跟踪

本章包含以下部分：

跟踪服务概述

思科安全邮件和网络管理器设备的跟踪服务是邮件安全设备的补充功能。利用安全管理设备，邮件管理员可以在单一位置处跟踪通过任意邮件安全设备的邮件的状态。

利用安全管理设备，可以很方便地查找邮件安全设备处理的邮件的状态。通过确定邮件的确切位置，邮件管理员可以快速解决支持中心的呼叫问题。使用安全管理设备，管理员可以确定特定邮件是已传送、包含病毒或放在垃圾邮件隔离区，还是位于邮件流的其他位置。

您可以使用安全管理设备灵活的跟踪界面来查找邮件，而不必使用 grep 或类似工具搜索日志文件。您可以组合使用多种搜索参数。

跟踪查询可以包括：

- **时间范围**：查找在指定的日期和时间之间发送的邮件。
- **信封信息**：通过输入要匹配的文本字符串，查找来自特定信封发件人或收件人的邮件。
- **主题**：与主题行中的文本字符串相匹配。警告：请勿在法规禁止此类跟踪的环境中使用此类型的搜索。
- **附件名称**：您可以根据附件名称搜索邮件。搜索结果中将显示至少包含一个采用查询名称的附件的邮件。

  出于性能原因，附件（如 OLE 对象）或存档文件（如 .ZIP 文件）内的文件名不会被跟踪。

对于某些附件，可能不跟踪。由于性能原因，附件名称扫描仅在其他扫描操作过程中发生，例如邮件或内容过滤、DLP 或免责声明印戳。只有通过正文扫描，且仍附带附件的邮件，才能获得其附件名称。附件名称将不会出现的一些示例包括（但不限于）：

- 如果系统只使用内容过滤器，并且邮件被删除或其附件被反垃圾邮件或防病毒过滤器隔离
- 如果在进行正文扫描之前，邮件拆分策略从某些邮件中删除了附件。

- **文件 SHA256**：查找具有邮件文件 SHA-256 值的邮件
- **思科主机**：将搜索条件缩小为特定的邮件安全设备，或在所有托管设备内搜索。
- **邮件 ID 信头和思科 MID**：通过标识 SMTP“Message-ID:”信头或思科邮件 ID (MID) 来查找邮件。
- **发件人 IP 地址/域/网络所有者**：搜索来自特定 IP 地址、域名或网络所有者的邮件。
- **邮件事件**：查找与指定的事件相匹配的邮件，例如标记为病毒邮件、垃圾邮件或疑似垃圾邮件的邮件，以及已传送、硬退回、软退回或发送到病毒爆发隔离区的邮件
- **拒绝的连接**：在搜索结果中搜索来自被拒绝连接的特定 IP 地址、域名或网络所有者的邮件

设置集中邮件跟踪

要设置集中邮件跟踪，请按顺序完成下列过程：

1. 启用集中邮件跟踪, on page 2
2. 在邮件安全设备上配置集中邮件跟踪 , on page 3
3. 向每台托管邮件安全设备添加集中邮件跟踪服务 , on page 4

启用集中邮件跟踪

- 在旧 Web 界面上启用集中邮件跟踪， 第 2 页
- 在新 Web 界面上启用集中邮件跟踪， 第 3 页

在旧 Web 界面上启用集中邮件跟踪

步骤 1 依次选择**管理设备 > 集中服务 > 邮件 > 集中邮件跟踪**。

步骤 2 在“邮件跟踪服务”(Message Tracking Services) 部分，单击**启用 (Enable)**。

步骤 3 如果在运行“系统设置向导”(System Setup Wizard) 后首次启用集中邮件跟踪，请查阅《最终用户许可证协议》，然后单击**接受 (Accept)**。

步骤 4 提交并确认更改。

What to do next

在邮件安全设备上配置集中邮件跟踪 , on page 3

在新 Web 界面上启用集中邮件跟踪

步骤 1 在安全管理设备上，单击**服务状态 (Service Status)**，然后将鼠标悬停在与**消息跟踪**卡对应的 图标上方。

步骤 2 单击**编辑设置 (Edit Settings)**。

步骤 3 如果您在运行“系统设置向导”(System Setup Wizard) 后首次启用集中邮件跟踪，请查看并接受许可协议，然后单击**继续 (Proceed)**。1

