思科高级网络钓鱼防护用户指南

2018 年 6 月 22 日

思科系统公司
www.cisco.com

思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices.

目 录

安装思科高级网络钓鱼防护传感器

简介

思科高级网络钓鱼防护传感器可以帮助您前所未有地深入洞察进入企业的流量。凭借**可信度分析**（思科独有的机器学习技术，基于组织的历史邮件流量）在技术上的支持，思科邮件安全网关可以对所有合法邮件发件人的独特行为建模，让您能够快速区分正常邮件与潜在恶意邮件。思科的数据平台基于对全球数十亿封邮件的分析而构建，它与可信度分析相结合，可以针对所有邮件以及所有向您的组织发送邮件的发件人，为您提供风险概况。

对存在风险的邮件（例如网络钓鱼企图或者可能并不含恶意负载或可疑链接的“企业邮件入侵”邮件）和已知的正常邮件加以清晰的划分。

思科高级网络钓鱼防护传感器可以捕获鱼叉式网络钓鱼，完善了传统的思科邮件安全网关解决方案，因为这种针对性强、攻击量小的零日攻击通常是传统的被动式思科邮件安全“层”的薄弱环节。

使用思科邮件安全网关内的策略引擎，您可以配置要向最终用户近乎实时发送的恶意邮件警报，甚至还可以将可能存在危险的邮件一起移出最终用户的收件箱。

支持

有关本指南的支持和/或问题/更新，请访问
http://www.cisco.com/support

如需安装或使用思科高级网络钓鱼防护传感器的相关支持，您可以直接通过以下邮箱与思科支持团队联系：support@cisco.com。

安装思科高级网络钓鱼防护传感器

思科高级网络钓鱼防护解决方案依靠高级网络钓鱼防护传感器来接收入站发送到您组织中的所有邮件的副本。

高级网络钓鱼防护传感器的目的是从您企业的入站邮件流中收集每封邮件的元数据，并将元数据中继到思科邮件安全网关云进行分析。高级网络钓鱼防护传感器旨在实现最小侵入性，并具备安全、轻型（需要最少的资源）和高性能的特点。

用于确定安装类型的问题

有几个基本的问题可以帮助您确定安装类型。

- **MX 传送至何处？**

  组织的 MX 记录是您的域的面向公众的邮件交换记录。MX 记录可能指向：

  - 思科邮件安全网关 - 安全的邮件网关。
  - Office 365 - Microsoft 的托管解决方案
  - Google - Google 的托管解决方案

- **入站邮件平台的第一跳是什么？**

  有些客户使用的是“分层”环境，其内部有一“跳”将邮件从 MX 记录环境的地址路由到第二个网关。例如，此“下一跳”可能是：

  - Google (G Suite)
  - Office 365 (O365)
  - 内部 Exchange
  - （有条件地）多个站点之一，每个站点各有内部 Exchange

- **所有用户邮箱的邮箱传送位于何处？**

  如果使用邮箱传送（最终用户邮箱的存储位置），则可能需要另一“跳”。例如，此问题的答案可能是：

  - 与邮件平台第一跳（上面的问题 2）相同的环境
  - 跨混合环境（Office 365 或内部 Exchange）
  - 取决于具体的邮箱（部分邮箱迁移的混合环境）

  有些客户使用的是混合环境，其中一些邮箱正从内部部署环境向托管环境过渡。

托管环境的问题

此外，如果您的环境托管在 G Suite 或 Office 365 中，以下问题还有助于确定您的高级网络钓鱼防护传感器安装策略：

- **这是同时包含 Office 365 与内部 Exchange 的混合环境吗？**

  混合环境允许用户邮箱从内部 Exchange 迁移到 Office 365

- **如果是这样，用户邮箱向 Office 365 迁移的过程当前处于什么状态？**

  邮箱迁移可能有 3 个阶段和关联的时间表

  - 迁移前 - 所有邮箱仍位于内部 Exchange 环境中
  - 部分迁移 - 一些邮箱已迁移至 O365，另一些仍位于内部 Exchange 环境中
  - 迁移后 - 所有邮箱均位于 O365 环境中

  了解客户端何时会将所有用户邮箱都迁移到 Office 365 环境中是实现以下目标的关键：

  - 最大限度提高您尽快使用所有思科高级网络钓鱼防护功能的能力。
  - 最大限度减少变更请求以及转变安装所产生的相关风险。

双重传送与内联安装

高级网络钓鱼防护传感器有两种可能的部署：**双重传送**和**内联**。

- **日志/API**

  如果要进行安装，双重传送是首选方法，因为它支持按需强制执行（适用于 Office 365 和 G Suite 客户）并可降低客户端变更管理带来的风险。

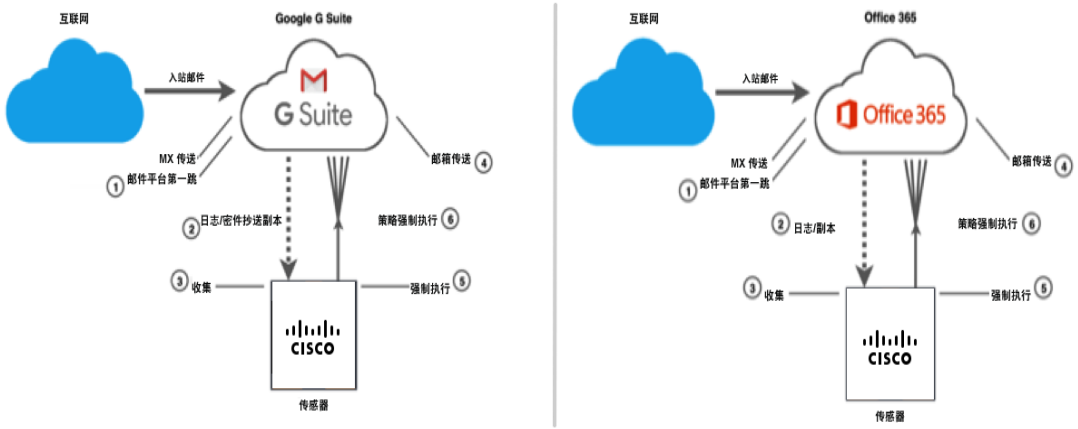
- **内联**

  内联传感器安装主要用于客户端邮箱尚未迁移到 Office 365 或 Google G Suite 的情况

双重传送

思科高级网络钓鱼防护传感器实质上是起 SMTP“邮件接收器”的作用，它通过 SMTP 接受邮件的副本并以流传输方式提取元数据。邮件正文和附件会被丢弃。没有任何 SMTP 邮件离开高级网络钓鱼防护传感器。双重传送通常用于 Office 365 和 G Suite 等托管邮件架构。

图 1-1　　使用日志记录/API 的双重传送安装的邮件流



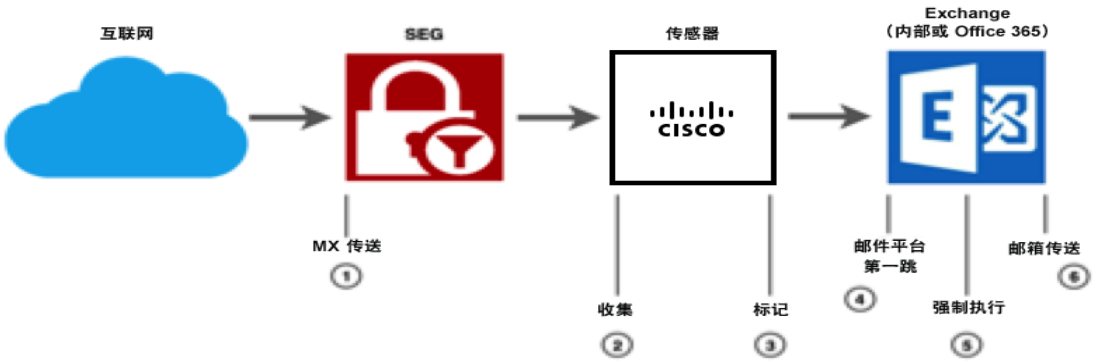
入站邮件被发送到邮件平台第一跳（思科邮件安全网关可能在其前面也可能不在其前面）：

1. Office 365 或 G Suite 将邮件的日志记录副本或密件抄送副本发送到高级网络钓鱼防护传感器并继续原件的传送。
2. 高级网络钓鱼防护传感器收集日志副本进行评分和策略评估。
3. Office 365 或 G Suite 将邮件原件传送至邮箱。
4. 传感器将强制执行策略，使用 API 访问各个邮箱。
5. 在邮箱中根据策略结果执行策略强制执行操作。

内联

在内联配置中，思科高级网络钓鱼防护传感器用作 MTA：它负责接受邮件并将其传送到下一跳（通常是另一个内部 MTA）。采用内联配置的客户可以根据思科高级网络钓鱼防护传感器添加的报头，使用下一跳 MTA 对传入邮件执行操作。

图 1-2　　内联安装的邮件流



1. 入站邮件被发送到位于思科邮件安全网关的 MX。
2. 思科邮件安全网关将邮件发送到下一跳的思科高级网络钓鱼防护传感器进行收集、评分和策略评估。
3. 高级网络钓鱼防护传感器使用策略结果标记邮件报头。
4. 高级网络钓鱼防护传感器将邮件发送到邮件平台第一跳。
5. Exchange 传输规则根据邮件报头中的标记强制执行策略操作。
6. 经过强制执行的邮件被传送至邮箱。

备注　在本指南中的一些屏幕截图中，思科高级网络钓鱼防护传感器可能会被称为“收集器”，这是它以前的名称。

将思科高级网络钓鱼防护传感器安装到您的基础设施中

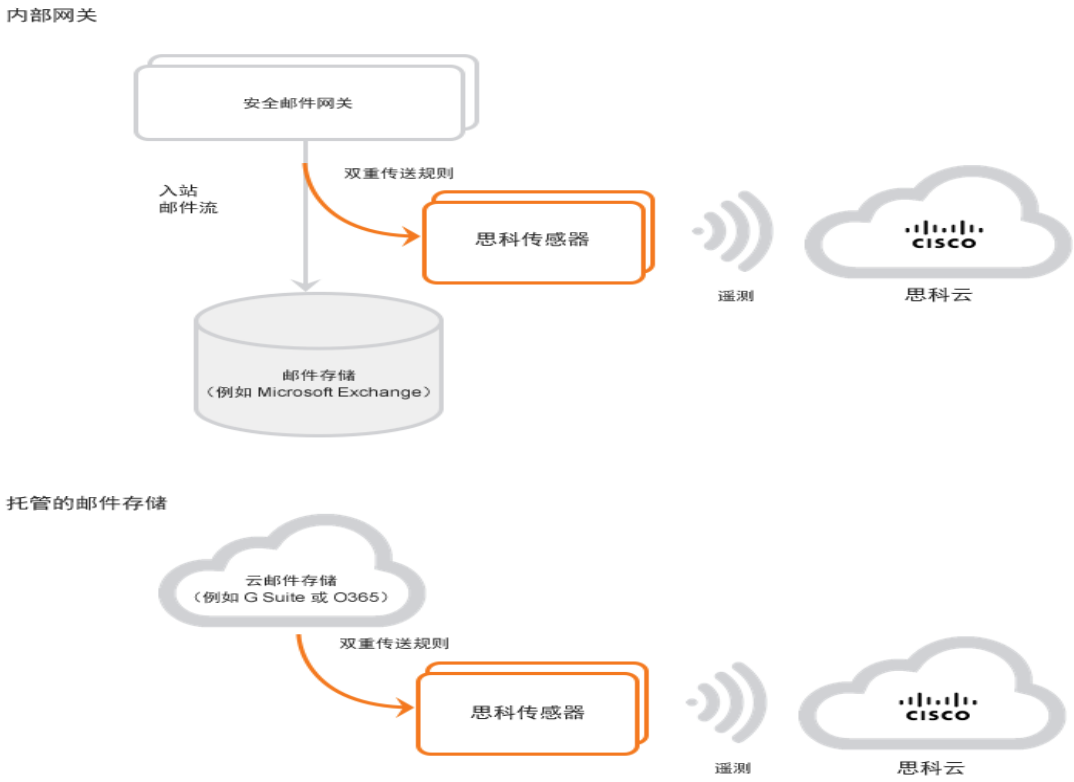
通常，思科高级网络钓鱼防护解决方案的客户会在自己的环境中调配主机系统，用于运行高级网络钓鱼防护传感器。（如果您愿意，思科可以代表您在单独管理的云中托管高级网络钓鱼防护传感器。如果您更愿意采用这种方法，请联系思科销售工程师。）

您应该将高级网络钓鱼防护传感器安装到基础设施中的如下位置：可以在邮件经过其他扫描（反垃圾邮件、防病毒、防恶意软件）*之后*，接收内部传送的邮件的副本。适用于 IronPort 的高级网络钓鱼防护传感器只应“看到”已通过这些过滤器并被认为值得传送的邮件。

如果您使用的是托管基础设施（例如 Google Apps 或 Microsoft Office 365），也适用同样的理论：您应该在所有其他过滤和扫描完成后，将邮件流副本定向到思科高级网络钓鱼防护传感器。

双重传送传感器架构和数据流

图 1-3　　双重传送传感器架构

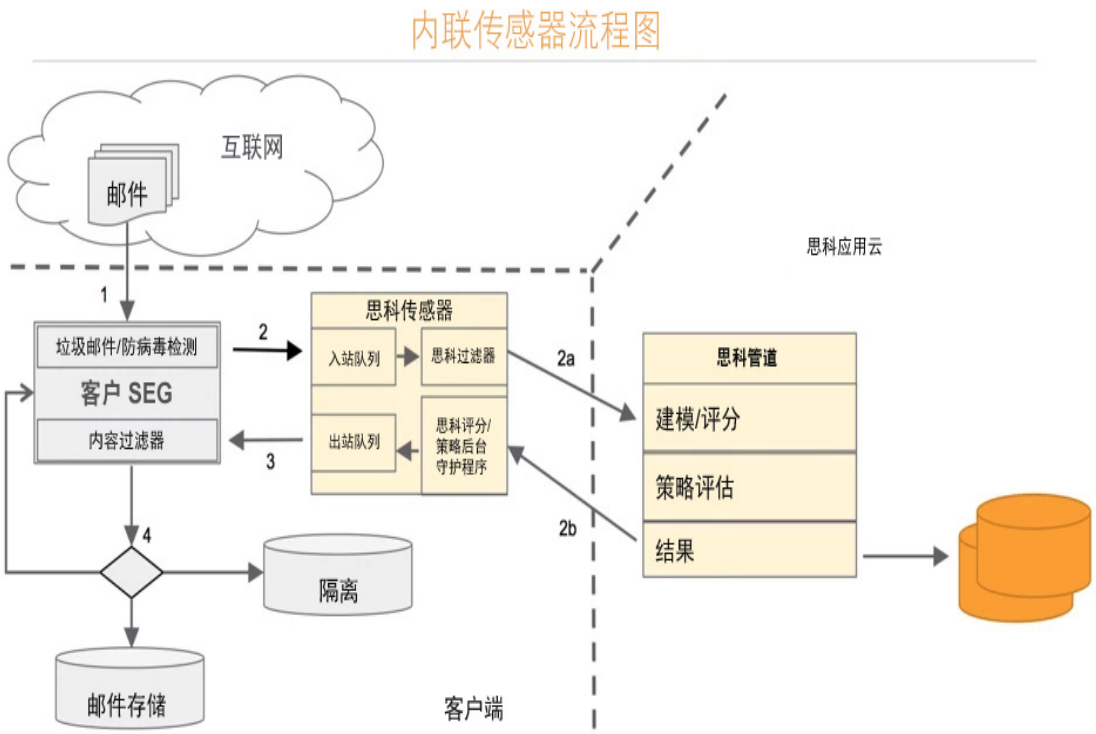


1. 邮件到达思科邮件安全网关或托管的邮件存储，并被接受进行垃圾邮件和病毒过滤。
2. 在第一级垃圾邮件和病毒过滤后，思科邮件安全网关通常在端口 25 上（但也可在安装思科高级网络钓鱼防护传感器时将此配置为不同的端口），通过 SMTP 连接将邮件副本（通过双重传送规则或日志记录功能）传送至思科高级网络钓鱼防护传感器。在入站邮件加入队列时，思科过滤器进程会解析要传输到思科管道中进行评分和策略评估的邮件数据。

   然后，使用端口 443 通过 HTTPS 连接将解析后的邮件数据发送到思科管道中。

内联传感器架构和数据流

图 1-4　　内联传感器架构



1. 邮件到达思科邮件安全网关，并被接受进行垃圾邮件和病毒过滤。

备注　邮件基础设施中通常在思科邮件安全网关前会有一个连接阻止步骤，用于阻止列入黑名单的 IP 地址发出的连接。（上图中未显示此步骤。）

2. 在第一级垃圾邮件和病毒过滤后，思科邮件安全网关通常在端口 25 上（但也可在安装思科高级网络钓鱼防护传感器时将此配置为不同的端口）通过 SMTP 连接将邮件传送至思科高级网络钓鱼防护传感器。

   在入站邮件加入队列时，思科过滤器进程会解析要传输到思科管道中进行评分和策略评估的邮件数据。

   a. 然后，使用端口 443 通过 HTTPS 连接将解析后的邮件数据发送到思科管道中。

   b. 在思科管道中对邮件进行评分和策略评估后，评估的结果会在强制执行队列中传回思科高级网络钓鱼防护传感器。思科高级网络钓鱼防护传感器会将这些结果写入新的邮件报头中。新的邮件报头将如下所示：

```
X-Agari-MsgInfo: 74771442-0e71-11e7-9bb3-0242ac110002;1490126610
X-Agari-Policy-Matched: Policy Name
X-Agari-Trust-Score: 1.0
```

   一封邮件中可能存在多个 X-Agari-Policy-Matched 报头。

X-Agari-Trust-Score 报头的值将为以下值之一：

- 0.0 - 10 之间的数值，表示可信度评分（0 为低，10 为高）。
- “None”（无）- 表示按照配置特意跳过对该邮件的评分
- “Unscored”（未评分）- 表示邮件评分超时，因此邮件在未评分的情况下传送。

然后，邮件将加入队列，以便从思科高级网络钓鱼防护传感器向外传送。

3. 通过 SMTP 将邮件传送至配置的下游 MTA 进行继续处理和传送。下游 MTA 可以是将邮件传送至思科高级网络钓鱼防护传感器的同一个系统，也可以是新的下游 MTA。

   建议当配置的下游 MTA 接收邮件时，将内容过滤器设置为读取新的 X-Agari 报头并根据这些报头中传达的策略和/或评分执行特定操作。

4. 根据最终内容过滤后的邮件性质，可以将邮件传送至最终邮件存储，传送至隔离区，重新传送回邮件流中进行进一步处理所需的点，或根本不传送（即，阻止）。

必备条件

在内部部署中，您可以选择裸机安装或在托管的虚拟机 (VM) 上安装高级网络钓鱼防护传感器。

思科高级网络钓鱼防护传感器由思科通过安装脚本（具有唯一密钥）分发给您的组织。安装脚本将安装通过 Docker 容器（请参阅 https://www.docker.com/what-docker）分发的传感器应用。容器将传感器应用封入完整的文件系统中，包含运行该应用所需的一切：代码、运行时间、系统工具和系统库。

您应该从思科销售代表处获取用于安装第一个高级网络钓鱼防护传感器的脚本。当您获取 Web 应用的访问权限后，您可以从“管理”>“传感器”页面获取用于安装其他传感器的脚本。此脚本具有唯一密钥供您的组织使用。

虚拟机硬件要求

操作系统	现代 64 位 Linux： • Red Hat Enterprise Linux 7.2 或更高版本 • CentOS 7.2 或更高版本 • Ubuntu 14.04 或更高版本
CPU	英特尔或 AMD x86_64 双核（最低） 4 核（建议）
内存	16 GB（最低） 32 GB（建议）
磁盘	50 GB（最低） 100 GB 以上（如果预计邮件数量多），分配给 /var 或 /var/opt/agari

防火墙要求

在您的基础设施中安装高级网络钓鱼防护传感器时，需要能够与思科云通信。下面列出了高级网络钓鱼防护传感器的防火墙要求：

入站：25 (SMTP)	用于从您的网关接收复制的入站邮件流。
出站：443 (HTTP/S)	对思科云和其他云服务的 HTTP/S 请求（详细信息请参阅下文） 注意：可以将传感器配置为对 HTTP/S 出站连接使用代理。
出站： 53 (DNS)	DNS 用于主机名/IP 地址解析。 注意：如果主机系统正在使用 `127.0.*` 或 `localhost` 进行 DNS 解析，Docker 将不会在容器的 /etc/resolv.conf 文件中复制它。相反，它将把 DNS 设置为 `8.8.8.8` 和 `8.8.4.4`,，并且如果通过防火墙无法使用这些地址，DNS 将失败。 您可能需要将主机的 DNS 服务器设置为您的企业中使用的内部 DNS 服务器的实际地址。

出站：
123 (NTP)
	NTP 用于时间同步服务。注意：在 RedHat 系统中，您可以发出以下命令验证 NTP 是否正常工作：
	`nptstat`
	`echo $?`
	如果正在访问 NTP 服务器，则最后一个命令的输出需要为 `0` 。有关检查 NTP 状态的详细信息，请参阅 RedHat 文档。
	https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s1-Checking_the_Status_of_NTP.html

防火墙规则：思科需要的 HTTPS 访问

将要运行安装脚本的系统需要访问以下终端才能使脚本成功执行：

- https://agari-ep-collector-config-prod.s3.amazonaws.com
- https://agari-ep-collector-config.s3.amazonaws.com
- https://agari-ep-collector-ingest-avro.s3.amazonaws.com
- https://agari-ep-collector-filter-prod.s3.amazonaws.com
- https://agari-ep-collector-filter.s3.amazonaws.com
- https://aws.amazon.com
- https://kinesis.us-west-2.amazonaws.com
- https://s3-us-west-2.amazonaws.com
- https://sns.us-west-2.amazonaws.com

软件包

您可能需要手动安装一些软件包。

如果您修改 Linux 发行版，则可能需要了解安装脚本和传感器需要的或兼容的软件包。

- Postfix

  有些 Linux 发行版（即 RHEL 版本 7.1）默认启用 Postfix 服务器。如果默认 Postfix 服务器正在运行，必须将其禁用后再运行传感器安装脚本。（传感器将安装思科自己的自定义版本 Postfix 服务器，用于接收邮件。）

  运行以下命令禁用并删除 Postfix 服务器：

  ```
  # sudo yum remove postfix
  ```

- APT

  APT（高级软件包工具）是一组用于管理软件包的工具。APT 解决依赖关系问题并从指定的软件包存储库中检索请求的软件包。

- wget

  wget 是采用非交互式方法从网络中下载文件的实用程序。您可能需要使用 wget 来获取 EPEL 软件包。

- EPEL（为 Enterprise Linux 额外提供的软件包）

  EPEL 是高质量附加软件包存储库，用于完善基于 Fedora 的 Red Hat Enterprise Linux (RHEL) 及其兼容衍生产品，例如 CentOS 和 Scientific Linux。

  您可以键入以下命令获取 EPEL：

  ```
  wget -r --no-parent -A 'epel-release-*.rpm' \
  http://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/
  ```

备注　要安装此软件包，您需要通过防火墙访问：

  - http://dl.fedoraproject.org
  - Docker 与 RedHat 版本 6.x。

  在 RHEL 版本 6.7 中，Docker 可能并非默认分发。如果您运行的是没有 Docker 的 RHEL 版本发行版，可以从以下地址安装此版本：

  https://docs.docker.com/v1.7/installation/rhel/#red-hat-enterprise-linux-6.5-installation

- Docker 与 CentOS 7.1 和 7.2

  您可能必须为运行 CentOS 7.1 和 7.2 的系统明确定义 Docker 存储库。

  以下命令将使用明确定义 Docker 的基本 URL 的文件，在 /etc/yum.reports.d 目录下创建一个文件：

  ```
  # cat >/etc/yum.repos.d/docker.repo <<-EOF
  [dockerrepo]
  name=Docker Repository
  baseurl=https://yum.dockerproject.org/repo/main/centos/7
  enabled=1
  gpgcheck=1
  gpgkey=https://yum.dockerproject.org/gpg
  EOF
  ```

创建 /etc/yum.repos.d/docker.repo 文件后，可以安装 Docker，然后启动 Docker 服务：

```
# yum install docker-engine
# service docker start
```

- Python YAML 和 Python PIP

  较早的发行版可能没有安装 Python YAML（另一种标记语言）和 Python PIP（Python 安装程序软件包）软件包。传感器安装脚本需要这些软件包。您可以发出以下命令安装它们：

  ```
  # yum install python-yaml
  # yum install python-pip
  ```

- Python 和 Python Argparse

  传感器安装脚本还需要 python 和 python-argparse 软件包。

  ```
  # yum install python
  # yum install python-argparse
  ```

