思科域保护用户指南

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

概述

简介

本指南为您介绍 **DMARC**（基于域的邮件身份验证、报告和一致性），以及如何使用思科域保护™引导您完成为贵组织实施 DMARC 的过程。

思科域保护旨在帮助您保护您的客户，通过为您的域建立 DMARC 策略，使您的客户免遭试图发送声称来自您方的虚假邮件的网络钓鱼者、垃圾邮件发件者和其他邮件滥用者的侵扰。

DMARC 是邮件身份验证、策略和报告协议。它基于广泛部署的 SPF 和 DKIM 协议构建，添加了相应链接指向作者（“发件人：”）域名、用于处理未通过身份验证情况的已发收件人策略，以及从接收者到发件人的报告，从而提升和监控对域的保护，避免受到欺诈邮件的侵扰。

受众

本指南旨在供将要开始为其组织管理 DMARC 的邮件管理员使用。

自助方式及按需帮助

您可以借助思科域保护和本指南来完成为域设置、管理和维护 DMARC 策略的过程。

思科域保护可让您查看涉及您的品牌的邮件相关的数据，为您提供以有意义的方式分析数据的工具以及生成各种文件用于实施 DMARC 的工具，此外它还会就如何完成无法通过用户界面实现的任务提供一些有用提示。

历史：使用 DMARC 的必要性

尽管邮件非常重要、无处不在且功能强大，但却一点儿也不安全。

之前在安全性方面所做的尝试未能解决邮件的基本缺陷 - 任何人均可使用他人的身份发送邮件。这种缺陷让犯罪分子对世界知名品牌的侵犯有了可乘之机：通过邮件，犯罪分子可以使用几乎任何品牌来发送垃圾邮件、网络钓鱼邮件以及安装的恶意软件，对客户造成直接损失，将公司花费多年建立的品牌资产毁于一旦。

全球许多极富盛名的品牌（包括 Facebook、Apple、JPMorgan Chase 和 PayPal）都采用 DMARC 标准保护自己的客户和品牌。

使用 DMARC，公司可获得对于使用其域名发送的合法邮件及欺诈邮件的空前可视性。DMARC 的强大之处在于能够了解声称是从您那里（第三方、业务部门、威胁实施者）发出的所有不同邮件流。采用 DMARC 的公司获得的整体收益是保留品牌资产，消除与邮件欺诈相关的客户支持成本，以及重拾客户对公司邮件通道的信任与使用。

DMARC 是全球 70% 的收件箱以及大多数注重安全的品牌所支持的开放标准，也是支持互联网规模邮件保护并防止欺诈性使用合法品牌进行邮件网络攻击的唯一解决方案。

基础知识：DMARC 是什么？

DMARC（基于域的邮件身份验证、报告和一致性）是 2012 年由行业联盟 DMARC.org 发布的一项开放邮件标准，旨在保护邮件通道的安全。DMARC 扩展了先前建立的身份验证邮件标准，是邮件发件人将他们正在发送的邮件确实为他们所发送这一消息告知邮件接收者的唯一方式。

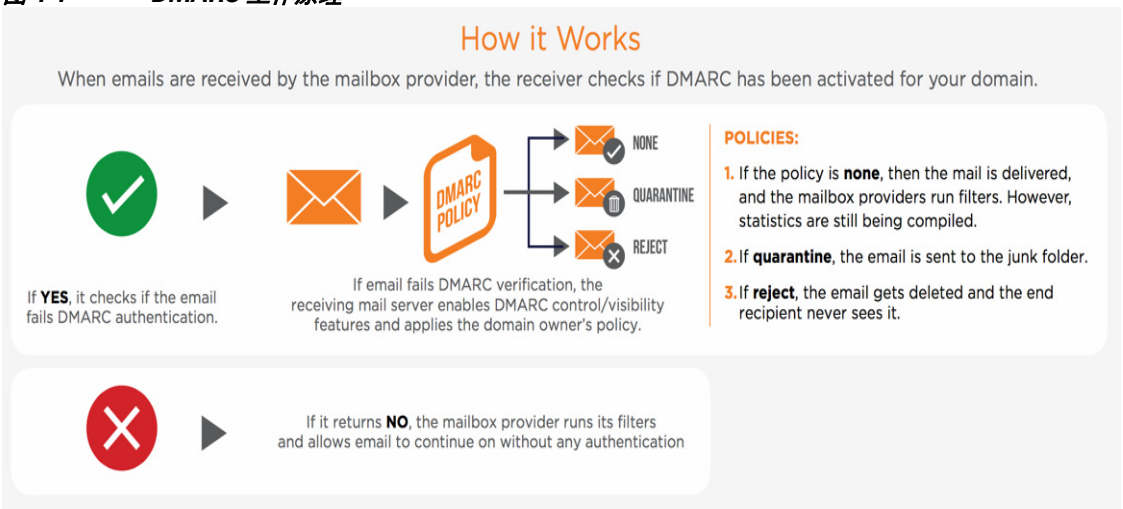
DMARC 允许发送邮件的公司：

- 面向其邮件发送域**验证所有合法邮件**邮件和域，包括从您自己的基础设施发送的邮件以及由第三方发送的邮件。
- **发布明确策略**，指示邮箱提供商如何处理可证明其真实性的邮件邮件。这些邮件可以发送到垃圾邮件文件夹，也可以完全被拒绝，从而保护未设防的收件人免遭攻击。
- 通过使他们知道正在从其域发送邮件的人来**获得有关其邮件流的信息情报**。此数据不仅可帮助公司识别对他们的客户产生的威胁，还可发现他们甚至可能不知道的合法发件人。

