邮件跟踪

本章包含以下部分：

邮件跟踪概览

邮件跟踪可提供邮件流的的详细视图，帮助解决支持中心呼叫。例如，如果邮件未能如期传送，您可以判断邮件是否包含病毒、被放入垃圾邮件隔离区，还是位于邮件流的其他位置。

您可以搜索一封匹配指定条件的特定电子邮件或一组邮件。

Note 使用邮件跟踪无法读取邮件内容。

启用邮件跟踪

Note 仅保留启用本功能之后所处理邮件的邮件跟踪数据。

准备工作

- 要在邮件跟踪中搜索和显示附件名称，并在日志文件中查看附件名称，您必须至少配置和启用一个正文扫描过程，例如邮件过滤器或内容过滤器。

- 日志文件必须配置为记录主题信头，才能实现按主题搜索。有关详细信息，请参阅日志记录。
- 如果要设置集中跟踪：请将思科安全管理器邮件和网络网关设置为支持对此邮件网关进行集中邮件跟踪。请参阅《思科安全邮件和网络管理器用户指南》。

Procedure

步骤 1 依次单击**安全服务 (Security Services) > 邮件跟踪 (Message Tracking)**。

即使您不计划集中使用此服务，也请使用此路径。

步骤 2 选择**启用邮件跟踪服务 (Enable Message Tracking Service)**。

步骤 3 如果在运行系统设置向导后首次启用邮件跟踪，请阅读最终用户许可协议，并单击**接受 (Accept)**。

步骤 4 选择邮件跟踪服务：

选项	说明
本地跟踪 (Local Tracking)	在此邮件网关上使用邮件跟踪。
集中跟踪 (Centralized Tracking)	使用思科安全管理器邮件和网络网关为包括本邮件网关在内的多个邮件安全设备跟踪邮件。

步骤 5 （可选）选中该复选框可保存被拒绝连接的信息。

为获得最佳性能，请禁用此设置。

步骤 6 提交并确认更改。

What to do next

如果您选择了本地跟踪：

- 选择可以访问 DLP 违规相关内容的用户。请参阅控制对“邮件跟踪”中敏感信息的访问权限。
- （可选）请调整用于存储邮件的磁盘空间分配。请参阅管理磁盘空间。

在旧界面上搜索邮件

Procedure

步骤 1 选择**监控 (Monitor) > 邮件跟踪 (Message Tracking)**

步骤 2 输入搜索条件。

- 要查看所有选项，请单击**高级 (Advanced)** 链接。

- 跟踪不支持通配符或正则表达式。
- 跟踪搜索不区分大小写。
- 查询是“AND”搜索，除非另行说明：查询返回满足搜索字段中指定的所有条件的邮件。例如，如果为信封收件人和主题行参数指定文本字符串，查询将仅返回与指定信封收件人和主题行的两者匹配的邮件。
- 搜索条件包括：

选项	说明
信封发件人 (Envelope Sender)	选择**起始字符 (Begins With)**、**为 (Is)** 或**包含 (Contains)**，然后输入要查找邮件发件人的邮件地址、用户名或域。 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**起始字符 (Begins With)**、**为 (Is)** 或**包含 (Contains)**，然后输入要查找邮件收件人的邮件地址、用户名或域。 您可以输入任何字符。不执行条目验证。
主题 (Subject)	选择**开头 (Begins With)**、**是 (Is)** 或**包含 (Contains)**，然后在邮件主题行中输入要搜索的文本字符串。 **警告**：不要在法规禁止这类跟踪的环境中使用此种搜索。
邮件接收时间 (Message Received)	指定日期和时间范围。 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。 使用邮件网关收到邮件的本地日期和时间。
高级选项：	
发件人 IP 地址/域/网络所有者 (Sender IP Address/ Domain / Network Owner)	指定远程主机的 IP 地址、域或网络所有者。 您可以仅在被拒连接中搜索，也可以搜索所有邮件。