思科高级网络钓鱼防护传感器安装脚本

您将从思科销售工程代表处获取第一个高级网络钓鱼防护传感器安装脚本。该脚本将以类似如下形式命名：

`sensor-install-<orgname>-<date>.sh`

您应该在收到脚本后立即运行脚本。尝试安装版本比较老旧过时的传感器安装脚本可能会导致错误。如有疑问，请确保您收到的是最新版本的高级网络钓鱼防护传感器安装脚本。

您可以重命名文件。

将文件移到主机系统中（例如通过 SCP）。如有必要，移动文件后您可能需要设置权限以使脚本可以执行。例如：

```
# chmod +x sensor-install-examplecom-2018-02-01.sh
```

除了安装思科高级网络钓鱼防护传感器，第 1-1 页中提到的必备条件外，请在运行传感器安装脚本前确保您已满足以下各项条件：

- 您是否对调配的 Linux 计算机具有根访问权限？
- 防火墙是否已配置为允许对思科云和安装存储库进行 DNS、NTP、SMTP（入站）和 HTTP/S 访问？
- 代理：如果对 HTTP 流量使用代理，您是否有可用的代理类型（HTTP 或 NTLMO）、主机名、端口、用户名和密码？
- TLS 流量：在安装期间，您可以配置通过 TLS 将入站流量传送至传感器。如果您计划将基于 TLS 的 SMTP 传送用于高级网络钓鱼防护传感器，您是否有私钥（.key 文件）、签名的 TLS 证书（.pem 文件）和证书链（.pem 文件）？

运行脚本

考虑所有必备条件和依赖关系后，即可执行安装脚本。

该脚本由以下阶段组成：

- 打印脚本的版本。
- 创建目录 `/opt/agari and /var/opt/agari/etc`
- 如有必要，停止任何现有的思科高级网络钓鱼防护传感器服务。
- 将安装文件提取到临时目录中。
- 安装 Docker。
- 安装 PyYAML（如有必要）。
- 安装 AWS 工具（AWS、AWS SSL）。

- 提示设置用于日志和配置文件的其他 UNIX 组权限（可选；默认情况下将使用根组）。
- 提示设置 HTTPS 代理配置（可选）。
- 测试能否访问正确的 S3 存储桶进行数据上传。
- 提示为与高级网络钓鱼防护传感器之间的连接设置 TLS 证书和 TLS 配置（默认值为“关”-需要 TLS 连接）。
- 提示设置调试级日志输出（默认情况下为“关”）。
- 将文件移到相应目录；删除临时文件。
- 升级高级网络钓鱼防护传感器的版本（如有必要）。

以下是 Linux Ubuntu 映像上运行的脚本示例。在下例中，请注意：

- 您的安装脚本输出不会完全相同。下面的文本仅为示例。
- 您的组织 ID 是唯一的。
- 访问密钥 ID 用于访问 AWS。
- 如果系统未在主机系统上找到 Docker 和 AWS 工具，则会安装这些工具。
- 您可以指定用于访问日志和配置数据的 UNIX 组权限。
- 您可以选择指定 HTTPS 代理。
- 您可以指定与传感器之间的 SMTP 连接要使用的 TLS 证书。
- 您可以指定调试级日志记录。

正在运行的高级网络钓鱼防护传感器脚本示例：

脚本的版本号 创建思科目录	$ sudo ./sensor-install-examplecom-2017-09-27.sh Cisco Advanced Phishing Protection Sensor Installation ... Wed Sep 27 21:49:03 UTC 2017 VERSION: 17.09.27035106 + mkdir -p /opt/agari /var/opt/agari/etc Extracting install files into /var/opt/agari/tmp/agari.df8jXF Running extracted install Running Install/Upgrade steps... • agari-collector.service - LSB: start and stop agari-collector-filter Loaded: loaded (/etc/init.d/agari-collector; bad; vendor preset: enabled) Active: inactive (dead) since Wed 2017-09-27 14:46:21 PDT; 2min 42s ago Docs: man:systemd-sysv-generator(8) Process: 4664 ExecStop=/etc/init.d/agari-collector stop (code=exited, status=0/SUCCESS) Process: 4284 ExecStart=/etc/init.d/agari-collector start (code=exited, status=0/SUCCESS) Sep 27 13:38:33 ubuntu systemd[1]: Starting LSB: start and stop agari-collector-filter... Sep 27 13:38:33 ubuntu agari-collector[4284]: net.ipv4.ip_forward = 1 Sep 27 13:38:33 ubuntu agari-collector[4284]: Waiting for agari-collectord to start... Sep 27 13:38:34 ubuntu agari-collector[4284]: Started agari-collectord: PID 4299. Sep 27 13:38:34 ubuntu systemd[1]: Started LSB: start and stop agari-collector-filter. Sep 27 14:46:21 ubuntu systemd[1]: Stopping LSB: start and stop agari-collector-filter... Sep 27 14:46:21 ubuntu agari-collector[4664]: agari-collectord is not running. Sep 27 14:46:21 ubuntu systemd[1]: Stopped LSB: start and stop agari-collector-filter. Sep 27 14:48:36 ubuntu systemd[1]: Stopped LSB: start and stop agari-collector-filter. Warning: agari-collector.service changed on disk. Run 'systemctl daemon-reload' to reload units. Writing sensor configuration to file: /var/opt/agari/tmp/agari.df8jXF/etc/collector.yml

您可以指定用于访问日志和配置数据的 UNIX 组权限 您可以指定 HTTPS 代理	Do you want to verify the AWS SSL server certificates used for communications from this sensor to AWS? [y/N](no)>no You may optionally specify a Unix group that will be given read access to logs as well as write access to the collector's configuration and data. Group name (root): Will this sensor use an HTTPS proxy to send data to the Agari cloud? [y/N](no)> Testing access to download S3 bucket... OK. Testing access to configuration S3 bucket... OK. Testing access to data ingest S3 bucket... OK. Testing access to statistical ping SNS topic... OK. Testing access to data ingest Kinesis stream... OK. Do you want to configure TLS Certificates for incoming SMTP traffic to this sensor? [y/N](no)> n Require that all SMTP sessions use TLS? [y/N](no)?> n Which port should this sensor listen on for incoming SMTP connections? [25]> Enable DEBUG-level logging? [y/N](no)> n + : Creating directories ... + mkdir -p /var/opt/agari/etc /var/opt/agari/run /var/opt/agari/spool /var/opt/agari/shared /var/opt/agari/log + mkdir -p /opt/agari/bin /opt/agari/lib + ln -Tsf /var/opt/agari/etc/ /opt/agari/etc + ln -Tsf /var/opt/agari/etc/ /etc/agari + ln -Tsf /var/opt/agari/log/ /var/log/agari

您可以指定与传感器之间的 SMTP 连接要使用的 TLS 证书 您可以指定调试级日志记录	Running Install/Upgrade steps... Moving new files to /opt/agari Downloading docker image from S3... Deleting old docker containers... Deleting old docker images... Loading new docker image... Updated version to 17.09.27035106 Running post-installation Running post-installation Running post-install steps... Removing temporary install files in /var/opt/agari/tmp/agari.df8jXF Installation Complete

此时，高级网络钓鱼防护传感器已成功安装。

如果您有权访问思科高级网络钓鱼防护门户，则应该能够导航至“管理”>“传感器”页面并看到传感器已连接。

图 2-1　　传感器状态

备注　高级网络钓鱼防护传感器应在大约 2 分钟后进行背景连线通信。

后续步骤

安装完第一个高级网络钓鱼防护传感器并且可以连接到思科之后，您可以将测试邮件直接发送到思科高级网络钓鱼防护传感器，第 2-5 页。

将测试邮件直接发送到思科高级网络钓鱼防护传感器

由于传感器在安装脚本中指定的端口上侦听 SMTP 会话，因此可以将测试邮件直接注入传感器。如果您可以通过 Telnet 连接到安装脚本中配置的 SMTP 端口并且您能轻松地直接发出 SMTP 命令，则可以创建一封测试邮件：

```
$telnet sensor_name:sensor_port
Trying IP_address...
```

```
Connected to sensor_name

Escape character is '^]'.
220 collector-filter ESMTP Postfix
HELO example.com
250 collector-filter
MAIL FROM: <test@example.com>
250 2.1.0 Ok
RCPT TO: user@yourcompany.com
DATA
354 End data with <CR><LF>.<CR><LF>

Received: from 1.2.3.4 by test.example.com
Received: from 192.168.3.3. by internal
From: “John Smith” <jsmith@example.com>
To: “Jane Doe” <jdoe@example.net>
Subject: test message sent from manual telnet session
Date: Wed, 11 May 2011 16:19:57 -0400
Message-Id: <testing-testing>

Hello World,
This is a test message sent from a manual telnet session.

Yours truly,
SMTP administrator
.
250 2.0.0 Ok: queued as message_ID
quit
```

请确保邮件 DATA 包含 Received: 报头。在单独的一行上输入“.”字符将结束 data 命令。“250 2.0.0.Ok: queued as…”命令表示您的测试邮件已成功被接受，并且传感器已准备好接受从您的双重传送配置路由的邮件。

排除测试邮件故障

如果您在输入 `MAIL FROM:` line:

```
451 4.7.1 Service unavailable - try again later
```

后收到类似如下所示的错误信息……有可能高级网络钓鱼防护传感器尚未启动并正常运行。请尝试以下操作：

- 查看主机上的 `/var/log/agari/container.log` 看看是否找到类似于以下内容的行：
  `Feb 01 2017 05:07:59 INFO collector-filter is ready.`
  如果找不到，则表示筛选进程尚未启动。再等待几分钟后重试。
- 自您启动高级网络钓鱼防护传感器以来是否已超过 5 分钟？如果不到 5 分钟，请等足 5 分钟，如果过滤器仍未启动，则重新启动容器：
  `$ /opt/agari/bin/agari-ep restart`
- 如果重新启动容器后问题仍然存在，请考虑重新启动整个收集器：
  `$ sudo service agari-collector restart`

安装其他传感器

思科高级网络钓鱼防护传感器评估各邮件的元数据而丢弃邮件正文，因此它们十分高效。根据您计划从网关复制的入站邮件数量，您可能需要配置更多高级网络钓鱼防护传感器以实现冗余或提高吞吐量。要安装其他高级网络钓鱼防护传感器，只需在新实例上运行安装脚本。

单个高级网络钓鱼防护传感器至少每天可以处理 500,000 封邮件，峰值吞吐量最高达 50 封邮件/秒。在生产环境中，强烈建议使用负载均衡的双传感器配置以实现冗余。

规划双重传送

安装高级网络钓鱼防护传感器后，现在应该配置思科邮件安全网关，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思科邮件安全网关的类型而异。请参阅您的思科邮件安全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）层或思科邮件安全网关；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。
- 均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第一道反垃圾邮件防线的替代品；更确切地说，它的设计宗旨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思科高级网络钓鱼防护传感器到思科的邮件。

- 思科高级网络钓鱼防护传感器本身包含“接收模式”设置，它默认设置为“上传数据”。

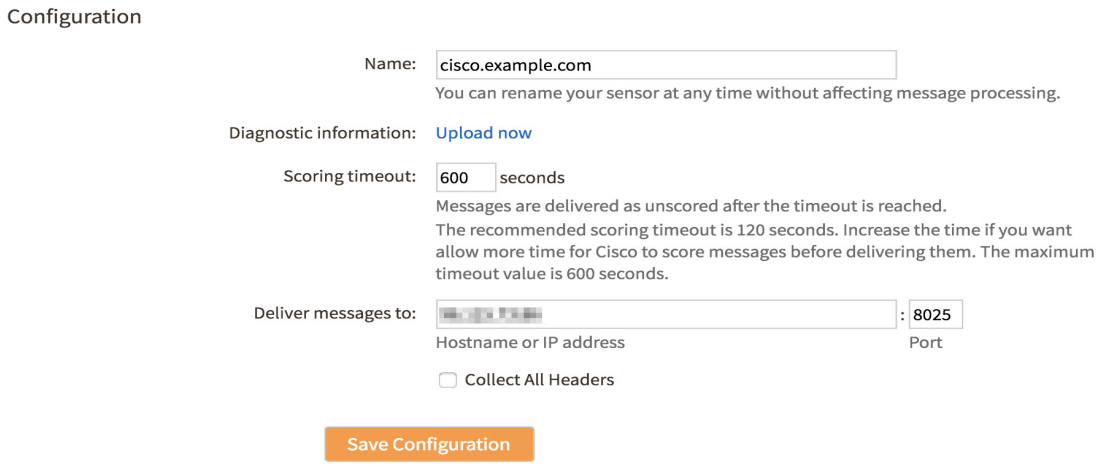
  如果您只需要测试向传感器传送邮件但不将数据上传到思科进行处理，您可以将“接收模式”设置为“不上传数据”。
- 您的组织有一个“收集模式”开关，必须由思科销售工程师配置该开关之后，邮件才会出现在思科高级网络钓鱼防护 Web 应用中。

  “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数据到系统中的流量突然飙升。

配置下游主机以接收邮件（仅内联安装）

安装高级网络钓鱼防护传感器并连接到思科后，您必须配置下游主机和端口以从传感器接收邮件。此配置在思科高级网络钓鱼防护门户的“管理”>“传感器”页面中完成。在页面底部，有一个标记为“将已评分邮件传送至：”部分，可用于输入 IP 地址或主机名和端口号

图 2-2　　配置下游主机（仅内联安装）



备注　需要对每个传感器完成此配置，并且必须为您安装的每个高级网络钓鱼防护传感器保存此配置。

保存这些配置更改后应等待 5 分钟左右，以便传感器接收更改并进行更新。

之后，您可以将测试邮件直接发送到传感器（请参阅“将测试邮件直接发送到思科高级网络钓鱼防护传感器”，第 5 页）。

配置高级网络钓鱼防护传感器的传送

安装高级网络钓鱼防护传感器后，现在应该配置思科邮件安全网关，以将邮件流定向到该网关。

配置传送的步骤因思科邮件安全网关的类型而异。请参阅您的思科邮件安全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。思科高级网络钓鱼防护并非第一道反垃圾邮件防线的替代品；更确切地说，它的设计宗旨是寻找已经通过此过滤的不可靠邮件。

配置双重传送

安装高级网络钓鱼防护传感器后，现在可以配置思科邮件安全网关，以将邮件流定向到该网关。

配置双重传送的步骤因邮件网关的类型而异。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）层或思科邮件安全网关；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。
- 均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第一道反垃圾邮件防线的替代品；更确切地说，它的设计宗旨是寻找已经通过此过滤的不可靠邮件。

双重传送的特定说明

本指南的双重传送：思科邮件安全网关，第 3-1 页部分介绍了如何为思科邮件安全网关配置双重传送。

第 3 章

双重传送：思科邮件安全网关

本文档介绍如何配置从思科邮件安全网关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 “密件抄送：”操作将把邮件复制到高级网络钓鱼防护传感器，创建使用此操作的内容过滤器。

步骤 2 的内容过滤器。配置退回处理以正确管理意外的传送失败。

步骤 3 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 4 考虑其他已加入白名单的邮件流。

步骤 5 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”报头的重要注意事项

高级网络钓鱼防护传感器依靠准确且未损坏的 **Authentication-Results** 报头的存在来帮助评估发送方身份。通常，您企业的“边界”MTA（意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 报头，而您企业中的所有下游 MTA 将仔细配置为保留此报头的完整性（即，它们不得用自己的报头覆盖此报头，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报头）。

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

因此，您可以将边界 MTA 配置为用替代名称创建（或复制）Authentication-Results 报头：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：创建用于转移邮件的“密件抄送：”过滤器

步骤 1　以管理员用户身份登录思科邮件安全网关。

步骤 2　导航至“邮件策略”>“传入内容过滤器”。

备注　如果已为集群管理配置了思科邮件安全网关环境：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思科邮件安全网关实例）完成以下步骤。

步骤 3　点击**添加过滤器**并将过滤器命名为 Cisco_collector。

步骤 4　在**说明**字段中提供合理的说明，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报头信息和身份验证数据。有问题吗？请通过邮箱 joeadmin@example.com 联系管理员 Joe”

步骤 5　确定该过滤器的顺序，使其能够让高级网络钓鱼防护传感器接收将要传送至最终用户的所有邮件（即：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后续过滤器，您应该考虑这些过滤器并正确放置高级网络钓鱼防护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。

内容过滤器可能不需要任何条件。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）。如果有什么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。同样，内容过滤器的目的是只对将要直接传送至最终用户的邮件起作用：请根据需要为此过滤器添加条件。

步骤 6　点击**添加操作**将操作与此过滤器关联。在**添加操作**窗口中，选择**添加/编辑报头**。

步骤 7　将两个新报头添加到邮件：用于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报头中）：

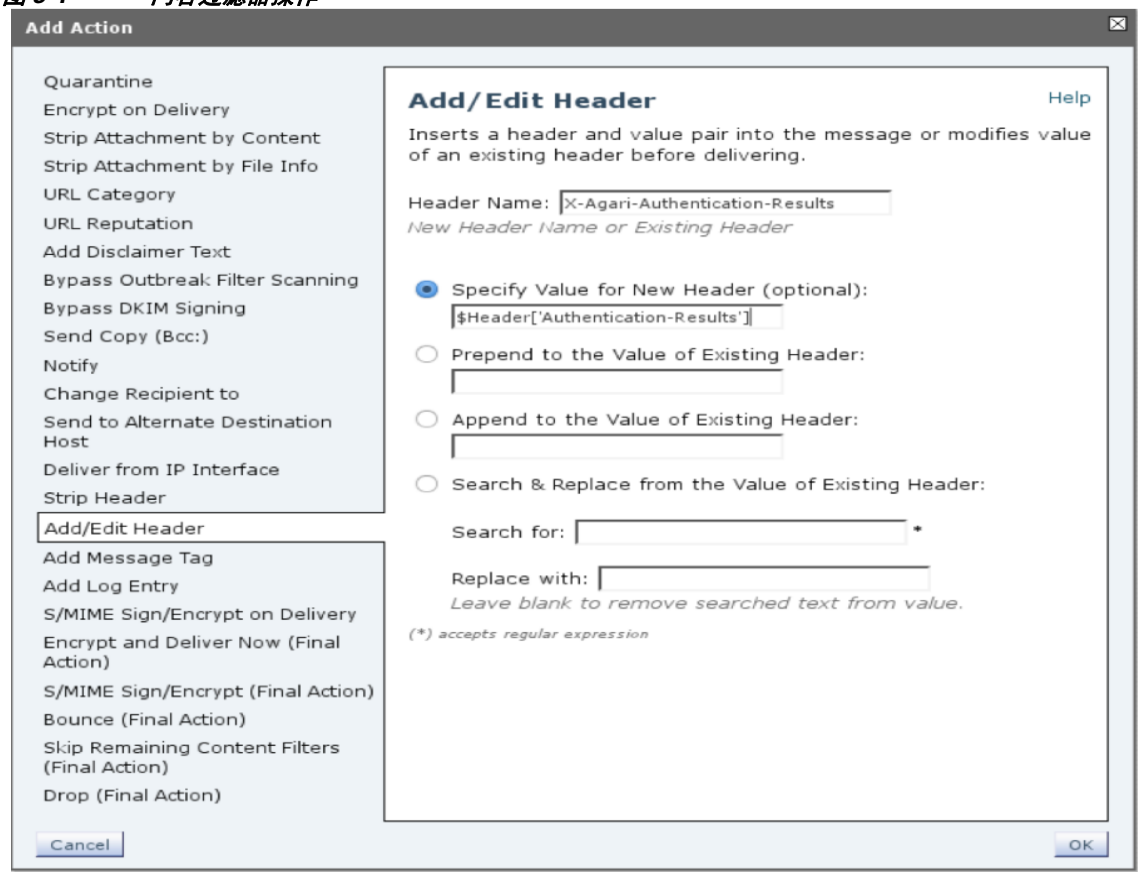
- 报头名称：**X-Agari-Original-From** 报头数据：**$EnvelopeFrom**
- 报头名称：**X-Agari-Original-To** 报头数据：**$enveloperecipients**

如果思科邮件安全网关是边界网关 MTA 且只有在这种情况下，还应添加以下报头：

- 报头名称：**X-Agari-Authentication-Results** 报头数据：**$Header['Authentication-Results']**

仔细检查所有报头名称有无拼写错误。

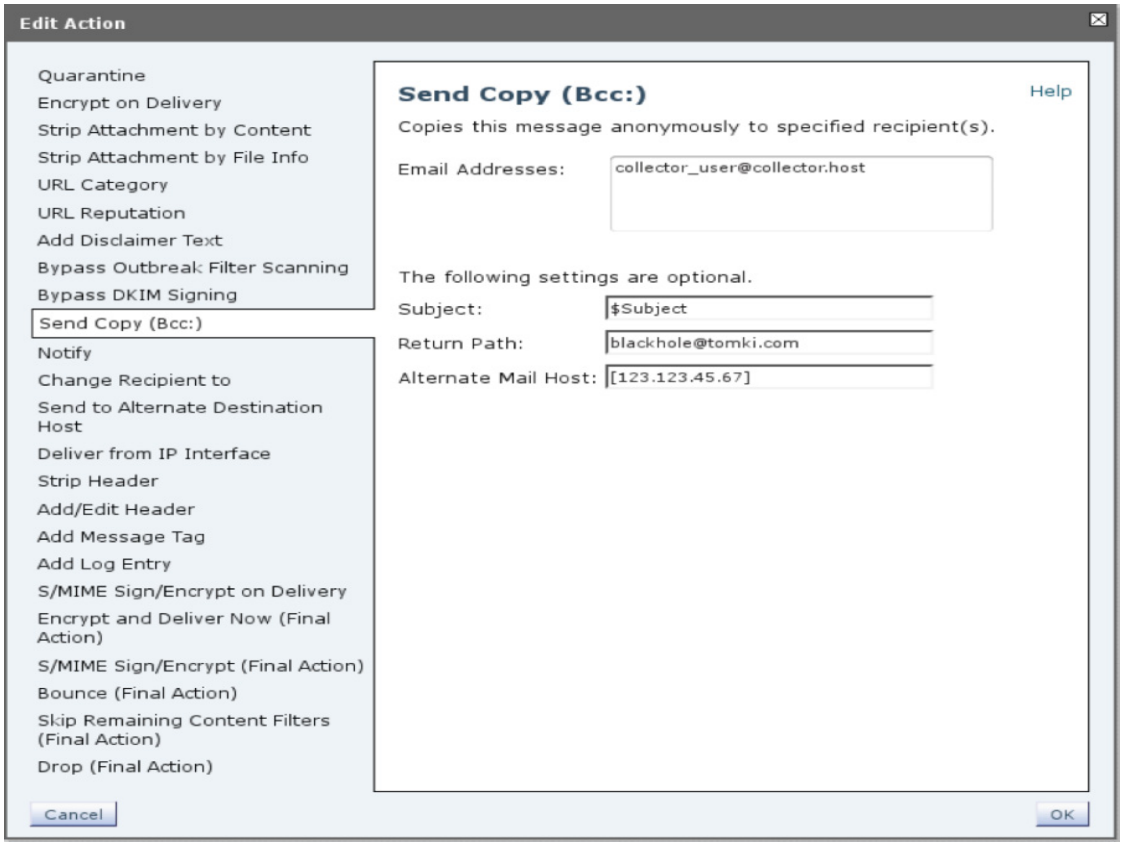
图 3-1　　内容过滤器操作



步骤 8　点击“提交”之前，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。

- 密件抄送操作的邮件地址可以是能够到达高级网络钓鱼防护传感器的可路由地址，也可以直接指定高级网络钓鱼防护传感器（请参阅下文）。
- 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高级网络钓鱼防护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，万一传送至高级网络钓鱼防护传感器时出现问题，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，而非传送至邮件地址的 MX 记录或思科邮件安全网关“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高级网络钓鱼防护传感器的主机或 IP 地址（IP 地址应该以方括号括起来，例如 [123.123.45.67]）。请注意，上面指定的邮件地址中使用的域仍与退回处理相关，如下所述。