DMARC 实施策略是什么？

当您为组织设置 DMARC 策略时，您作为邮件发件人即表示您的邮件受到保护。该策略会告知接收者在通过或未通过 DMARC 中的一种身份验证方法时，应当如何应对。

图 1-1　　DMARC 工作原理



DMARC 得到了哪些客户的认可？

DMARC 得到全球最大发件人、接收者和行业财团的认可。全球超过 25 亿个邮箱均已启用 DMARC。

支持 DMARC 标准的全球最大的一些邮件*发件人*包括以下组织：

图 1-2　　支持 DMARC 的发件人

支持 DMARC 的全球最大的一些邮件*接收者*包括以下组织：

图 1-3　　支持 DMARC 的接收者

此外，以下*政府机构和行业贸易组织*也认可 DMARC 标准：

政府机构：

- **NIST** - 美国国家标准技术研究所
  https://www.nist.gov/
- **FTC** - 美国联邦贸易委员会
  https://www.ftc.gov/
- **GOV.UK** - https://www.gov.uk/

行业协会

- **OTA** - 在线信任联盟
  https://otalliance.org/
- **M3AAWG** - 信息传递、恶意软件和移动反滥用工作组
  https://www.m3aawg.org/
- **DMARC.org** - https://dmarc.org/
- **FS-ISAC** - 金融服务信息共享和分析中心
  https://www.fsisac.com/
- **NH-ISAC** - 美国国家卫生信息共享与分析
  https://nhisac.org/

DMARC 的优势：它为何值得您关注

品牌保护

犯罪分子利用您的域来牟取个人利益只是时间问题。不管犯罪活动是网络钓鱼、恶意软件传播还是令人不快的垃圾邮件，它都会损害与这些攻击关联的品牌。

增加的邮件传送性

如果接收者无法分辨邮件的好坏，那么即使合法邮件也可能会被转至垃圾邮件文件夹。

通过部署 DMARC，您可以改进合法邮件的传送性，同时消除欺诈。

服务电话

如果客户起初未曾收到网络钓鱼邮件，则不会致电或发送邮件来询问此类邮件的事宜！一个思科客户在受到严重网络钓鱼攻击的域中发布拒绝策略后，能够重新部署 60 位工作人员。

对网络攻击风险的可视性

您是否知道代表您的公司发送邮件的每个第三方公司？尽管第三方发件人是不可或缺的，但是每次向第三方提供客户、员工或合作伙伴详细信息，都会增加遭受网络攻击的风险。DMARC 使您可以查看代表您发送邮件的第三方，以确保其遵循邮件最佳做法。

入站优势

实施 DMARC 还可避免一些入站邮件威胁，如 BEC。

什么是 BEC？

商务邮件入侵 (BEC) 是一种入站威胁，具体是指攻击者冒充公司高管发送欺诈邮件，请求电汇至欺诈性的备用帐户。通常，该威胁会导致成功入侵和访问受害者的凭证。

特征

- 通过社会工程和数字欺骗来驱动
- 不含恶意链接、恶意软件或恶意内容
- 轻松规避重要的安全邮件网关

DMARC 和入站威胁：部分解决方案

经过正确配置后，DMARC 会拦截网络钓鱼攻击（攻击者发送的邮件具有看似来自受保护域的“发件人”地址）。这使它非常适合出站网络钓鱼防御，但不是用于入站流量的可接受解决方案。

表 1-1　　由 DMARC 策略拦截的入站威胁

入站欺骗技术	由 DMARC 解决？
直接/相同域欺骗	是
显示名称欺骗	否
相似域欺骗	否

尽管 DMARC 可部分解决 BEC 和复杂的入站威胁，但您仍需要通过一种可识别各类发件人身份欺骗的全面保护层来加强网关保护。

标准 - 详细了解

SPF - 发件人策略框架

SPF（发件人策略框架；IETF 2014 年 4 月的 RFC 7208）是一种身份验证标准，这种标准允许域所有者指定授权哪些服务器发送在“发件人：”邮件地址中具有其域的邮件。SPF 支持接收者查询 DNS 来检索给定域的授权服务器列表。如果邮件通过授权服务器送达，则接收者可将邮件视为真实可靠。

图 1-4　　SPF 的 DNS 记录示例

```
example.net. IN TXT "v=spf1 a mx -all"
```

不足 - SPF 并非是适合所有邮件使用情况的理想标准，如果遇到邮件转发，可能会失败。邮件收件人无法轻松查看由 SPF 进行身份验证的“发件人:”域。

DKIM - Domainkey 识别的邮件

DKIM（域密钥识别的邮件；2018 年 1 月的 RFC 8301）是一种以加密方式将域名与邮件关联的身份验证标准。发件人将加密签名插入邮件，而接收者可以使用 DNS 托管的公钥来验证该邮件。验证成功后，DKIM 会提供在转发时继续存留的可靠域级别标识符（不同于 SPF)。

