思科域保护用户指南

首次发布：18-07-2020

思科系统公司

www.cisco.com

思科在全球设有 200 多个办事处。

各分支机构的地址、电话号码和传真号

www.cisco.com/go/offices。

目录

章 1

章 2 配置到传感器的传送

安装传感器后，您需要配置电子邮件网关，以将邮件流定向到传感器。

配置传送的步骤因电子邮件网关的类型而异。请参阅您的电子邮件网关所对应的传送配置指南。

应将传送配置为在初步的反垃圾邮件、防病毒、防恶意软件或任何其他过滤或沙盒分析完成后再进行传送。高级网络钓鱼防护 并非替代反垃圾邮件和防恶意软件的第一道防线。其目的是寻找已经通过此过滤的不可靠邮件。

配置双重传送

安装传感器后，现在应该配置电子邮件网关，以将邮件流定向到该网关(双重传送)。

配置双重传送的步骤因电子邮件网关的类型而异。请参阅您的电子邮件网关所对应的双重传送配置指南。

无论网关类型如何：

- 均应将双重传送配置为从您的企业中的“最后一跳”进行传送。某些企业有多个网关“层”或 MTA(邮件传输代理)层或 SEG(安全电子邮件网关)；请务必将双重传送配置为从最终路由点进行传送，最终路由点通常是您会发送邮件到内部邮件存储(例如 Microsoft Exchange)的位置。
- 应将双重传送配置为在所有反垃圾邮件、防病毒、防恶意软件或任何其他过滤或沙盒分析完成后再进行传送。思科高级网络钓鱼防护 并非替代反垃圾邮件和防恶意软件的第一道防线。其目的是寻找已经通过此过滤的不可靠邮件。

中断双重传送

可以在两个点中断从传感器到 思科 的邮件。

- 传感器本身包含“接收模式”设置，它默认设置为“上传数据”。

  如果您只需要测试向传感器传送邮件但不将数据上传到 思科 进行处理，您可以将“接收模式”设置为“不上传数据”。

- 您的组织有一个“收集模式”开关，必须由 思科 销售工程师配置该开关之后，邮件才会出现在 高级网络钓鱼防护 中。

  “收集模式”开关是 思科 的一项保护措施，用于防止新组织发送到系统中的数据流量突然飙升。

双重传送的特定说明

本指南包含有关如何为以下环境配置双重传送的信息：

- "配置双重传送：思科 ESA" 向下

配置双重传送：思科 ESA

此部分介绍如何配置从思科电子邮件安全设备(以前称为 IronPort)环境到 思科高级网络钓鱼防护 传感器的双重传送。

一般程序如下：

步骤 1：在思科 ESA 中启用 SPF/DKIM/DMARC 检查。

步骤 2：创建内容过滤器，以使用“密件抄送：”操作将邮件复制到传感器。

步骤 3：配置适当邮件策略以引用此过滤器，以便仅将传送的邮件(不是垃圾邮件或 PVO(策略、病毒和爆发)隔离邮件)复制到传感器。

步骤 4：配置退回处理以正确管理意外的传送失败。

步骤 5：确认已设置所需的任何系统警报，以向管理员通知任何问题。

步骤 6：考虑其他已加入白名单的电子邮件流。

步骤 7：将警报服务器加入白名单，确保您和您的用户收到警报。

有关“Authentication-Results”信头的重要注意事项

传感器依靠准确且未损坏的 Authentication-Results 信头来帮助评估发送方身份。通常，您企业的“边界”MTA(即从互联网上的发送方 MTA 进入企业的第一个入口点)将评估传入邮件并添加 Authentication-Results 信头，而您企业中的所有下游 MTA 将仔细配置为保留此信头的完整性(即，它们不得用自己的信头覆盖此信头，除非它们能够以准确的信息进行覆盖，而且它们也不得从邮件中剥离此信头)。

但是，邮件路由环境可能非常复杂，想要确保每个下游 MTA 的信头完整性有时候并不现实。为了简化这种情况，传感器将先查找该信头的副本(名为 X-Agari-Authentication-Results)。如果没有找到，传感器才会转而查看 Authentication-Results 信头。

因此，您可以将边界 MTA 配置为用替代名称创建(或复制) Authentication-Results 信头：它通过各下游 MTA 而不受损坏的可能性更大。本指南中介绍了有关如何对各种 MTA 产品执行此操作的说明。

步骤 1：在思科 ESA 中启用 SPF/DKIM/DMARC 检查

1. 转至邮件策略 > 邮件流策略。
2. 点击默认策略参数。
3. 确保 DKIM 验证、SPF/SIDF 验证和 DMARC 验证均设置为打开。按如下所示保留相关设置。

Security Features	
Spam Detection:	On Off
Virus Protection:	On Off
Encryption and Authentication:	TLS
	SMTP Authentication
	If Both TLS and SMTP Authentication ar enable
Domain Key/DKIM Signing:	On Off
DKIM Verification:	On Off
	Use DKIM Verification Profil
S/MIME Decryption/Verification:	On Off
	Signature After Processing
S/MIME Public Key Harvesting:	S/MIME Public Key Harvesting
	Harvest Certificates on Verification Failure
	Store Updated Certificate
SPF/SIDF Verification:	On Off
	Conformance Leve
	Downgrade PRA verification result if 'Resen Sender:' or 'Resent-From:' were used
	HELO Tes
DMARC Verification	On Off
	Use DMARC Verification Profil
	DMARC Feedback Reports:
Bounce Verification:	Consider Untagged Bounces to be Vali
	(Applies only if bounce verification address tag

“DKIM 验证”、“SPF/SIDF 验证”和“DMARC 验证”设置均在思科 ESA 中正确配置。

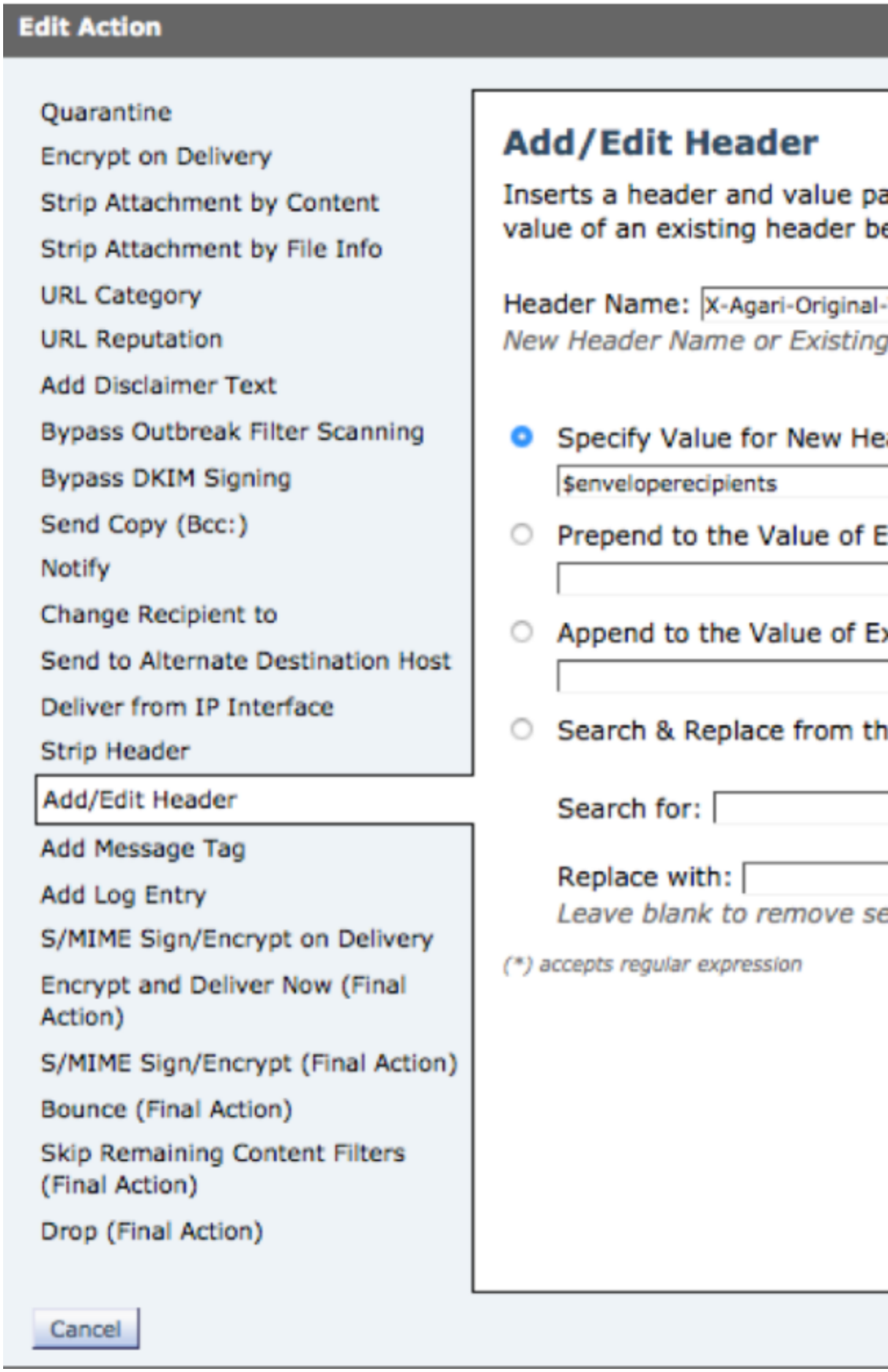
步骤 2：创建用于转移邮件的“密件抄送”过滤器

1. 以管理员用户身份登录思科 ESA(电子邮件安全设备)。
2. 转至邮件策略 ->传入内容过滤器。

   如果已为集群管理配置了思科 ESA 环境：应在集群顶级或子组级别(如果只希望操作影响一组特定的电子邮件安全设备 (ESA) 实例)完成以下步骤。

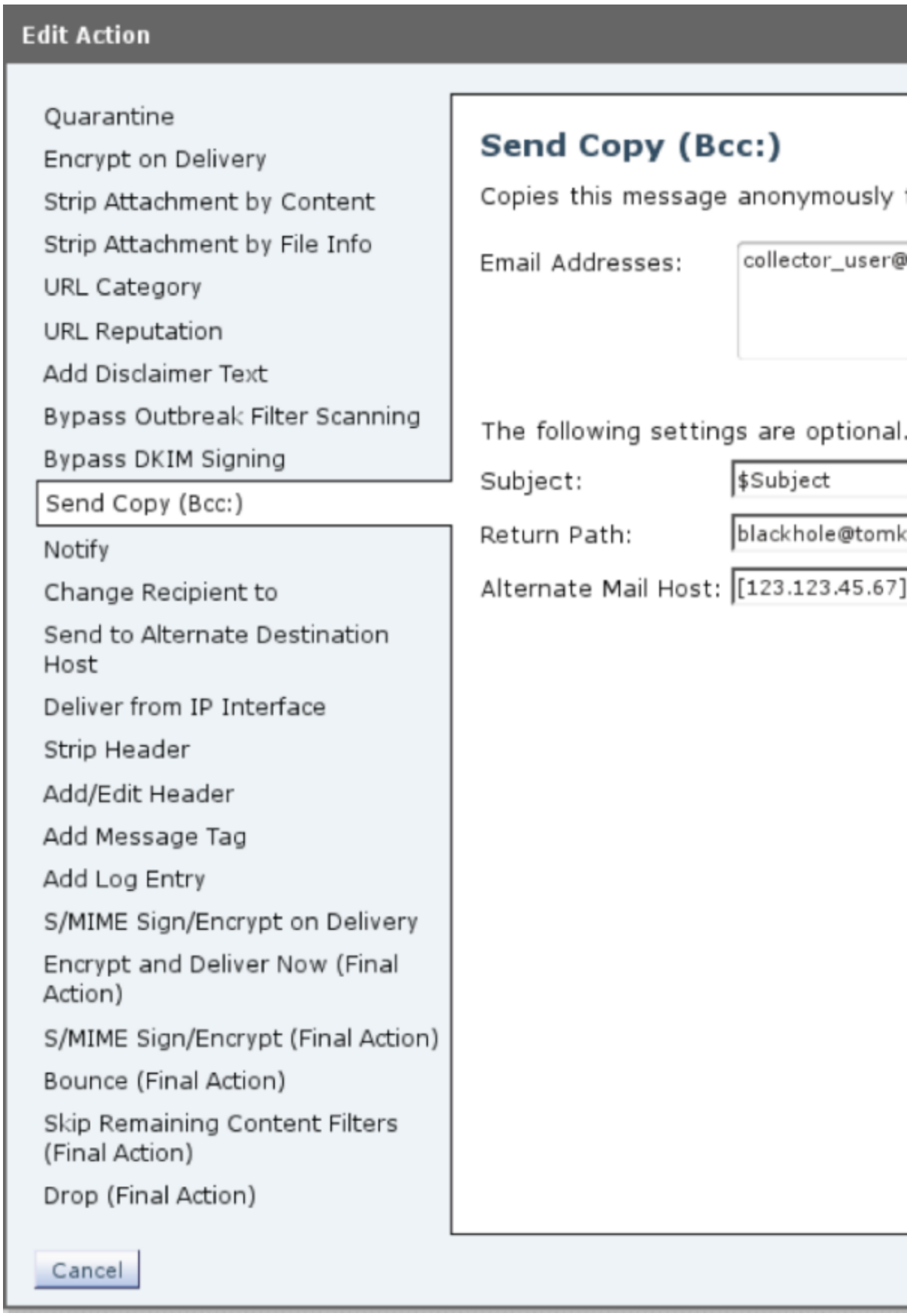
3. 点击添加过滤器，并为过滤器指定一个易于识别的名称“思科_sensor”。
4. 在“说明”字段中输入说明，以便将来的管理员了解过滤器的作用和应该联系的人员。例如：“此过滤器用于将邮件流密件抄送到传感器，并在传感器上保存和传递某些方面的邮件信头信息和身份验证数据。有问题吗？ 请发送电子邮件至 joeadmin@example.com 联系管理员 Joe”
5. 确定该过滤器的顺序，使其能够让传感器接收将要传送至最终用户的所有邮件(在所有垃圾邮件和病毒扫描完成后，以及任何可能丢弃邮件的其他邮件过滤策略执行完之后)。如果您使用的其他高级过滤中某个过滤器会触发即时传送并绕过内容过滤器“主列表”中的后续过滤器，您应该考虑这些过滤器并正确放置传感器过滤器以实现所需结果：收集传送至用户的所有邮件。
6. (可选)向内容过滤器添加条件。根据您的环境，可将该过滤器与特定收件人或域的特定传入邮件策略关联(请参阅下文相关说明)。如果有过滤逻辑会导致不丢弃反垃圾邮件或防病毒检测结果呈阳性的邮件(也不会传送至用户)，则您需要在该过滤器中包含条件，让传感器过滤器不进行匹配。如果没有，您可以跳过向内容过滤器添加条件的步骤，过滤器将对任何邮件评估为“True”。再次说明，内容过滤器的目标是仅处理将要直接传送至最终用户的邮件。
7. 向邮件添加信头的添加操作。您需向邮件添加 X-Agari-Original-From 和 X-Agari-Original-To，如果您的思科 ESA 是边界网关，您还需添加 X-Agari-Authentication-Results 信头。每次操作添加一个信头，因此请在每次操作中重复以下子步骤。
   a. 点击添加操作。
   b. 在“添加操作”对话框中，选择添加/编辑信头。
   c. 按照下表输入信头名称值。
   d. 选择指定新信头值，然后按下表输入值。
   e. 仔细检查名称中有无拼写错误。
   f. 点击确定。

信头名称值	指定新信头值
X-Agari-Original-From	$EnvelopeFrom
X-Agari-Original-To	$enveloperecipients
X-Agari-Authentication-Results	$Header['Authentication-Results'] 仅当您的思科 ESA 是边界网关 MTA 时才添加此信头。


Edit Action
Quarantine
Encrypt on Delivery
Strip Attachment by Content
Strip Attachment by File Info
URL Category
URL Reputation
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Bypass DKIM Signing
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add/Edit Header
Add Message Tag
Add Log Entry
S/MIME Sign/Encrypt on Delivery
Encrypt and Deliver Now (Final Action)
S/MIME Sign/Encrypt (Final Action)
Bounce (Final Action)
Skip Remaining Content Filters (Final Action)
Drop (Final Action)
Add/Edit Header
Inserts a header and value pa
value of an existing header be
Header Name: X-Agari-Original-
New Header Name or Existing
Specify Value for New He
$enveloperecipients
Prepend to the Value of E
Append to the Value of Ex
Search & Replace from th
Search for:
Replace with:
Leave blank to remove se
(*) accepts regular expression
Cancel

X-Agari-Original-To 信头内容过滤器操作的示例。

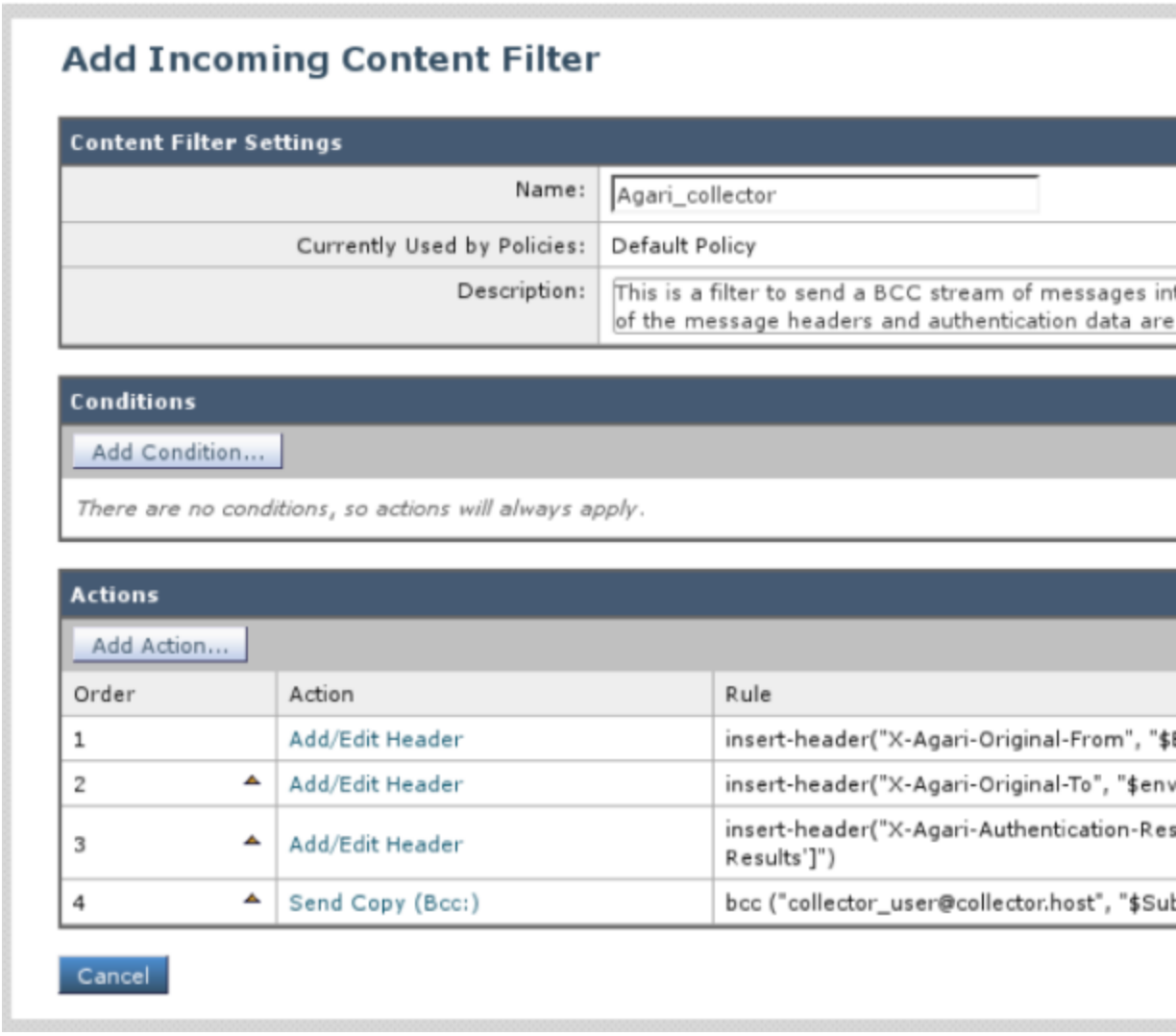
8. 为此过滤器创建主要操作：将整个邮件密件抄送到传感器中。
    - 密件抄送操作的电子邮件地址应为：
        - [用户名]@[symbolic_name].hosted.agari.com(适于 思科 托管的传感器)
        - [用户名]@[sensor_IP_address](当传感器在您自有基础设施中时)
    - 密件抄送邮件的主题应与原件相同，因此请将“主题”字段保留为“$Subject”
    - “返回路径”条目最初应设置为满足以下条件的适当地址：要么完全忽略邮件退回，要么监控邮件退回中是否存在传送至传感器中失败的情况。不要将“返回路径”字段留空。如果这样做，万一传送至传感器时出现问题，则可能会将邮件退回原始邮件发件人。当您确定您配置的传送工作正常后，您可于稍后将“返回路径”条目更改为“<>”，这将导致立即从传送队列中删除任何明确的传送失败。
    - 如果密件抄送邮件地址中指定的域无法让邮件传送至相应的预期目的地，您可以使用“备用邮件主机”条目。此设置的结果将导致系统尝试直接将邮件传送至指定主机，而非传送至电子邮件地址的 MX 记录或思科 ESA“SMTP 路由”功能所指定的任何地址。换言之，您可以使用此字段直接指定传感器的主机或 IP 地址(IP 地址应该以方括号括起来，例如 [123.123.45.67]) 。请注意，上面指定的电子邮件地址中使用的域仍与退回处理相关，如下所述。


Edit Action
Quarantine
Encrypt on Delivery
Strip Attachment by Content
Strip Attachment by File Info
URL Category
URL Reputation
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Bypass DKIM Signing
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add/Edit Header
Add Message Tag
Add Log Entry
S/MIME Sign/Encrypt on Delivery
Encrypt and Deliver Now (Final Action)
S/MIME Sign/Encrypt (Final Action)
Bounce (Final Action)
Skip Remaining Content Filters (Final Action)
Drop (Final Action)
Send Copy (Bcc:)
Copies this message anonymously
Email Addresses:
collector_user@
The following settings are optional.
Subject:
$Subject
Return Path:
blackhole@tomk
Alternate Mail Host:
[123.123.45.67]
Cancel

密件抄送操作

9. 点击确定。

此示例显示了上面的内容过滤器定义(点击“提交”之前)：

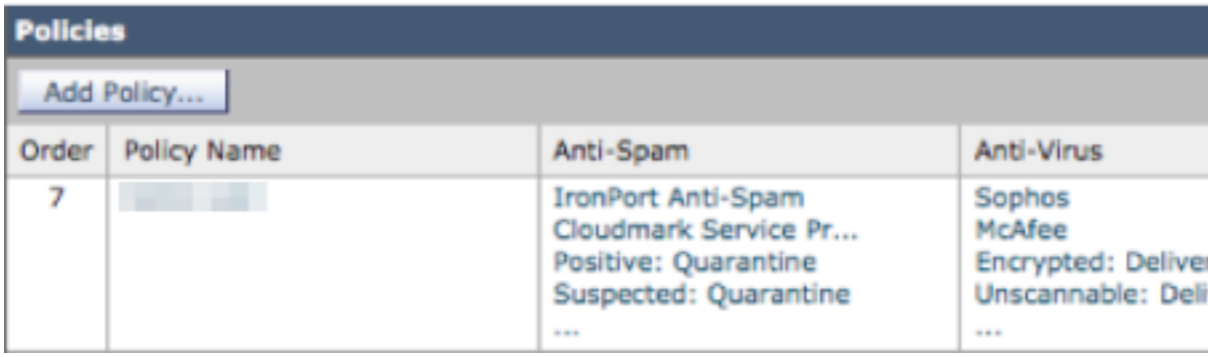


内容过滤器摘要

上图显示了添加的 X-Agari-Authentication-Results 信头：只有当思科 ESA MTA 是边界网关 MTA 时才应添加此信头。如果思科 ESA MTA 位于边界网关下游，则不应添加此信头。

10. 点击**提交**保存新过滤器。
11. 将过滤器与所有相应的传入邮件策略关联。
    a. 转到邮件策略 -> 传入邮件策略。
    b. 在相应行的内容过滤器列中编辑分配的内容过滤器以引用(启用)新创建的过滤器。在此过程中，您可能需要为该策略完全启用内容过滤器。

修改后的“策略”行可能如下所示：



包含内容过滤器的“策略”行

请记住，将邮件传送至最终用户(没有将邮件置于隔离文件夹或删除邮件)的任何策略应引用内容过滤器，以用于将邮件密件抄送至传感器。传感器应获取所有传送邮件的密件抄送副本，不包括已丢弃或隔离的任何垃圾邮件或病毒邮件。

12. 点击确认更改。

请注意，提交更改后，邮件将开始路由到传感器。如有任何邮件退回问题，可能会加重系统的负担。或者，您可以等到完成下一部分介绍的退回处理步骤后再提交更改。

步骤 3：避免隔离邮件复制到传感器

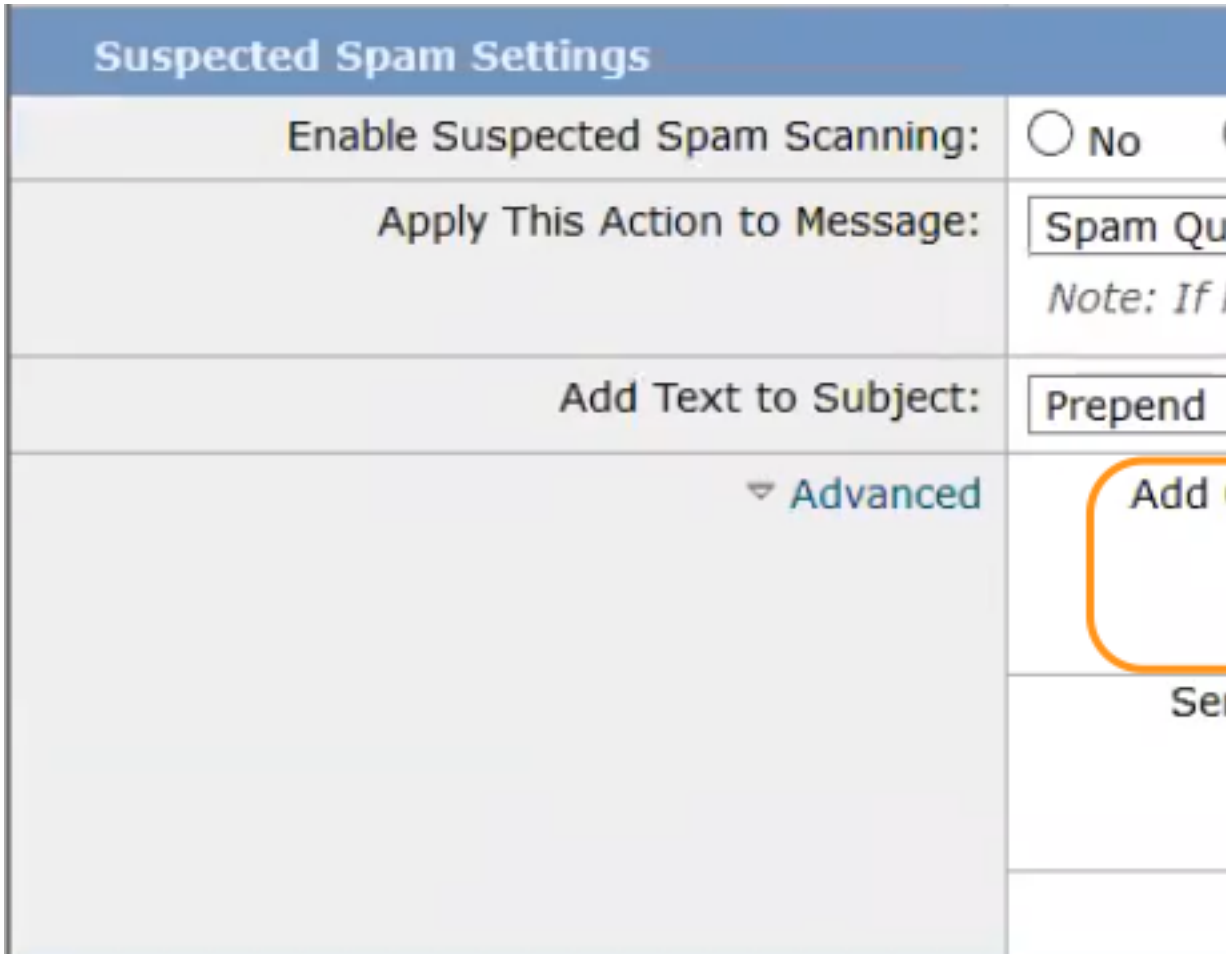
策略所隔离的垃圾邮件、病毒、灰色邮件和类似邮件不应发送到 思科 传感器。要避免这些隔离邮件受上面创建的密件抄送内容过滤器的影响，可以向传入邮件策略添加操作，以为不同类型的隔离邮件插入特定信头，然后使用其中任一信头的存在作为条件，避免这些邮件由内容过滤器触发并复制到传感器。

如果您的策略没有将自定义信头添加到邮件以将其识别为垃圾邮件，您还可能需要修改此过滤器将附加到的策略，使过滤器条件可以正确识别要排除的邮件。

修改将使用此过滤器的策略

这会将一个或多个自定义信头添加到策略。此过程的目标是对您定义的用于识别垃圾邮件和隔离邮件的策略执行此操作。

1. 转到邮件策略 > 传入邮件策略。
2. 在要编辑的策略的行中点击“反垃圾邮件”(用于垃圾邮件)、“防病毒”、“高级恶意软件防护”或“灰色邮件”(用于隔离邮件)设置。
3. 点击高级。(根据您在修改的设置，此处可能是“可疑垃圾邮件设置”、“感染病毒的邮件”或“批量电子邮件操作”部分。)



4. 在“添加自定义信头”部分中，输入信头和值。信头应是唯一的且不言自明的。例如，对于垃圾邮件，信头可以是 *MyCompany_suspected_spam*。值应是您使用的合理词汇，例如 *positive* 或 *true*。
5. 记下信头值，以便可以在下一部分"向过滤器添加条件" 向下中使用。
6. 点击提交。