步骤 4 单击切换开关以启用集中邮件跟踪。

步骤 5 选择适当的字段并单击**提交 (Submit)**。

What to do next

在邮件安全设备上配置集中邮件跟踪 , on page 3

在邮件安全设备上配置集中邮件跟踪

步骤 1 [仅限新 Web 界面] 在安全管理设备中，单击 加载旧 Web 界面。

步骤 2 确认邮件安全设备上是否已配置邮件跟踪，且其运行是否正常。

步骤 3 依次转至**安全服务 (Security Services) > 邮件跟踪 (Message Tracking)**。

步骤 4 单击**编辑设置 (Edit Settings)**。

步骤 5 选择**集中跟踪 (Centralized Tracking)**。

步骤 6 单击**提交 (Submit)**。

步骤 7 如果希望可以搜索和记录邮件附件名称：

请确保在邮件安全设备上，至少配置和启用了一种传入内容过滤器或其他正文扫描功能。有关内容过滤器和正文扫描的信息，请参阅邮件安全设备的文档或在线帮助。

步骤 8 提交并确认更改。

步骤 9 请为每个要管理的邮件安全设备重复上述步骤。

What to do next

向每台托管邮件安全设备添加集中邮件跟踪服务 , on page 4

向每台托管邮件安全设备添加集中邮件跟踪服务

执行的步骤取决于是否已在配置其他集中管理功能时添加了设备。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，单击 ⚙ 加载旧 Web 界面。

步骤 2 选择**管理设备 > 集中化服务 > 安全设备**。

步骤 3 如果已向此页面的列表中添加了邮件安全设备，请执行以下操作：

a) 单击邮件安全设备的名称。

b) 选择**集中邮件跟踪 (Centralized Message Tracking)** 服务。

步骤 4 如果您尚未添加邮件安全设备，请执行以下操作：

a) 单击“添加邮件设备”(Add Email Appliance)。

b) 在“设备名称 (Appliance Name)”和“IP 地址 (IP Address)”文本字段，键入设备名称和邮件安全设备管理接口的 IP 地址。

Note 如果在“IP 地址”(IP Address) 文本字段中输入 DNS 名称，则单击**提交 (Submit)**后，该名称将立即解析为 IP 地址。

c) 预先选择集中邮件跟踪服务。

d) 单击**建立连接 (Establish Connection)**。

e) 在要托管的设备上输入管理员账户的用户名和口令，然后单击**建立连接 (Establish Connection)**。

Note 输入登录凭证，以便将文件传输的公共 SSH 密钥从安全管理设备传递到远程设备。登录凭证不会存储在安全管理设备上。

f) 等待该页面表格上方显示成功消息。

g) 单击**测试连接 (Test Connection)**。

h) 阅读表格上方的测试结果。

步骤 5 提交并确认更改。

步骤 6 为要启用集中邮件跟踪的每个邮件安全设备重复执行此程序。

管理对敏感信息的访问权限

如果您要将管理任务分配给其他人，并且要限制他们对违反防数据丢失 (DLP) 策略的邮件中可能出现的敏感信息的访问，请参阅控制对“邮件跟踪”中敏感信息的访问权限。

检查邮件跟踪数据的可用性

您可以确定邮件跟踪数据包括的日期范围，并可识别这些数据中缺少的任何间隔。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，单击 ⚙ 加载旧 Web 界面。

步骤 2 选择**邮件** > **邮件跟踪** > **邮件跟踪数据可用性**。

搜索邮件

注释 升级到 AsyncOS 13.6.1 之后，升级前隔离区中的邮件状态不会发生变化。

- 在新 Web 界面上搜索邮件，第 5 页
- 上搜索邮件。，第 7 页
- 补救邮箱中的邮件，第 9 页

在新 Web 界面上搜索邮件

使用的跟踪服务可以搜索特定的邮件或与指定的条件相匹配的一组邮件，例如邮件主题行、日期和时间范围、信封发件人或收件人或处理事件（例如，邮件是否被标记为病毒邮件、垃圾邮件、硬退回、已传送等）。邮件跟踪允许您详细地了解邮件流。您还可以详细查看特定的邮件以了解邮件详细信息，例如处理事件、附件名称或信封和标题信息。

注释 虽然跟踪组件提供关于各封邮件的详细信息，但是您无法使用它阅读邮件的内容。

步骤 1 在安全管理设备上，选择**跟踪 (Tracking)** > **搜索 (Search)**。

步骤 2 选择**邮件**选项卡或**拒绝连接**选项卡以缩小搜索结果范围。

注释 您可以根据发件人 IP 地址、域或网络所有者搜索已拒绝的连接。

步骤 3 （可选）单击**高级搜索 (Advanced Search)**，以显示更多搜索选项。

步骤 4 输入以下搜索条件：

注释 跟踪搜索不支持通配符和正则表达式。跟踪搜索不区分大小写。

- [对于邮件或被拒连接] **收到邮件 (Message Received)**：使用“昨天”(Last Day)、“过去 7 天”(Last 7 Days) 或“自定义范围”(Custom Range) 为查询指定日期和时间范围。使用“昨天”(Last Day) 选项可搜索过去 24 小时内的邮件；使用“过去 7 天”(Last 7 Days) 选项可搜索过去七整天内的邮件（加上当天经过的时间）。