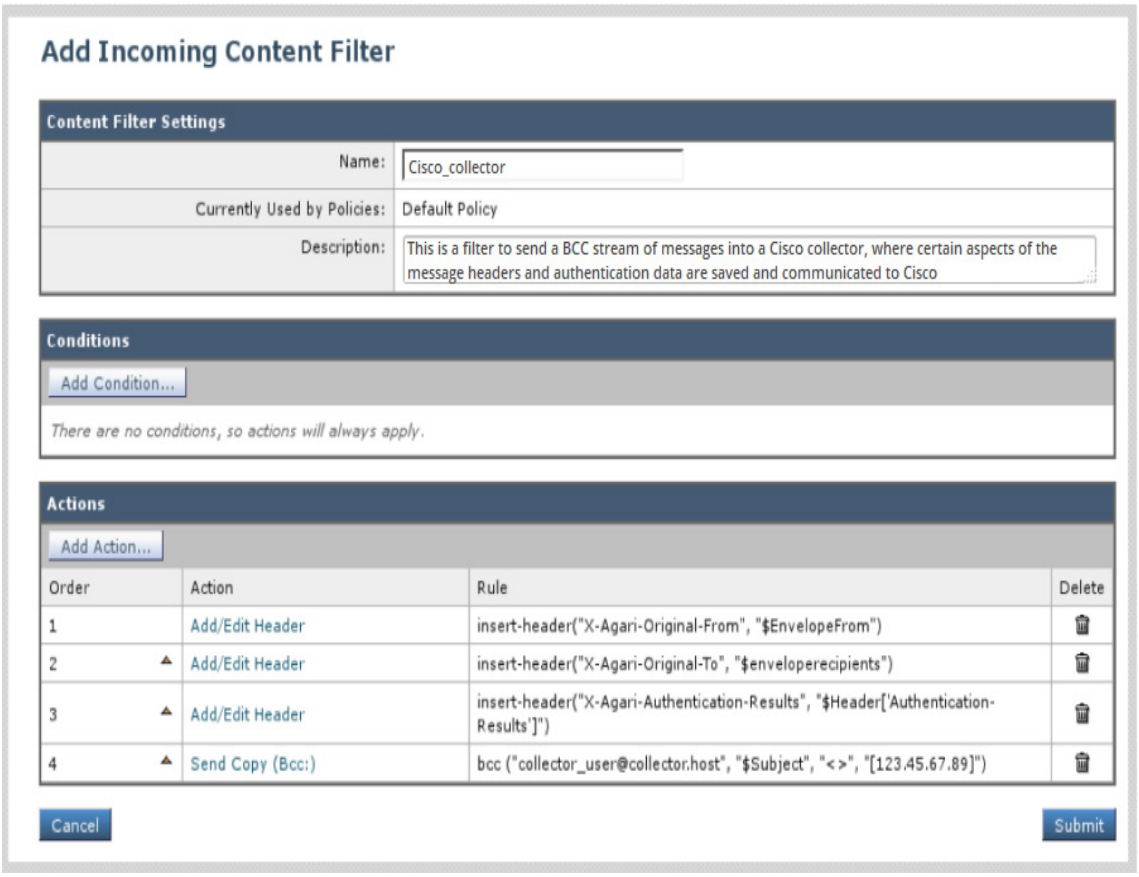
图 3-2　　密件抄送操作



步骤 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）：

图 3-3　　内容过滤器摘要



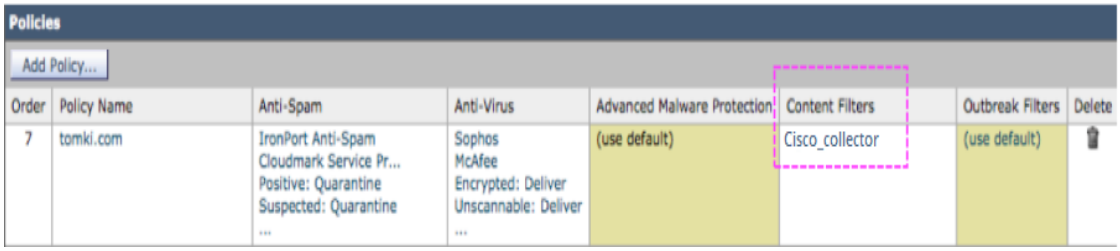
备注　上图显示了添加的 **X-Agari-Authentication-Results** 报头：只有当思科邮件安全网关 MTA 是边界网关 MTA 时才应添加此报头。如果思科邮件安全网关 MTA 位于边界网关下游，则不应添加此报头。

步骤 10　点击**提交**保存新过滤器。

步骤 11　将过滤器与相应的传入邮件策略关联。导航至“邮件策略”->“传入邮件策略”，并在相应行的“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。

步骤 12　修改后的策略行可能如下所示：

图 3-4　　包含内容过滤器的策略行



步骤 13　要提交更改，请点击**提交更改 >>** 按钮。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。

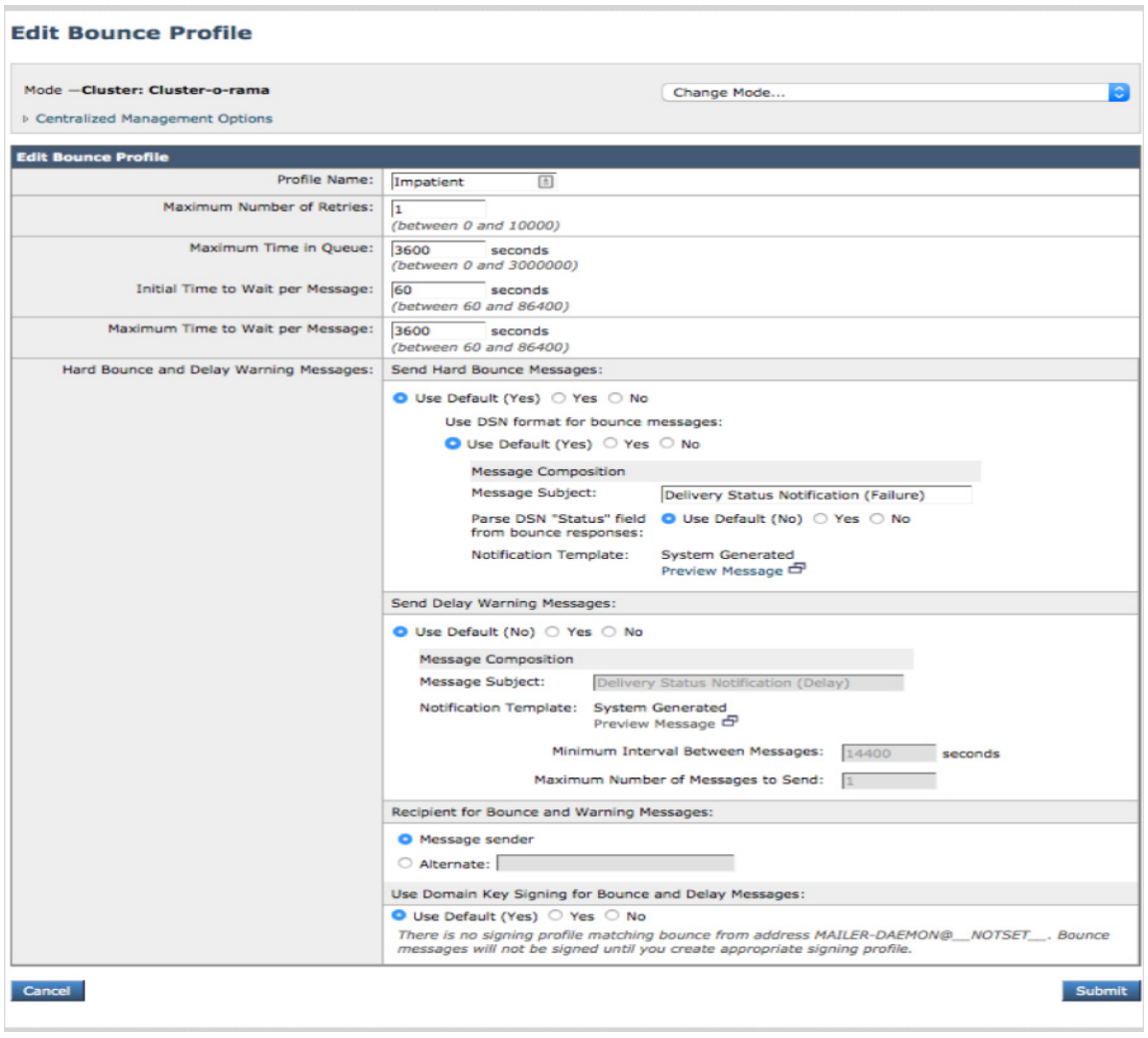
步骤 2：配置高级网络钓鱼防护传感器的退回处理

为了使用最少的思科邮件安全网关系统资源，您应该将系统配置为在高级网络钓鱼防护传感器传送失败的情况下邮件退回也快速失败。要安全地做到这一点，请按照以下步骤操作：

步骤 1　提供位于目的主机接受的唯一域或子域中的密件抄送传送邮件地址。“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“collector.host”用于该域。

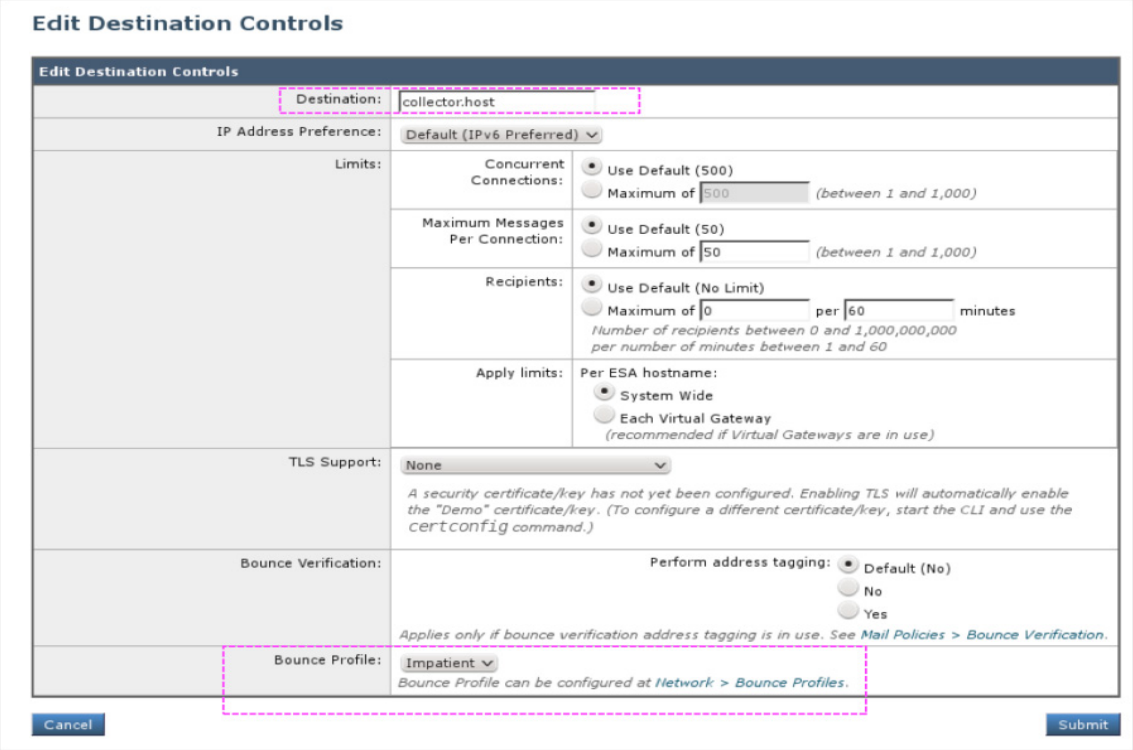
步骤 2　创建退回配置文件以便让邮件退回快速失败。导航至“网络”>“退回配置文件”，然后点击**添加退回配置文件**创建一个新条目。如下所示使用值：

图 3-5　　退回配置文件



步骤 3　接下来，为上述唯一的高级网络钓鱼防护传感器域（在本示例中为“collector.host”）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”）。导航至**邮件策略 > 目标控制**，然后使用下图所示的值创建一个条目：

图 3-6　　目标控制



如果高级网络钓鱼防护传感器不在受到保护的网络内，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”。思科邮件安全网关现在将安全地连接到远程传感器（在端口 25 上通过“STARTTLS”）。

步骤 4　正确进行配置并提交后，点击**提交更改 >>**。

系统警报

导航至**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。

考虑其他已加入白名单的邮件流

您可能已设置防火墙规则，将发送邮件到思科邮件安全网关的上游 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，在邮件管道中的稍后评估）。

此问题的解决取决于入站邮件流的详情，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，将副本发送到高级网络钓鱼防护传感器（使用本文档中介绍的相同配置），然后触发不进行进一步过滤而直接传送邮件（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 3：将警报服务器加入白名单

认为某封邮件可疑时，思科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邮件警报。

除了识别具有威胁的邮件之外，警报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高级网络钓鱼防护传感器和有关思科邮件安全网关服务整体运行状况的警报。鉴于这些警报的重要性和的实用性，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。

以下说明介绍了将警报服务器添加到白名单中的步骤。

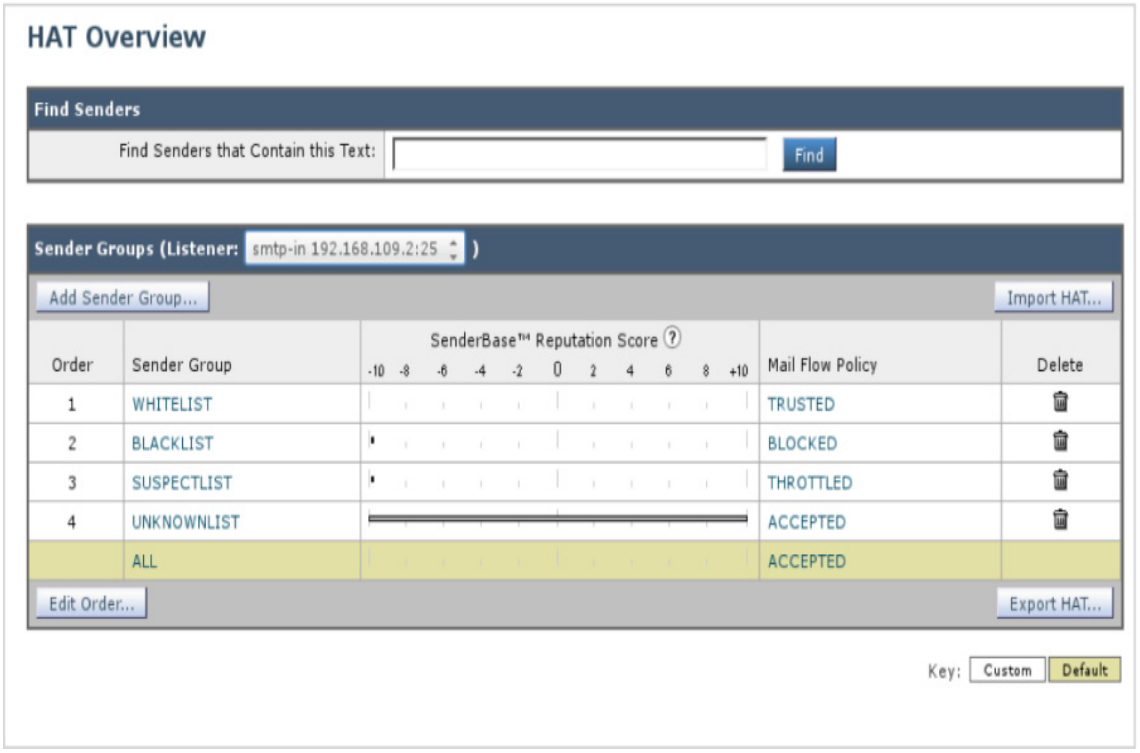
步骤 1　在思科邮件安全网关中，导航至**邮件策略 > HAT 概述**页面。

图 3-7　　主机访问表概述菜单项

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：

图 3-8　　主机访问表

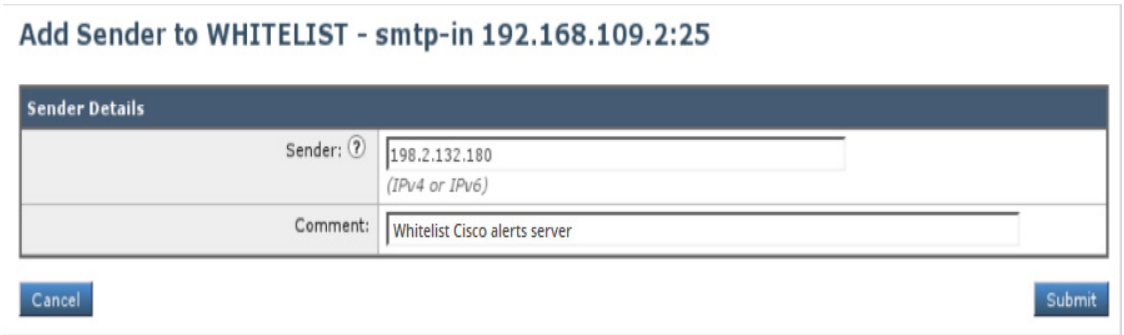


备注　您的配置可能与此存在各种不同，因此您可能需要根据您的特定环境调整这些说明。例如，您需要对每个入站侦听程序重复此配置，让所有已配置的入站侦听程序将警报服务器加入白名单。

步骤 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。

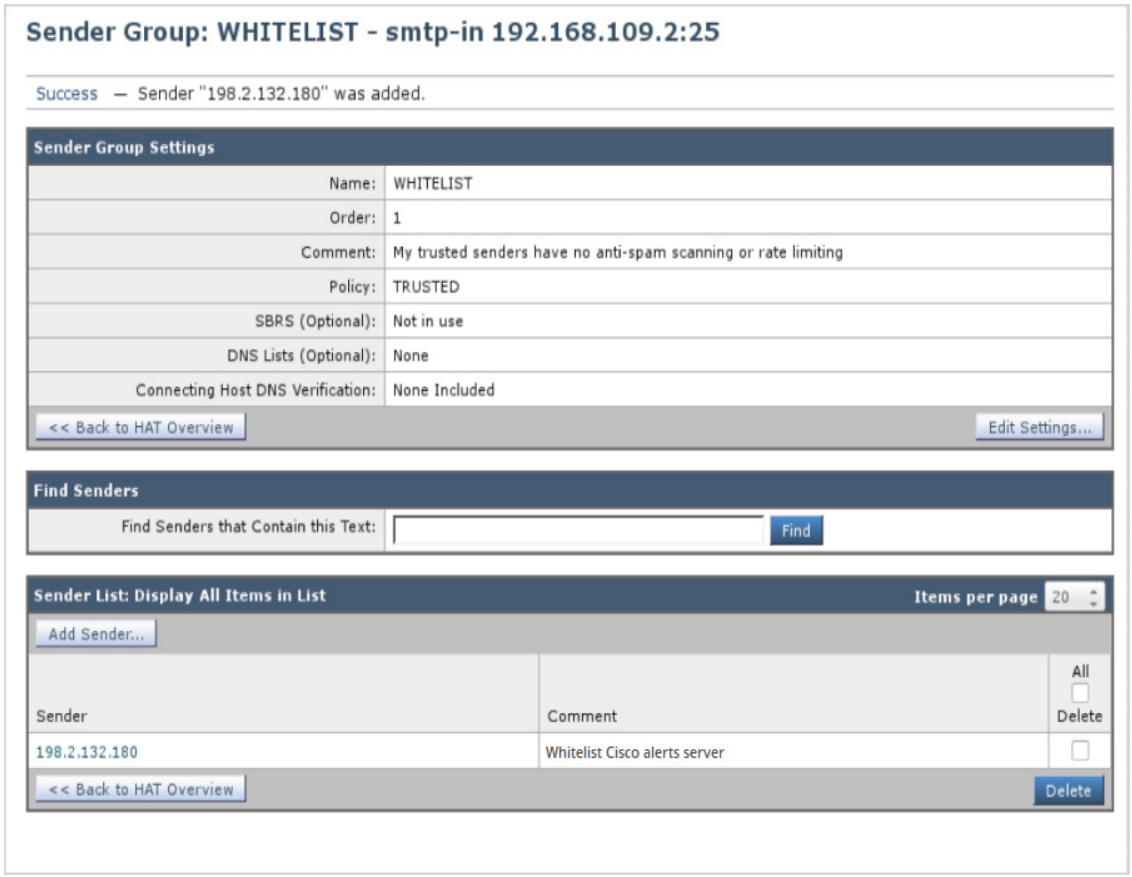
步骤 3　在出现的窗口中，点击**发件人列表：显示列表中的所有项目**部分中的**添加发件人**。在出现的窗口的**发件人：**字段中，输入警报服务器的 IP 地址：198.2.132.180。在**注释：**字段中添加注释，例如**白名单警报服务器**。

图 3-9　　将发件人加入白名单



步骤 4　点击“发件人组”窗格中的**提交**，确认该 IP 地址在**发件人列表**部分中：

图 3-10　　发件人列表部分



步骤 5　点击**提交更改 >>** 以使配置更改生效。

如上所示，警报服务器的 IP 地址是 198.2.132.180。此外还维护着位于“outbound.cisco.com”域的此地址的 DNS 条目。一般情况下，建议此白名单规则使用明确的 IP 地址。

步骤 4：配置思科邮件安全网关以添加 X-Agari-Authentication-Results 报头

此部分仅适用于您配置的思科邮件安全网关系统是边界网关并且不准备用于双重传送的情况。如果您使用思科邮件安全网关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 报头的正确方法。

如果思科邮件安全网关系统是边界网关且您想添加 X-Agari-Authentication-Results 报头，请执行以下步骤：

步骤 1　以管理员身份登录思科邮件安全网关。

步骤 2　导航至**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思科邮件安全网关实例）执行剩余步骤。请勿在计算机级别多执行以下步骤。

步骤 3　点击**添加过滤器**。

步骤 4　将过滤器命名为 **Agari_auth_header**。

步骤 5　为过滤器添加合理的说明，例如：向所有传入邮件添加 **X-Agari-Authentication-Results** 报头。

步骤 6　调整该过滤器的顺序，使其向所有传入邮件添加该报头。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。

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）。

步骤 7　点击**添加操作**将操作与此过滤器关联。在“添加操作”窗口中，选择**添加/编辑报头**。

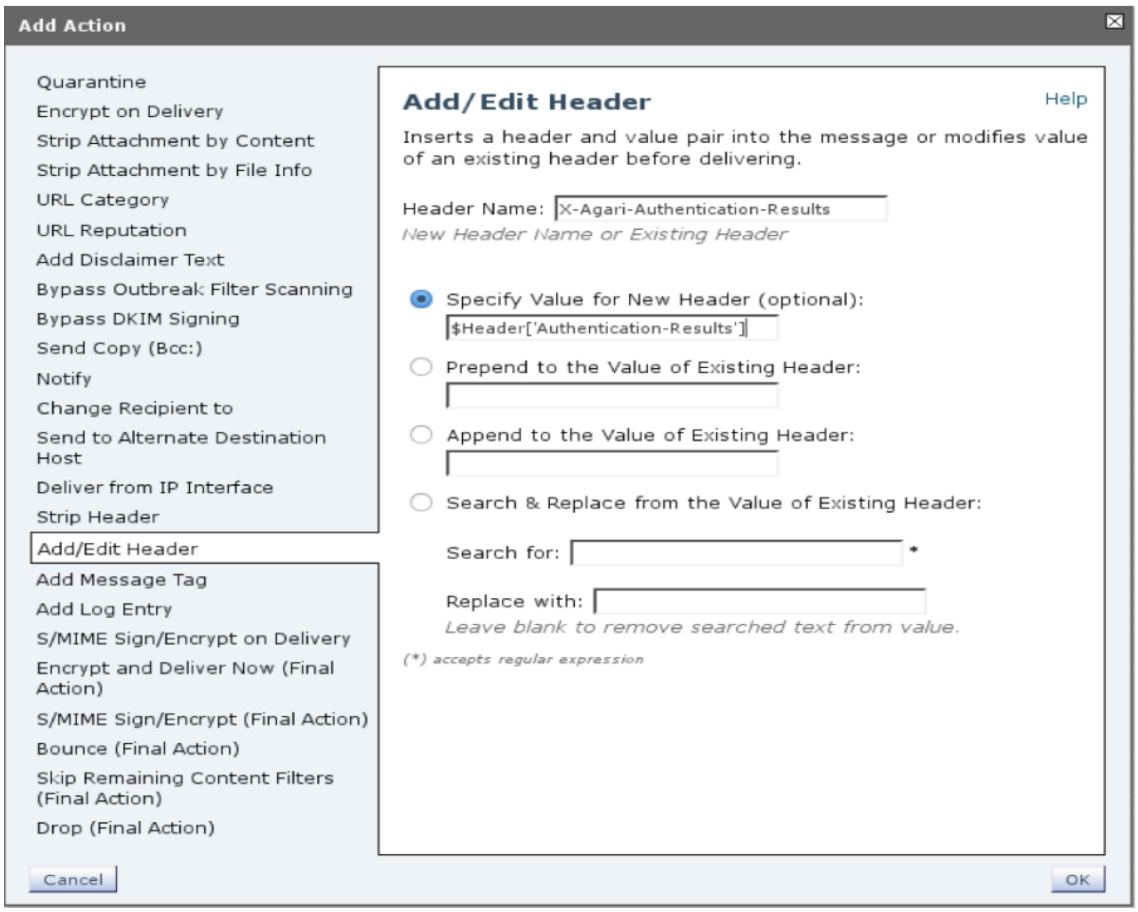
步骤 8　使用界面指定过滤器，用于将两个新报头添加到邮件来指示原始收件人和原始发件人（这些信息不一定会正确反映在可见的邮件报头中）：

- 报头名称：**X-Agari-Original-From** 报头数据：**$EnvelopeFrom**
- 报头名称：**X-Agari-Original-To** 报头数据：**$enveloperecipients**