图 1-5　　DKIM 的 DNS 记录示例

```
selector._domainkey.example. net IN TXT "v=DKIM1; k=rsa; p=public
key data"
```

不足 - DKIM 的设置通常比 SPF 更加复杂，要求发送的每封邮件都有加密签名。如果内容在传输过程中被修改，将无法通过 DKIM，如通过邮件列表发送的邮件

DMARC - 基于域的邮件身份验证、报告和一致性

DMARC（基于域的邮件身份验证、报告和一致性；2015 年 3 月的 RFC 7489）是一种邮件身份验证标准，可与 SPF 和 DKIM 结合使用，为邮件带来缺少的功能 - 使发件人可以获得对其邮件域使用方式和滥用方式的可视性，描述如何将现有身份验证技术组合使用来创建安全的邮件通道，以及为接收者提供有关如何安全地处理未授权邮件的明确指令，而且全部都达到互联网规模。

图 1-6　DMARC 的 DNS 记录示例

```
dmarc.domain.com. IN TXT "v=DMARC1; p=reject;
rua=mailto:d@rua.agari.com; ruf=mailto:d@ruf.agari.com;"
```

图 1-7　DMARC 基于 DKIM 和 SPF 构建以提供保护和报告

结构：DMARC 的工作原理

DMARC 模型使用 DNS 作为策略发布机制。DMARC 记录以 DNS TXT 记录的形式托管在 DMARC 特定的名称空间中。DMARC 名称空间的创建方式为：在要符合 DMARC 标准的邮件域前面附加“_dmarc.”。例如，如果邮件域“example.com”发布一条 DMARC 记录，则为“_dmarc.example.com”中的 TXT 记录发出 DNS 查询将检索该 DMARC 记录。

DMARC 规范允许发件人发布策略记录，其中包含相应参数供接收者用于通知对自称来自发件人邮件域的邮件的处理。DMARC 启用的功能包括：

- **灵活的策略**。DMARC 模型允许邮件发件人指定对未通过基础身份验证检查的邮件应用三个策略之中的一个：

表 1-2　DMARC 策略选项

DMARC 策略设置	语法	接收者采取的操作
无（“监控”）	`p=none`	“p=none”策略意味着不应用任何策略；也就是说，如果未通过 DMARC 检查，域所有者不要求接收者采取操作。此策略通常也称为“监控”策略。当发件人只是希望从接收者收集反馈时，可使用此选项。此策略允许域所有者接收有关使用其域的邮件的报告，即使他们没有部署 SPF/DKIM 也是如此，例如，便于他们确定其域是否正在被滥用。对其邮件的处理方式没有变化；但是，域所有者现在可对使用其域名发送的邮件获得一定的可视性。*如果尚未部署 SPF 或 DKIM，请先发布 DMARC 策略，因为其具有报告功能。*
隔离	`p=quarantine`	在隔离策略中，未通过身份验证检查的邮件应被视为可疑。隔离策略会指示接收者“隔离未通过 DMARC 的邮件进行其他处理”。大多数接收邮件的系统都会将这些邮件传送到最终用户的垃圾邮件文件夹。这可能意味着以某种方式增加最终用户的反垃圾邮件审查或标记为“可疑”工作。
拒绝	`p=reject`	不接受未通过 DMARC 检查的邮件。

- **子域特定的策略** DMARC 记录可以为顶级域和子域指定不同的策略（使用“p=”和“sp=”标签）。
- **分阶段的策略部署**。DMARC 记录可以包含“百分比”标记（“pct=”），以指定多少邮件流应受 DMARC 策略影响。使用此功能，发件人可以尝试逐渐增强的策略，直至获得足够的操作经验来移至“100% 的覆盖范围”。
- **标识符一致灵活性**。DMARC 规范允许域所有者控制标识符一致的语义。对于 SPF 和 DKIM 生成的经过身份验证的域标识符，域所有者可以指定是否需要严格的域匹配，或父和/或子域是否可被视为匹配。
- **反馈控制**。DMARC 记录包含相应参数，用于指定将反馈发送给邮件域所有者的位置、频率和使用的格式。

DMARC 和思科域保护带来的价值

DMARC 通过 SPF 和 DKIM 添加的重要功能：

- 针对未通过 SPF 和 DKIM 身份验证情况提供灵活的策略选项 - 这是 SPF 和 DKIM 规范中“缺少的部分”，也是消除恶意邮件所必不可少的。
- 能够收集有关使用您的域名的所有邮件发件人的数据。DMARC 采用 XML 格式将数据发送到您选择的地址。

DMARC 生成的 XML 数据很难处理，部分是因为邮件数据通常非常多。在处理和分析数据方面，请记住以下需求：

- 需要以聚合形式分析数据以呈现趋势。
- 各个邮件必须可用于分析发件人详细信息。
- 应封装历史数据，以获得其在威胁和合法发件人方面可带来的洞察力。

思科数据分析凭借其处理世界最多邮件发件人的丰富经验，可为您带来相应的优势，从而帮助您解释并了解来自 DMARC 的数据。此外，对于必须在任何用户界面之外执行的所有相关任务，思科会帮助您创建格式正确的文件。