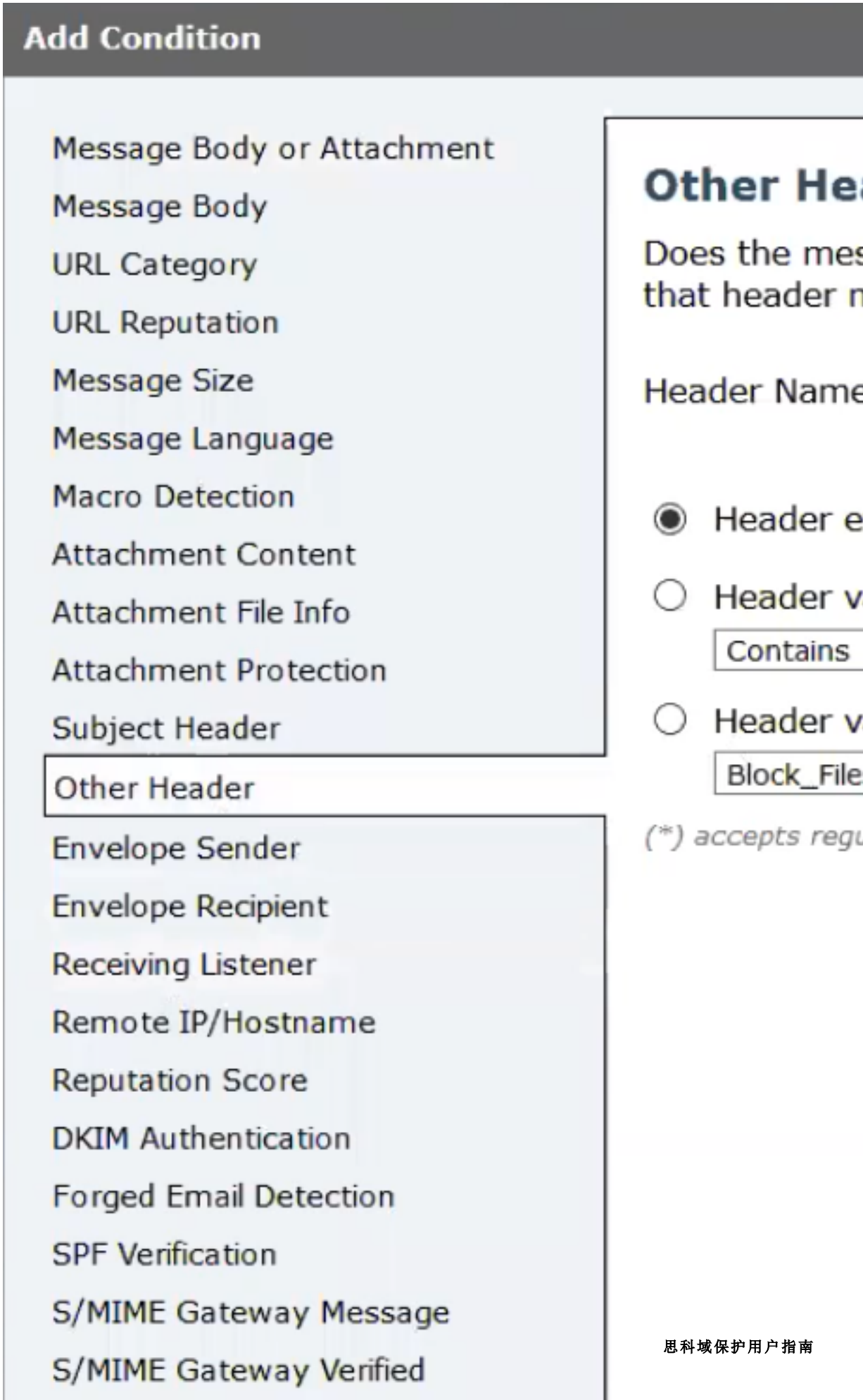
对隔离邮件的所有垃圾邮件、防病毒和灰色邮件策略重复此操作。

您的策略还可以在识别垃圾邮件时修改邮件主题。例如，一些公司将配置垃圾邮件规则，以将 [可疑垃圾邮件] 预置到识别的垃圾邮件中。可以配置策略条件以匹配主题中的邮件修改，但这种做法较为复杂和费时。匹配信头值的做法更快，也更可靠。

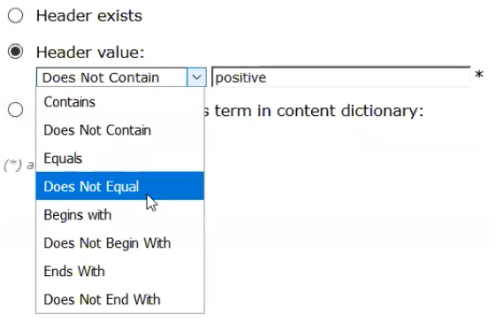
向过滤器添加条件

1. 转至邮件策略 > 传入邮件过滤器。
2. 点击您在步骤 1 中创建的过滤器的名称。
3. 点击添加条件。
4. 点击其他信头。
5. 在“信头名称”字段中，输入您在"修改将使用此过滤器的策略" 上一页中创建的

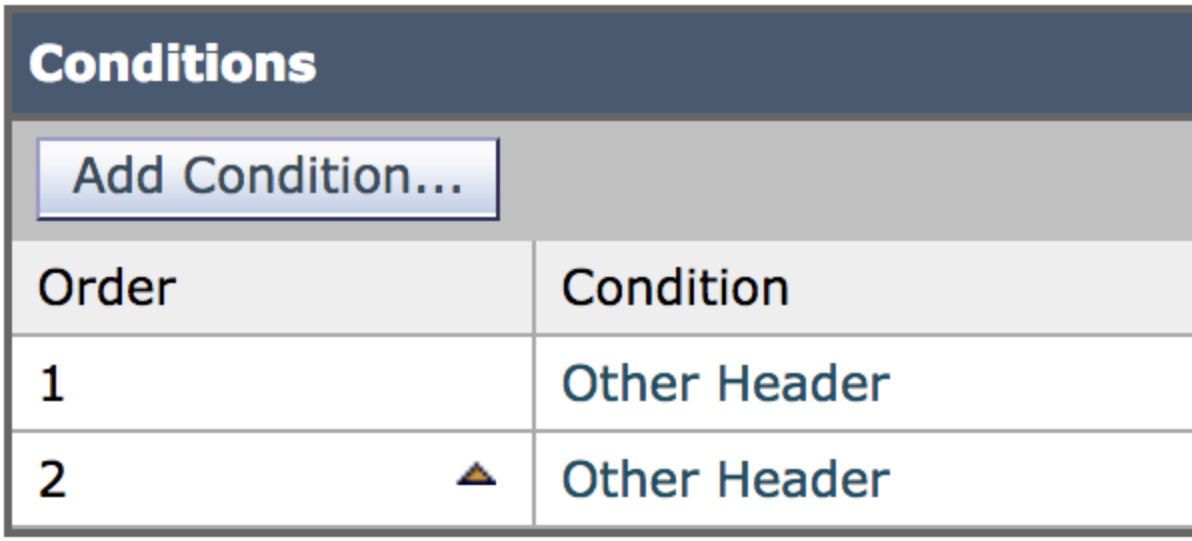
自定义信头的名称。


Add Condition
Message Body or Attachment
Message Body
URL Category
URL Reputation
Message Size
Message Language
Macro Detection
Attachment Content
Attachment File Info
Attachment Protection
Subject Header
Other Header
Envelope Sender
Envelope Recipient
Receiving Listener
Remote IP/Hostname
Reputation Score
DKIM Authentication
Forged Email Detection
SPF Verification
S/MIME Gateway Message
S/MIME Gateway Verified
Other He
Does the mes
that header n
Header Name
Header e
Header v
Contains
Header v
Block_File
(*) accepts regu

6. 在信头值下拉列表中，选择不等于，然后输入您上面创建的自定义信头的值。



7. 点击确定。
8. 对于在"修改将使用此过滤器的策略"在本页 15中添加的所有信头，请重复步骤 3 至 7。
9. 在应用规则下拉列表中，选择仅当所有条件同时匹配时。



10. 点击提交。

如果您记得的话，在步骤 1 中，此内容过滤器配置为通过密件抄送将副本发送到思科 传感器。此条件现在将此指令修改为，通过密件抄送将副本发送到 思科 传感器，除非因邮件被识别为垃圾邮件而使邮件中存在自定义信头。

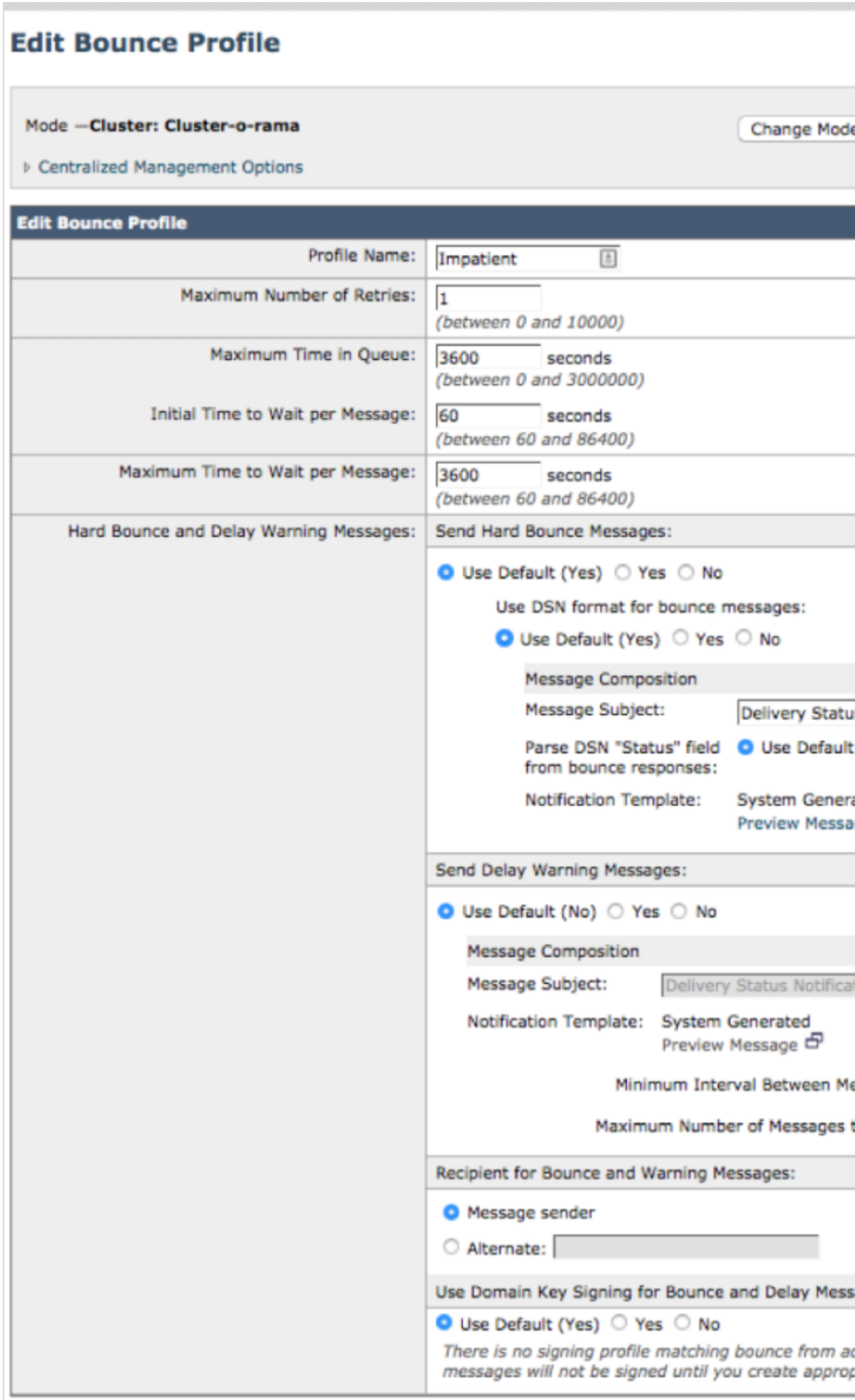
使用此内容过滤器的策略。

请注意，必须在您想要使用此过滤器的任何策略上引用和启用此内容过滤器。确保添加了内容过滤器所使用的自定义信头的策略中包含这些内容过滤器并且策略中的过滤器处于活动状态。

步骤 4：配置传感器的退回处理

为了使用最少的 ESA 系统资源，您应该将系统配置为在向传感器传送失败的情况下邮件退回也快速失败。

1. 提供目的主机接受的唯一域或子域中的密件抄送目标电子邮件地址。“备用邮件主机”传送操作应注意被定向到该服务器的邮件，无需为该电子邮件地址的域创建特定的 DNS 条目。在本示例中，我们会继续将“symbolic_ name.hosted.cisco.com”用于该域。
2. 创建退回配置文件以便让邮件退回快速失败。
    1. 转到网络 > 退回配置文件。
    2. 点击添加退回配置文件以创建新条目。
    3. 输入下图所示的值：



Edit Bounce Profile

Mode —Cluster: Cluster-o-rama Change Mode

Centralized Management Options

Edit Bounce Profile

Profile Name: Impatient

Maximum Number of Retries: 1
(between 0 and 10000)

Maximum Time in Queue: 3600 seconds
(between 0 and 3000000)

Initial Time to Wait per Message: 60 seconds
(between 60 and 86400)

Maximum Time to Wait per Message: 3600 seconds
(between 60 and 86400)

Hard Bounce and Delay Warning Messages:

Send Hard Bounce Messages:

Use Default (Yes) Yes No

Use DSN format for bounce messages:

Use Default (Yes) Yes No

Message Composition

Message Subject: Delivery Statu

Parse DSN "Status" field from bounce responses: Use Default

Notification Template: System Genera
Preview Messa

Send Delay Warning Messages:

Use Default (No) Yes No

Message Composition

Message Subject: Delivery Status Notifica

Notification Template: System Generated
Preview Message

Minimum Interval Between Me

Maximum Number of Messages t

Recipient for Bounce and Warning Messages:

Message sender

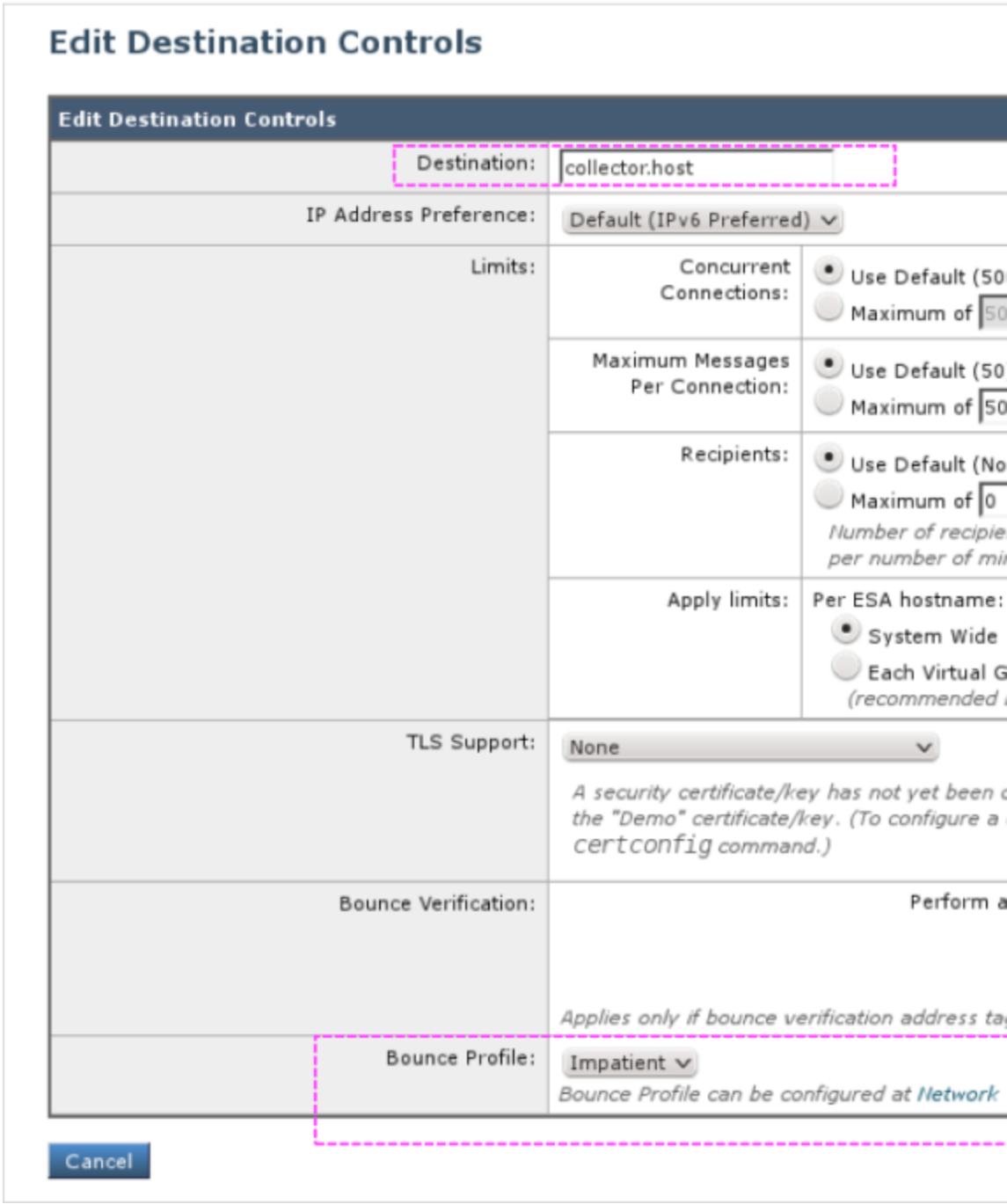
Alternate:

Use Domain Key Signing for Bounce and Delay Mess

Use Default (Yes) Yes No

There is no signing profile matching bounce from ac
messages will not be signed until you create approp

3. 为上述唯一的传感器域(在本示例中为“symbolic_name.hosted.cisco.com”)创建特定的“目标控制”，引用在上一步中创建的积极退回配置文件(在本示例中名为“Impatient”)：
   1. 转到邮件策略 > 目标控制。
   2. 输入下图所示的值：



4. 如果传感器不在受保护的网络内，而您想加密传入其中的邮件流，您可以将 TLS 支持选项更改为需要。思科 ESA 现在将安全地连接到远程传感器(在端口 25 上通过“STARTTLS”连接)。
5. 点击确认更改。

步骤 5：确认系统警报

转到系统管理 > 警报，确认系统和硬件警报会被发送到受到监控的地址，以防双重传送设置和配置存在任何问题。

步骤 6：考虑其他已加入白名单的电子邮件流

您可以设置防火墙规则，将发送邮件到思科 ESA 系统的上游 MTA 加入白名单。这通常使用主机访问表 (HAT) 实现，它会传送邮件并跳过任何后续的内容过滤器。假设您已如本文档中所述配置双重传送，此类邮件将无法复制到传感器，因为双重传送机制是内容过滤器的一部分，稍后在电子邮件管道中评估。

此问题的解决取决于入站电子邮件流的详情，但有一个可能采取的方法是使用内容过滤器而非主机访问表将入站流量加入白名单。您可以创建匹配发件人 IP 地址的内容过滤器规则，将副本发送到传感器（使用本文档中介绍的相同配置），然后触发邮件传送而不进行进一步过滤（使用跳过其余内容过滤器操作）。然后，您可以停用该发送方 IP 的相应 HAT 条目。

步骤 7：将警报服务器加入白名单

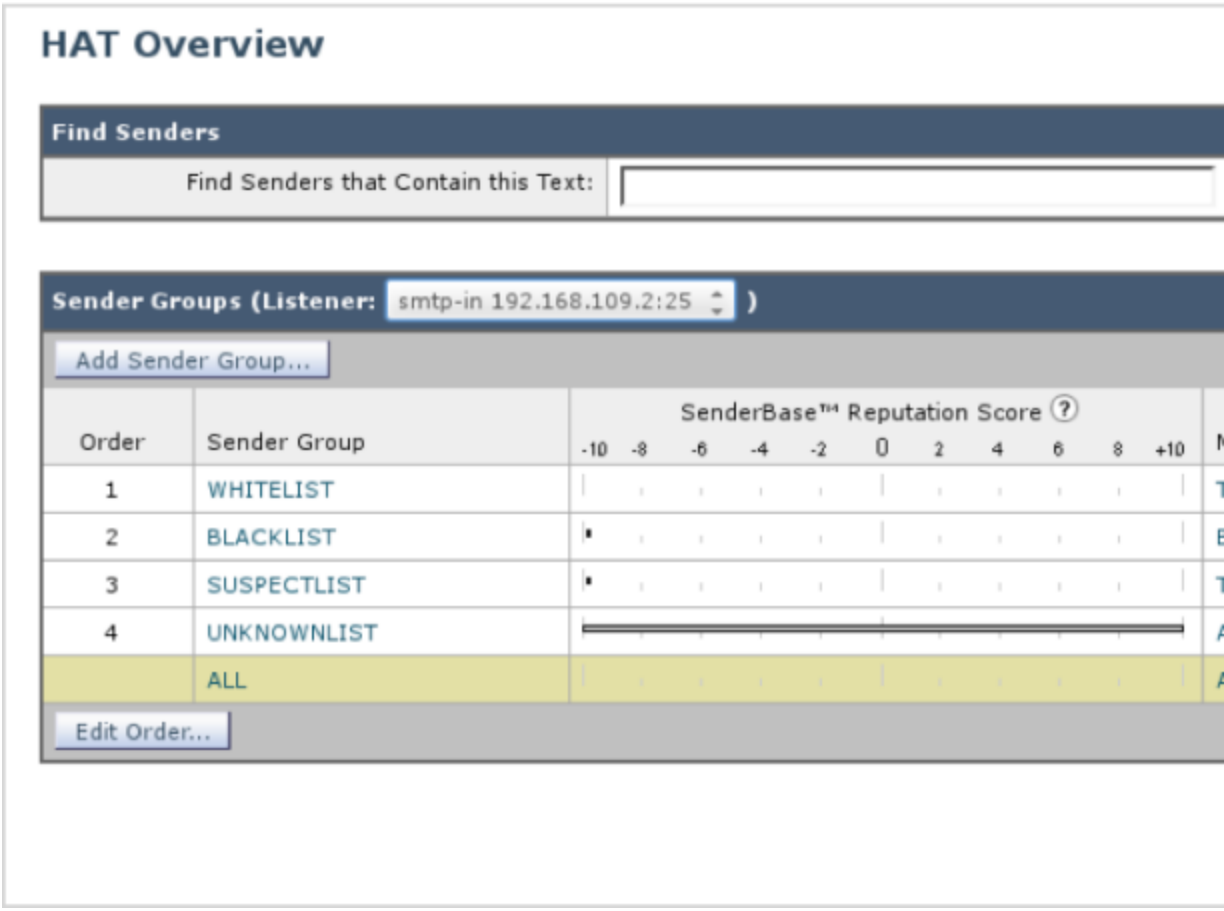
认为某封电子邮件可疑时，高级网络钓鱼防护 可以选择向管理员和/或可疑邮件的原始收件人发送电子邮件警报。

除了识别具有威胁的邮件之外，警报电子邮件还可能包含有关威胁类型或严重性的其他信息。如果是运营问题，通知服务器可能还会发出有关传感器和有关 高级网络钓鱼防护 服务整体运行状况的警报。鉴于这些警报的重要性和实用性，建议您将通知服务器加入白名单，确保系统不会阻止或隔离这些邮件。

例如，通知服务器发送的邮件有时可能包含原始邮件的部分内容。由于原始邮件可能包含垃圾邮件，或电子邮件过滤软件认为其在其他方面可疑，因此警报本身可能会意外地被视为威胁。

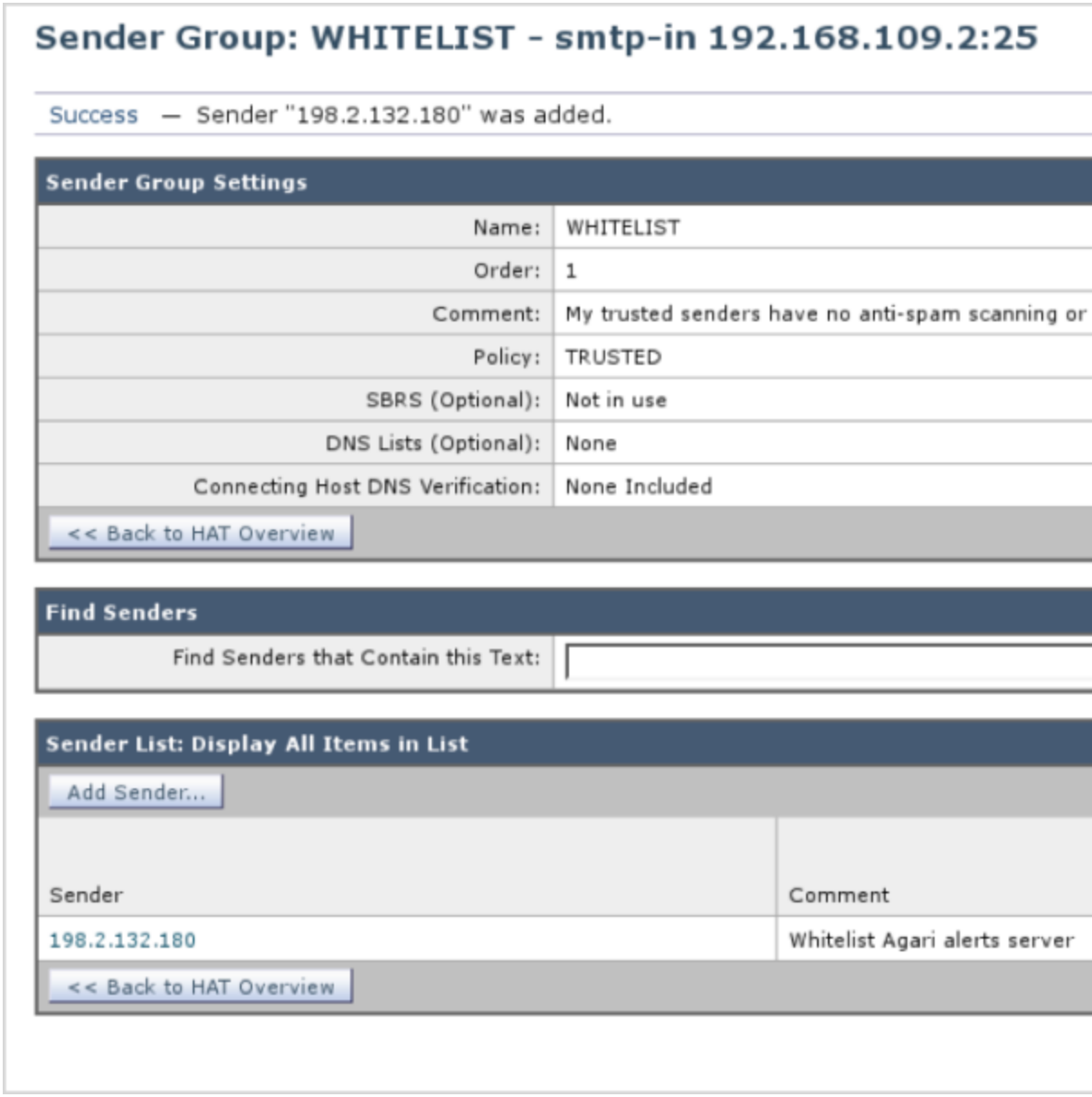
由此可见，将通知服务器加入白名单对于防止过滤软件中触发误报非常重要。如果存在中间过滤步骤（例如，其他中间 MTA 或其他过滤邮件的防网络钓鱼解决方案），也应对其进行配置，使其将通知服务器加入白名单。如有必要，销售工程和客户成功团队可以帮助配置白名单。

1. 转至邮件策略 > HAT 概览。此操作将打开“主机访问表”配置，您可通过它将警报服务器添加到可信发件人的列表中。该配置窗格将如下图所示：



您的配置可能与此存在各种不同，因此您可能需要根据您的特定环境调整这些说明。例如，您需要对每个入站侦听程序重复此配置，让所有已配置的入站侦听程序将警报服务器加入白名单。

2. 假设您已设置默认的发件人组，请点击白名单链接。如果您有备用发件人组，请使用映射到“可信”邮件流策略或等效策略的一个组。
3. 在发件人列表：显示列表中的所有项目部分中，点击添加发件人。
4. 在发件人字段中，输入警报服务器的 IP 地址：198.2.132.180。
5. 在注释字段中添加注释，例如“白名单警报服务器”。
6. 点击提交。
7. 在“发件人组”窗格中，确认此 IP 地址显示在发件人列表部分中：



8. 点击确认更改。

如上所示，警报服务器的 IP 地址是 198.2.132.180。此外还维护此地址的 DNS 条目，但在一般情况下，建议此白名单规则使用明确的 IP 地址。

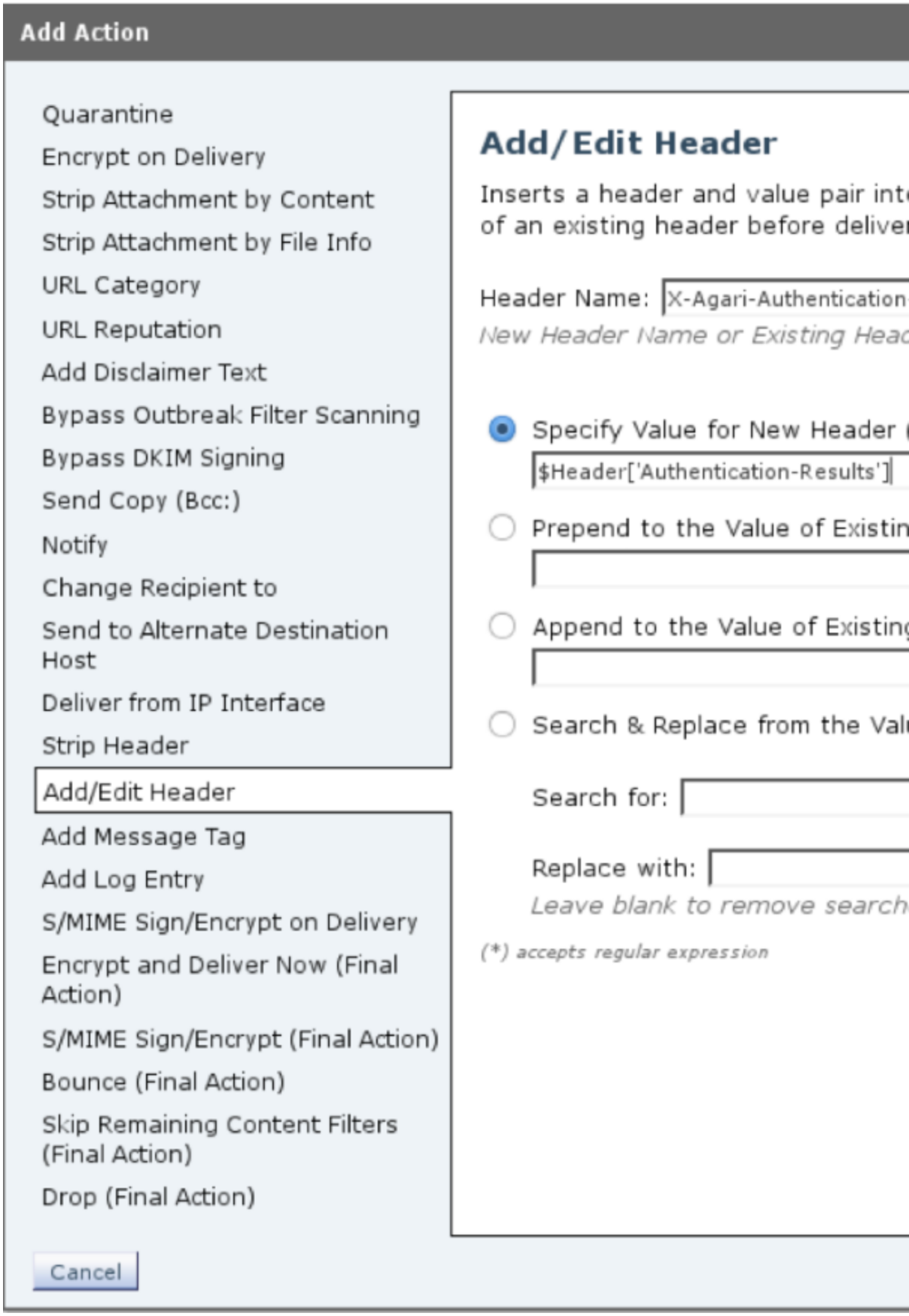
配置思科 ESA 以添加 X-Agari-Authentication-Results 信头