步骤 9　使用界面指示该过滤器复制 Authentication-Results 报头：

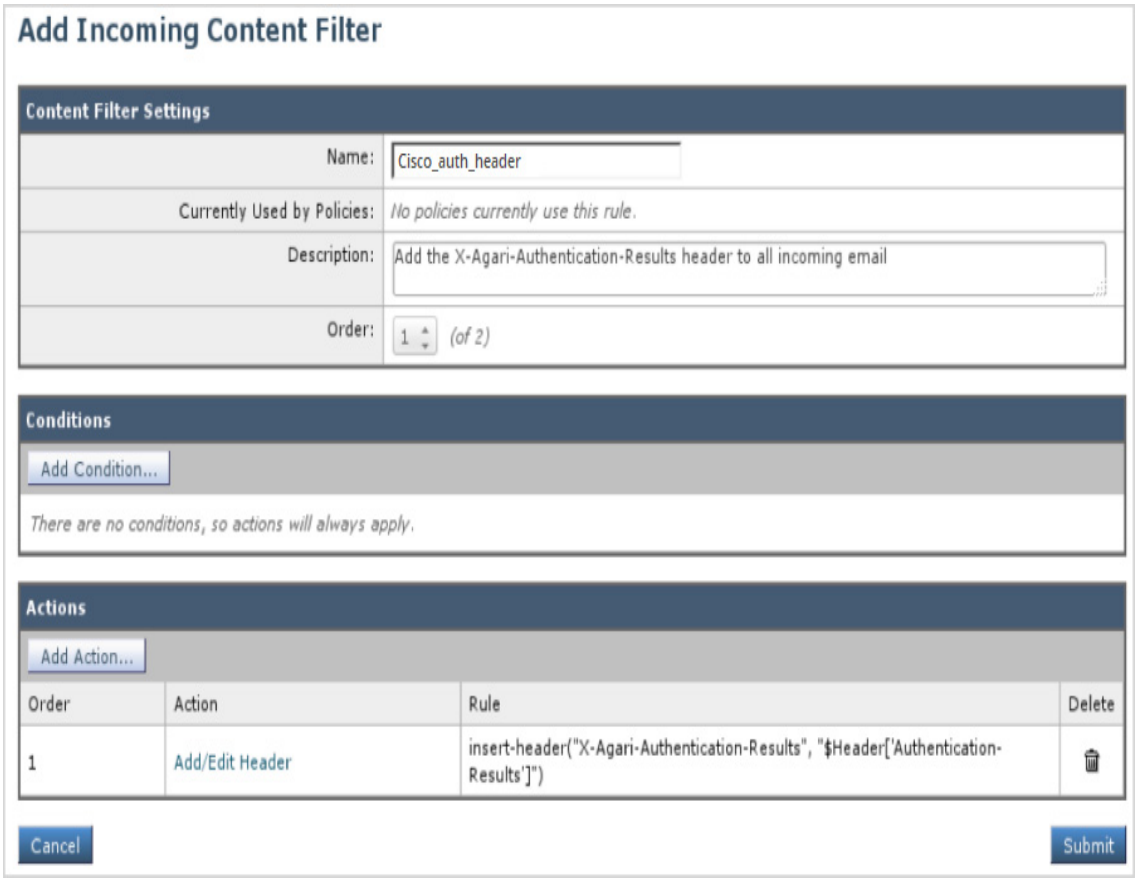
- 报头名称：X-Agari-Authentication-Results 为新报头指定值：$Header['Authentication-Results']

图 3-11　X-Authentication-Results 报头



步骤 10　确定报头名称正确，然后点击**确定**。完成后的传入内容过滤器将如下所示：

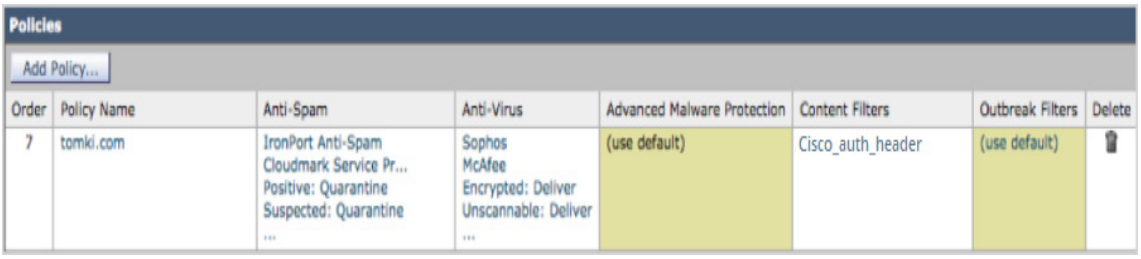
图 3-12　完成的传入内容过滤器



步骤 11　点击**提交**保存新过滤器。

步骤 12　要将该过滤器与相应的传入邮件策略关联，请导航至**邮件策略 > 传入邮件策略**，并在相应行的**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：

图 3-13　引用内容过滤器的策略页面



步骤 13　点击**提交更改 >>** 保存配置。

备注　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”报头。

完成安装

完成上述步骤后，高级网络钓鱼防护传感器将开始接收发送到您组织中的邮件的副本。在更改完全生效前，可能会有几分钟的短暂延迟。您可以通过以下方法确认流量流：登录思科高级网络钓鱼防护门户（网址为 https://appc.cisco.com），然后导航至**管理 > 传感器**查看您已安装的高级网络钓鱼保护传感器的状态。

用户任务：开始使用

本章介绍以下任务：

- 获取 Web 应用的访问权限
- 创建/编辑用户
- 分析传入邮件流量

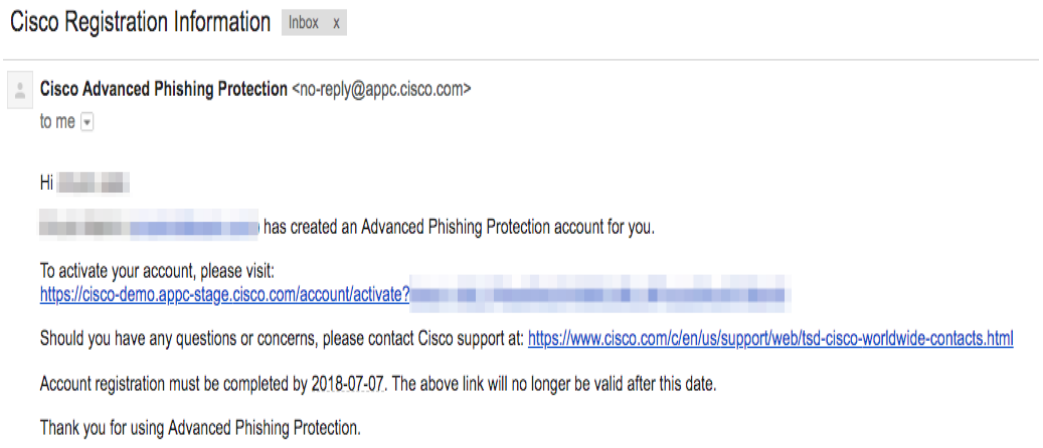
获取 Web 应用的访问权限

思科高级网络钓鱼防护可以帮助您前所未有地深入洞察组织的入站邮件流量。

您的销售代表必须启用第一个管理员账户，用于访问 Web 应用。通常，第一个账户具有“管理员”权限，以便您可以为组织创建更多用户账户。

您的销售代表创建第一个用户账户后，您应该收到一封邀请邮件，其中包含用于激活该用户账户的链接：

图 4-1　　邀请邮件示例


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-contacts.html

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.

请打开邀请邮件中发送的链接激活您的用户账户。选择一个安全的密码。

下次登录时，您就可以访问此门户（https://appc.cisco.com）了。

创建/编辑用户

用户角色

只读用户

只读用户可以在应用中搜索和查看数据，但不能在应用中的任何位置进行更改或编辑。

- 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。

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，审核用户还可以查看用户审核日志。

- 在“管理”>“用户”页面中查看并搜索用户审核日志。

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，用户管理员还可以创建和编辑组织中的其他用户。

- 在“管理”>“用户”页面中创建并编辑用户。

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。

分析传入邮件流量

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

概述页面以独特的方式直观显示组织入站邮件流量的风险概况。思科高级网络钓鱼防护传感器收到的每封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？

  和

- **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）？

可信度评分

系统对传送至组织用户的每封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。

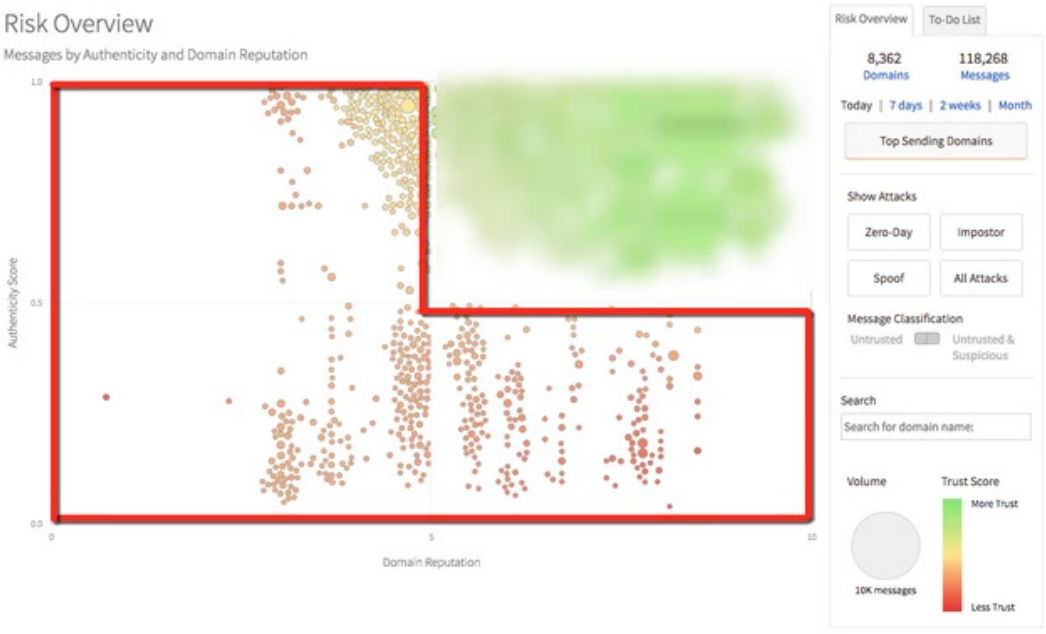
可信度评分会考虑域信誉评分、邮件真实性评分和每封邮件的特征。值得注意的是，邮件的内容并非可信度评分中考虑的因素。

- 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

“分析”>“概述”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。

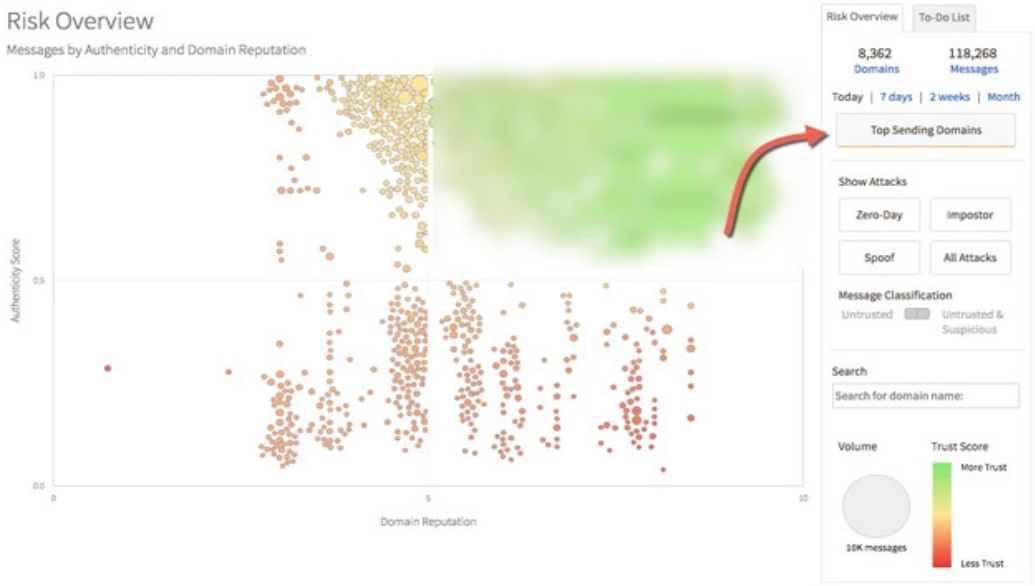
图 4-2　　“概述”页面中的象限



您可以点击页面左侧“显示攻击”部分的复选框来筛选结果，将其限制于三个基本攻击类型中仅仅一个类型或全部三个类型。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“排名靠前的发送方域”过滤器。

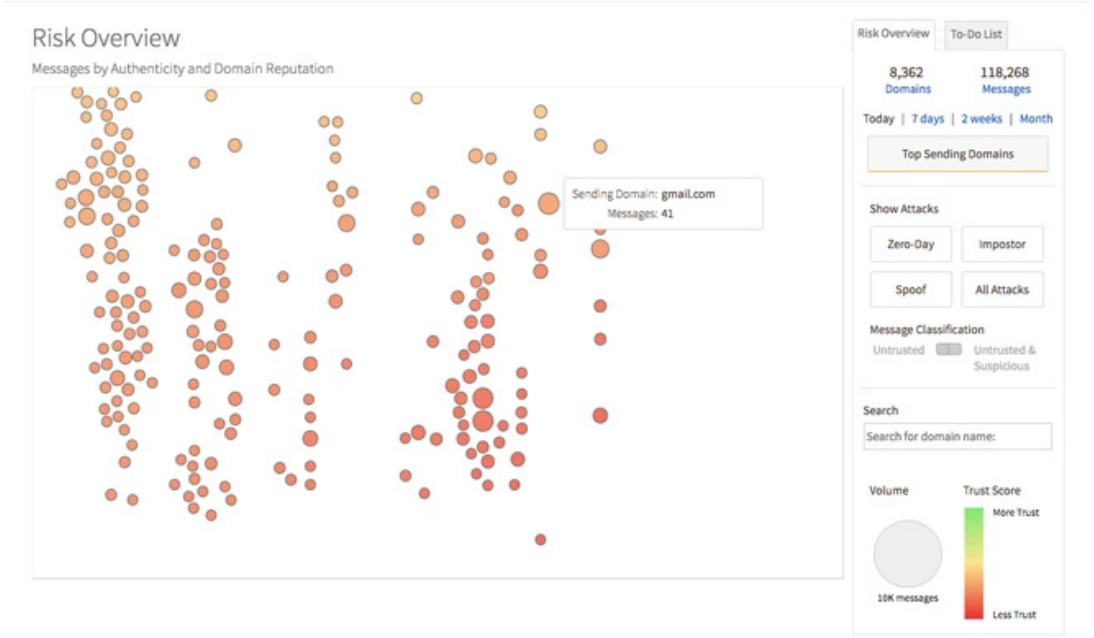
图 4-3　　排名靠前的发送方域过滤器



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：

图 4-4　　放大的象限

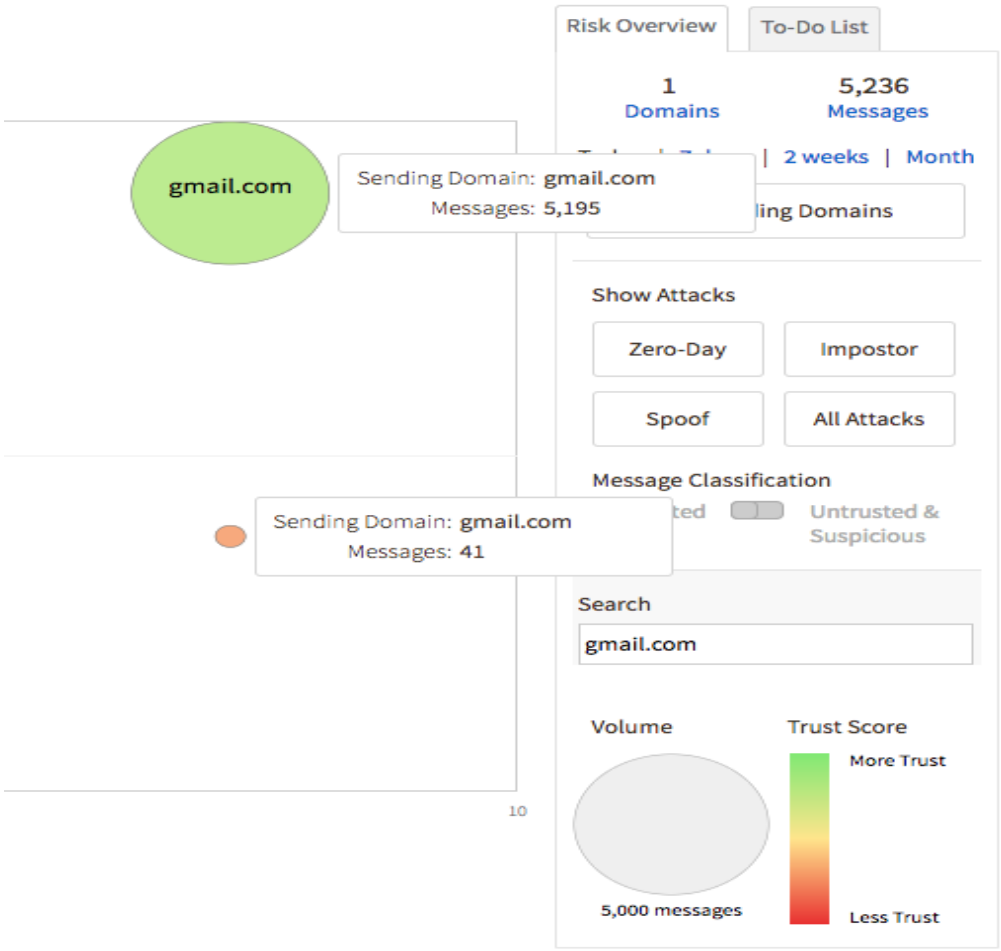


再次点击空白处可缩小。

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图案：

图 4-5　　搜索来自域 Gmail.com 的邮件



这表示 IronPort 在过去一天中已分析来自 gmail.com 域的 5,195 封合法邮件；将鼠标悬停在较小的圆圈上将显示，有 41 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。

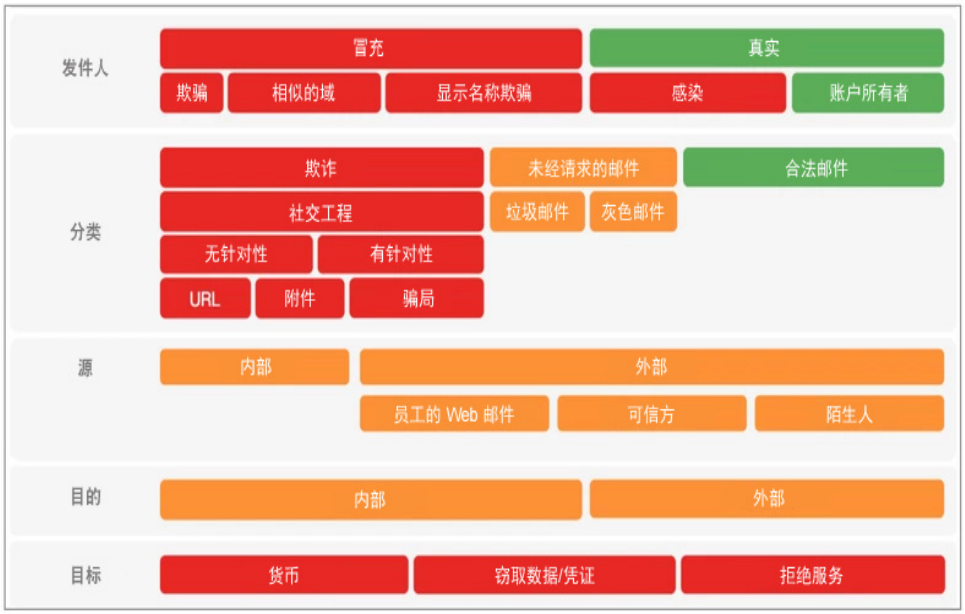
清除搜索框将返回到原始视图。

攻击分类

- 域详细信息，第 4-12 页
- 标记域，第 4-14 页

攻击分类法

图 4-6　　攻击分类的分类法



不可信（按照邮件可信度评分而定）的邮件将归入上图所示的攻击分类法的一个或多个攻击类中。攻击分类将显示于“邮件详细信息”视图中。

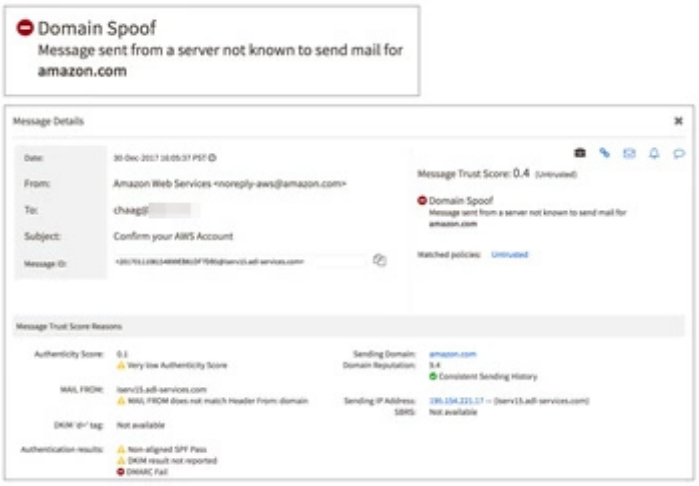
备注　该分类法的攻击分类当前不可用于搜索和策略，它们只是“邮件详细信息”视图中的信息性备注。

以下是该分类法各攻击分类的说明和示例。

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，但思科高级网络钓鱼防护发现其并非来自该域的真正发送源。