  如果未指定日期，查询将返回所有日期的数据。如果仅指定时间范围，查询将返回所有可用日期内该时间范围的数据。如果您指定当前日期，并将 23:59 指定为结束日期和时间，查询则返回当前日期的所有数据。

  日期和时间存储在数据库时会转换为 GMT 格式。在设备上查看日期和时间时，它们将按设备的本地时间显示。

只有邮件安全设备中已记录邮件，且安全管理设备检索到邮件时，结果中才会显示邮件。根据日志大小和轮询频率，邮件的发送时间与其实际在跟踪和报告结果中的显示时间可能存在小的差距。

- **信封发件人 (Envelope Sender)**：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后在“信封发件人”(Envelope Sender) 中输入要搜索的文本字符串。您可以输入邮件地址、用户名或域。使用以下格式：
  - 对于邮件域：*example.com*、*[203.0.113.15]*、*[ipv6:2001:db8:80:1::5]*
  - 对于完整的邮件地址：*user@example.com*、*user@[203.0.113.15]* 或 *user@[ipv6:2001:db8:80:1::5]*。
  - 您可以输入任何字符。不执行条目验证。
- **主题 (Subject)**：选择“开头为”(Begins With)、“是”(Is)、“包含”(Contains) 或“为空”(Is Empty)，然后在邮件主题行中输入要搜索的文本字符串。
- **信封收件人 (Envelope Recipient)**：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后在“信封收件人”(Envelope Recipient) 中输入要搜索的文本字符串。您可以输入邮件地址、用户名或域。

  如果对邮件安全设备上的的别名扩展使用别名表，搜索将查找扩展的收件人地址，而不是原始信封地址。在任何其他情况下，邮件跟踪查询将查找原始信封收件人地址。

  否则，信封收件人的有效搜索条件与信封发件人的搜索条件相同。

  您可以输入任何字符。不执行条目验证。
- **附件名称 (Attachment name)**：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后为要查找的一个附件名称输入 ASCII 或 Unicode 文本字符串。前导空格和尾部空格不会从您输入的文本中删除。
- **回复 (Reply-To)**：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后输入文本字符串以根据邮件的回复 (`Reply-To`) 信头搜索邮件。
- **文件 SHA256**：输入消息的文件 SHA-256 值。

  有关基于 SHA-256 散列识别文件的详细信息，请参阅通过 SHA-256 散列标识文件。
- **Cisco Host**：选择所有主机以在所有邮件安全设备中进行搜索，或从下拉菜单中选择所需的邮件安全设备。
- **邮件 ID 标题和 Cisco MID (Message ID Header and Cisco MID)**：输入邮件 ID 标题、Cisco IronPort 邮件 ID 或两者的文本字符串。
- [对于邮件和拒绝的连接]**发件人 Ip 地址/域/网络所有者**：输入发件人 ip 地址、域或网络所有者详细信息。
  - IPv4 地址必须是用句点隔开的 4 个数字。每个数字的值必须介于 0 和 255 之间。（示例：203.0.113.15）。
  - IPv6 地址包含 8 组 16 位十六进制值，用冒号分隔。

    可以在一个位置使用零压缩，例如 2001:db8:80:1::5。
  - **邮件事件 (Message Event)**：选择要跟踪的事件。选项为“病毒 (Virus Positive)”、“垃圾邮件 (Spam Positive)”、“可疑垃圾邮件 (Suspect Spam)”、“包含恶意 URL (contained malicious URLs)”、“包含指定类别的 URL (contained URL in specified category)”、“DLP 违规 (DLP Violations)”（可以选择 DLP 策略的名称，并选择违规严重程度或采取的操作）、“DMARC 违规 (DMARC violations)”、“已传送 (Delivered)”、“高级恶意软件保护 (Advanced Malware Protection Positive)”（适用于附件中的恶意软

件）、“硬退回 (Hard Bounced)”、“软退回 (Soft Bounced)”、“当前在策略、病毒或病毒爆发隔离区 (currently in a policy, virus, or outbreak quarantine)”、“被邮件过滤器或内容过滤器拦截 (caught by message filters or content filters)”和“作为垃圾邮件隔离 (Quarantined as Spam)”。与您添加到跟踪查询的大多数条件不同，事件是使用“OR”运算符添加的。选择多个事件可扩大搜索。

