使用集中邮件安全报告

本章包含以下部分：

集中邮件报告概述

您的思科安全邮件和Web管理器设备显示来自单台或多台邮件安全设备的汇聚信息，以便您可以监控邮件流量模式和安全风险。可以实时运行报告来查看特定时间段内系统活动的交互显示，也可以安排并定期运行报告。此外，报告功能还可将原始数据导出到文件。

此功能将集中显示邮件安全设备的“监控 (Monitor)”菜单下列出的报告。

“集中邮件报告”(Centralized Email Reporting) 功能不仅可生成概要报告，使您可以了解网络上发生的情况，而且还使您可以深入分析并查看特定域、用户或类别的流量详细信息。

使用“集中跟踪”(Centralized Tracking) 功能可以跟踪跨越多台邮件安全设备的邮件。

Note 邮件安全设备仅在使用本地报告时才存储数据。如果为邮件安全设备启用了集中报告，则邮件安全设备不会保留任何报告数据（系统容量和系统状态除外）。如果未启用集中邮件报告，则仅会生成系统状态和系统容量报告。

有关过渡到集中报告期间或之后的时间报告数据可用性的详细信息，请参阅邮件安全设备的文档或在线帮助的“集中报告模式”部分。

设置集中邮件报告

要设置集中邮件报告，请按顺序完成以下操作程序：

1. 启用集中邮件报告, on page 2
2. [仅适用于旧 Web 界面] 创建邮件报告组, on page 4。
3. 将集中邮件报告服务添加到每台受管邮件安全设备 , on page 4
4. 在邮件管理设备上启用集中邮件报告 , on page 5

Note 如果报告和跟踪没有一致且同时启用且不能正常运行，或者没有一致且同时地在每个邮件安全设备上进行集中或本地存储，则深入了解报告时获得的邮件跟踪结果与预期结果不匹配。这是因为仅当启用了各个功能（报告、跟踪）时才会捕获该功能的数据。

启用集中邮件报告

- 在旧 Web 界面上启用集中邮件报告， 第 2 页
- 在新 Web 界面上启用集中邮件报告

在旧 Web 界面上启用集中邮件报告

Before you begin

- 在启用集中报告之前，应配置所有邮件安全设备并确保其按预期工作。
- 启用集中邮件报告之前，请确保为该服务分配了足够的磁盘空间。请参阅管理磁盘空间。

步骤 1 选择管理设备 **(Management Appliance)** > 集中服务 **(Centralized Services)** > 邮件 **(Email)** > 集中报告 **(Centralized Reporting)**。

步骤 2 点击启用 **(Enable)**。

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报告，请查看最终用户许可协议，然后点击**接受 (Accept)**。

步骤 4 提交并确认更改。

Note 如果您已在设备上启用邮件报告，但未为此操作分配磁盘空间，则在分配磁盘空间之前，集中邮件报告功能将无法正常工作。只要您为“邮件报告和跟踪”(Email Reporting and Tracking) 设置的配额超过当前已用的磁盘空间，就不会丢失任何报告和跟踪数据。有关更多信息，请参阅管理磁盘空间部分。

What to do next

创建邮件报告组, on page 4

在新 Web 界面上启用集中邮件报告

Before you begin

- 在启用集中报告之前，应配置所有邮件安全设备并确保其按预期工作。
- 启用集中邮件报告之前，请确保为该服务分配了足够的磁盘空间。请参阅管理磁盘空间。

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

步骤 2 点击**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报告，请查看并接受许可协议，然后点击**继续 (Proceed)**。

步骤 4 点击切换开关以启用集中邮件报告。

步骤 5 创建邮件报告组：

a) 点击 + 图标以添加组。

b) 为组输入一个唯一的名称。

邮件安全设备列表会显示您添加到安全管理设备的邮件安全设备。选择要添加到组的设备。

可以添加的组的最大数量小于或等于可以连接的邮件设备的最大数量。

Note 如果将邮件安全设备添加到了安全管理设备，但该设备并未显示在列表中，则编辑邮件安全设备的配置，以便安全管理设备从其收集报告数据。

c) 点击**添加 (Add)** 以将设备添加到“组成员”(Group Members) 列表。

步骤 6 点击**提交 (Submit)**。

What to do next

有关管理报告组的详细信息，请参阅将集中邮件报告服务添加到每台受管邮件安全设备 , on page 4。

创建邮件报告组

可以从安全管理设备创建要查看其报告数据的邮件安全设备组。

一个组可以包含一个或多个设备，而一个设备可以属于多个组。

Before you begin

Note 本部分仅适用于旧 Web 界面。

请确保为每台设备启用了集中报告。请参阅将集中邮件报告服务添加到每台受管邮件安全设备 , on page 4。

步骤 1 选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 集中报告 (Centralized Reporting)**。

步骤 2 点击**添加组 (Add Group)**。

步骤 3 为组输入一个唯一的名称。

邮件安全设备列表会显示您添加到安全管理设备的邮件安全设备。选择要添加到组的设备。

可以添加的组的最大数量小于或等于可以连接的邮件设备的最大数量。

Note 如果将邮件安全设备添加到了安全管理设备，但该设备并未显示在列表中，则编辑邮件安全设备的配置，以便安全管理设备从其收集报告数据。

步骤 4 点击**添加 (Add)** 以将设备添加到“组成员”(Group Members) 列表。

步骤 5 提交并确认更改。

What to do next

将集中邮件报告服务添加到每台受管邮件安全设备 , on page 4

将集中邮件报告服务添加到每台受管邮件安全设备

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，点击 ⚙ 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**集中报告 (Centralized Reporting)** 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，键入设备名称和安全管理设备管理接口的 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) 集中报告服务已预先选中。
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 单击**提交 (Submit)**。

步骤 6 为要启用集中报告的每个邮件安全设备重复执行此程序。

步骤 7 确认您的更改。

What to do next

在邮件管理设备上启用集中邮件报告 , on page 5

在邮件管理设备上启用集中邮件报告

必须在每个托管的邮件安全设备上启用集中邮件报告。

有关说明，请参阅邮件安全设备的文档或在线帮助的“配置邮件安全设备以使用集中报告”部分。

处理邮件报告数据

- 有关访问和查看报告数据的选项，请参阅查看报告数据的各种方法。
- 要自定义报告数据您的视图，请参阅自定义报告数据的视图。
- 要在您的数据中搜索特定信息，请参阅搜索与交互式邮件报告页面 , on page 6。
- 要打印或导出报告信息，请参阅并导出报告和跟踪数据。
- 要了解各个交互式报告页面，请参阅了解“邮件报告”页面, on page 7。

- 要按需生成报告，请参阅按需生成邮件报告 , on page 105。
- 以安排报告在您指定的时间间隔和时间自动运行，请参阅计划邮件报告, on page 103。
- 要查看已存档的按需报告和计划报告，请参阅查看和管理已存档的邮件报告 , on page 106。
- 有关背景信息，请参阅安全管理设备如何收集报告的数据。
- 要在处理大量数据时提高性能，请参阅提高邮件报告的性能。
- 要获取有关图表或表中显示为蓝色链接的实体或数字的详细信息，请点击该实体或数字。

  例如，如果您的权限允许您执行此操作，您可以使用此功能查看有关违反内容过滤策略或防数据丢失策略的邮件的详细信息。这样做会在“邮件跟踪”(Message Tracking) 中执行相关的搜索。向下滚动以查看搜索结果。

使用旧 Web 界面上的邮件报告数据

- 有关访问和查看报告数据的选项，请参阅查看报告数据的各种方法。
- 要自定义报告数据您的视图，请参阅自定义报告数据的视图。
- 要打印或导出报告信息，请参阅并导出报告和跟踪数据。
- 要了解各个交互式报告页面，请参阅使用交互式报告页面。
- 要按需生成报告，请参阅按需生成邮件报告 ， 第 105 页。
- 以安排报告在您指定的时间间隔和时间自动运行，请参阅计划邮件报告 ， 第 103 页。
- 要查看已存档的按需报告和计划报告，请参阅查看和管理已存档的邮件报告 ， 第 106 页。
- 有关背景信息，请参阅安全管理设备如何收集报告的数据。
- 要在处理大量数据时提高性能，请参阅提高邮件报告的性能。
- 要获取有关图表或表中显示为蓝色链接的实体或数字的详细信息，请点击该实体或数字。

  例如，如果您的权限允许您执行此操作，您可以使用此功能查看有关违反内容过滤策略或防数据丢失策略的邮件的详细信息。这样做会在“邮件跟踪”(Message Tracking) 中执行相关的搜索。向下滚动以查看搜索结果。

搜索与交互式邮件报告页面

许多交互式邮件报告页面均在页面底部包含“**搜索：**”**(Search For:)** 下拉菜单。

从下拉菜单中，您可以搜索多种类型的条件，包括以下条件：

- IP 地址
- 域 (Domain)
- 网络所有者 (Network owner)

- 内部用户 (Internal User)
- 目标域 (Destination domain)
- 内部发件人域 (Internal sender domain)
- 内部发件人 IP 地址 (Internal sender IP address)
- 传入 TLS 域 (Incoming TLS domain)
- 传出 TLS 域 (Outgoing TLS domain)
- SHA-256

对于大多数搜索，请选择是要精确匹配搜索文本还是查找以输入的文本开头的项（例如，以“ex”开头将匹配“example.com”）。

对于 IPv4 搜索，输入的文本始终会解释为点分十进制格式的多达四组 IP 八位二进制数。例如，“17”将在范围 17.0.0.0 至 17.255.255.255 中搜索，因此它将匹配 17.0.0.1，但不匹配 172.0.0.1。对于精确匹配搜索，请输入所有四组二进制八位数。IP 地址搜索还支持无类别域间路由 (CIDR) 格式 (17.16.0.0/12)。

对于 IPv6 搜索，您可以使用以下示例中的格式输入地址：

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

了解“邮件报告”页面

Note 此列表显示邮件安全设备的 AsyncOS 最新支持版本中可用的报告。如果您的邮件安全设备运行的是早期版本的 AsyncOS，并非上述所有报告均可用。

Table 1: 邮件报告选项卡选项

邮件报告菜单	操作
“邮件报告概述”页面	“概述”(Overview) 页面提供您的邮件安全设备上的活动的概要。它包括传入和传出邮件的图和摘要表。 有关详细信息，请参阅“邮件报告概述”页面, on page 14。
“传入邮件”页面	“传入邮件”(Incoming Mail) 页面为连接到您的托管邮件安全设备的所有远程主机提供实时信息的交互报告。您可以收集有关发送邮件到您的系统的 IP 地址、域和网络所有者（组织）的信息。 有关详细信息，请参阅“传入邮件”(Incoming Mails) 页面, on page 17。

邮件报告菜单	操作
“发件人组 (Sender Groups)”报告页面	“发件人组报告”(Sender Groups report) 页面按发件人组和邮件流策略操作提供连接摘要，允许您查看 SMTP 连接和邮件流策略趋势。 有关详细信息，请参阅“发件人组 (Sender Groups)”报告页面, on page 21。
“发件人域信誉”页面	您可以使用此报告页面，根据从 SDR 服务接收的判定和威胁类别查看传入邮件 有关详细信息，请参阅“发件人域信誉”页面, on page 21。
“外发目标”(Outgoing Destinations) 页面	“外发目标”(Outgoing Destinations) 页面提供有关您的组织将邮件发送到的各个域的信息。页面顶部包括按传出威胁邮件描绘外发目标排行榜的图形，以及按传出正常邮件描绘外发目标排行榜的图形。页面底部显示一个按收件人总数对列排序（默认设置）的图表。 有关详细信息，请参阅“外发目标”(Outgoing Destinations) 页面, on page 22。
“传出邮件发件人”页面	“传出邮件发件人”(Outgoing Senders) 页面提供有关从网络中的 IP 地址和域发送的邮件的数量和类型的信息。 有关详细信息，请参阅“传出邮件发件人”页面, on page 23。
“内部用户”页面	“内部用户”(Internal Users) 按邮件地址提供有关您的内部用户发送和接收的邮件的信息。 单个用户可以具有多个邮件地址。报告中未合并邮件地址。 有关详细信息，请参阅“内部用户”页面, on page 24。
DLP 事件	“DLP 事件摘要”(DLP Incident Summary) 页面显示传出邮件中发生的防数据丢失 (DLP) 策略违规事件的信息。 有关详细信息，请参阅DLP 事件 , on page 26。
邮件过滤器	“邮件过滤器”(Message Filters) 页面显示有关传入和传出邮件的邮件过滤器匹配项排行榜的信息（那些邮件过滤器具有最大数量的匹配邮件）。 有关更多信息，请参阅 邮件过滤器 , on page 27
地理分布	“地理分布”页面显示： • 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。 • 以表格格式显示的基于源国家/地区的传入邮件连接总数。 有关详细信息，请参阅地理分布, on page 28。

邮件报告菜单	操作
大量邮件	“大量邮件”(High Volume Mail) 页面列出涉及来自单个发件人的大量邮件的攻击或在移动一小时期间内具有相同对象的攻击。 有关详细信息，请参阅大量邮件 , on page 28。
“内容过滤器”(Content Filters) 页面	“内容过滤器”(Content Filters) 页面显示有关传入和传出内容过滤器匹配项排行榜的信息（那些内容过滤器具有最多的匹配邮件）。该页面还以条形图和列表形式显示数据。使用“内容过滤器(Content Filters)”页面，可以按内容过滤器或用户查看企业策略。 有关详细信息，请参阅“内容过滤器”(Content Filters) 页面, on page 28。
DMARC 验证	“DMARC 验证”(DMARC Verification) 页面显示未通过基于域的邮件身份验证、报告和一致性 (DMARC) 验证的发件人域排行榜，并显示对来自每个域的传入邮件执行的各项操作的摘要。 有关详细信息，请参阅DMARC 验证 , on page 29。
宏检测	“宏检测”(Macro Detection) 报告页显示内容或邮件过滤器检测到的启用宏的传入和传出附件排行榜。 有关更多信息，请参阅 宏检测, on page 29
“外部威胁源”页面	“外部威胁源”(External Threat Feeds) 页面显示下列报告： • 排名靠前的用于检测邮件威胁的 ETF 来源。 • 排名靠前的与检测到的邮件威胁相匹配的 IOC。 • 排名靠前的用于过滤恶意传入邮件连接的 ETF 来源 有关详细信息，请参阅“外部威胁源”(External Threat Feeds) 页面, on page 30。
“病毒类型”(Virus Types) 页面	“病毒类型 (Virus Types)”页面提供发送至网络以及从网络发出的病毒的概述。“病毒类型 (Virus Types)”页面显示已由运行于邮件安全设备之上的病毒扫描引擎检测到并且显示在安全管理设备上的病毒。使用此报告针对特定病毒采取相应措施。 有关详细信息，请参阅“病毒类型”(Virus Types) 页面, on page 30。
“URL 过滤”页面	使用此页面可以查看邮件中出现最频繁的 URL 类别、垃圾邮件中最常见的 URL 以及邮件中可见的恶意和可疑 URL。 有关详细信息，请参阅“URL 过滤”页面 , on page 31。

邮件报告菜单	操作
“网络交互跟踪”页面	标识单击了由策略或病毒爆发过滤器重写的 URL 的最终用户，以及与每次用户单击相关联的操作。 有关详细信息，请参阅“网络交互跟踪”(Web Interaction Tracking) 页面, on page 32。
“伪造邮件检测”页面	“伪造邮件检测”页面包括以下报告： • **排名靠前的伪造邮件检测**。显示内容字典中与传入邮件中的伪造“发件人：”信头匹配的前十个用户。 • **伪造邮件检测：详细信息**。显示内容词典中与传入邮件中的伪造“发件人：”信头匹配所有用户的列表，对于给定用户，还会显示匹配的邮件的数量。 请参阅“伪造邮件检测”(Forged Email Detection) 页面, on page 33。
安全打印	您可以使用“安全打印”(Safe Print) 报告页面查看： • 以图形格式显示的基于文件类型的安全打印附件的数量。 • 基于表格格式的文件类型的安全打印附件摘要。 有关详细信息，请参阅“安全打印”(Safe Print) 页面 , on page 33。
高级网络钓鱼防护页面	您可以在“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面上查看以下内容： • 已成功转发到思科高级网络钓鱼防护云服务的邮件总数。 • 未转发到思科高级网络钓鱼防护云服务的邮件总数。 有关详细信息，请参阅传统 Web 界面上的高级网络钓鱼防护页面, on page 33。
“高级恶意软件防护”（文件信誉和文件分析）报告页面	有三个显示文件信誉和分析数据的报告页面。 有关详细信息，请参阅“高级恶意软件防护”（文件信誉和文件分析）报告页面 , on page 34。
邮箱自动补救	使用此页面可查看邮箱补救结果的详细信息。 请参阅邮箱自动补救, on page 39
“TLS 连接”页面	“TLS 连接 (TLS Connections)”页面显示所收发邮件的 TLS 连接的整体使用情况。该报告还显示使用 TLS 连接发送邮件的每个域的详细信息。 有关详细信息，请参阅“TLS 连接”页面, on page 40。

邮件报告菜单	操作
入站 SMTP 身份验证页面	“入站 SMTP 身份验证”(Inbound SMTP authentication) 页面显示了使用客户端证书和“SMTP AUTH”命令对邮件安全设备与用户的邮件客户端之间的 SMTP 会话进行身份验证。 有关详细信息，请参阅入站 SMTP 身份验证页面, on page 41。
“病毒爆发过滤器”页面	“病毒爆发过滤器”(Outbreak Filters) 页面显示了有关最近的病毒爆发和由病毒爆发过滤器隔离的邮件的信息。使用此页面可监控针对病毒攻击的防御。 有关详细信息，请参阅“爆发过滤器”(Outbreak Filters) 页面, on page 42。
速率限制页面	“速率限制”(Rate Limits) 页面显示了超过您为每个发件人的邮件收件人数量设置的阈值的邮件发件人（根据MAIL-FROM地址）。 有关详细信息，请参阅速率限制页面 , on page 41。
系统容量页面	可用于查看将报告数据发送到安全管理设备的总体工作负载。 有关详细信息，请参阅系统容量页面, on page 44。
报告数据可用性 (Reporting Data Availability) 页面	可用于概括了解报告数据对每个设备上的安全管理设备的影响。有关详细信息，请参阅报告数据可用性 (Reporting Data Availability) 页面, on page 47。
计划邮件报告	允许您为指定时间范围安排报告。有关详细信息，请参阅计划邮件报告, on page 103。
查看和管理已存档的邮件报告	使您可以查看和管理已存档的报告。有关详细信息，请参阅查看和管理已存档的邮件报告 , on page 106。 还使您可以生成按需报告。请参阅按需生成邮件报告 , on page 105。

邮件报告页面的表列说明

Table 2: 邮件报告页面的表列说明

列名	
传入邮件的详细信息	
已拒绝连接数 (Connections Rejected)	由 HAT 策略阻止的所有连接。当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。
已接受连接数 (Connections Accepted)	所有已接受的连接。

列名	
尝试的总数 (Total Attempted)	已尝试的所有已接受和已阻止的连接。
由发件人限制拦截 (Stopped by Recipient Throttling)	这是“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 的一个组件。表示由于超出下列任何 HAT 限制而拦截的收件人邮件的数量：每小时的最大收件人数、每封邮件的最大收件人数或每个连接的最大邮件数。此值加上与被拒绝或被 TCP 拒绝的收件人邮件估算值就得到了“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 的值。
由 IP 信誉过滤拦截	“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 的值根据多个因素进行计算： • 来自此发件人的“受限制”邮件数 • 已拒绝或 TCP 拒绝的连接数（可能是部分计数） • 每个连接的邮件数量的保守倍数 当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。在这种情况下，显示的值可以解释为“下限”，即至少已拦截这么多邮件。 **Note** “概述”(Overview) 页面上的“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 总计始终基于所有已拒绝的连接的完整计数。只有每个发件人的连接计数会因负载而受到限制。
作为无效收件人拦截 (Stopped as Invalid Recipients)	由会话 LDAP 拒绝和所有 RAT 拒绝予以拒绝的所有邮件收件人。
由域信誉过滤拦截	根据发件人域的信誉来判定阻止的邮件总数。
检测到的垃圾邮件 (Spam Detected)	检测到的任何垃圾邮件。
检测到的病毒 (Virus Detected)	检测到的任何病毒
内容过滤器拦截	由内容过滤器拦截的邮件总数。
威胁邮件总数 (Total Threat)	威胁邮件总数（由信誉拦截、作为无效收件人拦截、垃圾邮件以及病毒）
市场营销部门	被检测为不需要的营销邮件的邮件数。

列名	
正常 (Clean)	所有正常邮件。 未启用灰色邮件功能的设备上处理的邮件被计为正常邮件。
用户邮件流详细信息（内部用户页面）	
检测到的传入垃圾邮件 (Incoming Spam Detected)	检测到的所有传入垃圾邮件
检测到的传入病毒 (Incoming Virus Detected)	检测到的传入病毒。
传入邮件内容过滤器匹配数 (Incoming Content Filter Matches)	检测到的传入内容过滤器匹配项。
由内容过滤器拦截的传入邮件 (Incoming Stopped by Content Filter)	由已设置的内容过滤器拦截的传入邮件。
传入的正常邮件 (Incoming Clean)	所有传入的正常邮件。
检测到的传出垃圾邮件 (Outgoing Spam Detected)	检测到的传出垃圾邮件。
检测到的传出病毒 (Outgoing Virus Detected)	检测到的传出病毒。
传出邮件内容过滤器匹配数 (Outgoing Content Filter Matches)	检测到的传出内容过滤器匹配项。
由内容过滤器拦截的传出邮件 (Outgoing Stopped by Content Filter)	由已设置的内容过滤器拦截的传出邮件。
传出的正常邮件 (Outgoing Clean)	所有传出的正常邮件。
传入和传出的 TLS 连接：“TLS 连接”(TLS Connections) 页面	
必需的 TLS：失败 (Required TLS: Failed)	失败的所有必需的 TLS 连接。
必需的 TLS：成功 (Required TLS: Successful)	成功的所有必需的 TLS 连接。
首选的 TLS：失败 (Preferred TLS: Failed)	失败的所有首选的 TLS 连接。
首选的 TLS：成功 (Preferred TLS: Successful)	成功的所有首选的 TLS 连接。
总连接数 (Total Connections)	TLS 连接的总数。
邮件总数 (Total Messages)	TLS 邮件的总数。
爆发过滤器	
病毒爆发名称	病毒爆发的名称。
病毒爆发 ID	病毒爆发 ID。

列名	
全局首见时间 (First Seen Globally)	在全局首次发现病毒的时间。
保护时间 (Protection Time)	保护病毒的时间。
隔离的邮件 (Quarantined Messages)	与隔离区相关的邮件。

“邮件报告概述”页面

安全管理设备上的**邮件 > 报告 > 概述**页提供您的邮件安全设备的邮件消息活动的概要。“概述 (Overview)”页面包括传入邮件和传出邮件的图形和摘要表。

概述 (Overview) 页面概要显示了传入和传出邮件图形，以及传入和传出邮件摘要。

邮件趋势图以可视化方式表示了邮件流。可以使用该页面上的邮件趋势图监控进出设备的所有邮件的流量。

Note “基于域的执行摘要”(Domain-Based Executive Summary) 报告和“执行摘要”(Executive Summary report) 报告基于“邮件报告概述”页面, on page 14。有关详细信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告, on page 100和“执行摘要”报告 , on page 103

Table 3: “邮件”>“报告”>“概述”页面上的详细信息

部分	说明
时间范围	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看以下项的数据 (View Data for)	选择要查看其概述数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。

如何对传入邮件计数

传入邮件的计数取决于每封邮件的收件人数。例如，从 example.com 发送给三个收件人的一封传入邮件被计为来自该发件人的三封邮件。

由于由发件人信誉过滤拦截的邮件不会实际进入工作队列，因此设备无权访问传入邮件的收件人列表。在此情况下，将使用倍数来估算收件人的数量。此倍数基于对大量现有客户数据样本的研究。

设备如何对邮件分类

由于邮件持续通过邮件管道，因此其可以应用于多个类别。例如，邮件可以标记为垃圾邮件或病毒邮件；它还可以与内容过滤器相匹配。各种过滤器和扫描活动的优先顺序会极大地影响邮件处理的结果。

在上面的示例中，各种判定遵循以下优先顺序规则：

- 垃圾邮件
- 病毒邮件
- 匹配内容过滤器

按照这些规则，如果某个邮件被标记为具有垃圾邮件特征，并且您的反垃圾邮件设置被设置为丢弃具有垃圾邮件特征的邮件，则该邮件将被丢弃，垃圾邮件计数器会增加。

此外，如果反垃圾邮件设置被设置为允许具有垃圾邮件特征的邮件继续在邮件通道中通行，并且后续内容过滤器将会丢弃、退回或隔离该邮件，则垃圾邮件计数器仍会增加。仅当该邮件不具有垃圾邮件或病毒特征时，内容过滤器才会增加。

或者，如果邮件被爆发过滤器隔离，则在该邮件从隔离中释放出来并再次进入工作队列之前，不会进行计数。

有关邮件处理优先级的完整信息，请参阅邮件安全设备在线帮助或用户指南中有关邮件通道的章节。

在“概述”(Overview) 页面上对邮件进行分类

“概述”(Overview) 报告页面上的“传入邮件摘要”(Incoming Mail Summary) 中报告的邮件按以下所述进行分类：

Table 4: *“概述”(Overview) 页面上的邮件类别*

类别	说明
由 IP 信誉过滤拦截	由 HAT 策略拦截的所有连接乘以固定倍数（请参阅如何对传入邮件计数, on page 14），加上由收件人限制拦截的所有收件人。 “由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 的值根据多个因素进行计算： • 来自此发件人的“受限制”邮件数 • 已拒绝或 TCP 拒绝的连接数（可能是部分计数） • 每个连接的邮件数量的保守倍数 当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。在这种情况下，显示的值可以解释为“下限”，即至少已拦截这么多邮件。 “概述”(Overview) 页面上的“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 总计始终基于所有已拒绝的连接的完整计数。只有每个发件人的连接计数会因负载而受到限制。
无效收件人	由会话 LDAP 拒绝和所有 RAT 拒绝予以拒绝的所有邮件收件人。
由域信誉过滤拦截	根据发件人域的信誉来判定阻止的邮件总数。
检测到的垃圾邮件	反垃圾邮件扫描引擎检测为具有垃圾邮件特征或可疑的邮件总数。此外，还包括同时具有垃圾邮件和病毒特征的邮件。

类别	说明
检测到的病毒邮件	被检测为病毒但不是垃圾邮件的邮件总数和百分比。 以下消息计入 " 检测到病毒 " 类别中： • 病毒扫描结果为“已修复”(Repaired) 或“感染”(Infectious) 的邮件 • 在选中了将已加密的邮件计为包含病毒的选项时，病毒扫描结果为“已加密”(Encrypted) • 在针对不可扫描的邮件执行的操作不是“传送”(Deliver) 时，病毒扫描结果为“不可扫描”(Unscannable) • 在选中了传送到备用邮件主机或备用收件人的选项时，病毒扫描结果为“不可扫描”(Unscannable) 或“已加密”(Encrypted) 的邮件 • 以手动方式或通过超时从“病毒爆发”(Outbreak) 隔离区删除的邮件。
由高级恶意软件防护检测到 (Detected by Advanced Malware Protection)	文件信誉过滤发现邮件附件是恶意软件。该值不包括通过文件分析发现为恶意的判定更新或文件。
带恶意 URL 的邮件 (Messages with Malicious URLs)	URL 过滤发现邮件中的一个或多个 URL 是恶意的。
内容过滤器拦截	由内容过滤器拦截的邮件总数。 如果您的访问权限允许您查看邮件跟踪数据：要在此报告中查看内容过滤器违规的邮件跟踪详细信息，请点击表中的蓝色数字链接。
由 DMARC 拦截 (Stopped by DMARC)	未通过 DMARC 验证的邮件总数。
S/MIME 验证/解密失败	未通过 S/MIME 验证、解密或两者的邮件总数。
营销邮件	由公认的专业营销组织（如 Amazon.com）发送的广告邮件总数。 仅当系统中存在营销数据时，此列表项才会出现在页面上。 此数字包括由启用了灰色邮件功能的邮件安全设备识别的营销邮件，以及由在反垃圾邮件设置下启用了“营销邮件扫描” 的设备识别的营销邮件。
社交网络邮件 (Social Networking Messages)	来自社交网络的、交友网站、论坛等的通知邮件总数。示例包括 LinkedIn 和 CNET 论坛。此信息由灰色邮件功能确定。
批量邮件 (Bulk Messages)	由非公认的营销组织（如技术媒体公司 TechTarget）发送的广告邮件总数。 此信息由灰色邮件功能确定。