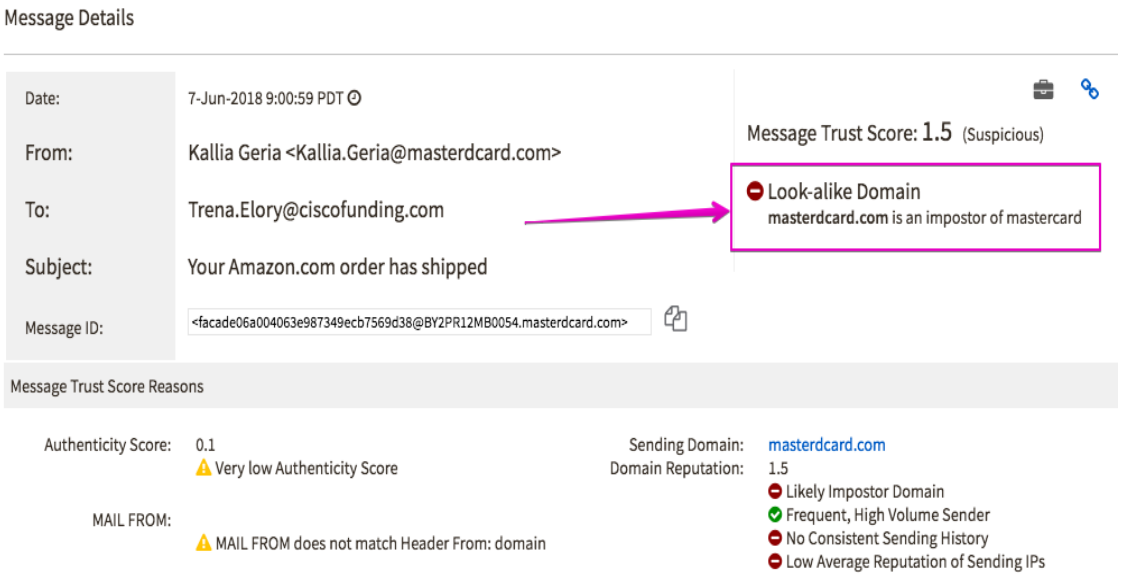
图 4-7　域欺骗示例



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。

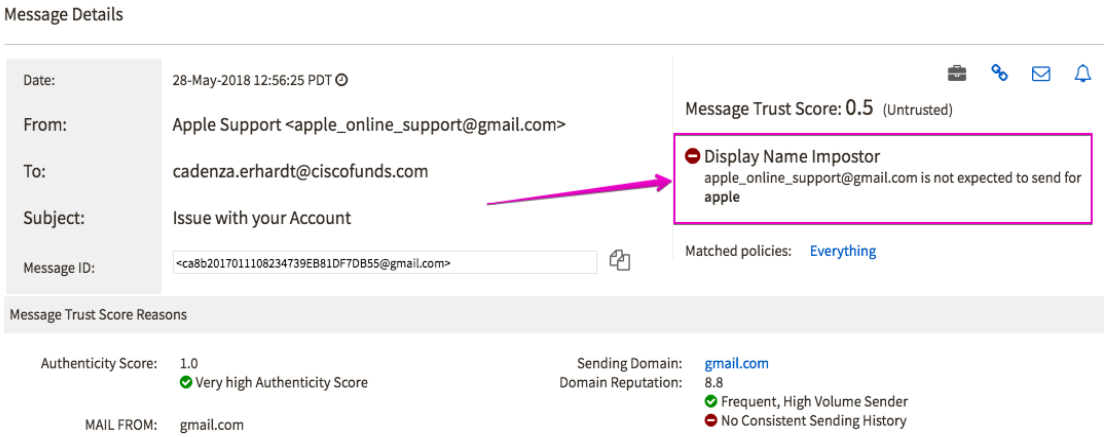
图 4-8　相似的域示例



冒充显示名称

冒充显示名称是指“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账户等其他攻击类型一起使用。

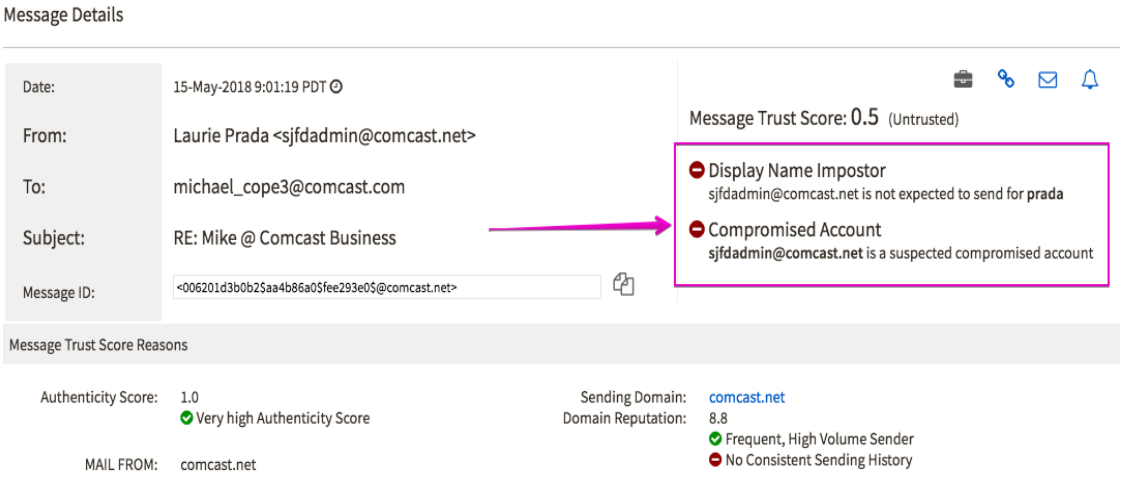
图 4-9　　冒充显示名称示例



受感染账户（账户接管）

受感染账户是属于真正的人/用户但已被恶意攻击者接管并用于恶意用途的账户。当 IronPort 发现账户接管迹象时，我们会将其归类为来自受感染账户的邮件。

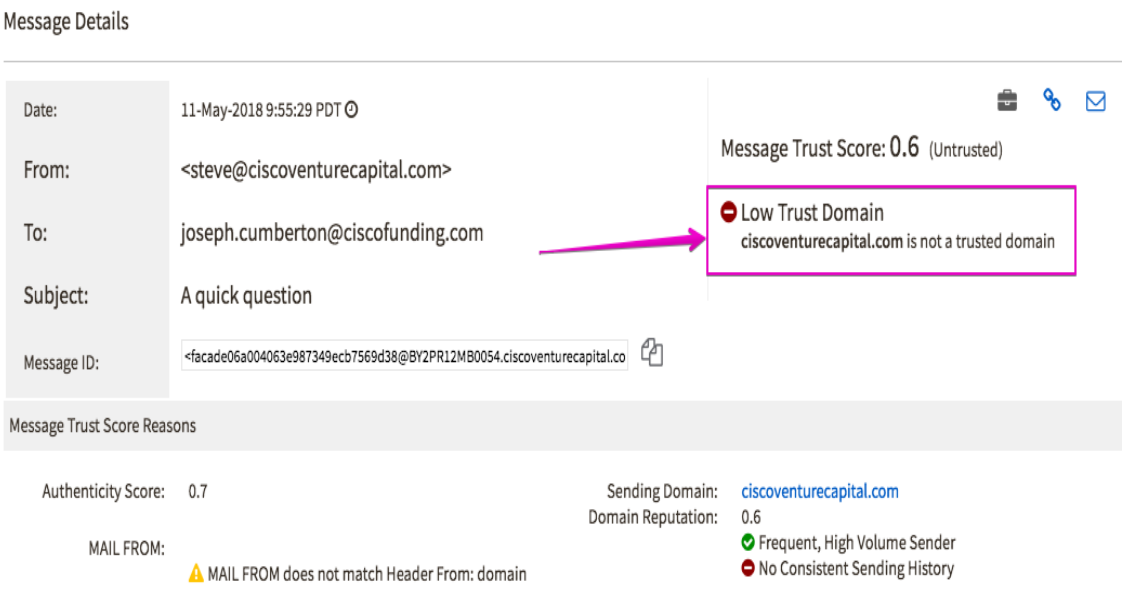
图 4-10　　受感染账户示例



低可信度域

除了前文提及的发件人分类，思科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邮件和未经请求的邮件（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）。

图 4-11　　低可信度域示例



恶意附件

如果启用了附件扫描，思科高级网络钓鱼防护会在附件可能属于恶意时通知您。

图 4-12　　恶意附件示例

传统攻击类

下面三种攻击类在思科高级网络钓鱼防护 Web 应用中仍将保持可用。在今后的版本中，它们会并入更加新的分类法攻击类中。您可以利用这些分类执行进一步操作，例如根据攻击分类发出警报。您可以在思科高级网络钓鱼防护 Web 应用中的多个位置按这些传统类过滤邮件，这些位置包括“风险概况”、“邮件”控制面板（按通用属性过滤时）和“搜索邮件”页面。以下是每个攻击分类的简短说明。

冒充

冒充攻击包括相似的域和一些冒充显示名称（主要是显示名称中使用的知名品牌）攻击。要确保您的内部域或合作伙伴域被用于识别冒充攻击而本身不会被分类为冒充攻击，请在思科高级网络钓鱼防护 Web UI 的“分析”>“域”页面中对这些域进行标记。

欺骗

欺骗攻击是新分类法攻击类中的域欺骗。邮件使用的是信誉评分高的发件人域，但来自不可靠的源。这些攻击“假冒”某个已知发件人的可信身份。要了解有关如何确定邮件来源真实性的详细信息，请参阅“真实性评分”部分。

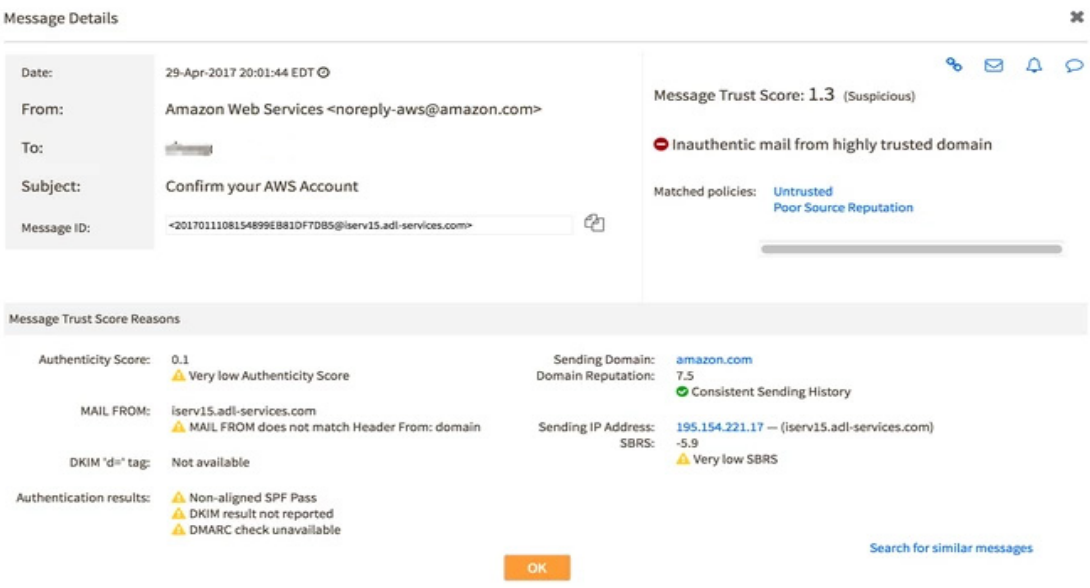
零日

在新分类法中，零日攻击是低可信度域攻击类的子集。零日攻击是指新的域出现并突然向您的组织中大量收件人发送邮件的情况（也称为弹出域）。这些域通常开始只有很低的发件人域信誉，并且数据中没有或只有极少发送历史记录。您会发现，此分类中捕获的往往是一般垃圾邮件和“业务垃圾邮件”。

邮件详细信息

既然您已经发现了几个不可信的发件人，点击其中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。点击邮件可查看邮件详细信息。请记住，思科高级网络钓鱼防护不跟踪邮件的正文。

图 4-13　　“邮件详细信息”窗格



“邮件详细信息”页面显示邮件的报头和评分信息，包括对邮件给出该评分的原因。在邮件详细信息视图右上角，您可以点击钟形图标 () 快速创建一个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“通过策略管理传入邮件”。

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？

工作流程

“概述”页面用于查找有问题的发件人和邮件。点击右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记（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。
- 查看评分。
- 使用**邮件详细信息**页面中的链接创建策略。
- 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。

IP 和域

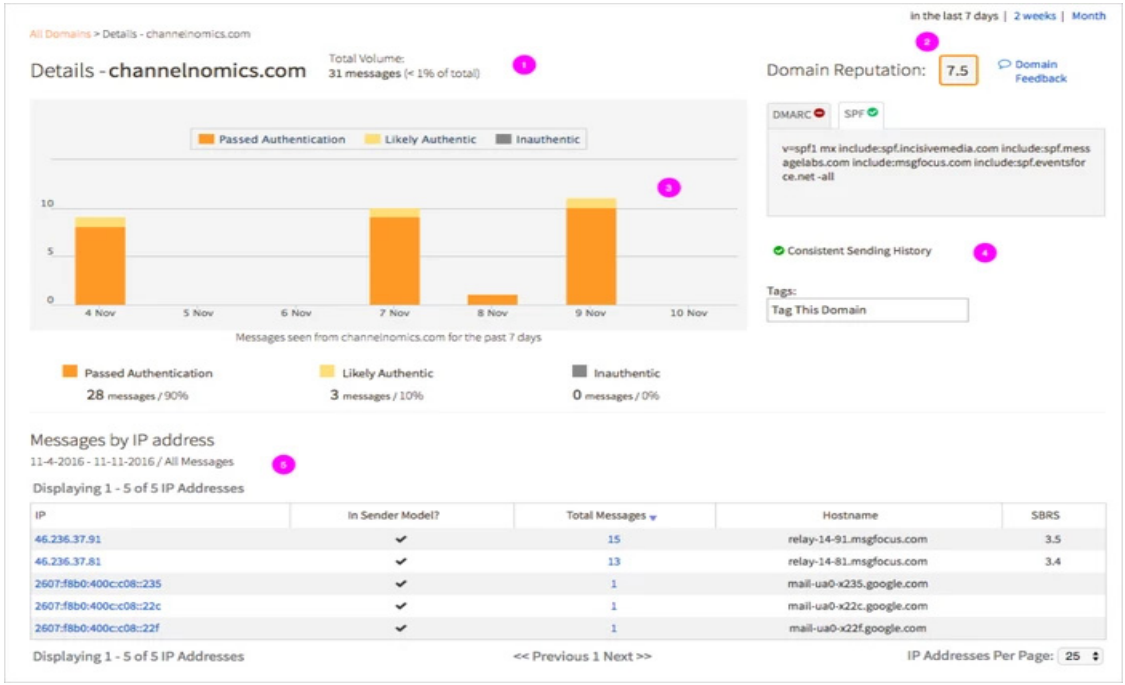
在“分析”菜单中，您可以查看发送方 IP 和域的列表（“分析”>“域”和“分析”>“IP 地址”)。两个页面的功能非常相似，而且您在调查传入流量时将在两个页面间切换。当您点击列表中的 IP 地址或域时，您可以看到该项目的“详细信息”页面。对 IP 地址，“详细信息”页面显示有关该 IP 的信息，包括从该 IP 地址发送到您组织的域的列表，以及每个域发送的邮件的链接。同样，点击“分析”>“域”页面上的列表中的域将显示该域的“详细信息”页面，包括从该域发送到您组织的 IP 地址的列表，以及发送的邮件。

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。

域详细信息

在思科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。

图 4-14　“域详细信息”页面



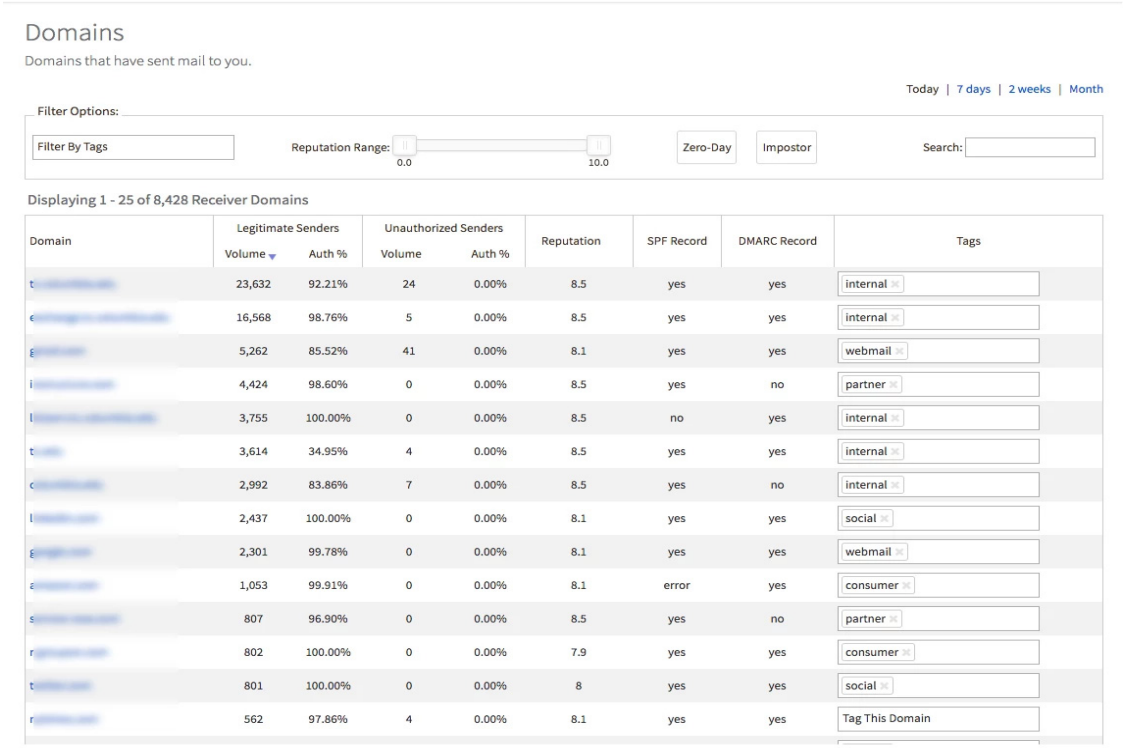
1	域名、域的数量和来自该域的入站邮件流总量所占的百分比列于页面顶部。
2	域信誉（由 IronPort 评分）列于右上角。如果您认为域的评分不正确，您可以通过“域反馈”链接发送反馈。域信誉的评分从 0.0 到 10.0，0.0 表示最低的信誉，10.0 表示信誉最佳。
3	页面中间是来自发送方域的邮件数量图。邮件分类如下：“已通过身份验证”、“不可靠”或“可能真实”。 • 真实可靠的邮件是遵守域本身发布的以下身份验证标准的域：SPF、DMARC 或 DKIM。 • 不可靠的邮件是身份验证失败并被认为不符合该域发件人模型的邮件。 • 可能真实的邮件是未通过身份验证但被认为“可能确实”来自发送方域的邮件。 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”。
5	“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。 • 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。

标记域

在“分析”>“域”页面或在“域详细信息”页面中，您可以在右侧的列中为域指定标记。在必要时，您可能需要对一些内部域和合作伙伴域应用标记。标记域可以帮助进行分析和创建策略。“内部”和“合作伙伴”标记用于评分过程中。其他自定义标记在评分时不会使用，但可用于策略，并有助于直观显示“分析”>“概述”页面和搜索结果。

图 4-15　域索引页面

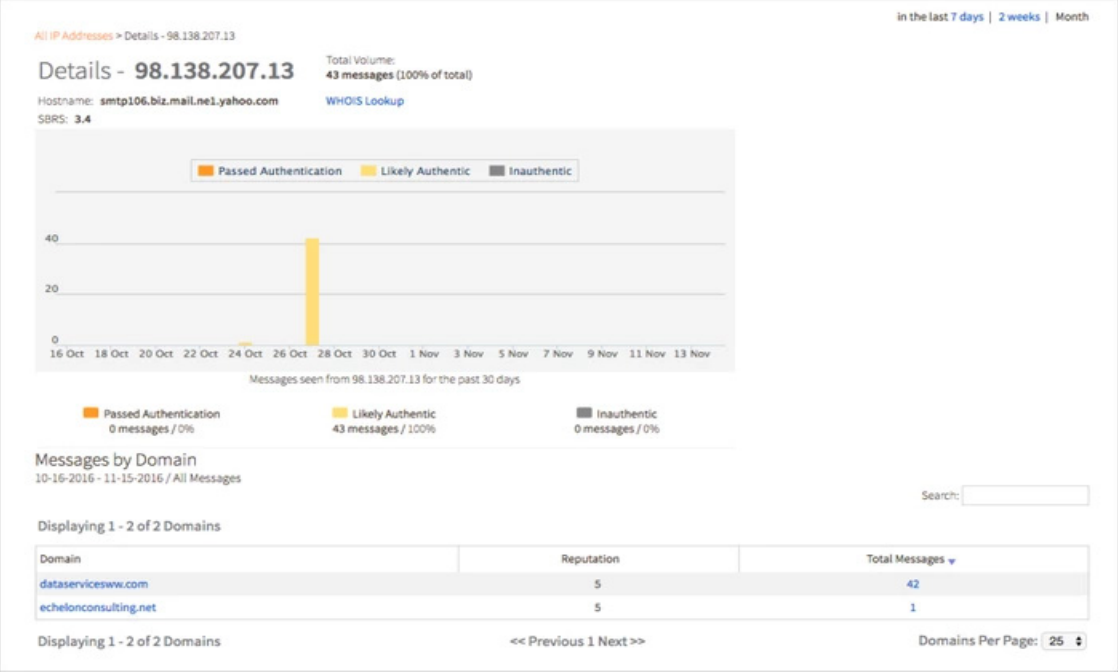


IP 详细信息

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）

图 4-16　　“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 的邮件总数和思科给出的 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。

在此示例中，发送 IP 地址 98.138.207.13 的主机名是“`smtp106.biz.mai.nel.yahoo.com`”，已向组织内发送了 42 封邮件：其中向域“`dataservicesww.com`”发送了 42 封邮件，向“`echelonconsulting.net`”发送了 1 封邮件。

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。

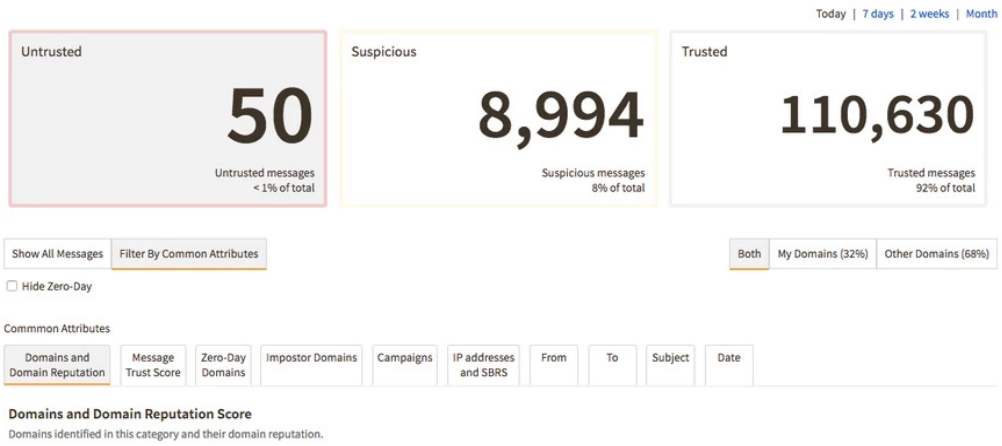
邮件

“概述”页面以交互式的方式直观显示欺骗、零日域和正常邮件，而“分析”>“邮件”页面则提供更多操作视图来帮助您了解数据。

图 4-17　“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”

图 4-18　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？
- **零日域** - 在这些不可信邮件中，哪些是从零日域发送的？
- **冒充域** - 在评为可疑的所有邮件中，哪些是从冒充域发送的？
- **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？
- **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？
- **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？

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。

点击搜索结果页面中的“邮件反馈”链接可发送有关发送方域的评论。

当您点击搜索列表中（或“分析”>“邮件”页面中）的邮件时，系统将显示“邮件详细信息”页面：

图 4-19　　“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，包括报头和评分（以及获得该评分的原因）、邮件匹配的策略（如有），以及（如果已启用强制执行）是否已对该邮件强制执行操作。

您可以使用“邮件详细信息”页面右上角的图标：

- 链接到主窗口中的邮件详细信息视图（通过一个 URL 直接链接到此视图）。
- 通过邮件将邮件详细信息视图发送给同事
- 创建与此邮件的条件相关的策略
- 提供有关邮件评分的反馈

管理可疑邮件

现在，您已确定一些可疑发件人和邮件，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（如果已启用强制执行）。

有关创建策略的详细信息，请参阅通过策略管理传入邮件，第 5-1 页。

用户任务：策略

本章介绍以下任务：

- 通过策略管理传入邮件
- 按需策略

通过策略管理传入邮件

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，您可以创建一条策略将可疑邮件移到隔离文件夹（仅适用于强制执行客户）。总之，基本思路是在传入邮件流量中对某些条件（由您指定）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（仅适用于强制执行客户），甚至完全删除邮件（仅适用于强制执行客户）。

“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。有关您的策略的详细信息，请参阅“我的策略效果如何？”。

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。
- 如果邮件与多条强制执行策略匹配，其强制执行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. 按照组织强制执行设置中所设置的顺序移到其他文件夹（请参阅管理思科高级网络钓鱼防护，第 6-1 页）。
- 您可以创建没有通知或强制执行操作的策略；与策略匹配的所有邮件都记录在事件日志和报告中。

条件

输入条件，根据邮件报头信息匹配邮件，报头信息具体指：`From:`、`To:` 和 `Reply-to:` 报头、邮件主题和/或发送域。

您还可以在此处指定要匹配的域标记。域标记在“分析”>“域”页面中分配，此内容已在“分析传入邮件流量”部分介绍过。

其他条件可在高级对话框（参见下文）中使用。

在策略中使用地址组

您可能需要指定一组要对其匹配策略的邮件地址。例如，您可能需要创建一条策略，查找发送给一群高管中任何一人的邮件。您可以创建一个包含名称列表的地址组，然后在单个策略中引用该地址组，而无需在多个策略中分别输入名称。

一条策略可以引用一个或多个地址组。可以在策略的“发件人”、“收件人”和“回复”条件中使用地址组。

您可以通过“管理”>“地址组”页面创建并管理地址组。

在 `From:` field 中

当您需要检测地址组中用户的冒充者时，请在策略条件的“发件人”字段中使用地址组。该条件会在“发件人”报头的显示名称（即“Friendly-From”）中查找地址组成员的名称。如果给定的“发件人”报头未使用显示名称，则该条件会评估地址组中邮件地址的本地部分是否与“发件人”报头中的邮件地址匹配。

备注　如果“发件人”地址与输入的地址匹配，该条件还会考虑邮件的真实性。

例如，假设某个地址组包含以下地址：

```
"John Doe" <jdoe@example.com>
```

- 如果收到一封发件人为“John Doe”<jdoe@not-example.com> 的邮件，则该条件会将其匹配为“Friendly-From”中的 John Doe 的冒充者，并执行为该策略定义的操作（发出警报、强制执行等）。
- 如果收到一封发件人为“John Doe”<jdoe@example.com> 的不可靠邮件，则该条件会将其匹配为 John Doe 的冒充者，因为即使邮件使用的邮件地址是真的，邮件也并不真实可靠。系统会执行操作。
- 如果不存在“Friendly-From”部分，则评估地址的本地部分，因此在对“发件人”报头进行匹配时，地址 <jdoe@example3.com> 将根据邮件地址的本地部分进行匹配。

在 `To:` field 中

地址组只会查找“收件人”字段与地址组中某个条目完全匹配的邮件，忽略显示名称部分。在“收件人”字段中对地址组进行匹配的策略通常可与“主题”字符串匹配和邮件可信度评分等其他条件一起使用。例如，您的策略条件可以是：收件人为“财务”地址组成员，“主题”包含“发票”，并且邮件可信度评分为 0-4.9 分。

填充地址组

输入组中每个用户的名字、姓氏和邮件地址，即可填充地址组。在用户有多个内部邮件地址等情况下，可以多次输入某个用户。

地址组匹配使用您在评估邮件地址的“Friendly-From”部分时输入的名字和姓氏字段。（在上例中，“John Doe”是“Friendly-From”部分；在 Office 365、Gmail 或 iOS 上的邮件应用等一些邮件用户代理 (MUA) 上，可见的通常是“收件人”报头的此部分。）

地址组例外情况

例外列表中的地址是为了指定地址组中人员的“已知正常”邮件地址或个人邮件地址以免误报。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。您可以将该地址添加到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，除非邮件不可靠，而且只有当“发件人”和“回复”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冒用时（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”。