您无需填写每个字段。除“邮件事件”(Message Event) 选项外，该查询是一种“AND”搜索。该查询返回与搜索字段中指定的“AND”条件相匹配的邮件。例如，如果您为信封收件人和主题行参数指定文本字符串，则查询只会返回与指定信封收件人和主题行都匹配的邮件。

注释 在新 Web 界面中，要执行部分 URL 搜索，则需要在搜索字符串前后添加“*”以便检索结果。

步骤 5 单击**搜索 (Search)**。

每行与一封邮件相对应。向下滚动，以在视图中加载更多邮件。

如有必要，请通过输入新的搜索条件细化搜索，然后重新运行查询。或者，您可以通过缩小结果集细化搜索，如以下各部分所述。

单击“导出”(Export) 以导出搜索结果。

下一步做什么

- 缩小结果集，第 10 页
- 关于邮件跟踪和高级恶意软件防护功能 ，第 11 页
- 了解跟踪查询结果，第 12 页

上搜索邮件。

通过安全管理设备的跟踪服务，可以搜索与指定条件匹配的特定邮件或邮件组，这些条件包括邮件主题行、日期和时间范围、信封发件人或收件人，或处理事件（例如，邮件是否为病毒邮件、垃圾邮件、硬退回、已传送邮件等）等。邮件跟踪允许您详细地了解邮件流。您还可以详细查看特定的邮件以了解邮件详细信息，例如处理事件、附件名称或信封和标题信息。

Note 虽然跟踪组件提供关于各封邮件的详细信息，但是您无法使用它阅读邮件的内容。

步骤 1 选择**邮件 > 邮件跟踪 > 邮件跟踪**。

步骤 2 （可选）单击“高级”(Advanced) 链接显示更多搜索选项。

步骤 3 输入搜索条件：

Note 跟踪搜索不支持通配符和正则表达式。跟踪搜索不区分大小写。

- 信封发件人 (Envelope Sender)：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后在“信封发件人”(Envelope Sender) 中输入要搜索的文本字符串。您可以输入邮件地址、用户名或域。使用以下格式：
  - 对于邮件域：example.com、[203.0.113.15]、[ipv6:2001:db8:80:1::5]
  - 对于完整的邮件地址：user@example.com、user@[203.0.113.15] 或 user@[ipv6:2001:db8:80:1::5]。
  - 您可以输入任何字符。不执行条目验证。
- 信封收件人 (Envelope Recipient)：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后在“信封收件人”(Envelope Recipient) 中输入要搜索的文本字符串。您可以输入邮件地址、用户名或域。

如果对邮件安全设备上的的别名扩展使用别名表，搜索将查找扩展的收件人地址，而不是原始信封地址。在任何其他情况下，邮件跟踪查询将查找原始信封收件人地址。

否则，信封收件人的有效搜索条件与信封发件人的搜索条件相同。

您可以输入任何字符。不执行条目验证。

- 主题 (Subject)：选择“开头为”(Begins With)、“是”(Is)、“包含”(Contains) 或“为空”(Is Empty)，然后在邮件主题行中输入要搜索的文本字符串。
- 收到邮件 (Message Received)：使用“昨天”(Last Day)、“过去 7 天”(Last 7 Days) 或“自定义范围”(Custom Range) 为查询指定日期和时间范围。使用“昨天”(Last Day) 选项可搜索过去 24 小时内的邮件；使用“过去 7 天”(Last 7 Days) 选项可搜索过去七整天内的邮件（加上当天经过的时间）。

如果未指定日期，查询将返回所有日期的数据。如果仅指定时间范围，查询将返回所有可用日期内该时间范围的数据。如果您指定当前日期，并将 23:59 指定为结束日期和时间，查询则返回当前日期的所有数据。

日期和时间存储在数据库时会转换为 GMT 格式。在设备上查看日期和时间时，它们将按设备的本地时间显示。

只有邮件安全设备中已记录邮件，且安全管理设备检索到邮件时，结果中才会显示邮件。根据日志大小和轮询频率，邮件的发送时间与其实际在跟踪和报告结果中的显示时间可能存在小的差距。