类别	说明
灰色邮件	此数字包括由灰色邮件功能检测到的营销邮件，以及社交网络邮件和批量邮件。它不包括未启用灰色邮件功能的设备上识别的营销邮件，即使这些合计包括在“营销邮件”(Marketing Messages) 值中。 点击与任一灰色邮件类别对应的数字，以使用“邮件跟踪”(Message Tracking) 查看属于该类别的邮件列表。 另请参阅灰色邮件报告 , on page 43。
S/MIME 验证/解密成功	已使用 S/MIME 成功验证、解密或解密并验证的邮件总数。
已接受的正常邮件	此类别是已接受并被视为非病毒和垃圾邮件的邮件。 最准确地表示了在将按收件人的扫描操作考虑在内时（例如拆分的邮件由单独的邮件策略处理）接受的正常邮件。 但是，由于未对标记为垃圾邮件或确定感染病毒且仍然传送的邮件进行计数，因此传送的实际邮件数可能不同于干净邮件计数。 如果邮件与邮件过滤器匹配并且不被过滤器丢弃或退回，则将这些邮件视为正常邮件。总计中未计入邮件过滤器丢弃或退回的邮件。 未启用灰色邮件功能的设备上处理的邮件被计为正常邮件。
尝试的邮件总数 (Total Attempted Messages)	此数字包括垃圾邮件、营销邮件（无论是由灰色邮件功能还是由反垃圾邮件设置下的“营销邮件扫描”[Marketing Email Scanning] 功能发现）、社交网络邮件、批量邮件和正常邮件。

Note 如果您已配置防病毒设置以传送无法扫描或已加密的邮件，这些邮件将被计为正常邮件，而不是病毒。否则，邮件将被计为含有病毒的邮件。此外，如果邮件与某个邮件过滤器相匹配，且未被该过滤器丢弃或退回，则这些邮件将被视为正常邮件。邮件过滤器丢弃或退回的邮件不计入总数。

“传入邮件”(Incoming Mails) 页面

安全管理设备上的**邮件 > 报告 > 传入邮件**页为连接到您的托管安全管理设备的所有远程主机提供实时信息的交互报告。您可以收集有关发送邮件到您的系统的 IP 地址、域和网络所有者（组织）的信息。也可以基于 IP 地址、域以及向您发送邮件的组织执行发件人配置文件搜索。

“传入邮件详细信息”(Incoming Mail Details) 交互式表显示了关于特定 IP 地址、域或网络所有者（组织）的详细信息。您可以访问任一 IP 地址、域或网络所有者的“发件人配置文件”(Sender Profile) 页面，方法是点击**传入邮件 (Incoming Mail)** 页面顶部或其他“发件人配置文件”(Sender Profile) 页面上的相应链接。

从“传入邮件”(Incoming Mail) 页面可以执行如下操作：

- 基于将邮件发送至安全管理设备的 IP 地址、域或网络所有者（组织）进行搜索。请参阅搜索与交互式邮件报告页面 , on page 6。
- 查看“发件人组”(Sender Groups) 报告以根据特定发件人组和邮件流策略操作监控连接。有关详细信息，请参阅 “发件人组 (Sender Groups)”报告页面, on page 21。
- 查看关于已将邮件发送到您的设备的发件人的详细统计信息。统计信息包括按安全服务（发件人信誉过滤、反垃圾邮件、防病毒等）细分的所尝试邮件数量。
- 按照向您发送大量垃圾邮件或病毒邮件（由反垃圾邮件或防病毒安全服务决定）的发件人进行分类。
- 使用 SenderBase 信誉服务检查特定 IP 地址、域和组织之间的关系以获取有关发件人的信息。
- 从 SenderBase 信誉服务获取有关发件人的详细信息，包括发件人的 SenderBase 信誉得分 (SBRS)、域最近匹配哪个发件人组等。将发件人添加到发件人组。
- 获取更多有关发送大量垃圾邮件或病毒邮件（由反垃圾邮件或防病毒安全服务决定）的特定发件人的信息。

在“传入邮件”(Incoming Mail) 页面内查看

传入邮件页面有三种不同的视图：

- IP 地址
- 域
- 网络所有者

这些视图在选定视图的情景中提供连接到系统的远程主机的快照。

此外，在“传入邮件”(Incoming Mails) 页面的“传入邮件详细信息”(Incoming Mail Details) 部分，您可以点击发件人的 IP 地址、域名或网络所有者信息以检索特定的发件人配置文件信息。有关发件人配置文件信息的详细信息，请参阅发件人配置文件页面, on page 20。

Note 网络所有者是包含域的实体。域 *(Domains)* 是包含 IP 地址的实体。

根据所选的视图，“传入邮件详细信息 (Incoming Mail Details)”交互式表格中显示将邮件发送至邮件安全设备上配置的所有公共侦听器的排名靠前的 IP 地址、域或网络所有者。可以监控传入设备的所有邮件的流量。

在“发件人配置文件 (Sender Profile)”页面上点击 IP 地址、域或网络所有者可访问有关发件人的详细信息。“发件人配置文件”(Sender Profile) 页面是与特定 IP 地址、域或网络所有者相关的“传入邮件”(Incoming Mail) 页面。

要按发件人组访问邮件流信息，请点击“传入邮件”(Incoming Mails) 页面底部的**发件人组报告 (Sender Groups Report)** 链接。请参阅发件人配置文件页面, on page 20。

在某些情况下，某些报告页面包含可从顶层页面访问的几个独特的子报告。例如，通过安全管理设备中的“传入邮件 (Incoming Mail)”报告页面可以查看各个 IP 地址、域和网络所有者的信息。其中每个页面均是可从“传入邮件 (Incoming Mail)”报告页面访问的子页面。

当您在顶层页面的右上角点击“可打印的 PDF”(Printable PDF) 链接时，这些子报告页面的结果会在一个合并的报告上生成；在这种情况下是“传入邮件”(Incoming Mails) 报告页面。请参阅了解“邮件报告”页面, on page 7中的重要信息。

邮件 > 报告 > 传入邮件页面提供以下视图：**IP 地址**、**域**或**网络所有者**

如需获得对“传入邮件详细信息”(Incoming Mail Details) 交互式表中包括的数据的解释，请参阅传入邮件详细信息 (Incoming Mail Details) 表, on page 19。

从**传入邮件**页面中，您还可以生成 PDF 或将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅了解“邮件报告”页面, on page 7。

Note 您可以生成“传入邮件”(Incoming Mail) 报告页面的计划报告。请参阅 计划邮件报告, on page 103。

“没有域信息”(No Domain Information) 链接

已连接至安全管理设备并且无法通过双 DNS 查找进行验证的域将自动分组到名为“没有域信息”的特殊域。可以控制通过发件人验证来管理此类未验证主机的方式。有关发件人验证的详细信息，请参阅邮件安全设备的文档或在线帮助。

您可以使用“显示的项”(Items Displayed) 菜单选择要在列表中显示的发件人数量。

邮件趋势图中的时间范围

可以选择不同程度的粒度以在邮件图中查看数据。您可以选择相同数据的天、周、月和年视图。由于数据实时受到监控，因此会在数据库中定期更新和汇总信息。

有关时间范围的详细信息，请参阅选择报告的时间范围。

传入邮件详细信息 (Incoming Mail Details) 表

传入邮件页面底部的“传入邮件详细信息”交互式表列出了已连接至邮件安全设备上的公共侦听程序的排名靠前的发件人。下表根据所选视图显示域、IP 地址或网络所有者。单击列标题可对数据进行排序。

系统通过执行双 *DNS* 查找来获得和验证远程主机 IP 地址的有效性。有关双 DNS 查找和发件人验证的更多信息，请参阅邮件安全设备的文档或在线帮助。

对于“传入邮件详细信息”(Incoming Mail Details) 表第一列中列出的或“按威胁邮件总数列出的发件人排行榜”(Top Senders by Total Threat Messages) 上的发件人（即网络所有者、IP 地址或域），单击**发件人 (Sender)** 或**没有域信息 (No Domain Information)** 链接可查看有关发件人的详细信息。结果显示在**发件人配置文件**页面上，其中包括来自 SenderBase 信誉服务的实时信息。从“发件人配置文件”(Sender Profile) 页面中，您可以查看有关特定 IP 地址或网络所有者的详细信息。有关详细信息，请参阅发件人配置文件页面, on page 20。

您还可以查看“发件人组”(Sender Groups) 报告，方法是单击“传入邮件”(Incoming Mail) 页面底部的**发件人组报告 (Sender Groups report)**。有关“发件人组报告”(Sender Groups report) 页面的详细信息，请参阅“发件人组 (Sender Groups)”报告页面, on page 21。

如果您的访问权限允许您查看邮件跟踪数据：要在此报告中查看内容过滤器违规的邮件跟踪详细信息，请单击表中的蓝色数字链接。

发件人配置文件页面

当您在**邮件流详细信息** [新 Web 界面] 或**传入邮件**页面上的交互式表中单击收件人时，会出现“发件人配置文件”页面。它显示关于特定 IP 地址、域或网络所有者（组织）的详细信息。通过单击邮件流详细信息页面或其他“发件人配置文件”页面上的相应链接，您可以访问任何 IP 地址、域或网络所有者的“发件人配置文件”页面。

网络所有者是包含域的实体。域 *(Domains)* 是包含 IP 地址的实体。

为 IP 地址、域和网络所有者显示的“发件人配置文件”(Sender Profile) 页面稍有不同。对于每项，该页面包含来自特定发件人的传入邮件的图形和摘要表。在图形下方，表列出与发件人相关联的域或 IP 地址。（单个 IP 地址的“发件人配置文件”[Sender Profile] 页面不包含更精细的列表。）“发件人配置文件”(Sender Profile) 页面还包括一个信息部分，其中包含当前 SenderBase、发件人组和发件人的网络信息。

- 网络所有者配置文件页面包含网络所有者以及与该网络所有者关联的域和 IP 地址的信息。
- 域配置文件页面包含与该域关联的域和 IP 地址。
- IP 地址配置文件页面只包含有关该 IP 地址的信息。

每个“发件人配置文件 (Sender Profile)”页面底部的“当前信息 (Current Information)”表格中都包含以下数据：

- 来自 SenderBase 信誉服务的全局信息，包括：
  - IP 地址、域名和/或网络所有者
  - 网络所有者类别（仅限网络所有者）
  - CIDR 范围（仅限 IP 地址）
  - IP 地址、域和/或网络所有者的日量级和月量级
  - 自从此发件人收到第一封邮件以来的天数
  - 上一个发件人组以及是否进行了 DNS 验证（仅 IP 地址发件人配置文件页面）

  日流量用于衡量某个域在最近 24 小时内发送了多少邮件。SenderBase 流量类似于用来衡量地震的里氏震级，使用以 10 为底数的对数标尺计算邮件数量。该标尺的最大理论值设置为 10，等同于 100% 的实际邮件数量。使用该对数标尺时，流量每增加 1 个单位，实际数量就会增加 10 倍。

  月流量的计算方法与日流量相同，只是百分比基于最近 30 天发送的邮件数量来计算。

  - 平均量级（仅限 IP 地址）
  - 生命周期数量/30 天数量（仅限 IP 地址配置文件页面）
  - 有担保发件人状态（仅限 IP 地址配置文件页面）

- SenderBase 信誉得分（仅限 IP 地址配置文件页面）
- 自从第一封邮件以来的天数（仅限网络所有者和域配置文件页面）
- 与此网络所有者相关联的域数量（仅限网络所有者和域配置文件页面）
- 此网络所有者中的 IP 地址数量（仅限网络所有者和域配置文件页面）
- 用于发送邮件的 IP 地址数量（仅限网络所有者页面）

单击**来自 SenderBase 的详细信息 (More from SenderBase)** 可查看包含 SenderBase 信誉服务提供的所有信息的页面。

- 有关由此网络所有者控制的域和 IP 地址的详细信息显示在网络所有者配置文件页面上。有关域中的 IP 地址的详细信息，将显示在域页面上。

从域配置文件页面中，您可以单击特定 IP 地址以查看特定信息，或查看组织配置文件页面。

“发件人组 (Sender Groups)”报告页面

发件人组报告页按发件人组和邮件流策略操作提供连接摘要，允许您查看 SMTP 连接和邮件流策略趋势。“按发件人组的邮件流量 (Mail Flow by Sender Group)”列表显示每个发件人组的连接的百分比和数量。“按邮件流量策略操作的连接”(Connections by Mail Flow Policy Action) 图表显示每个邮件流量策略操作的连接百分比。此页面概述了主机访问表 (HAT) 策略的有效性。有关 HAT 的详细信息，请参阅邮件安全设备的文档或在线帮助。

要查看“发件人组 (Sender Groups)”报告页面，请选择**电子邮件 > 报告 (Reporting) > 发件人组 (Sender Groups)**。

从**发件人组报告**页中，您还可以生成 PDF 或将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅了解“邮件报告”页面, on page 7。

Note 您可以生成“发件人组报告”(Sender Groups report) 页面的计划报告。请参阅计划邮件报告, on page 103。

“发件人域信誉”页面

您可以使用“发件人域信誉”报告页面：

- 以图形格式根据从 SDR 服务接收的判定查看传入邮件。
- 以表格格式根据从 SDR 服务接收的威胁类别和判定查看传入邮件摘要。
- 以图形格式根据从 SDR 服务接收的威胁类别查看传入邮件。

注释 只有那些 SDR 判为 "不受信任" 或 "有问题 "的信息才被归入 SDR 威胁类别，如 "垃圾邮件"、"恶意 "等。

- 根据从 SDR 服务中表格的形式接收的威胁类别的传入邮件摘要。

在“SDR 处理的传入邮件摘要”(Summary of Incoming Messages handled by SDR) 部分，您可以单击与特定判定对应的邮件数量，在“邮件跟踪”(Message Tracking) 中查看相关邮件。

“外发目标”(Outgoing Destinations) 页面

邮件 > 报告 > 外发目标页面提供有关贵组织发送邮件的目标域的信息。

使用“外发目标 (Outgoing Destinations)”页面可回答以下类型的问题：

- 邮件安全设备将邮件发送至哪些域？
- 向每个域发送多少邮件？
- 该邮件中有多少是正常的、具有垃圾邮件特征、具有病毒特征、恶意软件或由内容过滤器拦截？
- 传送了多少封邮件？目标服务器硬退回了多少封邮件？

以下列表解释了**外发目标**页面上的各部分：

Table 5: “邮件”>“报告”>“外发目标”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
按威胁邮件总数列出的目标排行榜 (Top Destination by Total Threat)	您的组织发送的传出威胁邮件（垃圾邮件、病毒等）的目标域排行榜。威胁总数包括属于垃圾邮件或病毒的威胁，或触发了内容过滤器的威胁。
按正常邮件数列出的目标排行榜 (Top Destination by Clean Messages)	您的组织发送的正常传出邮件的目标域排行榜。

部分	说明
外发目标详细信息 (Outgoing Destination Details)	与您的组织发送的所有传出邮件的目标域相关的所有详细信息，按收件人总数排序。详细信息包括检测到的垃圾邮件、病毒、正常、硬退回邮件等。 **Note** 计算硬退回邮件时，仅包括以下退回类型： • FiveXX 硬退回 • 过滤器硬退回 • 其他硬退回 • DNS 硬退回 • 过期的硬退回 如果您的访问权限允许您查看邮件跟踪数据：要在此报告中查看内容过滤器违规的邮件跟踪详细信息，请单击表中的蓝色数字链接。

从**外发目标**页面中，您还可以生成 PDF 或将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅了解“邮件报告”页面, on page 7。

Note 您可以生成“外发目标”(Outgoing Destinations) 页面的计划报告。请参阅计划邮件报告, on page 103。

“传出邮件发件人”页面

邮件 > 报告 > 传出邮件发件人页面提供有关从网络中的 IP 地址和域所发送邮件的数量和类型信息。

使用“传出邮件发件人”(Outgoing Senders) 页面可回答以下类型的问题：

- 哪些 IP 地址正在发送最具病毒、垃圾邮件或恶意软件的特征邮件？
- 哪些 IP 地址最频繁触发内容过滤器？
- 哪些域发送最多邮件？
- 已尝试传送后正在处理的收件人总数。

要查看**传出邮件发件人**页面，请执行以下操作：

您可以使用两种类型的视图查看传出邮件发件人的结果：

- **域 (Domain)**：此视图使您可以查看每个域发送的邮件量。
- **IP 地址 (IP address)**：此视图使您可以查看哪些 IP 地址发送的病毒邮件最多或触发内容过滤器。

以下列表从两种视图角度解释了**传出邮件发件人**页面上的各部分：

Table 6: “邮件报告传出邮件发件人”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
排名靠前的发件人（按有害邮件总数）	您的组织中的传出威胁邮件（垃圾邮件、病毒等）的发件人排行榜（按 IP 地址或域）。
按正常邮件列出的发件人排行榜	您的组织中发送的正常传出邮件的发件人排行榜（按 IP 地址或域）。
发件人详细信息	关于您的组织发送的所有传出邮件的发件人的详细信息（按 IP 地址或域）。详细信息包括检测到的垃圾邮件、病毒、正常邮件等。 如果您的访问权限允许您查看邮件跟踪数据：要在此报告中查看 DLP 和内容过滤器违规的邮件跟踪详细信息，请单击表中的蓝色数字链接。

Note 此页面未显示有关邮件发送的信息。要跟踪发送信息，例如从特定域退回的邮件数，请登录到相应的邮件安全设备，然后选择**监控 (Monitor) > 发送状态 (Delivery Status)**。

从**传出邮件发件人**页面中，您还可以生成 PDF 或将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅了解“邮件报告”页面, on page 7。

Note 您可以生成**传出邮件发件人 (Outgoing Senders)** 页面的计划报告。请参阅计划邮件报告, on page 103。

“内部用户”页面

邮件 > 报告 > 内部用户页面按邮件地址提供有关您的内部用户发送和接收的邮件的信息。 单个用户可以具有多个邮件地址。报告中未合并邮件地址。

使用“内部用户”(Internal Users) 交互式报告页面可回答以下类型的问题：

- 谁发送的外部邮件最多？
- 谁接收的正常邮件最多？
- 谁接收的灰色邮件最多？
- 谁接收的垃圾邮件最多？
- 谁触发了哪些内容过滤器？
- 谁的邮件被内容过滤器拦截？

Table 7: “邮件报告内部用户”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
按正常的传入邮件排名靠前的用户 (Top Users by Clean Incoming Messages)	您的组织中发送的正常传入邮件的用户排行榜（按 IP 地址或域）。
按正常的传出邮件排名靠前的用户 (Top Users by Clean Outgoing Messages)	您的组织中发送的正常传出邮件的用户排行榜（按 IP 地址或域）。
用户邮件控制详细信息 (User Mail Flow Details)	“用户邮件流详细信息”(User Mail Flow Details) 交互式部分会细分每个邮件地址接收和发送的邮件。您可以通过单击列标题对列表排序。 要查看用户的详细信息，请单击“内部用户”(Internal User) 列的用户名。有关详细信息，请参阅“内部用户详细信息”(Internal User Details) 页面, on page 25。 如果您的访问权限允许您查看邮件跟踪数据：要在此报告中查看内容过滤器违规的邮件跟踪详细信息，请单击表中的蓝色数字链接。

从**内部用户**页面中，您还可以生成 PDF 或将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅了解“邮件报告”页面, on page 7。

Note 您可以生成“内部用户”(Internal Users) 页面的计划报告。请参阅 计划邮件报告, on page 103。

“内部用户详细信息”(Internal User Details) 页面

“内部用户详细信息”页面显示关于用户的详细信息，细分了传入和传出邮件，显示每种类别（如检测到的垃圾邮件、检测到的病毒邮件、高级恶意软件保护检测到的邮件、内容过滤器拦截的邮件等）的邮件数。还显示传入和传出内容过滤器匹配项。

入站内部用户是您根据“收件人：”(Rcpt To:) 地址为其收到邮件的用户。出站内部用户基于“发件人: (Mail From:)”地址，在跟踪内部网络中的发件人所发送邮件的类型时非常有用。

单击内容过滤器名称可在相应的内容过滤器信息页面上查看该过滤器的详细信息（请参阅“内容过滤器”(Content Filters) 页面, on page 28）。您可以使用此方法查看发送了或接收了与特定内容过滤器相匹配的邮件的所有用户列表。

Note 某些出站邮件（例如退回）的发件人为空。这些邮件被计为出站“未知”(unknown)。

搜索特定的内部用户

利用用户邮件摘要页面和用户邮件流详细信息页面底部的搜索表单，您可以搜索特定的内部用户（邮件地址）。选择是要精确匹配搜索文本还是查找以输入的文本开头的项（例如，以“ex”开头将匹配“example.com”）。

DLP 事件

邮件 > 报告 > DLP 事件（**DLP 事件摘要**）页显示传出邮件中发生的防数据丢失 (DLP) 策略违规事件的信息。邮件安全设备使用在“传出邮件策略 (Outgoing Mail Policies)”表中启用的 DLP 邮件策略来检测用户发送的敏感数据。违反 DLP 策略的每个传出邮件均报告为一个事件。

使用“DLP 事件摘要”(DLP Incident Summary) 报告可回答以下类型的问题：

- 用户发送什么类型的敏感数据？
- 这些 DLP 事件具有什么样的严重性？
- 传送的这些邮件有多少数量？
- 丢弃的这些邮件有多少数量？
- 是谁在发送这些邮件？

“DLP 事件摘要”(DLP Incident Summary) 页面包括两个主要部分：

- 按严重性（低 [Low]、中 [Medium]、高 [High]、严重 [Critical]）总结 DLP 事件排行榜的 DLP 事件趋势图，以及策略匹配项
- DLP 事件详细信息列表

Table 8: *“邮件”(Email) >“报告”(Reporting) >“DLP 事件摘要”(DLP Incident Summary)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
按严重性排名考前的事件 (Top Incidents by Severity)	按严重性列出的 DLP 事件排行榜。
事件概要	**DLP 事件摘要 (DLP Incident Summary)** 页面底部的“DLP 事件详细信息”(DLP Incident Details) 交互式表中列出了当前已为每台邮件设备的传出邮件策略启用的 DLP 策略。点击 DLP 策略的名称可查看更详细的信息。
排名靠前的 DLP 策略匹配项 (Top DLP Policy Matches)	已匹配的 DLP 策略排行榜。

部分	说明
DLP 事件详细信息 (DLP Incident Details)	“DLP 事件详细信息”(DLP Incident Details) 表显示每个策略的 DLP 事件总数，其细分依据为严重性级别，以及是否已传送类别为“已传送（清除）”(Delivered [clear])、“已传送（已加密）”(Delivered [encrypted]) 或“已丢弃”(Dropped) 的任何邮件。 有关“DLP 事件详细信息”(DLP Incident Details) 表的更多信息，请参阅 “DLP 事件详细信息”(DLP Incidents Details) 表, on page 27。

点击 DLP 策略的名称可查看有关策略检测到的 DLP 事件的详细信息。使用此方法可以获取发送的邮件包含策略检测到的敏感数据的用户列表。

“DLP 事件详细信息”(DLP Incidents Details) 表

“DLP 事件详细信息”(DLP Incident Details) 交互式表按策略显示 DLP 事件总数，其细分依据为严重性级别，以及是否已传送类别为“已传送（清除）”(Delivered [clear])、“已传送（已加密）”(Delivered [encrypted]) 或“已丢弃”(Dropped) 的任何邮件。点击列标题可对数据进行排序。

要了解有关此表中列出的任何 DLP 策略的详细信息，请点击 DLP 策略的名称，此时会出现“DLP 策略”(DLP Policy) 页面。有关详细信息，请参阅“DLP 策略详细信息”(DLP Policy Detail) 页面, on page 27。

如果您的访问权限允许您查看邮件跟踪数据：要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

“DLP 策略详细信息”(DLP Policy Detail) 页面

如果您在“DLP 事件详细信息”(DLP Incident Details) 表中点击某个 DLP 策略的名称，出现的“DLP 策略详细信息”(DLP Policy Detail) 页面会显示该策略的 DLP 事件数据。该页面会显示基于严重性的 DLP 事件图形。

该页面还在页面底部包括“按发件人列出的事件”(Incidents by Sender)，其中列出了发送的邮件违反 DLP 策略的每个内部用户。该表还按用户显示此策略的 DLP 事件总数，其细分依据为严重性级别，以及是否已传送类别为“已传送（清除）”(Delivered [clear])、“已传送（已加密）”(Delivered [encrypted]) 或“已丢弃”(Dropped) 的任何邮件。您可以使用“按发件人列出的事件”(Incidents by Sender) 表了解哪些用户可能正在将组织的敏感数据发送给网络外部的人员。

点击“事件详细信息”(incident detail) 页面上的发件人名称将打开“内部用户”(Internal Users) 页面有关详细信息，请参阅 “内部用户”页面, on page 24。

邮件过滤器

“邮件过滤器”(Message Filters) 页面显示有关传入和传出邮件的邮件过滤器匹配项排行榜的信息（那些邮件过滤器具有最大数量的匹配邮件）。

地理分布

可以使用“地理分布”报告页面查看：

- 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。
- 以表格格式显示的基于源国家/地区的传入邮件连接总数。

以下是不显示传入邮件连接排行榜和总数的国家/地区信息的情景：

- 发件人 IP 地址是私有 IP 地址
- 发件人 IP 地址未获得有效 SBRS。

大量邮件

使用此页上的报告执行以下操作：

- 识别涉及来自单个发件人的大量邮件的攻击或在移动一小时期间内具有相同对象的攻击。
- 监控排名靠前的域以确保此类攻击不从您自己的域发起。如果发生这种情况，您的组织中的一个或多个账户可能受到影响。
- 帮助识别误报，使您可以相应地调整过滤器。

此页面上的报告所显示的数据仅来自使用“标题重复”(Header Repeats) 规则的邮件过滤器，以及超过您在该规则中设置的邮件数阈值的邮件过滤器。当与其他规则结合使用时，系统会最后计算“标题重复”(Header Repeats) 规则，如果邮件处理由之前的条件决定，则完全不计算。同样，由“速率限制”(Rate Limiting) 捕获的邮件绝不会到达“标题重复”(Header Repeats) 邮件过滤器。因此，本来可能被视为大量邮件的某些邮件可能不会包括在这些报告中。如果您配置了过滤器以将某些邮件列入允许列表，这些邮件也从这些报告中排除。

有关邮件过滤器和信头重复规则的详细信息，请参阅邮件安全设备的在线帮助或用户指南。

相关主题

- 速率限制页面 , on page 41

“内容过滤器”(Content Filters) 页面

电子邮件 > 报告 (Reporting) > 内容过滤器 (Content Filters) 页面显示关于传入和传出内容过滤器匹配项排行榜的信息（哪个内容过滤器具有最匹配的邮件）。该页面以条形图和列表的形式显示数据。使用“内容过滤器”(Content Filters) 页面，可以按内容过滤器或按用户查看公司策略，并且回答以下类型的问题：

- 传入或传出邮件最多触发了哪些内容过滤器？
- 哪些用户最常发送或接收触发特定内容过滤器的邮件？

要查看有关特定过滤器的详细信息，请点击过滤器的名称。此时将出现“内容过滤器详细信息”(Content Filter Details) 页面。有关“内容过滤器详细信息”(Content Filter Details) 页面的更多信息，请参阅“内容过滤器详细信息”页面, on page 29。

如果您的访问权限允许您查看邮件跟踪数据：要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

从**内容过滤器**页面中，您还可以生成 PDF 或将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅了解“邮件报告”页面, on page 7。