评分

您可以设置评分阈值和是否匹配零日域或冒充域（或者都不匹配）。

高级

高级条件提供更精细的评分匹配（真实性、域信誉或 SBRS 范围）以及匹配特定 IP 地址的选项。

备注 策略只需要有一个条件就是有效的策略。通过用于创建策略的界面，您可以创建范围非常小的条件来匹配一组非常具体的邮件（例如，“发件人为 UserA，收件人为 UserB，发送方 IP 信誉介于 -6.7 到 -6.6 之间”）。您也可以使用该界面设置非常宽泛的条件，这种条件可能会匹配非常多（或几乎全部）传入邮件（例如，“可信度评分介于 2.2 到 10.0 之间的任何邮件”）。配置策略时请小心，不要创建条件过多的策略。

操作

指定当邮件与此策略匹配时思科高级网络钓鱼防护应该执行的操作。

通知

您可以指定要通知的人员以及通知方式（摘要等）。

通知原始收件人将向与该条件匹配的邮件的所有收件人发送单独的通知。（请注意，这可能会导致退回邮件，例如在思科高级网络钓鱼防护传感器解析邮件并尝试向不存在的邮箱发送通知的情况下）。

通知管理员将为每封匹配的邮件发送一封通知邮件，当与给定策略匹配的邮件数超过您定义的阈值时，则发送一封摘要通知。

您可以通过**管理 > 策略**页面中的“为原始收件人配置策略文本”链接来自定义全局通知用户收到的内容。

备注 此通知模板由所有策略共用。

强制执行

如果您使用 O365 或 G Suite 作为邮件存储并已启用强制执行，您可以选择将匹配的邮件删除或移出收件箱并移入指定文件夹。您还可以选择当匹配一组策略条件时将邮件移到收件箱，从而创建“白名单”策略。请注意，强制执行操作可以与通知原始收件人配合使用，使最终用户在每次 IronPort 根据策略条件匹配项移动邮件时都可以收到通知。

- 如果邮件与多条强制执行策略匹配，其强制执行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. 按照组织强制执行设置中所设置的顺序移到其他文件夹（请参阅“管理思科高级网络钓鱼防护”，第 1 页）。

策略使用入门

开箱即用的策略

您一开始有 6 条默认策略，用于匹配思科客户使用思科高级网络钓鱼防护所捕获的最常见条件。这些策略需要启用才能开始匹配邮件，而且还需要为这些策略设置通知和/或强制执行操作。建议您先启用策略但不包含操作，等到记录策略匹配项并监控结果后再选择通知和强制执行操作。

以下是默认策略：

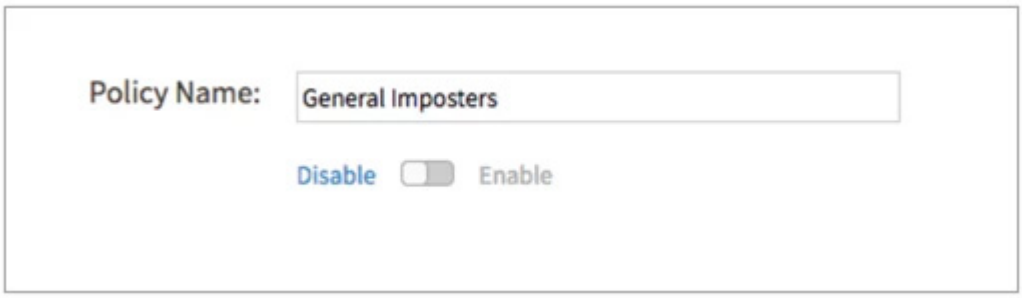
名称	条件	备注
首席级高管冒充者	发件人与“首席级高管”地址组中的显示名称匹配	捕获 BEC 攻击/冒充首席执行官、首席财务官和其他最高级别高管的攻击。请注意，此策略需要您填充“首席级高管”地址组，该地址组也是作为默认地址组为您创建的。
高管冒充者	发件人与“高管”地址组中的显示名称匹配	捕获 BEC 攻击 /冒充组织中其他高管的攻击。请注意，此策略需要您填充“高管”地址组，该地址组也是作为默认地址组为您创建的。
快速 DMARC	域标记为“内部” 真实性评分 < 0.4	捕获向您员工发送的您自己的域的欺骗攻击。此策略模仿 DMARC 拒绝策略，无需经过对所有源进行身份验证的冗长过程。思科的可信度模式可获知入站源的真实性。
合作伙伴域欺骗	域标记为“合作伙伴” 真实性评分 < 0.4	捕获合作伙伴的域的欺骗攻击
常规冒充者	冒充域/品牌 邮件可信度评分 < 5.0	捕获故意使用类似名称的冒充域，例如 cisco.com 或 paypa1.com。此外还会捕获冒充品牌的攻击，即在显示名称中冒充常见品牌。
邮件可信度低和发件人信誉低	邮件可信度评分 < 2.5 SBRS 评分 < -2.0	捕获躲过思科邮件安全网关的一般垃圾邮件和灰色邮件。

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。

启用或禁用策略

要启用策略，请点击索引页面（**管理 > 策略**）中的策略名称转到**编辑策略**页面。在此页面的顶部，您将在策略名称正下方看到用于启用该策略的滑块。

图 5-1　　启用策略



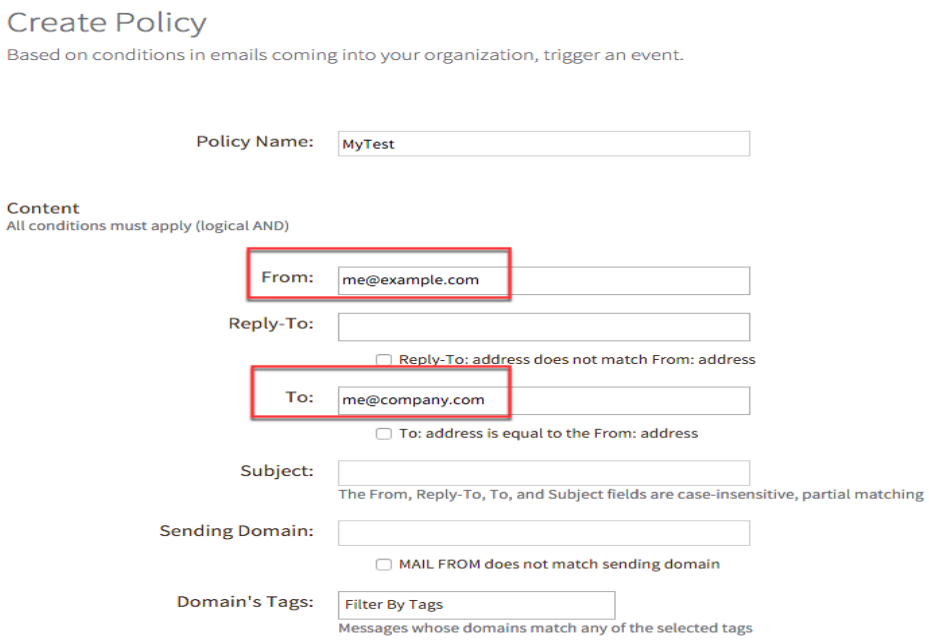
不要忘记使用页面底部的“保存”按钮保存您已启用的策略。

创建您自己的测试策略

我们开始创建测试策略吧。方法很简单：只需要输入三项信息。

步骤 1　在**管理 > 策略**页面中，点击**创建策略**。命名策略，然后在 `From:` 字段中输入您的个人邮件地址，在 `To:` 字段中输入您的收件箱的公司邮件地址。

图 5-2　　创建策略



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。

步骤 2　点击**创建**。

步骤 3　从您的个人账户向您的公司地址发送一封邮件。

步骤 4　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。

图 5-3　　策略事件的策略事件日志

就是这样了。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，您可以添加更多细节并提高复杂性，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。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

既然您已经能轻松创建策略来匹配邮件，现在是时候指定出现匹配项时要采取的操作了。除了默认的日志记录外，您还可以指定另外两项操作：通知和强制执行（仅适用于强制执行客户）。我们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强制执行操作。因此，您在快速了解策略时，最初应该只尝试日志记录，然后仅仅通知管理员，再通知邮件收件人，最后才考虑强制执行。

强制执行客户：请在启用强制执行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）。

我的策略效果如何？

创建一些策略后，您可能需要对结果有一定了解。这些策略能按预期工作吗？匹配的邮件有多少？匹配数量是否呈上升趋势？等等问题。您可以在三个位置检查此类信息。策略日志是正在运行的策略匹配项日志，“管理”>“报告”页面是一段时间内的策略匹配项的综合视图，此外您还可以在“搜索邮件”页面中搜索匹配的策略。

事件日志

点击**管理 > 策略**页面中的**策略日志**选项卡，查看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）。在策略日志中，您可以点击策略名称查看匹配的策略，也可以点击“事件”列中的行查看匹配该策略的邮件的邮件详细信息。您还可以过滤策略日志以显示特定策略的匹配邮件，也可以选择是否在此视图中显示系统通知。

要按策略查看匹配项（一段特定时间内与某个策略匹配的所有邮件），请通过“管理”>“报告”使用策略报告。

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策略报告。

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。

有关强制执行的报告

从“显示策略”列表中选择“含强制执行操作”可查看所有包含强制执行操作的策略的已移动和未移动邮件摘要。

图 5-4　　按强制执行操作过滤策略报告

按需策略

按需策略适用于已为其 G Suite 或 Office 365 环境启用强制执行的思科高级网络钓鱼防护客户。

使用按需策略，您可以选择性地对一组邮件强制执行策略操作。这包括将邮件从用户的收件箱移到特定文件夹（您可有多个文件夹可用于向其中移动邮件），删除邮件或将邮件移回用户的收件箱。思科高级网络钓鱼防护能够在邮件传送至用户的收件箱后对其强制执行操作，为您提供了又一个缓解威胁的工具。例如，如果某些邮件已成功逃过现有防线（例如垃圾邮件和病毒过滤），您可以使用思科高级网络钓鱼防护中的按需策略功能将这些邮件移出用户的收件箱。

备注　按需策略仅当您已为组织启用强制执行时可用。

按需策略从搜索结果页面启动。

在搜索结果页面中，如果您的组织已启用强制执行，将显示“立即强制执行”按钮。

对于超过 2000 封邮件的结果，该按钮将被禁用；您一次只能使用按需策略对 2000 封或更少的邮件强制执行操作。

例如，请注意每个示例中的按钮状态和结果数：

图 5-5　　立即强制执行...按钮可用

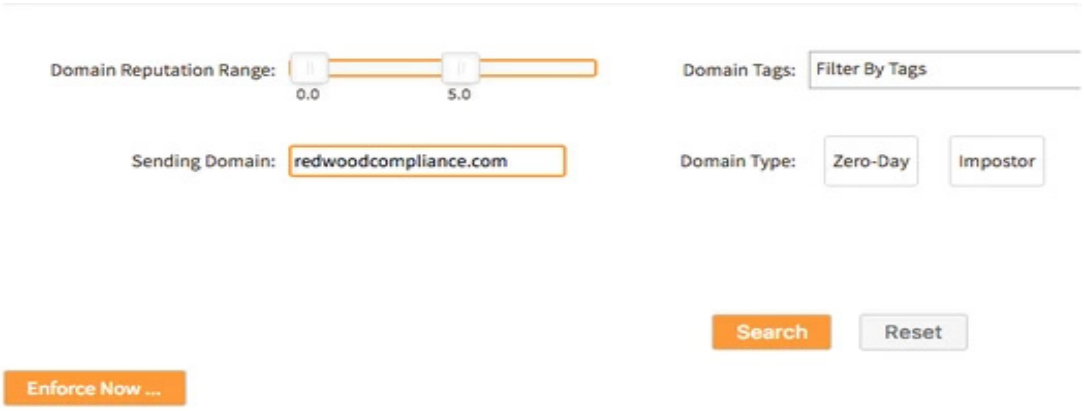


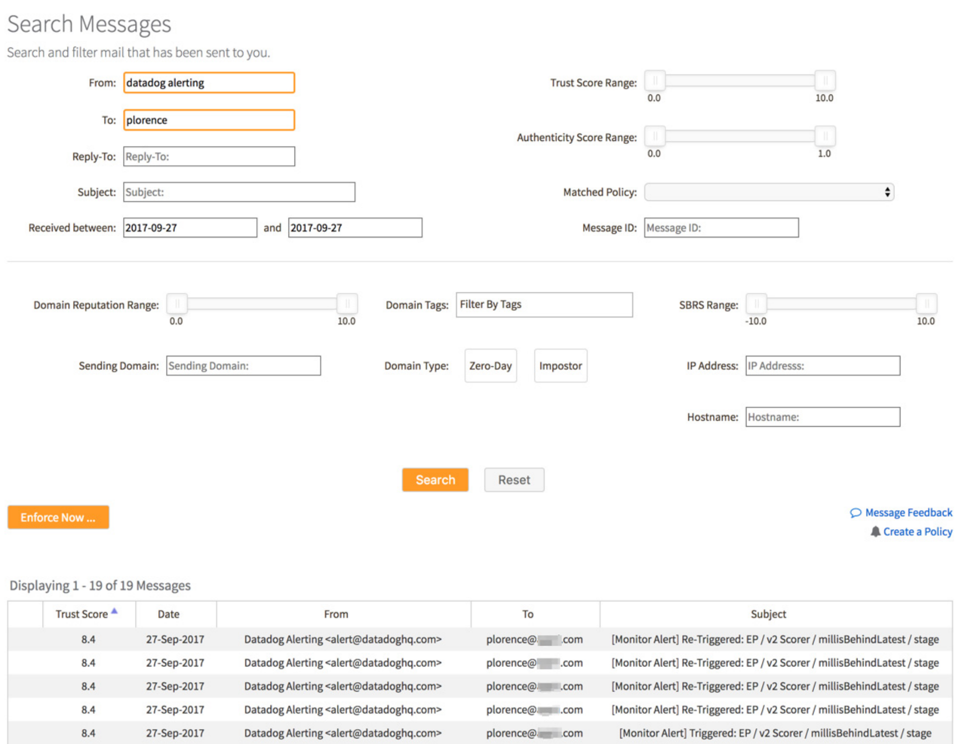
图 5-6　　立即强制执行...按钮不可用

要开始强制执行，请缩小搜索条件范围，让显示的结果少于 2000 封邮件。

您可以将更多条件添加到搜索条件中以缩小结果的范围，例如您可以向“收件人”、“发件人”和“主题”等搜索条件中添加具体的邮件 ID。

在以下示例中，搜索条件缩小到从特定域到一名用户的一组邮件：

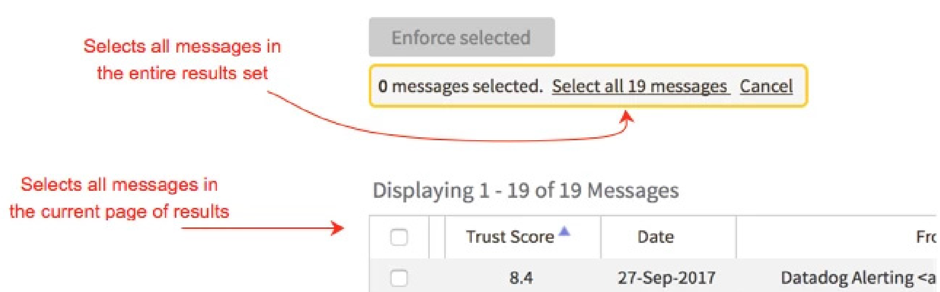
图 5-7　　缩小搜索结果范围



点击“立即强制执行”按钮选择一组结果中的单个或所有邮件。

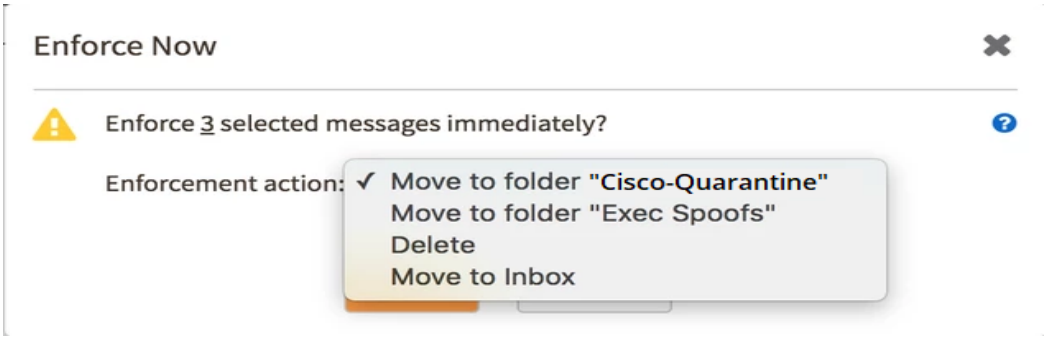
请注意选择整组结果中的所有邮件与选择当前结果页面中显示的所有邮件的区别：

图 5-8　　选择单个邮件与选择所有邮件



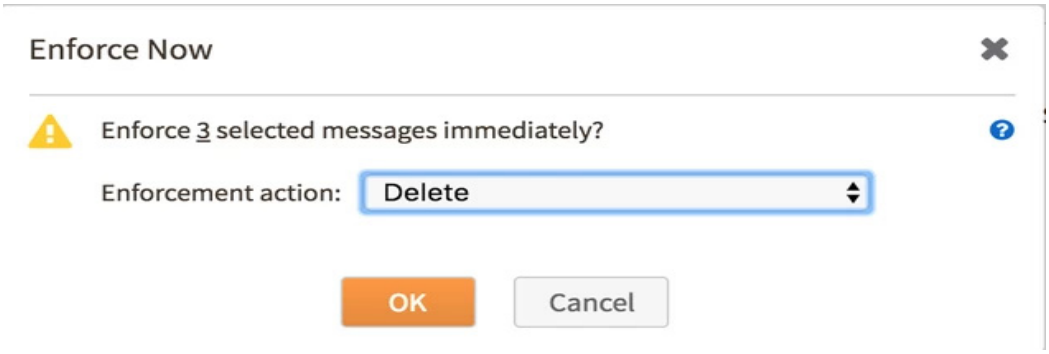
至少选择一封邮件后，点击“对选定内容强制执行”。系统将显示一个对话框，您可在其中确认要对其强制执行操作的邮件数，然后选择您要执行的强制执行操作或取消该过程。（问号图标对不能移动某些邮件的原因提供了更多信息。）

图 5-9　选择强制执行操作



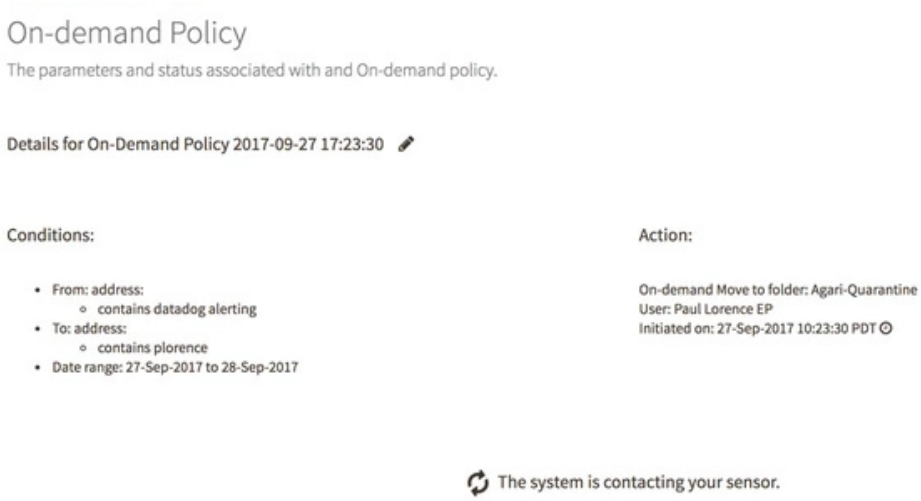
选择强制执行操作后，点击**确定**立即对邮件强制执行操作。

图 5-10　确认按需策略操作



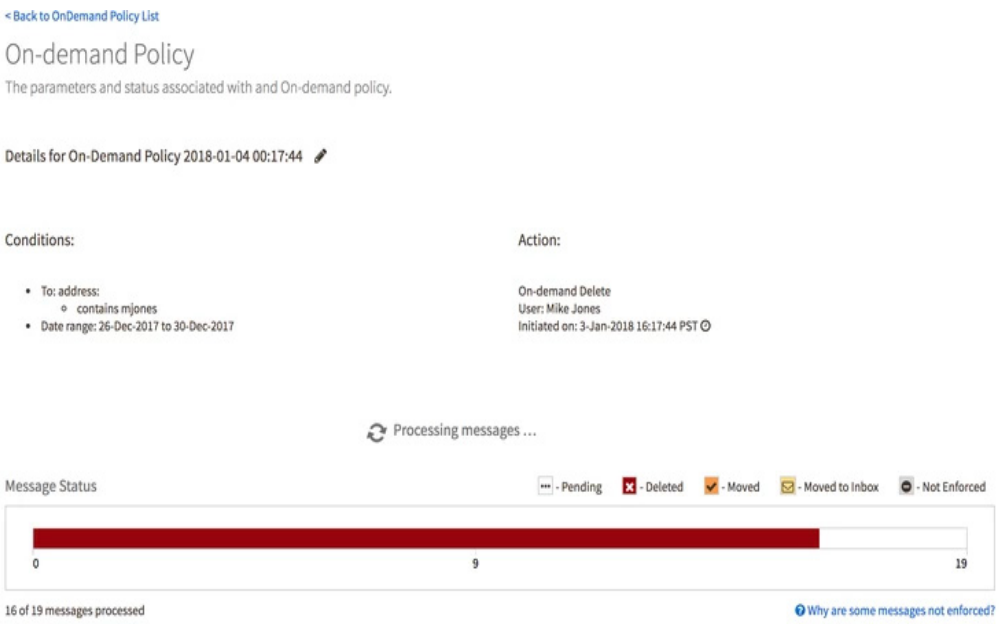
点击确定后将显示按需策略详细信息页面，同时思科 EP 系统会与您的思科高级网络钓鱼防护传感器联系：