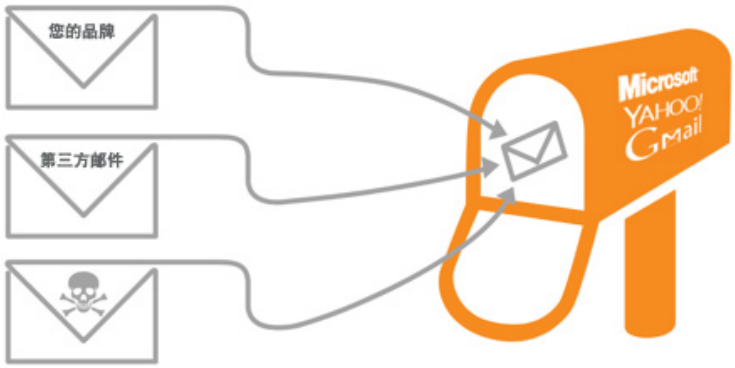
思科域保护填补了协议之间缺少的部分：

- 基于对邮件生态系统的行业了解进行报告解释
- 对实际邮件示例的可见性
- 在实施中指导执行关键步骤

优势 - 实施 DMARC 之前和之后

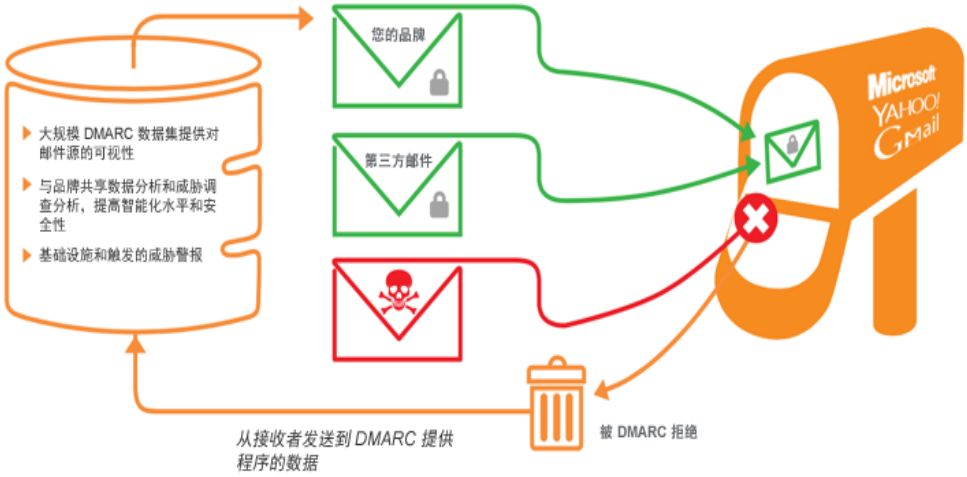
如没有 DMARC，各个品牌对于使用域发送邮件的方式的可视性有限：

图 1-8　　实施 DMARC 之前



DMARC 提供对所有邮件流量的可视性，然后指示接收者如何处理未经身份验证的邮件，一切都在邮件流外部进行：

图 1-9　　实施 DMARC 之后



一般流程 - DMARC 的实际应用

本指南的其余部分介绍了使用思科域保护实施 DMARC 的详细过程；概括过程如下：希望成为符合 DMARC 标准的域所有者根据需要为其计划要保护的域执行 3 项活动：

步骤 1　**发布 DMARC 记录。**要开始收集接收者的反馈，请以域名为“_dmarc.<您的域.com>”的 TXT 记录形式发布 DMARC 记录：

```
"v=DMARC1; p=none; rua=mailto:dmarc-feedback@<your-domain.com>;
```

执行此操作将导致符合 DMARC 标准的接收者生成聚合反馈，并将其发送到“dmarc-feedback@<您的域.com>”。“p=none”标记使接收者可以了解域所有者仅对收集反馈感兴趣。

步骤 2　**部署邮件身份验证：SPF 和 DKIM**。

- SPF 的部署涉及创建和发布 SPF 记录，该记录描述经授权代表邮件域发送邮件的所有服务器。小型组织通常具有简单的 SPF 记录，而复杂的组织通常会维护为各种数据中心、合作伙伴和第三方发件人授权的 SPF 记录。DMARC 提供的聚合反馈可帮助识别合法的服务器，同时引导 SPF 记录。
- DKIM 部署要求域所有者配置邮件服务器，以将 DKIM 签名插入邮件并在 DNS 中发布公钥。DKIM 广泛可用，且受到各大主要邮件供应商的支持。DMARC 提供的聚合反馈可帮助识别发出无 DKIM 签名的邮件的服务器。

步骤 3　**确保满足标识符一致要求**。DMARC 提供的聚合反馈可以用于识别以下情况：基础身份验证技术生成与邮件域不一致的经过身份验证的域标识符。识别不一致后，可以快速进行更正。

为什么实施 DMARC 是一项挑战

可视性较低

大多数公司都是等到开始通过 DMARC 报告获取聚合数据，才意识到自己的邮件生态系统的复杂性。标准报告采用单个 XML 文件的形式，这些文件指定域名、IP 地址和身份验证详细信息。尽管许多工具可以分析和可视化此 XML 数据，但明确流的意义并了解要执行哪些后续操作来改进域的身份验证状态非常困难且容易出错，需要深入了解邮件流。