- 发件人 IP 地址 (Sender IP Address)：输入发件人 IP 地址并选择是要搜索邮件还是仅搜索已拒绝的连接。
  - IPv4 地址必须是用句点隔开的 4 个数字。每个数字的值必须介于 0 和 255 之间。（示例：203.0.113.15）。
  - IPv6 地址包含 8 组 16 位十六进制值，用冒号分隔。可以在一个位置使用零压缩，例如 2001:db8:80:1::5。
- 邮件事件 (Message Event)：选择要跟踪的事件。选项为“病毒”、“垃圾邮件”、“可疑垃圾邮件”、“包含恶意 URL”、“包含指定类别的 URL”、“DLP 违规”（可以输入 DLP 策略的名称，并选择违规严重程度或所采取的操作）、“DMARC 违规”、“已传送”、“高级恶意软件保护”（适用于附件中的恶意软件）、“硬退回”、“软退回”、“当前在策略、病毒或病毒爆发隔离区”、“被邮件过滤器或内容过滤器拦截”、“已检测到的宏文件类型”、“地理位置”、“低风险”和“作为垃圾邮件隔离” 。与您添加到跟踪查询的大多数条件不同，事件是使用“OR”运算符添加的。选择多个事件可扩大搜索。
- 邮件 ID 标题和 Cisco IronPort MID (Message ID Header and Cisco IronPort MID)：输入邮件 ID 标题、Cisco IronPort 邮件 ID 或两者的文本字符串。
- 查询设置 (Query Settings)：从下拉菜单中，选择您希望查询在超时之前运行多久。选项包括“1 分钟”(1 minute)“2 分钟”(2 minutes)、“5 分钟”(5 minutes)、“10 分钟”(10 minutes) 和“无时间限制”(No time limit)。此外，请选择您希望查询返回的最大结果数量（最多为 1000 个）。
- 附件名称 (Attachment name)：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后为要查找的一个附件名称输入 ASCII 或 Unicode 文本字符串。前导空格和尾部空格不会从您输入的文本中删除。

您无需填写每个字段。除“邮件事件”(Message Event) 选项外，该查询是一种“AND”搜索。该查询返回与搜索字段中指定的“AND”条件相匹配的邮件。例如，如果您为信封收件人和主题行参数指定文本字符串，则查询只会返回与指定信封收件人和主题行都匹配的邮件。

步骤 4 单击**搜索 (Search)**。

查询结果出现在页面顶部。每行与一封邮件相对应。

您的搜索条件在每行中突出显示。

如果返回的行数大于“每页项目数”(Items Per Page) 字段中指定的值，则结果显示在多个页面上。要浏览各个页面，请单击列表顶部或底部的页码。

如有必要，请通过输入新的搜索条件细化搜索，然后重新运行查询。或者，您可以通过缩小结果集细化搜索，如以下各部分所述。

What to do next

- 缩小结果集, on page 10
- 关于邮件跟踪和高级恶意软件防护功能 , on page 11
- 了解跟踪查询结果, on page 12

补救邮箱中的邮件

思科内容安全管理设备提供对已传送到用户邮箱的恶意邮件进行补救的功能。您可以使用邮件跟踪过滤器来配置设备以补救邮件。

您可以对已传送到用户邮箱的邮件手动执行补救操作。例如，监控传入邮件的管理员可以使用邮件跟踪过滤器来对用户邮箱中的邮件执行补救操作。

您还可以使用“邮件跟踪”(Message Tracking) 页面来搜索和补救已传送到用户邮箱的邮件。“邮件跟踪”(Message Tracking) 页面是一个统一位置，可用于搜索已传送到邮箱的所有邮件。从搜索结果中，您可以选择要补救的邮件，并应用要对邮件执行的操作。

搜索和补救邮件工作流程

1. 邮件到达设备并被传送给收件人。
2. 用户使用邮件跟踪过滤器来搜索传送给收件人的邮件。
3. 用户从收件人的邮箱中选择要补救的邮件，并对邮件采取补救操作。

在邮箱中对邮件执行搜索和补救操作

开始之前

- 请确保已启用邮箱自动补救并在思科邮件安全网关上配置帐户设置。

- 在设备上启用邮件跟踪。请参阅设置集中邮件跟踪 ，第 2 页。
- 如果您使用的是集中邮件跟踪服务，请确保已在托管思科邮件安全网关上启用了 trailblazer 端口和 AsyncOS API HTTP 端口，并且思科内容安全管理设备可以访问该 trailblazer 端口。如果禁用 trailblazer 端口，请确保思科内容安全管理设备可以访问托管的思科邮件安全网关上的 AsyncOS API HTTP 端口。
- 如果受管思科邮件安全设备正在使用其证书颁发机构未存在于思科内容安全管理设备信任存储区中的证书，则内容安全管理设备上的服务器证书验证将失败。要允许通信，请将思科邮件安全设备使用的签名证书的证书颁发机构添加到思科内容安全管理设备。要添加证书颁发机构，请在 CLI 中使用 `certconfig` > `CERTAUTHORITY` 子命令。