Note 您可以生成“内容过滤器”(Content Filters) 页面的计划报告。请参阅计划邮件报告, on page 103。

“内容过滤器详细信息”页面

“内容过滤器详细信息”(Content Filter Details) 页面显示过滤器在一段时间内的匹配项，以及按内部用户列出的匹配项。

在“按内部用户列出的匹配项”(Matches by Internal User) 部分中，单击用户名（邮件地址）可查看该内部用户的详细信息页面。有关详细信息，请参阅“内部用户详细信息”(Internal User Details) 页面, on page 25。

如果您的访问权限允许您查看邮件跟踪数据：要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的蓝色数字链接。

DMARC 验证

“DMARC 验证”(DMARC Verification) 页面显示未通过基于域的邮件身份验证、报告和一致性 (DMARC) 验证的发件人域排行榜，并显示对来自每个域的传入邮件执行的各项操作的摘要。您可以使用此报告微调 DMARC 设置并回答以下类型的问题：

- 哪些域发送了最多未通过 DMARC 验证的邮件？
- 对于每个域，对 DMARC 验证失败的邮件执行了什么操作？

有关 DMARC 验证的详细信息，请参阅邮件安全设备的在线帮助或用户指南中的“邮件身份验证”章节。

宏检测

可以使用“宏检测”(Macro Detection) 报告页面查看：

- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传入附件。
- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传出附件。

您可以点击启用宏的附件数量，以在邮件跟踪中查看相关邮件。

注释 报告生成期间：

- 如果在存档文件中检测到一个或多个宏，则存档文件的文件类型将按一递增。不计算存档文件中启用宏的附件数量。
- 如果在嵌入文件中检测到一个或多个宏，则父文件类型将递增一。不计算嵌入文件中启用宏的附件数量。

“外部威胁源”(External Threat Feeds) 页面

您可以使用“外部威胁源”(External Threat Feeds) 报告页面查看：

- 以图形格式查看用于检测邮件威胁的排名靠前的 ETF 来源
- 以表格格式查看用于检测邮件威胁的 ETF 来源的摘要。
- 以图形格式查看与检测到的邮件威胁相匹配的排名靠前的 IOC。
- 以图形格式查看用于过滤恶意传入邮件连接的排名靠前的 ETF 来源。
- 以表格格式查看用于过滤恶意传入邮件连接的 ETF 来源的摘要。

在“外部威胁源来源摘要”(Summary of External Threat Feed Sources) 部分：

- 您可以点击特定 ETF 来源的邮件数量，在邮件跟踪中查看相关邮件。
- 您可以点击特定威胁源来源，根据 IOC 查看 ETF 来源的分布情况。

在“感染指标 (IOC) 匹配摘要”部分：

- 您可以点击特定 ETF 来源的 IOC 数量，在邮件跟踪中查看相关邮件。
- 您可以点击特定 IOC，根据 ETF 来源查看 IOC 的分布情况。

“病毒类型”(Virus Types) 页面

邮件 > 报告 > 病毒页提供有关发送到网络和从网络发送的病毒的概述。“病毒类型 (Virus Types)”页面显示已由运行于邮件安全设备之上的病毒扫描引擎检测到并且显示在安全管理设备上的病毒。使用此报告针对特定病毒采取相应措施。例如，如果发现收到已知嵌入 PDF 文件中的大量病毒，则可以创建过滤器操作来隔离具有 PDF 附件的邮件。

Note 爆发过滤器可以隔离这些类型的感染了病毒的邮件，无需用户干预。

如果您运行多个病毒扫描引擎，则“病毒类型”(Virus Types) 页面包含来自所有已启用的病毒扫描引擎的结果。页面上出现的病毒名称由病毒扫描引擎决定。如果多个扫描引擎检测到病毒，则同一病毒可能有多个条目。

Table 9: “邮件”>“报告”>“病毒类型”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
检测到的传入病毒类型排行榜 (Top Incoming Virus Types Detected)	此部分显示已发送到您的网络的病毒的图表视图。
检测到的传出病毒类型排行榜 (Top Outgoing Virus Types Detected)	此部分显示已从您的网络发送的病毒的图表视图。
病毒类型详细信息 (Virus Types Detail)	显示每个病毒类型详细信息的交互式表。

Note 如需查看哪些主机将受病毒感染的邮件发送到您的网络，请转到“传入邮件”(Incoming Mail) 页面，指定同一报告时间段，并按病毒邮件排序。同样，如需查看您网络中的哪些 IP 地址发送了病毒邮件，请查看“传出邮件发件人”(Outgoing Senders) 页面，并按病毒邮件排序。

从**病毒类型**页中，您还可以生成PDF或将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅了解“邮件报告”页面, on page 7。

Note 您可以生成**病毒类型 (Virus Types)** 页面的计划报告。请参阅 计划邮件报告, on page 103。

“URL 过滤”页面

- 仅当启用 URL 过滤时，才会填充 URL 过滤报告模块。
- 提供传入和传出邮件的“URL 过滤”(URL Filtering) 报告。
- 只有由 URL 过滤引擎扫描的邮件（作为反垃圾邮件/病毒爆发过滤器扫描的一部分或通过邮件/内容过滤器）才会包含在这些模块中。但是，并非所有结果都有必要专门可归属于URL过滤功能。
- “排名靠前的 URL 类别”(Top URL Categories) 模块包含已扫描的邮件中找到的所有类别，无论其是与内容过滤器还是邮件过滤器匹配都如此。
- 每封邮件只能与一个信誉级别相关联。对于包含多个 URL 的邮件，统计信息反映邮件中任何 URL 的最低信誉。
- 在“安全服务”(Security Services) >“URL 过滤”(URL Filtering) 中配置的全局允许列表内的 URL 未包含在报告中。

报告中包含个别过滤器中使用的允许列表内的 URL。

- 恶意 URL 是病毒爆发过滤器确定为信誉不佳的 URL。不确定 URL 是病毒爆发过滤器确定需要单击时间保护的 URL。因此，不确定 URL 已被重写，从而重定向到思科网络安全代理。
- 基于 URL 类别的过滤器的结果会反映在内容和邮件过滤器报告中。
- 思科网络安全代理的单击时间 URL 评估结果不会反映在报告中。

“网络交互跟踪”(Web Interaction Tracking) 页面

- 仅当在受管邮件安全设备上启用了“网络交互跟踪”功能时，才会填充“网络交互跟踪”报告模块。
- 网络交互跟踪报告适用于传入和传出邮件。
- 这些模块中仅包含最终用户（通过策略或爆发过滤器）点击的重写 URL。
- “网络交互跟踪”(Web Interaction Tracking) 页面包括以下报告：

  最终用户点击的排名靠前的重写恶意 URL。点击 URL 可查看包含以下信息的详细报告：

  - 点击了重写恶意 URL 的最终用户列表。
  - 点击该 URL 的日期和时间。
  - URL 是否已由策略或爆发过滤器重写。
  - 点击重写的 URL 时采取的操作（允许、阻止或未知）。请注意，如果 URL 被爆发过滤器重写，且未提供最终判定，则状态显示为“未知”(unknown)。

Note 由于限制原因，所有病毒爆发重写的 URL 的状态都将显示为未知。

  点击重写的恶意 URL 的排名靠前的最终用户

  跟踪网络交互详细信息。包括以下信息：

  - 所有重写的 URL 列表（恶意和非恶意）。点击 URL 可查看详细报告。
  - 点击重写的 URL 时采取的操作（允许、阻止或未知）。

    在最终用户点击 URL 时，如果对该 URL（正常或恶意）的判定为“未知”(unknown)，则状态显示为“未知”(unknown)。这可能是因为，需要进一步审查该URL，或用户点击时网络服务器停止服务或无法访问。

  - 最终用户点击重写的 URL 的次数。点击数字可查看包含点击的 URL 的所有邮件列表。

- 请注意以下提示：
  - 如果您已配置内容或邮件过滤器以在重写恶意URL后传送邮件并通知另一个用户（例如管理员），则在被通知的用户点击已重写的 URL 时，原始收件人的网络交互跟踪数据会增加。
  - 如果您使用网络界面向原始收件人之外的用户（如管理员）发送包含已重写URL的已隔离邮件副本，则在另一个用户点击已重写的 URL 时，原始收件人的网络交互跟踪数据会增加。

“伪造邮件检测”(Forged Email Detection) 页面

- “伪造邮件检测”(Forged Email Detection) 页面包括以下报告：
  - **排名靠前的伪造邮件检测**。显示内容字典中与传入邮件中的伪造“发件人：”信头匹配的前十个用户。
  - **伪造邮件检测详细信息**。显示内容词典中与传入邮件中的伪造“发件人：”信头匹配所有用户的列表，对于给定用户，还会显示匹配的邮件的数量。
- 只有在使用“伪造邮件检测”内容过滤器或 forged-email-detection 邮件过滤器时，才会填充“伪造邮件检测”报告。

“安全打印”(Safe Print) 页面

您可以使用“安全打印操作”报告页面查看：

- 以图形格式显示的基于文件类型的安全打印附件的数量。
- 基于表格格式的文件类型的安全打印附件摘要。

在“安全打印文件类型的摘要”(Summary of Safe Print File Types) 部分中，点击要在邮件跟踪中查看邮件详细信息的安全打印附件总数。

邮件策略详细信息报告页面

您可以使用“邮件策略详细信息”(Mail Policy Details) 报告页面查看：

- 排名靠前的与配置的邮件策略匹配的传入邮件（图形和表格格式）。
- 排名靠前的与已配置邮件策略匹配的传出邮件（图形和表格格式）。

在“传入策略”(Incoming Policies) 部分中，单击与特定邮件策略匹配的传入邮件总数，以查看“邮件跟踪”(Message Tracking) 中的邮件详细信息。

在“传出策略”(Outgoing Policies) 部分中，单击与特定邮件策略匹配的传入邮件总数，以查看“邮件跟踪”(Message Tracking) 中的邮件详细信息。

高级网络钓鱼防护页面

- 传统 Web 界面上的高级网络钓鱼防护页面，第 33 页
- 新 Web 界面上的高级网络钓鱼防护页面，第 34 页

传统 Web 界面上的高级网络钓鱼防护页面

邮件 (Email) > 报告 (Reporting) > 高级网络钓鱼防护 (Advanced Phishing Protection) 报告页面会显示以下内容：

- 已成功转发到思科高级网络钓鱼防护云服务的邮件总数。
- 未转发到思科高级网络钓鱼防护云服务的邮件总数。

注释 如果邮件元数据转发失败，则必须验证“高级网络钓鱼防护”(Advanced Phishing Protection) 功能的配置。有关详细信息，请参阅思科邮件安全设备 的 *AsyncOS* 用户指南中的“将思科邮件安全网关与思科高级网络钓鱼防护集成”一章。

您可以在“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面上查看以下内容：

- 尝试转发到思科高级网络钓鱼防护云服务的邮件总数，以图形格式显示。
- 已转发到思科高级网络钓鱼防护云服务的邮件摘要（图形格式）。

新 Web 界面上的高级网络钓鱼防护页面

监控 (Monitoring) > 高级网络钓鱼防护 (Advanced Phishing Protection) 报告页面会显示以下内容：

- 已成功转发到思科高级网络钓鱼防护云服务的邮件总数。
- 未转发到思科高级网络钓鱼防护云服务的邮件总数。

注释 如果邮件元数据转发失败，则必须验证“高级网络钓鱼防护”(Advanced Phishing Protection) 功能的配置。有关详细信息，请参阅思科邮件安全设备 的 *AsyncOS* 用户指南中的“将思科邮件安全网关与思科高级网络钓鱼防护集成”一章。

您可以在“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面上查看以下内容：

- 尝试转发到思科高级网络钓鱼防护云服务的邮件总数，以图形格式显示。

“高级恶意软件防护”（文件信誉和文件分析）报告页面

- 文件分析报告详细信息的要求 , on page 34
- 通过 SHA-256 散列标识文件 , on page 36
- 文件信誉和文件分析报告页面, on page 37
- 查看其他报告中的文件信誉过滤数据 , on page 38

文件分析报告详细信息的要求

- （云文件分析）确保管理设备可以连接到文件分析服务器 , on page 35

- （云文件分析）配置管理设备以显示详细的文件分析结果 , on page 35
- （本地文件分析）激活文件分析账户 , on page 36
- 其它要求 , on page 36

（云文件分析）确保管理设备可以连接到文件分析服务器

要获取文件分析报告详细信息，设备必须能够通过端口 443 连接到文件分析服务器。请参阅防火墙资讯中的详细信息

（云文件分析）配置管理设备以显示详细的文件分析结果

为了使组织中的所有内容安全设备都可以在云中显示有关从组织中的任何思科邮件安全设备或思科网络安全设备送交分析的文件的详细结果，您需要将所有设备加入到同一设备组。

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。

步骤 1 在旧 Web 界面中，点击**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**，然后向下滚动到“文件分析”(File Analysis) 部分。

步骤 2 如果您管理的设备指向不同的文件分析云服务器，请选择从中显示结果详细信息的文件分析服务器。

将不提供由任何其他云服务器处理的文件的结果详细信息。

步骤 3 [如果在 Cisco 安全邮件和网页管理器上禁用智能许可，则适用] 在 **组名称** 字段中输入文件分析报告的组名称，然后点击 **立即分组**。

或

[如果在 Cisco 安全邮件和网页管理器上启用智能许可，则适用] 系统自动将智能账户 ID 注册为组 ID 并在 **组名称** 字段中显示。

步骤 4 在将与此设备共享数据的每个管理设备上配置相同的组。

说明：

- 您可以随时修改组名称。编辑名称并点击 **立即分组**。此更改会立即生效；它不需要“确认”(Commit)。
- 该组名称区分大小写。在共享上传以供分析的文件的相关数据的所有设备上，此值必须是相同的。
- 建议将您的 CCOID 用于此值。
- 一台设备只能属于一个组。
- 您可以随时将设备添加到组，但是只能添加一次。
- 如果启用智能许可，则使用智能帐户 ID 对设备进行分组。

What to do next

相关主题

可以在云中查看哪些文件的详细文件分析结果？ , on page 39

（本地文件分析）激活文件分析账户

如果您已部署本地（私有云）的思科 AMP Threat Grid 设备，必须激活思科内容安全管理设备的文件分析账户，才能查看 Threat Grid 设备上提供的报告详细信息。您通常只需执行此操作一次。

Before you begin

确保您接收“严重”(Critical) 级别的系统警报。

步骤 1 首次尝试从 Threat Grid 设备访问文件分析报告详细信息时，请等待几分钟，然后您将收到包含一个链接的警报。

如果您没有收到此警报，请转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)**，然后点击**查看警报排行榜 (View Top Alerts)**。

步骤 2 点击警报消息中的链接。

步骤 3 激活您的管理设备账户。

其它要求

有关任何其他要求，请参阅安全管理设备版本的版本说明，位置：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

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（以缩写格式）。

文件信誉和文件分析报告页面

报告	说明
高级恶意软件防护	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“高级恶意软件防护”(Advanced Malware Protection) 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“高级恶意软件防护”(Advanced Malware Protection) 报告中。 **注释** 从 AsyncOS 9.6.5 开始，高级恶意软件保护报告已得到增强，以显示其他字段、图形等。升级后显示的报告不包括升级前的报告数据。要在 AsyncOS 9.6.5升级之前查看思科高级恶意软件保护报告，请点击页面底部的超链接。 **按类别划分的传入恶意软件文件**部分显示以下信息： • 从 AMP 信誉服务器接收的分类为**恶意软件**且已列入阻止列表的文件 SHA 百分比。 • 从面向终端的 AMP 控制台接收的分类为**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 AMP 控制台获取的已列入阻止列表的文件SHA百分比在报告的“传入恶意软件威胁文件”部分中显示为**简单自定义检测**。 • 从面向终端的 AMP 控制台接收的分类为**自定义阈值**且已列入阻止列表的文件 SHA 百分比。 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 AMP 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
高级恶意软件防护文件分析	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。 对于采用现场思科 AMP Threat Grid 设备的部署：在 AMP Threat Grid 设备上包含在允许列表中的文件显示为“正常”(clean)。有关允许列表的信息，请参阅 AMP Threat Grid 文档或联机帮助。 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。 要在分析了文件的服务器上查看详细信息，请参阅文件分析报告详细信息的要求 ， 第 34 页。 如果从某个已压缩或已存档的文件中提取的某个文件送交分析，则只有这个已提取文件的 SHA 值包括在“文件分析”(File Analysis) 中。 **注释** 从 AsyncOS 9.6.5 开始，文件分析报告已得到增强，以显示其他字段、图形等。升级后显示的报告不包括升级前的报告数据。要在 AsyncOS 9.6.5 升级之前查看文件分析报告，请点击页面底部的超链接。
高级恶意软件保护裁决更新	由于“高级恶意软件防护”(Advanced Malware Protection) 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 裁定更新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，请参阅邮件安全设备的相应文档。 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。在适用的报告中，“由高级恶意软件防护检测到”(Detected by Advanced Malware Protection) 列在默认情况下可能处于隐藏状态。要显示其他列，请点击表底部的“列”(Columns) 链接。

可以在云中查看哪些文件的详细文件分析结果？

如果您部署了公共云文件分析，则可以查看从已添加到文件分析设备组的任何受管设备上传的所有文件的详细结果。

如果您已将管理设备添加至组，可以查看组中的受管设备列表，单击 **管理设备 > 集中服务 > 安全设备 > 文件分析** 页面上的 **查看组中设备** 按钮。

分析组中的设备由文件分析客户端 ID 标识。要确定特定设备的此标识符，请查看以下位置：

设备	文件分析客户端 ID 的位置
邮件安全设备	**安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)** 页面上的“文件分析的高级设置”(Advanced Settings for File Analysis) 部分。
网络安全设备	**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)** 页面上的“文件分析高级设置”部分。
思科内容安全管理设备	在**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)** 页面的底部。

相关主题

- （云文件分析）配置管理设备以显示详细的文件分析结果 , on page 35

邮箱自动补救

您可以使用“邮箱自动补救”报告页查看邮箱补救结果的详细信息。使用此报告可以查看详细信息，如：

- 对其邮箱执行的补救操作成功或不成功的收件人的列表
- 对邮件执行的修复操作
- 与 SHA-256 散列关联的文件名

在以下情景中，**对其邮箱执行的补救操作不成功的收件人**字段将更新：

- 收件人不是有效的 Office 365 用户，或者收件人不属于您的设备上配置的 Office 365 域账户。
- 包含附件的邮件在邮箱中不再可用，例如，最终用户删除了邮件。
- 当设备尝试执行配置的补救操作时，您的设备与 Office 365 服务之间存在连接问题。

单击 SHA-256 散列可查看邮件跟踪中的相关邮件。

Note 升级到 AsyncOS 13.6.1 后，升级前收到的邮件的邮件跟踪状态会继续保持“已传送”(Delivered)，而不会是“已补救”(Remediated)。

“TLS 连接”页面

邮件 > 报告 > TLS 连接页会显示已发送和接收邮件的 TLS 连接的整体使用情况。该报告还显示使用 TLS 连接发送邮件的每个域的详细信息。

“TLS 连接 (TLS Connections)”页面可用于确定以下信息：

- 总体而言，哪个部分的传入/传出连接使用 TLS？
- 我与哪些合作伙伴建立成功的 TLS 连接？
- 我与哪些合作伙伴建立的 TLS 连接失败？
- 哪些合作伙伴的 TLS 证书有问题？
- 合作伙伴的全部邮件中有多少百分比使用 TLS？

Table 10: *“邮件”>“报告”>“TLS 连接”页面上的详细信息*

部分	说明
时间范围 (Time Range) （下拉列表）	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围。
传入 TLS 连接图 (Incoming TLS Connections Graph)	该图根据您选择的时间段显示上一小时、上一天或上一周内的传入 TLS 加密和未加密连接视图。
传入 TLS 连接概要 (Incoming TLS Connections Summary)	此表显示传入邮件总量、加密和未加密邮件数量，以及成功和失败的传入 TLS 加密邮件数量。
传入 TLS 邮件摘要 (Incoming TLS Message Summary)	此表显示传入邮件总量的摘要。
传入 TLS 连接详细信息 (Incoming TLS Connections Details)	下表显示发送或接收加密邮件的域的详细信息。对于每个域，您可以查看连接总数、已发送的邮件，以及成功或失败的 TLS 连接数量。您还可以查看每个域的成功和失败连接的百分比。
传出 TLS 连接图 (Outgoing TLS Connections Graph)	该图根据您选择的时间段显示上一小时、上一天或上一周内的传出 TLS 加密和未加密连接视图。
传出 TLS 连接概要 (Outgoing TLS Connections Summary)	此表显示传出邮件总量、加密和未加密邮件数量，以及成功和失败的传出 TLS 加密邮件数量。
传出 TLS 邮件摘要 (Outgoing TLS Message Summary)	此表显示传出邮件总量。
传出 TLS 连接详细信息 (Outgoing TLS Connections Details)	下表显示发送或接收加密邮件的域的详细信息。对于每个域，您可以查看连接总数、已发送的邮件、成功或失败的 TLS 连接数量，以及最后的 TLS 状态。您还可以查看每个域的成功和失败连接的百分比。

入站 SMTP 身份验证页面

“入站 SMTP 身份验证”(Inbound SMTP Authentication)页面显示如何使用客户端证书和 SMTP AUTH 命令对邮件安全设备与用户的邮件客户端之间的 SMTP 会话进行验证。如果设备接受证书或 SMTP AUTH 命令，则会建立到邮件客户端的 TLS连接 ，供客户端用来发送邮件。因为设备无法逐个用户跟踪这些尝试，因此报告会根据域名和域 IP 地址显示有关 SMTP 身份验证的详细信息。

使用此报告可确定以下信息：

- 总体而言，多少入站连接使用 SMTP 身份验证？
- 多少连接使用经过认证的客户端？
- 多少连接使用 SMTP AUTH？
- 当尝试使用 SMTP 身份验证时，哪些域无法连接？
- 当 SMTP 身份验证失败时，多少连接成功使用回退？

“入站 SMTP 身份验证”(Inbound SMTP Authentication) 页面包含一个表示已接收的连接的图形、一个表示已尝试 SMTP 身份验证连接的邮件收件人的图形，以及一个包含有关对连接进行身份验证的尝试的详细信息的表。

“已接收的连接”(Received Connections) 图形显示在指定时间范围内来自尝试使用 SMTP 身份验证对其连接进行身份验证的邮件客户端的传入连接。该图表显示设备接收的连接总数、未尝试使用 SMTP 身份验证进行验证的次数，使用客户端证书验证连接的成功和失败次数，以及使用 SMTP AUTH 命令进行验证的成功和失败次数。

“已接收的收件人”(Received Recipients) 图形显示了收件人的数量，这些收件人的邮件客户端尝试对其与邮件安全设备的连接进行身份验证以使用 SMTP 身份验证来发送邮件。该图形还显示其连接已进行身份验证的收件人数和其连接未进行身份验证的收件人数。

“SMTP 身份验证详细信息”(SMTP Authentication details) 表显示了域的详细信息，这些域的用户尝试对其与邮件安全设备的连接进行身份验证以发送邮件。对于每个域，可以查看尝试使用客户端证书进行连接的成功或失败次数、尝试使用 SMTP AUTH 命令进行连接的成功或失败次数，以及在客户端证书连接尝试失败后回退到 SMTP AUTH 的次数。可以使用页面顶部的链接按域名或域 IP 地址显示此信息。

速率限制页面

通过按信封发件人进行速率限制，您可以根据发件人地址从单个发件人限制每个时间间隔的邮件收件人数。“速率限制”(Rate Limits) 报告显示最严重超过此限制的发件人。

使用此报告可帮助确定以下内容：

- 可能用于批量发送垃圾邮件的有漏洞用户账户。
- 组织中的失控应用程序，这些应用程序使用邮件发送通知、风险通告、自动声明等内容。
- 组织中具有大量邮件活动的来源，用于内部计费或资源管理目的。
- 可能未被视为垃圾邮件的大量入站邮件流量的来源。

请注意，包含内部发件人（例如内部用户或传出邮件发件人）的统计信息的其他报告仅测量已发送的邮件数；它们不会向大量收件人表明少数邮件的发件人的身份。

“按事件划分的排名靠前的危害”图表显示最频繁尝试向超过配置限制的收件人发送邮件的信封发件人。每次尝试都是一个事件。此图表汇总所有侦听程序的事件计数。

“按已拒绝收件人划分的排名靠前的危害”图表显示向高于配置限制的最大数量的收件人发送邮件的信封发件人。此图表汇总所有侦听程序的收件人计数。

速率限制设置（包括“信封发件人的速率限制 (Rate Limit for Envelope Senders)”设置）在邮件安全设备的“邮件策略 (Mail Policies)”>“邮件流量策略 (Mail Flow Policies)”中配置。有关速率限制的详细信息，请参阅邮件安全设备的文档或在线帮助。

相关主题

- 大量邮件 , on page 28

“爆发过滤器”(Outbreak Filters) 页面

邮件 > 报告 > 爆发过滤器页显示有关最近的爆发的信息，并显示由于“爆发过滤器”而隔离的邮件的相关信息。您可以使用此页面可以监控对针对性的病毒、诈骗和网络钓鱼攻击的防御。

使用“爆发过滤器”(Outbreak Filters) 页面可回答以下类型的问题：

- 多少封邮件被隔离？依据的是哪项“爆发过滤器”(Outbreak Filters) 规则？
- “爆发过滤器”(Outbreak Filters) 功能一直针对病毒爆发提供多久的提前时间？
- 本地病毒爆发与全球病毒爆发相比如何？
- 邮件在病毒爆发隔离区中停留多长时间？
- 哪些可能是恶意的 URL 是最常见的？

“按类型划分的威胁”(Threats By Type) 部分显示设备接收的不同类型的威胁邮件。“威胁摘要”(Threat Summary) 部分按“病毒”(Virus)、“网络钓鱼”(Phish) 和“诈骗”(Scam) 细分邮件。

“过去一年爆发摘要 (Past Year Outbreak Summary)”会列出过去一年的全局及局部爆发，以便将局部网络趋势与全局趋势进行比较。全局爆发列表是所有爆发情况（包括病毒和非病毒）的超集，而局部爆发仅限于影响设备的病毒爆发。局部爆发数据不包括非病毒威胁。全局病毒爆发数据表示威胁操作中心检测到的所有病毒爆发，该数据超过病毒爆发隔离区的当前配置的阈值。本地病毒爆发数据表示在此设备上检测到的所有病毒爆发，该数据超过病毒爆发隔离区的当前配置的阈值。“本地防护总时间”(Total Local Protection Time) 始终基于威胁操作中心检测到各病毒爆发的时间与主要供应商发布防病毒签名的时间之间的时间差。请注意，并非每个全局爆发都会影响设备。值“--”表示保护时间不存在，或防病毒供应商未提供特征码时间（某些供应商可能不报告特征码时间）。这并不表示保护时间为零，而是表示计算保护时间所需的信息不可用。

“隔离的邮件”(Quarantined Messages) 部分汇总爆发过滤器隔离情况，是测量爆发过滤器捕获的潜在威胁邮件数的有用计量器。隔离的邮件在放行时计数。通常，邮件在防病毒和反垃圾邮件规则可用之前会被隔离。放行时，它们会被防病毒和反垃圾邮件软件进行扫描并确定是阳性还是正常邮件。由于爆发跟踪的动态性质，当邮件处于隔离区中时，用于隔离邮件的规则（甚至关联的爆发）可能会更改。在放行时（而不是在进入隔离区中时）对邮件进行计数可避免混淆计数增加和减少的情况。

“威胁详细信息”(Threat Details) 列表显示有关特定病毒爆发的信息，包括威胁类别（病毒、诈骗或网络钓鱼）、威胁名称、该威胁的说明和识别的邮件数。对于病毒爆发，“过去一年病毒爆发 (Past

Year Virus Outbreaks)”包括爆发名称和 ID、首次全局出现病毒爆发的时间和日期、爆发过滤器提供的保护时间以及隔离的邮件数。您可以选择是要查看全球还是本地爆发。