此部分仅适用于您配置的思科 ESA 系统是边界网关并且不准备用于双重传送的情况。如果您使用思科 ESA 系统生成双重传送流，则请勿使用此部分；而应按照上文说明操作，那些说明中包括添加 X-Agari-Authentication-Results 信头的正确方法。

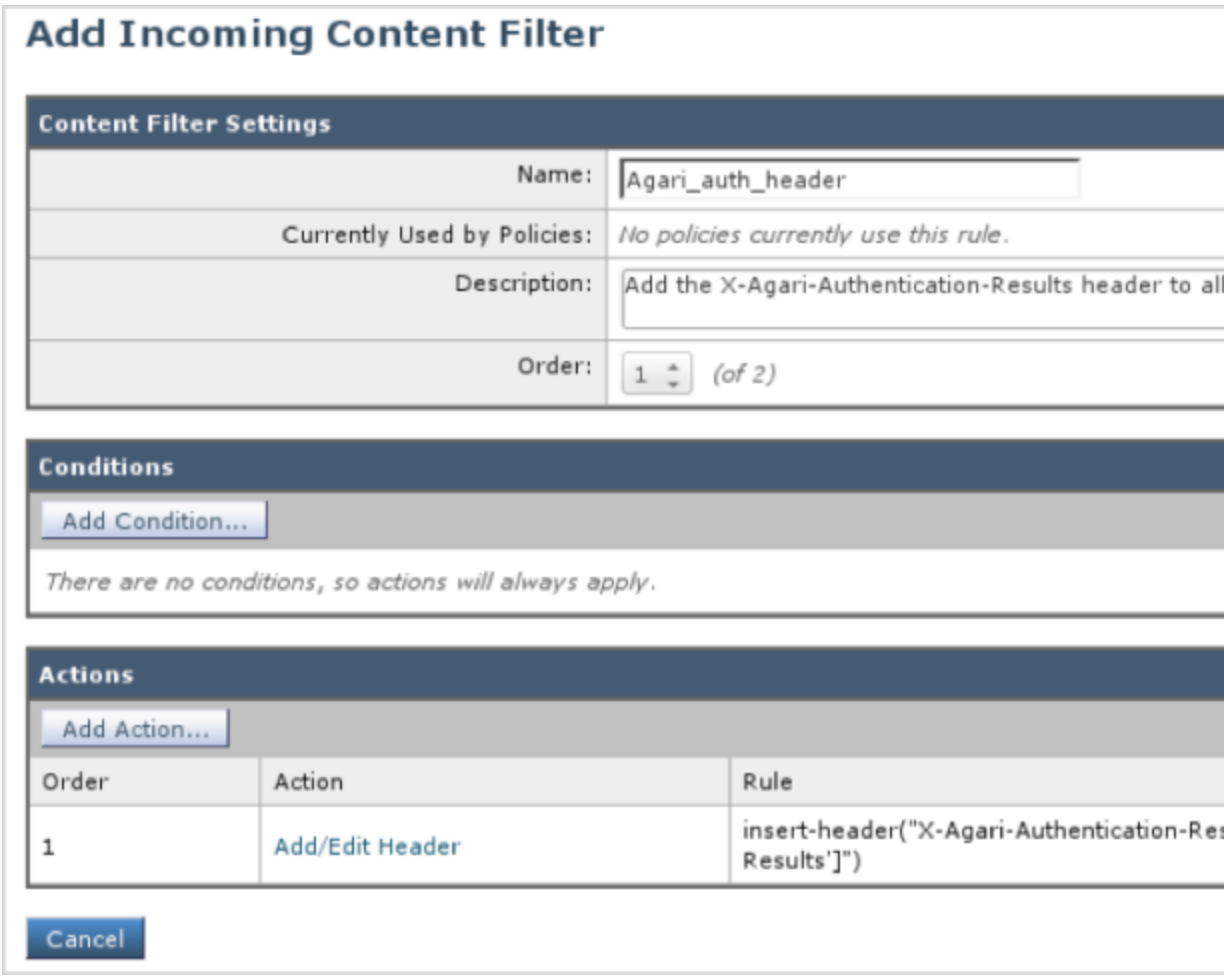
1. 以管理员身份登录思科 ESA。
2. 转到邮件策略 > 传入内容过滤器。

如果您的环境是集群环境，请在顶级或组级别(如果只希望操作影响一组特定的 ESA 实例)执行剩余步骤。请勿在计算机级别执行以下步骤。

3. 点击添加过滤器。
4. 将过滤器命名为“Agari_auth_header”。
5. 为过滤器添加合理的说明，例如：“向所有传入电子邮件添加 X-Agari-Authentication-Results 信头”。
6. 调整该过滤器的顺序，使其向所有传入电子邮件添加该信头。然后，应将该过滤器放在列表顶部或靠近顶部的位置：考虑此过滤器相对于现有过滤器的位置。
7. 该过滤器不需要任何条件；没有条件的过滤器默认匹配所有邮件。根据具体的环境，您可以将该过滤器与特定收件人或域的特定传入邮件策略关联(如下所述)。
8. 点击添加操作将操作与此过滤器关联。
9. 在“添加操作”窗口中，选择添加/编辑信头。
10. 使用界面指定过滤器，用于将两个新信头添加到邮件来指示原始收件人和原始发件人(这些信息不一定会正确反映在可见的邮件信头中)：
    - 信头名称：X-Agari-Original-From 信头数据：$EnvelopeFrom
    - 信头名称：X-Agari-Original-To 信头数据：$enveloperecipients
11. 使用界面指示该过滤器复制 Authentication-Results 信头：
    - 信头名称：X-Agari-Authentication-Results“指定新信头值”：$Header ['Authentication-Results']


Add Action
Quarantine
Encrypt on Delivery
Strip Attachment by Content
Strip Attachment by File Info
URL Category
URL Reputation
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Bypass DKIM Signing
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add/Edit Header
Add Message Tag
Add Log Entry
S/MIME Sign/Encrypt on Delivery
Encrypt and Deliver Now (Final Action)
S/MIME Sign/Encrypt (Final Action)
Bounce (Final Action)
Skip Remaining Content Filters (Final Action)
Drop (Final Action)
Cancel
Add/Edit Header
Inserts a header and value pair int
of an existing header before deliver
Header Name:
X-Agari-Authentication
New Header Name or Existing Head
Specify Value for New Header
$Header['Authentication-Results']
Prepend to the Value of Existin
Append to the Value of Existing
Search & Replace from the Val
Search for:
Replace with:
Leave blank to remove search
(*) accepts regular expression

12. 点击“确定”。完成后的传入内容过滤器将如下所示：



13. 点击提交。
14. 将过滤器与相应的传入邮件策略关联：
    1. 转到邮件策略 > 传入邮件策略。
    2. 在相应行的“内容过滤器”列中，编辑分配的内容过滤器以引用新创建的过滤器。在此过程中，您可能需要为该策略启用内容过滤器。修改后的策略行将与下图所示类似：

15. 点击确认更改。

您还应确认已在 ESA 上启用 SPF、DKIM 和任何其他身份验证机制(发件人 ID、DMARC 等)的评估，以便使用正确的数据填充“X-Agari-Authentication-Results”信头。

总结

完成上述步骤后，传感器将开始接收发送到您组织中的电子邮件的副本。在更改完全生效前，可能会有几分钟的短暂延迟。您可以通过在 https://appc.cisco.com 登录高级网络钓鱼防护 并导航至“管理”>“传感器”，查看已安装传感器的状态，以确认流量。

使用 高级网络钓鱼防护 章 3

高级网络钓鱼防护 完全配置好后，您将使用它来监控电子邮件流量并识别该流量中的任何问题。

工作流程

“概览”页面用于查找有问题的发件人和邮件。点击左侧的各攻击分类有助于您的调查。

通过“IP 地址”和“域”页面调查发件人，在两个页面间切换，识别可疑发件人及其发送的邮件。在必要时，您可能需要对一些内部域和合作伙伴域应用标签(请参阅下文“标记域”)。您会发现，所有分析页面最终都会转到“搜索邮件”结果，只不过是多条大路通罗马而已。

搜索和/或查看可疑邮件并：

- 查看评分
- 使用“邮件详细信息”页面的链接创建策略
- 发送对特定邮件的反馈
- 在主窗口中查看邮件并直接链接到该邮件

管理可疑邮件

确定一些可疑发件人和邮件后，接下来您需要创建策略(“管理”>“策略”)对邮件执行实际操作。

提示：在“邮件详细信息”页面中查看邮件时，您可以使用钟形图标创建策略；查看邮件搜索结果时，点击“创建策略”链接可以执行相同的操作。

您可以使用策略在可疑邮件到达时发送通知，甚至可以将邮件移到不同的邮箱/文件夹(如果已启用实施)。

有关创建策略的详细信息，请参阅"策略" 在本页 53。

分析传入电子邮件流量

思科高级网络钓鱼防护 可以帮助您洞察组织的传入电子邮件流量、电子邮件来源(IP、域)以及与这些邮件和发件人相关的风险。

“概览”页面以独特的方式直观显示组织入站电子邮件流量的风险概况。高级网络钓鱼防护 传感器收到的每封入站邮件都会获得一个可信度评分，并按照以下方面标绘在图中：

- **邮件真实性** - 邮件真的来自其声称的发件人吗？
- **域信誉** - 这是信誉良好的域吗(即，我与其之间是否建立了可靠的业务关系)？
- **发件人合法性** - 发件人 IP 地址经过 SenderBase 信誉评分 (SBRS) 评估后是否合法？

可信度评分

系统对传送至组织用户的每封入站邮件都会计算可信度评分。它回答了一个基本问题：我对这封邮件的可信度应该达到多少？ 可信度评分用于将邮件分成三组：“不可信”、“可疑”、“可信”。邮件按从 0 到 10 评分，其中 0 的可信度最低，10 最高。

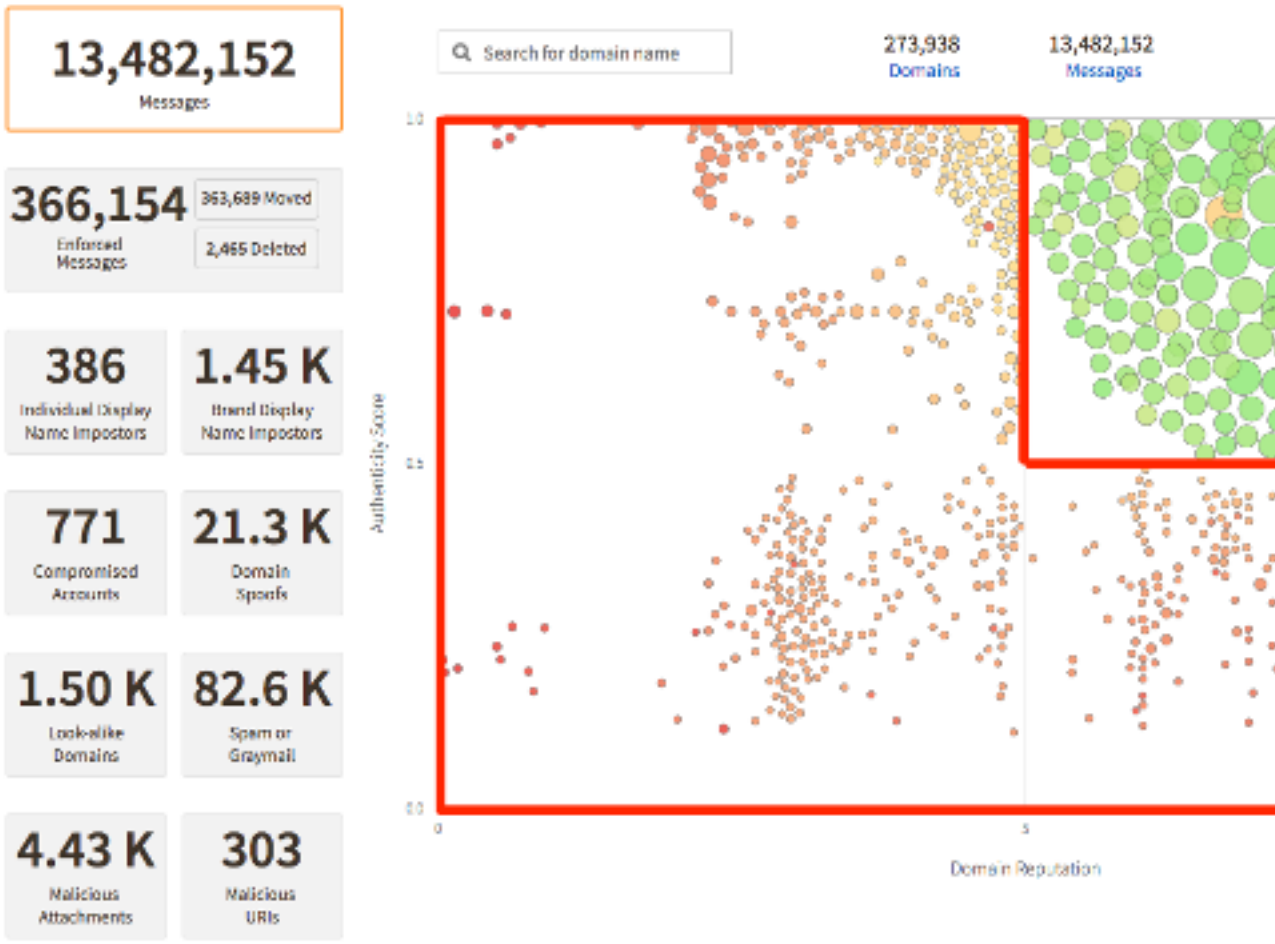
可信度评分会考虑域信誉评分、邮件真实性评分和每封邮件的特征。

邮件正文不是可信度评分的考虑因素。例外情况是，您启用了 URI 分析(请参阅启用附件和 URI 分析)后，从邮件正文提取的 URI 的评分为潜在恶意。

- 来自某个发件人的真实性评分高而域信誉评分低 = 可疑
- 来自某个发件人的真实性评分高且域信誉评分高 = 可信
- 来自某个发件人的真实性评分低而域信誉评分高 = 可疑，特别是在域经常正确进行身份验证的情况下
- 来自某个发件人的真实性评分低且域信誉评分低 = 通常属于群发邮件、零日域或相似的域

“概览”页面中的每个圆圈代表一个发送方域，这些圆圈的大小根据其在所选时段内发送的流量的相对数量来确定。右上部分的绿色圆圈代表信誉良好、数量多的正常邮件。您应该在这个象限中看到熟悉的发件人名称。每个象限中会显示排名靠前的 200 个域。将鼠标悬停在圆圈上可以查看来自该发送方域的邮件数。

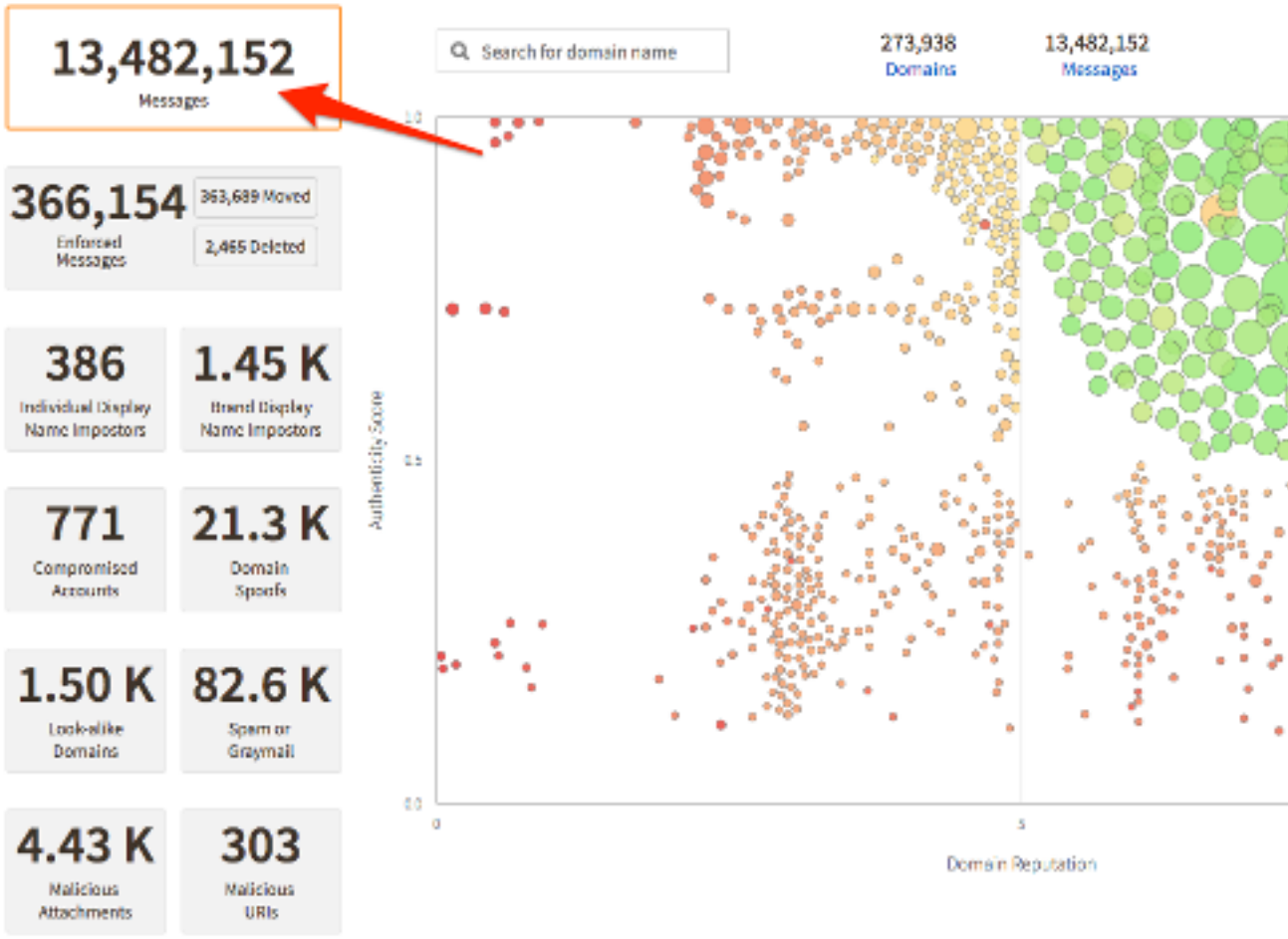
越不可信的发件人越靠下靠左。



“概览”页面中的象限

您可以点击象限显示左侧的任何小方框来过滤结果，将结果限制为仅一种基本攻击类型。此功能可用于快速识别可能有问题的邮件和发件人。

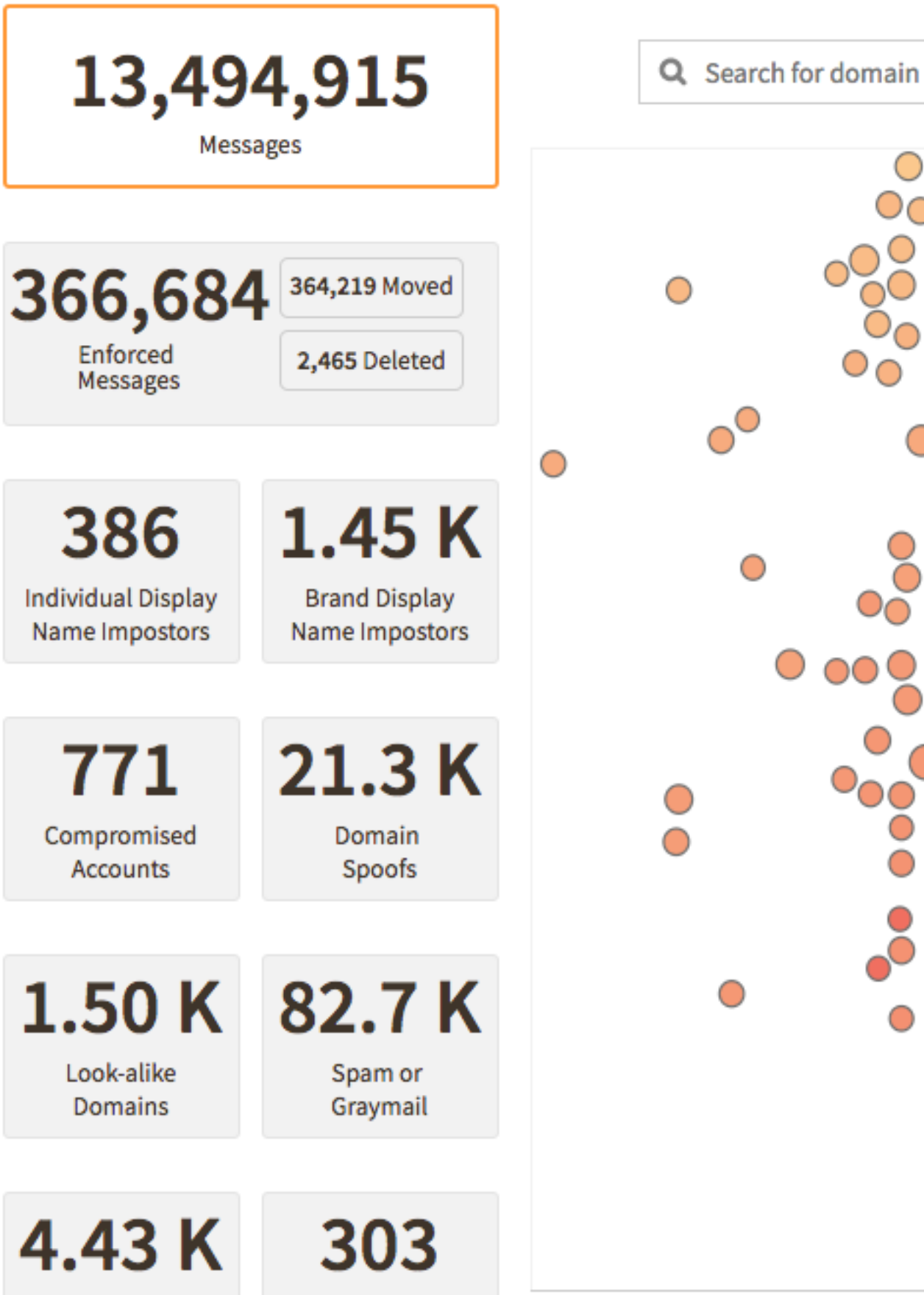
要返回到原始流量视图，请点击“邮件过滤器”。



邮件过滤器

放大

点击一个象限内部的空白处可放大该象限。这样应该更容易查看恶意发件人。将鼠标悬停在圆圈上可查看发送方域。例如：


13,494,915
Messages
Search for domain
366,684
Enforced Messages
364,219 Moved
2,465 Deleted
386
Individual Display Name Impostors
1.45 K
Brand Display Name Impostors
771
Compromised Accounts
21.3 K
Domain Spoofs
1.50 K
Look-alike Domains
82.7 K
Spam or Graymail
4.43 K
Malicious Attachments
303
Malicious URIs

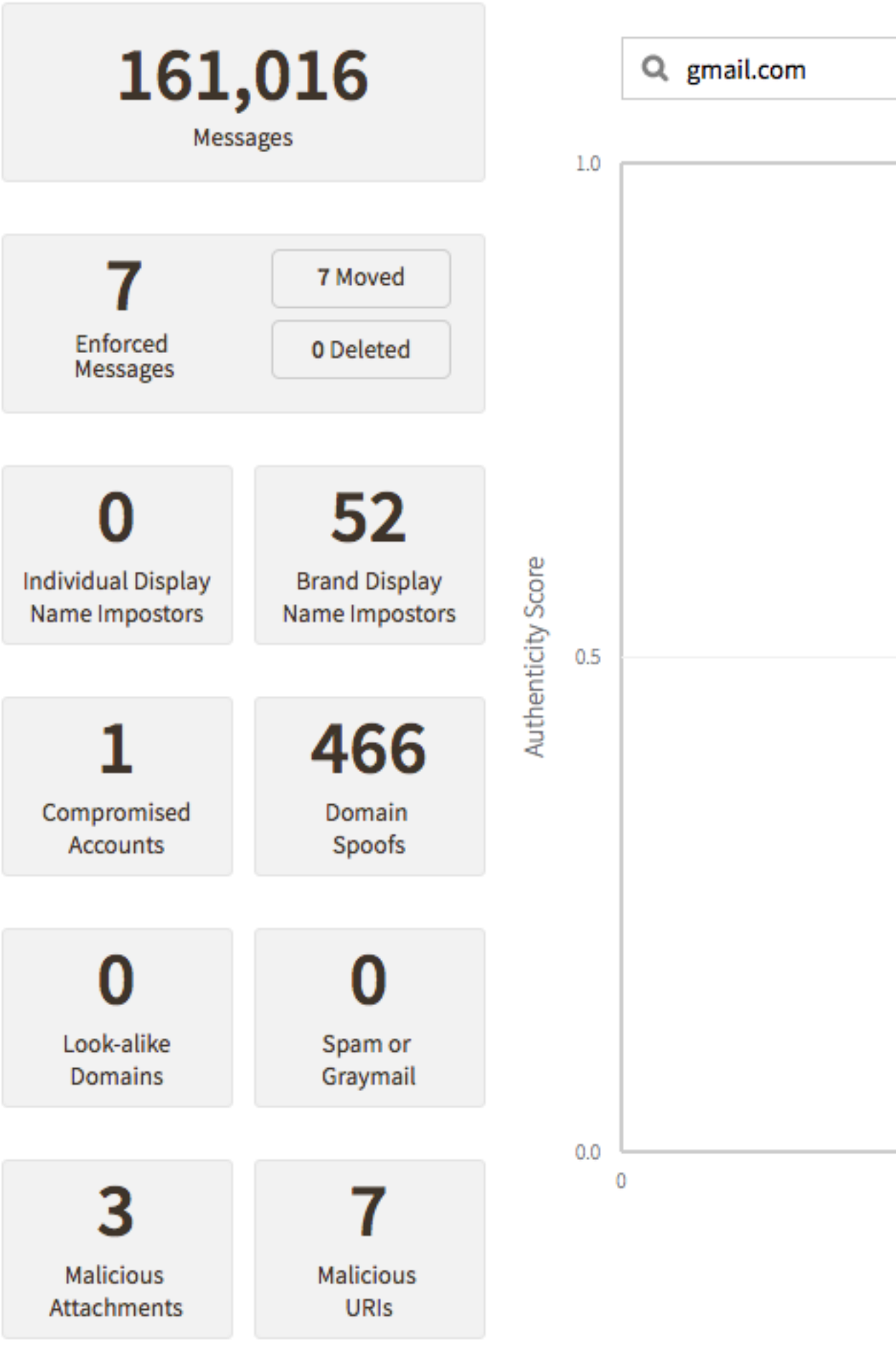
放大的象限

再次点击空白处可缩小。

快速搜索域

您还可以使用直观的主页面上的搜索框对您从特定域接收的邮件的真实性进行快速分类。

例如，在搜索框中键入“gmail.com”。您可能会看到如下所示的模式：


161,016
Messages
7
Enforced Messages
7 Moved
0 Deleted
0
Individual Display Name Impostors
52
Brand Display Name Impostors
1
Compromised Accounts
466
Domain Spoofs
0
Look-alike Domains
0
Spam or Graymail
3
Malicious Attachments
7
Malicious URIs
gmail.com
Authenticity Score
1.0
0.5
0.0
0

搜索来自域 gmail.com 的邮件

这表示 高级网络钓鱼防护 在过去 7 天中已分析来自 gmail.com 域的 161,016 封合法邮件；将鼠标悬停在较小的圆圈上将显示，有 818 封邮件可能有必要进行进一步调查，因为它们的真实性评分较低。