发现第三方发件人并向其授权

DMARC 之旅中最具挑战性的步骤是了解所有第三方发件人，并确保合法发件人正确进行身份验证。平均来说，客户通过第三方（如 Salesforce.com、Marketo 或 MailChimp）发送的合法邮件百分比为 64%。

图 1-10　第三方发件人的流行率

“操作错误”的成本

尽管出现新的邮件传送平台，但邮件仍是组织进行通信和数字互动的最重要媒介。错误地配置身份验证会导致误报、传送性问题和品牌受损。如果无法传送邮件的业务影响未知或无法预测，则执行拒绝策略的最后一步会让人望而生畏。

指定“真实可信”邮件

思科域保护和 DMARC 规范允许您识别并授权合法（已批准）发件人，他们“从”您的域发送邮件，与可能滥用您的品牌的非法发件人不同。

您需要做些什么

DMARC 实施涉及对规范及其使用方式有一定的技术了解，还涉及管理和通信。在一段时间后，您很可能会对贵组织内外的邮件发件人有深刻的了解。

转为使用 DMARC 的“p=reject”策略

最初，通过在您的域的 DNS 记录中添加 TXT 记录来实施 DMARC。该文件包含相关属性和值，供您进行编辑以指定 DMARC 如何对您控制的域应用策略。

您在实施 DMARC 过程中的目标是移动，最终实现“p=reject”策略（标记为“p”）。拒绝策略会通知邮件接收者应丢弃所有不符合标准的邮件。但是，DMARC 规范包含各种策略，支持渐进式实施，而且不会影响您的邮件流。允许增量部署和强化 DMARC 策略是该规范的主要设计目标。请参阅表 1-2“DMARC 策略选项”（第 7 页）。

您应从子域或域的简单“监控模式”记录开始，该子域或域要求 DMARC 接收者向您发送有关其使用您的（子）域看到的邮件的统计信息。即使您在邮件传送基础设施中实施 SPF 或 DKIM 之前，也可执行此操作（尽管在它们到位后，您将无法逾越该步骤）。

引入 SPF（第 4 章“发件人策略框架”（第 1 页））和 DKIM（第 5 章“DomainKey 识别的邮件”（第 1 页））时，报告将提供通过和未通过这些检查的邮件数量和来源。您可以轻松查看这些检查覆盖或未覆盖的合法流量，并解决任何问题。您还将开始看到发送的欺诈邮件数量，以及它们的来源位置。

当您认为所有或大多数合法流量均受 SPF 和 DKIM 保护时，可以实施“隔离”策略 — 您现在正在请求 DMARC 接收者将使用您的域且未通过这些检查的邮件放在垃圾邮件文件夹的本地等同项中。您甚至可以请求仅对特定百分比的邮件流量应用此策略 — 您仍将获得统计信息报告，以便查看邮件发生的情况。

最终，在解决任何实施问题后，您可以以适合自己的节奏将百分比增加到 100%。最后，未通过 DMARC 检查的所有邮件都应转至垃圾邮件文件夹而不是客户的收件箱。

在开始之前

在开始使用思科域保护进行 DMARC 实施前，您将需要执行以下任务：

步骤 1　确保您有权访问思科域保护门户

您的思科代表应已提供对思科域保护门户的至少一个用户帐户的访问权限，该门户的网址为：https://dmp.cisco.com。

请联系思科支持部门 https://www.cisco.com/support/，或向 support@cisco.com 提交支持案例。对于紧急问题，请拨打 855-682-1708 致电思科支持部门

这一用户帐户是管理帐户；可通过此原始帐户创建其他用户帐户（具有不同的角色和委派管理权限或只读权限）。有关详细信息，请参阅第 8 章“用户帐户”（第 1 页）。

步骤 2　收集域列表

您将需要计划为贵组织保护的域（和子域）的列表。此列表应包括贵组织的主域，即与贵组织最相关且最常用语发送邮件的域（例如：`coltrane.net`）以及贵组织拥有和维护的*防御*域或*测试*域（例如：`blue.coltrane.net`、`coltrane-soprano.net`、`coltrane-tenor.net`、`a-love-supreme.net` 等等）。谨记任何合并和收购历史记录以及创建并使用域来区分产品和进程的特定实例。

步骤 3　能够进行 DNS 更改

您将需要能够更改您计划保护的域的域名系统 (DNS) 记录。DMARC 身份验证协议（以及 SPF 和 DKIM 协议）依赖于 DNS 服务来执行身份验证。您将需要在保护域的整个过程中更改 DNS — 从获取进入思科域保护的初始数据流，到将 DMARC 策略从监控修改为拒绝。

步骤 4　编写利益相关方列表

对贵组织的所有出站邮件进行身份验证的过程可能会涉及很多组，具体取决于贵组织的规模。例如，您可能具有与潜在客户进行通信的专门出站营销，与现有客户进行通信的支持团队，以及承担从后端系统发送订单确认邮件或回执任务的业务连续性团队。所有团队都需要注意他们代表贵组织发送的邮件的身份验证要求，以及随着您启用的 DMARC 策略变得更加严格，在未能正确进行身份验证时出现的传送性问题。在此整个过程中及早且频繁地进行通信！