“在全球首次发现”(First Seen Globally) 时间由威胁行动中心根据来自 SenderBase 的数据确定，SenderBase 是全球最大的邮件和网络流量监控网络。保护时间始终基于威胁操作中心检测到各个威胁的时间与主要供应商发布防病毒特征码的时间之间的差异。

值为“--”表示防护时间不存在，或者防病毒供应商未提供签名时间（某些供应商可能不会报告签名时间）。这并不表示防护时间为零。相反，这表示计算保护时间所需的信息不可用。

此页面上的其他模块提供：

- 爆发过滤器在所选时间段处理的传入邮件的数量。

非病毒性威胁包括网络钓鱼邮件、诈骗和使用指向外部网站的链接进行的恶意软件分发。

- 爆发过滤器捕获的威胁严重性。

级别 5 威胁表示在范围或影响方面非常严重，而级别 1 威胁表示威胁风险较低。有关威胁级别的说明，请参阅邮件安全设备的在线帮助或用户指南。

- 邮件在爆发隔离区中存在的时间长度。

此持续时间取决于系统需要多长时间收集关于潜在威胁的足够数据以对其安全性做出判定。带有病毒性威胁的邮件通常比带有非病毒性威胁的邮件在隔离区中花费更多时间，因为它们必须等待防病毒程序更新。还会反映您为每个邮件策略指定的最大保留时间。

- 最频繁重写的 URL，重写的目的是将邮件收件人重定向到思科网络安全代理，以便在收件人点击邮件中可能是恶意的链接时对网站进行点击时间评估。

此列表可能包括非恶意的 URL，因为如果邮件中的任何 URL 被视为恶意，则邮件的所有 URL 均会被重写。

Note 为了正确填充“爆发过滤器”(Outbreak Filters) 报告页上的各个表，设备必须能够与中指定的思科更新服务器进行通信。管理设备 (Management Appliance) > 系统管理 (System Administration) > 更新设置 (Update Settings)。

有关详细信息，请参阅的爆发过滤器章节。

灰色邮件报告

以下报告中反映了灰色邮件统计信息：

报告	包含以下灰色邮件数据
“邮件流摘要”页面 > “传入”选项卡	每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。
“邮件流详细信息”页面 > “传出发件人”选项卡	排名靠前的灰色邮件发件人。

报告	包含以下灰色邮件数据
“邮件流详细信息”页面>“传入邮件”选项卡	所有IP地址、域名或网络所有者的每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。
“用户邮件摘要”页面 > “按灰色邮件排名靠前的用户”	接收灰色邮件的排名靠前的最终用户。
“用户邮件摘要”页面 > 用户邮件详细信息	所有用户的每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。

相关主题

- 在升级到 AsyncOS 9.5 后报告营销邮件 , on page 44

在升级到 AsyncOS 9.5 后报告营销邮件

在升级到 AsyncOS 9.5 后：

- 营销邮件的数量是在升级前后检测到的营销邮件之和。
- 灰色邮件总数不包括在升级之前检测到的营销邮件数量。
- 尝试的邮件总数还包括在升级前检测到的营销邮件数量。
- 如果未在托管的邮件安全设备上启用灰色邮件功能，则营销邮件会被计为正常邮件。

系统容量页面

邮件 > 报告 > 系统容量页详细地表示了系统负载，包括工作队列中的邮件、传入和传出邮件（量、大小和数量）、CPU 总体使用率、按功能列出的 CPU 使用率和内存页面交换信息。

“系统容量 (System Capacity)”页面可用于确定以下信息：

- 确定邮件安全设备何时超出推荐的 CPU 容量；这可用于确定何时需要优化配置或添加设备。
- 确定系统行为方面指向即将发生的容量问题的历史趋势。
- 要进行故障排除，需确定系统的哪些部分使用大多数资源。

监控邮件安全设备以确保容量适合邮件量。随着时间的推移，邮件量会不可避免地增加，适当的监控可确保主动添加容量或进行配置更改。监控系统容量的最有效方式是跟踪总量、工作队列中的邮件数，以及“资源节约模式”(Resource Conservation Mode) 的事件数。

- **量**：了解您的环境中的“正常”邮件量和“异常”尖峰非常重要。随着时间的推移跟踪此数据以测量邮件量增长。您可以使用“传入邮件”(Incoming Mail) 和“传出邮件”(Outgoing Mail) 页面长期跟踪数量。有关详细信息，请参阅系统容量 - 传入邮件, on page 46和系统容量 - 传出邮件, on page 46。
- **工作队列 (Work Queue)**：工作队列旨在作为“减震器”- 缓冲并过滤垃圾邮件攻击，并处理非垃圾邮件的异常增加。但是，工作队列也可能表明系统处于压力之下。拖延和频繁的工作队列

备份可能表示存在容量问题。可以使用“系统容量 - 工作队列 (System Capacity – Workqueue)”页面跟踪工作队列中的活动。有关详细信息，请参阅系统容量 - 工作队列, on page 45。

- **资源节约模式 (Resource Conservation Mode)**：当设备变得过载时，它会进入“资源节约模式”(Resource Conservation Mode, RCM) 并发送“严重”(CRITICAL) 系统警报。这旨在保护设备，使其可以处理任何邮件积压情况。设备不应频繁进入RCM，并且应仅在邮件量出现超大或异常增长期间进入。频繁的 RCM 警报可能表明系统正在超负荷。请参阅资源节约活动 , on page 47。

如何解释在“系统容量”(System Capacity) 页面上看到的数据

当选择时间范围来查看“系统容量”(System Capacity) 页面上的数据时，记住以下内容非常重要：

- 日报告 (Day Report) - 日报告查询小时表并显示设备在 24 小时内每小时收到的准确查询数量。此信息收集自小时表。这是一个准确的数字。
- 月报告 - 月报告查询 30 或 31 天（取决于该月份的实际天数）的日表，为您提供 30 或 31 天内查询数量的确切报告。再次重申，这是一个精确的数字。

“系统容量”(System Capacity) 页面上的“最大值”(Maximum) 值指示符是在指定时间段内看到的最高值。“平均值”(Average) 值是指定时间段内所有值的平均值。汇聚的时间取决于为该报告选择的时间间隔。例如，如果图表表示某个月时间段，您可以选择查看每天的“平均值”(Average) 和“最大值”(Maximum) 值。

可以点击特定图表的“查看详细信息 (View Details)”链接以查看各个邮件安全设备的数据以及连接到安全管理设备的设备的总体数据。

系统容量 - 工作队列

“工作队列”(Workqueue) 页面显示邮件在工作队列中花费的平均时间，在垃圾邮件隔离区中或在策略、病毒或病毒爆发隔离区中花费的任何时间除外。您可以查看时间段，从一小时到一个月。此平均值可以帮助确定延迟邮件传送的短期事件和确定系统上工作负载的长期趋势。

Note 如果邮件从隔离区释放到工作队列中，“工作队列中的平均时间”指标将忽略此时间。这可防止重复计数，以及由于在隔离区中花费的时间延长而造成统计信息失真。

此报告也显示指定时间段内的工作队列中的邮件量，并且显示相同时间段内工作队列中的最大邮件数量。工作队列中的最大邮件数图表还显示工作队列阈值级别。

工作队列图形中的偶尔峰值是正常的，并在预期之内。如果工作队列中的邮件数长时间保持高于配置的阈值，可能表示存在容量问题。这种情况下，请考虑调整阈值级别或审核系统配置。

要更改工作队列阈值级别，请参阅调整邮件安全设备的系统运行状况图中的参考阈值。

Tip 当查看工作队列页面时，您可能要测量工作队列备份的频率，并标注超过 10000 封邮件的工作队列备份。

系统容量 - 传入邮件

“系统容量”(System Capacity) 下的“传入邮件”(Incoming Mail) 页面显示传入连接、传入邮件总数、平均邮件大小和传入邮件总大小。您可以查看一天、一周、一月或一年的结果。了解环境中的正常邮件量和尖峰的趋势非常重要。您可以使用“系统容量”(System Capacity) 下的“传入邮件”(Incoming Mail) 页面跟踪一段时间内的邮件量增长并为系统容量制定计划。您可能还希望将传入邮件数据与发件人配置文件数据进行比较，以查看从特定域发送到网络的邮件的邮件量趋势。

Note 传入连接数增加不一定会影响系统负载。

系统容量 - 传出邮件

“系统容量”(System Capacity) 下的“传出邮件”(Incoming Mail) 页面显示传出连接、传出邮件总数、平均邮件大小和传出邮件总大小。您可以查看一天、一周、一月或一年的结果。了解环境中的正常邮件量和尖峰的趋势非常重要。您可以使用“系统容量”(System Capacity) 下的“传出邮件”(Outgoing Mail) 页面跟踪一段时间内的邮件量增长并为系统容量制定计划。您可能还希望将传出邮件数据与外发目标数据进行比较，以查看从特定域或 IP 地址发送的邮件的邮件量趋势。

系统容量 - 系统负载

系统负载报告显示如下信息：

- CPU 总体使用情况, on page 46
- 内存页面交换, on page 46
- 资源节约活动 , on page 47

CPU 总体使用情况

邮件安全设备经过优化，可使用空闲 CPU 资源提高邮件吞吐量。高 CPU 使用率并不一定表示存在系统容量问题。如果高CPU使用率与持续的大容量内存页面交换一同出现，则可能表示存在容量问题。

Note 此图还指明了一个仅用于视觉参考的CPU使用率阈值。要调整此行的位置，请参阅调整邮件安全设备的系统运行状况图中的参考阈值。您可以将邮件安全设备配置为向您发送警报，建议您可以为解决容量问题采取什么操作。

该页面还包含一个图，用于显示不同功能（包括邮件处理、垃圾邮件和病毒引擎、报告和隔离）使用的 CPU 量。按功能划分的 CPU 图形可以很好地指示产品的哪些方面在系统上使用最多资源。如果需要优化设备，则此图有助于确定哪些功能可能需要调整或禁用。

内存页面交换

内存页面交换图形显示了系统必须分页到磁盘的频率（以每秒千字节数为单位）。

系统旨在定期交换内存，因此发生一些内存交换在意料之中，并不是表明设备有问题。除非系统一致地大量交换内存，否则内存交换正常，并且是预期行为（尤其在C170设备上）。为提高性能，您可能需要将邮件安全设备添加到网络或调整配置以确保实现最大吞吐量。

Note 此图还指明了一个仅用于视觉参考的内存页面交换阈值。要调整此行的位置，请参阅调整邮件安全设备的系统运行状况图中的参考阈值。您可以将邮件安全设备配置为向您发送警报，建议您可以为解决容量问题采取什么操作。

资源节约活动

资源节约活动图显示邮件安全设备进入资源节约模式 (RCM) 的次数。例如，如果图中显示 n 次，则意味着设备进入了 RCM n 次，并已退出至少 n-1 次。

设备应当很少进入 RCM 模式，并且仅在邮件量非常大或异常增加时才进入此模式。如果“资源节约活动”(Resource Conservation Activity) 图显示您的设备频繁进入 RCS，则可能表明系统变得过载。

系统容量 - 全部

全部 (All) 页面将所有以前的系统容量报告整合到单个页面，使您可以查看不同报告之间的关系。例如，您可能发现消息队列很高，同时发生过多的内存切换。这可能表明存在容量问题。您可能希望将此页面另存为 PDF 文件，以保留系统性能的快照，供以后参考（或与支持人员共享）。

系统容量图形中的阈值指示符

在某些图形中，某行表示默认值，如果频繁或始终如一地超过该值，则可能表明存在问题。要调整此可视指示符，请参阅调整邮件安全设备的系统运行状况图中的参考阈值。

报告数据可用性 (Reporting Data Availability) 页面

使用**邮件 > 报告 > 报告数据可用性**页面可以查看、更新数据和对数据排序，实时洞察资源利用率和邮件流量故障点。

所有数据资源利用率和邮件流量问题位置都显示在此页面上，包括由安全管理设备管理的整体设备的数据可用性。

在此报告页面中，还可以查看特定设备和时间范围的数据可用性。

了解新 Web 界面上的“邮件报告”页面

注释 此列表显示 Web 界面**报告**下拉列表中邮件安全设备的 AsyncOS 最新支持版本中可用的报告。有关详细信息，请参阅使用交互式报告页面。如果您的邮件安全设备运行的是早期版本的 AsyncOS，并非上述所有报告均可用。

表 *11:* 邮件报告下拉选项

报告下拉选项	操作
“邮件流摘要”页面	“邮件流摘要”报告页面提供您的邮件安全设备上的活动概要。它包括传入和传出邮件的图和摘要表。 有关详细信息，请参阅“邮件流摘要”页面 ， 第 52 页。
系统容量页面	“系统容量”报告页显示发送到安全管理设备的报告数据的总工作量的详细信息。 有关详细信息，请参阅系统容量页面 ， 第 57 页。
文件和恶意软件报告	
”高级恶意软件保护“页面（文件信誉和文件分析）	“高级恶意软件保护”报告页显示报告视图，其中展示针对传入和传出基于文件的威胁的摘要、文件信誉、文件分析、文件追溯和邮箱自动补救的详细信息。 有关详细信息，请参阅“高级恶意软件保护”页面 ， 第 60 页。
“病毒过滤”页面	“病毒过滤”报告页面概述了从您的网络发送的病毒和发送到您的网络的病毒。此页面显示已由运行于邮件安全设备之上的病毒扫描引擎检测到并且显示在安全管理设备上的病毒。使用此报告针对特定病毒采取相应措施。 有关详细信息，请参阅“病毒过滤”(Virus Filtering) 页面 ， 第 66 页。
“宏检测”页	“宏检测”(Macro Detection) 报告页显示内容过滤器和邮件过滤器检测到的启用宏的传入和传出附件排行榜，这些附加按文件类型分类。 有关详细信息，请参阅“宏检测”(Macro Detection) 页面 ， 第 67 页。
电子邮件威胁报告	
“DMARC 验证”页面	“DMARC 验证”报告页面显示未通过基于域的邮件身份验证、报告和一致性 (DMARC) 验证的发件人域排行榜，并显示对来自每个域的传入邮件执行的各项操作摘要。 有关详细信息，请参阅“DMARC 验证”(DMARC Verification) 页面 ， 第 68 页。
“病毒爆发过滤”页面	“病毒爆发过滤器”(Outbreak Filters) 页面显示了有关最近的病毒爆发和由病毒爆发过滤器隔离的邮件的信息。使用此页面可监控针对网络钓鱼、垃圾邮件、病毒和恶意软件攻击的防御。 有关详细信息，请参阅“病毒爆发过滤”页面 ， 第 69 页。

报告下拉选项	操作
“URL 过滤”页面	使用此页面可以查看邮件中出现最频繁的 URL 类别、垃圾邮件中最常见的 URL 以及邮件中可见的恶意和可疑 URL 的数量。 有关详细信息，请参阅“URL 过滤”(URL Filtering) 页面 ， 第 71 页。
“URL 追溯报告”页面	“URL 追溯报告”页面显示由 URL 追溯服务处理的 URL。此页面列出恶意 URL、从 URL 追溯服务收到判定的日期和时间，以及受影响邮件的补救状态。 有关详细信息，请参阅“URL 追溯报告”(URL Retrospection Report) 页面 ， 第 72 页。
“伪造邮件检测”页面	“伪造邮件检测”报告页包括以下报告: • **排名靠前的伪造邮件检测**。显示内容字典中与传入邮件中的伪造“发件人：”信头匹配的前十个用户。 • **伪造邮件检测：详细信息**。显示内容词典中与传入邮件中的伪造“发件人：”信头匹配所有用户的列表，对于给定用户，还会显示匹配的邮件的数量。 有关详细信息，请参阅“伪造邮件检测”页面 ， 第 72 页。
“发件人域信誉”页面	您可以使用此报告页面，根据从SDR服务接收的判定和威胁类别查看传入邮件 有关详细信息，请参阅“发件人域信誉”(Sender Domain Reputation) 页面 ， 第 73 页。
“外部威胁源”页面	“外部威胁源”(External Threat Feeds) 页面显示下列报告： • 排名靠前的用于检测邮件威胁的 ETF 来源。 • 排名靠前的与检测到的邮件威胁相匹配的 IOC。 • 排名靠前的用于过滤恶意传入邮件连接的 ETF 来源 有关详细信息，请参阅外部威胁源页面 ， 第 73 页。
安全打印	您可以使用“安全打印”(Safe Print) 报告页面查看： • 以图形格式显示的基于文件类型的安全打印附件的数量。 • 基于表格格式的文件类型的安全打印附件摘要。 有关详细信息，请参阅“安全打印”(Safe Print) 页面 ， 第 33 页。

报告下拉选项	操作
高级网络钓鱼防护页面	您可以在“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面上查看以下内容： • 已成功转发到思科高级网络钓鱼防护云服务的邮件总数。 • 未转发到思科高级网络钓鱼防护云服务的邮件总数。 有关详细信息，请参阅高级网络钓鱼防护报告页面，第 74 页。
连接和流报告	
“邮件流详细信息”页面	“邮件流详细信息”报告页为连接到托管邮件安全设备的所有远程主机提供实时信息的交互报告。您可以收集有关发送邮件到您的系统的 IP 地址、域和网络所有者（组织）的信息。 有关详细信息，请参阅“邮件流详细信息”页面，第 74 页。
“发件人组”页面	“发件人组报告”(Sender Groups report) 页面按发件人组和邮件流策略操作提供连接摘要，允许您查看 SMTP 连接和邮件流策略趋势。 有关详细信息，请参阅“发件人组”(Sender Groups) 页面，第 81 页。
“外发目标”(Outgoing Destinations) 页面	“外发目标”报告页面提供有关您的组织向其发送邮件的各个域的信息。页面顶部包括按传出威胁邮件描绘外发目标排行榜的图形，以及按传出正常邮件描绘外发目标排行榜的图形。页面底部显示一个按收件人总数对列排序（默认设置）的图表。 有关详细信息，请参阅“外发目标”(Outgoing Destinations) 页面，第 81 页。
“TLS 加密”页面	“TLS 加密”报告页面显示所收发邮件的 TLS 连接的整体使用情况。该报告还显示使用 TLS 连接发送邮件的每个域的详细信息。 有关详细信息，请参阅“TLS 加密”(TLS Encryption) 页面，第 83 页。
入站 SMTP 身份验证页面	“入站 SMTP 身份验证”报告页面显示使用客户端证书和“SMTP AUTH”命令对邮件安全设备与用户的邮件客户端之间的 SMTP 会话进行身份验证。 有关详细信息，请参阅入站 SMTP 身份验证页面，第 86 页。
速率限制页面	“速率限制”报告页面显示了超过您为每个发件人的邮件收件人数量设置的阈值的邮件发件人（根据 MAIL-FROM 地址）。 有关详细信息，请参阅速率限制页面，第 88 页。

报告下拉选项	操作
“按国家/地区划分的连接”页面	“按国家/地区连接”报告页显示： • 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。 • 以表格格式显示的基于源国家/地区的传入邮件连接和邮件总数。 有关详细信息，请参阅“按国家/地区划分的连接”页面，第 88 页。
域保护页面	您可以使用设备新 Web 界面的“域保护”(Domain Protection) 报告页面查看： • 分类为合法或威胁的邮件摘要（图形格式）。 • 基于发件人的目标域摘要摘要（表格格式）。 有关详细信息，请参阅域保护页面，第 89 页。
用户报告	
“用户邮件摘要”页	“用户邮件摘要”报告按邮件地址提供有关您的内部用户发送和接收的邮件的信息。单一用户可以有多个邮件地址。报告中未合并邮件地址。 有关详细信息，请参阅用户邮件摘要，第 89 页。
“DLP 事件摘要”页面	“DLP事件摘要”报告页面显示传出邮件中发生的防数据丢失(DLP)策略违规事件的信息。 有关详细信息，请参阅“DLP 事件摘要”(DLP Incident Summary)页面，第 92 页。
“网络交互”页面	“网络交互” (Web Interaction) 报告页面标识单击了由策略或病毒爆发过滤器重写的 URL 的最终用户，以及与每次用户单击相关联的操作。 有关详细信息，请参阅“网络交互”(Web Interaction) 页面，第 93 页。

报告下拉选项	操作
补救报告页面	现在，您可以使用补救报告来监控邮箱自动补救以及邮箱搜索和补救的补救结果。 此报告提供以下内容的摘要： • 使用邮箱自动补救以及邮箱搜索和补救进行补救的邮件总数。 • 为已配置的补救操作成功补救的邮件数。 • 补救失败的邮件数。 单击报告中的“邮箱自动补救”(Mailbox Auto Remediation) 和“邮箱搜索和补救”(Mailbox Search and Remediate) 选项卡，查看有关尝试进行补救的邮件的详细信息。 有关更多信息，请参阅 补救报告页面 ，第 95 页
过滤器报告	
“邮件过滤器”页面	“邮件过滤器”报告页面显示有关传入和传出邮件的邮件过滤器匹配项排行榜的信息（那些邮件过滤器具有最大数量的匹配邮件）。 有关详细信息，请参阅“邮件过滤器”(Message Filters) 页面 ，第 96 页。
“大量邮件”页面	“大量邮件”报告页面标识了涉及来自单个发件人的大量邮件的攻击或在移动一小时期间内具有相同对象的攻击。 有关详细信息，请参阅“大量邮件”(High Volume Mail) 页面 ，第 97 页。
“内容过滤器”页面	“内容过滤器”报告页面显示有关传入和传出内容过滤器匹配项排行榜的信息（那些内容过滤器具有最多的匹配邮件）。该页面还以条形图和列表的形式显示数据。 有关详细信息，请参阅“内容过滤器”(Content Filters) 页面 ，第 97 页。

“邮件流摘要”页面

安全管理设备上的“邮件流摘要”报告页面提供您的邮件安全设备的邮件活动的概要。“邮件流摘要”页面包括传入邮件和传出邮件的图形和摘要表。

“邮件流摘要：传入”报告页面显示由设备处理和阻止的邮件总数以及传入邮件摘要的传入邮件图表。

您可以使用此页面上的邮件趋势图来根据所选的时间范围监控设备处理和阻止的所有传入邮件的流。有关详细信息，请参阅选择报告的时间范围。

要在您的数据中搜索特定信息，请参阅 搜索与交互式邮件报告页面 ，第 6 页

以下邮件趋势图提供传入邮件流的视觉表达。

- 威胁检测摘要
- 内容摘要

您可以根据相应类别的所需计数器查看传入邮件的邮件趋势。有关详细信息，请参阅使用计数器过滤趋势图上的数据。

“邮件流摘要：传出”报告页面显示由设备处理和传送的邮件总数以及传出邮件摘要的传出邮件图表。

您可以使用此页面上的邮件趋势图来根据所选的时间范围监控设备处理和传送的所有传出邮件的流。有关详细信息，请参阅选择报告的时间范围。

以下邮件趋势图提供传出邮件的邮件流的视觉表达。

您可以根据所处理邮件的所需计数器查看传出邮件的邮件趋势。有关详细信息，请参阅使用计数器过滤趋势图上的数据。

以下列表解释“邮件流摘要”报告页面上的各部分：

表 *12*:“邮件流摘要”页面上的详细信息

部分	说明
邮件流摘要：传入	
邮件数量	“邮件数量”图表提供所处理邮件总数的视觉表达，包括处理为威胁邮件的邮件。
威胁邮件	“威胁邮件”图表提供邮件安全设备阻止的邮件总数的视觉表达。
威胁检测摘要	“威胁检测摘要邮件”趋势图提供基于以下类别的视觉表达： • **连接和信誉过滤**：由信誉过滤和无效收件人归类为威胁的邮件。 • **垃圾邮件检测**：被反垃圾邮件扫描引擎归类为威胁的邮件。 • **邮件欺骗**：由于DMARC验证失败而被归类为威胁的邮件。 • **病毒爆发威胁摘要**：由病毒爆发过滤引擎归类为网络钓鱼、欺诈、病毒或恶意软件的邮件。 • **附件和恶意软件检测**：被防病毒和 AMP 引擎归类为威胁的邮件。 • **所有类别**：归类为威胁的所有邮件。

部分	说明
内容摘要	“内容摘要”邮件趋势图提供基于以下类别的视觉表达： • **灰色邮件**：归类为市场营销、批量或社交网络的邮件。 • **内容过滤器**：由内容过滤器分类的邮件。 • **所有类别**：由灰色邮件引擎和内容过滤器分类的所有邮件。
邮件流摘要：传出	
邮件数量	“邮件数量”图表提供所处理邮件总数的视觉表达，包括处理为正常邮件的邮件。
邮件传输	“邮件传送”图表提供所传送邮件的视觉表达，包括硬退回。
传出邮件	“传出邮件”趋势图提供基于以下类别的视觉表达： • 垃圾邮件 • 病毒邮件 • 由 AMP 检测到 • 由内容过滤器拦截 • DLP 拦截

相关主题

- 设备如何对邮件分类，第 14 页
- 如何对传入邮件计数，第 14 页
- 在“邮件流摘要”页面上对邮件进行分类，第 55 页

如何对传入邮件计数

传入邮件的计数取决于每封邮件的收件人数。例如，从 example.com 发送给三个收件人的一封传入邮件被计为来自该发件人的三封邮件。

由于由发件人信誉过滤拦截的邮件不会实际进入工作队列，因此设备无权访问传入邮件的收件人列表。在此情况下，将使用倍数来估算收件人的数量。此倍数基于对大量现有客户数据样本的研究。

设备如何对邮件分类

由于邮件持续通过邮件管道，因此其可以应用于多个类别。例如，邮件可以标记为垃圾邮件或病毒邮件；它还可以与内容过滤器相匹配。各种过滤器和扫描活动的优先顺序会极大地影响邮件处理的结果。

在上面的示例中，各种判定遵循以下优先顺序规则：

- 垃圾邮件
- 病毒邮件
- 匹配内容过滤器

按照这些规则，如果某个邮件被标记为具有垃圾邮件特征，并且您的反垃圾邮件设置被设置为丢弃具有垃圾邮件特征的邮件，则该邮件将被丢弃，垃圾邮件计数器会增加。

此外，如果反垃圾邮件设置被设置为允许具有垃圾邮件特征的邮件继续在邮件通道中通行，并且后续内容过滤器将会丢弃、退回或隔离该邮件，则垃圾邮件计数器仍会增加。仅当该邮件不具有垃圾邮件或病毒特征时，内容过滤器才会增加。

或者，如果邮件被爆发过滤器隔离，则在该邮件从隔离中释放出来并再次进入工作队列之前，不会进行计数。

有关邮件处理优先级的完整信息，请参阅邮件安全设备在线帮助或用户指南中有关邮件通道的章节。

在“邮件流摘要”页面上对邮件进行分类

被视为威胁的传入邮件以及在“邮件流摘要”报告页面中传送的传出邮件按照如下方式进行分类：

表 *13*:“邮件流摘要”页面上的邮件类别

类别	说明
邮件流摘要：传入	
信誉过滤	由 HAT 策略拦截的所有连接乘以一个固定倍数（请参阅如何对传入邮件计数，第 14 页），再加上由收件人限制拦截的所有收件人。 “由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 值的计算取决于多种因素： • 此发件人的“受限制”邮件数量。 • 被拒绝或被 TCP 拒绝的连接数量（可能是部分计数）。 • 每个连接的邮件数量的保守倍数。 当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。在这种情况下，所显示的值可以解释为指示被拦截的最小邮件数的值。 “邮件流摘要”报告页面上的“信誉过滤”总数和百分比始终基于所有被拒绝连接的完整计数。只有每个发件人的连接计数会因负载而受到限制。
无效收件人	除所有 RAT 拒绝外，还包括会话 LDAP 拒绝所拒绝的所有邮件收件人的总数和百分比。
反垃圾邮件	反垃圾邮件扫描引擎检测为具有垃圾邮件特征或可疑的传入邮件总数和百分比。此外还包括同时是垃圾邮件和具有病毒特征的邮件。