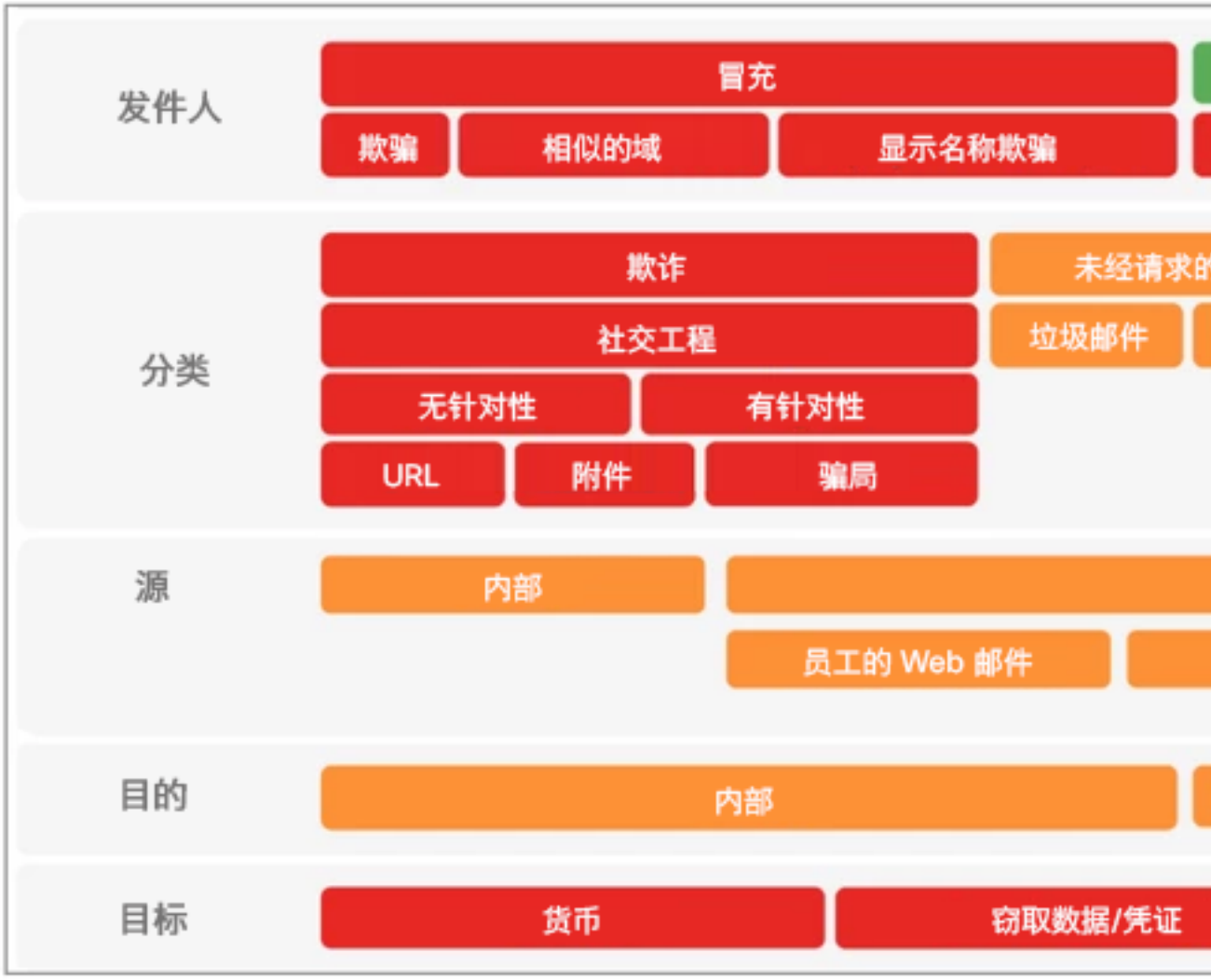
清除搜索框将返回到原始视图。

攻击分类

此主题说明了电子邮件攻击的不同类型。

攻击分类法

不可信(按照邮件可信度评分而定)的邮件将由 高级网络钓鱼防护 归入下图所示的攻击分类法的一个或多个攻击类中。



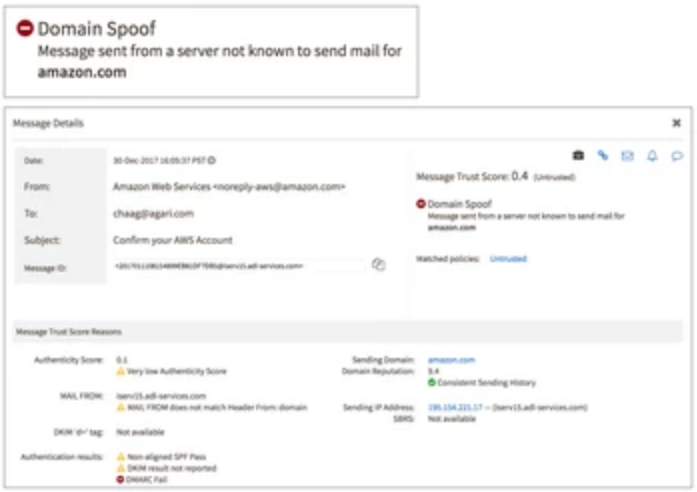
攻击分类的分类法

攻击分类将显示在“邮件详细信息”视图中，并可用于搜索和策略。

分类法攻击分类将在下面详细说明。

域欺骗

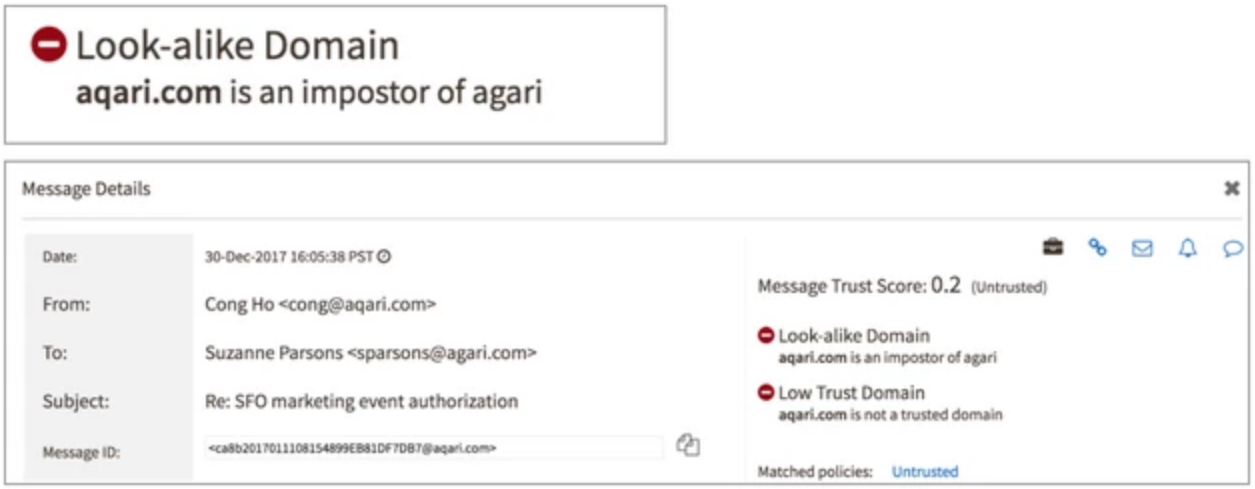
域欺骗是一种邮件，它声称是由信誉评分高的域所发送，但 高级网络钓鱼防护 发现其并非来自该域的真正发送源。



域欺骗示例

相似的域

相似的域攻击是指某个域企图看起来像某个非常可信的知名域(比如您的一个内部域或合作伙伴域)的情况。

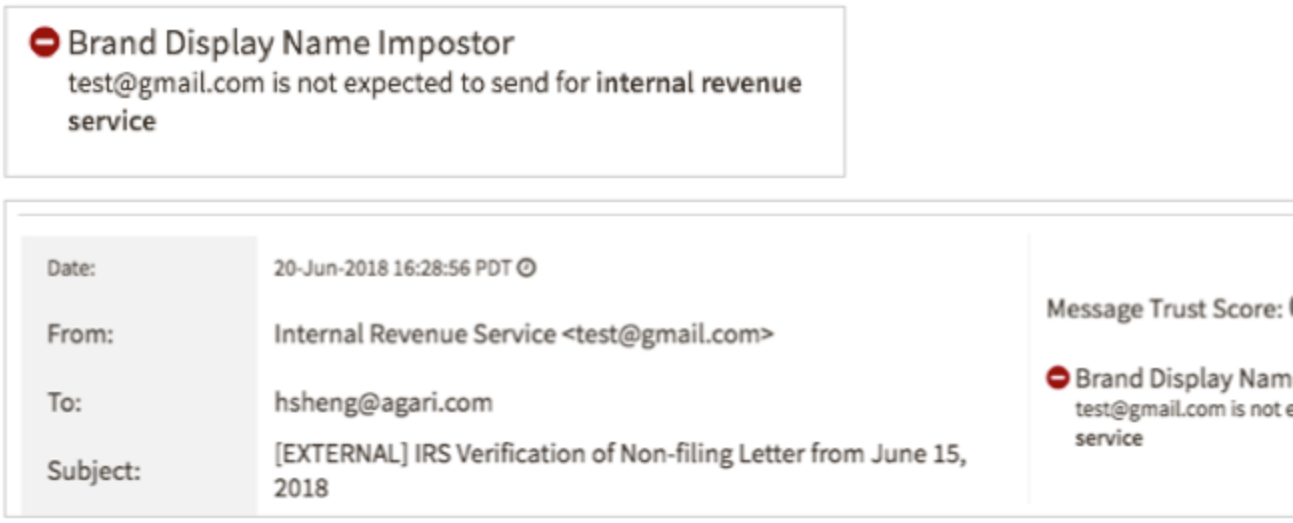


相似的域示例

显示名称冒充

显示名称冒充是指“发件人”字段的显示名称部分被改得像某个知名品牌或另一个人的情况。显示名称欺骗往往与相似的域或受感染帐户等其他攻击类型一起使用。在 高级网络钓鱼防护 中，显示名称冒充分为两类：个人显示名称冒充和品牌显示名称冒充。

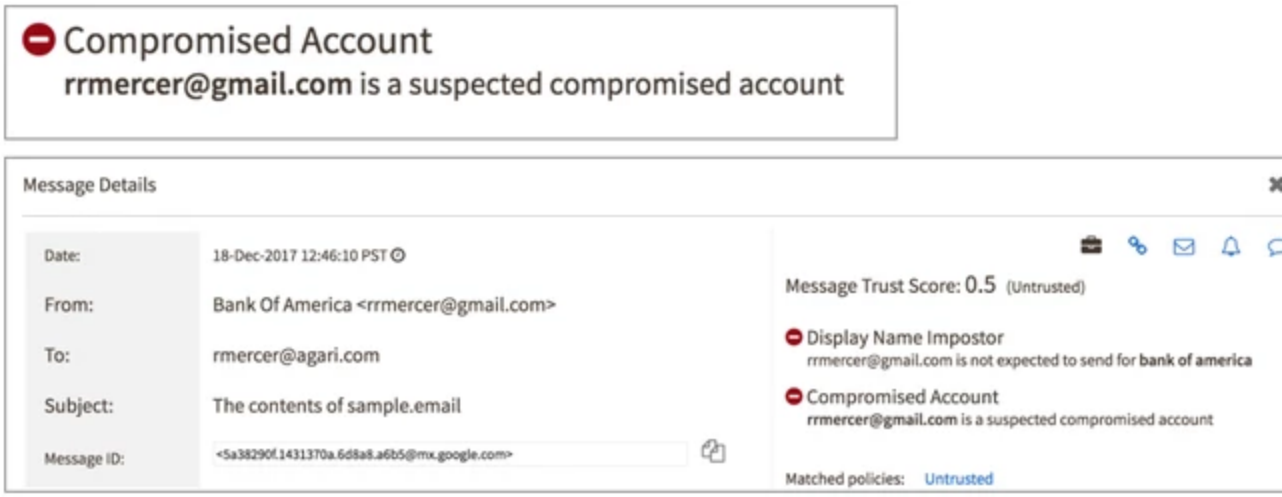
个人显示名称冒充示例



品牌显示名称冒充示例

受感染帐户(帐户接管)

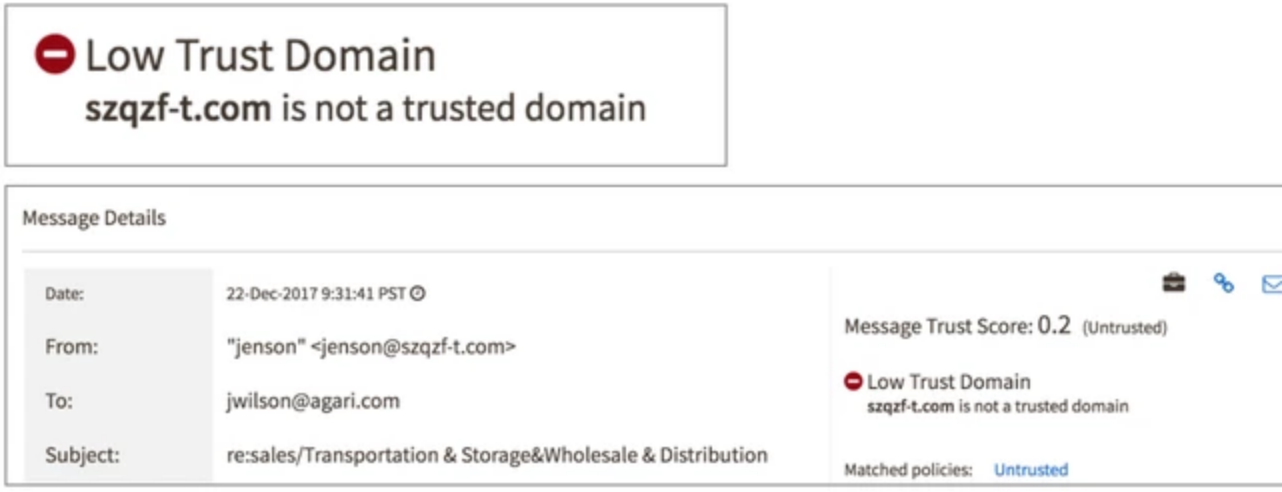
受感染帐户是属于真正的人/用户、但已被恶意攻击者接管并用于恶意用途的帐户。当 高级网络钓鱼防护 发现帐户接管迹象时，我们会将其归类为来自受感染帐户的邮件。



受感染帐户示例

低可信度域

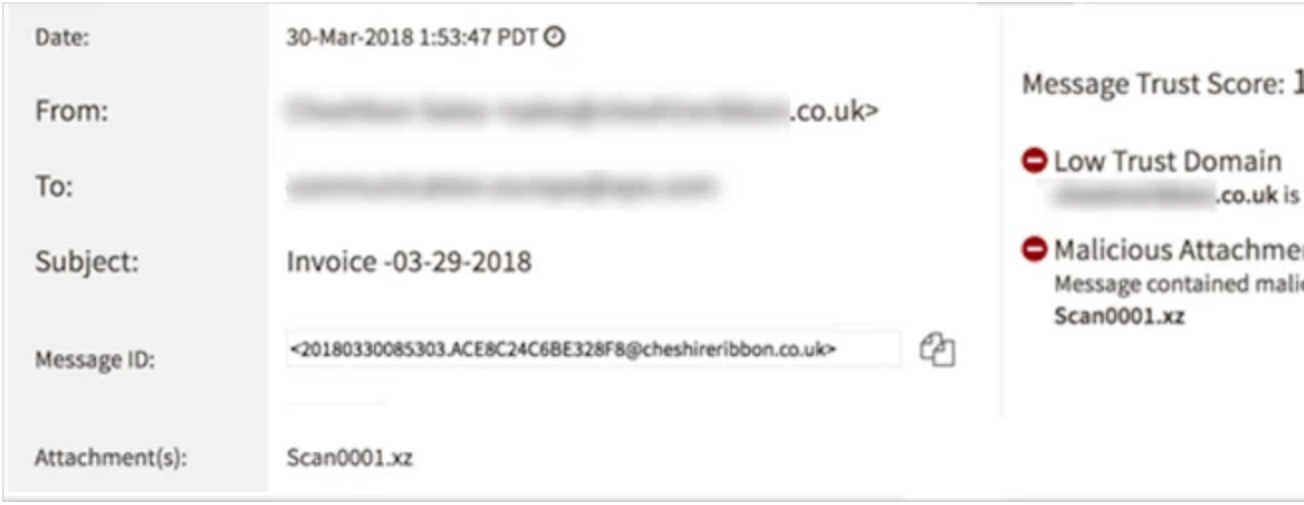
除了前文提及的发件人分类，高级网络钓鱼防护 还对来自低可信度域的邮件直接归类。有许多邮件适合分类法的欺诈电子邮件和未经请求的电子邮件(垃圾邮件和灰色邮件)这两个分类，这些邮件来自不应该受到信任的域(无论发件人分类如何)。



低可信度域示例

恶意附件

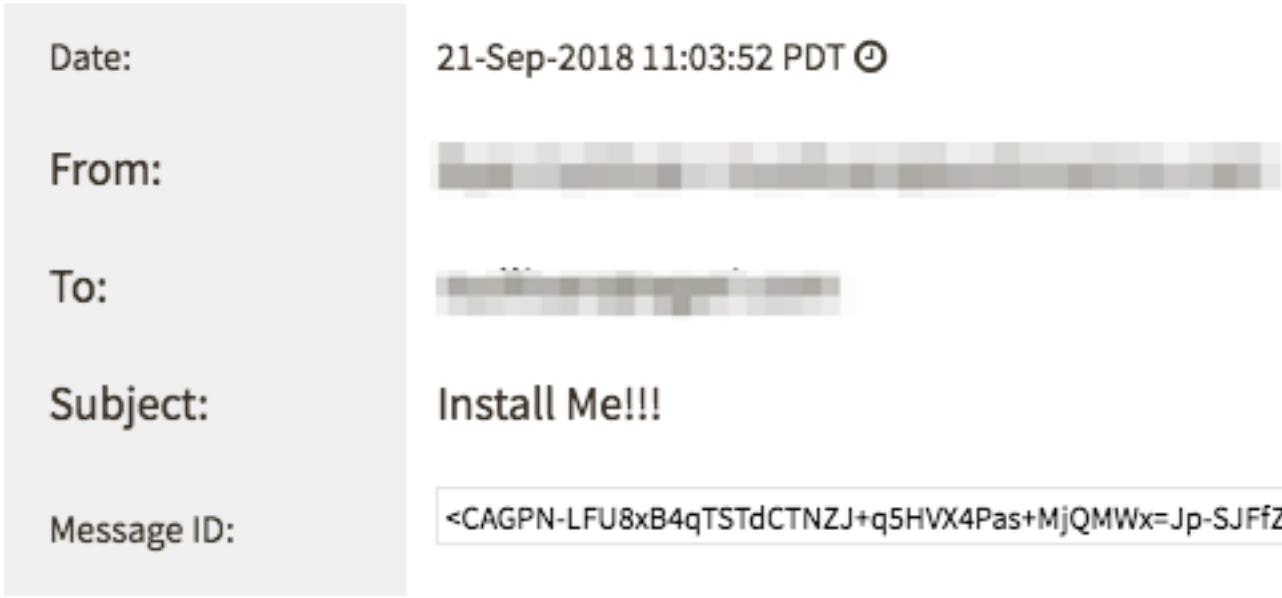
如果启用了附件扫描，高级网络钓鱼防护 会在附件可能属于恶意时通知您。



恶意附件示例

可能的恶意 URI

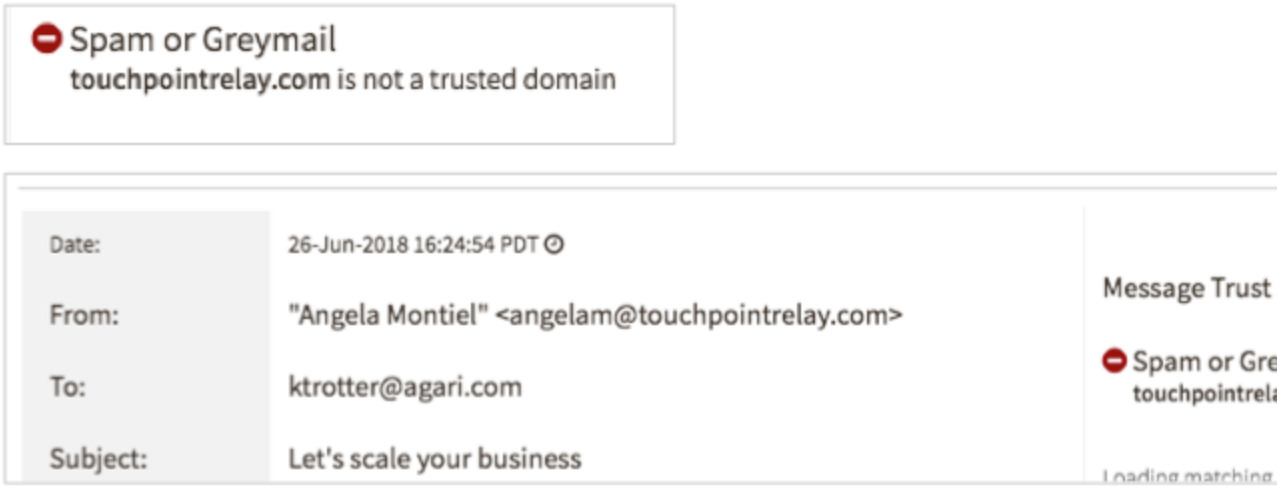
如果启用了 URI 扫描，高级网络钓鱼防护 将告知您在可能是恶意的邮件正文中找到 URI 时的情况。



恶意 URI 示例

垃圾邮件或灰色邮件

除了识别恶意邮件的发件人分类之外，高级网络钓鱼防护 还会对不一定恶意的邮件进行分类，但代表不需要或未经请求的电子邮件。不应信任属于垃圾邮件或灰色邮件类的邮件(无论其他发件人分类为何)。



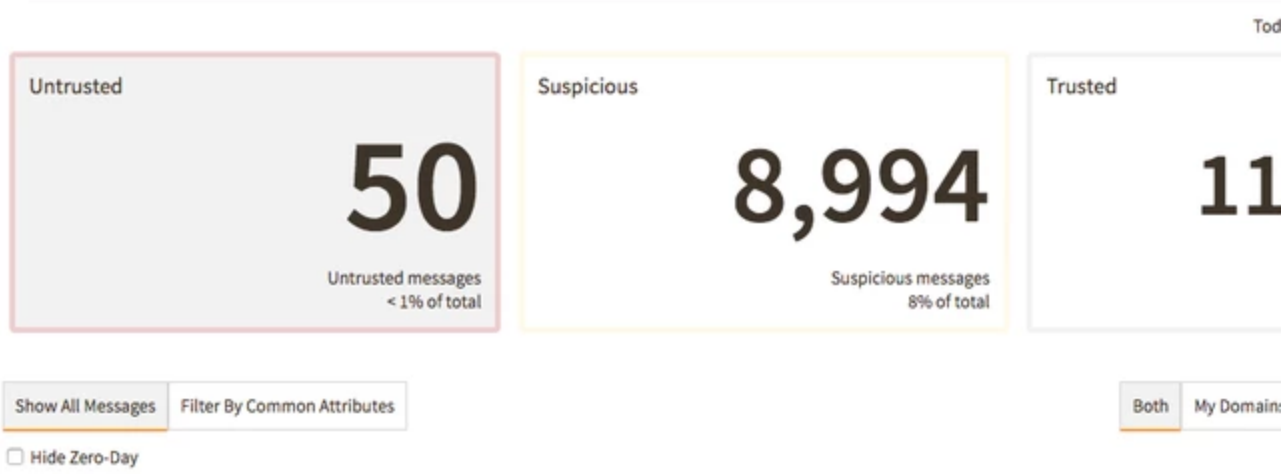
垃圾邮件或灰色邮件示例

邮件

可以通过多种方式查看通过 思科高级网络钓鱼防护 分析的邮件以及有关这些邮件的数据和威胁分析。除了实时控制板视图(分析 > 控制板、实时选项卡)之外，其他两个有用的视图分别是邮件列表(分析 > 邮件)和邮件搜索(分析 > 搜索邮件)。

查看邮件

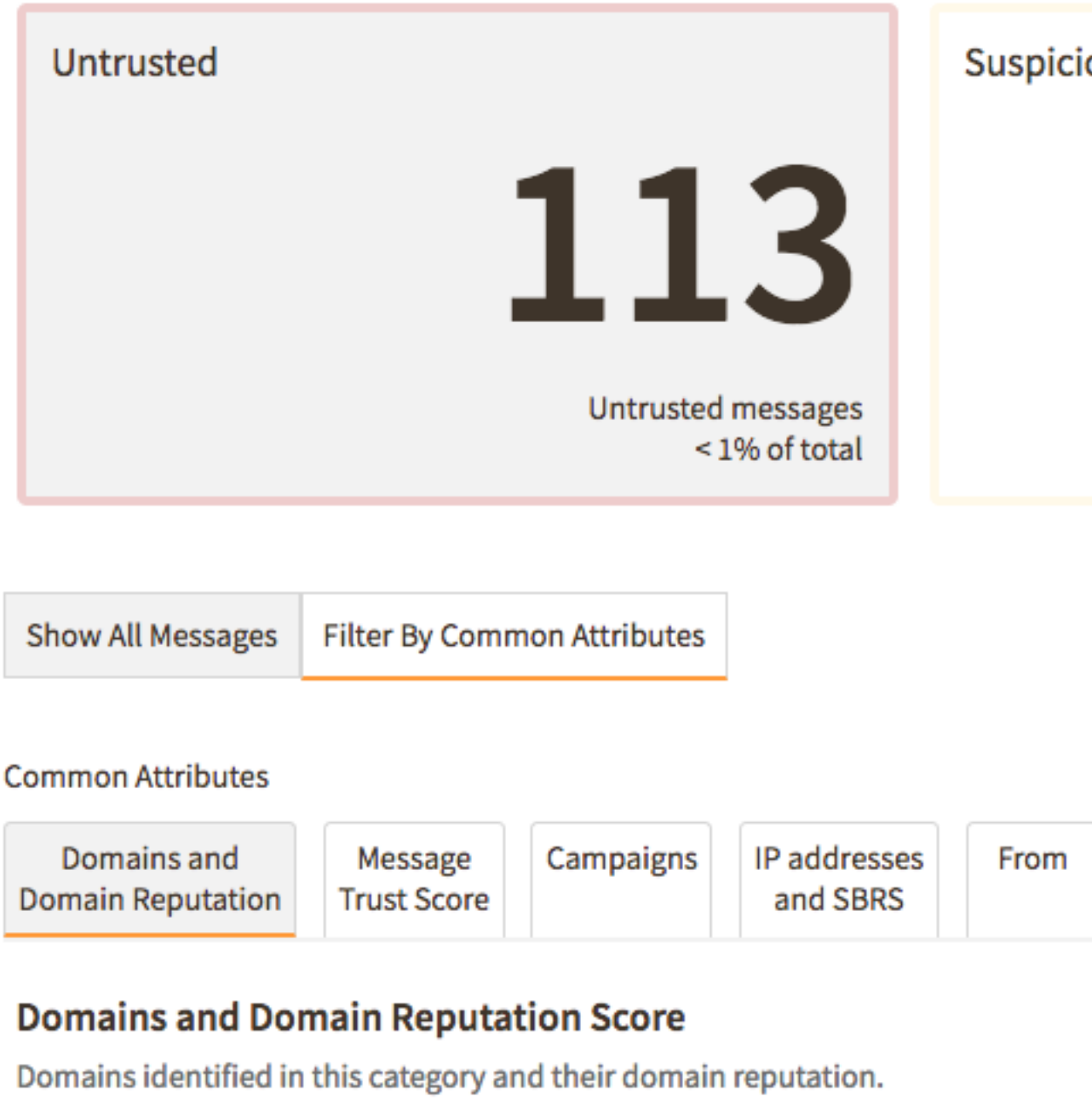
“概览”页面以交互式的方式直观显示欺骗、名称冒充者、相似域和正常邮件，而“分析”>“邮件”页面则提供更多操作视图来帮助您了解数据。



邮件页面摘要计数

邮件分为三个类别：“不可信”、“可疑”和“可信”。您可以点击对应的文本框选择该类别。

要进一步深入了解，请点击“按通用属性过滤”：



按通用属性过滤

默认视图按域对不可信邮件排序。您也可以点击其他选项卡进行排序以显示：

- **邮件可信度评分** - 按可信度评分来看，这些不可信邮件是如何分布的？
- **攻击活动** - 这些不可信邮件中有多少来自一个发件人并且主题相同？
- **IP 地址/SBRS** - 在评为不可信的所有邮件中，这些邮件的哪些发送方 IP 地址排名靠前？这些 IP 的信誉评分是多少？
- **发件人/收件人/主题/日期** - 对我来说，风险最大的发件人是谁？对我来说，风险最大的收件人是谁？我是否在某个特定日期受到攻击？

查看邮件详细信息

您通常希望查看不可信发件人(由红色圆圈表示)发送的邮件的详细信息。

1. 点击一个红色圆圈可查看该发件人发送的邮件的列表。来自该发件人的邮件显示于搜索邮件结果中。您可以进行过滤，以便进一步限制列表。
2. 点击邮件可查看邮件详细信息。

“邮件详细信息”窗格

“邮件详细信息”页面显示有关邮件的信息，包括：

- 信头和评分(以及收到评分的原因)
- 邮件的方向性(入站、出站或内部)
- 邮件匹配的策略(如果有)
- 是否已实施邮件(如果已启用实施)

内部和出站邮件不显示“邮件可信度评分原因”部分。

请记住，高级网络钓鱼防护 不跟踪邮件的正文。

不过，打开“发送方域”和“发送方 IP 地址”的交叉链接通常更有用。

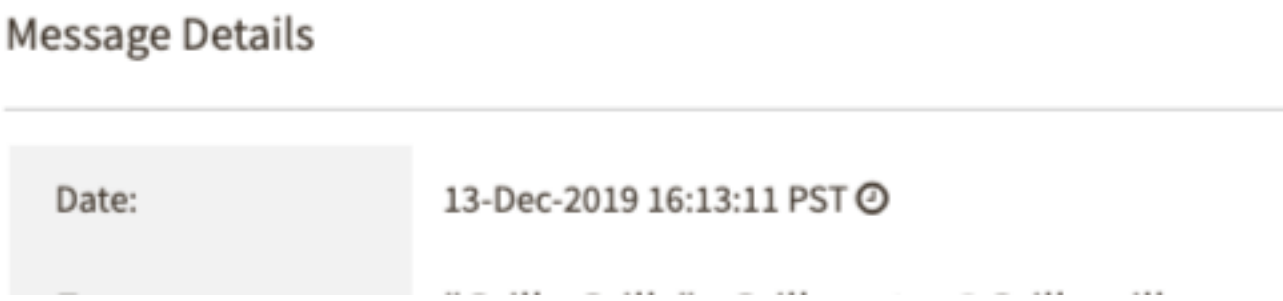
- “发送方域”链接可以回答以下问题：此域多长时间向我的组织中发送一次邮件？从多少个 IP 地址发送？其中大部分邮件是合法的吗？
- “发送方 IP 地址”链接可以回答以下问题：此 IP 地址还会为哪些其他域向我的组织发送邮件？该 IP 是否信誉良好？它为几个域还是许多域发送邮件？

在“邮件详细信息”页面右上角，您可以点击：

- 主窗口中的邮件详细信息链接图标 ( ) 以查看邮件详细信息(通过一个 URL 直接链接到此视图)。
- 信头图标 ( ) 以查看邮件中的所有信头。
- 邮件图标 ( ) 以将邮件详细信息视图发送给同事。
- 铃状图标 ( ) 以创建条件与此邮件匹配的策略。有关创建策略的详细信息，请参阅"创建策略" 在本页 55。
- 邮件反馈图标 ( ) 以提供有关邮件评分的反馈。有关详细信息，请参阅发送邮件反馈。

将邮件发送给事件响应团队

如果您还订用了 网络钓鱼响应，可以将您在 高级网络钓鱼防护 中查看的邮件发送给 网络钓鱼响应，以便 网络钓鱼响应 和您的安全团队进一步调查。当您拥有 网络钓鱼响应 并查看邮件详细信息(请参阅"查看邮件详细信息" 向上)时，您将在邮件的左上角看到一个额外的图标：



邮件详细信息页面右上角的“发送到 Agari 网络钓鱼响应”按钮。

1. 查看单个邮件。有关信息，请参阅"查看邮件详细信息" 上一页。
2. 点击右上角的发送到 Agari 网络钓鱼响应 按钮 (A)。
3. 点击发送。

以下两种情况之一将会出现：

- 如果确定此邮件与 网络钓鱼响应 中的当前开放调查相关，此邮件将添加到此调查中以及调查分析和分类中。
- 如果确定此邮件与 网络钓鱼响应 中现有的开放调查不相关，系统将会打开一个包含此邮件的新调查，并在 网络钓鱼响应 中对此调查发起自动分析和分类。

邮件搜索

高级网络钓鱼防护 包括一种非常强大、非常详细的邮件搜索功能。您不仅可以搜索特定的邮件数据，还可以搜索由 高级网络钓鱼防护 识别的邮件特征。

高级网络钓鱼防护 的一个优点是，邮件搜索不只是白纸一张，也不只是定义每个搜索条件的起点。在很多地方，都可以跳转至预定义了一个或多个搜索条件的邮件搜索结果页面。例如，如果您在控制板开始，点击“域欺骗”，然后点击“显示邮件”，就会转到预定义了以下条件的邮件搜索结果页面：

