相关的所有数据点。这其中包括与下列类型的事件相关的数据点：

- 无论关联 IP 地址作为发送方还是接收方的任何文件传送
- 涉及关联 IP 地址的任何面向终端的 AMP 生成的恶意软件事件（“基于终端的恶意软件事件”）

- 如果涉及另一个 IP 地址，无论该关联 IP 地址作为发送方还是接收方的所有文件传送
- 如果涉及另一个 IP 地址，涉及该 IP 地址的任何面向终端的 AMP 生成的恶意软件事件（“基于终端的恶意软件事件”）

同时突出显示与任何突出显示的数据点相关的所有 IP 地址和时间戳。同时突出显示事件表中的相应事件。如果一条轨迹中包含截略事件，则用虚线突出显示轨迹本身。可能有截略事件与轨迹相交，但并不在映射中进行显示。

使用网络文件轨迹

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

提示 如果您的组织已部署 Cisco Secure Endpoint，则该产品还具有网络文件轨迹功能。要从 防火墙管理中心 跳转至 Cisco Secure Endpoint，请参阅 使用 Cisco Secure Endpoint 控制台中的事件数据，第 33 页。有关 Cisco Secure Endpoint中的文件轨迹功能的详细信息，请参阅 Cisco Secure Endpoint 文档。

开始之前

如果您正在使用 恶意软件防护，则需要 恶意软件防御 许可证。

您必须是管理员或安全分析师用户才能执行此任务。

过程

步骤 1 选择**分析** > **文件** > **网络文件轨迹**。

提示
您还可以从情景管理器、控制面板或具有文件信息的事件视图来访问文件轨迹。

步骤 2 点击列表中的**文件 SHA 256 (File SHA 256)** 链接。

步骤 3 或者，在搜索字段输入完整的 SHA-256 散列值、主机 IP 地址或要跟踪的文件的名称，然后按 Enter 键。

提示
如果只有一个结果匹配，系统将显示该文件的 Network File Trajectory 页面。

步骤 4 在“摘要信息”(Summary Information) 部分中，可以执行以下操作：

- 将文件添加到文件列表 - 要在干净的列表或自定义检测列表中添加或删除文件，请点击 **编辑** ()。
- 下载文件 - 要下载文件，请点击下 **下载** （），并在出现提示时，确认要下载该文件。如果该文件无法下载，则此下载文件呈灰色显示。
- 报告 - 点击威胁评分，查看“动态分析摘要”报告。

- 提交动态分析 - 点击 **AMP 云** 以提交文件进行动态分析。如果该文件无法提交或您无法连接到 AMP 云，则此 AMP 云呈灰色显示。
- 查看存档内容 - 要查看有关存档文件内容的信息，请点击 **视图** ( )。
- 查看文件组成 - 要查看文件的组成，请点击 **文件列表**。如果系统未生成文件组成报告，则此文件列表呈灰色显示。
- 查看威胁评分相同的捕获文件 - 点击威胁评分链接，查看具有该威胁评分的所有捕获文件。

注释
思科强烈建议**不要**下载恶意软件，因为其可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

步骤 5 在轨迹映射上，可以执行以下操作：

- 确定第一个实例 - 点击一个 IP 地址，确定第一次发生涉及 IP 地址的文件事件的位置。突出显示连至该数据点的路径，以及与第一个文件事件相关的任何介于其间的文件事件和 IP 地址。同时突出显示事件表中的相应事件。如当前不可见，映射会滚动至该数据点。
- 跟踪 - 点击任意数据点，突出显示包含与所选数据点相关的所有数据点的轨迹，从而通过网络跟踪文件的进度。
- 查看隐藏事件 - 点击箭头，查看“文件摘要”事件视图中未显示的所有事件。
- 查看匹配文件事件 - 将指针悬停在 **匹配文件事件** 上方，查看事件的摘要信息。如果点击任何事件摘要信息链接，则会在新窗口中显示“文件事件”(File Events) 默认工作流程的首页，其中包含基于文件类型限制的所有其他事件。“文件摘要”(File Summary) 事件视图在新窗口中打开，显示与所点击的条件值相匹配的所有文件事件。

步骤 6 在“事件”(Events) 表中，可以执行以下操作：

- 突出显示 - 选择表行，突出显示映射中的数据点。如当前不可见，映射会滚动至选定文件事件并显示该事件。
- 排序 - 点击列标题以按升序或降序对事件进行排序。

使用 Cisco Secure Endpoint 控制台中的事件数据

如果您的组织已部署 Cisco Secure Endpoint，则您可以在 Cisco Secure Endpoint 控制台中查看 恶意软件事件数据，并可以使用该应用的全局网络文件轨迹工具。

提示 有关使用 Cisco Secure Endpoint 及其控制台的信息，请参阅控制台中的在线帮助或 https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html中提供的其他文档

要从 Cisco Secure Firewall Management Center访问 Cisco Secure Endpoint 控制台，请执行以下操作之一：

开始之前

- 必须配置与 Cisco Secure Endpoint 的连接（请参阅 集成 *Cisco Secure EndpointCisco Secure Firewall* 和 中的 《Cisco Secure Firewall Management Center 设备配置指南》）并且 Cisco Secure Firewall Management Center 必须能够连接到 AMP 云。
- 您将需要您的 Cisco Secure Endpoint 凭证。
- 您必须是管理员用户才能执行此任务。
- 如果要从防火墙管理中心中的恶意软件事件转向别处的恶意软件事件，请确保正确启用了 Cisco Secure Endpoint 上下文交叉启动选项。请参阅使用基于 Web 的资源的事件调查下的主题。

过程

步骤 1 方法 1：

a) 选择**集成** > **AMP** > **AMP 管理**。

b) 点击表中的云名称。

步骤 2 方法 2：

a) 导航到**分析** > **文件** > 、**捕获的文件**下的表中的恶意软件事件。

b) 右键点击文件 SHA，然后选择 Cisco Secure Endpoint 选项。

文件/恶意软件事件和网络文件轨迹的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
文件和恶意软件事件中的 MITRE 信息。	7.4	7.4	系统现在在文件和恶意软件事件中包含 MITRE 信息（来自本地恶意软件分析）。您可以在经典和统一事件视图中查看MITRE信息。请注意，默认情况下，MITRE 列在两个事件视图中都是隐藏的。
用于动态分析的改进的预分类文件。	6.7	任意	额外的评估可避免发送不必要的文件以进行动态分析。未根据此评估发送到云的文件的新动态分析状态为 **已拒绝分析**。 新增/修改后的屏幕： **分析** > **捕获的文件** > **捕获文件的表视图**。
系统日志中连接事件的唯一标识符。	6.4.0.4	任意	以下系统日志字段共同唯一标识连接事件并在文件和恶意软件事件的系统日志中显示：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

功能	防火墙管理中心最低版本	最低版本	详细信息
通过系统日志发送文件和恶意软件事件	6.4	任意	本章中的字段说明指定了系统日志消息中包含的字段。 有关配置信息，请参阅 文件和恶意软件事件系统日志的配置位置。

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。