类别	说明
防病毒	被检测为具有病毒特征但不是垃圾邮件的传入邮件总数和百分比。 以下消息计入 " 检测到病毒 " 类别中： • 病毒扫描结果为“已修复”(Repaired) 或“感染”(Infectious) 的邮件 • 在选中了将已加密的邮件计为包含病毒的选项时，病毒扫描结果为“已加密”(Encrypted) • 在针对不可扫描的邮件执行的操作不是“传送”(Deliver) 时，病毒扫描结果为“不可扫描”(Unscannable) • 在选中了传送到备用邮件主机或备用收件人的选项时，病毒扫描结果为“不可扫描”(Unscannable) 或“已加密”(Encrypted) 的邮件 • 以手动方式或通过超时从“病毒爆发”(Outbreak) 隔离区删除的邮件。
高级恶意软件防护	文件分析服务阻止的传入邮件的总数和百分比。 文件信誉过滤发现邮件附件是恶意软件。该值不包括通过文件分析发现为恶意的判定更新或文件。
内容过滤器	由邮件和内容过滤器拦截的传入邮件的总数和百分比。
DMARC 策略	DMARC 验证策略失败的传入邮件的总数和百分比。
S/MIME 验证/解密失败	未通过 S/MIME 验证和/或解密的传入邮件的总数和百分比。
邮件流摘要：传出	
硬退回	永久无法传送的传出邮件的总数和百分比。
已送达	已传送的传出邮件的总数和百分比。

注释 如果您已配置防病毒设置以传送不可扫描或已加密的邮件，这些邮件将被计为正常邮件，而不是病毒。否则，邮件将被计入具有病毒特征的邮件。

此外，如果邮件与某个邮件过滤器相匹配，且未被该过滤器丢弃或退回，则这些邮件被视为正常邮件。邮件过滤器丢弃或退回的邮件不计入总数。

相关主题

“邮件流详细信息”页面，第 74 页

系统容量页面

“系统容量”报告页面详细地表示了系统负载，包括工作队列中的邮件、传入和传出邮件（量、大小和数量）、CPU 总体使用率、按功能列出的 CPU 使用率和内存页面交换信息。

“系统容量”报告页面可用于确定以下信息：

- 确定邮件安全设备何时超出推荐的 CPU 容量；这可用于确定何时需要优化配置或添加设备。
- 确定系统行为方面指向即将发生的容量问题的历史趋势。
- 要进行故障排除，需确定系统的哪些部分使用大多数资源。

要在安全管理设备上查看“系统容量”(System Capacity) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 系统容量 (System Capacity)**。有关详细信息，请参阅使用交互式报告页面。

您可以监控邮件安全设备以确保容量适合邮件量。随着时间的推移，邮件量会不可避免地增加，适当的监控可确保主动添加容量或进行配置更改。监控系统容量的最有效方式是跟踪总量、工作队列中的邮件数，以及“资源节约模式”(Resource Conservation Mode) 的事件数。

- **量**：了解您的环境中的“正常”邮件量和“异常”峰值非常重要。随着时间的推移跟踪此数据以测量邮件量增长。您可以使用“传入邮件”(Incoming Mail) 和“传出邮件”(Outgoing Mail) 页面长期跟踪数量。有关详细信息，请参阅系统容量 - 传入邮件，第 46 页和系统容量 - 传出邮件，第 46 页。
- **工作队列**：工作队列旨在作为“减震器”，从而缓冲并过滤垃圾邮件攻击，并处理非垃圾邮件的异常增加。但是，工作队列也可能表明系统处于压力之下。拖延和频繁的工作队列备份可能表示存在容量问题。可以使用“系统容量 - 工作队列 (System Capacity － Workqueue)”页面跟踪工作队列中的活动。有关详细信息，请参阅系统容量 - 工作队列，第 45 页。
- **资源节约模式**：当设备变得过载时，它会进入“资源节约模式”(RCM) 并发送“严重”系统警报。这旨在保护设备，使其可以处理任何邮件积压情况。设备不应频繁进入 RCM，并且应仅在邮件量出现超大或异常增长期间进入。频繁的 RCM 警报可能表明系统正在超负荷。请参阅资源节约活动 ，第 47 页。

相关主题

- 如何解释在“系统容量”(System Capacity) 页面上看到的数据，第 45 页
- 系统容量 - 工作队列，第 45 页
- 系统容量 - 传入邮件，第 46 页
- 系统容量 - 传出邮件，第 46 页
- 系统容量 - 全部，第 47 页
- 系统容量图形中的阈值指示符 ，第 47 页

如何解释在“系统容量”(System Capacity) 页面上看到的数据

当选择时间范围来查看“系统容量”(System Capacity) 页面上的数据时，记住以下内容非常重要：

- 日报告 (Day Report) - 日报告查询小时表并显示设备在 24 小时内每小时收到的准确查询数量。此信息收集自小时表。这是一个准确的数字。
- 月报告 - 月报告查询 30 或 31 天（取决于该月份的实际天数）的日表，为您提供 30 或 31 天内查询数量的确切报告。再次重申，这是一个精确的数字。

“系统容量”(System Capacity) 页面上的“最大值”(Maximum) 值指示符是在指定时间段内看到的最高值。“平均值”(Average) 值是指定时间段内所有值的平均值。汇聚的时间取决于为该报告选择的时间间隔。例如，如果图表表示某个月时间段，您可以选择查看每天的“平均值”(Average) 和“最大值”(Maximum) 值。

可以点击特定图表的“查看详细信息 (View Details)”链接以查看各个邮件安全设备的数据以及连接到安全管理设备的设备的总体数据。

系统容量 - 工作队列

“工作队列”(Workqueue) 页面显示邮件在工作队列中花费的平均时间，在垃圾邮件隔离区中或在策略、病毒或病毒爆发隔离区中花费的任何时间除外。您可以查看时间段，从一小时到一个月。此平均值可以帮助确定延迟邮件传送的短期事件和确定系统上工作负载的长期趋势。

Note 如果邮件从隔离区释放到工作队列中，“工作队列中的平均时间”指标将忽略此时间。这可防止重复计数，以及由于在隔离区中花费的时间延长而造成统计信息失真。

此报告也显示指定时间段内的工作队列中的邮件量，并且显示相同时间段内工作队列中的最大邮件数量。工作队列中的最大邮件数图表还显示工作队列阈值级别。

工作队列图形中的偶尔峰值是正常的，并在预期之内。如果工作队列中的邮件数长时间保持高于配置的阈值，可能表示存在容量问题。这种情况下，请考虑调整阈值级别或审核系统配置。

要更改工作队列阈值级别，请参阅调整邮件安全设备的系统运行状况图中的参考阈值。

Tip 当查看工作队列页面时，您可能要测量工作队列备份的频率，并标注超过 10000 封邮件的工作队列备份。

系统容量 - 传入邮件

“系统容量”(System Capacity) 下的“传入邮件”(Incoming Mail) 页面显示传入连接、传入邮件总数、平均邮件大小和传入邮件总大小。您可以查看一天、一周、一月或一年的结果。了解环境中的正常邮件量和尖峰的趋势非常重要。您可以使用“系统容量”(System Capacity) 下的“传入邮件”(Incoming Mail) 页面跟踪一段时间内的邮件量增长并为系统容量制定计划。您可能还希望将传入邮件数据与发件人配置文件数据进行比较，以查看从特定域发送到网络的邮件的邮件量趋势。

Note 传入连接数增加不一定会影响系统负载。

系统容量 - 传出邮件

“系统容量”(System Capacity) 下的“传出邮件”(Incoming Mail) 页面显示传出连接、传出邮件总数、平均邮件大小和传出邮件总大小。您可以查看一天、一周、一月或一年的结果。了解环境中的正常邮件量和尖峰的趋势非常重要。您可以使用“系统容量”(System Capacity) 下的“传出邮件”(Outgoing Mail) 页面跟踪一段时间内的邮件量增长并为系统容量制定计划。您可能还希望将传出邮件数据与外发目标数据进行比较，以查看从特定域或 IP 地址发送的邮件的邮件量趋势。

系统容量 - 系统负载

系统负载报告显示如下信息：

- CPU 总体使用情况, on page 46
- 内存页面交换, on page 46
- 资源节约活动 , on page 47

CPU 总体使用情况

邮件安全设备经过优化，可使用空闲 CPU 资源提高邮件吞吐量。高 CPU 使用率并不一定表示存在系统容量问题。如果高CPU使用率与持续的大容量内存页面交换一同出现，则可能表示存在容量问题。

Note 此图还指明了一个仅用于视觉参考的CPU使用率阈值。要调整此行的位置，请参阅调整邮件安全设备的系统运行状况图中的参考阈值。您可以将邮件安全设备配置为向您发送警报，建议您可以为解决容量问题采取什么操作。

该页面还包含一个图，用于显示不同功能（包括邮件处理、垃圾邮件和病毒引擎、报告和隔离）使用的 CPU 量。按功能划分的 CPU 图形可以很好地指示产品的哪些方面在系统上使用最多资源。如果需要优化设备，则此图有助于确定哪些功能可能需要调整或禁用。

内存页面交换

内存页面交换图形显示了系统必须分页到磁盘的频率（以每秒千字节数为单位）。

系统旨在定期交换内存，因此发生一些内存交换在意料之中，并不是表明设备有问题。除非系统一致地大量交换内存，否则内存交换正常，并且是预期行为（尤其在C170设备上）。为提高性能，您可能需要将邮件安全设备添加到网络或调整配置以确保实现最大吞吐量。

Note 此图还指明了一个仅用于视觉参考的内存页面交换阈值。要调整此行的位置，请参阅调整邮件安全设备的系统运行状况图中的参考阈值。您可以将邮件安全设备配置为向您发送警报，建议您可以为解决容量问题采取什么操作。

资源节约活动

资源节约活动图显示邮件安全设备进入资源节约模式 (RCM) 的次数。例如，如果图中显示 n 次，则意味着设备进入了 RCM n 次，并已退出至少 n-1 次。

设备应当很少进入 RCM 模式，并且仅在邮件量非常大或异常增加时才进入此模式。如果“资源节约活动”(Resource Conservation Activity) 图显示您的设备频繁进入 RCS，则可能表明系统变得过载。

系统容量 - 全部

全部 (All) 页面将所有以前的系统容量报告整合到单个页面，使您可以查看不同报告之间的关系。例如，您可能发现消息队列很高，同时发生过多的内存切换。这可能表明存在容量问题。您可能希望将此页面另存为 PDF 文件，以保留系统性能的快照，供以后参考（或与支持人员共享）。

系统容量图形中的阈值指示符

在某些图形中，某行表示默认值，如果频繁或始终如一地超过该值，则可能表明存在问题。要调整此可视指示符，请参阅调整邮件安全设备的系统运行状况图中的参考阈值。

“高级恶意软件保护”页面

高级恶意软件防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。

此功能适用于传入和传出邮件。

有关文件信誉过滤和文件分析的详细信息，请参阅《适用于邮件安全设备的 *AsyncOS* 的用户指南或联机帮助》。

要查看报告页面，请从“报告”下拉列表的“过滤器和恶意软件报告”部分中选择**高级恶意软件保护**。

“高级恶意软件保护”报告页面显示以下报告视图：

- 高级恶意软件防护 - 摘要，第 61 页
- 高级恶意软件保护 - AMP 信誉，第 61 页
- 高级恶意软件保护 - 文件分析，第 62 页
- 高级恶意软件防护 - 文件追溯，第 63 页
- 高级恶意软件保护 - 邮箱自动修复，第 63 页

要在安全管理设备上查看“高级恶意软件保护”(Advanced Malware Protection) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控**

(Monitoring) > 高级恶意软件保护 (Advanced Malware Protection)。有关详细信息，请参阅使用交互式报告页面。

"高级恶意软件保护"报告页面显示的指标栏提供连接到Cisco威胁Grid设备的所有设备的实时数据。

注释

- 您必须在CLI上使用 `trailblazerconfig > enable` 命令来填充指标栏上的数据。有关详细信息，请参阅Trailblazerconfig 命令。
- 您只能在思科威胁网格设备中查看“天”、“周”和“月”的数据。

相关主题

- 通过 SHA-256 散列标识文件 ， 第 36 页
- 文件分析报告详细信息的要求 ， 第 34 页
- 查看其他报告中的文件信誉过滤数据 ， 第 38 页

高级恶意软件防护 - 摘要

“高级恶意软件保护 - 摘要”页显示由文件信誉和文件分析服务标识的基于传入和传出文件的威胁完整摘要。

有关详细信息，请参阅 高级恶意软件保护 - AMP 信誉 ， 第 61 页 和 高级恶意软件保护 - 文件分析 ， 第 62 页。

高级恶意软件保护 - AMP 信誉

“高级恶意软件保护 - AMP 信誉”(Advanced Malware Protection - AMP Reputation) 页面显示由文件信誉服务标识的基于文件的传入和传出威胁。

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“高级恶意软件防护”(Advanced Malware Protection) 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“高级恶意软件防护”(Advanced Malware Protection) 报告中。

AMP处理的传入文件部分按不同的类别显示传入恶意软件文件，例如恶意、安全、未知、不可扫描和低风险。

传入恶意文件分类如下：

- 从 AMP 信誉服务器接收的分类为**恶意软件**且已列入阻止列表的文件 SHA 百分比。
- 从面向终端的 AMP 控制台接收的分类为**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 AMP 控制台获取的已列入阻止列表的文件 SHA 百分比在报告的“传入恶意软件威胁文件”部分中显示为**简单自定义检测**。
- 根据阈值设置分类为**自定义阈值**且已列入阻止列表的文件的 SHA 百分比。

您可以点击报告的“更多详细信息”(More Details) 部分中的链接，以查看在面向终端的 AMP 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。

您可以使用“高级恶意软件保护: 传入”报告页面的“AMP 信誉”视图查看以下内容：

- 由高级恶意软件保护引擎的文件信誉服务标识的传入文件的摘要，以图形格式表示。
- 基于所选时间范围的所有传入恶意软件威胁文件的趋势图。
- 传入恶意软件威胁文件排行榜。
- 基于文件类型的传入威胁文件排行榜。
- 列出了传入恶意软件威胁文件排行榜的“传入恶意软件威胁文件”交互式表。

  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。

  如果您的访问权限允许您查看填充此报告之邮件的邮件跟踪数据，请点击表中的蓝色数字链接。

您可以使用“高级恶意软件保护: 传出”报告页面的“AMP 信誉”视图查看以下内容：

- 由高级恶意软件保护引擎的文件信誉服务标识的传出文件的摘要，以图形格式表示。
- 基于所选时间范围的所有传出恶意软件威胁文件的趋势图。
- 传出恶意软件威胁文件排行榜。
- 基于文件类型的传出威胁文件排行榜。
- 列出了由文件信誉服务标识的传出恶意软件威胁文件的排行榜的“传出恶意软件威胁文件”交互式表。

  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。

  如果您的访问权限允许您查看填充此报告之邮件的邮件跟踪数据，请点击表中的蓝色数字链接。

高级恶意软件保护 - 文件分析

高级恶意软件保护 -“文件分析”(File Analysis) 页面显示了发送以供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。

对于采用现场思科 AMP Threat Grid 设备的部署：在 AMP Threat Grid 设备上包含在允许列表中的文件显示为“正常”(clean)。有关允许列表的信息，请参阅 AMP Threat Grid 文档或联机帮助。

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。有关详细信息，请参阅通过 SHA-256 散列标识文件 ，第 36 页。

如果您的访问权限允许您查看填充此报告的邮件的邮件跟踪数据，请点击表中的**详细信息 (Details)** 链接。

要在分析了文件的服务器上查看详细信息，请参阅文件分析报告详细信息的要求 ，第 34 页。

如果从某个已压缩或已存档的文件中提取的某个文件送交分析，则只有这个已提取文件的SHA值包括在“文件分析”(File Analysis) 中。

您可以使用“思科高级恶意软件保护报告”(Advanced Malware Protection) 页面中的“文件分析”(File Analysis) 视图进行查看：

- 由高级恶意软件保护引擎的分析服务上传以进行文件分析的传入和传出文件的数量。
- 已完成文件分析请求的传入和传出文件的列表。
- 具有待处理文件分析请求的传入和传出文件的列表。

高级恶意软件防护 - 文件追溯

“高级恶意软件防护 - 文件追溯”(Advanced Malware Protection - File Retrospection) 页面列出了由此设备处理的文件，对于这些文件，自收到邮件以来判定已经发生变化。有关此场景的详细信息，请参阅邮件安全设备的相应文档。

由于“高级恶意软件防护”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。

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。

您可以使用“高级恶意软件保护”报告页的“文件追溯”视图来查看：

- 带有追溯性判决更改的传入和传出文件的列表。

高级恶意软件保护 - 邮箱自动修复

“高级恶意软件保护 - 邮箱自动修复”报告页显示传入文件的邮箱修复结果的详细信息。

您可以使用“高级恶意软件保护 - 邮箱自动修复”页查看追溯性安全详细信息，例如：

- 与 SHA-256 散列关联的文件名。
- 对邮件执行的修复操作。
- 邮箱修复成功或不成功的收件人列表。

在以下情况下，将更新未成功修复的收件人字段：

- 当设备尝试执行配置的补救操作时，您的设备与 Office 365 服务之间存在连接问题。

点击 SHA-256 散列可查看邮件跟踪中的相关邮件。

文件分析报告详细信息的要求

- （云文件分析）确保管理设备可以连接到文件分析服务器 , on page 35

- （云文件分析）配置管理设备以显示详细的文件分析结果 , on page 35
- （本地文件分析）激活文件分析账户 , on page 36
- 其它要求 , on page 36

（云文件分析）确保管理设备可以连接到文件分析服务器

要获取文件分析报告详细信息，设备必须能够通过端口 443 连接到文件分析服务器。请参阅防火墙资讯中的详细信息

（云文件分析）配置管理设备以显示详细的文件分析结果

为了使组织中的所有内容安全设备都可以在云中显示有关从组织中的任何思科邮件安全设备或思科网络安全设备送交分析的文件的详细结果，您需要将所有设备加入到同一设备组。

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。

步骤 1 在旧 Web 界面中，点击**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**，然后向下滚动到“文件分析”(File Analysis) 部分。

步骤 2 如果您管理的设备指向不同的文件分析云服务器，请选择从中显示结果详细信息的文件分析服务器。

将不提供由任何其他云服务器处理的文件的结果详细信息。

步骤 3 [如果在 Cisco 安全邮件和网页管理器上禁用智能许可，则适用] 在 **组名称** 字段中输入文件分析报告的组名称，然后点击 **立即分组**。

或

[如果在 Cisco 安全邮件和网页管理器上启用智能许可，则适用] 系统自动将智能账户 ID 注册为组 ID 并在 **组名称** 字段中显示。

步骤 4 在将与此设备共享数据的每个管理设备上配置相同的组。

说明：

- 您可以随时修改组名称。编辑名称并点击 **立即分组**。此更改会立即生效；它不需要“确认”(Commit)。
- 该组名称区分大小写。在共享上传以供分析的文件的相关数据的所有设备上，此值必须是相同的。
- 建议将您的 CCOID 用于此值。
- 一台设备只能属于一个组。
- 您可以随时将设备添加到组，但是只能添加一次。
- 如果启用智能许可，则使用智能帐户 ID 对设备进行分组。

What to do next

相关主题

可以在云中查看哪些文件的详细文件分析结果？ , on page 39

（本地文件分析）激活文件分析账户

如果您已部署本地（私有云）的思科 AMP Threat Grid 设备，必须激活思科内容安全管理设备的文件分析账户，才能查看 Threat Grid 设备上提供的报告详细信息。您通常只需执行此操作一次。

Before you begin

确保您接收“严重”(Critical) 级别的系统警报。

步骤 1 首次尝试从 Threat Grid 设备访问文件分析报告详细信息时，请等待几分钟，然后您将收到包含一个链接的警报。

如果您没有收到此警报，请转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)**，然后点击**查看警报排行榜 (View Top Alerts)**。

步骤 2 点击警报消息中的链接。

步骤 3 激活您的管理设备账户。

其它要求

有关任何其他要求，请参阅安全管理设备版本的版本说明，位置：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

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（以缩写格式）。

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。在适用的报告中，“由高级恶意软件防护检测到”(Detected by Advanced Malware Protection) 列在默认情况下可能处于隐藏状态。要显示其他列，请点击表底部的“列”(Columns) 链接。

可以在云中查看哪些文件的详细文件分析结果？

如果您部署了公共云文件分析，则可以查看从已添加到文件分析设备组的任何受管设备上传的所有文件的详细结果。

如果您已将管理设备添加至组，可以查看组中的受管设备列表，单击 **管理设备 > 集中服务 > 安全设备 > 文件分析** 页面上的 **查看组中设备** 按钮。

分析组中的设备由文件分析客户端 ID 标识。要确定特定设备的此标识符，请查看以下位置：

设备	文件分析客户端 ID 的位置
邮件安全设备	**安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)** 页面上的“文件分析的高级设置”(Advanced Settings for File Analysis) 部分。
网络安全设备	**安全服务 (Security Services) > 防恶意软件和信誉 (Anti-Malware and Reputation)** 页面上的“文件分析高级设置”部分。
思科内容安全管理设备	在**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)** 页面的底部。

相关主题

- （云文件分析）配置管理设备以显示详细的文件分析结果 , on page 35

“病毒过滤”(Virus Filtering) 页面

“病毒过滤”报告页面概述了从您的网络发送的病毒和发送到您的网络的病毒。“病毒类型”(Virus Types) 页面显示已由运行于邮件安全设备之上的病毒扫描引擎检测到并且显示在安全管理设备上的病毒。使用此报告针对特定病毒采取相应措施。例如，如果发现收到已知嵌入 PDF 文件中的大量病毒，则可以创建过滤器操作来隔离具有 PDF 附件的邮件。

要在安全管理设备上查看“病毒过滤”(Virus Filtering) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 病毒过滤 (Virus Filtering)**。有关详细信息，请参阅使用交互式报告页面。

如果运行多个病毒扫描引擎，则“病毒过滤”报告页面包括来自所有启用的病毒扫描引擎的结果。页面上出现的病毒名称由病毒扫描引擎决定。如果多个扫描引擎检测到病毒，则同一病毒可能有多个条目。

以下列表解释了“病毒过滤”报告页面上的各部分：

表 *14:*“病毒过滤”*(Virus Filtering)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。
检测到的传入病毒类型排行榜	此部分显示已发送到您的网络的邮件中检测到的病毒的图表视图。
检测到的外发病毒类型排行榜	此部分显示从您的网络发送的邮件中检测到的病毒的图表视图。

部分	说明
病毒类型详细信息 (Virus Types Detail)	显示每个病毒类型详细信息的交互式表。 有关详细信息，请参阅“病毒类型详细信息”(Virus Types Detail) 表，第 67 页

注释 如需查看哪些主机将受病毒感染的邮件发送到您的网络，请转到“传入邮件”(Incoming Mails) 页面，指定同一报告时间段，并按具有病毒特征的邮件排序。同样，如需查看您网络中的哪些 IP 地址发送了病毒邮件，请转至“传出邮件发件人”(Outgoing Senders) 页面，并按具有病毒特征的邮件排序。

在“病毒过滤”报告页面中，可以将原始数据导出到CSV 文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

您可以生成“病毒过滤”报告页面的计划报告。请参阅 计划邮件报告，第 103 页。

“病毒类型详细信息”(Virus Types Detail) 表

“病毒类型详细信息”(Virus Types Detail) 表是一个交互式表，显示了受病毒感染的邮件总数，这些邮件按传入和传出邮件进行了细分。点击列标题可对数据进行排序。

下表显示了“病毒类型详细信息”(Virus Types Detail) 表的表列说明：

表 *15:*“病毒类型详细信息”*(Virus Types Detail)* 表的表列说明

列名	说明
病毒类型	病毒类型的名称。
传入邮件数	检测为病毒的传入邮件数。
传出邮件数	检测为病毒的传出邮件数。
被感染的邮件总数	感染病毒的邮件（传入和传出）总数。

“宏检测”(Macro Detection) 页面

可以使用“宏检测”(Macro Detection) 报告页面查看：

- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传入附件。
- 按文件类型排列的启用宏的传入附件总数，采用表格格式。
- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传出附件。
- 按文件类型排列的启用宏的传出附件总数，采用表格格式。

要在安全管理设备上查看“宏检测”(Macro Detection) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 宏检测 (Macro Detection)**。有关详细信息，请参阅使用交互式报告页面。

在“宏检测”(Macro Detection) 报告页面中，可以将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

您可以点击启用宏的附件数量，以在邮件跟踪中查看相关邮件。

注释 报告生成期间：

- 如果在存档文件中检测到一个或多个宏，则存档文件的文件类型将按一递增。不计算存档文件中启用宏的附件数量。
- 如果在嵌入文件中检测到一个或多个宏，则父文件类型将递增一。不计算嵌入文件中启用宏的附件数量。

“DMARC 验证”(DMARC Verification) 页面

“DMARC 验证”报告页面显示未通过基于域的邮件身份验证、报告和一致性 (DMARC) 验证的发件人域排行榜，并显示对来自每个域的传入邮件执行的各项操作摘要。您可以使用此报告微调DMARC设置并回答以下类型的问题：

- 哪些域发送了最多未通过 DMARC 验证的邮件？
- 对于每个域，对未通过 DMARC 验证的邮件采取了哪些操作？

可以使用“DMARC 验证报告”页查看：

- 以图形格式显示的 DMARC 验证失败的域排名榜。
- 以表格格式显示的 DMARC 验证详细信息的总域。有关详细信息，请参阅“按 DMARC 验证排名的域详细信息”(Domains by DMARC Verification Details) 表 ， 第 69 页。

要在安全管理设备上查看“DMARC 验证”(DMARC Verification) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > DMARC 验证 (DMARC Verification)**。有关详细信息，请参阅使用交互式报告页面。

如果您的访问权限允许您查看填充此报告之邮件的邮件跟踪数据，请点击表中的蓝色数字链接。

在“DMARC 验证”报告页面中，您可以将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

有关 DMARC 验证的详细信息，请参阅邮件安全设备的在线帮助或用户指南中的“邮件身份验证”章节。

“按 DMARC 验证排名的域详细信息”(Domains by DMARC Verification Details) 表

“按 DMARC 验证排名的域详细信息”(Domains by DMARC Verification Details) 表是一个交互式表，显示基于域的邮件身份验证、报告和一致性 (DMARC) 验证已失败（被拒绝、隔离或无操作）、尝试和通过的发件人预的详细信息。

要自定义和排序表中的信息，请参见自定义报告页面上的表。

要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

“病毒爆发过滤”页面

“病毒爆发过滤”报告页面显示有关最近的病毒爆发的信息，并显示由于“病毒爆发过滤器”而隔离的邮件的相关信息。使用此页面可以监控对针对性病毒、诈骗和网络钓鱼攻击的防御。

使用“病毒爆发过滤”报告页面可回答以下类型的问题：

- 多少封邮件被隔离？依据的是哪项“病毒爆发过滤器”(Outbreak Filters) 规则？
- 邮件在病毒爆发隔离区中停留多长时间？
- 哪些可能是恶意的 URL 是最常见的？

要在安全管理设备上查看“病毒爆发过滤”(Outbreak Filtering) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 病毒爆发过滤 (Outbreak Filtering)**。有关详细信息，请参阅使用交互式报告页面。

下表解释了“病毒爆发过滤”报告页面上的各部分：

表 *16*:“病毒爆发过滤”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。
按类型划分的威胁	“按类型划分的威胁”部分显示设备接收的不同类型的威胁邮件。
威胁概要	“威胁概要”部分按恶意软件、网络钓鱼、垃圾邮件和病毒显示威胁邮件的细分。 要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的蓝色数字链接。