选项	说明
附件 (Attachment)	选择**开头 (Begins With)**、**是 (Is)** 或**包含 (Contains)**，然后输入要查找的一个附件的 ASCII 或 Unicode 文本字符串。系统不删除所输入文本的前导空格和结尾空格 只有执行下列操作后，才能按附件文件名搜索邮件： • 使用邮件过滤器扫描正文 • 使用内容过滤器扫描正文 • 高级恶意软件防护 (AMP) 扫描。 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。 您可以根据威胁名称搜索被高级恶意软件保护引擎检测为恶意的邮件。在**威胁名称**字段中，输入 *Simple_Custom_ Detection* 或 *Custom_Threshold*，根据“自定义检测”和“自定义阈值”类别搜索被检测为恶意的邮件。如果某个特定文件被高级恶意软件保护引擎检测为携带病毒，您也可以按病毒名称搜索邮件。
邮件事件 (Message Event)	选择一个或多个邮件处理事件。例如，您可以搜索已传送、被隔离或硬退回的邮件。 使用“OR”运算符添加邮件事件：选择多个事件查找满足任何指定条件的邮件。
邮件 ID 信头 (Message ID Header)	输入 SMTP 邮件 ID 信头的文本字符串。 此 RFC 822 邮件信头是邮件的唯一标识，初次创建邮件时，即在邮件中插入该信头。
思科 IronPort MID (Cisco IronPort MID)	输入要搜索的邮件编号。IronPort MID 唯一标识邮件网关上的每封邮件。
思科 IronPort 主机 (Cisco IronPort Host)	选择一台邮件安全设备，将邮件搜索范围限制为该邮件网关处理的邮件，或选择所有邮件网关。

步骤 3 单击**搜索 (Search)** 提交查询。

查询结果将显示在页面底部。

What to do next

相关主题

- 处理邮件跟踪搜索结果 , on page 7

在新 Web 界面上搜索邮件

邮件网关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。

过程

步骤 1　单击**跟踪 (Tracking)** 选项卡。

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。在邮件网关上查看日期和时间时，它们将按邮件网关的本地时间显示。

  只有邮件网关中已记录邮件，且思科安全邮件和网络网关检索到邮件时，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。

  如果对邮件网关上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网关中进行搜索，或从下拉菜单中选择所需的邮件网关。
- **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。例如，您可以搜索已传送、被隔离或硬退回的邮件。使用“OR”运算符添加邮件事件：选择多个事件查找满足任何指定条件的邮件。

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 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。

下一步做什么

- 处理邮件跟踪搜索结果 ， 第 7 页

处理邮件跟踪搜索结果

请注意以下问题：

- 只有邮件网关中已记录邮件，且思科安全管理器邮件和网络网关检索到邮件时，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。
- 有关涉及高级恶意软件防护的搜索（文件信誉扫描和文件分析）的信息，请参阅关于邮件跟踪和高级恶意软件保护功能。

使用搜索结果可以执行以下操作：

- 显示超过 250 个搜索结果，方法是返回搜索条件，单击“高级”(Advanced)，滚动到“查询设置”(Query Settings)，然后将结果最大数量设为 1000。
- 从搜索结果部分的右上角选择选项，可在每页显示更多结果。
- 从搜索结果部分的右上角在多个搜索结果页面之间导航。
- 将光标悬停在搜索结果中要添加为条件的某一值上，可缩小搜索结果范围。显示橙色高亮时，可以单击该值按该条件缩小搜索范围。可通过此操作在搜索条件中添加更多条件。例如，如果搜索发送到特定收件人的邮件，可以单击搜索结果中的发件人姓名，查找在最初指定的时间范围内从该发件人发送给该收件人（并满足任何其他条件）的所有邮件。
- 如果超过1000封邮件匹配您的搜索条件，则您可以单击“全部导出”（位于搜索结果部分右上角的链接），将多达 50,000 个搜索结果导出为逗号分隔值文件，并在其他应用中处理这些数据。
- 在邮件行中单击“显示详细信息”(Show Details) 可查看该邮件的更多详细信息。系统随即打开新的浏览器窗口，显示邮件的详细信息。
- 对于已隔离的邮件，可以单击邮件跟踪搜索结果中的链接，查看邮件被隔离的原因等详细信息。
- 使用“邮箱搜索和补救”操作来补救用户邮箱中的恶意邮件。有关详细信息，请参阅在邮箱中搜索和补救邮件