图 5-11　　按需策略报告



联系思科高级网络钓鱼防护传感器后，要对其强制执行操作的邮件列表将显示于邮件状态区域中。最初，列出的整组邮件的状态为**待处理**。

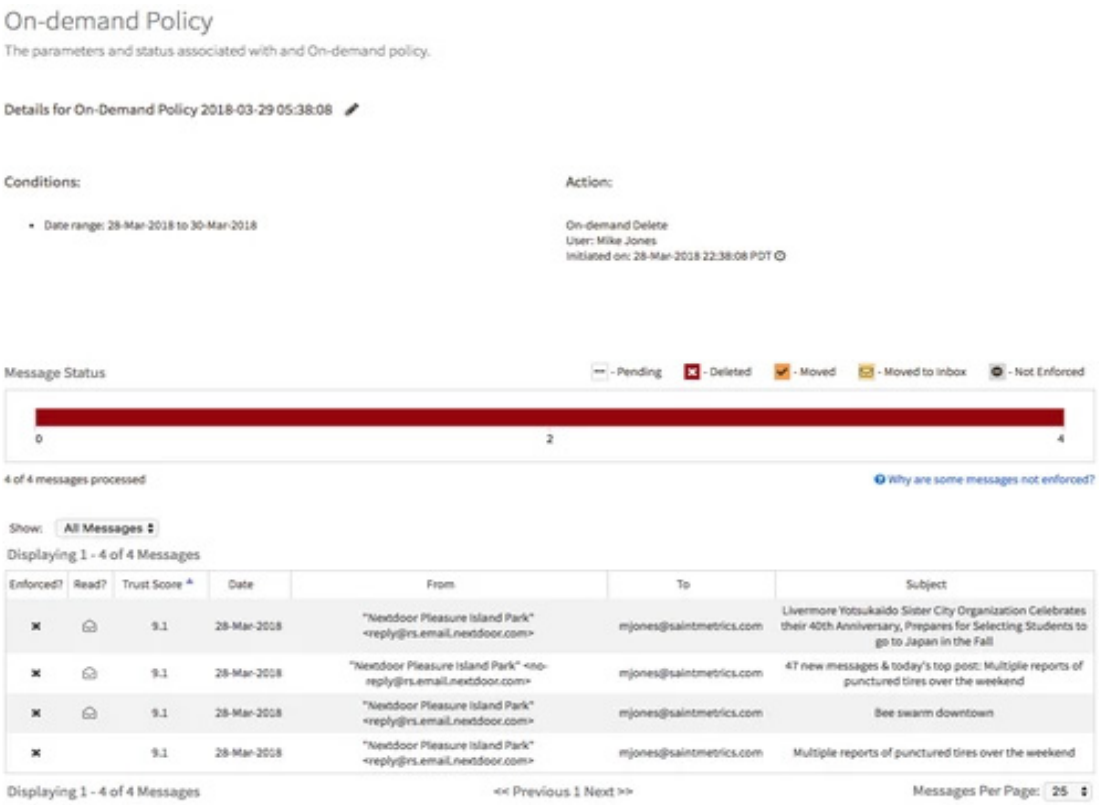
图 5-12　　按需策略的处理中状态



随着系统继续处理这一组邮件，该页面也将在收到有关邮件处置情况（“已删除”、“已移动”、“已移至收件箱”或“未强制执行”）的新信息时刷新。

处理完所有邮件后，该页面将显示按需策略的最终结果：

图 5-13　　按需策略的最终状态



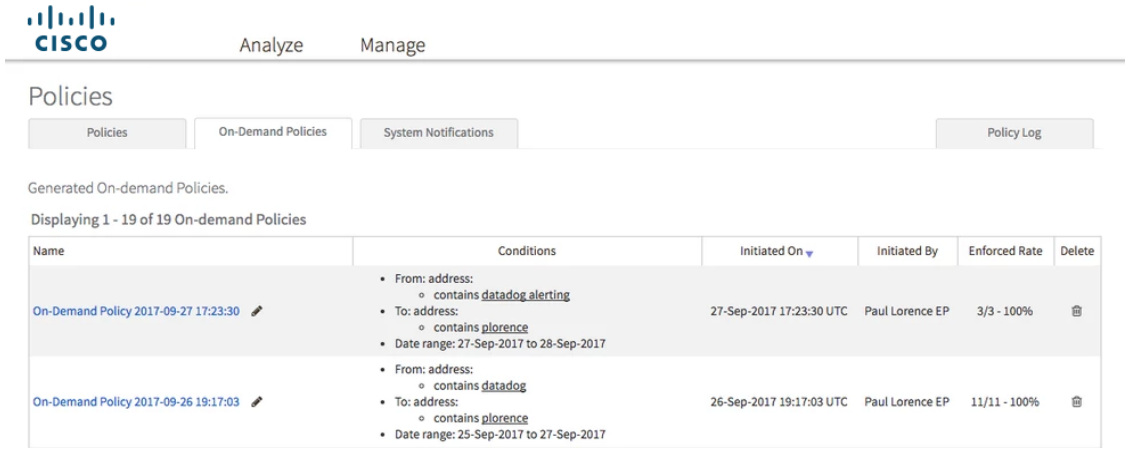
根据需要点击铅笔图标重命名按需策略。（例如，“已删除垃圾邮件”。）

除了强制执行操作的状态外，您还能在强制执行时查看邮件的收件人是否已阅读该邮件。如果“是否已读？”列包含一个打开的信封，则表示收件人已阅读该邮件。

按需策略索引页面

所有按需策略均按时间顺序列于按需策略索引页面中。点击**管理 > 策略**页面中的**按需策略**选项卡可进行查看。

图 5-14　　按需策略索引页面



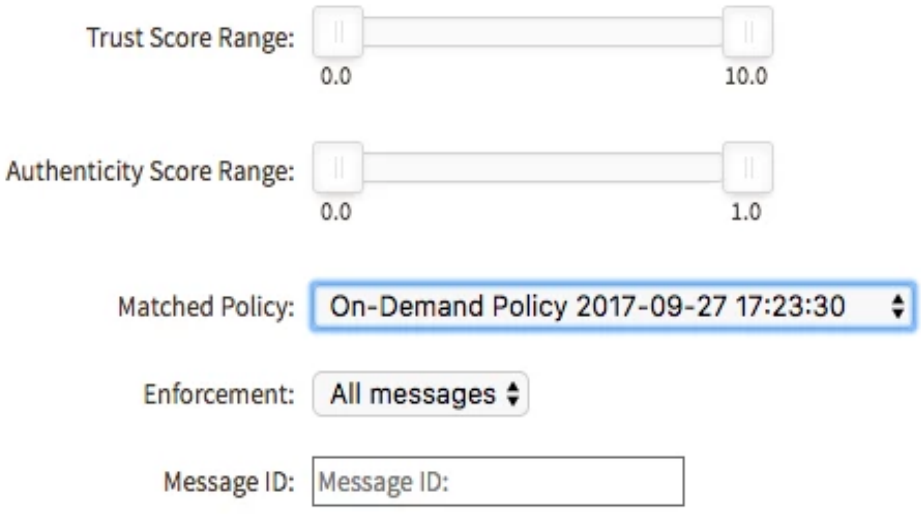
在此视图中，您可以重命名按需策略，并查看条件、启动策略的人和策略的强制执行率。

点击“删除”图标可从此列表中删除按需策略。请注意，点击删除只会从列表中删除按需策略，不会影响邮件的处置情况。

最终说明

按需策略可从搜索页面进行搜索：

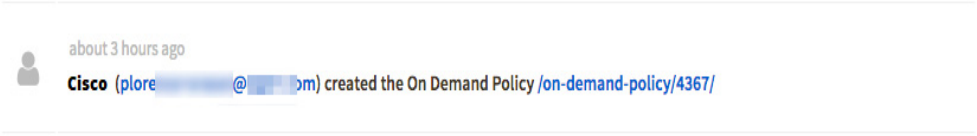
图 5-15　　搜索按需策略



审核日志中将对组织的按需策略进行跟踪。

要查看审核日志，请在“管理”>“组织”页面中点击“审核”链接查看相关条目：

图 5-16　　审核日志中的按需策略



性能注意事项

移动邮件的速度取决于邮箱提供商（G Suite 或 Office 365）中的 API 调用速度和延迟。

按需策略和“常规”（持续使用的）邮件策略的强制执行操作使用的是同一个队列系统。如果您经常从邮件策略对大量邮件强制执行操作，从按需策略向队列中添加更多强制执行操作会影响思科高级网络钓鱼防护中对邮件执行操作的整体性能。队列系统同时接受来自所有传感器的强制执行操作。您可以在以下位置查看任何传感器上的强制执行操作的日志：
`/var/log/agari/enforcer.log`.

管理思科高级网络钓鱼防护

本章介绍以下任务：

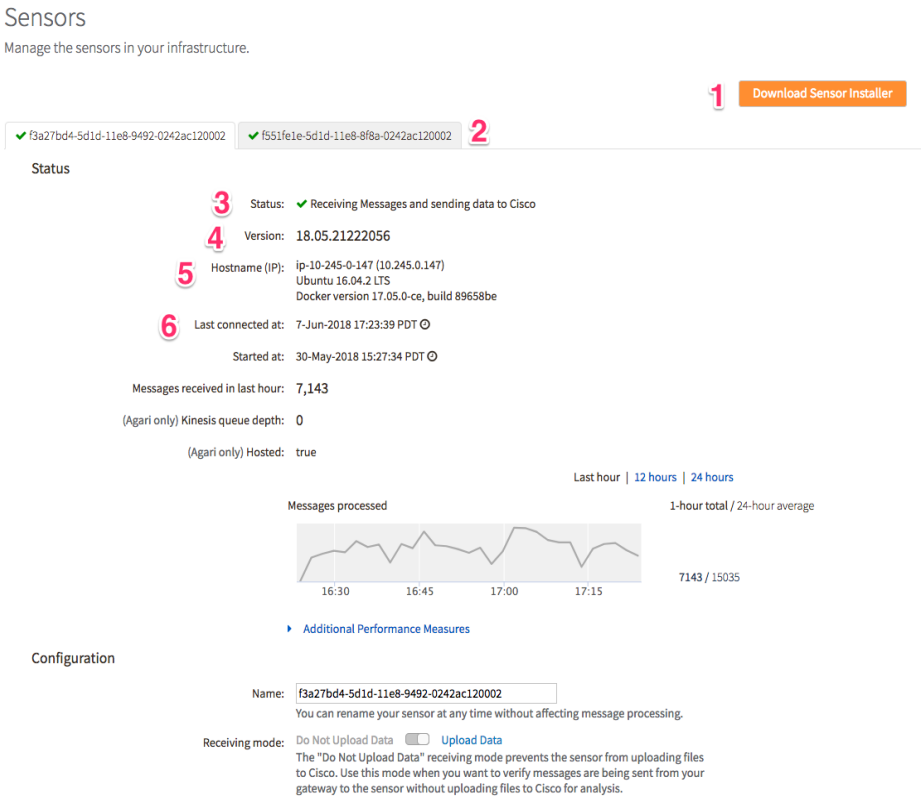
- 管理思科高级网络钓鱼防护
- 发件人管理和快速 DMARC
- 附件分析
- Azure AD 与思科地址组同步

管理思科高级网络钓鱼防护

高级网络钓鱼防护传感器

通过**管理** > **传感器**页面查看思科高级网络钓鱼防护传感器的状态并对其进行管理。

图 6-1　　思科高级网络钓鱼防护传感器页面



1	您可以从思科高级网络钓鱼防护传感器页面下载传感器安装脚本，该脚本具有专门为您的组织生成的密钥。使用此脚本安装其他传感器以处理增加的流量。
2	如果您有多个传感器，请从选项卡列表中选择一个传感器。您可以在此页面中查看思科高级网络钓鱼防护传感器的当前状态并进行配置更改。传感器的总体状态以选项卡上的图标（绿色/黄色/红色）表示。
3	如果您已启用“强制执行”，您可以在选项卡内部看到单独的“发送/接收”和“强制执行”状态图标。当应该对其强制执行操作的邮件有 80% 以上已强制执行时，强制执行图标为绿色，低于该阈值时则为黄色。请参阅“策略报告”页面中的“为什么不能移动某些邮件？”链接，了解包含“强制执行”操作的任何策略（点击“管理”>“报告”页面中策略名称右侧的“匹配邮件数”栏）。
4	更新传感器。从可用版本列表中进行选择，然后点击“更新”。
5	部署了传感器的虚拟机的主机名和 IP 地址。
6	“上次连接”是上次向思科登记思科高级网络钓鱼防护传感器的时间。此时间应该在过去两分钟内（如果思科高级网络钓鱼防护传感器处于活动状态）。

备注　只有当客户为 Office 365 客户时，可能会有一个“下载凭证文件”按钮，供思科高级网络钓鱼防护传感器使用的凭证执行强制执行活动。

点击**保存配置**保存对思科高级网络钓鱼防护传感器所做的任何更改。这些更改将传播到思科高级网络钓鱼防护传感器，最多可能需要 5 分钟才会生效。

系统通知

系统通知是通过**管理** > **策略**页面管理的系统警报。点击**系统通知**选项卡配置并订用通知。您可以基于思科高级网络钓鱼防护传感器、主机系统本身或策略的条件来配置通知。

用户

为思科高级网络钓鱼防护创建并管理用户。用户可以与思科高级网络钓鱼防护交互，以便执行分析并管理策略、用户、组织、思科高级网络钓鱼防护传感器等。

点击“审核用户”链接可以允许用户查看该用户的事件日志，包括登录/注销和更改配置等操作。在“审核日志”页面上，点击页面顶部的“帮助”图标（问号）可了解有关搜索和使用日志的详细信息。

您可以在“编辑组织”页面的“用户账户设置”部分，如下所述为用户设置全局访问策略 - 密码策略、会话超时等。

组织

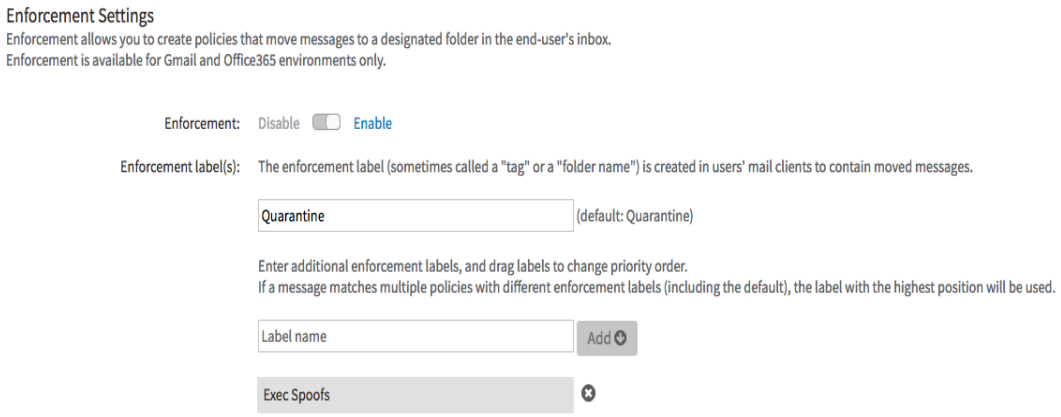
您可以在“组织”页面中管理您的组织。点击**审核**链接可查看您的组织的审核日志，包括用户登录/注销和配置更改等信息。在“审核日志”页面上，点击页面顶部的“帮助”图标（问号）可了解有关搜索和使用日志的详细信息。

点击组织名称可访问“编辑组织”页面。

强制执行设置

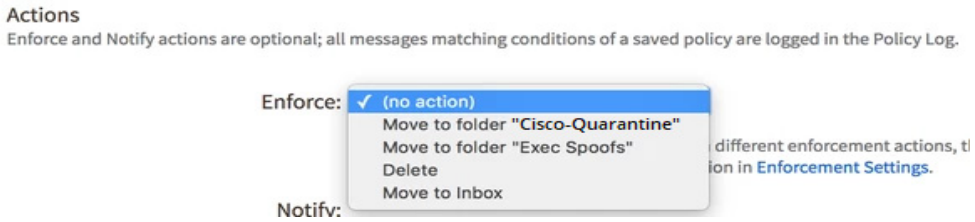
您可以在“强制执行设置”中为您的组织启用或禁用强制执行。

图 6-2　“强制执行设置”部分



您可以在“强制执行设置”中更改默认的强制执行文件夹并设置其他文件夹。这些文件夹显示于所有策略的强制执行操作中，并且是最终用户在其邮件客户端中看到的文件夹的名称或标记：

图 6-3　　强制执行操作



思科高级网络钓鱼防护传感器设置

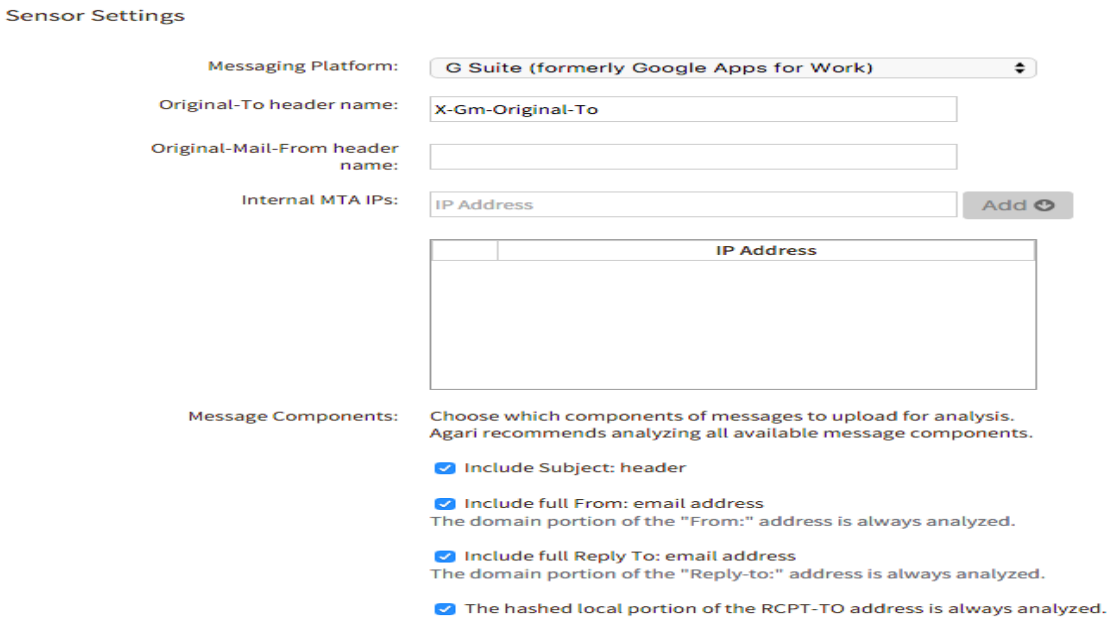
思科高级网络钓鱼防护传感器设置部分是指组织的全局传感器设置。选择上传邮件的哪些组成部分供思科进行分析。思科建议您启用邮件的所有组成部分。

内部 MTA IP 地址

列出发送您要捕获的流量的任何上游 MTA 的 IP 地址。该表单接受使用 CIDR 表示法指定 IP 地址范围。

备注　此设置仅适用于上游 MTA 的情况。

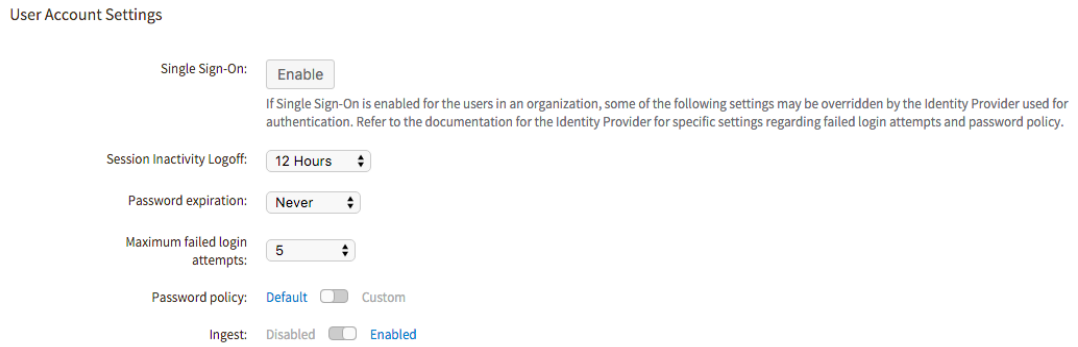
图 6-4　　“传感器设置”部分



用户账户设置

管理全局用户账户访问设置：用户的登录方式、将其注销的时间和密码策略。

图 6-5　　“用户账户设置”部分



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知名发件人。您可以快速了解思科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，您可以在思科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。

使用发件人页面管理发件人

导航至“管理”>“发件人”查看您的域的知名发件人。

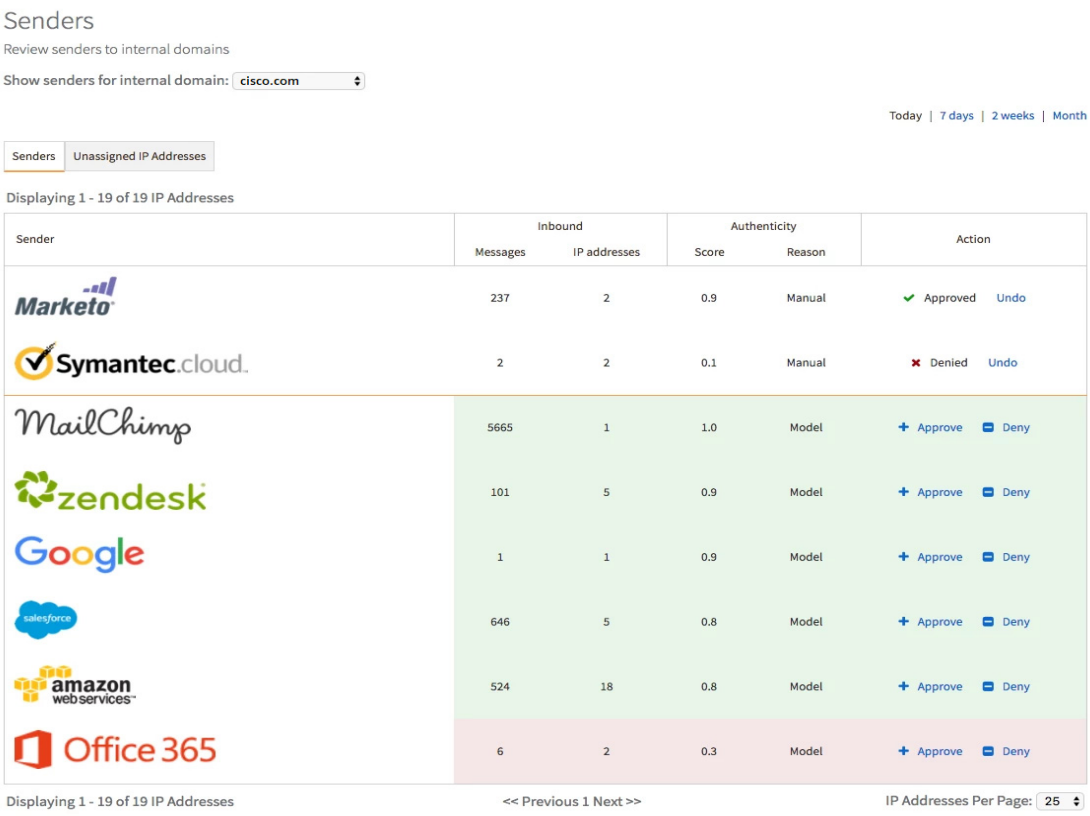
该页面将默认过滤出数量最高的内部域并显示今天的数据。

要更改您正在查看的域，可以点击域名旁的向上/向下箭头。

备注　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。要查看未分配给知名发件人的 IP 地址，请切换到“未分配的 IP 地址”选项卡。

图 6-6　　“发件人”页面



各列的含义和用途

- **发件人**：知名发件人的名称/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**：在指定时间段内发现的来自该域/发件人组合的邮件数。
- **入站 - IP 地址**：在指定时间段内发现从该域/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/域组合的思科发件人建模的平均全局真实性评分。

备注　此处显示的真实性评分是整个时间段内在整个思科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*表示评分是根据思科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思科高级网络钓鱼防护的发件人建模功能对其建模的状态。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，确保思科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，确保思科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。

关联发件人管理与快速 DMARC

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强制执行策略，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 IronPort 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 EP 中的发件人操作后，您可以转到“管理”>“策略”页面并设置用于强制执行的快速 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。

步骤 1　在**管理 > 策略**页面中点击快速 DMARC 策略名称转到**编辑策略**页面。

步骤 2　在“策略名称”下，将滑块移到**启用**。

步骤 3　向下滚动到**操作**部分为此策略设置强制执行操作并/或启用策略匹配警报。

步骤 4　点击页面底部的**保存**。

2018 年 1 月之前在 EP 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：

步骤 1　点击**管理 > 策略**页面中的**创建策略**。

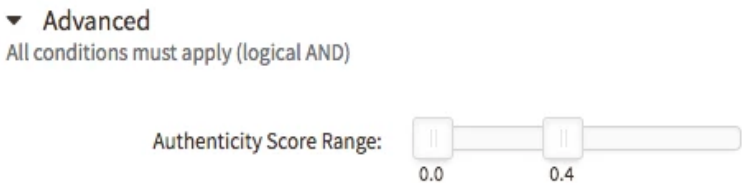
步骤 2　在“策略名称”中输入“快速 DMARC”。

步骤 3　向下滚动到“域标记”并点击空文本框。从可用域标记列表中选择“内部”。

步骤 4　向下滚动并打开**高级**切换开关。

步骤 5　将**真实性评分范围**的上限移到 0.4。结果应如下所示：

图 6-7　　“策略”页面中的真实性评分滑块



步骤 6　点击页面底部的**保存**。

附件分析

思科高级网络钓鱼防护能够分析邮件附件，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。

思科高级网络钓鱼防护中可能有两个级别的附件分析：

- 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。

启用附件分析

思科高级网络钓鱼防护中的附件分析是一个多步骤流程，具体取决于您要执行哪个级别的分析。

附件基本信息收集

如果只收集附件名称和文件扩展名信息而不执行完整的附件扫描，您必须启用组织级别的设置才能让思科高级网络钓鱼防护收集此信息。

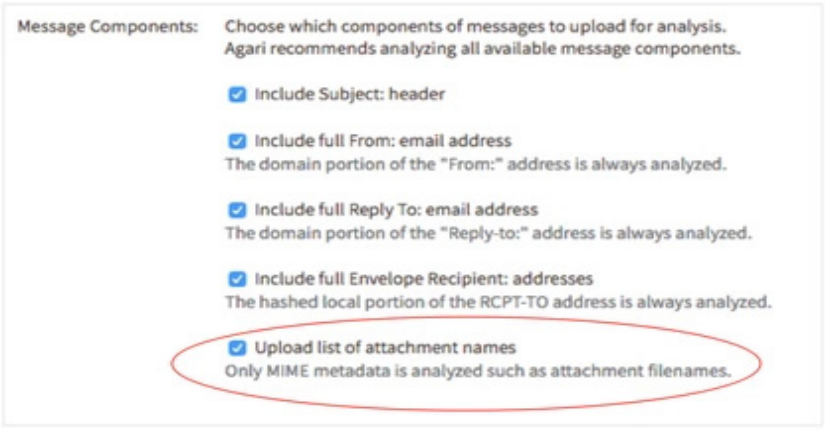
步骤 1　导航至“管理”>“组织”

步骤 2　向下滚动到思科高级网络钓鱼防护传感器设置部分，再向下滚动到“邮件组件：”设置。

步骤 3　选中“上传附件名称列表”旁的复选框为您的组织启用此设置。

步骤 4　滚动至页面底部并点击**保存**。

图 6-8　　“上传附件名称列表”复选框



附件扫描

必须逐个传感器启用附件内容恶意企图扫描。如果您自行管理思科高级网络钓鱼防护传感器环境，您可以选择只在一部分传感器设备上扫描附件，将包含附件的邮件路由到这些特定传感器。