部分	说明
威胁详情	威胁详情交互表会显示有关特定病毒爆发的详细信息信息，包括威胁类别（病毒、诈骗或网络钓鱼）、威胁名称、威胁说明和识别的邮件数。 要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的蓝色数字链接。
传入邮件中的被拦截邮件	“传入邮件中被拦截的邮件"部分显示在所选时间段内由病毒爆发过滤器处理的传入邮件数的图表和摘要。 非病毒性威胁包括网络钓鱼邮件、诈骗和使用指向外部网站的链接进行的恶意软件分发。
按威胁级别划分的被拦截邮件	“按威胁级别划分的被拦截邮件”部分显示病毒爆发过滤器捕获的威胁的严重性级别图表和摘要。 级别 5 威胁表示在范围或影响方面非常严重，而级别 1 威胁表示威胁风险较低。有关威胁级别的说明，请参阅邮件安全设备的在线帮助或用户指南。
病毒爆发隔离区中驻留的邮件	“病毒爆发隔离区中驻留的邮件”显示邮件在病毒爆发隔离区中所驻留的时间长度。 此持续时间取决于系统需要多长时间收集关于潜在威胁的足够数据以对其安全性做出判定。带有病毒性威胁的邮件通常比带有非病毒性威胁的邮件在隔离区中花费更多时间，因为它们必须等待防病毒程序更新。还会反映您为每个邮件策略指定的最大保留时间。
频繁重写的 URL	“频繁重写的URL”部分显示重写最频繁的URL，重写的目的是将邮件收件人重定向到思科网络安全代理，以便在收件人单击邮件中潜在恶意链接时对网站进行单击时间评估。 此列表可能包括非恶意的URL，因为如果邮件中的任何URL被视为恶意，则邮件的所有 URL 均会被重写。 要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的蓝色数字链接。

注释 为了正确填充“病毒爆发过滤器”报告页面上的各个表，设备必须能够与思科更新服务器进行通信。

有关详细信息，请参阅邮件安全设备的在线帮助或用户指南中的病毒爆发过滤器章节。

“URL 过滤”(URL Filtering) 页面

提供传入和传出邮件的“URL 过滤”(URL Filtering) 报告。

只有由 URL 过滤引擎扫描的邮件（作为反垃圾邮件/爆发过滤器扫描的一部分或通过邮件/内容过滤器）才会包含在这些模块中。但是，并非所有结果都有必要专门可归属于 URL 过滤功能。

注释 仅当启用 URL 过滤时，才会填充 URL 过滤报告模块。

在“URL 过滤”报告页面中，您可以查看：

- “排名靠前的 URL 类别”(Top URL Categories) 模块包含已扫描的邮件中找到的所有类别，无论其是与内容过滤器还是邮件过滤器匹配都如此。

  每封邮件只能与一个信誉级别相关联。对于包含多个 URL 的邮件，统计信息反映邮件中任何 URL 的最低信誉。

- 排名靠前的 URL 垃圾邮件

  在邮件安全设备的**安全服务 (Security Services) > URL 过滤 (URL Filtering)** 页面中配置的全局允许列表中的 URL 不包含在报告中。

  报告中包含个别过滤器中使用的允许列表内的 URL。

- 恶意 URL 是爆发过滤器确定为信誉不佳的 URL。不确定 URL 是爆发过滤器确定需要点击时间保护的 URL。因此，不确定 URL 已被重写，从而重定向到思科网络安全代理。

  基于 URL 类别的过滤器的结果会反映在内容和邮件过滤器报告中。

  思科网络安全代理的点击时间 URL 评估结果不会反映在报告中。

要在安全管理设备上查看“URL 过滤”(URL Filtering) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > URL 过滤 (URL Filtering)**。有关详细信息，请参阅使用交互式报告页面。

下表解释“URL 过滤”报告页面上的各部分：

表 *17:* “*URL* 过滤”*(URL Filtering)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。

部分	说明
排名靠前的 URL 类别	本部分显示排名靠前的传入和传出邮件 URL 类别的图形视图和摘要。 要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。
排名靠前的 URL 垃圾邮件	本部分显示排名靠前的传入和传出邮件 URL 垃圾邮件的图形视图和摘要。
恶意和中性 URL	本部分显示传入和传出邮件中恶意和中性URL的图表视图和摘要。 要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

在“URL过滤”报告页面中，可以将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

“URL 追溯报告”(URL Retrospection Report) 页面

“URL 追溯报告”(URL Retrospection Report) 页面显示由 URL 追溯服务处理的 URL。它显示以下详细信息：

- **URL** - 思科安全邮件云网关发送到 URL 追溯服务分析的 URL。
- **接收判定** - 思科安全邮件云网关从 URL 追溯服务收到判定的日期和时间。
- **受影响邮件的补救状态** - 对恶意 URL 采取的操作以及针对每种补救状态的邮件数。可能的补救状态包括：正在进行、成功、失败和已跳过。

“伪造邮件检测”页面

“伪造邮件检测”页面包括以下报告：

- **排名靠前的伪造邮件检测**。显示内容字典中与传入邮件中的伪造“发件人：”信头匹配的前十个用户。
- **伪造邮件检测：详细信息**显示内容词典中与传入邮件中的伪造“发件人：”信头匹配所有用户的列表，对于给定用户，还会显示匹配的邮件的数量。

要在安全管理设备上查看“伪造邮件检测”(Forged Email Detection) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 伪造邮件检测 (Forged Email Detection)**。有关详细信息，请参阅使用交互式报告页面。

只有在使用“伪造邮件检测”内容过滤器或 `forged-email-detection` 邮件过滤器时，才会填充“伪造邮件检测”报告。

从“伪造邮件检测”报告页面中，您还可以将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

“发件人域信誉”(Sender Domain Reputation) 页面

您可以使用“发件人域信誉”(Sender Domain Reputation) 报告页面：

- 以图形格式根据从 SDR 服务接收的判定查看传入邮件。
- 以表格格式根据从 SDR 服务接收的威胁类别和判定查看传入邮件摘要。
- 以图形格式根据从 SDR 服务接收的威胁类别查看传入邮件。

注释 只有那些 SDR 判为 "不受信任" 或 "有问题 "的信息才被归入 SDR 威胁类别，如 "垃圾邮件"、"恶意 "等。

- 根据从 SDR 服务中表格的形式接收的威胁类别的传入邮件摘要。

要在安全管理设备上查看“发件人域信誉”(Sender Domain Reputation) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 发件人域信誉 (Sender Domain Reputation)**。有关详细信息，请参阅使用交互式报告页面。

外部威胁源页面

您可以使用“外部威胁源”(External Threat Feeds) 报告页面查看：

- 以图形格式查看用于检测邮件威胁的排名靠前的 ETF 来源
- 以表格格式查看用于检测邮件威胁的 ETF 来源的摘要。
- 以图形格式查看与检测到的邮件威胁相匹配的排名靠前的 IOC。
- 以图形格式查看用于过滤恶意传入邮件连接的排名靠前的 ETF 来源。
- 以表格格式查看用于过滤恶意传入邮件连接的 ETF 来源的摘要。

在“外部威胁源来源摘要”(Summary of External Threat Feed Sources) 部分：

- 您可以单击特定 ETF 来源的邮件数量，在邮件跟踪中查看相关邮件。
- 您可以单击特定威胁源来源，根据 IOC 查看 ETF 来源的分布情况。

在“感染指标 (IOC) 匹配摘要”部分：

- 您可以单击特定 ETF 来源的 IOC 数量，在邮件跟踪中查看相关邮件。
- 您可以单击特定 IOC，根据 ETF 来源查看 IOC 的分布情况。

要在安全管理设备上查看“外部威胁源”(External Threat Feeds) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 外部威胁源 (External Threat Feeds)**。有关详细信息，请参阅使用交互式报告页面。

“安全打印”(Safe Print) 页面

您可以使用“安全打印操作”报告页面查看：

- 以图形格式显示的基于文件类型的安全打印附件的数量。
- 基于表格格式的文件类型的安全打印附件摘要。

在“安全打印文件类型的摘要”(Summary of Safe Print File Types) 部分中，点击要在邮件跟踪中查看邮件详细信息的安全打印附件总数。

高级网络钓鱼防护报告页面

您可以在“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面上查看以下内容：

- 已成功转发到思科高级网络钓鱼防护云服务的邮件总数。
- 未转发到思科高级网络钓鱼防护云服务的邮件总数。

注释 如果邮件元数据转发失败，则必须验证“高级网络钓鱼防护”(Advanced Phishing Protection) 功能的配置。有关详细信息，请参阅思科邮件安全设备 的 *AsyncOS* 用户指南中的“将思科邮件安全网关与思科高级网络钓鱼防护集成”一章。

要在安全管理设备上查看“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件**(Email)，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 高级网络钓鱼防护 (Advanced Phishing Protection)**。有关详细信息，请参阅 使用交互式报告页面。

您可以在“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面上查看以下内容：

- 尝试转发到思科高级网络钓鱼防护云服务的邮件总数。
- 已转发到思科高级网络钓鱼防护云服务的邮件摘要（图形格式）。

“邮件流详细信息”页面

安全管理设备上的“邮件流详细信息”报告页面为连接到您的托管安全管理设备的所有远程主机提供实时信息的交互报告。您可以收集有关发送邮件到您的系统的 IP 地址、域和网络所有者（组织）的信息。您还可以收集有关传出发件人的 IP 地址和域的信息。

要在安全管理设备上查看“邮件流详细信息”(Mail Flow Details) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 邮件流详细信息 (Mail Flow Details)**。有关详细信息，请参阅使用交互式报告页面。

“邮件流详细信息”报告页面包含以下选项卡：

- 传入邮件

- 传出邮件发件人

要在您的数据中搜索特定信息，请参阅搜索与交互式邮件报告页面 ，第 6 页。

您可以从“传入邮件”选项卡中执行以下操作：

- 按威胁邮件总数查看发件人排行榜（采用图形格式）。
- 按安全邮件数查看发件人排行榜（采用图形格式）。
- 按恶意邮件数查看发件人排行榜（采用图形格式）。
- 请参阅已将邮件发送至安全管理设备的 IP 地址、域或网络所有者（组织）。
- 查看关于已将邮件发送到您的设备的发件人的详细统计信息。统计信息包括连接数（接受或拒绝）、按安全服务（发件人信誉过滤、反垃圾邮件、防病毒等）细分的所尝试邮件数量、威胁邮件总数、恶意邮件和安全邮件总数。
- 有关特定 IP 地址、域或网络所有者（组织）的详细信息，请参阅“传入邮件”交互式表。有关详细信息，请参阅“传入邮件”表 ，第 77 页。

  如果您的访问权限允许您查看填充此报告的邮件的邮件跟踪数据，请单击表中的数字链接。

您可以从“传出发件人”选项卡中执行以下操作：

- 按威胁邮件总数查看发件人排行榜（采用图形格式）。
- 按安全邮件数查看发件人排行榜（采用图形格式）。
- 查看您的组织中传出威胁邮件（垃圾邮件、病毒等）的发件人排行榜（按 IP 地址或域）。
- 查看关于已从您的设备发送邮件的发件人的详细统计信息。统计信息包括按安全服务（发件人信誉过滤、反垃圾邮件、防病毒等）细分的威胁邮件总数。
- 有关特定 IP 地址或域的详细信息，请参阅“发件人详细信息”交互式表。有关详细信息，请参阅“发件人详细信息”(Sender Details) 表 ，第 80 页。

  如果您的访问权限允许您查看填充此报告的邮件的邮件跟踪数据，请单击表中的数字链接。

相关主题

- “没有域信息”(No Domain Information) 链接 ，第 19 页
- 邮件趋势图中的时间范围 ，第 19 页
- “邮件流详细信息”(Mail Flow Details) 页面中的视图 ，第 75 页
- “传入邮件”表 ，第 77 页
- “发件人详细信息”(Sender Details) 表 ，第 80 页

“邮件流详细信息”(Mail Flow Details) 页面中的视图

“邮件流详细信息: 传入”报告页面有三种不同的视图：

- IP 地址
- 域
- 网络所有者

这些视图在选定视图的情景中提供连接到系统的远程主机的快照。

此外，在“邮件流详细信息”(Mail Flow Details) 页面的“传入邮件”(Incoming Mails) 表中，您可以点击“发件人的 IP 地址”(Sender’s IP Address)、“域名”(Domain name) 或“网络所有者信息”(Network Owner Information) 以检索特定的发件人配置文件信息。有关发件人配置文件信息的详细信息，请参阅发件人配置文件页面，第 20 页。

注释 网络所有者 (Network owners) 是包含域的实体。域 (Domains) 是包含 IP 地址的实体。

根据所选的视图，“传入邮件详细信息 (Incoming Mail Details)”交互式表格中显示将邮件发送至邮件安全设备上配置的所有公共侦听器的排名靠前的 IP 地址、域或网络所有者。可以监控传入设备的所有邮件的流量。

在“发件人配置文件 (Sender Profile)”页面上点击 IP 地址、域或网络所有者可访问有关发件人的详细信息。“发件人配置文件”(Sender Profile) 页面是与特定 IP 地址、域或网络所有者相关的“邮件流详细信息”(Mail Flow Details) 页面。

如需获得对“传入邮件”交互式表中包括的数据的解释，请参阅“传入邮件”表，第 77 页。

在“邮件流详细信息”(Mail Flow Details) 页面中，可以将原始数据导出到 CSV 文件。

“邮件流详细信息: 传出”报告页面有两种不同的视图：

- IP 地址
- 域

这些视图在选定视图的情景中提供连接到系统的远程主机的快照。

根据所选的视图，“发件人详细信息”交互式表显示了从公共侦听程序（从邮件安全设备配置）发送邮件的收件人 IP 地址或域排行榜。您可以监控从设备传出的所有邮件流。

如需获得对“发件人详细信息”交互式表中包括的数据的解释，请参阅“发件人详细信息”(Sender Details) 表，第 80 页。

“没有域信息”(No Domain Information) 链接

已连接至安全管理设备并且无法通过双DNS查找进行验证的域将自动分组到名为“没有域信息”的特殊域。可以控制通过发件人验证来管理此类未验证主机的方式。有关发件人验证的详细信息，请参阅邮件安全设备的文档或在线帮助。

您可以使用“显示的项”(Items Displayed) 菜单选择要在列表中显示的发件人数量。

邮件趋势图中的时间范围

可以选择不同程度的粒度以在邮件图中查看数据。您可以选择相同数据的天、周、月和年视图。由于数据实时受到监控，因此会在数据库中定期更新和汇总信息。

有关时间范围的详细信息，请参阅选择报告的时间范围。

“传入邮件”表

“邮件流详细信息:传入邮件”页面底部的“传入邮件”交互式表列出了已连接至邮件安全设备上的公共侦听程序的排名靠前的发件人。下表根据所选视图显示域、IP 地址或网络所有者。

系统通过执行双重 DNS 查找来获得和验证远程主机 IP 地址的有效性。有关双 *DNS* 查找和发件人验证的更多信息，请参阅 AsyncOS 邮件安全设备的用户指南或在线帮助。

对于发件人，即“传入邮件”(Incoming Mails) 表的第一列或“按威胁邮件总数排名靠前的发件人”(Top Senders by Total Threat Messages) 中列出的网络所有者、IP 地址或域，请单击“发件人”(Sender) 或“无域信息”(No Domain Information) 链接查看有关发件人的详细信息。结果显示在发件人配置文件 (Sender Profile) 页面上，其中包括来自 SenderBase 信誉服务的实时信息。从“发件人配置文件”(Sender Profile) 页面中，您可以查看有关特定 IP 地址或网络所有者的详细信息。有关详细信息，请参阅发件人配置文件页面，第 20 页。

您还可以查看“发件人组”(Sender Groups) 报告，方法是单击“邮件流详细信息”(Mail Flow Details) 页面底部的发件人组报告。有关“发件人组报告”(Sender Groups report) 页面的详细信息，请参阅“发件人组”(Sender Groups) 页面，第 81 页。

要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的数字超链接。

下表显示了“传入邮件”表的表列说明：

表 *18:* 用于“传入邮件”表的表列说明

列名	说明
发件人域（域）	发件人的域名。
发件人 IP 地址（IP 地址）	发件人的 IP 地址。
主机名（IP 地址）	发件人的主机名。
已验证的 DNS（IP 地址）	由 DNS 验证的 IP 地址。
SBRS（IP 地址）	发件人的 SenderBase 信誉得分。
上一个发件人组（IP地址）	上一个发件人组的详细信息。
上一个发件人组（IP地址）	上一个发件人组的详细信息。
网络所有者（网络所有者）	发件人的网络所有者。
拒绝的连接（域和网络所有者）	由 HAT 策略阻止的所有连接。当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。

列名	说明
接受的连接（域和网络所有者）	所有已接受的连接。
尝试的总数 (Total Attempted)	已尝试的所有已接受和已阻止的连接。
由收件人限制（域和网络所有者）拦截	这是“由信誉过滤拦截”(Stopped by Reputation Filtering) 的一个组件。表示由于超出下列任何 HAT 限制而拦截的收件人邮件的数量：每小时的最大收件人数、每封邮件的最大收件人数或每个连接的最大邮件数。此值加上与被拒绝或被 TCP 拒绝的收件人邮件估算值就得到了“由信誉过滤拦截”(Stopped by Reputation Filtering) 的值。
由 IP 信誉过滤拦截	“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 的值根据多个因素进行计算： • 来自此发件人的“受限制”邮件数 • 已拒绝或 TCP 拒绝的连接数（可能是部分计数） • 每个连接的邮件数量的保守倍数。 当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。在这种情况下，显示的值可以解释为“下限”，即至少已拦截这么多邮件。 **注释** “邮件流摘要”页面上的“信誉过滤”总数始终基于所有被拒绝连接的完整计数。只有每个发件人的连接计数会因负载而受到限制。
由域信誉过滤拦截	根据发件人域的信誉来判定阻止的邮件总数。
作为无效收件人拦截 (Stopped as Invalid Recipients)	由会话 LDAP 拒绝和所有 RAT 拒绝予以拒绝的所有邮件收件人。
检测到的垃圾邮件 (Spam Detected)	检测到的任何垃圾邮件。
检测到的病毒 (Virus Detected)	检测到的任何病毒
由高级恶意软件保护检测到	高级恶意软件保护引擎检测到的邮件总数。
内容过滤器拦截	由内容过滤器拦截的邮件总数。
由 DMARC 拦截 (Stopped by DMARC)	基于域的邮件身份验证、报告和一致性 (DMARC) 验证失败的邮件总数。

列名	说明
威胁邮件总数 (Total Threat)	威胁邮件总数（由信誉拦截、作为无效收件人拦截、垃圾邮件以及病毒）
市场营销部门	被检测为不需要的营销邮件的邮件数。
社交	被检测为营销邮件的邮件数。
统计数据	检测为批量的邮件数。
灰色邮件总数	检测为灰色邮件的邮件数。
正常 (Clean)	所有正常邮件。 未启用灰色邮件功能的设备上处理的邮件被计为正常邮件。

发件人配置文件页面

当您在**邮件流详细信息** [新 Web 界面] 或**传入邮件**页面上的交互式表中单击收件人时，会出现“发件人配置文件”页面。它显示关于特定 IP 地址、域或网络所有者（组织）的详细信息。通过单击邮件流详细信息页面或其他“发件人配置文件”页面上的相应链接，您可以访问任何 IP 地址、域或网络所有者的“发件人配置文件”页面。

网络所有者是包含域的实体。域 *(Domains)* 是包含 IP 地址的实体。

为 IP 地址、域和网络所有者显示的“发件人配置文件”(Sender Profile) 页面稍有不同。对于每项，该页面包含来自特定发件人的传入邮件的图形和摘要表。在图形下方，表列出与发件人相关联的域或 IP 地址。（单个 IP 地址的“发件人配置文件”[Sender Profile] 页面不包含更精细的列表。）“发件人配置文件”(Sender Profile) 页面还包括一个信息部分，其中包含当前 SenderBase、发件人组和发件人的网络信息。

- 网络所有者配置文件页面包含网络所有者以及与该网络所有者关联的域和 IP 地址的信息。
- 域配置文件页面包含与该域关联的域和 IP 地址。
- IP 地址配置文件页面只包含有关该 IP 地址的信息。

每个“发件人配置文件 (Sender Profile)”页面底部的“当前信息 (Current Information)”表格中都包含以下数据：

- 来自 SenderBase 信誉服务的全局信息，包括：
  - IP 地址、域名和/或网络所有者
  - 网络所有者类别（仅限网络所有者）
  - CIDR 范围（仅限 IP 地址）
  - IP 地址、域和/或网络所有者的日量级和月量级
  - 自从此发件人收到第一封邮件以来的天数

- 上一个发件人组以及是否进行了 DNS 验证（仅 IP 地址发件人配置文件页面）

日流量用于衡量某个域在最近 24 小时内发送了多少邮件。SenderBase 流量类似于用来衡量地震的里氏震级，使用以 10 为底数的对数标尺计算邮件数量。该标尺的最大理论值设置为 10，等同于 100% 的实际邮件数量。使用该对数标尺时，流量每增加 1 个单位，实际数量就会增加 10 倍。

月流量的计算方法与日流量相同，只是百分比基于最近 30 天发送的邮件数量来计算。

- 平均量级（仅限 IP 地址）
- 生命周期数量/30 天数量（仅限 IP 地址配置文件页面）
- 有担保发件人状态（仅限 IP 地址配置文件页面）
- SenderBase 信誉得分（仅限 IP 地址配置文件页面）
- 自从第一封邮件以来的天数（仅限网络所有者和域配置文件页面）
- 与此网络所有者相关联的域数量（仅限网络所有者和域配置文件页面）
- 此网络所有者中的 IP 地址数量（仅限网络所有者和域配置文件页面）
- 用于发送邮件的 IP 地址数量（仅限网络所有者页面）

单击**来自 SenderBase 的详细信息 (More from SenderBase)** 可查看包含 SenderBase 信誉服务提供的所有信息的页面。

- 有关由此网络所有者控制的域和 IP 地址的详细信息显示在网络所有者配置文件页面上。有关域中的 IP 地址的详细信息，将显示在域页面上。

从域配置文件页面中，您可以单击特定 IP 地址以查看特定信息，或查看组织配置文件页面。

“发件人详细信息”(Sender Details) 表

“邮件流详细信息: 传出邮件”(Mail Flow Details: Outgoing) 页面底部的“发件人详细信息”(Sender Details) 交互式表列出了已连接至邮件安全设备上的公共侦听器的发件人排行榜。下表根据所选视图显示了域或 IP 地址。

要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的数字超链接。

下表显示了“发件人详细信息”(Sender Details) 表的表列说明：

表 *19:*“发件人详细信息”*(Sender Details)* 表的表列说明

列名	说明
发件人域（域）	发件人的域名。
发件人 IP 地址（IP 地址）	发件人的 IP 地址。
主机名（IP 地址）	发件人的主机名。

列名	说明
检测到的垃圾邮件 (Spam Detected)	检测到的任何垃圾邮件。
检测到的病毒 (Virus Detected)	检测到的任何病毒。
由高级恶意软件保护检测到	高级恶意软件保护引擎检测到的邮件总数。
内容过滤器拦截	由内容过滤器拦截的邮件总数。
DLP 拦截	由 DLP 引擎拦截的邮件总数。
威胁邮件总数	威胁邮件（垃圾邮件、病毒）总数
正常 (Clean)	所有正常邮件。 未启用灰色邮件功能的设备上处理的邮件被计为正常邮件。
邮件总数	所有邮件的总数。

“发件人组”(Sender Groups) 页面

“发件人组报告”(Sender Groups report) 页面按发件人组和邮件流策略操作提供连接摘要，允许您查看 SMTP 连接和邮件流策略趋势。“按发件人组的邮件流量 (Mail Flow by Sender Group)”列表显示每个发件人组的连接的百分比和数量。“按邮件流量策略操作的连接”(Connections by Mail Flow Policy Action) 图表显示每个邮件流量策略操作的连接百分比。此页面概述了主机访问表 (HAT) 策略的有效性。有关 HAT 的详细信息，请参阅邮件安全设备的文档或在线帮助。

要在安全管理设备上查看“发件人组”(Sender Groups) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 发件人组 (Sender Groups)**。有关详细信息，请参阅使用交互式报告页面。

在“发件人组”报告页面中，可以将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

注释 您可以生成“发件人组报告”(Sender Groups report) 页面的计划报告。请参阅 计划邮件报告，第 103 页。

“外发目标”(Outgoing Destinations) 页面

“外发目标”报告页面提供有关您的组织向其发送邮件的各个域的信息。

您可以使用“外发目标”页面查看：

- 邮件安全设备将邮件发送至哪些域？

- 向每个域发送多少邮件？
- 该邮件中有多少是正常的、具有垃圾邮件特征、具有病毒特征、具有恶意软件特征或由内容过滤器拦截？
- 传送了多少封邮件？目标服务器硬退回了多少封邮件？

要在安全管理设备上查看“外发目标”(Outgoing Destinations) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 传出目标 (Outgoing Destinations)**。有关详细信息，请参阅使用交互式报告页面。

要在您的数据中搜索特定信息，请参阅搜索与交互式邮件报告页面 ，第 6 页。

以下列表解释了“外发目标”报告页上的各部分：

表 *20*:“外发目标”页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。
目标排行榜(按威胁邮件总数)	您的组织发送的传出威胁邮件（垃圾邮件、病毒等）的目标域排行榜。威胁邮件总数包括垃圾邮件或具有病毒特征的邮件，或者内容过滤器触发的邮件。
目标排行榜(按正常邮件数)	您的组织发送的正常传出邮件的目标域排行榜。
外发目标详细信息	与您的组织发送的所有传出邮件的目标域相关的所有详细信息，按收件人总数排序。详细信息包括检测到的垃圾邮件、病毒、正常邮件等。 有关详细信息，请参阅外发目标详细信息表 ，第 83 页。 要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的蓝色数字链接。

从“外发目标”报告页中，您可以将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

您可以生成“外发目标”(Outgoing Destinations) 页面的计划报告。请参阅计划邮件报告 ，第 103 页。

相关主题

外发目标详细信息表 ，第 83 页

外发目标详细信息表

“外发目标详细信息”表是一个交互表格，它显示处理和传递的邮件总数，并列出被处理为威胁（垃圾邮件、病毒等）或安全邮件的明细数据，以及被硬退回或投递的邮件明细数据。单击列标题可对数据进行排序。

若要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的蓝色数字链接。

下表展示“外发目标详细信息”表的表列说明：

表 *21:* 外发目标详细信息表的表列说明

列名	说明
目标域名	目标域的名称。
垃圾邮件	检测为垃圾邮件的邮件数。
病毒邮件	检测为垃圾邮件的邮件数。
内容过滤器拦截	内容过滤器拦截的邮件数。
威胁邮件总数	被检测为威胁（垃圾邮件、病毒等）的邮件总数
清洁	被检测为安全邮件的邮件数，
处理的邮件总数	作为威胁或安全邮件处理的邮件总数。
硬退回	标记为永久无法投递的邮件数。 **注释** 计算硬退回邮件时，仅包括以下退回类型： • FiveXX 硬退回 • 过滤器硬退回 • 其他硬退回 • DNS 硬退回 • 过期的硬退回
已投递	已投递的邮件数。
已投递的邮件总数	已投递的邮件总数（包括硬退回）。

“TLS 加密”(TLS Encryption) 页面

“TLS 加密”(TLS Encryption) 页面显示所收发邮件的 TLS 连接的整体使用情况。该报告还显示使用 TLS 连接发送邮件的每个域的详细信息。

“TLS 连接”(TLS Connections) 页面可用于确定以下信息：

- 总体而言，哪个部分的传入/传出连接使用 TLS？
- 我与哪些合作伙伴建立成功的 TLS 连接？
- 我与哪些合作伙伴建立的 TLS 连接失败？
- 在 DANE 支持下，我与哪些合作伙伴成功建立了传出 TLS 连接？
- 在 DANE 支持下，我未能与哪些合作伙伴成功建立传出 TLS 连接？
- 哪些合作伙伴的 TLS 证书有问题？
- 合作伙伴的全部邮件中有多少百分比使用 TLS？

要在安全管理设备上查看“TLS 加密”(TLS Encryption) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > TLS 加密 (TLS Encryption)**。有关详细信息，请参阅使用交互式报告页面。

“TLS 加密”报告页面具有以下选项卡：

- 传入
- 传出

要在您的数据中搜索特定信息，请参阅搜索与交互式邮件报告页面 ，第 6 页。

以下列表解释“TLS 加密”报告页面上的各部分：

表 *22:* “*TLS* 加密”*(TLS Encryption)* 页面上的详细信息

时间范围 (Time Range) （下拉列表）	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。
TLS 连接图	“TLS 加密：传入”(TLS Encryption: Incoming) 页面显示在最后一个小时、一天、一周、一个月或一年（具体取决于您选择的时间范围）内传入的加密和未加密的 TLS 连接的图形视图。 “TLS 加密：传出”(TLS Encryption: Outgoing) 页面显示在最后一个小时、一天、一周、一个月或一年（具体取决于您选择的时间范围）内传出的加密和未加密的 TLS 连接的图形视图。