参考资料

Patrick Peterson，“DMARC 白板会话”
https://www.youtube.com/watch?v=6ZyzR1xNV0E

实施思科域保护的流程

整体流程

思科域保护是帮助客户实施 DMARC 和邮件身份验证方面的领导者。

概括来说，此流程包括以下五个*阶段*：

表 2-1　　实施思科域保护的总体流程

阶段	步骤
第 1 阶段	1. 获取门户访问权限并接受思科提供的入门级培训。 2. 在监控策略中发布 DMARC 记录 3. 将域添加到门户
第 2 阶段	4. 监控流量 5. 识别目标域 6. 识别所有发件人并对其进行分类（常见发件人和自定义发件人）
第 3 阶段	7. 推荐新的 SPF 记录 8. 发布新的 SPF 记录 9. 识别内部企业所有者 10. 对邮件网关启用 DKIM 签名 11. 验证 DKIM 在邮件网关上的运行情况 12. 从第三方所有者请求 DKIM 签名 13. 对所有第三方发件人实施 DKIM 密钥 14. 对所有第三方发件人验证 DKIM 运行情况
第 4 阶段	15. 获取所有企业所有者的签名 16. 将 DMARC 记录移动到拒绝策略
第 5 阶段	17. 查看警报和报告

图 2-1　　实施 DMARC 的各个阶段

思科对于使用思科域保护对您的所有域进行身份验证的最佳做法通常包含下表中的具体*步骤*：

备注　您可以将步骤 2 和步骤 4-17 视为可对贵组织中您计划保护的每个域重复执行的过程。

某些域可以快速完成此过程 - 例如您虽然拥有，但从未计划用来发送任何合法邮件的*防御*或*内部*域。

其他域（例如，您的主域或具有极高量的域）将需要您系统地完成过程中的每个步骤，并将所做的更改相应地传达给利益相关方。

下面的章节提供了有关了解和完成每个步骤方面的帮助，尤其是思科域保护中可用的支持数据方面的帮助。

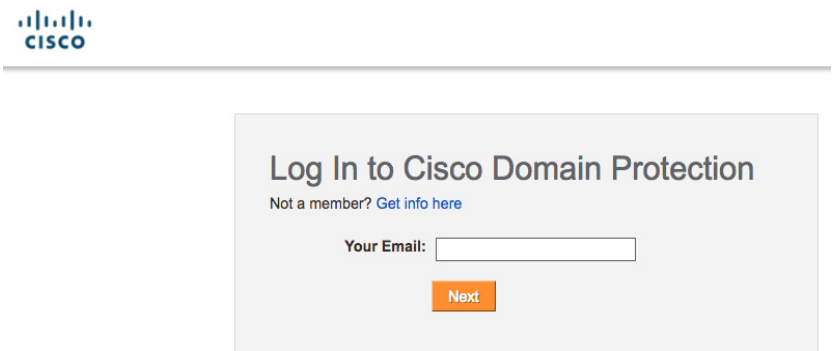
步骤 1：获取门户访问权限

在典型的发起和自行激活过程中，您应该会收到有关访问思科域保护门户的一份简要概述。

在此启动会议期间，您的思科代表会授予您思科域保护的访问权限，网址为：https://dmp.cisco.com。

思科向您发送一封包含访问信息的邮件；此帐户是贵组织的第一个管理帐户，将用于为贵组织创建其他用户帐户。

图 2-2　　思科域保护登录页面



高级主题

在此阶段需考虑的一些方面如下：

- 思科域保护包含基于角色的权限和访问控制 (RBAC)，可为门户中的用户帐户授予不同级别的权限。您可能需要考虑创建一个只读用户、仅审计用户或仅可以在门户中管理报告的用户（举例而言）。要详细了解权限，请参阅第 4 章“发件人策略框架”（第 1 页）。
- 登录到门户后，系统会将您重定向到贵组织的唯一 URL，例如：https://organization_name.dmp.cisco.com。
- 思科提供了一个 API，可用于以编程方式访问产品的某些部分。要访问 API 文档，您需要创建一个用户帐户并为该用户授予 API 访问权限。
- 此外，思科还支持单点登录 (SSO)，可从服务提供商发起（SP 启动），也可直接从身份提供商发起（IdP 启动）。要详细了解如何为贵组织设置 SSO，请联系思科代表。
- 管理员帐户（以及具有用户创建权限的任何后续帐户）可以为您创建的用户重置密码。

步骤 2：在监控策略中发布 DMARC 记录

在监控策略中发布 DMARC 记录是您在保护域的过程中所要执行的前几个步骤之一；它也是开始使数据流入思科域保护门户的方法，同时可以间接地向思科证明您是域的所有者。DMARC 策略以文本 (TXT) 资源记录 (RR) 形式发布在 DNS 中，并声明邮件接收者应如何处理从给定域收到的不一致邮件。

对于计划保护的每个域，您需要发布为策略设置“none”标记的 DMARC 记录；这要求接收者向思科发送数据报告。然后，您可以使用思科域保护分析数据，并根据需要修改您的邮件流。