- 日期范围：您在控制板页面上设置的范围
- 攻击类型：域欺骗
- 可信度评分范围：0.0 到 5.1

同样，如果转到“分析”>“邮件”页面，请点击“可疑邮件”，点击常见属性(例如“发件人”)，然后点击列表中的数字，然后您将转到邮件搜索结果页面，从中可看到在指定的时间段内以及可疑邮件的可信度评分范围内来自该地址的所有邮件的列表。

这些快捷方式非常方便，但无论您从头开始还是从诸多快捷方式中任选一种，都能找到优化搜索结果。

搜索已运行时，用于搜索的字段显示橙色轮廓。

本主题介绍“搜索邮件”页面上的所有字段。

搜索字段	说明
发件人、收	当 高级网络钓鱼防护 注入邮件时，系统将从邮件信头中的相应字段收集这些信息。输入所有或部分电子邮件地址或主题行。对这些字段的搜索是部

搜索字段	说明
件人、回复收件人、主题	分匹配的，不区分大小写。例如，如果在“主题”字段中输入“pens”，则包含“Shop My Etsy Pens Store”、“That's too expensive for me”和“Please buy some pens from Amazon”等主题的邮件全会被找到。 ❑限制在 100 个字符以内。
附件	仅当在组织设置(请参阅组织设置)中启用附件扫描时，此字段才可用，并包含 5 个选项： • 有任何附件 - 查找带任何附件的任何邮件。 • 可能有恶意附件 - 查找至少有一个附件被 高级网络钓鱼防护 确定为潜在恶意附件的任何邮件。 • 有附件名称 - 查找附件文件名中包含此字段中输入的全部或部分内容的邮件。与其他文本搜索字段相似，这是部分匹配的，不区分大小写。 • 有附件文件名扩展名 - 查找附件文件名有任何输入的扩展名的邮件。文件名扩展名是文件名最右边句点之后的部分。输入一个或多个扩展名，用逗号分隔。与其他文本搜索字段相似，这是部分匹配的，不区分大小写。例如，如果您输入 PROP，系统将查找名为 system.properties 的文件。 • 有附件散列值 - 查找与输入的散列值匹配的邮件。散列值由加密算法生成，用于唯一标识文件的内容。如果对文件进行任何更改，则为该文件生成的散列值会发生变化，而且通常变化显著，因此通过比较原始散列值和当前散列值，很容易确定文件是否已更改。这是完全匹配的，区分大小写。 ❑限制在 100 个字符以内。
接收日期范围	这将定义搜索的开始和结束日期(包含两端)。 • 开始日期不能早于当前日期前 60 天。(高级网络钓鱼防护 会清除 60 天之前的邮件数据。) • 结束日期不能晚于当前日期。
可信度评分范围	这将定义搜索中将查找的邮件可信度评分的上限和下限，包括您选择的值。拖动上下限滑块以更改范围。
真实性评分范围	这将定义搜索中将查找的邮件真实性评分的上限和下限，包括您选择的值。拖动上下限滑块以更改范围。
匹配的策略	这将定义邮件要被搜索到而必须已实施的单个策略。可从中选择的策略列表包括 高级网络钓鱼防护 中的所有策略：已启用(和活动)、已禁用和按需策略(请参阅按需策略)。
实施	这定义了邮件是否已实施任何策略，以及如何实施。从下方选择一个选项： • 所有邮件(默认) - 以任何方式实施的邮件。 • 待处理 - 与已定义实施的策略匹配但尚未执行实施的邮件。 • 已实施 - 策略已实施的邮件。还可以选择实施的子类别：

搜索字段	说明
	• 已移动(到任何文件夹) • 已移至收件箱 • 已删除 • 未实施 - 与包含实施操作的策略匹配但策略未实施该操作的邮件。(此选项可用于确定哪些邮件与策略匹配，以查看该策略是否在启用任何移动或删除邮件的实施操作之前捕捉符合的邮件，或用于发现策略实施失败的情况。)
邮件 ID	在此字段中输入单个邮件 ID，以搜索 高级网络钓鱼防护 中与邮件 ID 匹配的特定邮件。 ❑限制在 100 个字符以内。
方向	这定义了邮件的方向性。在字段中点击以从中选择一个或多个方向： • 入站 - 从组织外部的某个地方发送到贵组织的邮件。在“方向”列中，入站邮件以 ★图标表示。 • 出站 - 从贵组织发送到组织外部的某个地方的邮件。在“方向”列中，入站邮件以 ✦图标表示。 • 内部 - 在您的组织内开始和结束的邮件。在“方向”列中，入站邮件以 ” 图标表示。
攻击类型	在字段中点击以选择一个或多个攻击类型。系统将在搜索中查找与任何选定的攻击类型匹配的邮件。
域信誉范围	这将定义搜索中将查找的邮件域信誉范围的上限和下限，包括您选择的值。拖动上下限滑块以更改范围。
发送域	输入一个或多个发件人域，以逗号分隔。系统将在搜索中查找与任何域匹配的邮件。 ❑限制在 100 个字符以内。
域标签	在字段中点击以选择一个或多个域标签。系统将在搜索中查找与任何选定域标签匹配的邮件。
主机名	输入一个指向 IP 地址的 PTR 主机名。系统将在搜索中查找包含该主机名的邮件。 ❑限制在 100 个字符以内。
SBRS 范围	这将定义搜索中将查找的邮件 SenderBase 信誉评分 (SBRS) 范围的上限和下限，包括您选择的值。拖动上下限滑块以更改范围。
IP 地址	输入单个 IP 地址或 CDR。系统将在搜索中查找包含该 IP 地址的邮件。 ❑限制在 100 个字符以内。

搜索邮件

“搜索邮件”页面用于搜索和过滤传入邮件。您可以通过菜单或通过点击域详细信息或 IP 地址详细信息页面中的邮件数直接转到“分析”>“搜索邮件”页面。

1. 转至分析 > 搜索邮件。
2. 输入搜索条件。有关每个搜索字段的详细信息，请参阅"邮件搜索" 在本页 45。
3. 点击搜索。

域和 IP 地址

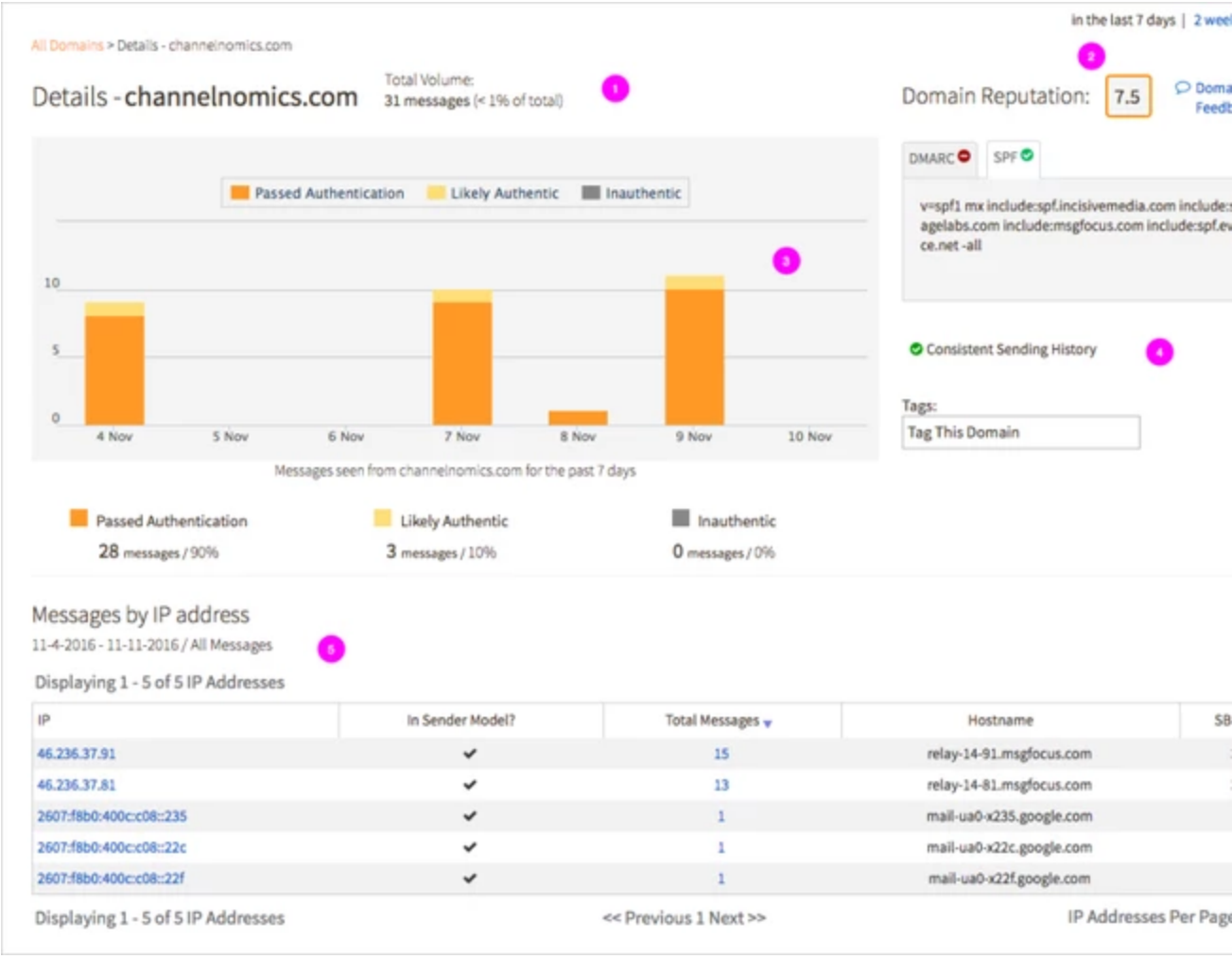
在“分析”菜单中，您可以查看发送方域和 IP 地址的列表(分析 > 域和分析 > IP 地址)。两个页面的功能相似，而且您在调查传入流量时将在两个页面间切换。当您点击列表中的 IP 地址或域时，您可以看到该项目的“详细信息”页面。对于 IP 地址，“详细信息”页面显示有关该 IP 的信息，包括从该 IP 地址发送到您组织的域的列表，以及每个域发送的邮件的链接。对于域，“详细信息”页面显示有关该域的信息，包括从该域发送到您组织的 IP 地址的列表，以及发送的邮件。

来回查看 IP 地址和域以及来自各 IP 地址和域的相关邮件是深入了解详细信息并分析传入流量的有效方法。

查看域详细信息

在 高级网络钓鱼防护 的发件人建模功能中，域与 IP 地址的关系是一个关键组成部分，而“域详细信息”页面正显示了有关发件人模型的许多信息。

1. 转至分析 > 域。
2. 点击域名。



“域详细信息”页面

“域详细信息”页面显示以下信息。

1 域名、域的数量和来自该域的入站邮件流总量所占的百分比列于页面顶部。

2 域信誉(由 高级网络钓鱼防护 评分)列于右上角。如果您认为域的评分不正确，您可以通过“域反馈”链接发送反馈。域信誉的评分从 0.0 到 10.0，0.0 表示最低的信誉，10.0 表示信誉最佳。

3 页面中间是来自发送方域的邮件数量图。邮件分类如下：“已通过身份验证”、“不可靠”或“可能真实”。

- 真实可靠的邮件是遵守域本身发布的以下身份验证标准的域：SPF、DMARC 或 DKIM。
- 不可靠的邮件是身份验证失败并被认为不符合该域发件人模型的邮件。
- 可能真实的邮件是未通过身份验证但被认为“可能确实”来自发送方域的邮件。

点击图表顶部的图例可以切换显示条形图中的“已通过身份验证”、“不可靠”和“可能真实”条形。同理，图表的时间范围通过页面右上角的时间范围选择器控制(7 天/2 周/30 天)。

点击条形图中的任一个条形可以选择特定的日期。要清除选择，请选择“按 IP 地址

显示的邮件”表标题中的“清除”。

4 根据情况，此处还会显示域的 DMARC 和 SPF 记录。该区域下将显示影响域信誉的积极和消极因素。例如，此屏幕显示该域具有“一致的发送历史”。

“按 IP 地址显示的邮件”会编录在选定时间段内为该域发送邮件的每个 IP 地址。

5
- 点击 IP 地址将有效地转换视图：不查看给定域的所有 IP，而是查看该单个 IP 为其发送邮件的所有域。
- 点击“详细信息”页面“邮件总数”列中的数字可在“搜索邮件”页面中查看该发件人(IP 或域)的邮件列表。

域标签

可以为域分配标签。标签用于影响评分、分析域使用情况以及创建策略。您可以在 高级网络钓鱼防护 中从定义的标签列表将一个或多个标签分配给您的组织跟踪的任何域。

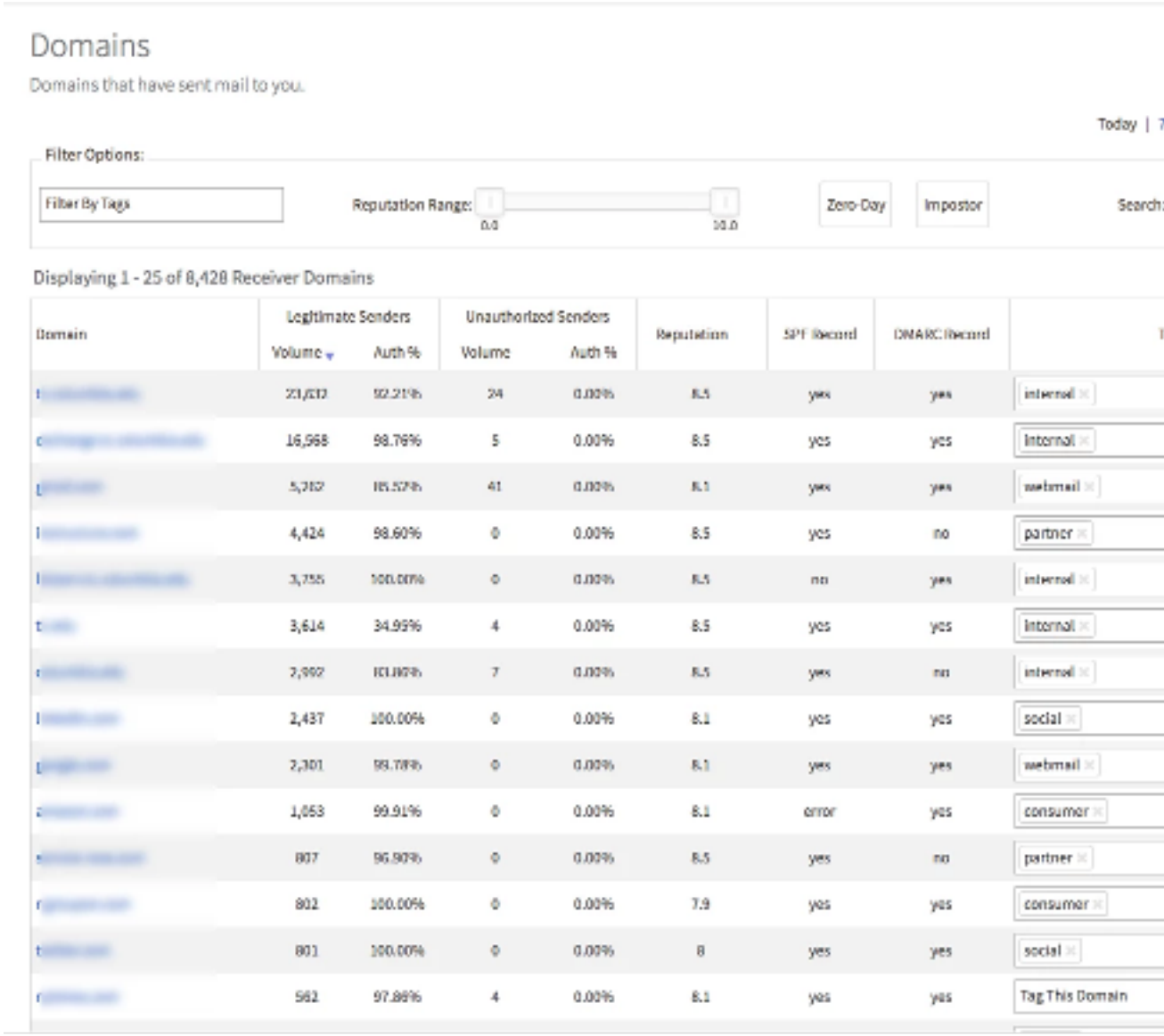
邮件评分过程中使用内部和合作伙伴两个标签。一般情况下，您需要提供：

- 内部标签给您拥有的、可控制的域，以及域信誉得到您内在信任的域
- 合作伙伴标签给与您交换电子邮件、已建立信任关系以及域信誉受到您信任的外部组织的域

将内部或合作伙伴标签添加到域会提高域的信誉，以便正确验证邮件。

您应避免同时将内部和合作伙伴标签添加到同一个域。

其他标签也可添加到域中，有助于在“分析”>“概览”页面上直观呈现搜索结果和创建策略过程。



域索引页面

将标签添加到域

1. 转至分析 > 域。
2. 点击任何域的“标签”字段。
3. 选择未使用的标签。

此标签将自动添加。

还可以在“域详细信息”页面上将标签添加到域(分析 > 域，然后点击域名)。“标签”字段位于右侧。

从域中删除标签

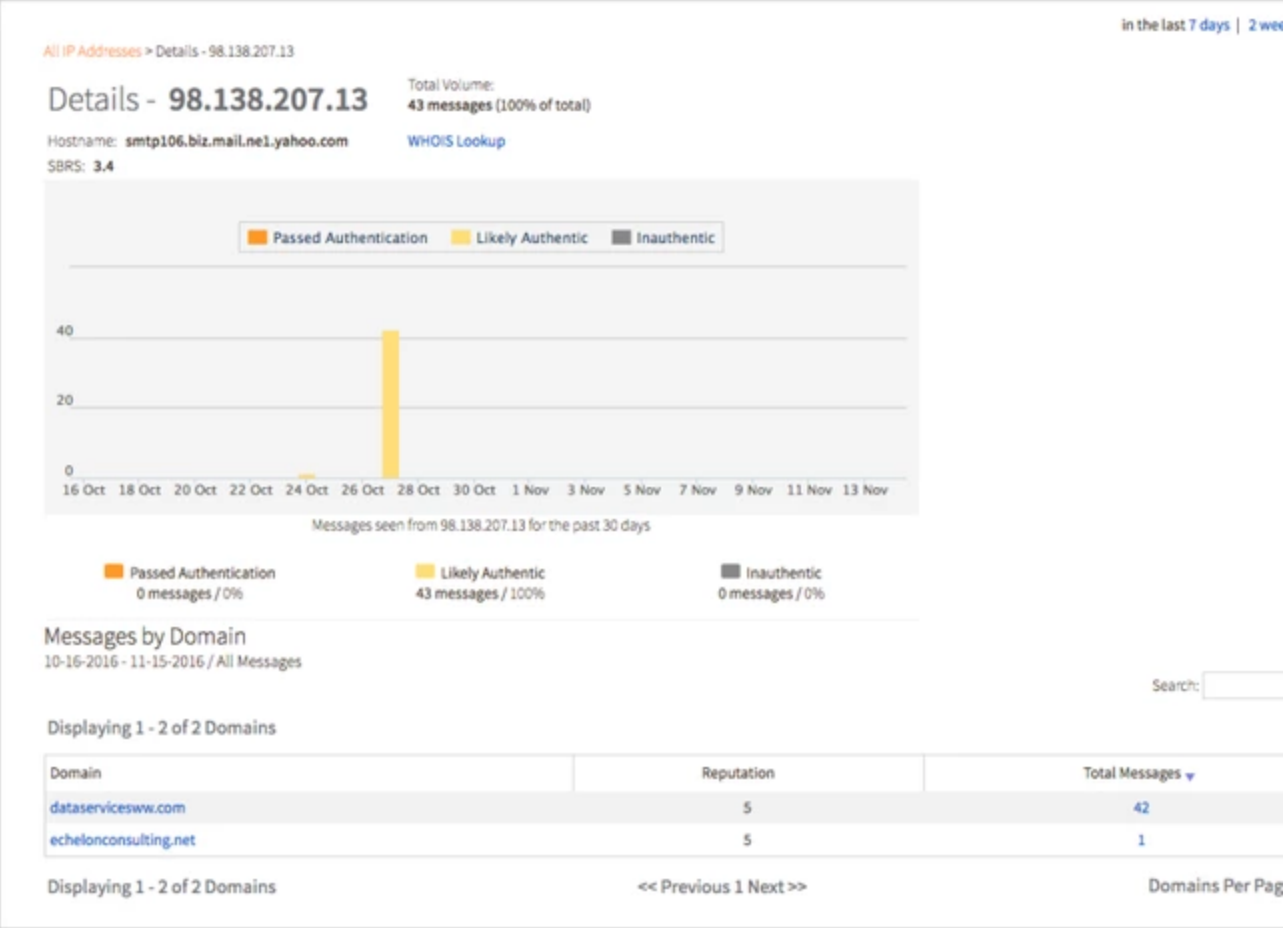
1. 转至分析 > 域。
2. 在域的“标签”字段中，点击要从域中删除的标签上的 x。

该标签会立即删除。

查看 IP 地址详细信息

查看给定 IP 地址的详细信息可帮助您确认该 IP 地址是否：

- 完全由发送方域所拥有(只为极少数域发送邮件)
- 共享的 IP 地址(为许多域发送邮件)
- 邮件转发地址(为大量域发送邮件)



“IP 详细信息”页面

在“IP 详细信息”页面中，您可以看到 IP 的主机名、您的组织在指定的一段时间内收到的来自该 IP 的邮件总数和 高级网络钓鱼防护 给出的 SBRS(SenderBase 信誉评分)。

该页面还包含给定 IP 地址的 WHOIS 信息的链接。

如同域详细信息页面上的时间序列图一样，您可以更改时间范围并切换显示真实、不可靠和可能真实的邮件计数。

在本示例中，发送方 IP 地址 98.138.207.13(其主机名为“smtp106.biz.mail.ne1.yahoo.com”) 已将 42 封邮件发送到组织：42 封邮件代表域“dataserviceswww.com”，一封邮件代表“echelonconsulting.net”。

点击“详细信息”页面“邮件总数”列中的数字可在“搜索邮件”页面中查看该发件人(IP 或域) 的邮件列表。

通知

高级网络钓鱼防护 提供可通知系统事件发生的通知系统。这些通知分为以下类别：

- 传感器
- 主机系统
- 策略

您可以启用的通知取决于您的系统配置。例如，如果您使用 Google G Suite，则可以启用的通知之一是为 G Suite 提供的凭证阻止正确进行身份验证。

选中您想要发送的任何通知的复选框。清除您不想发送的任何通知的复选框。完成后点击保存。

您选择的任何通知都将发送到“通知”部分中的“电子邮件地址”列表中的所有电子邮件地址。

添加通知收件人

1. 转至管理 > 策略。
2. 点击系统通知选项卡。
3. 在“通知”部分的其他收件人字段中，输入电子邮件地址。
4. 点击添加。
5. 点击保存。

删除通知收件人

1. 转至管理 > 策略。
2. 点击系统通知选项卡。
3. 在“通知”部分中，点击“电子邮件地址”列表中名称旁的 x。
4. 点击保存。

策略

使用策略指定当您的组织收到满足特定条件的邮件时应该怎么办。例如，您可以编写一条策略，查找来自特定发送方域的所有邮件并通知收件人和管理员。或者，您可以创建一个将可疑邮件移动到隔离文件夹的策略(仅适用于实施客户)。基本思路是对传入电子邮件流量中的特定条件(指定的)作出反应。

可能采取的操作包括记录传入邮件日志以便在 Web UI 中进行搜索和报告(默认操作)、发送通知(到原始收件人和/或指定的管理员用户)、将邮件移到特定的邮件文件夹(仅适用于实施配置)，甚至完全删除邮件(仅适用于实施配置)。

“策略”页面列出了现有策略。在该页面中，您可以创建策略，订用系统通知，并查看策略的事件日志条目。有关策略的详细信息，请参阅"查看策略结果" 在本页 58。有关为您预定义的策略的信息，请参阅"默认策略" 对页。请参阅"创建测试策略" 在本页 56，自己尝试创建策略。

默认策略

当组织最初在 高级网络钓鱼防护 中创建时，系统将自动创建一组默认、预先配置的策略。这些策略与 思科 客户使用 高级网络钓鱼防护 捕获的最常见情况相匹配，并且必须在启用后才能开始匹配邮件，并为其定义通知和/或实施操作。建议您先启用不包含操作的策略。先仅记录策略匹配项并监控结果，然后选择您的通知和实施操作。

本部分介绍默认策略的开箱即用配置。

如果您已更改任何策略的配置，需要将其恢复为默认状态，此信息会很有用。

未在下表中明确定义的任何设置具有以下值：

- 方向：入站
- 文本字段：空
- 复选框：未选中
- 下拉列表：未选择值
- 具有两个控点的滑块：左端的左控点，右端的右控点(超出邮件计数时控件只有一个控点，默认值为 10)

策略名称	设置	值	说明
品牌显示名称冒充者	攻击类型	品牌显示名称冒充者	攻击类型包括品牌 DNI。捕获在显示名称中冒充常见品牌的冒充者。
首席级高管冒充者	发件人	首席级高管(地址组)	与“首席级高管”地址组中的显示名称匹配。捕获 BEC 攻击/首席执行官、首席财务官和其他最高级别高管的冒充者。请注意，此策略需要您填充“首席级高管”地址组，该地址组同样作为默认地址组为您创建。
高管冒充者	发件人	高管(地址组)	与“高管”地址组中的显示名称匹配。捕获 BEC 攻击 /组织中其他高管的冒充者。请注意，此策略需要您填充“高管”地址组，该地址组同样作为默认地址组为您创建。
相似的域	攻击类型	相似的域	攻击类型包括相似的域。捕获故意使用类似名称的冒充域，例如 ciisco.com 或 paypa1.com。
邮件可信度低和服务器信誉低	可信度评分范围	0.0 到 2.5	邮件可信度评分 <= 2.5，SBRS 评分 <= -2.0。捕获躲过 SEG 的一般垃圾邮件和灰色邮件。
	SBRS 范围	-10.0 到 -2.0	
快速 DMARC	域标签	内部	域标签为“内部”，攻击类型包括域欺骗。捕获向您员工发送的您自己的域的欺骗攻击。此策略模仿 DMARC 拒绝策略，无需经过对所有源进行身份验证的冗长过程。Agari 的可信

策略名称	设置	值	说明
	攻击类型	域欺骗	度模式可获知入站源的真实性。
合作伙伴域欺骗	域标签 攻击类型	合作伙伴 域欺骗	域标签为“合作伙伴”，攻击类型包括域欺骗。捕获合作伙伴域的欺骗攻击。
发送到首席级主管的可疑邮件	收件人 可信度评分范围	首席级高管(地址组) 0.0 到 3.0	对“首席级主管”中的电子邮件地址匹配邮件可信度评分，评分范围为 0 - 3.0(含 0 和 3.0)。捕获发送到一名首席级高管的不可信或非常可疑的邮件。
不可信邮件	可信度评分范围	0.0 到 1.1	邮件可信度评分范围为 0 - 1.0(含 0 和 1.0)。

可以根据您的经验和您组织的邮件流特征编辑这些默认策略中的条件。开箱即用的条件以整个 思科 客户群认为有效的条件为基础。

创建策略

创建策略非常简单：指定要用于匹配某种邮件的条件，然后设置要对匹配这些条件的邮件执行的操作。

在创建策略之前，您应该了解几个重要事项：

- 系统会为每封邮件评估每条策略，且一封邮件可能与多条策略匹配。
- 如果邮件与多条实施策略匹配，其实施操作的优先级顺序如下：
  a. 收件箱
  b. 删除
  c. 移到默认文件夹
  d. 按照组织实施设置(请参阅组织设置)中的顺序移到其他文件夹。

您可以创建没有通知或实施操作的策略；与策略匹配的所有邮件都记录在事件日志和报告中。

1. 转至管理 > 策略。
2. 点击创建策略。
3. 定义策略设置。(有关详细信息，请参阅策略设置。)
4. 点击创建。

编辑策略

1. 转至管理 > 策略。
2. 点击策略名称。
3. 对策略设置进行任何所需更改。(有关详细信息，请参阅策略设置。)
4. 点击保存。

启用或禁用策略

1. 转至管理 > 策略。
2. 点击策略名称。
3. 点击策略名称下方的滑块以启用或禁用此策略。

4. 点击保存。

删除策略

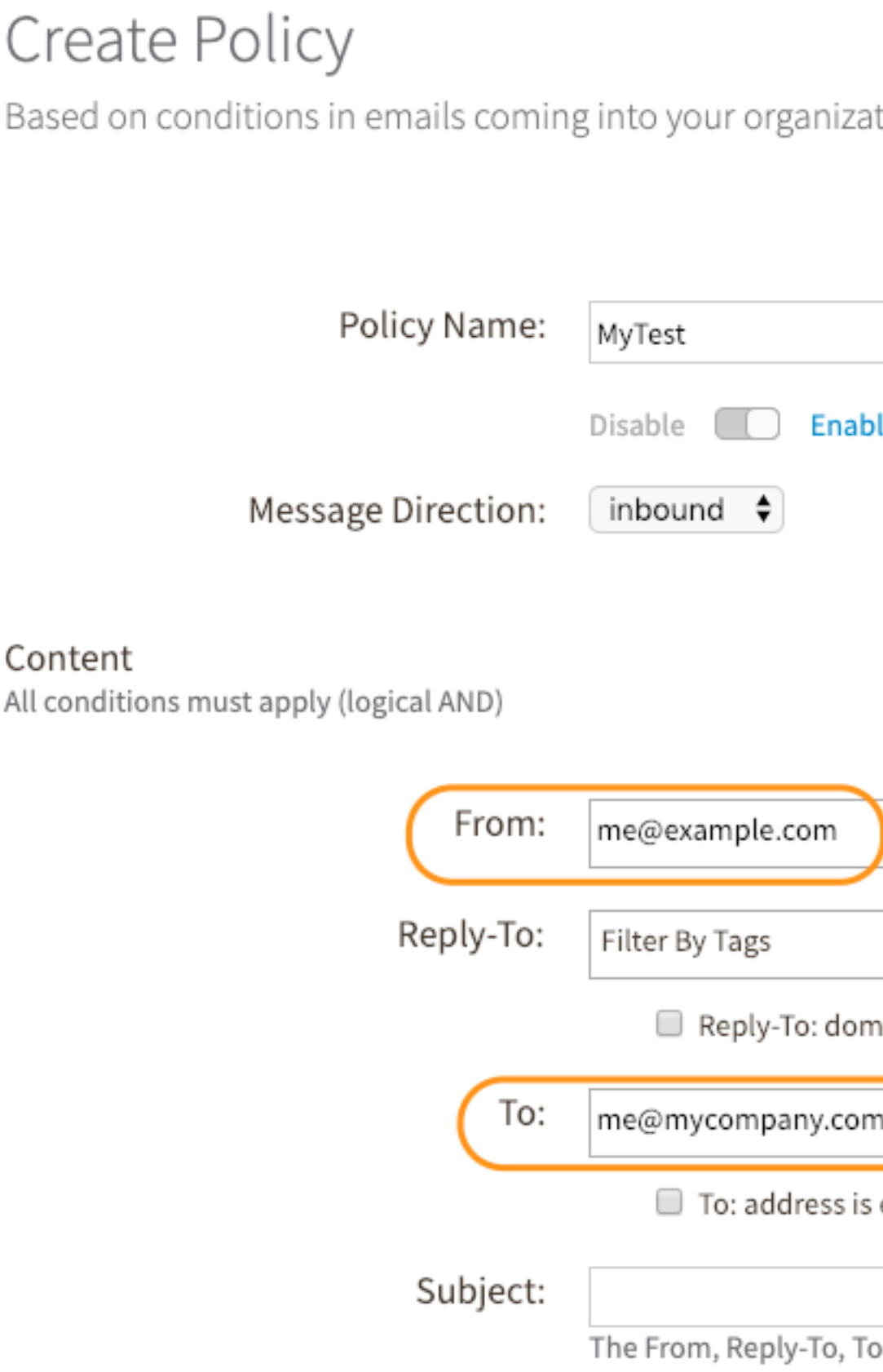
1. 转至管理 > 策略。
2. 点击策略名称。
3. 在页面底部，点击删除 [策略名称] 链接。
4. 点击确定。