备注　附件扫描可能需要升级传感器主机系统虚拟机或计算机。您还需要为这些传感器打开一个新的防火墙缺口。有关思科高级网络钓鱼防护传感器主机系统规格的更新，请参阅安装思科高级网络钓鱼防护传感器，第 1-1 页。

步骤 1　首先，您必须执行上述步骤设置有关附件名称收集的组织级别策略。

步骤 2　导航至**管理 > 传感器**页面。

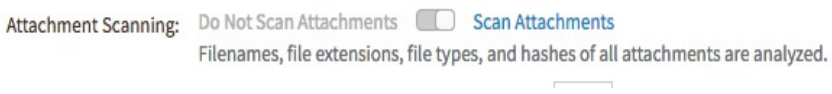
步骤 3　向下滚动到**配置**部分。

步骤 4　将“附件扫描：”滑块移至“扫描附件”。

步骤 5　点击页面底部的**保存配置**。

步骤 6　如有多个传感器，请在您希望其执行附件扫描的每个传感器所对应的选项卡中重复这些步骤。

图 6-9　　启用附件扫描

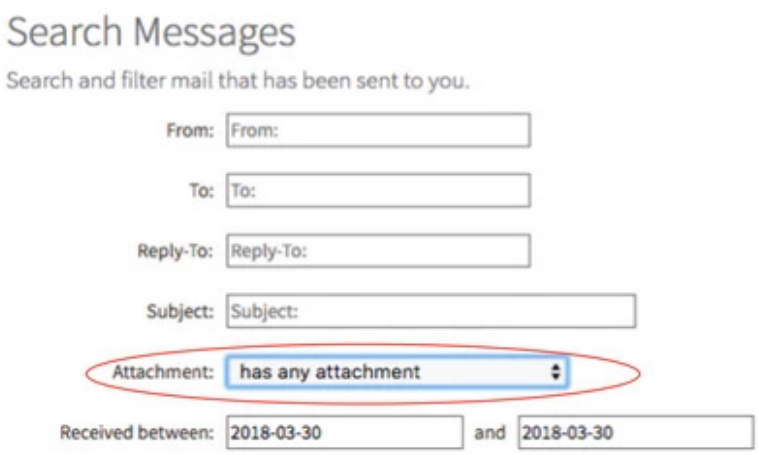


使用附件分析

在搜索和策略中使用附件分析结果

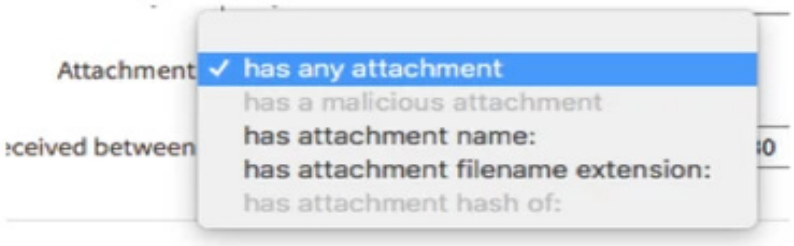
您会发现，“分析”>“搜索邮件”页面中有一个新选项。当您要创建或编辑策略时，“管理”>“策略”页面中也会显示相同的字段。

图 6-10　搜索包含附件的邮件



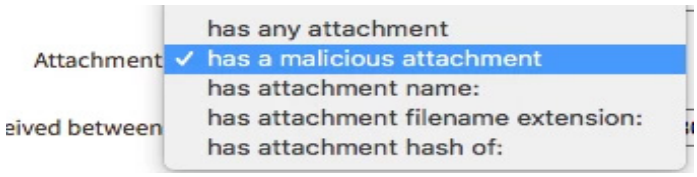
如果只收集附件名称信息，则以下选项可用于搜索和设置策略。

图 6-11　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。

图 6-12　　搜索附件：已启用附件扫描

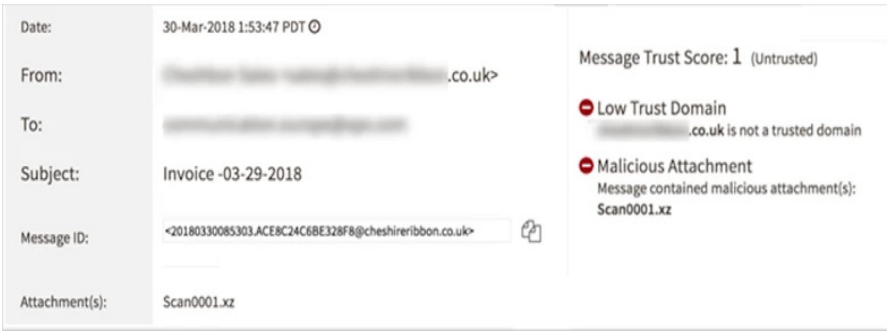


附件扫描结果

启用附件扫描时，思科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。

备注　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。

图 6-13　　“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

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

思科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、邮件文件、图像文件、平面数据文件、RTF
- Flash、视频格式、Javascript、VBA

Azure AD 与地址组同步

通过将 IronPort 地址组与 Azure Active Directory 组同步，可以更高效地管理基于地址组的策略。IronPort 会自动将 Azure AD 组的成员拉到同步后的地址组中，让您不必再为手动更新而担心。

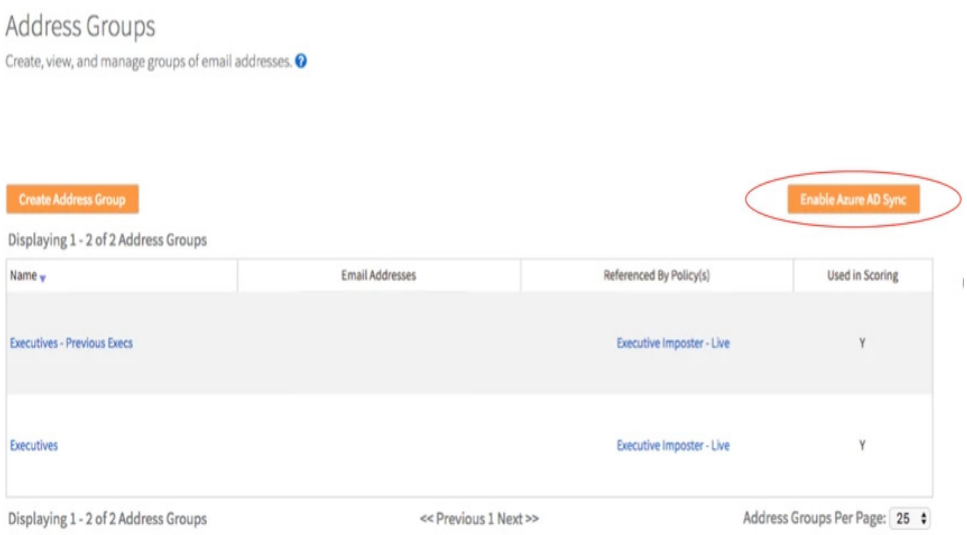
要了解如何在策略中使用地址组，请参阅通过策略管理传入邮件，第 5-1 页。

设置地址组同步

要设置地址组同步，首先必须授权思科与您的 Azure AD 同步。

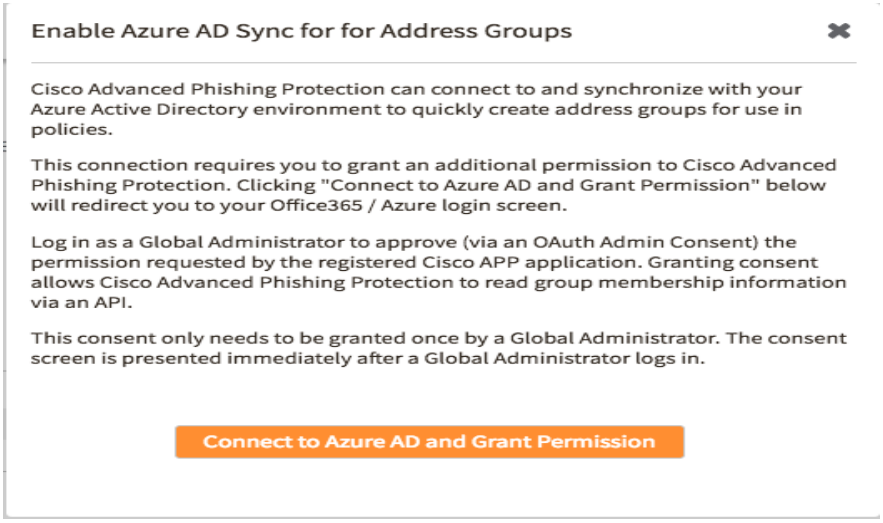
步骤 1　点击**管理** > **地址组**页面中的**启用 Azure AD 同步**。

图 6-14　“启用 Azure AD 同步”按钮



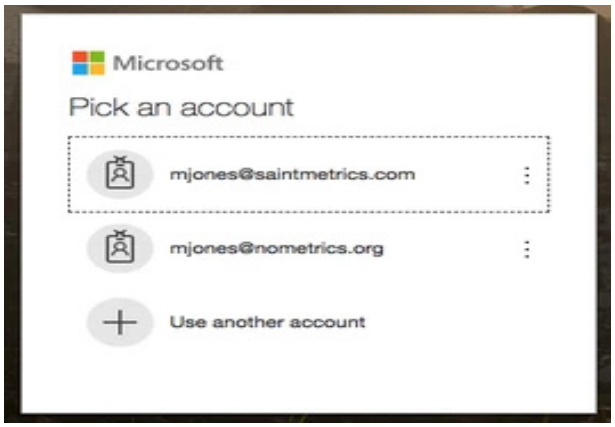
步骤 2　系统将显示一个对话框，用于连接到 Azure AD 并授予权限。您需要以全局管理员身份登录才能执行此操作。

图 6-15　连接到 AD



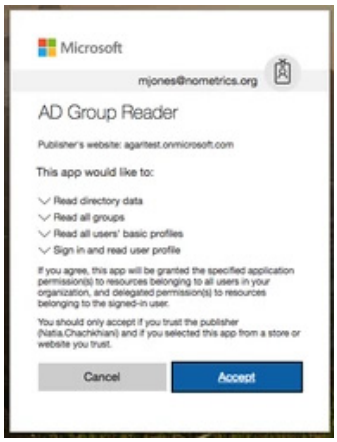
步骤 3　您将被定向至 Microsoft 以选择您要用于授予许可的账户，并需要登录该账户。

图 6-16　　向 AD 进行身份验证



步骤 4　登录时，系统将显示用于批准思科 AD 组阅读器应用的选项。

图 6-17　　授予权限



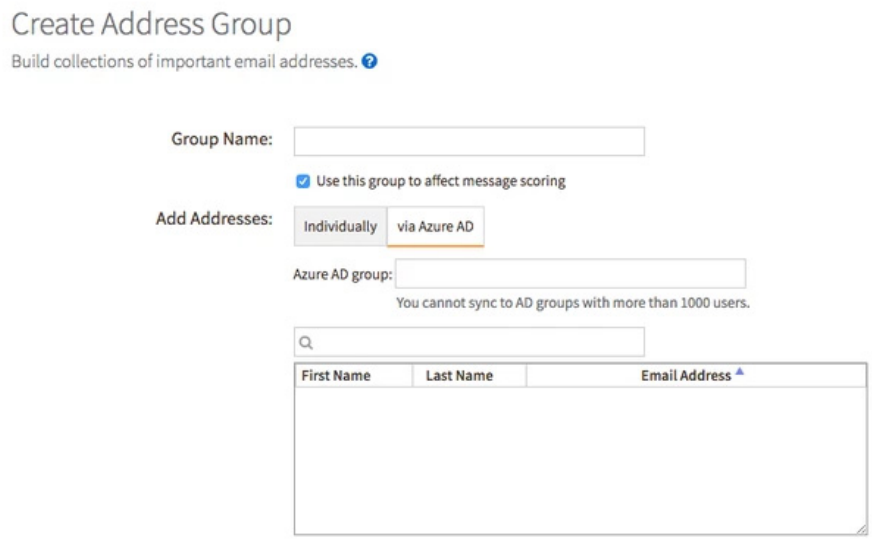
步骤 5　批准后，您将被重新定向回思科高级网络钓鱼防护应用，并将获得与 Azure AD 进行组同步的授权。

创建已同步的地址组

步骤 1　现在，您已与 Azure AD 同步，请点击**管理 > 地址组**页面中的**创建地址组** 。

步骤 2　您现在可以使用“通过 Azure AD”选项添加地址。

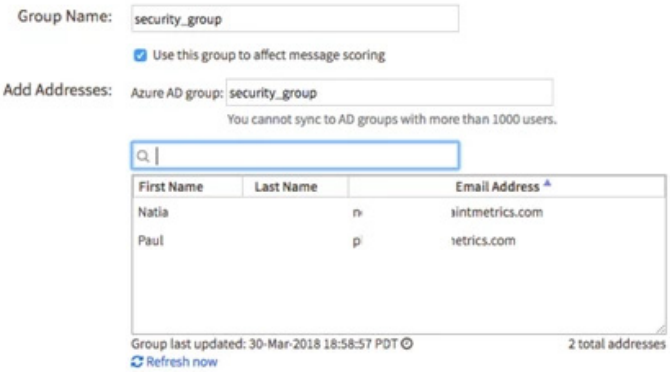
图 6-18　从 AD 组创建地址组



步骤 3　点击 **Azure AD 组**下拉框查看可用组列表。

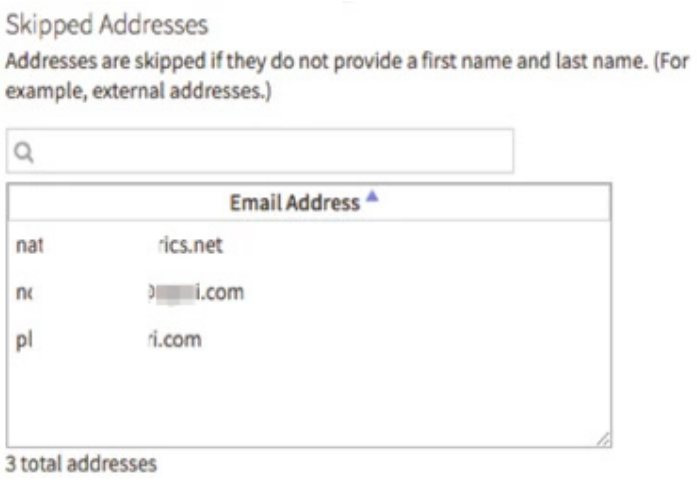
步骤 4　选择您要同步的组。系统将显示该组中的名称和邮件地址。

图 6-19　选择 AD 组



步骤 5　如果 Azure AD 组中存在无法与地址组同步的成员，它们将显示于**跳过的地址**部分。

图 6-20　　跳过的地址



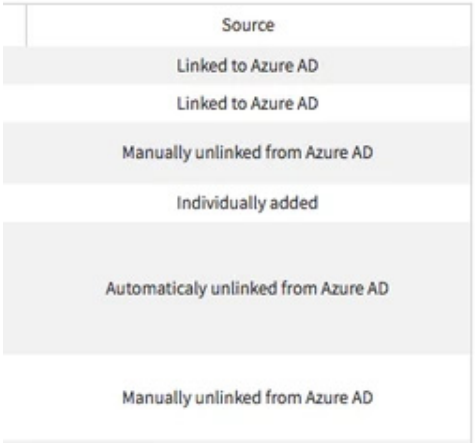
步骤 6　点击页面底部的**创建**保存地址组。

解除已同步地址组的关联

查看“管理”>“地址组”页面中的“来源”列可以得知地址组已同步。您将看到“与 Azure AD 关联”。

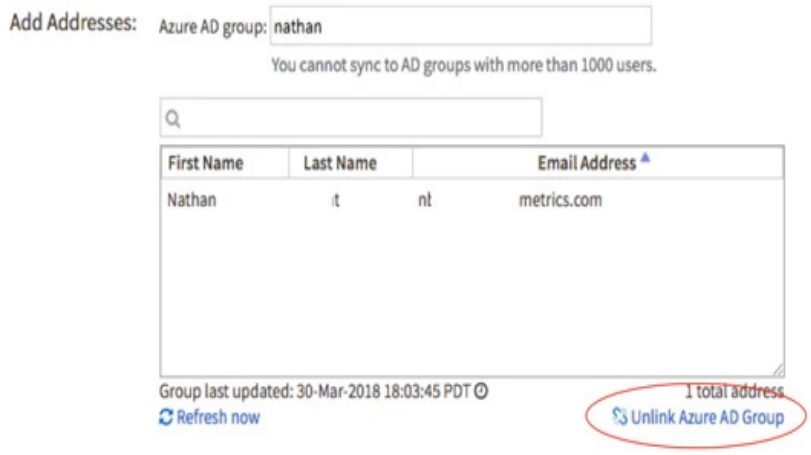
其他状态包括“单独添加”、“已手动解除与 Azure AD 的关联”和“已自动解除与 Azure AD 的关联”。

图 6-21　　地址组索引页面中的“来源”列



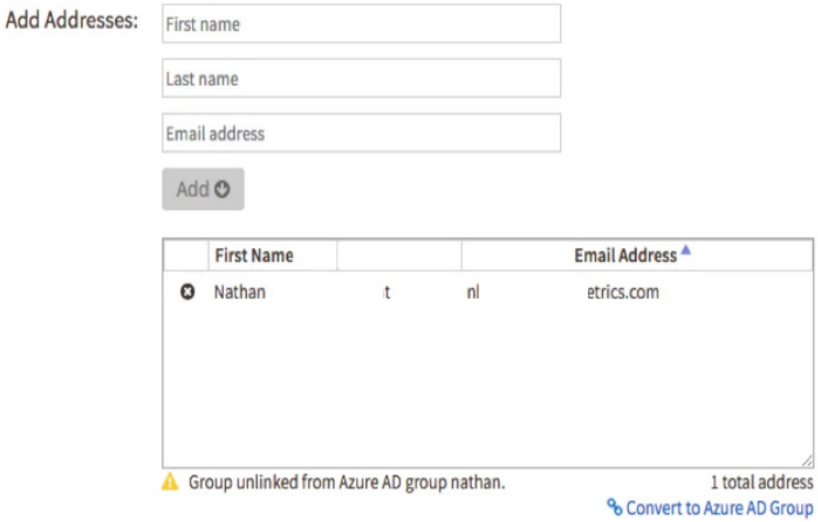
步骤 1　点击已关联组的名称转到“编辑地址组”页面。在名称框下方的右侧，您将看到“解除 Azure AD 组的关联”链接。

图 6-22　　解除 Azure AD 组的关联



步骤 2　点击该链接将阻止该组与 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。

图 6-23　　与 Azure AD 解除关联的地址组



步骤 3　点击页面底部的**保存**以保存地址组。

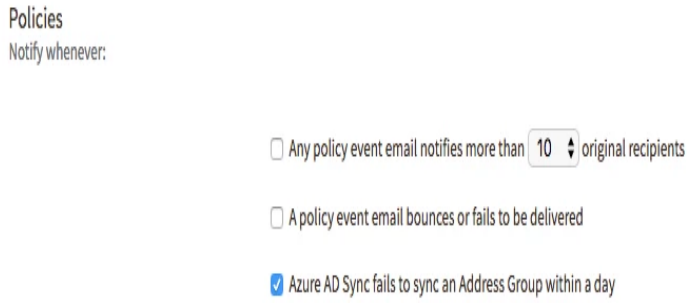
Azure AD 组同步失败通知

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。

步骤 1　导航至“管理”>“策略”，然后点击**系统通知**选项卡。

步骤 2　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。

图 6-24　　启用 Azure AD 同步失败系统通知



单点登录 (SSO)

思科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（账户）与思科高级网络钓鱼防护用户名绑定，无需单独的思科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 提供程序中删除访问权限，而不必直接登录思科高级网络钓鱼防护门户。
- 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）只向思科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）向 IronPort 中存储的凭证进行身份验证。

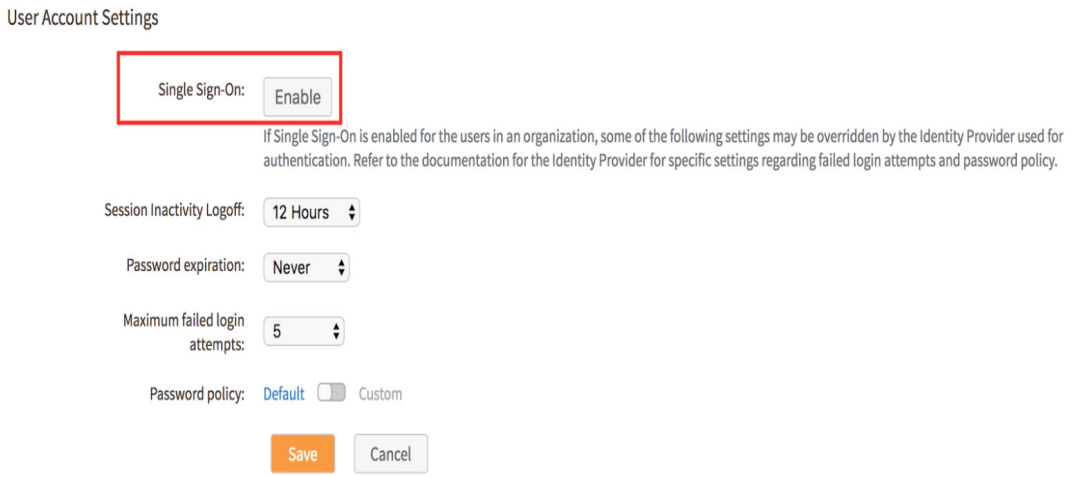
要为组织启用单点登录，请执行以下操作：

步骤 1 登录思科高级网络钓鱼防护并导航至“管理”>“组织”页面。

步骤 2 导航至“用户账户设置”配置部分。

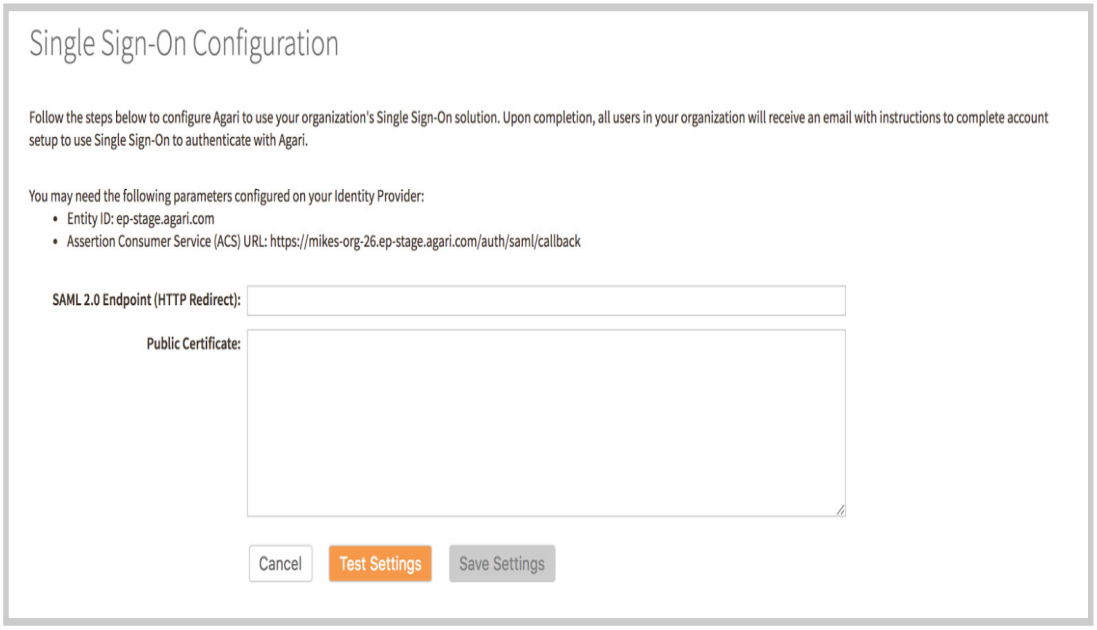
步骤 3 点击“启用”以启用单点登录。

图 7-1　　单点登录“启用”按钮



系统将显示“单点登录配置”页面。

图 7-2　　配置和测试单点登录



在该对话框中，输入如下信息：

- 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)

  这两个值都应该由单点登录身份提供程序向您提供。

a. 点击**测试设置**验证身份提供程序提供的终端 URL 和证书值。

   测试设置按钮将调用在您输入的位置具有公共证书凭证的身份提供程序。

   如果设置正确，浏览器会被重定向至思科高级网络钓鱼防护，并显示成功消息。

b. 点击页面底部的**保存设置**，为组织保存所有设置并为用户账户启用单点登录。

备注　警告! 此时将启用单点登录并且：

- 所有现有用户将收到一封邮件，指导他们如何执行用户名与 SSO 账户的一次性绑定，以便在访问思科高级网络钓鱼防护时使用单点登录身份提供程序凭证。
- 当前已登录系统的用户将继续其会话而不中断；但是，他们将在以后尝试登录时被定向至身份提供程序

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，用户需要进入思科高级网络钓鱼防护登录页（https://appc.cisco.com）并输入其邮件地址。IronPort 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思科高级网络钓鱼防护概述页面。