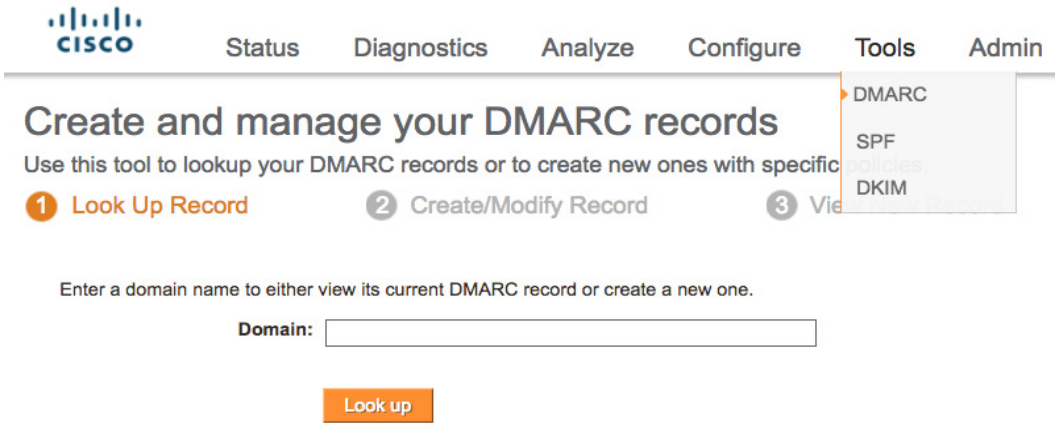
备注　为其策略设置了“none”标记的 DMARC 记录不会影响邮件流或从该域发送的邮件的传送性。“none”标记只是对来自您的域的邮件进行身份验证过程的第一步：您可以从中收集数据进行分析。一段时间后，在您为域实施 SPF 和 DKIM 并为发件人授权时（在本指南的后续步骤中执行），可以将 DMARC 策略标记修改为更严格的策略（如“隔离”和最终的“拒绝”）。

2a：使用 DMARC 生成器创建记录

利用思科的 DMARC 生成器，您可以查找任何域的 DMARC 策略记录。然后，您可以使用 DMARC 生成器修改或创建域的有效 DMARC 记录文本。最后，DMARC 生成器会提供域的 DNS 提供商以及如何发布 DMARC 记录的信息。

步骤 1　在登录思科域保护门户后，请导航至“工具”>“DMARC”页面。

图 2-3　生成器 DMARC 步骤 1



步骤 2　输入一个域名，然后点击“查找”以查看该域的当前 DMARC 记录或创建一个新记录。

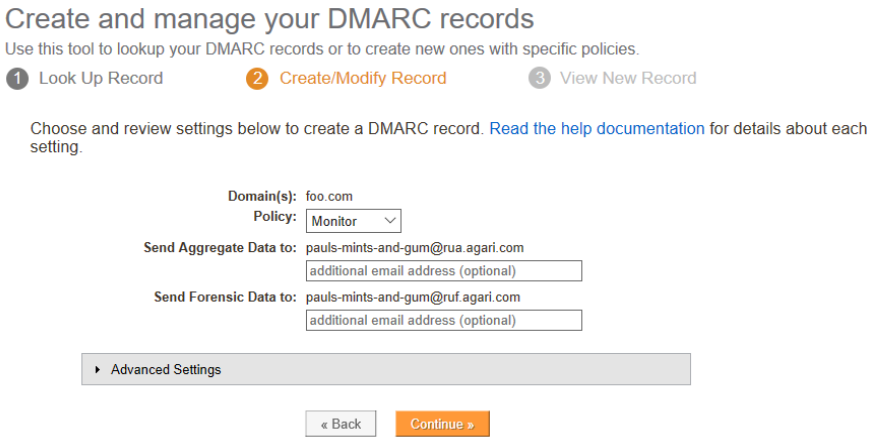
如果域没有 DMARC 策略，系统会为您提供相应选项来创建新的 DMARC 记录或在思科托管新的 DMARC 记录：

点击“新建 DMARC 记录”以创建新记录。

（本指南假定您编辑的是自己的 DNS 基础设施。如果希望在思科托管 DMARC 记录，请联系思科支持部门。）

例如：

图 2-4　DMARC 生成器步骤 2



在此示例中，域为“foo.com”，策略为“监控”，思科向该域发送报告数据所用的邮件地址为“pauls-mints-and-gum@rua.cisco.com”和“pauls-mints-and-gum@ruf.cisco.com”。

下文说明了您可以在 DMARC 生成器中编辑的不同 DMARC 策略记录字段。

域：您要为其创建或修改 DMARC 记录的域名。此字段可以是单个域，也可以是逗号分隔的域名列表。

策略：域所有者请求邮件接收者对使用其报头“发件人”地址中的域且未通过 DMARC 检查的邮件所执行的操作。

无：此策略将告诉接收者不对未通过 DMARC 检查的邮件执行任何特殊操作，只是将 DMARC 数据发送到在域的 DMARC 记录中指定的报告地址。**注意：建议在此步骤中选择选择此策略。**

隔离：此策略请求接收者将未通过 DMARC 检查的邮件放在收件人的垃圾邮件文件夹或将邮件视为可疑的其他隔离区域中。

拒绝：此策略请求接收者拒绝未通过 DMARC 检查的任何邮件，并在 DMARC 数据中报告相应操作。被拒绝的邮件绝不会提供给接收者。

将聚合数据发送到：将 DMARC 聚合数据发送到的邮件地址。默认情况下，思科的 DMARC 生成器会设置思科的报告地址。除思科的地址外，您还可以指定另一个报告地址，这两个地址都会显示在 DMARC 记录中。DMARC 接收者应向这两个地址发送报告数据。