创建测试策略

创建基本策略很简单：只需要输入三项信息。

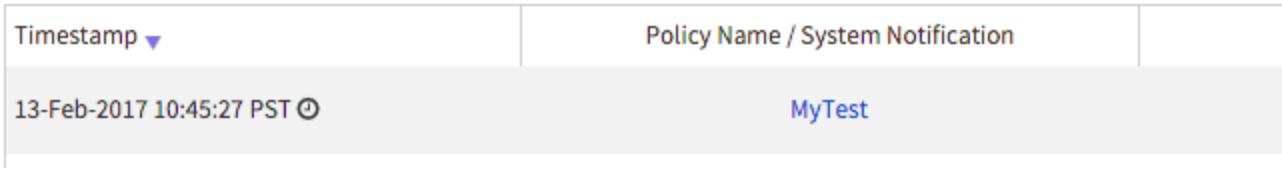
1. 转至管理 > 策略。
2. 点击创建策略。
3. 输入以下信息：
   - 策略名：MyTest
   - 发件人：您的个人电子邮件地址

- 收件人：您的公司电子邮件地址



此时，您的策略已完成。请注意，我们并未指定操作。所有匹配策略的默认操作是将邮件记录到策略日志中。

4. 点击创建。
5. 从您的个人帐户向您的公司地址发送一封邮件。
6. 在管理 > 策略页面中，点击策略日志选项卡。日志中应该出现您的策略和您刚发送的邮件的条目。



策略事件的策略事件日志

就是这样。您已经成功创建用于匹配传入邮件的策略。

根据条件匹配传入邮件是创建策略的基本组成部分。在此基础上，您可以添加更多详细信息并提高复杂性，匹配主题或匹配特定的域或 IP 地址。您可以创建地址组，用于匹配一组发件人或收件人。(有关详细信息，请参阅"地址组" 在本页 78。) 您可以指定评分选项范围。

接下来，您需要指定要对匹配的邮件执行的操作。

指定操作

现在您已能轻松创建策略来匹配邮件，现在应指定出现匹配项时要采取的操作。除了默认的日志记录外，您还可以指定另外两项操作：通知和实施(仅适用于实施客户)。可以将这些操作想像成频谱的不同部分：日志记录是影响最小的操作，后跟通知操作，然后才是影响最大的实施操作。因此，您在快速了解策略时，最初应该只尝试日志记录，然后仅通知管理员，再通知邮件收件人，最后才考虑实施。

实施客户：请在启用实施前测试策略以确保其不会太宽泛(过于宽泛的策略可能会导致误报)。

查看策略结果

创建并启用一些策略后，您将需要对如下问题的结果和答案有一定了解

- 这些策略能按预期工作吗？
- 匹配的邮件有多少？
- 匹配数量是否有增长趋势？

您可以通过三种方式检查此类信息：

- 策略日志是策略匹配项的运行日志
- “管理”>“报告”页面上显示长期以来的聚合策略匹配量。
- 在“搜索邮件”页面上，您可以搜索匹配的策略。

策略日志

在管理 > 策略页面中，点击策略日志选项卡。这是所有策略匹配和系统通知事件的日志。

策略日志实时显示发生的每个策略匹配项。这是按邮件显示的策略匹配项列表(每个匹配项一封邮件)。

点击策略的名称，查看匹配的策略。点击“事件”列中的行，查看与策略匹配的邮件的详细信息。

您可以过滤策略日志，以显示特定策略的匹配邮件，并选择是否在此视图中显示系统通知。

策略报告

管理 > 报告页面显示一段时间内的策略事件摘要：每个策略有多少匹配项。

点击策略名称可在策略编辑器中查看策略条件和操作。

点击邮件数(或水平控制栏)可查看该策略的详细报告。

策略报告显示当天的匹配项数量。在右侧选择更长的时间段可延长时间轴。此视图可以显示该策略的匹配趋势。现在匹配该策略的邮件是否更多？更少？点击策略报告中的邮件数可在搜索邮件结果中查看邮件。

有关实施的报告

从显示策略下拉列表中选择含实施操作可查看所有包含实施操作的策略下已移动和未移动邮件的摘要。

按实施操作过滤策略报告

搜索邮件

在分析 > 搜索邮件页面上，您可以在匹配的策略字段中选择一个策略，以搜索触发所选策略的邮件。

报告

思科高级网络钓鱼防护 提供两种类型的报告：

- 关于策略的信息，在 高级网络钓鱼防护 中定义，带或不带实施策略，在“管理”>“报告”页面上提供。
- 关于关键威胁指标的信息，以图表形式显示，在 高级网络钓鱼防护 控制板 (“分析”>“控制板”或点击产品徽标) 的“执行摘要”和“威胁趋势”选项卡上提供。

“报告”页面

“报告”页面显示一段时间内的策略事件摘要。特别显示在选定时段内与每个策略匹配的邮件数。点击策略名称可在策略编辑器中查看策略配置。点击邮件数 (或水平控制栏) 可查看该策略的策略报告。

默认情况下，策略报告显示当天的匹配项数量。在右侧选择更长的时间段可延长时间轴。此视图可显示匹配该策略的邮件随时间推移的趋势。现在匹配该策略的邮件是否更多？更少？点击策略报告中的邮件数可在搜索邮件结果中查看邮件列表。

“威胁趋势”和“执行摘要”报告

主页上的“威胁趋势”和“执行摘要”选项卡 (分析 > 控制板) 总结了 高级网络钓鱼防护 累计的最近数据。

在折线图和条形图显示报告中，可将鼠标悬停在任何日期表示上并查看弹出窗口，其中包含此日期的详细数据。

您可以在页面上选择所有报告的时段。选项包括：

- 7 天
- 2 周
- 1 个月
- 自定义 (选择开始日期和结束日期)

报告中的聚合数据不包括来自当前日期的数据或组织数据的起始累积日期之前的数据。数据如下显示在图表中：

- 如果时段为 7 天和 2 周，则每个数据点代表一整天的数据。例如，如果您选择 7 天，将看到过去 7 整天的数据，但没有今天的数据。
- 如果时段为 1 个月，每个数据点代表一整周 (周一到周日) 的数据，始于从 1 个月前的星期一开始的那一周。根据当天是星期几和当月的天数，这意味着第一周或最后一周的数据可能少于 7 天。

- 对于自定义时段，如果您选择从一天到最长 2 周的时段，则每个数据点代表一整天的数据。如果您选择的时段超过 2 周，则每个数据点代表一整周(周一到周日)的数据。如果您设置的开始日期早于您的组织开始累积报告数据的日期，则每个图表顶部的“始于...”符号将指示图表中数据的最早日期。自定义日期范围也有“粘性”，因为它们在您导航离开该选项卡或页面时不会重置，只有在您注销时才会重置。

可以将当前页面下载为 Adobe Acrobat (PDF) 格式。有关详细信息，请参阅"下载威胁趋势或执行摘要报告" 在本页 72。

有关详细信息，请参阅"威胁趋势报告" 对页和"执行摘要报告" 在本页 65，以及每个报告的单独说明部分。要更改这些报告的全局设置，请参阅组织 部分设置中的报告设置。

“威胁趋势”选项卡

“威胁趋势”选项卡包含详细描述一段时间内主要的攻击趋势的数据视图。它显示了以下内容：

- 邮件

  此图显示一段时间内的各种关键数字，包括邮件总数、垃圾邮件/灰色邮件数、攻击数以及每日按策略匹配的邮件数。

- 攻击数

  此图显示 高级网络钓鱼防护 发现的攻击数。

- 排名靠前的策略

  此图显示触发的前 5 名策略。

请参阅"威胁趋势报告" 对页。

“执行摘要”选项卡

“执行摘要”选项卡包含详细说明 高级网络钓鱼防护 的累积影响和对员工的保护价值的数据视图。它回答以下问题：

- 发现了多少攻击？

  此图显示 高级网络钓鱼防护 发现的攻击数。(请注意，一封邮件可能包含多个攻击媒介。)

- 我通过部署 思科高级网络钓鱼防护 节省了多少？

  此图估算了您的组织通过 高级网络钓鱼防护 防御网络钓鱼和其他恶意攻击而节省的资金量。

- 相对于我的对等组，我的受攻击和受保护水平如何？

  这个双图面板显示攻击数以及相对于对等组织 高级网络钓鱼防护 对您的保护程度。

请参阅"执行摘要报告" 在本页 65。

“威胁趋势”和“执行摘要”选项卡上的报告显示聚合的数据。聚合数据每日午夜 (UTC) 更新一次。

威胁趋势报告

威胁趋势报告是在 思科高级网络钓鱼防护 主页的“威胁趋势”选项卡上以控制板形式显示的一组报告(分析 > 控制板)。这些报告汇总 高级网络钓鱼防护 生成的关键数据，并通过易于查看的图表来显示这些数据。

威胁趋势报告包括：

- 邮件，显示我的组织面临的威胁和攻击。(请参阅"邮件报告" 向下)
- 攻击，显示我的组织面临的攻击类型。(此图表中的数据与“执行摘要”选项卡上发现了多少攻击？ 报告相同，但在图表顶部没有攻击总数。查看“发现了多少攻击”报告"发现了多少攻击 报告" 在本页 65)
- 前 5 名策略，显示触发次数最多的策略。(请参阅"“排名靠前的策略”报告" 在本页 64)

此页面上的报告视图旨在让您了解一段时间内的关键趋势，而不只是累计数字。

可以自定义某些报告的数据集。有关报告中使用的数据以及有关如何配置报告的说明，请参阅每个报告上的部分了解详细信息。

*邮件*报告

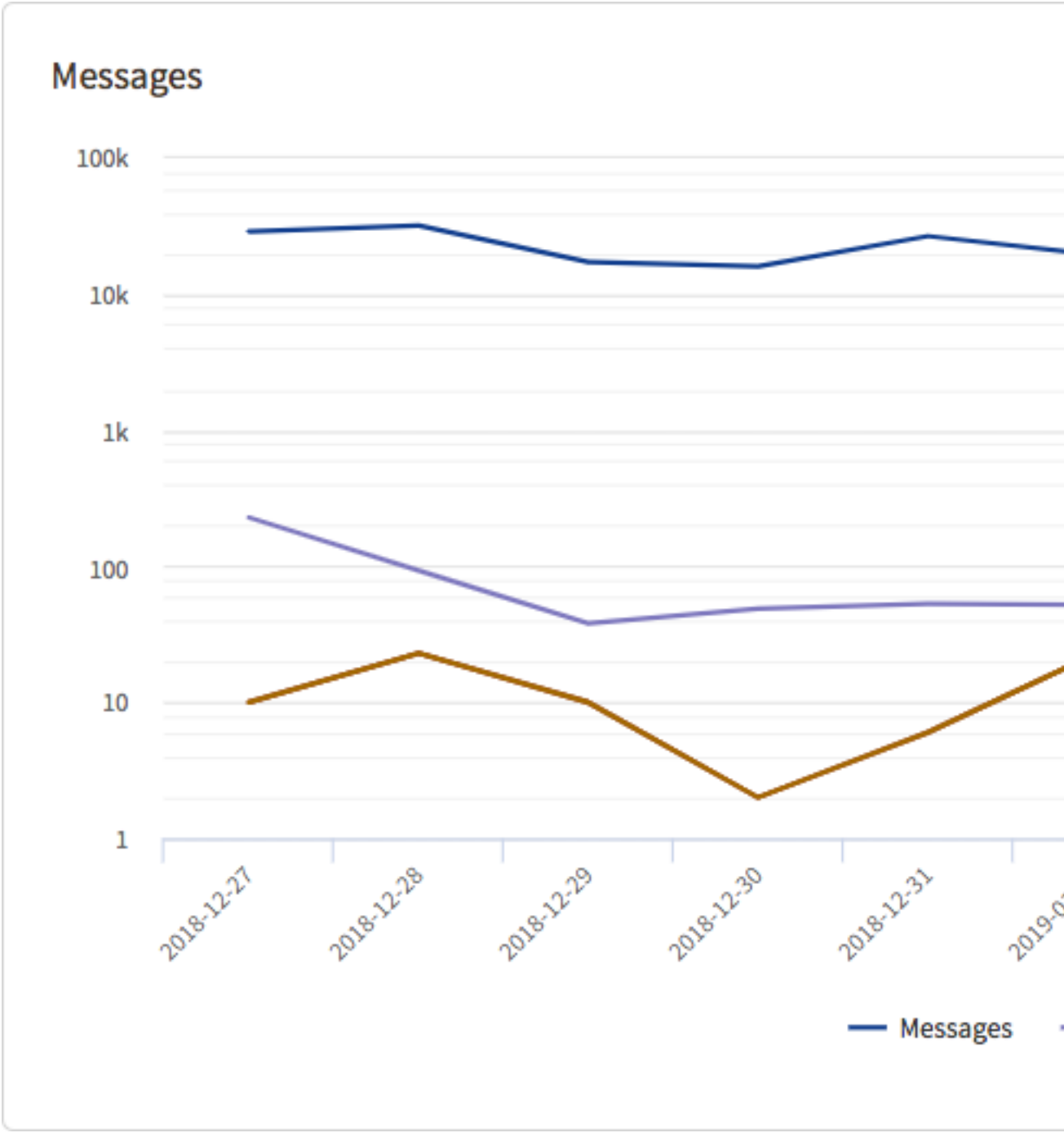
“邮件”报告将向您显示：

- 接收的邮件数量 高级网络钓鱼防护
- 属于以下类型的邮件数量
  - 垃圾邮件或灰色邮件
  - 识别为任何攻击类型
  - 匹配任何策略的攻击

此图表为折线图形式。将鼠标悬停在折线的任何点(表示单个时段，日或周)上，可查看此时段的数据。

在查看 7 天或 2 周数据时，每个点表示 1 天。在查看 1 个月数据时，每个点表示 1 周数据。

图例中的各项也是切换开关。可以点击图例中的某项，以将其包括在或排除出报告。



显示 2 周邮件的报告示例。

与其他报告不同，此图表中的 Y 轴为对数坐标轴。

如果您的策略经过适当调整以匹配您收到的攻击(请参阅"策略"在本页 53)，则攻击和策略匹配行应非常接近甚至重叠。(在此示例中，这两条折线重叠，这意味着至少一个策略匹配所收到的每个攻击，因此您只能看到 3 条可见折线。)

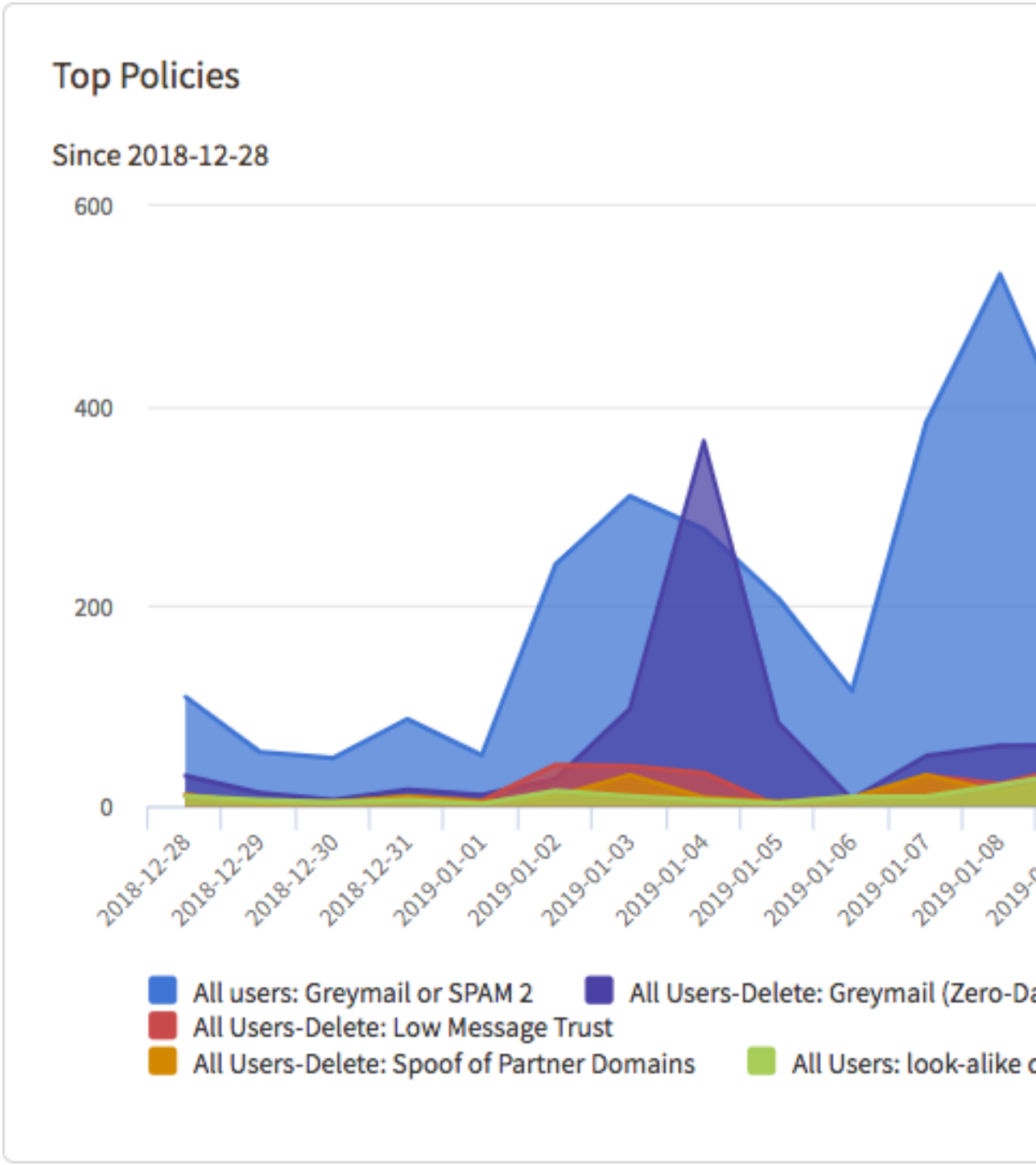
*攻击*报告

“攻击类型”报告中包含的数据和交互与“执行摘要”选项卡上发现了多少攻击？ 报告相同，但在图表顶部没有总数。请参阅"发现了多少攻击 报告"在本页 65以详细了解

此报告提供的数据以及如何自定义报告显示的内容。

*“排名靠前的策略”*报告

此报告显示每个时段内匹配邮件数最多的 5 个策略。具体而言，当您选择时段(7 天、2 周或月)时，高级网络钓鱼防护 会查看在该时段内匹配邮件数较多的 5 个策略，然后为每个策略创建一个增量图，7 天和 2 周视图中为每日增量，月视图中为每周增量。



显示 2 周内策略匹配量的报告示例。

执行摘要报告

执行摘要报告是 思科高级网络钓鱼防护 主页上“执行摘要”选项卡上以控制板形式显示的一组报告(分析 > 控制板)。这些报告汇总 高级网络钓鱼防护 生成的关键数据，并通过易于查看的图表来显示这些数据。

“执行摘要”页面上的报告将解答以下问题：

- 发现了多少攻击？(查看"发现了多少攻击 报告" 向下)
- 我通过部署 思科高级网络钓鱼防护 节省了多少？(请参阅""“我通过部署 高级网络钓鱼防护 节省了多少”报告" 在本页 67)
- 相对于我的对等组，我的受攻击和受保护水平如何？(请参阅"相对于我的对等组，我的受攻击/受保护水平如何 报告" 在本页 69)

可以自定义某些报告的数据集。有关报告中使用的数据以及有关如何配置报告的说明，请参阅每个报告上的部分了解详细信息。

发现了多少攻击 报告

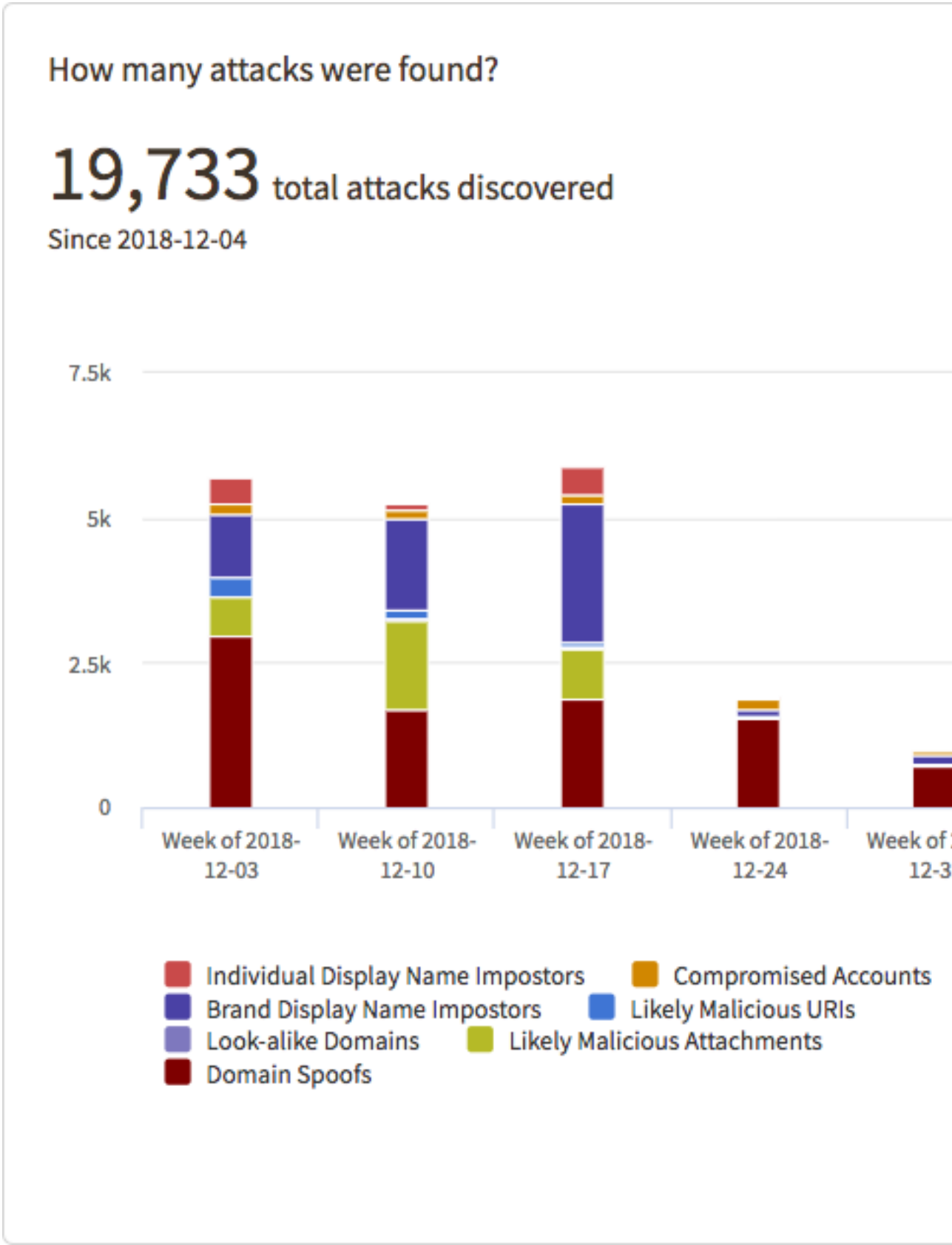
此报告以条形图形式显示 高级网络钓鱼防护 发现的攻击数，包括攻击总数和按攻击类型划分的攻击数。将鼠标悬停在某个条形中表示特定攻击类型的任何部分上，可查看此类型的攻击数。

顶部数字回答标题问题，即在显示时段内发现的攻击总数。这始终为所有攻击类型的累计数量。

在查看 7 天或 2 周数据时，每个条形表示 1 天。在查看 1 个月数据时，每个条形表示 1 周数据。

攻击类型图例也是切换开关。可以点击攻击类型以将其包括在或排除出条形图。

更改条形图中显示的攻击类型不会更改顶部显示的攻击总数。



显示一个月攻击的报告示例。

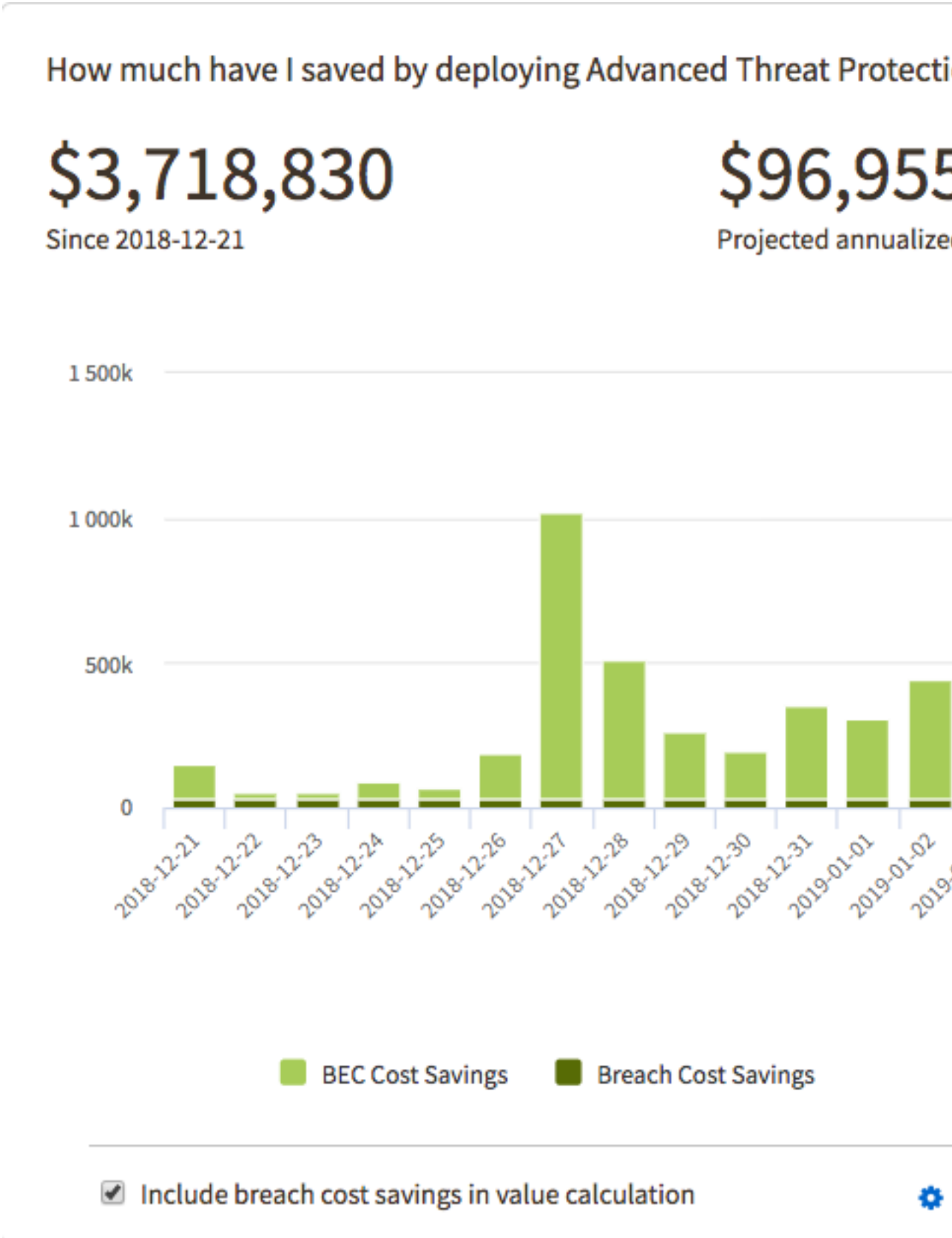
每个条形显示每个时段(在 7 天和 2 周视图中为每天，在月视图中为每周)的攻击总数。图表中的各部分对应于每种攻击类型的攻击数。将鼠标悬停在某个部分上可查看此部分表示的类型的攻击数。

“我通过部署 高级网络钓鱼防护 节省了多少”报告

此报告显示 高级网络钓鱼防护 为您节省的资金。它跟踪您的实时策略和按需策略删除或移动了多少商业电子邮件诈骗威胁邮件，并以图表形式说明如果这些邮件被允许进入或保留在组织收件箱中，会给您的组织造成多少损失。

您还可以选择包括通过阻止电子邮件漏洞所节省的资金。

请参阅配置“我通过部署 高级网络钓鱼防护 节省了多少”报告，以获取有关如何配置此报告中使用的值的详细信息。



显示 2 周节省资金的报告示例。

顶部数字回答标题问题。第一个数字是您在显示的时段内节省的金额(基于输入的值)。第二个数字是通过第一个数字推断出的年化数字。

相对于我的对等组，我的受攻击/受保护水平如何 报告

此报告显示您如何受到攻击以及 思科高级网络钓鱼防护 为组织提供的保护程度，并与您的对等组织比较。如果没有足够的对等组织，则报告将回退到更广泛的数据集。“对等”层次结构如下：

- 区域、行业和组织的邮箱数
- 行业和组织的邮箱数
- 组织的邮箱数
- 整个 思科 数据集中所有组织的平均值

“区域”是定义的地理区域，如北美洲或 EMEA(欧洲、中东和非洲)