  注意：如果要在内容安全管理设备上禁用服务器证书验证，请在 CLI 中使用 `esaapiconfig` 命令。出于安全考虑，思科不建议您禁用证书验证。

步骤 1 在安全管理设备上，单击设备新 Web 界面上的**跟踪 (Tracking)** 选项卡。

步骤 2 单击**邮件 (Messages)** 选项卡以缩小搜索结果范围。有关详细信息，请参阅在新 Web 界面上搜索邮件 ，第 5 页。

步骤 3 选择要补救的邮件。您一次最多可以选择 1000 封邮件。您只能补救处于已传送状态的邮件。

步骤 4 单击**补救 (Remediate)**。

步骤 5 输入下列详细信息：

- 输入补救的批处理名称。
- 选择以下任一补救操作：
  - 删除邮件。选择此选项可从最终用户的邮箱中永久删除邮件。
  - 转发到某个邮件地址。选择此选项可将邮件转发给指定用户，例如邮件管理员。
  - 转发到邮件地址并删除邮件。选择此选项可将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。

步骤 6 单击**应用 (Apply)**。

单击**应用 (Apply)** 后，您可以在“邮件跟踪”(Message Tracking) 页面的右下角查看“补救报告状态”(Remediation Report Status) 小组件。可使用此小组件来检查补救报告生成的状态。生成补救报告后，单击小组件上的查看详细信息 (View Details) 转至补救报告，以便查看补救结果。

注释 您还可以通过导航至 **报告 (Reports)** > **用户报告 (User Reports)** > > **补救报告 (Remediation Report)** 并单击“邮箱搜索和补救 (Mailbox Search And Remediate)” 选项卡来直接查看补救报告。

缩小结果集

在运行查询后，您可能发现结果集包括的信息比您需要的信息更多。请通过在结果列表中单击某行内的值缩小结果集，而不必创建新的查询。单击值会将该参数值添加为搜索中的一个条件。例如，

如果查询结果包括来自多个日期的邮件，请单击某行内的某个特定日期以仅显示在该日期收到的邮件。

步骤 1 将光标悬停在要添加为条件的值上方。该值以黄色突出显示。

使用以下参数值细化搜索：

- 日期和时间
- 邮件ID (MID)
- 主机（邮件安全设备）
- 发件人
- 接收方
- 邮件的主题行或主题的起始词语

步骤 2 [仅限新 Web 界面] 在邮件跟踪搜索条件中，单击**修改 (Modify)**。

使用以下参数值细化搜索：

- 日期和时间
- 邮件ID (MID)
- 思科主机（邮件安全设备）
- 发件人
- 接收方
- 邮件的主题行或主题的起始词语
- 邮件事件 (Message Event)
- 更多详细信息（邮件最后状态、SBRS、发件人 IP 和发件人组）

步骤 3 单击值以细化搜索。

“结果”(Results) 部分显示与原始查询参数和您添加的新条件相匹配的邮件。

步骤 4 如有必要，请在结果中单击其他值以进一步细化搜索。

Note 要删除查询条件，请单击**清除 (Clear)**，然后运行新的跟踪查询。

关于邮件跟踪和高级恶意软件防护功能

在“邮件跟踪”(Message Tracking) 中搜索文件威胁信息时，请记住以下几点：

- 要搜索由文件信誉服务找到的恶意文件，请在“邮件跟踪”(Message Tracking) 的“高级”(Advanced) 部分为“邮件事件”(Message Event) 选项选择**高级恶意软件防护阳性 (Advanced Malware Protection Positive)**。

- “邮件跟踪”(Message Tracking) 仅包括关于文件信誉处理的信息，以及在处理邮件时返回的原始文件信誉判定。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；
  - 邮件的整体最终高级恶意软件防护判定，以及
  - 发现包含恶意软件的任何附件。

    对于干净或不可扫描的附件，不提供任何信息。

- 判定更新仅在AMP判定更新报告中可用。系统不会使用判定更改来更新“邮件跟踪”(Message Tracking) 中的原始邮件详细信息。要查看具有特定附件的邮件，请在判定更新报告中单击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。

  有关已分析的文件的其他信息，可从云端获取。要查看某个文件的任何可用的文件分析信息，请依次选择**监控 (Monitor) > 文件分析 (File Analysis)**，然后输入 SHA-256 搜索该文件。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。

  如果设备处理了已送交分析的某个文件的后续实例，则这些实例将出现在邮件跟踪搜索结果中。

了解跟踪查询结果

如果结果不符合您的期望，请参阅邮件跟踪故障排除, on page 16。

跟踪查询结果列出了与跟踪查询中指定的条件相匹配的所有邮件。除“邮件事件”(Message Event) 选项外，查询条件是使用“AND”运算符添加的。结果集内的邮件必须满足所有“AND”条件。例如，如果您指定信封发件人以 J 开头，并且指定主题以 T 开头，则查询仅在这两个条件对于某封邮件而言都成立时才返回该邮件。