TLS 连接摘要	“TLS 加密：传入”(TLS Encryption: Incoming) 页面显示传入邮件总量、加密和未加密邮件数量，以及成功和失败的传入TLS加密邮件数量的表格视图。 “TLS 加密：传出”(TLS Encryption: Outgoing) 页面显示传出邮件总量、加密和未加密邮件数量、成功或失败的传出TLS加密邮件数量，以及在 DANE 支持下成功和失败的传出 TLS 连接的表格视图。
TLS 邮件	“TLS 加密：传入”(TLS Encryption: Incoming) 页面显示传入的TLS加密和未加密邮件总数和百分比的图表视图。 “TLS 加密：传出”(TLS Encryption: Outgoing) 页面显示传出的TLS加密和未加密邮件总数和百分比的图表视图。
TLS 邮件摘要	此表显示传入和传出的TLS加密和未加密邮件和总数和百分比摘要。
TLS 连接详细信息	此表显示发送或接收加密邮件的域的详细信息。对于每个域，您可以查看连接总数、已发送的邮件，以及成功或失败的TLS连接数量。您还可以查看每个域的成功和失败连接的百分比。 有关详细信息，请参阅“TLS 连接详细信息”(TLS Connections Details) 表，第 85 页。

相关主题

“TLS 连接详细信息”(TLS Connections Details) 表，第 85 页

“TLS 连接详细信息”(TLS Connections Details) 表

“TLS 连接详细信息”(TLS Connections Details) 表是一个交互式表，显示连接的总数、发送的邮件数、成功或失败的TLS连接数以及传入和传出邮件最后的TLS状态。您还可以查看每个域的成功和失败连接的百分比。

下表显示了“TLS 连接详细信息”(TLS Connections Details) 表的表列说明：

表 *23:*“*TLS* 连接详细信息”*(TLS Connections Details)* 表的表列说明

列名	说明
域	发件人的域名。
TLS 需要失败	失败的所有必需的 TLS 连接。

列名	说明
TLS 需要成功	成功的所有必需的 TLS 连接。
TLS 首选失败 (TLS Pref. Failed)	失败的所有首选的 TLS 连接。
TLS 首选成功 (TLS Pref. Success)	成功的所有首选的 TLS 连接。
上次 TLS 状态	基于以下内容映射的 TLS 连接的状态： • 0：N/A • 1：必需 - 失败 • 2：首选 - 失败 • 3：必需 - 成功 • 4：首选 - 成功
DANE 故障	在 DANE 支持下未成功建立传出 TLS 连接的总数
DANE 成功	在 DANE 支持下成功建立传出 TLS 连接的总数
TLS 连接总数 (Total TLS Connections)	TLS 连接的总数。
未加密连接	未加密的 TLS 连接总数。
所有连接中的 TLS 百分比 (% TLS of all Connections)	所有 TLS 连接的 TLS 加密的百分比。
按 TLS 连接的邮件 (Messages by TLS)	TLS 邮件的总数。

入站 SMTP 身份验证页面

“入站 SMTP 身份验证”报告页面显示使用客户端证书和“SMTP AUTH”命令对邮件安全设备与用户的邮件客户端之间的 SMTP 会话进行身份验证。如果设备接受证书或 SMTP AUTH 命令，则会建立到邮件客户端的 TLS连接，供客户端用来发送邮件。因为设备无法逐个用户跟踪这些尝试，因此报告会根据域名和域 IP 地址显示有关 SMTP 身份验证的详细信息。

使用此报告可确定以下信息：

- 总体而言，多少入站连接使用 SMTP 身份验证？
- 多少连接使用经过认证的客户端？
- 多少连接使用 SMTP AUTH？
- 当尝试使用 SMTP 身份验证时，哪些域无法连接？

- 当 SMTP 身份验证失败时，多少连接成功使用回退？

要在安全管理设备上查看“入站 SMTP 身份验证”(Inbound SMTP Authentication) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 入站 SMTP 身份验证 (Inbound SMTP Authentication)**。有关详细信息，请参阅使用交互式报告页面。

入站 SMTP 身份验证有两种不同的视图：

- 域
- IP 地址

这些视图在选定视图的情景中提供连 SMTP 身份验证的快照。

“入站 SMTP 身份验证”报告页面包括已接收连接的图表，尝试 SMTP 身份验证连接的收件人图表，以及包含身份验证连接尝试详细信息的表格。

以下列表解释“传入 SMTP 身份验证”报告页面上的各部分：

表 *24:*“入站 *SMTP* 身份验证”*(Inbound SMTP Authentication)* 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。
“接收的连接”图表	“已接收的连接”(Received Connections) 图形显示在指定时间范围内来自尝试使用 SMTP 身份验证对其连接进行身份验证的邮件客户端的传入连接。该图表显示设备接收的连接总数、未尝试使用 SMTP 身份验证进行验证的次数，使用客户端证书验证连接的成功和失败次数，以及使用 SMTP AUTH 命令进行验证的成功和失败次数。
“接收的收件人”图表	“已接收的收件人”(Received Recipients) 图形显示了收件人的数量，这些收件人的邮件客户端尝试对其与邮件安全设备的连接进行身份验证以使用 SMTP 身份验证来发送邮件。该图形还显示其连接已进行身份验证的收件人数和其连接未进行身份验证的收件人数。
SMTP 身份验证详细信息（按域名或 IP 地址划分）。	“SMTP 身份验证详细信息”（按域名或 IP 地址划分）表显示有关尝试验证其与邮件安全设备的连接以发送邮件的用户的详细信息。对于每个域，可以查看尝试使用客户端证书进行连接的成功或失败次数、尝试使用 SMTP AUTH 命令进行连接的成功或失败次数，以及在客户端证书连接尝试失败后回退到SMTP AUTH 的次数。

速率限制页面

通过按信封发件人进行速率限制，您可以根据发件人地址从单个发件人限制每个时间间隔的邮件收件人数。“速率限制”(Rate Limits) 报告显示最严重超过此限制的发件人。

使用此报告可帮助确定以下内容：

- 可能用于批量发送垃圾邮件的有漏洞用户账户。
- 组织中的失控应用程序，这些应用程序使用邮件发送通知、风险通告、自动声明等内容。
- 组织中具有大量邮件活动的来源，用于内部计费或资源管理目的。
- 可能未被视为垃圾邮件的大量入站邮件流量的来源。

要在安全管理设备上查看“速率限制”(Rate Limits) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 速率限制 (Rate Limits)**。有关详细信息，请参阅使用交互式报告页面。

请注意，包含内部发件人（例如内部用户或传出邮件发件人）的统计信息的其他报告仅测量已发送的邮件数；它们不会向大量收件人表明少数邮件的发件人的身份。

“按事件划分的排名靠前的危害”图表显示最频繁尝试向超过配置限制的收件人发送邮件的信封发件人。每次尝试都是一个事件。此图表汇总所有侦听程序的事件计数。

“按已拒绝收件人划分的排名靠前的危害”图表显示向高于配置限制的最大数量的收件人发送邮件的信封发件人。此图表汇总所有侦听程序的收件人计数。

速率限制设置（包括“信封发件人的速率限制 (Rate Limit for Envelope Senders)”设置）在邮件安全设备的“邮件策略 (Mail Policies)”>“邮件流量策略 (Mail Flow Policies)”中配置。有关速率限制的详细信息，请参阅邮件安全设备的文档或在线帮助。

相关主题

“大量邮件”(High Volume Mail) 页面，第 97 页

“按国家/地区划分的连接”页面

您可以使用“按国家/地区划分的连接”报告页面查看：

- 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。
- 以表格格式显示的基于源国家/地区的传入邮件连接和邮件总数。

要在安全管理设备上查看“按国家/地区划分的连接”(Connections by Country) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 按国家/地区划分的连接 (Connections by Country)**。有关详细信息，请参阅使用交互式报告页面。

以下是不显示传入邮件连接排行榜和总数的国家/地区信息的情景：

- 发件人 IP 地址属于私有 IP 地址。

- 发件人 IP 地址未获得有效 SBRS。

如果您的访问权限允许您查看填充此报告之邮件的邮件跟踪数据，请单击表中的蓝色数字链接。

从“按国家/地区划分的连接”报告页面，可以将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

域保护页面

思科域保护云服务接口能够自动识别、监控和管理第三方代表您发送的邮件。这为发现和消除非法邮件并阻止恶意邮件提供了一种简便方法，可抵御冒充您公司域的网络钓鱼攻击。域保护甚至可以检测以假乱真的仿冒域，从而快速阻止恶意 URL。

您可以使用设备新 Web 界面的**监控 (Monitoring) > 域保护 (Domain Protection)** 报告页面查看：

- 分类为合法或威胁的邮件摘要（图形格式）。
- 基于发件人的目标域摘要摘要（表格格式）。

确保您拥有有效的许可证，可使用管理员访问权限访问思科域保护云服务接口。要获取许可证，请使用以下 URL 转至思科域保护注册页面：https://www.cisco.com/c/en/us/buy.html.

如果您已在思科域保护注册，请输入以下详细信息以便进行身份验证并查看设备上的域保护报告：

- **客户端 ID**：这是用于从思科域保护云服务导入报告的 API 访问 UID。
- **客户端密钥**：这是用于从思科域保护云服务导入报告的 API 访问密钥。

要生成 API 访问 UID 和密钥，您必须登录到思科域保护云服务并转至**设置 (Settings) > API 客户端密钥 (API Client Secret) > 生成 API 凭证 (Generate API Credentials)**。有关详细信息，请参阅《思科域保护用户指南》。

注释 要在设备的新 Web 界面上查看域保护报告页面，请确保在设备上启用了 `traceblazerconfig`。

用户邮件摘要

“用户邮件摘要”报告页面按邮件地址提供有关您的内部用户发送和接收的邮件的信息。单一用户可以有多个邮件地址。报告中未合并邮件地址。

您可以使用“用户邮件摘要”报告页面查看：

- 谁发送的外部邮件最多？
- 谁接收的正常邮件最多？
- 谁接收的灰色邮件最多？
- 谁接收的垃圾邮件最多？

- 谁触发了哪些内容过滤器？
- 谁的邮件被内容过滤器拦截？

要在安全管理设备上查看“用户邮件摘要”(User Mail Summary) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring)** > **用户邮件摘要 (User Mail Summary)**。有关详细信息，请参阅使用交互式报告页面。

要在您的数据中搜索特定信息，请参阅搜索与交互式邮件报告页面 ，第 6 页。

下面的列表解释“用户邮件摘要”报告页面的各个部分：

表 *25:* “用户邮件摘要”页上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。
排名靠前的用户(按正常的传入邮件)	组织收到的安全传入邮件的用户排行榜（按域分类）。
排名靠前的用户(按正常的传出邮件)	组织发送的安全传入邮件的用户排行榜（按域分类）。
排名靠前的用户(按灰色邮件)	灰色邮件的用户排行榜（按域分类）。
用户邮件控制详细信息	“用户邮件流详细信息”交互表按每个邮件地址对接收和发送的邮件进行了分类。您可以通过单击列标题对列表排序。 有关详细信息，请参阅“用户邮件流详细信息”(User Mail Flow Details) 表 ，第 91 页。 若要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的蓝色数字链接。

从“用户邮件摘要”报告页中，可以将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

注释 可以为“用户邮件摘要”页面生成计划报告。请参阅计划邮件报告 ，第 103 页。

相关主题

- “用户邮件流详细信息”(User Mail Flow Details) 表 ，第 91 页
- 搜索特定的内部用户 ，第 26 页

“用户邮件流详细信息”(User Mail Flow Details) 表

“用户邮件流详细信息”(User Mail Flow Detail) 表显示关于用户的详细信息，其中包括传入和传出邮件的细分以及每种类别（如检测到的垃圾邮件、检测到的病毒邮件、由内容过滤器拦截的邮件等）中的邮件数。还显示传入和传出内容过滤器匹配项。

入站内部用户是您根据“收件人：”(Rcpt To:) 地址为其收到邮件的用户。出站内部用户基于“邮件发件人:”地址，在跟踪内部网络中的发件人所发送邮件的类型时非常有用。

某些出站邮件（例如退回）的发件人为空。这些邮件被计为出站“未知”(unknown)。

要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的数字超链接。

下表显示了“用户邮件流详细信息”(User Mail Flow Details) 表的表列说明：

表 *26:*“用户邮件流详细信息”*(User Mail Flow Details)* 表的表列说明

列名	说明
内部用户	内部用户的域名。
检测到的传入垃圾邮件 (Incoming Spam Detected)	检测到的所有传入垃圾邮件。
检测到的传入病毒 (Incoming Virus Detected)	检测到的传入病毒。
高级恶意软件保护检测到的传入威胁	由高级恶意软件保护（文件分析和文件信誉）检测到的传入邮件。
传入邮件内容过滤器匹配数	检测到的传入内容过滤器匹配项。
由内容过滤器拦截的传入邮件 (Incoming Stopped by Content Filter)	由已设置的内容过滤器拦截的传入邮件。
传入的营销邮件	被检测为营销邮件的传入邮件。
传入的社交网络邮件	被检测为社交网络邮件的传入邮件。
传入的批量邮件	被检测为批量邮件的传入邮件。
传入的灰色邮件	被检测为灰色邮件的传入邮件。
传入的正常邮件 (Incoming Clean)	所有传入的正常邮件。
检测到的传出垃圾邮件 (Outgoing Spam Detected)	检测到的传出垃圾邮件。
检测到的传出病毒 (Outgoing Virus Detected)	检测到的传出病毒。

列名	说明
传出邮件内容过滤器匹配数	检测到的传出邮件内容过滤器匹配项。
由内容过滤器拦截的传出邮件 (Outgoing Stopped by Content Filter)	由已设置的内容过滤器拦截的传出邮件。
传出的正常邮件 (Outgoing Clean)	所有传出的正常邮件。

搜索特定的内部用户

利用用户邮件摘要页面和用户邮件流详细信息页面底部的搜索表单，您可以搜索特定的内部用户（邮件地址）。选择是要精确匹配搜索文本还是查找以输入的文本开头的项（例如，以“ex”开头将匹配“example.com”）。

“DLP 事件摘要”(DLP Incident Summary) 页面

“DLP 事件”（“DLP 事件摘要”）报告页面显示传出邮件中发生的防数据丢失 (DLP) 策略违规事件的信息。邮件安全设备使用在“传出邮件策略 (Outgoing Mail Policies)”表中启用的 DLP 邮件策略来检测用户发送的敏感数据。违反 DLP 策略的每个传出邮件均报告为一个事件。

使用“DLP 事件摘要”(DLP Incident Summary) 报告可回答以下类型的问题：

- 用户发送什么类型的敏感数据？
- 这些 DLP 事件具有什么样的严重性？
- 传送的这些邮件有多少数量？
- 丢弃的这些邮件有多少数量？
- 是谁在发送这些邮件？

“DLP 事件摘要”(DLP Incident Summary) 页面包括两个主要部分：

- DLP 事件趋势图，按严重性（“低”、“中”、“高”、“严重”）和策略匹配总结排名靠前的 DLP 事件。
- “DLP 事件详细信息”列表

要在安全管理设备上查看“DLP 事件摘要”(DLP Incident Summary) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > DLP 事件摘要 (DLP Incident Summary)**。有关详细信息，请参阅使用交互式报告页面。

从“DLP 事件”报告页面中，您可以将原始数据导出到 CSV 文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

要在您的数据中搜索特定信息，请参阅搜索与交互式邮件报告页面 ， 第 6 页。

以下列表解释了“DLP 事件摘要”报告页面上的各部分：

表 27: “DLP 事件摘要”(DLP Incident Summary) 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。
按严重性排名考前的事件 (Top Incidents by Severity)	按严重性列出的 DLP 事件排行榜。
事件概要	“DLP 事件摘要”(DLP Incident Summary) 页面底部的“DLP 事件详细信息”(DLP Incident Details) 交互式表中列出了当前已为每台邮件设备的传出邮件策略启用的 DLP 策略。点击 DLP 策略的名称可查看更详细的信息。
排名靠前的 DLP 策略匹配项 (Top DLP Policy Matches)	已匹配的 DLP 策略排行榜。
DLP 事件详细信息 (DLP Incident Details)	“DLP 事件详细信息”表显示每个策略的 DLP 事件总数，其细分依据为严重性级别，以及是否已传送类别为“清除”、“已传送 [已加密]”或“已删除”的任何邮件。 要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

“网络交互”(Web Interaction) 页面

您可以使用“网络交互”报告页面查看：

- 最终用户点击的恶意 URL 排行榜。
- 点击重写恶意 URL 的最终用户排行榜。
- 网络交互跟踪详细信息。

注释 仅当受管邮件安全设备上启用了“网络交互跟踪”功能时，才会填充“网络交互”报告模块。

为传入和传出邮件提供网络交互报告。这些模块中仅包含最终用户（通过策略或爆发过滤器）点击的重写 URL。

要在安全管理设备上查看“网络交互”(Web Interaction) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 网络交互 (Web Interaction)**。有关详细信息，请参阅使用交互式报告页面。

在“网络交互”报告页面，可以将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

以下列表解释了“网络交互”报告页面上的各部分：

表 *28:*“网络交互”*(Web Interaction)* 页面上的详细信息

部分	说明
时间范围 (Time Range)（下拉列表）	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围。
查看数据（下拉列表）	选择要查看其数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据。
最终用户点击数排名靠前的恶意URL	本部分显示传入和传入邮件中最终用户点击的恶意URL排行榜摘要。
点击恶意URL的最终用户排行榜。	本部分显示点击传入和传出邮件中重写恶意URL的最终用户排行榜摘要。
网络互动跟踪详细资料	本部分显示传入和传出邮件中恶意和中性URL的图表视图和摘要。 要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

网络互动跟踪详细资料

“网络交互跟踪详细信息”(Web Interaction Tracking Details) 表是一个包含以下信息的交互式表格：

- 所有重写的URL列表（恶意和非恶意）。
- 单击重写的URL时采取的操作（允许、阻止或未知）。
- 在最终用户单击URL时，如果对该URL（正常或恶意）的判定为“未知”(unknown)，则状态显示为“未知”(unknown)。这可能是因为，需要进一步审查该URL，或用户单击时网络服务器停止服务或无法访问。
- 最终用户单击重写的URL的次数。
- 请注意以下提示：
  - 如果您已配置内容或邮件过滤器以在重写恶意URL后传送邮件并通知另一个用户（例如管理员），则在被通知的用户单击已重写的URL时，原始收件人的网络交互跟踪数据会增加。

- 如果您使用网络界面向原始收件人之外的用户（如管理员）发送包含已重写URL的已隔离邮件副本，则在另一个用户单击已重写的 URL 时，原始收件人的网络交互跟踪数据会增加。

要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的蓝色数字链接。

补救报告页面

补救报告页面会显示使用邮箱自动补救以及邮箱搜索和补救进行补救的邮件总数。

在安全管理设备上，点击**监控 (Monitoring)** 选项卡，然后选择**邮件流摘要 (Mail Flow Summary)** > **用户报告 (User Reports)** > **补救报告 (Remediation Report)**。

您可以使用此报告执行以下操作：

- 使用“邮箱自动补救”(Mailbox Auto Remediation) 和“邮箱搜索和补救”(Mailbox Search and Remediate) 以查看尝试补救的邮件。
- 了解补救失败原因。例如，连接错误、身份验证错误等。

以下列表解释“补救报告”(Remediation Report) 页面上的各部分：

表 *29:* 补救报告页面上的详细信息

部分	说明
摘要	“摘要”部分显示以下信息： • 使用邮箱自动补救以及邮箱搜索和补救进行补救的邮件总数。 • 为已配置的补救操作成功补救的邮件数。 • 补救失败的邮件数。
邮箱自动修复报告	“邮箱自动补救”报告部分显示以下信息： • 邮箱修复成功或不成功的收件人列表。 • 对邮件执行的修复操作。 • 与 SHA-256 散列关联的文件名。点击 SHA-256 散列可查看邮件跟踪页面中的相关邮件。 • 为其邮箱执行补救操作成功或不成功的收件人定义的配置文件名称列表。 • 补救失败原因。 **注释** 升级到 AsyncOS 13.6.1 后，升级前收到的邮件的邮件跟踪状态会继续保持“已传送”(Delivered)，而不会是“已补救”(Remediated)。

部分	说明

邮箱搜索和补救	“邮箱搜索和补救”部分显示以下详细信息：
	• 正在进行或已完成的补救批处理列表。
	• 批处理中邮件的补救状态。
	• 批处理名称和批处理 ID。点击批处理名称可查看批处理详细信息：
	  • 启动补救的日期和时间。
	  • 发起补救的来源。
	  • 发起邮件补救的主机。
	  • 对邮件执行的补救操作。
	  • 消息的思科 Ironport 邮件 ID。
	  • 一个已读回执图标，用于显示收件人在成功补救邮件之前是否已阅读该邮件。
	  • 特定批处理中的邮件补救状态为“成功”(Success)、“失败”(Failed) 或“进行中”(In Progress)。
	  • 发送邮件的发件人的邮件地址。
	  • 传送邮件并稍后尝试补救的收件人的邮件地址。
	  • 将邮件发送给收件人的日期和时间。

“邮件过滤器”(Message Filters) 页面

“邮件过滤器”报告页面显示有关传入和传出邮件的邮件过滤器匹配项排行榜的信息（那些邮件过滤器具有最大数量的匹配邮件）。

可以使用“邮件过滤器”报告页面查看：

- 按匹配数排列的排名靠前的邮件过滤器，采用图形格式。
- 按匹配数排列的邮件过滤器总数，采用图表格式。

要在安全管理设备上查看“邮件过滤器”(Message Filters) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 邮件过滤器 (Message Filters)**。有关详细信息，请参阅使用交互式报告页面。

在“邮件过滤器”报告页面中，可以将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

“大量邮件”(High Volume Mail) 页面

可以使用“大量邮件”报告页面：

- 识别涉及来自单个发件人的大量邮件的攻击或在移动一小时期间内具有相同对象的攻击。
- 监控排名靠前的域以确保此类攻击不从您自己的域发起。如果发生这种情况，您的组织中的一个或多个账户可能受到影响。
- 帮助识别误报，使您可以相应地调整过滤器。

可以使用“大量邮件”报告页面查看：

- 主题排名靠前的邮件，采用图形格式。
- 信封发件人排名靠前的邮件，采用图形格式。
- 按匹配数排列的排名靠前的邮件过滤器，采用图形格式。
- 按匹配数排列的邮件过滤器总数，采用图表格式。

要在安全管理设备上查看“大量邮件”(High Volume Mail) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 大量邮件 (High Volume Mail)**。有关详细信息，请参阅使用交互式报告页面。

在“大量邮件”报告页面中，可以将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

此页面上的报告所显示的数据仅来自使用“标题重复”(Header Repeats) 规则的邮件过滤器，以及超过您在该规则中设置的邮件数阈值的邮件过滤器。当与其他规则结合使用时，系统会最后计算“标题重复”(Header Repeats) 规则，如果邮件处理由之前的条件决定，则完全不计算。同样，由“速率限制”(Rate Limiting) 捕获的邮件绝不会到达“标题重复”(Header Repeats) 邮件过滤器。因此，本来可能被视为大量邮件的某些邮件可能不会包括在这些报告中。如果您配置了过滤器以将某些邮件列入允许列表，这些邮件也从这些报告中排除。

有关邮件过滤器和信头重复规则的详细信息，请参阅邮件安全设备的在线帮助或用户指南。

“内容过滤器”(Content Filters) 页面

“内容过滤器”报告页面显示有关传入和传出内容过滤器匹配项排行榜的信息（那些内容过滤器具有最多的匹配邮件）。该页面以条形图和列表的形式显示数据。使用“内容过滤器”报告页面，可以回答以下类型的问题：

- 传入或传出邮件最多触发了哪些内容过滤器？
- 哪些用户最常发送或接收触发特定内容过滤器的邮件？

可以使用“内容过滤器”报告页面查看：

- 图形格式的传入和传出内容过滤器匹配项排行榜。
- 表格格式的传入和传出内容过滤器匹配项排行榜。

要在安全管理设备上查看“内容过滤器”(Content Filters) 报告页面，请从“产品”(Product) 下拉列表中选择**电子邮件 (Email)**，然后从“报告”(Reports) 下拉列表中选择**监控 (Monitoring) > 内容过滤器 (Content Filters)**。有关详细信息，请参阅使用交互式报告页面。

在“内容过滤器”报告页面中，可以将原始数据导出到CSV文件。有关打印或导出文件的信息，请参阅并导出报告和跟踪数据。

注释 请注意，您可以生成“内容过滤器”(Content Filters) 页面的计划报告。请参阅 计划邮件报告，第 103 页。

“内容过滤器详细信息”页面

“内容过滤器详细信息”(Content Filter Details) 页面显示过滤器在一段时间内的匹配项，以及按内部用户列出的匹配项。

在“按内部用户列出的匹配项”(Matches by Internal User) 部分中，单击用户名（邮件地址）可查看该内部用户的详细信息页面。有关详细信息，请参阅用户邮件摘要，第 89 页。

如果您的访问权限允许您查看邮件跟踪数据：要查看填充此报告的邮件的邮件跟踪详细信息，请单击表中的蓝色数字链接。

报告数据可用性 (Reporting Data Availability) 页面

在“报告”(Reports) 下拉列表中，选择设备新 Web 界面上的**监控 (Monitoring) > 报告数据可用性 (Reporting Data Availability)**，以便查看、更新数据和对数据排序，实时洞察资源利用率和邮件流量故障点。

所有数据资源利用率和邮件流量问题位置都显示在此页面上，包括由安全管理设备管理的整体设备的数据可用性。

在此报告页面中，还可以查看特定设备和时间范围的数据可用性。

灰色邮件报告

以下报告中反映了灰色邮件统计信息：

报告	包含以下灰色邮件数据
“邮件流摘要”页面 > “传入”选项卡	每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。
“邮件流详细信息”页面 > “传出发件人”选项卡	排名靠前的灰色邮件发件人。
“邮件流详细信息”页面>“传入邮件”选项卡	所有IP地址、域名或网络所有者的每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。

报告	包含以下灰色邮件数据
“用户邮件摘要”页面 > “按灰色邮件排名靠前的用户”	接收灰色邮件的排名靠前的最终用户。
“用户邮件摘要”页面 > 用户邮件详细信息	所有用户的每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。

相关主题

- 在升级到 AsyncOS 9.5 后报告营销邮件 , on page 44

在升级到 AsyncOS 9.5 后报告营销邮件

在升级到 AsyncOS 9.5 后：

- 营销邮件的数量是在升级前后检测到的营销邮件之和。
- 灰色邮件总数不包括在升级之前检测到的营销邮件数量。
- 尝试的邮件总数还包括在升级前检测到的营销邮件数量。
- 如果未在托管的邮件安全设备上启用灰色邮件功能，则营销邮件会被计为正常邮件。

关于计划和按需的邮件报告

可用的报告类型

除非另有说明，否则以下类型的邮件安全报告均以计划报告和按需报告的形式提供：

- “内容过滤器”(Content Filters) - 此报告包括多达 40 个内容过滤器。有关此页面上所包括内容的其他信息，请参阅“内容过滤器”(Content Filters) 页面, on page 97。
- “DLP 事件摘要”(DLP Incident Summary) - 有关此页面上所包括内容的信息，请参阅“DLP 事件摘要”(DLP Incident Summary) 页面, on page 92。
- “传送状态”(Delivery Status) - 此报告页面显示有关至特定收件人域或虚拟网关地址的传送问题的信息，对于由系统在过去三个小时传送的邮件，页面显示由前 20 个、50 个或 100 个收件人域构成的列表。可以通过点击每项统计数据列标题中的链接，按最新主机状态、有效收件人（默认）、连接超时、发送的收件人、软退回事件以及硬退回收件人进行排序。有关邮件安全设备上的“发送状态”(Delivery Status) 页面可执行的功能的详细信息，请参阅的文档或在线帮助。
- 基于域的执行摘要 - 该报告基于“邮件流摘要”页面, on page 52，并且限于一组指定的域。有关所包括内容的信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告, on page 100。
- “执行摘要”(Executive Summary) - 此报告基于来自“邮件流摘要”页面, on page 52的信息。有关所包括内容的信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告, on page 100。