“行业”是制造业或金融业等类别

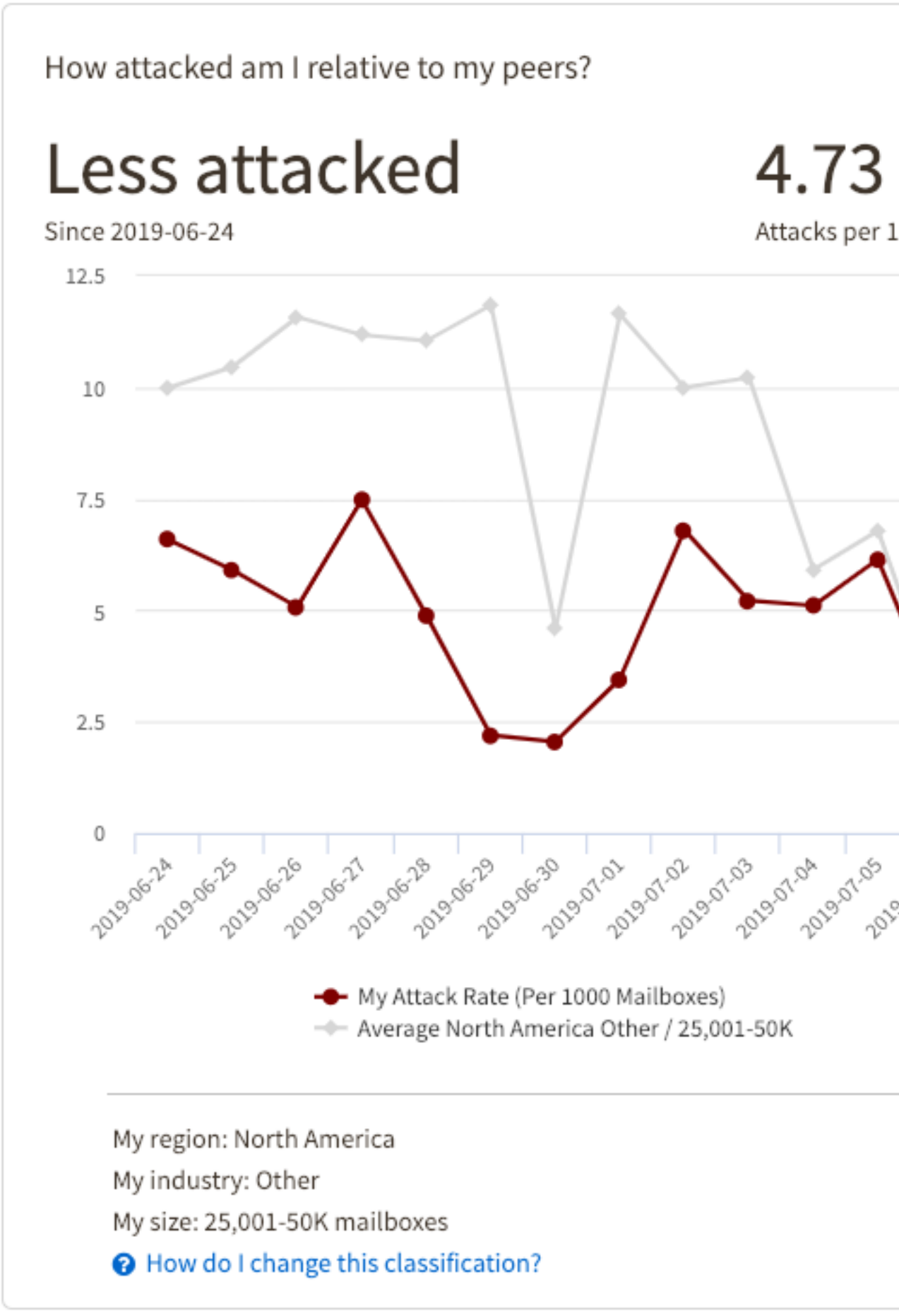
“邮箱数”由一组层定义。例如，如果组织有 10,000 个邮箱，则将仅限于与具有 10,000 个邮箱的层中的其他组织进行比较。

对于层次结构中的每个级别，如果级别中可用于比较的组织未达到至少 5 个，则将使用下一级别。例如，假设您是南美洲一家飞机零件制造商，而南美洲从事同一行业的其他公司只有 2 家。因此不会使用第一级别。但在全球有 5 家以上，如果有足够公司的大小相同(“大小”定义为相同数量的邮箱)，则将在此报告中使用第二级别。

在报告底部，将显示为组织定义并用于当前报告的区域、行业和邮箱大小。点击“与其他对等组比较”以更改对组织的比较方面。有关详细信息，请参阅"与其他对等组比较" 在本页 71。

报告本身将使用 高级网络钓鱼防护 而非 高级网络钓鱼防护 的每日值绘制成图表。对于执行控制板上的所有报告，可以选择过去 7 天(默认值)、过去 2 周或过去一个月的时段。

有关如何配置此报告的详细信息，请参阅"与其他对等组比较" 在本页 71。


How attacked am I relative to my peers?
Less attacked
4.73
Since 2019-06-24
Attacks per 1
12.5
10
7.5
5
2.5
0
2019-06-24
2019-06-25
2019-06-26
2019-06-27
2019-06-28
2019-06-29
2019-06-30
2019-07-01
2019-07-02
2019-07-03
2019-07-04
2019-07-05
My Attack Rate (Per 1000 Mailboxes)
Average North America Other / 25,001-50K
My region: North America
My industry: Other
My size: 25,001-50K mailboxes
How do I change this classification?

显示 2 周比较数据的报告示例

在相对于我的对等组，我的受攻击水平如何折线图中，一条折线表示每个时段(在 7 天和 2 周视图中为每天，在月视图中为每周) 内每 1000 个邮箱的攻击率。另一条折线是对等组(区域、行业、邮箱数) 的平均攻击率。如果额外增加了一个对等组进行比较，则第三条折线将显示此组的攻击率。

顶部摘要回答图表的标题问题，并确定所显示时段的每日平均攻击率(每 1000 个邮箱)。提供以下答案之一：

- 攻击更多 - 在所显示时段内，比对等组平均攻击率高 10% 以上
- 攻击略多 - 在所显示时段内，比对等组平均攻击率高 2% 到 10%
- 大致相同 - 在所显示时段内，与对等组平均保护率的差别在 ±2% 之间
- 攻击略少 - 在所显示时段内，比对等组平均攻击率低 2% 到 10%
- 攻击少得多 - 在所显示时段内，比对等组平均攻击率低 10% 以上

在“相对于我的对等组，我的受保护水平如何”条形图中，一个条形表示每个时段(在 7 天和 2 周视图中为每天，在月视图中为每周) 内的保护率。另一条形是对等组(区域、行业、邮箱数) 的平均保护率。如果额外增加了一个对等组进行比较，则第三个条形将显示此组的保护率。如果已启用策略实施，则将显示内部条形以比较实施率与保护率。

计算方法如下：

- 保护率的计算方法是，匹配任何策略的攻击邮件数除以攻击邮件总数除以 100。
- 实施率的计算方法是，任何现有策略实施的攻击邮件数除以攻击邮件总数除以 100。

它们可能不同，因为您可能在 高级网络钓鱼防护 中配置了与邮件匹配、但不实施邮件的策略，这意味着邮件不会从收件箱中移出或删除。

顶部摘要回答图表的标题问题，并确定所显示时段的每日平均保护率(每 1000 个邮箱)。提供以下答案之一：

- 保护更多 - 在所显示时段内，比对等组平均保护率高 10% 以上
- 保护略多 - 在所显示时段内，比对等组平均保护率高 2% 到 10%
- 大致相同 - 在所显示时段内，与对等组平均保护率的差别在 ±2% 之间
- 保护略少 - 在所显示时段内，比对等组平均保护率低 2% 到 10%
- 保护少得多 - 在所显示时段内，比对等组平均保护率低 10% 以上

较高数字意味着您配置的策略能够有效避免您受到所面临的攻击。

与其他对等组比较

用于在相对于我的对等组，我的受攻击/受保护水平如何报告中进行比较的公司是您所在地区和行业中的公司，与您的邮箱大小相似。还可以添加与其他地区、行业或邮箱大小的比较。

1. 转至分析 > 控制板。
2. 点击执行摘要选项卡。

3. 在相对于我的对等组，我的受攻击/受保护水平如何报告底部，点击与其他对等组比较。
4. 选择：
    - 地区。您可以选择：
        - 所有 思科 客户
        - 北美地区
        - EMEA(欧洲、中东和非洲)
        - APAC(亚太地区)
    - 行业。您可以选择：
        - 所有 思科 客户
        - 金融
        - 政府
        - 医疗业
        - 其他
        - 零售业
        - 技术
    - (邮箱) 大小。您可以选择：
        - 所有 思科 客户
        - 0-250
        - 250-1000
        - 1001- 3000
        - 3001-5000
        - 5001-10000
        - 10,001-25,000
        - 25,001-50,000
        - 50,001-100,000
        - 100,000 以上
5. 点击更新。

报告将使用新的比较方面进行刷新。请注意，如果没有足够数据源供您选择，并且报告扩展到下一层(请参阅 "相对于我的对等组，我的受攻击/受保护水平如何报告" 在本页 69了解详细信息)，报告可能不会更改。图例会反映您的选择，但报告将使用包含足够数据的第一层来进行有用比较。

当添加一组用于此报告的对等组时，所做更改将“停留”。也就是说，如果您在离开页面后返回，数据仍将显示添加的这一组对等组。

下载威胁趋势或执行摘要报告

可以将“威胁趋势”或“执行摘要”报告的当前视图下载为 Adobe Acrobat (PDF) 文件，其中包括所有图表。

1. 转至分析 > 控制板。
2. 点击威胁趋势或执行摘要选项卡。
3. 配置报告的时段。如果您查看的是执行摘要报告，还可以配置我通过部署 高级网络钓鱼防护 节省了多少？ 和相对于我的对等组，我的受攻击/受保护水平图表中的数据。请参阅配置“我通过部署 高级网络钓鱼防护 节省了多

少”报告和"与其他对等组比较" 在本页 71以获取详细信息。
4. 点击下载 PDF。

系统将创建当前视图的 PDF，并自动下载至浏览器的默认下载位置。

附件和 URL 分析

思科高级网络钓鱼防护 能够分析邮件附件和邮件正文中的 URLI，并使用该分析的结果加之身份情报来确定邮件的总体可信度。

高级网络钓鱼防护 可以进行两个级别的恶意内容分析：

- 收集名称和文件扩展名等可用于搜索和策略中的附件基本信息。
- 扫描附件中是否存在恶意企图迹象，以便增强评分和邮件分类。

URL 分析将：

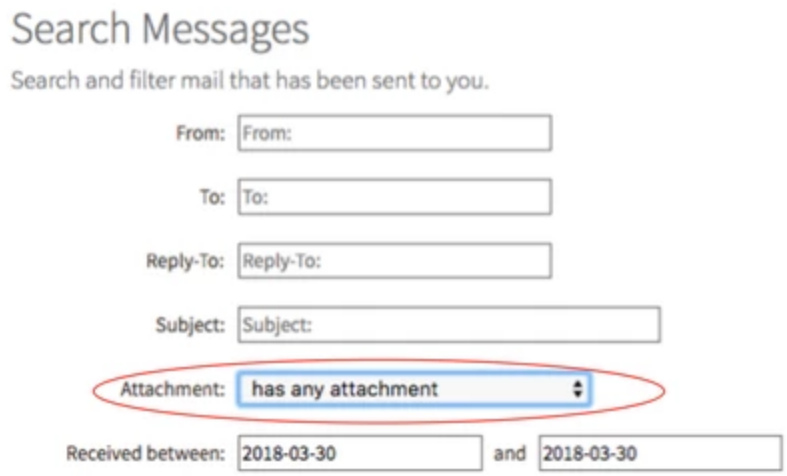
- 从以下内容提取 URL：
  - 邮件的文本/HTML MIME 部分，包括邮件头部分中的基本 URL
  - 附加到邮件的 Microsoft Office 和 Adobe Acrobat 文档
- 解析 http 和 https 方案
- 将在邮件详细信息视图中显示 URL，但无法点击这些 URI
- 识别使用常见 URL 缩短器的 URL，以及这些 URL 缩短器背后的网站

使用附件分析

启用附件分析后，可通过不同方式使用附件分析结果。

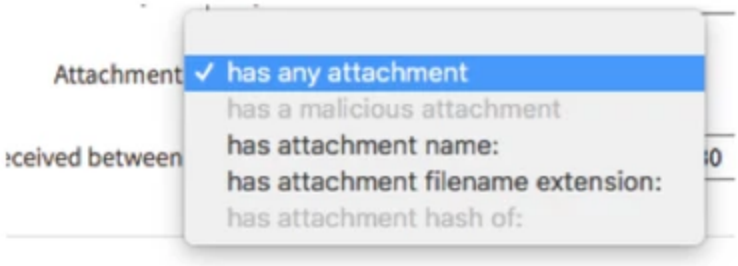
在搜索和策略中使用附件分析结果

您会发现，“分析”>“搜索邮件”页面中有一个新选项。当您要创建或编辑策略时，“管理”>“策略”页面中也会显示相同的字段。



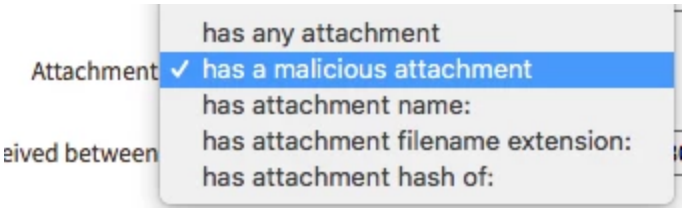
搜索包含附件的邮件

如果只收集附件名称信息，则以下选项可用于搜索和设置策略。



搜索附件：有限的选择

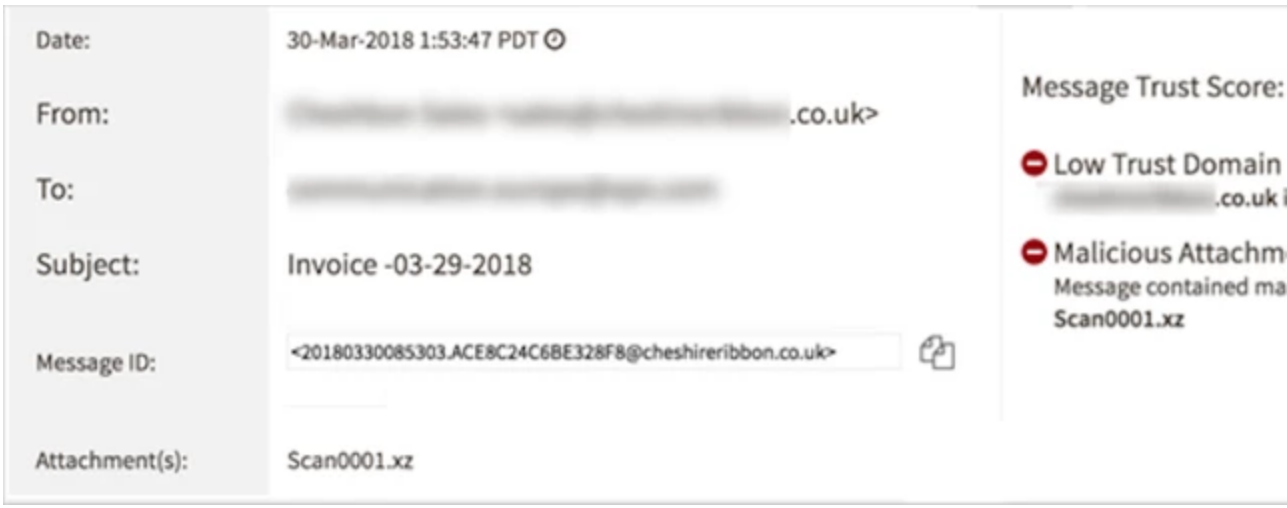
如果您已启用附件扫描，则所有选项均可用于搜索和策略。



搜索附件：已启用附件扫描

附件扫描结果

启用附件扫描时，高级网络钓鱼防护 将在其评分模型和邮件分类模型中使用扫描结果。例如，您将在“邮件详细信息”中看到如下“恶意附件”邮件分类。(注：不久的将来，您还可以展开恶意附件分类，查看检测到的恶意组件的详细信息。)



“邮件详细信息”窗格中的附件扫描结果

附件扫描的详细信息

高级网络钓鱼防护 附件扫描功能侧重于识别基于文档的附件中的潜在恶意行为。它并非沙盒分析，也不会尝试强制恶意代码执行。

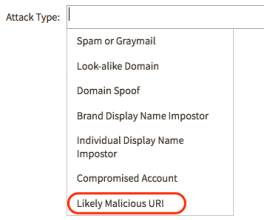
高级网络钓鱼防护 将对以下类型的文件解压缩、反混淆并执行静态分析：

- 存档文件格式 (zip/rar/tar/{gz/gzip/tgz}/{bz2/bzip2/tbz2/tbz}/cab)
- Office 文件、PDF、MHTML、电子邮件文件、图像文件、平面数据文件、RTF

- Flash、视频格式、Javascript、VBA

使用 URL 分析

可以在邮件搜索和策略创建中使用 URL 分析。在这两种情况下，可以从“攻击类型”下拉列表中选择可能的恶意 URI 以包括在搜索或策略过滤器中。



选择此选项可将带有可能恶意 URL 的邮件包括在搜索或策略中。

发件人管理和快速 DMARC

思科高级网络钓鱼防护 中的“发件人”页面显示发现使用您的内部域将邮件发送到您组织中的常见发件人。您可以快速了解 高级网络钓鱼防护 如何对发件人发往内部域的流量进行建模，而且只需点击一下鼠标就可以明确批准或拒绝特定发件人。借助对发件人模型的这一了解和进行手动调整的能力，您可以在 高级网络钓鱼防护 中安全地实施快速 DMARC 策略，拒绝来自您自己的域的不可靠邮件。

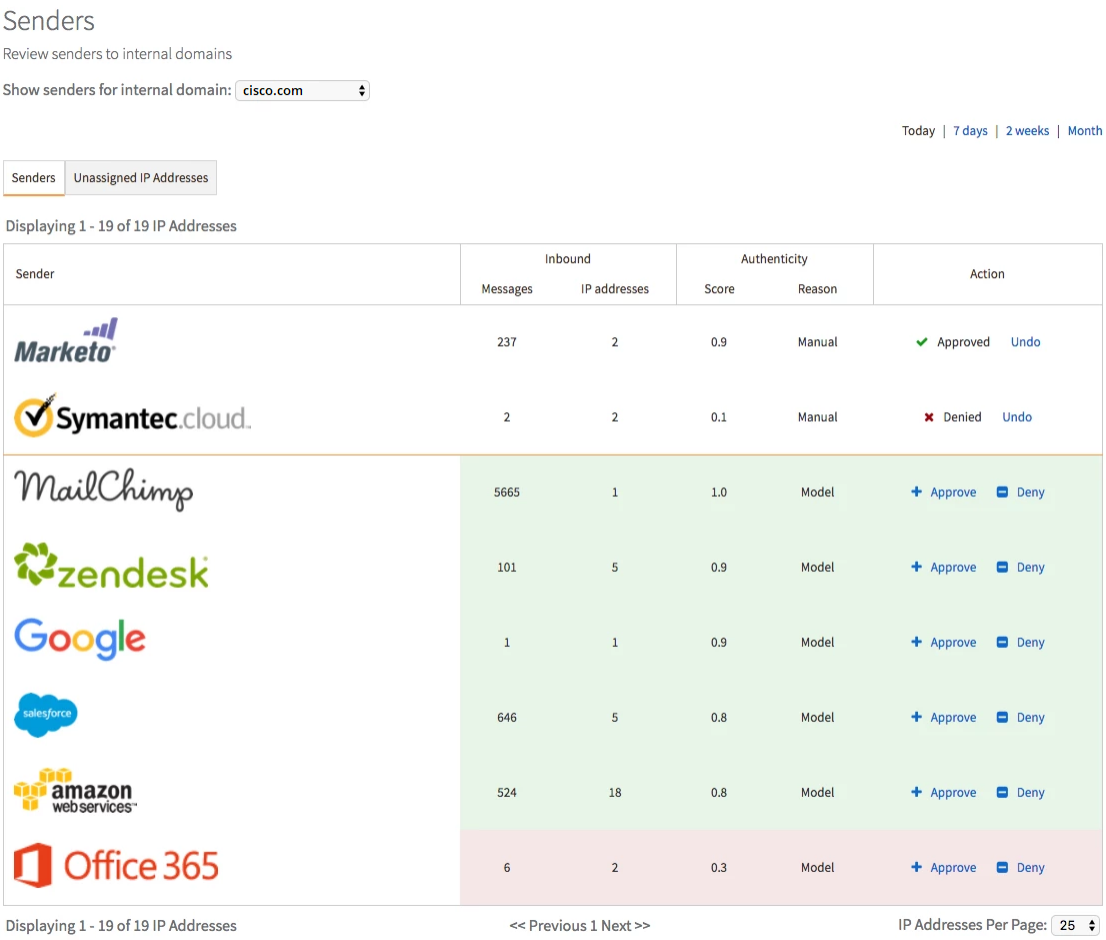
管理发件人

导航至管理 > 发件人查看您的域的常见发件人。该页面将默认过滤出数量最高的内部域并显示今天的数据。

要更改您正在查看的域，可以点击域名旁的向上/向下箭头。

您已在“分析”>“域”页面中标记为“内部”的任何域都将显示于此处的域列表中。

该页面还将默认设置为查看发件人，如下图所示。要查看未分配给常见发件人的 IP 地址，请点击“未分配的 IP 地址”选项卡。



“发件人”页面

各列的含义和用途

发件人：常见发件人的名称/徽标。点击发件人将向下深入一级，显示来自单个 IP 的邮件计数。

入站 - 邮件：在指定时段内发现的来自该域/发件人组合的邮件数。

入站 - IP 地址：在指定时段内发现从该域/发件人组合发送那些邮件的 IP 地址数。

真实性 - 评分：这是来自该发件人/域组合的 Agari 发件人建模的平均全局真实性评分。

此处显示的真实性评分是整个时段内在整个 Agari 平台中发现的来自与该发件人/域组合关联的所有 IP 的所有邮件的平均值。因此，当您深入查看具体邮件时，单独一封邮件的真实性评分略有变化是意料之中的正常情况。

真实性 - 原因：我们如何确定真实性评分。

手动 表示手动批准或拒绝发件人。真实性平均分不会在批准或拒绝某个发件人或 IP 地址后立即更改，但来自该发件人/域或 IP/域组合的新邮件会在更改后数分钟内开始得到真实性评分 1.0(如果批准) 或真实性评分 0(如果拒绝) 。

建模 表示评分是根据 高级网络钓鱼防护 的发件人建模计算的。

经过身份验证 表示发现来自该发件人/域组合的大多数邮件正在通过具有完全 DMARC 一致性的身份验证标准。

操作：如果要批准或拒绝发件人或撤消以前的批准或拒绝，以下是您可以执行的操作。

撤消 会将发件人的状态恢复为 高级网络钓鱼防护 的发件人建模功能开始建模时的状态。您可以随时撤消批准或拒绝。

批准 将明确批准该域的发件人，确保 高级网络钓鱼防护 将今后来自该发件人的邮件视为真实可靠的邮件。

拒绝 将明确拒绝该域的发件人，确保 高级网络钓鱼防护 将今后来自该发件人的邮件视为不可靠的邮件。

使用快速 DMARC 管理发件人

与公共 DMARC 策略一样，在快速 DMARC 中，您也必须对发件人正确执行身份验证才能安全地实施策略，将不可靠的邮件从您的域中删除或隔离。

区别在于，快速 DMARC 的发件人管理既快速又简单。您只需查看内部域的发件人和 IP，了解 高级网络钓鱼防护 如何对其建模。如果您同意建立的模型，则无需执行进一步操作，但也可以选择明确批准大批量发件人。如果有些发件人难以使用公共 DMARC 匹配其身份，您也不必担心快速 DMARC 在这方面的问题。无需联系发件人并实施 DNS 更改；只需在您的“发件人”页面上点击“批准”即可完成操作。

当您熟悉 高级网络钓鱼防护 中的发件人操作后，您可以转到“管理”>“策略”页面并设置用于实施的快速 DMARC 策略。

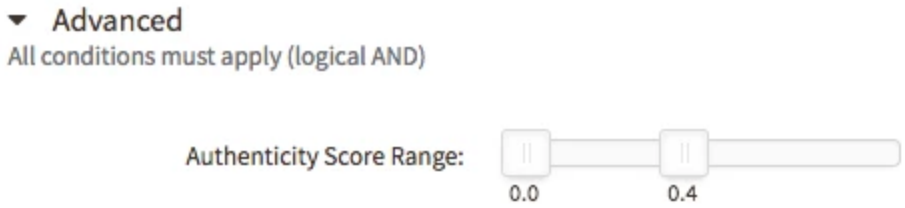
从 2018 年 1 月开始，自注册的客户有已经为您创建好的默认快速 DMARC 策略。

1. 转至管理 > 策略。
2. 点击快速 DMARC 策略名称。
3. 在“策略名称”下，将滑块移到启用。
4. 向下滚动到“操作”部分为此策略设置实施操作并/或启用策略匹配警报。
5. 点击保存。

2018 年 1 月之前在 高级网络钓鱼防护 中设置的客户并未获得快速 DMARC 策略。您可以通过以下步骤创建快速 DMARC 策略：

1. 转至管理 > 策略。
2. 点击创建策略。
3. 在策略名称中输入“快速 DMARC”。
4. 向下滚动到域标签并点击空文本框。从可用域标签列表中选择内部。
5. 向下滚动并打开高级切换开关。

6. 将真实性评分范围的上限移到 0.4。结果应如下所示：



7. 点击保存。

地址组

地址组是一个或多个(最多 1000)电子邮件地址的命名组。地址组通常在策略中使用，可用于以下原因：

- 确定一组用户的欺骗。在策略的发件人字段中指定地址组时，策略将匹配地址组成员的显示名称欺骗。默认情况下，识别为显示名称欺骗的邮件的可信度评分将降低。要对地址组进行策略匹配，但不影响可信度评分，请清除使用此组影响邮件评分策略设置。下面提供了收件人字段中地址组匹配的详细示例。
- 基于邮件收件人组过滤策略。在策略的收件人字段中指定地址组时，策略将仅在邮件收件人包含在此地址组中时进行匹配。在收件人字段中使用地址组不会影响邮件评分。
- 基于回复收件人地址组过滤策略。在策略的回复收件人字段中指定地址组时，策略将仅在回复收件人地址包含在此地址组中时进行匹配。在回复收件人字段中使用地址组不会影响邮件评分。

创建新组织时，将为您预先创建三个地址组：

- 高管(自动与*高管冒充者*策略关联，请参阅"默认策略" 在本页 54了解详细信息)
- 首席级高管(自动与*首席级高管冒充者*和*发送到首席级高管的可疑邮件*策略关联，请参阅"默认策略" 在本页 54了解详细信息)
- 主要合作伙伴和供应商(自动填充合作伙伴或供应商标签域中的最多 1000 个电子邮件地址，请参阅"域标签" 在本页 50了解详细信息)

在设置新组织时，您首先应完成的任务之一是在这些地址组中填充管理人员和首席级高管的电子邮件地址，然后配置关联策略。

“主要合作伙伴和供应商”地址组每周自动更新。高级网络钓鱼防护 将检测合作伙伴和供应商处定期与您的组织中的员工通信的个人(来自标记为“合作伙伴”或“供应商”的域，请参阅"域标签" 在本页 50了解详细信息)，并在“主要合作伙伴和供应商”地址组中最多填充 1000 个此类人员。

地址组例外情况

例外列表中的地址用于指定地址组中人员的“已知正常”电子邮件地址或个人电子邮件地址以免误报。

例如，假设要从地址 <yourco_announce@example.com> 使用您公司高管的名称发送合法邮件。您可以将该电子邮件地址添加到“高管”地址组的例外列表中。现在，当检测到来自 <yourco_announce@example.com> 的真实邮件时，系统不会根据此地址组触发警报。

例外列表中的地址永远不会标记为冒充者，除非邮件本身不可靠，而且只有当发件人和回复收件人条件引用地址组时才会考虑这些地址。

您可以添加 messenger@webex.com 或 reply@chatter.salesforce.com 等地址，以便地址组中的用户被合法欺骗时（例如“John Doe <messenger@webex.com>”或“John Doe <reply@chatter.salesforce.com>”），相应条件不进行匹配。

您还可以添加可能与上述地址共用 Friendly From 的个人地址，例如“johndoe@gmail.com”。

某些电子邮件服务根据 Sieve 过滤标准使用“+”地址。在此类情况下，电子邮件地址的本地部分将随地址中“+”后面的随机文本字符串而变化，这会导致在地址组中设置例外的做法产生问题。例如“John Doe <notifications+2hef98h2uibf8h@yammer.com>”。在此类情况下，地址组匹配将自动忽略“+”以及“+”和“@”之间的所有字符。因此，您可以仅在例外列表中添加“notifications@yammer.com”以进行忽略，这样它就不会匹配 John Doe 显示名称。

某些邮件将自动例外于 思科 的地址组显示名称匹配。例如，通过身份验证并来自于标记为“内部”、“合作伙伴”或“服务”的邮件不会触发地址组匹配。

地址组示例

此部分说明了地址组和策略如何共同工作。

策略“发件人”字段中的地址组

当策略的发件人字段引用了地址组时，将使用组中用户的名字和姓氏来确定传入电子邮件中组成员的冒充者。

例如，您的天才地址组包括 Albert Einstein <aeinstein@genius.com>，此组在名为天才欺骗的策略中使用。由于 aeinstein@genius.com 是其合法的业务地址，因此，任何时候在传入电子邮件中发现来自“Albert Einstein <aeinstein@genius.com >”的真实电子邮件，高级网络钓鱼防护 都不会触发此策略，因为这是 Albert Einstein 的已知正常电子邮件来源。

但是，如果发现来自 Albert Einstein <genius_spoofer@not-a-genius.com > 的电子邮件传入您的组织，高级网络钓鱼防护 将触发天才欺骗策略的策略匹配。

如果 Einstein 先生有时使用他的个人 AOL 地址 <IQ160@aol.com> 向组织发送电子邮件，该怎么办？这正是例外列表的用途。如果将 IQ160@aol.com 添加到例外列表，则来自“Albert Einstein <IQ160@aol.com>”的真实电子邮件也不会触发天才欺骗策略的策略匹配。

策略“收件人”字段中的地址组

当策略的收件人字段引用地址组时，这只是用于为策略过滤收件人。此策略仅在地址组中包含收件人地址时应用。

例如，您的天才地址组现在包含 Albert Einstein <aeinstein@genius.com> 和 Stephen Hawking <shawking@genius.com>。如果现在创建名为发送到天才的不可信邮件的策略，并将天才地址组置于此策略的收件人字段，则此策略将仅匹配符合信任条件并将 aeinstein@genius.com 或 shawking@genius.com 作为收件人的邮件。例外不适用于在收件人字段中使用地址组的情况。

创建地址组

一个地址组可以由单个的电子邮件地址组成，每次可添加一个；如果您连接到 Azure Active Directory，则地址组可包含现有的 Active Directory 组。