Note 如果单击报告页面上的链接来查看邮件跟踪中的邮件详细信息，但结果没有达到预期，这可能是因为查阅时没有同时启用报告和跟踪。

相关主题

- 邮件跟踪详细信息 , on page 8

邮件跟踪详细信息

项目	说明
信封和信头概要部分：	
接收时间	邮件网关收到邮件的时间。 日期和时间显示为邮件网关上配置的本地时间。
MID	唯一 IronPort 邮件 ID。
消息大小	邮件的大小
主题	邮件的主题行。 如果邮件没有主题，或如果日志文件未配置为记录主题信头，跟踪结果中主题行的值可能为“（无主题）”。有关详细信息，请参阅日志记录
信封发件人	SMTP 信封中的发件人地址。
信封收件人	如果部署使用别名表进行别名扩展，搜索将查找扩展的收件人地址，而不是原始信封地址。有关别名表的详细信息，请参阅“配置路由和传送功能”一章中的“创建别名表”。 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。
邮件 ID 信头	RFC 822 邮件信头。
SMTP 身份验证用户 ID	发件人的 SMTP 身份验证用户名，如果发件人使用 SMTP 身份验证发送邮件。否则，该值为“N/A”。

项目	说明
附件	附加到邮件的文件的名称。 搜索结果中将显示采用查询的名称，且至少包含一个附件的邮件。 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。附件名称不会出现在搜索结果中的情况包括（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。 由于性能原因，不会搜索附件中文件的名称，例如 OLE 对象或 ZIP 文件等存档。
[仅限新 Web 界面] **邮件事件**	选择多个事件以包含与各个事件类型匹配的邮件。
发送主机摘要部分	
反向 DNS 主机名	发送主机的名称，由反向 DNS (PTR) 查找验证。
IP 地址	发送主机的 IP 地址
IP 信誉**得分**	IP 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。 有关 IP 信誉服务的详细信息，请参阅邮件网关的IP 信誉过滤
处理详细信息部分	
摘要信息 （如果显示下面选项卡之一，则此信息将显示在某个选项卡中。摘要信息始终显示。）	“摘要”选项卡显示处理邮件过程中记录的状态事件。 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（邮件分流和内容或邮件过滤器添加的自定义日志条目等）。 如果邮件已传送，则显示传送的详细信息。 处理详细信息中将突出显示最后记录的事件。

项目	说明
“DLP 匹配内容”(DLP Matched Content) 选项卡	仅对 DLP 策略捕获的邮件显示此选项卡。 此选项卡包括匹配相关信息，以及触发 DLP 策略匹配的敏感内容。 必须配置邮件网关才能显示此信息。请参阅在邮件跟踪中显示敏感 DLP 数据。 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。
“URL 详细信息”(URL Details) 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。 必须配置邮件网关才能显示此信息。请参阅在邮件跟踪中显示 URL 详细信息。 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。

相关主题

- 在旧界面上搜索邮件 , on page 2

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。

Procedure

步骤 1 [仅限新 Web 界面] 单击页面右上角的齿轮图标以加载旧 Web 界面。

步骤 2 依次选择**监控 (Monitor) > 邮件跟踪 (Message Tracking)**。

步骤 3 在搜索框的右上角查找**数据时间范围：**。

步骤 4 单击**数据时间范围: (Data in time range:)** 的值。

What to do next

相关主题

- 关于邮件跟踪和升级 , on page 11

关于邮件跟踪和升级

全新的邮件跟踪功能可能不适用于在升级前处理的邮件，因为可能没有为这些邮件保留所需的数据。有关邮件跟踪数据和升级的可能限制，请参阅所用版本的版本说明。

邮件跟踪故障排除

相关主题

- 搜索结果中不显示的附件 , on page 11
- 搜索结果中缺少预期邮件 , on page 11

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

请参阅启用邮件跟踪, on page 1（）中的配置要求。另请参阅邮件跟踪详细信息 , on page 8中的附件名称搜索限制。

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

- 搜索的结果，特别是涉及邮件事件的搜索，取决于您的邮件网关配置。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网关来实现预期的行为。例如，检查邮件策略、内容和邮件过滤器及隔离区设置。
- 如果单击报告中的链接后缺少预期的信息，请参阅邮件报告故障排除。