要查看关于邮件的详细信息，请单击新 Web 界面中的**更多详细信息 (More Details)** 链接，或单击旧 Web 界面中此邮件的**显示详细信息 (Show Details)**链接。有关详细信息，请参阅邮件详细信息, on page 13。

Note

- 具有50个或更多收件人的邮件将不会出现在跟踪查询结果中。该问题将在未来的版本中得到解决。
- [仅限新 Web 界面] 指定查询时，您可以向下滚动显示搜索结果。向下滚动时，视图中会显示更多结果。
- 您可以使用“搜索结果”部分上面的**导出**链接，将搜索结果导出至 .csv 文件。

  指定查询时，可以选择最多显示 1000 条搜索结果。要查看与您的搜索条件相匹配的多达 50000 封邮件，请在搜索结果部分的上方单击**全部导出 (Export All)** 链接，然后在另一个应用中打开生成的 .csv 文件。
- 如果单击了报告页面的链接来查看邮件跟踪中的邮件详细信息，但结果出现意外。如果查看期限内未同时和连续启用报告及跟踪，就可能出现这种情况。
- 有关打印或导出邮件跟踪搜索结果的信息，请参阅并导出报告和跟踪数据。

相关主题

邮件详细信息, on page 13

邮件详细信息

要查看有关特定邮件的详细信息，包括邮件头信息和处理详细信息，请为搜索结果列表中的任一项单击**更多详细信息**链接。系统将打开一个新窗口，其中显示邮件详细信息。

邮件详细信息包括以下部分：

判定图表和上次状态判定

“判定图表”显示邮件安全设备的每个引擎触发的各种可能判定的信息。

注释 12.0 之前的 AsyncOS 的判定图表不会显示，最后状态判定显示为“最后状态不可用”(Last State Not Available)。

下表显示了每个引擎的各种判定：

表 *1:* 判定图表

连接行为	邮件过滤器	反垃圾邮件	防病毒	AMP	Graymail	内容过滤器	病毒爆发过滤器	DLP
不适用 (Not Applicable) 已接受 已中继	未评估 匹配 不匹配	未评估 负 可疑 批量邮件 社交邮件 营销邮件 很好	未评估 负 已修复 已加密 无法扫描 很好	未评估 干净 FA 待处理 未知 已跳过 恶意 (Malicious) 不可扫描 (Unscannable) 低风险	未评估 负 很好	未评估 匹配 不匹配	未评估 匹配 不匹配	未评估 无触发器 违规 无违规

邮件的“上次状态”判定决定了在设备中每个引擎的所有可能判定之后触发的最终判定。

下面列出了一些上次状态判定：

- **已送达**：传送邮件时。
- **已丢弃**：丢弃邮件时。
- **已中止 (Aborted)**：邮件被中止时。（示例：由于邮件策略限制）
- **已退回**：邮件被退回时。
- **已拆分**：邮件 MID 拆分为多个 MID 且具有多个最终状态时。
- **已隔离 (Quarantined)**：邮件被引擎隔离时。
- **已排队 (Queued)**：当邮件排队等待传送到最终收件人/机下垃圾邮件隔离区或集中策略、病毒或病毒爆发隔离区时。
- **处理中**：邮件未被所有引擎完全处理时；或者邮件在特定引擎的队列中等待时。
- **最后状态不可用 (Last State Not Available)**：无法检索邮件的最后状态时。（示例：当消息仍由引擎处理且未达到任何最终状态时。

信封和信头概要

此部分显示来自邮件信封和信头的信息，例如信封发件人和收件人。该页面包括以下信息：

接收时间：邮件安全设备收到邮件的时间。

MID：邮件 ID。

主题 (Subject)：邮件的主题行。

如果邮件无主题或未将邮件安全设备配置为在日志文件中记录主题行，则跟踪结果中主题行的值可能是“（无主题）”。

信封发件人：SMTP 信封中的发件人地址。

信封收件人 (Envelope Recipients)：SMTP 信封中的收件人地址。

邮件ID 标题 (Message ID Header)：唯一地标识每封邮件的“Message-ID:”标题。首次创建邮件时，系统会将其插入邮件中。当您搜索特定邮件时，“Message-ID:”标题可能会非常有用。