从单个电子邮件地址创建地址组

1. 转至管理 > 地址组。
2. 点击创建地址组。
3. 输入名称。该名称应反映您计划放入组中的电子邮件地址。
4. 添加一个或多个地址：
    1. 请确保已选择了个人选项卡。
    2. 输入名字、姓氏和有效的电子邮件地址。
    3. 点击添加。
5. 如果要添加例外电子邮件地址，请每次输入一个有效的电子邮件地址，并在输入每个地址后点击添加。
6. 点击创建。

从 Azure Active Directory 组创建地址组

1. 转至管理 > 地址组。
2. 点击创建地址组。
3. 输入名称。该名称应反映您计划放入组中的电子邮件地址。
4. 点击通过 Azure AD 选项卡。
5. 点击 Azure AD 组字段。
6. 选择一个 Active Directory 组。包含名字和姓氏的 Active Directory 组中的姓名和电子邮件地址将添加到地址组列表中。
7. 如果要添加例外电子邮件地址，请每次输入一个有效的电子邮件地址，并在输入每个地址后点击添加。
8. 点击创建。

将电子邮件地址添加到地址组

1. 转至管理 > 地址组。
2. 点击地址组的名称。
3. 在添加地址部分中，输入名字、姓氏和电子邮件地址。
4. 点击添加。
5. 点击保存。

从地址组中删除电子邮件地址

1. 转至管理 > 地址组。
2. 点击地址组的名称。
3. 在添加地址列表中，点击电子邮件地址旁边的 。
4. 点击保存。

编辑地址组

如果地址组由单个地址组成，则可以添加、编辑或删除任何地址组条目。如果将地址组链接到 Azure Active Directory，则只能切换地址组中使用的 Active Directory 组。

编辑由单个电子邮件地址组成的地址组

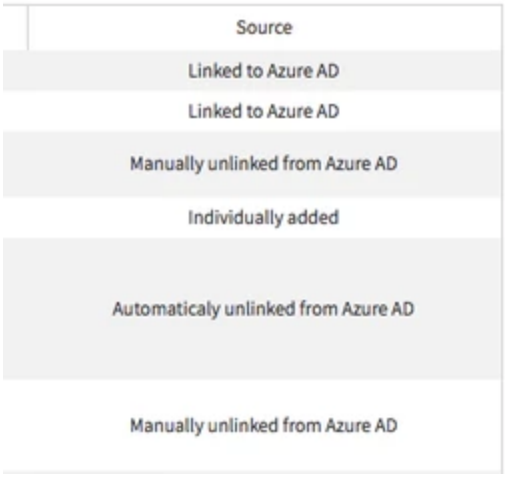
1. 转至管理 > 地址组。
2. 点击“来源”为“单独添加”的地址组的名称。
3. 进行所需的更改。您可以执行以下操作：
   - 更改地址组名称。
   - 输入名字、姓氏和有效的电子邮件地址，然后点击添加，向地址组中添加成员。
   - 点击地址列表中的一个名称旁边的 ，从地址组中删除成员。
   - 输入有效的电子邮箱地址，然后点击添加，以添加例外项。
   - 点击例外列表中的一个名称旁边的 ，以删除例外项。
4. 点击保存。

编辑链接到 Azure Active Directory 的地址组

1. 转至管理 > 地址组。
2. 点击“来源”为“与 Azure AD 关联”的地址组的名称。
3. 进行所需的更改。您可以执行以下操作：
   - 更改地址组名称。
   - 在 Azure AD 组字段中点击，然后选择 Active Directory 组。
   - 解除同步地址组的关联。
   - 输入有效的电子邮箱地址，然后点击添加，以添加例外项。
   - 点击例外列表中的一个名称旁边的 ，以删除例外项。
4. 点击保存。

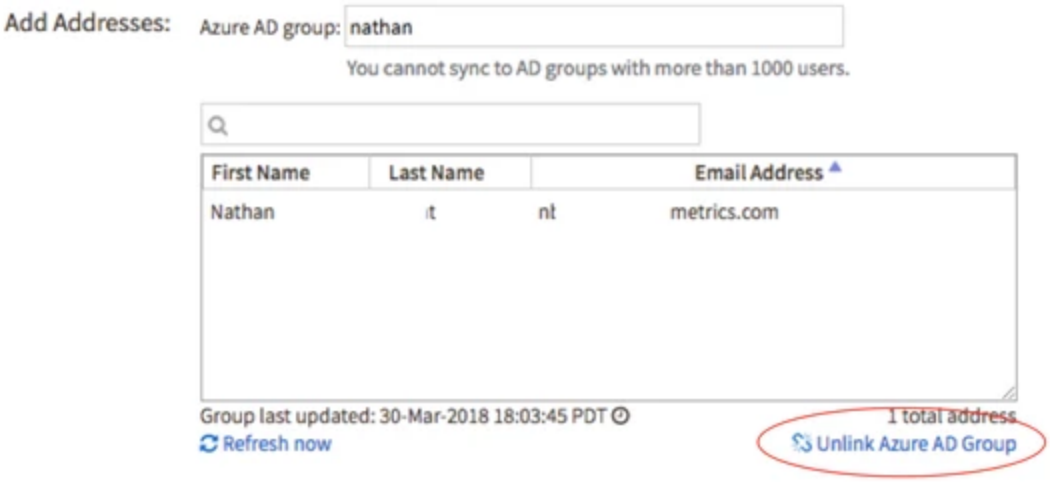
解除地址组与 Azure Active Directory 的关联

您可以通过查看“管理”>“地址组”页面中的“来源”列得知地址组已与 Azure Active Directory 同步。您将看到与 Azure AD 关联。其他状态包括单独添加、已手动解除与 Azure AD 的关联和已自动解除与 Azure AD 的关联。



地址组索引页面中的“来源”列

1. 点击已关联组的名称以转到“编辑地址组”页面。在名称框下方的右侧，您将看到解除 Azure AD 组的关联链接。



2. 点击解除 Azure AD 组的关联链接。这将阻止该组与 Azure AD 进一步同步，但当前组成员身份保持不变。此时，您可以手动修改该组，且下次同步不会覆盖您的修改。
3. 点击保存。

删除地址组

不能删除策略中正在使用的地址组。

1. 转至管理 > 地址组。
2. 点击地址组的名称。
3. 在页面底部，点击删除 [地址组名称] 链接。
4. 点击确定。

Azure Active Directory 与地址组同步

通过将 高级网络钓鱼防护 地址组与 Azure Active Directory 组同步，更高效地管理基于地址组的策略。高级网络钓鱼防护 会自动将 Azure AD 组中的成员纳入同步的 高级网络钓鱼防护 地址组，因此您不再需要担心手动更新。

要了解如何在策略中使用地址组，请参阅"策略" 在本页 53。

Azure AD 组同步失败通知

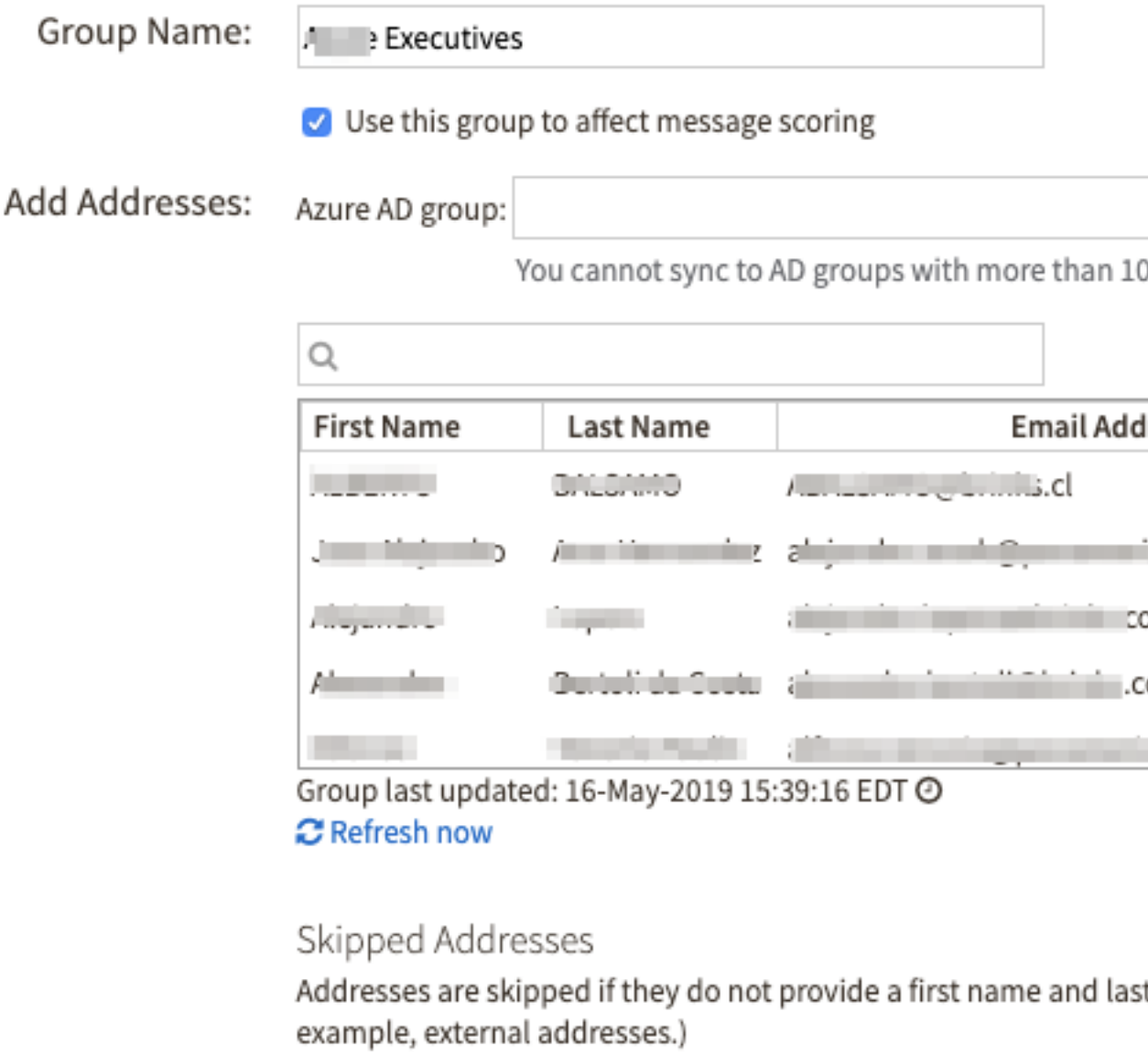
设置同步的地址组之后，建议您注册有关常规同步作业失败的系统通知。

1. 转至管理 > 策略。
2. 点击系统通知选项卡。
3. 向下滚动至“策略”部分，然后选中Azure AD 同步在一天内无法同步地址组复选框。
4. 点击保存。

有关详细信息，请参阅"通知" 在本页 53。

跳过的地址

当 高级网络钓鱼防护 与某个 Azure Active Directory 地址组同步，但此地址组中有条目缺少名字、姓氏或电子邮件地址时，则这些条目将不会包括在地址组中。高级网络钓鱼防护 会向地址组添加“跳过的地址”部分，并在此部分中列出这些条目。



地址组中“跳过的地址”部分。

管理

章 4

高级网络钓鱼防护 管理包括定义组织的设置、查看组织中的活动以及管理组织中的高级网络钓鱼防护 用户。

您可以对组织设置进行更改，查看审计追踪，并仅在拥有组织管理员角色的情况下管理用户。

审计跟踪

高级网络钓鱼防护 创建详尽的审计追踪，以记录和验证组织中的所有活动。您的组织(请参阅"查看组织活动" 向下) 和组织中每个用户(请参阅"查看用户活动" 在本页 87) 的审核活动日志页面上均按时间逆序列出所有活动。列表中使用图标对活动类型进行分类。

图标	活动类别
	表示用户已登录 高级网络钓鱼防护 或 高级网络钓鱼防护 中的一个组织。
	表示用户已从 高级网络钓鱼防护 或 高级网络钓鱼防护 中的一个组织注销。
	表示用户已创建、编辑或删除用户帐户、策略或地址组。
	表示用户已创建、编辑、删除域或对其执行了其他操作。
◆	表示用户已创建、编辑、删除发件人或对其执行了其他操作。
	表示用户已创建一个报告请求。
	表示用户已创建、编辑、删除域组或对其执行了其他操作。
	表示用户执行了组织级活动，例如接受 思科服务条款 (TOS) 或更改组织设置。

查看组织活动

高级网络钓鱼防护 创建详尽的审计追踪，以记录和验证组织中的所有活动。

您必须拥有组织管理员角色，才能查看组织活动。

1. 转到管理 > 组织。
2. 点击组织名称下的审核链接。

高级网络钓鱼防护 组织中的所有活动按时间倒序列出。列表中使用图标对活动类型进行分类。有关每个图标的说明，请参阅"审计跟踪" 向上。

用户帐户

用户帐户定义 高级网络钓鱼防护 用户的凭证和访问能力。高级网络钓鱼防护 使用基于角色的访问控制 (RBAC)，使您可以为每个用户分配一个或多个角色以访问 高级网络钓鱼防护 功能。

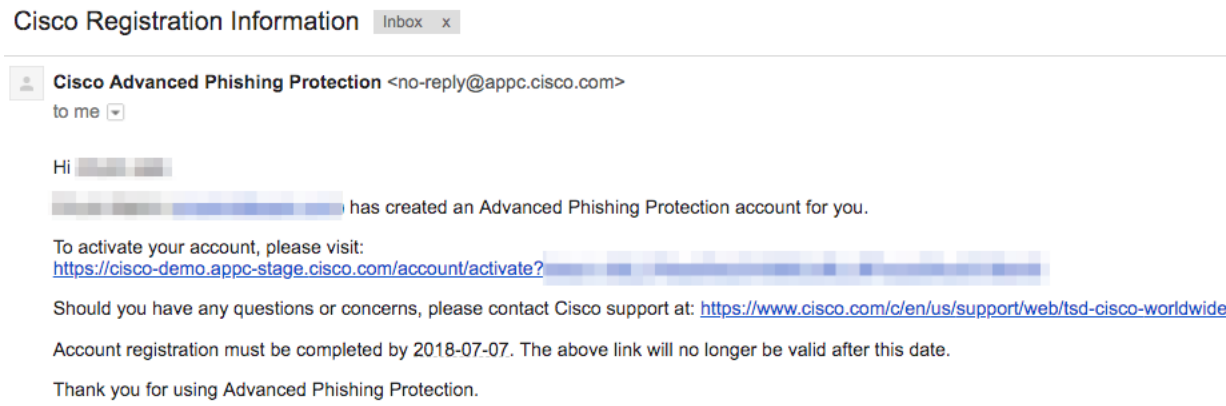
思科 支持人员无权在您的 高级网络钓鱼防护 组织中创建、启用、编辑或删除用户帐户。

创建用户帐户

只有具有组织管理员角色的用户才能创建用户帐户。

1. 转到管理 > 用户。
2. 点击创建用户。
3. 输入全名和电子邮件地址。

   您必须输入有效的电子邮件地址。邀请电子邮件将发送到该电子邮件地址。邀请电子邮件包含一个唯一的链接，新用户必须点击该链接才能验证新帐户。


Cisco Registration Information Inbox x

Cisco Advanced Phishing Protection <no-reply@appc.cisco.com>
to me

Hi [redacted]

[redacted] has created an Advanced Phishing Protection account for you.

To activate your account, please visit:
https://cisco-demo.appc-stage.cisco.com/account/activate?[redacted]

Should you have any questions or concerns, please contact Cisco support at: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide

Account registration must be completed by 2018-07-07. The above link will no longer be valid after this date.

Thank you for using Advanced Phishing Protection.

   邀请电子邮件示例。

4. 选择是否要允许此用户帐户使用辅助身份验证(密码形式的本地身份验证)配合或取代单点登录(有关详细信息，请参阅"单点登录 (SSO)" 在本页 91)。如果选择此选项，则还要选择：
   - 仅当单点登录失败时 - 允许此用户帐户在单点登录不起作用时输入密码。
   - 独占(不通过单点登录进行身份验证) - 要将此用户帐户限制为仅本地授权，即用户始终必须输入用户名和密码，并且不能使用 SSO。
5. 选择您希望用户帐户拥有的角色。有关详细信息，请参阅"用户角色" 在本页 89。
6. 点击邀请新用户。

系统将向您输入的电子邮件地址发送一封电子邮件，其中包含用于验证用户并让用户设置帐户密码的链接。

您的销售代表必须启用第一个管理员帐户，用于访问 高级网络钓鱼防护。通常，系统会为该第一个帐户分配多个管理员角色，包括组织管理员角色，以便您可以为您的组织创建其他用户帐户。

编辑用户帐户

1. 转到管理员 > 用户。
2. 点击用户的姓名。
3. 对用户信息和设置进行任何所需更改。有关详细信息，请参阅"用户帐户设置"下一页。
4. 点击更新。

登录到 高级网络钓鱼防护

在登录到 高级网络钓鱼防护 之前，您必须已创建自己的帐户(请参阅"创建用户帐户"上一页)，然后必须点击欢迎电子邮件中的链接，以验证您的电子邮件地址。

1. 在受支持的浏览器中，转到 高级网络钓鱼防护 URL：https://appc.cisco.com。
2. 输入您的电子邮件地址。
3. (可选) 如果您的组织未启用单点登录 (SSO)，请输入您的密码。
4. 点击下一步。

查看用户活动

高级网络钓鱼防护 创建详尽的审计追踪，以记录和验证所有用户活动。您必须具有审核用户角色才能查看用户活动。

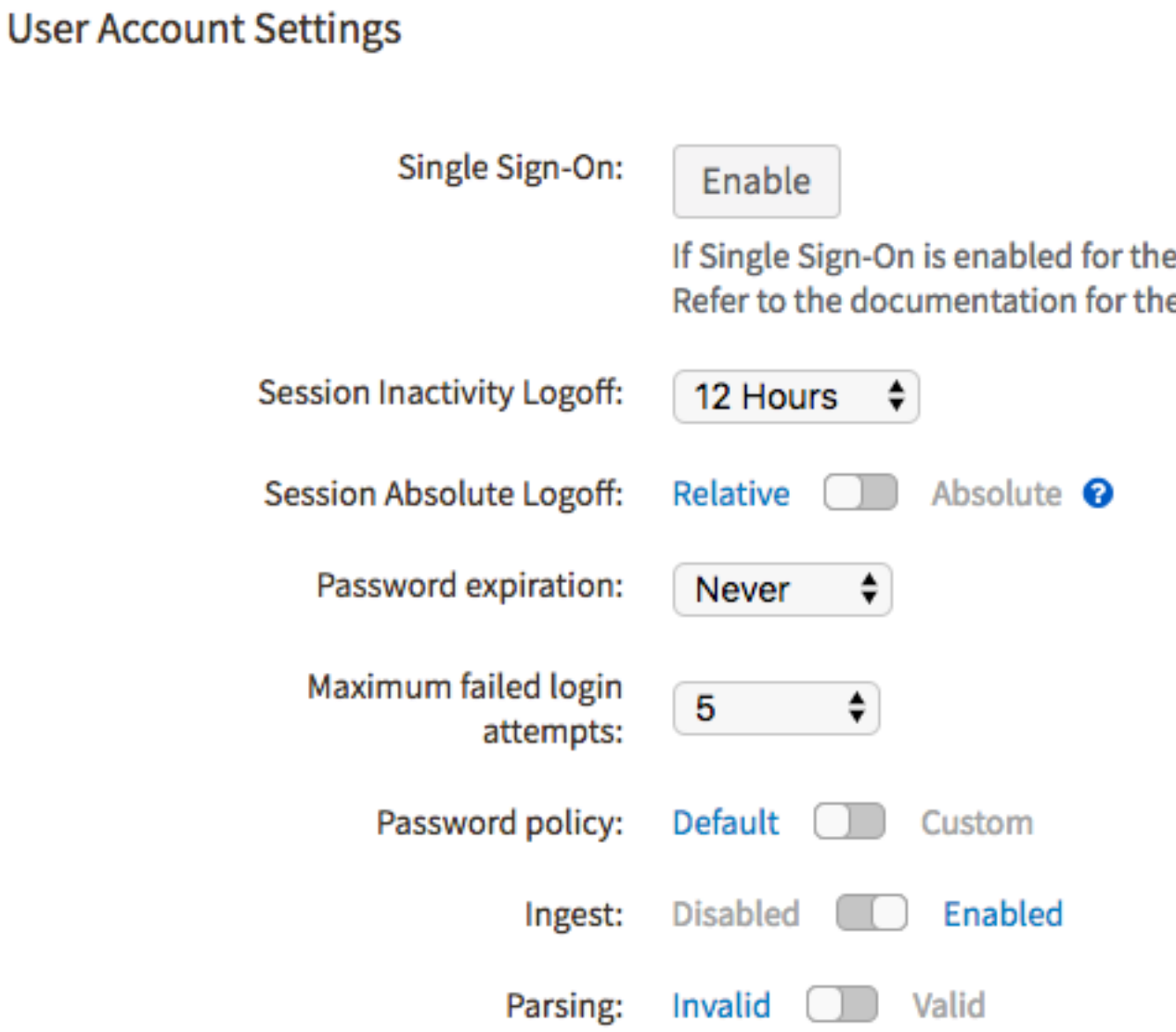
1. 转到管理员 > 用户。
2. 点击用户名下的审核链接。

高级网络钓鱼防护 组织中的所有用户活动按时间倒序列出。列表中使用图标对活动类型进行分类。有关每个图标的说明，请参阅"审计跟踪"在本页 85。

您还可以点击“下载 CSV”，下载包含所有用户活动记录的逗号分隔值文本文件。

配置全局用户帐户设置

全局用户帐户设置包括用户的登录方式、注销时间和密码策略。



“用户帐户设置”部分

1. 转到管理 > 组织。
2. 点击组织名称。
3. 对用户帐户设置进行任何所需更改。有关详细信息，请参阅组织设置中的“用户帐户设置”部分。
4. 点击保存。

用户帐户设置

本主题介绍 高级网络钓鱼防护 用户帐户的设置。

用户信息

设置	说明
全称	在用户登录后显示在每个页面顶部以及显示在活动的审核日志中的用户全名，与用户列表中的名称一致。

设置	说明
电子邮件	用户的电子邮件地址，其用于用户的登录凭证，以及报告和警报的目标地址。请注意，此电子邮件地址用于接收包含初始激活令牌的邀请邮件。
辅助身份验证	如果您的组织使用单点登录 (SSO)，则此选项可确定辅助身份验证(用户名和密码)是可选的还是必填的。如果不选择此选项，则始终使用 SSO，并且如果 SSO 提供程序在登录时不可用，则无法访问应用程序。如果选择此选项，系统会提供两个附加选项： • 仅当 SSO 失败时：如果 SSO 提供程序失败，系统会提示用户输入密码字段 • 独占(不通过 SSO 验证身份)：系统始终提示用户输入密码(不使用 SSO)

此外，用户将分配到一个或多个角色。有关 高级网络钓鱼防护 用户角色的信息，请参阅"用户角色" 向下。

用户角色

本主题介绍在 高级网络钓鱼防护 中可分配给用户帐户的用户角色。高级网络钓鱼防护 中的角色分为两类：

- 用户角色，这是只读角色，允许用户仅查看 高级网络钓鱼防护 中的特定区域，即常见“CRUD”(创建、读取、更新、删除)范例中的“R”。
- 管理员角色，允许用户更改 高级网络钓鱼防护 中的各个区域，即“CRUD”中的“C”、“U”和“D”。

默认情况下，角色是分层的。也就是说，为用户帐户分配一个角色时，该帐户也会自动分配到所选角色“下”的所有角色。可以手动取消分配所选角色下的角色。

下表按分层结构的顺序列出了可用角色。

角色	说明
	管理员角色
组织管理员	组织管理员将默认拥有只读用户、审核用户和用户管理员的所有权限，除非专门取消选中这些角色。此外，组织管理员还可以对组织设置、策略和地址组进行更改： • 在“管理”>“组织”页面中查看并编辑组织设置。 • 在“管理”>“策略”页面中查看、创建并编辑策略配置。 • 在“搜索邮件”页面中创建按需策略(如果适用于客户的配置)。 • 在“管理”>“发件人”页面中查看、批准、拒绝或撤消发件人和 IP。 • 在“管理”>“传感器”页面中查看指标并更新配置。 • 在“管理”>“地址组”页面中查看、创建并编辑地址组。
用户管理员	用户管理员将默认拥有只读用户和审核用户的所有权限，除非专门取消选中这些角色。此外，审核用户可以： • 在“管理”>“用户”页面中创建并编辑用户。

角色	说明
	用户角色
审核用户	审核用户将默认拥有只读用户的所有权限，除非专门取消选中只读角色。此外，审核用户可以： • 在“管理”>“用户”页面中查看并搜索用户审核日志。 只读用户可以在 高级网络钓鱼防护 中搜索和查看数据，但不能在任何位置进行更改或编辑。
只读用户	• 在“分析”菜单下的所有页面(“概述”、“邮件”、“域”、“IP 地址”和“搜索邮件”) 中查看并搜索数据。 • 在“管理”>“策略”页面中查看策略配置。不能创建新策略和按需策略，也不能编辑策略。 • 在“管理”>“报告”页面中查看报告。 • 在“管理”>“发件人”页面中查看发件人。不能“批准”、“拒绝”或“撤消”发件人或 IP。 • 在“管理”>“传感器”页面中查看指标和配置。不能修改传感器配置。 • 在“管理”>“用户”页面中查看自己的用户设置并启用 API 凭证。不能更改自己的用户角色。 • 在“管理”>“地址组”页面中查看地址组配置。不能创建或编辑地址组。

角色示例

本主题包含如何为某些特定使用案例配置角色的示例。

创建可接收通过邮件发送的报告和警报的只读用户

当您为某个用户选择只读角色时，默认情况下还会选择报告收件人角色。若要创建还可以接收通过电子邮件发送的报告和警报的只读用户，只需接受这些默认值。如果您取消选择“报告收件人”角色，则只读用户不会显示在可向其发送报告的用户列表或可为其订用警报的用户列表中。

创建具有只读访问权限以及可以创建其他只读用户的用户管理员

选择“用户管理员”作为该用户的最高访问角色。由于您希望此用户管理员只能创建和管理具有只读访问权限及更低权限的用户，因此您需要在“用户管理员”角色正下方的“管理用户”框中取消选择“所有权限”选项。然后，选择“只读”和“报告收件人”选项。现在，该用户将能够创建和管理具有只读及更低权限的用户。

创建仅可以创建其他用户的用户管理员

创建仅用于创建或编辑其他用户的用户管理员。此角色无法使用本产品来查看数据或接收报告和警报。

创建新用户，为您要创建的用户选择“用户管理员”角色，然后取消选择在“用户管理员”下自动选择的所有角色。系统会允许您创建的用户管理员创建具有“所有权限”的其他用户，除非您在“用户管理员”角色下面的“管理用户”框中更改相关设置。

如果您希望此新用户管理员能够创建除组织管理员和用户管理员之外的所有角色，请选择“x”以删除“所有权限”。然后，使用“选择角色类型”选项来选择除“组织管理员”和“用户管理员”之外的每个角色。

单点登录 (SSO)

高级网络钓鱼防护 现在包括供您启用单点登录(“SSO”)机制的功能，以便通过 SAML 2.0 协议为组织中的用户进行身份验证。

借助单点登录机制，您可以：

- 打造“一键”登录体验。您可以将您现有的公司登录身份(帐户)与 高级网络钓鱼防护 用户名绑定，无需单独的 高级网络钓鱼防护 密码。
- 集中撤销用户访问权限。当员工离开公司时，您可以在 SSO 提供程序内删除 高级网络钓鱼防护 访问权限，而不是在 高级网络钓鱼防护 内单个删除。
- 提供可选的辅助身份验证。您可以允许特定用户(例如，身份提供程序系统中不可用的承包商)只使用 高级网络钓鱼防护 中存储的凭证进行身份验证(这可以有效绕过单点登录机制)。您还可以允许特定用户仅当 SSO 身份识别服务发生故障时(例如停电期间)使用 高级网络钓鱼防护 中存储的凭证进行身份验证。

使用 SSO 登录

启用 SSO 后的用户登录过程将取决于 SSO 的实施方式。

- 对于身份提供程序启动的 SSO，用户不需要输入凭证或转到登录页。他们将通过您组织的身份识别服务提供程序发起连接并登录。
- 对于服务提供程序启动的 SSO，用户需要进入 高级网络钓鱼防护 登录页 (https://appc.cisco.com) 并输入其电子邮件地址。高级网络钓鱼防护 登录页不会显示密码字段，除非您启用辅助身份验证。(辅助身份验证允许用户根据需要通过密码登录。)相反，用户将被重定向至身份提供程序。如果用户尚未向身份提供程序验证身份，系统将提示他们进行身份验证(身份提供程序可能会在多个屏幕中提供身份验证。)用户向身份提供程序进行身份验证后，他们会再一次被重定向至 高级网络钓鱼防护 概述页面。

为您的组织启用单点登录

在开始之前，您必须从单点登录提供商处获取两条信息：

- SAML 2.0 终端 (HTTP) URL(在身份提供程序系统中，这有时称为“目的”或“SAML 收件人”。)
- 公共证书 (X.509)

您必须拥有组织管理员角色才能执行此任务。

1. 转到管理员 > 组织。
2. 点击编辑组织详细信息。
3. 在“用户帐户设置”部分中，选择启用单点登录。
4. 在确认消息中，点击确定。
5. 输入 SSO 参数：

单点登录参数	说明
名称标识符格式	选项如下： • urn:oasis:names:tc:SAML:1.1nameid-format:unspecified • urn:oasis:names:tc:SAML:1.1nameid-format:emailAddress • urn:oasis:names:tc:SAML:2.0nameid-format:persistent (default)
SAML 2.0 终端(HTTP 重定向)	输入您从单点登录提供商处获取的 SAML 2.0 终端 URL。
公共证书	输入单点登录提供商发给您的完整证书文本。(最简单的做法是复制粘贴。

6. 点击测试设置以验证您的身份提供程序所提供的终端 URL 和证书值。高级网络钓鱼防护 在您的输入位置调用身份提供程序和公共证书凭证。

   如果您尚未登录身份提供程序，可能需要接受身份提供程序的身份验证。

7. 点击保存设置。
8. 在确认消息中，点击确定。
9. 点击更新信息。

此时将启用单点登录并且：

- 所有现有用户将收到一封电子邮件，指示他们在访问 高级网络钓鱼防护 时使用其单点登录身份提供程序凭证。
- 当前已登录系统的用户 高级网络钓鱼防护 将继续会话而不中断；但是，他们将在以后尝试登录时被定向至身份提供程序。

应用编程接口

章 5

高级网络钓鱼防护 包括一个应用编程接口 (API)，允许贵组织内的开发人员以编程方式访问 高级网络钓鱼防护 中的数据。

高级网络钓鱼防护 API 基于使用 JSON 数据表示的 RESTful 原则构建。客户端使用 OAuth 2.0 协议对 API 请求进行身份验证。可为用户帐户分配一个 API 凭证，其中包含 API 客户端 ID 和客户端密钥。通过这些凭证提供的资源和数据直接与帐户管理员在 高级网络钓鱼防护 用户界面中分配给该用户的权限相关联。