- 邮件流详细信息 - 有关此页面上所包括内容的信息，请参阅“邮件流详细信息”页面, on page 74。
- 用户邮件摘要 - 有关此页面上所包括内容的信息，请参阅用户邮件摘要, on page 89。
- “外发目标”(Outgoing Destinations) - 有关此页面上所包括内容的信息，请参阅“外发目标”(Outgoing Destinations) 页面, on page 81。
- “发件人组”(Sender Groups) - 有关此页面上所包括内容的信息，请参阅“发件人组”(Sender Groups) 页面, on page 81。
- TLS 加密 - 有关此页面上所包括内容的信息，请参阅“TLS 加密”(TLS Encryption) 页面, on page 83。
- “病毒类型”(Virus Types) - 有关此页面上所包括内容的信息，请参阅“病毒过滤”(Virus Filtering) 页面, on page 66。

时间范围

根据报告，这些报告可以配置为包括前一天、前七天、前一个月、前历日（最多 250 天）或前历月（最多 12 个月）的数据。或者，您可以包括自定义天数（从 2 天到 100 天）或自定义月数（从 2 个月到 12 个月）的数据。

无论您何时运行报告，均会从上一个时间时间间隔（小时、天、星期或月）返回数据。例如，如果您计划在凌晨 1 点运行每日报告，则该报告将包含前一天从午夜到午夜（00:00 到 23:59）的数据。

语言和区域设置

Note 您可以使用单个报告的特定区域设置，计划 PDF 报告或将原始数据导出为 CSV 文件。使用“计划的报告”(Scheduled Reports) 页面上的语言下拉菜单可以按用户当前选择的区域设置和语言查看或计划 PDF 报告。请参阅并导出报告和跟踪数据的重要信息。

已存档报告的存储

有关报告存储时长以及何时从系统中删除已存档报告的信息，请参阅查看和管理已存档的邮件报告, on page 106。

其他报告类型

在安全管理设备的**邮件 > 报告**部分中，可以生成的两个特殊报告为：

- “基于域的执行摘要”(Domain-Based Executive Summary) 报告, on page 100
- “执行摘要”报告 , on page 103

“基于域的执行摘要”(Domain-Based Executive Summary) 报告

“基于域的执行摘要”(Domain-Based Executive Summary) 报告概述了网络中的一个或多个域的传入和传出邮件活动。它类似于“执行摘要”(Executive Summary report) 报告，但是它将报告数据限制为发送到您指定的域和从该域发送的邮件。“传出邮件摘要”(Outgoing Mail Summary) 仅在发送服务

器的 PTR（指针记录）中的域与您指定的域相匹配时才显示数据。如果指定了多个域，则设备会将所有域的数据整合在一个报告中。

要生成子域的报告，必须将其父域添加为邮件安全设备和安全管理设备的报告系统中的第二级域。例如，如果添加 example.com 作为第二级域，则其子域（例如 subdomain.example.com）可用于报告。要添加第二级域，请在邮件安全设备 CLI 中使用 **reportingconfig -> mailsetup -> tld**，在安全管理设备 CLI 中使用 **reportingconfig -> domain -> tld**。

与其他计划报告不同，系统不会存档“基于域的执行摘要”(Domain-Based Executive Summary) 报告。

“基于域的执行摘要”(Domain-Based Executive Summary) 报告和由发件人信誉过滤拦截的邮件

由于由发件人信誉过滤拦截的邮件不会进入工作队列，因此 AsyncOS 不处理这些邮件以确定域目标。某个算法会估计每个域的被拒绝邮件数。要确定每个域中阻止的邮件的确切数量，可以在安全管理设备上延迟 HAT 拒绝，直到邮件达到收件人级别 (RCPT TO)。这使得 AsyncOS 可以从传入邮件中收集收件人数据。可以在邮件安全设备上使用 **listenerconfig -> setup** 命令延迟拒绝。但是，该选项会影响系统性能。有关延迟的 HAT 拒绝的详细信息，请参阅邮件安全设备的相应文档。

Note 要查看安全管理设备上“基于域的执行摘要”报告中的“由信誉过滤拦截”结果，则必须在邮件安全设备和安全管理设备上都启用 **hat_reject_info**。要在安全管理设备上启用 **hat_reject_info**，请运行 **reportingconfig > domain > hat_reject_info** 命令。

管理“基于域的执行摘要”(Domain-Based Executive Summary) 报告的域和收件人列表

您可以使用配置文件管理“基于域的执行摘要”(Domain-Based Executive Summary) 报告的域和收件人。配置文件是设备的配置目录中存储的一个文本文件。该文件中的每一行均会生成一个单独的报告。这使您可以在单个报告中包括大量的域和收件人，以及在单个配置文件中定义多个域报告。

配置文件的每行包括一个由空格分隔的域名列表，以及一个由空格分隔的报告收件人邮件地址列表。逗号将域名列表与邮件地址列表隔开。您可以包括子域，方法是在父域名的开头附加子域名和一个句点，例如 subdomain.example.com。

以下是会生成三个报告的单个报告配置文件。

```
yourdomain.com sampledomain.com, admin@yourdomain.com
sampledomain.com, admin@yourdomain.com user@sampledomain.com
subdomain.example.com mail.example.com, user@example.com
```

Note 您可以使用配置文件和为单个命名报告定义的设置同时生成多个报告。例如，一家名为 Bigfish 的公司收购其他两家公司 Redfish 和 Bluefish，并继续保持这两家公司的域名。Bigfish 使用一个配置文件创建单个“基于域的执行摘要”(Domain-Based Executive Summary) 报告，该配置文件包含与单独的域报告相对应的三行。当设备生成“基于域的执行摘要”(Domain-Based Executive Summary) 报告时，Bigfish 的一位管理员收到关于 Bigfish.com、Redfish.com 和 Bluefish.com 域名的报告，同时 Redfish 的一位管理员收到关于 Redfish.com 域名的报告，Bluefish 的一位管理员收到关于 Bluefish.com 域名的报告。

您可以将每个命名报告的不同配置文件上传到设备。您还可以为多个报告使用相同的配置文件。例如，您可能创建单独的命名报告，提供关于相同的域在不同时间段的数据。如果您更新设备上的配置文件，您不必更新 GUI 中的报告设置，除非您更改文件名。

创建“基于域的执行摘要”(Domain-Based Executive Summary) 报告

步骤 1 在安全管理设备中，可以安排报告或立即生成报告。

要安排报告，请执行以下操作：

a) [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。
b) 依次选择**电子邮件 > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。
c) 单击**添加计划的报告 (Add Scheduled Report)**。

要创建按需的报告，请执行以下操作：

- 依次选择**邮件 (Email) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。
- 单击**立即生成报告 (Generate Report Now)**。

步骤 2 从**报告类型 (Report Type)** 下拉列表中，选择**基于域的执行摘要 (Domain-Based Executive Summary)** 报告类型。

步骤 3 指定要包括在报告中的域和报告收件人的邮件地址。您可以为生成报告选择以下选项之一：

- 通过指定各个域生成报告 (Generate report by specifying individual domains)。输入报告的域和报告收件人的邮件地址。使用逗号分隔多个条目。您还可以使用子域，例如 subdomain.yourdomain.com。如果您为预计不会频繁发生变化的少量域创建报告，建议指定各个域。
- 通过上载文件生成报告 (Generate reports by uploading file)。导入包含域列表和报告收件人邮件地址的配置文件。您可以从设备上的配置目录选择一个配置文件，或从您的本地计算机上传一个配置文件。如果您为频繁发生变化的大量域创建报告，建议使用配置文件。有关基于域的报告的配置文件的详细信息，请参阅管理“基于域的执行摘要”(Domain-Based Executive Summary) 报告的域和收件人列表 , on page 101。

Note 如果您将报告发送到外部账户（如 Yahoo! 邮箱或 Gmail），则可能需要将报告回信地址添加到外部账户的允许列表，以防止报告邮件被错误地归类为垃圾邮件。

步骤 4 在“标题”(Title) 文本字段中，键入报告标题的名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

步骤 5 在“外发域 (Outgoing Domain)”部分中，选择传出邮件摘要的域类型。选项包括：按服务器或按邮件地址。

步骤 6 从要包括的时间范围 (Time Range to Include) 下拉列表中，选择报告数据的时间范围。

步骤 7 在“格式”(Format) 部分中，选择报告的格式。

选项包括：

- PDF。创建格式化的 PDF 文档以用于传送和/或存档。可以通过单击“预览 PDF 报告”(Preview PDF Report) 来立即以 PDF 文件的形式查看报告。
- CSV。创建以逗号分隔值格式包含原始数据的 ASCII 文本文件。每个 CSV 文件可包含多达 100 行。如果报告包含多种类型的表格，则会为每种表格创建一个单独的 CSV 文件。

步骤 8 从“计划”(Schedule) 部分中，为生成报告选择一个计划。

选项包括：“每日”(Daily)、“每周”(Weekly)（包括星期几的下拉列表）或“每月”(Monthly)。

步骤 9 （可选）上传报告的自定义徽标。徽标出现在报告的顶部。

- 徽标应为 .jpg、.gif 或 .png 文件，最大尺寸为 550 x 50 像素。
- 如果未提供徽标文件，则使用默认的思科徽标。

步骤 10 为此报告选择一种语言。要以亚洲语言生成 PDF，请参阅并导出报告和跟踪数据的重要信息。

步骤 11 单击**提交 (Submit)** 以提交对页面所做的更改，然后单击**确认更改 (Commit Changes)** 以确认所做的更改。

“执行摘要”报告

执行摘要报告是对邮件安全设备中传入和传出邮件活动的高级概述，可以在安全管理设备上查看该报告。

此报告总结了您可以在“邮件流摘要”页面, on page 52上查看的信息。有关“邮件报告概述”(Email Reporting Overview) 页面的详细信息，请参阅“邮件流摘要”页面, on page 52。

“计划的报告”(Scheduled Reports) 页面

- 计划邮件报告, on page 103
- 计划 Web 报告

计划邮件报告

可以计划在关于计划和按需的邮件报告 , on page 99中列出的任何报告。

要管理报告计划，请参阅以下内容：

- 添加计划的报告, on page 104
- 编辑计划的报告, on page 104
- 终止计划的报告 , on page 105

我的邮件报告是“计划报告”菜单下的用户报告。用户报告只能由创建它们的用户查看。

Note 旧 Web 界面的计划报告不会显示在新 Web 界面的 **计划报告** 选项卡下。新 Web 界面的计划报告不会显示在旧 Web 界面的 **计划报告** 页面上。

添加计划的报告

要添加计划的邮件报告，请执行以下步骤：

步骤 1 依次选择**电子邮件 > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 2 点击**添加计划的报告 (Add Scheduled Report)**。

步骤 3 选择您的报告类型。

有关报告类型的说明，请参阅关于计划和按需的邮件报告 , on page 99。

Note - 有关“基于域的执行摘要”报告设置的信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告, on page 100。

- 计划的报告的可用选项因报告类型而异。本操作程序其余部分介绍的选项不一定适用于所有报告。

步骤 4 在**标题 (Title)** 字段中，键入报告的标题。

为了避免创建多个使用相同名称的报告，我们建议使用说明性的标题。

步骤 5 从**要包括的时间范围**下拉菜单中选择报告的时间范围。

步骤 6 选择所生成的报告的格式。

默认格式为 PDF。大多数报告还允许您将原始数据另存为 CSV 文件。

步骤 7 根据报告，对于“行数”，请选择要包括的数据量。

步骤 8 根据报告，选择要作为报告排序依据的列。

步骤 9 从**计划 (Schedule)** 区域中，为计划的报告选中天、周或月旁边的单选按钮。此外，请包括您要计划报告的时间。时间增量基于午夜到午夜（00:00 到 23:59）。

步骤 10 在**电子邮件** 文本字段中，输入生成的报告将发送到的邮件地址。

如果不指定邮件收件人，则系统仍会将报告存档。

您可以根据需要为报告添加任意数量的收件人，不添加收件人也没问题。但是，如果您需要将报告发送到大量地址，则可能需要创建邮件列表，而不是逐个列出收件人。

步骤 11 选择报告的语言。

有关亚洲语言，请参阅并导出报告和跟踪数据的重要信息。

步骤 12 点击**提交 (Submit)**。

编辑计划的报告

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

步骤 2 依次选择**电子邮件 > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 3 在“报告标题”(Report Title) 列中点击要修改的报告的名称链接。

步骤 4 修改报告设置。

步骤 5 提交并确认更改。

终止计划的报告

要防止未来继续生成计划的报告，请执行以下步骤：

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

步骤 2 依次选择**电子邮件 > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 3 选中与要终止生成的报告相对应的复选框。要删除所有计划的报告，请选中**全部 (All)** 复选框。

步骤 4 单击**删除 (Delete)**。

Note 未自动删除已删除的报告的任何存档版本。要删除以前生成的报告，请参阅删除已存档的报告, on page 107。

按需生成邮件报告

除可以使用了解新 Web 界面上的“邮件报告”页面, on page 47中介绍的交互报告页面查看（并为其生成 PDF）的报告之外，您还可以随时在指定的时间段为关于计划和按需的邮件报告 , on page 99中列出的报告保存 PDF 或原始数据 CSV 文件。

要生成按需的报告，请执行以下操作：

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

步骤 2 选择**电子邮件 > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

步骤 3 点击**立即生成报告 (Generate Report Now)**。

步骤 4 选择报告类型。

有关报告类型的说明，请参阅关于计划和按需的邮件报告 , on page 99。

步骤 5 在“标题”(Title) 文本字段中，键入报告标题的名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

Note 有关“基于域的执行摘要”(Domain-Based Executive Summary) 报告的设置信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告, on page 100。

计划报告的可用选项因报告类型而异。本操作程序其余部分介绍的选项不一定适用于所有报告。

步骤 6 从“要包括的时间范围”(Time Range to Include) 下拉列表中，为报告数据选择一个时间范围。

请注意自定义时间范围选项。

步骤 7 在“格式”(Format) 部分中，选择报告的格式。

选项包括：

- PDF。创建格式化的 PDF 文档以用于传送和/或存档。可以通过点击“预览 PDF 报告”(Preview PDF Report) 来立即以 PDF 文件的形式查看报告。
- CSV。创建以逗号分隔值格式包含原始数据的 ASCII 文本文件。每个 CSV 文件可包含多达 100 行。如果报告包含多种类型的表格，则会为每种表格创建一个单独的 CSV 文件。

步骤 8 选择要为其运行报告的设备或设备组。如果您尚未创建任何设备组，此选项不会出现。

步骤 9 从“传送选项”(Delivery Option) 部分中，选择以下选项：

- 选中**将报告存档 (Archive Report)** 复选框，将报告存档。

如果选择此选项，报告将在“已存档的报告”(Archived Reports) 页面上列出。

Note 无法对“基于域的执行摘要”(Domain-Based Executive Summary) 报告进行存档。

- 选中**立即通过邮件发送给收件人 (Email now to recipients)** 复选框，通过邮件发送报告。

在文本字段中，请输入报告的收件人邮件地址。

步骤 10 为此报告选择一种语言。要以亚洲语言生成 PDF，请参阅并导出报告和跟踪数据的重要信息。

步骤 11 点击**传送此报告 (Deliver This Report)** 生成报告。

存档的邮件报告页面

- 关于计划和按需的邮件报告 , on page 99
- 按需生成邮件报告 , on page 105
- 查看和管理已存档的邮件报告 , on page 106

查看和管理已存档的邮件报告

计划的报告和按需报告会存档一段时间。

安全管理设备会保留其生成的最新报告 - 对于每个计划报告，可包含多达 30 个最近的实例，并且对于所有报告，可包含 1000 个总版本。最多可将 30 个实例应用到具有相同名称和时间范围的计划报告。

存档的报告会自动删除。在添加新的报告时，系统会删除较旧的报告以将数量保持在 1000 个。

已存档的报告存储在设备上的 /periodic_reports 目录。（有关详细信息，请参阅IP 接口和访问设备。）

“存档”报告下的“我的邮件”报告只能由创建“计划”报告的用户查看。

Note 旧 Web 界面的存档报告显示在新 Web 界面的 **查看旧存档报告** 选项卡下。新 Web 界面的存档报告不会显示在旧 Web 界面上。

访问存档的报告

邮件 > 报告 > 存档的报告页面列出了您已选择存档的计划和按需报告，这些报告已生成但未清除。

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

步骤 2 选择**邮件 (Email) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

步骤 3 如果列表很长，要找到特定的报告，请通过从**显示 (Show)** 菜单中选择报告类型来过滤列表，或者单击某个列标题以按该列进行排序。

步骤 4 单击报告标题可查看该报告。

删除已存档的报告

系统会根据查看和管理已存档的邮件报告 , on page 106概述的规则自动删除报告。但是您可以手动删除不需要的报告。

要手动删除已存档的报告，请执行以下操作：

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

步骤 2 依次选择**电子邮件 > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

此时将显示可用的已存档报告。

步骤 3 选中一个或多个要删除的报告的复选框。

步骤 4 点击**删除 (Delete)**。

步骤 5 要防止未来继续生成计划的报告，请参阅终止计划的报告 , on page 105。

在新 Web 界面上计划和存档邮件报告

我的邮件报告是“计划报告”菜单下的用户报告。用户报告只能由创建它们的用户查看。“存档”报告下的“我的邮件”报告只能由创建“计划”报告的用户查看。

- 在新 Web 界面上计划邮件报告 ， 第 108 页
- 新Web 界面上的已存档邮件报告页面 ， 第 110 页

注释 旧 Web 界面的计划报告不会显示在新 Web 界面的 **计划报告** 选项卡下。新 Web 界面的计划报告不会显示在旧 Web 界面的 **计划报告** 页面上。

旧 Web 界面的存档报告显示在新 Web 界面的 **查看旧存档报告** 选项卡下。新 Web 界面的存档报告不会显示在旧 Web 界面上。

在新 Web 界面上计划邮件报告

在新 Web 界面上添加计划的报告

注释 您可以计划收藏夹报告（“我的邮件报告”(My Email Reports)）页面。有关如何计划存档报告的信息，请参阅在新 Web 界面上计划邮件报告。

要添加计划的邮件报告，请执行以下步骤：

步骤 1 登录设备的新 Web 界面。

步骤 2 选择**监控 (Monitoring)** > **计划和存档 (Schedule & Archive)**。

步骤 3 在**计划报告**选项卡中，单击+按钮。

步骤 4 选择您的报告类型。

有关报告类型的说明，请参阅关于计划和按需的邮件报告 ， 第 99 页。

注释 - 有关“基于域的执行摘要”报告设置的信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告 ， 第 100 页。

- 计划的报告的可用选项因报告类型而异。本操作程序其余部分介绍的选项不一定适用于所有报告。

步骤 5 在**标题 (Title)** 字段中，键入报告的标题。

为了避免创建多个使用相同名称的报告，我们建议使用说明性的标题。

步骤 6 从**要包括的时间范围**下拉菜单中选择报告的时间范围。

步骤 7 选择所生成的报告的格式。

默认格式为 PDF。

注释 您可以导出“我收藏的报告”(My Favorite Reports) 页面或者下载“我收藏的报告”(My Favorite Reports) 页面。有关详细信息，请参阅导出报告和跟踪数据。

步骤 8 从**邮件设备 (Email Appliance)** 部分的下拉列表中选择邮件安全设备。

步骤 9 从“传送选项”(Delivery Option) 部分中，选择以下任一选项：

如果选择此选项，报告将在“已存档的报告”(Archived Reports) 页面上列出。

注释 无法对“基于域的执行摘要”(Domain-Based Executive Summary) 报告进行存档。

- 要存档报告，请选择**仅存档 (Only Archive)**。
- 要存档并通过邮件发送报告，请单击**存档并通过邮件发送至收件人 (Archive and Email to Recipients)**。
- 要通过邮件发送报告，请单击**仅发送邮件至收件人 (Only Email to Recipients)**。

在**邮件 ID** 字段中，输入收件人邮箱地址。

步骤 10 从**计划**区域中，为计划报告选中天、周或月旁边的单选按钮。此外，请包括您要计划报告的时间。时间增量基于午夜到午夜（00:00 到 23:59）。

步骤 11 选择报告的语言。

步骤 12 点击**提交**。

在新 Web 界面上编辑计划报告

步骤 1 登录设备的新 Web 界面。

步骤 2 选择**监控 (Monitoring) > 计划和存档 (Schedule & Archive)**。

步骤 3 在“计划报告”选项卡中，选中所需的报告标题列旁边的复选框，然后单击  按钮。

步骤 4 修改报告设置。

步骤 5 提交并确认更改。

在新 Web 界面上终止计划报告

要防止未来继续生成计划的报告，请执行以下步骤：

步骤 1 登录设备的新 Web 界面。

步骤 2 选择**监控 (Monitoring) > 计划和存档 (Schedule & Archive)**。

步骤 3 在“计划报告”选项卡中，选中与要终止生成的报告相对应的复选框。要删除所有计划的报告，请选中**全部 (All)** 复选框。

步骤 4 点击**删除 (Delete)**。

注释 未自动删除已删除的报告的任何存档版本。要删除以前生成的报告，请参阅访问新 Web 界面上的存档报告，第 110 页。

新Web 界面上的已存档邮件报告页面

访问新 Web 界面上的存档报告

计划和存档 (Schedule & Archive 页面的**查看存档的报告 (View Archived Reports)** 选项卡列出了您已选择存档的计划和按需报告，这些报告已生成但未清除。

注释 您可以存档收藏夹报告（“我的邮件报告”(My Email Reports)）页面。有关如何添加存档报告的信息，请参阅新Web 界面上的已存档邮件报告页面。

步骤 1 登录设备的新 Web 界面。

步骤 2 选择**监控 (Monitoring) > 计划和存档 (Schedule & Archive)**。

步骤 3 单击**查看存档报告 (View Archived Reports)** 选项卡。

步骤 4 如果列表很长，要找到特定的报告，您可搜索报告名称，或者单击某个列标题以按该列进行排序。

按需生成邮件报告

除了您可以使用了解新 Web 界面上的“邮件报告”页面, on page 47中介绍的交互式报告页面查看（和为其生成 PDF）的报告之外，您还可以随时在指定的时间段为关于计划和按需的邮件报告 , on page 99中列出的报告保存 PDF 或原始数据 CSV 文件。

要生成按需的报告，请执行以下操作：

步骤 1 登录设备的新 Web 界面。

步骤 2 选择**监控 (Monitoring) > 计划和存档 (Schedule & Archive)**。

步骤 3 在“查看存档报告”(View Archived Reports) 选项卡中，点击 + 按钮。

步骤 4 选择报告类型。

有关报告类型的说明，请参阅关于计划和按需的邮件报告 , on page 99。

步骤 5 在**标题**字段中，输入报告标题的名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

Note 有关“基于域的执行摘要”(Domain-Based Executive Summary) 报告的设置信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告, on page 100。

计划报告的可用选项因报告类型而异。本操作程序其余部分介绍的选项不一定适用于所有报告。

步骤 6 从**要包括的时间范围**下拉列表中，为报告数据选择一个时间范围。

请注意自定义时间范围选项。

步骤 7 在“格式”(Format) 部分中，选择报告的格式。

选项包括：

- PDF。创建格式化的 PDF 文档以用于传送和/或存档。可以通过点击“预览 PDF 报告”(Preview PDF Report) 来立即以 PDF 文件的形式查看报告。
- CSV。创建以逗号分隔值格式包含原始数据的 ASCII 文本文件。每个 CSV 文件可包含多达 100 行。如果报告包含多种类型的表格，则会为每种表格创建一个单独的 CSV 文件。

步骤 8 选择要为其运行报告的设备或设备组。如果您尚未创建任何设备组，此选项不会出现。

步骤 9 从“邮件设备”部分的下拉列表中选择邮件安全设备。

步骤 10 从“传送选项”(Delivery Option) 部分中，选择以下任一选项：

如果选择此选项，报告将在“已存档的报告”(Archived Reports) 页面上列出。

Note 无法对“基于域的执行摘要”(Domain-Based Executive Summary) 报告进行存档。

- 要存档报告，请选择**仅存档 (Only Archive)**。
- 要存档并通过邮件发送报告，请点击**存档并通过邮件发送至收件人 (Archive and Email to Recipients)**。
- 要通过邮件发送报告，请点击**仅发送邮件至收件人 (Only Email to Recipients)**。

在**邮件 ID** 字段中，输入收件人邮箱地址。

步骤 11 为此报告选择一种语言。要以亚洲语言生成 PDF，请参阅并导出报告和跟踪数据的重要信息。

步骤 12 点击**提交 (Submit)** 生成报告。

删除新 Web 界面上的存档报告

系统会根据查看和管理已存档的邮件报告 ，第 106 页概述的规则自动删除报告。但是您可以手动删除不需要的报告。

要手动删除已存档的报告，请执行以下操作：

步骤 1 登录设备的新 Web 界面。

步骤 2 选择**监控 (Monitoring)** > **计划和存档 (Schedule & Archive)**。

步骤 3 在“查看存档报告”(View Archived Reports) 选项卡中，选中一个或多个要删除的报告的复选框。

步骤 4 点击垃圾桶按钮。

步骤 5 要防止未来继续生成计划的报告，请参阅在新 Web 界面上终止计划报告 ， 第 109 页。

邮件报告故障排除

另请参阅对所有报告进行故障排除。

爆发过滤器报告未正确显示信息

问题

爆发过滤器报告未正确显示威胁信息。

解决方案

确认设备可以与管理设备 > 系统管理 > 更新设置中指定的思科更新服务器通信。

在点击报告中的链接后，邮件跟踪结果与报告结果不匹配

问题

在从报告中进行深入分析时，邮件跟踪结果与预期的结果不相符。

解决方案

如果报告和跟踪没有一致且同时启用，而且不能正常运行，或者没有一致且同时地在每个邮件安全设备上进行集中或本地存储，则会发生该情况。仅当启用每项功能（报告、跟踪）时，才会获取该功能的数据。

相关主题

- 检查邮件跟踪数据的可用性

高级恶意软件保护判定更新报告结果存在差异

问题

网络安全设备和邮件安全设备发送同一文件进行分析，而网络和邮件的 AMP 裁定更新报告针对该文件显示不同的裁定。

解决方案

这种情况是暂时的。下载了所有判定更新后，结果便会匹配。实现匹配最多需要 30 分钟。

查看文件分析报告详细信息的问题

文件分析报告详细信息不可用

问题

文件分析报告详细信息不可用。

解决方案

请参阅文件分析报告详细信息的要求 , on page 34。

查看文件分析 (File Analysis) 报告详细信息时出错

问题

当您尝试查看“文件分析”(File Analysis) 报告详细信息时，出现没有可用的云服务器配置 (No cloud server configuration is available) 错误。

解决方案

转到**管理设备 > 集中服务 > 安全设备**，然后添加至少一个启用了文件分析功能的邮件安全设备。

使用私有云 Cisco AMP Threat Grid 设备查看文件分析 (File Analysis) 报告详细信息时出错

问题

当您尝试查看“文件分析”(File Analysis) 报告详细信息时，出现 API 密钥、注册或激活错误。

解决方案

如果您使用私有云（本地部署的）Cisco AMP Threat Grid 设备进行文件分析，请参阅（本地文件分析）激活文件分析账户 , on page 36。

如果 Threat Grid 设备主机名发生更改，您必须重复执行所引用操作程序中的流程。

文件分析相关错误的记录

注册及其他与文件分析相关的错误均记录在 GUI 日志中。

灰色邮件或营销邮件总数似乎不正确

问题

“营销”、“社交”和“批量”邮件的计数超过灰色邮件总数。

解决方案

“营销”(Marketing) 邮件总数包括在升级到 AsyncOS 9.5 前后收到的营销邮件，但是灰色邮件的总数仅包括在升级后收到的邮件。请参阅在升级到 AsyncOS 9.5 后报告营销邮件 , on page 44。

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。