思科主机：处理邮件的邮件安全设备。

经过 SMTP 身份验证的用户 ID：经过 SMTP 身份验证的发件人用户名（如果发件人使用了 SMTP 身份验证来发送邮件）。否则，该值为“N/A”。

附件 (Attachments)：附加到邮件的文件的名称。

发件人组：接收邮件的发件人组。

邮件大小： 邮件大小。

策略匹配项（传入或传出）：接收邮件的策略。

Note 如果引擎无法获取详细信息，此值将显示为"不适用"。

正在发送主机概要

反向 DNS 主机：反向 DNS (PTR) 查询验证的发送主机的主机名。

IP 地址 (IP Address)：发送主机的 IP 地址。

SBRS 得分：（SenderBase 信誉得分）。范围是 10（可能是可信的发件人）到 -10（明显是垃圾邮件发送者）。得分“无 (None)”表示处理该邮件时，无此主机的相关信息。

正在处理详细信息

此部分在处理邮件期间显示各种已记录的状态事件。

条目包括有关邮件策略处理的信息，例如反垃圾邮件和防病毒扫描，以及其他事件（例如邮件拆分）。

如果传送了邮件，则传送详细信息显示在此处。例如，邮件可能已传送，但副本保留在隔离区。

最后记录的事件会在处理详细信息中高亮显示。

“摘要”选项卡

此选项卡显示了处理邮件过程中所有事件的摘要日志。

与 DLP 匹配的内容 (DLP Matched Content) 选项卡

此选项卡显示违反数据丢失防护 (DLP) 策略的内容。

由于这些内容通常包括敏感信息，例如企业机密信息或个人信息（包括信用卡号码和健康记录），您可能想要禁止有权访问安全管理设备，但并非管理员级别访问权限的用户访问这些内容。请参阅控制对“邮件跟踪”中敏感信息的访问权限。

URL 详细信息选项卡

此选项卡仅向由 URL 信誉和 URL 类别内容过滤器以及病毒爆发过滤器（而非邮件过滤器）捕获的邮件显示。

此选项卡显示以下信息：

- 与 URL 关联的信誉得分或类别
- 对 URL 执行的操作（重写、去除或重定向）
- 如果邮件包含多个 URL，显示哪一个 URL 触发了过滤器操作。

仅当您将邮件安全设备配置为显示此信息时，您才可以看到此选项卡。请参阅《思科邮件安全设备 *AsyncOS* 用户指南》。

若要控制对此选项卡的访问，请参阅 控制对“邮件跟踪”中敏感信息的访问权限

SMTP 日志选项卡

此部分显示了邮件发件人 SMTP 身份验证失败时的邮件日志。

AMP 日志选项卡

此部分显示高级恶意软件保护文件信誉和文件分析服务捕获的邮件日志。

邮件跟踪故障排除

- 搜索结果中缺少预期邮件 , on page 16
- 搜索结果中不显示的附件 , on page 17

搜索结果中缺少预期邮件

问题

搜索结果中不包括本应满足条件的邮件。

解决方案

- 许多搜索的结果都取决于设备配置，特别是邮件事件搜索。例如，如果搜索未经过滤的URL类别，则找不到任何结果，即使邮件包含该类别的URL亦不例外。确认您是否已正确配置邮件安全设备来实现预期的行为。例如，检查邮件策略、内容和邮件过滤器及隔离区设置。
- 请参阅检查邮件跟踪数据的可用性 , on page 4。

搜索结果中不显示的附件

问题

搜索结果中找不到且未显示附件名称。

解决方案

在 ESA 上配置和启用至少一个入站内容过滤器或其他正文扫描功能。请参阅在旧 Web 界面上启用集中邮件跟踪, on page 2中的配置要求和跟踪服务概述中对附件名称搜索的限制。

导出邮件服务

您可以查看其他字段，以便使用“导出文件”(Export file) 选项以及邮件对相关邮件执行分析和调查。

步骤 1 选择**跟踪 (Tracking)** > **邮件 (Messages)**。

步骤 2 选择条件。

步骤 3 单击**导出 (Export)**。

您可以查看其他字段，以便使用“导出文件”(Export file) 选项以及邮件对相关邮件执行分析和调查。您可以查看的其他字段包括：

- “邮件大小”(Message Size) - 邮件大小。
- “附件详细信息”(Attachment Details) - 附加到邮件的文件的名称。
- “传送详细信息”(Delivery Details) - 传送信息，例如已退回的来自特定域的邮件数。
- “源 IP/FQDN”(Source IP/FQDN) - 发件人的 IP 地址。
- “发件人组”(Sender Group) - 接收邮件的发件人组。
- “DKIM、SPF 或 DMARC 状态”(DKIM, SPF, or DMARC Status) - 用于验证邮件是否由所有者实际发送的身份验证方式。
- “URL 列表”(URL List) - 思科安全邮件和 Web 管理器只会显示 1024 个字符的 URL。