将调查分析数据发送到：将 DMARC 调查分析数据发送到的邮件地址。默认情况下，思科的 DMARC 生成器会设置思科的报告地址。除思科的地址外，您还可以指定另一个报告地址，这两个地址都会显示在 DMARC 记录中。DMARC 接收者应向这两个地址发送报告数据。

警告　调查分析数据是未通过 DMARC 检查的实时邮件流。数据量可以非常大，而且非常分散。在此处添加您自己的报告地址可能会引发本地邮件服务器问题。

高级设置

“高级设置”下的记录元素是可选的，默认采用建议的设置。

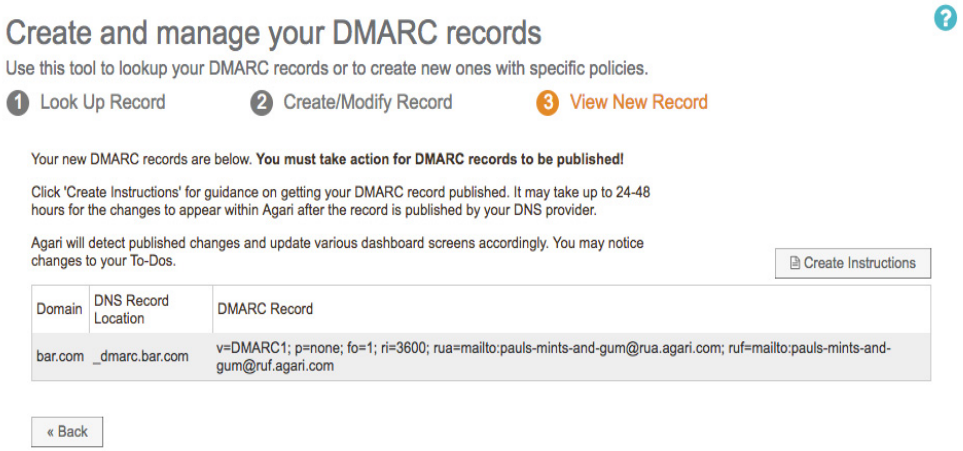
备注　思科建议您一开始不要更改这些设置。

有关子域策略的说明：默认情况下，一个域的 DMARC 策略适用于其所有子域。如果需要，您可以通过 DMARC 规范为子域应用其他策略。不管您指定了哪个子域策略，它都适用于所有子域。如果您希望为特定子域应用其他策略，可以为该子域专门发布一个 DMARC 记录。

步骤 3　点击“继续”。

DMARC 记录将显示如下：

图 2-5　　DMARC 生成器步骤 3



域“bar.com”的此 DMARC 记录定义以下参数：

- **DNS 记录位置** - 必须为 `_dmarc.bar.com` 安装 DNS 文本记录
- **v=DMARC** - 这是 DMARC 规范的第 1 版
- **p=none** - 此记录的策略 (p=) 为无，或为仅监控策略
- **ri=3600** - 报告时间间隔 (ri=) 应为 3600 秒，即每小时一次
- **rua=*organization_name*@rua.cisco.com** - 应将**聚合**信息 (rua=) 发送到的报告用户邮件地址。此地址对于贵组织是唯一的，也是思科接收数据所采用的机制。
- **ruf=*organization_name*@ruf.cisco.com** - 应将**调查分析**信息 (ruf=) 发送到的报告用户邮件地址。此地址对于贵组织是唯一的，也是思科接收数据所采用的机制。

步骤 4　点击“创建说明”下载要在下一步中使用的文本文件 (.txt)。

备注　对于您计划在思科域保护中保护的每个域重复此部分中的步骤。

2b：在 DNS 中发布记录

为域获得了格式正确的 DMARC 记录后，您需要更新域的 DNS 记录。

发布 DMARC 记录的具体步骤因域的 DNS 的管理方式而异。但是，如提交 DNS 更改请求，则需要请求将此 DMARC 记录发布为 TXT 资源记录。该记录必须在通过在前面附加“`_dmarc`”创建的子域发布，如上一步骤中列出的“DNS 记录位置”部分所示。请确保包含完整的 DMARC 记录，包括引号内的所有内容（但不含引号本身）。不应有换行、换行符或空格，下面记录中明确指明的空格除外。

注意：

- 如果您有直接访问权限，可通过在线 DNS 管理工具管理域的 DNS，请查找要发布 TXT 记录的部分或特定于 DMARC 记录的部分。
- 如果您有权通过 Web 托管在线管理界面管理域的 DNS，请查找 DNS 设置以及可输入 TXT 记录或 DMARC 记录的位置。
- 如果贵公司在内部管理其 DNS，您可能需要提交请求来通过贵公司的 DNS 管理团队发布 DNS 记录。
- 如果某个第三方为您的域托管 DNS，则您可能需要向他们提交申请单来更新域的 DNS 设置。

您已成功完成所有步骤！

向您的 DNS 提供商发布 DMARC 记录后，可能最多需要 24-48 小时才能使更改显示在思科域保护中。

步骤 3：将域添加到门户

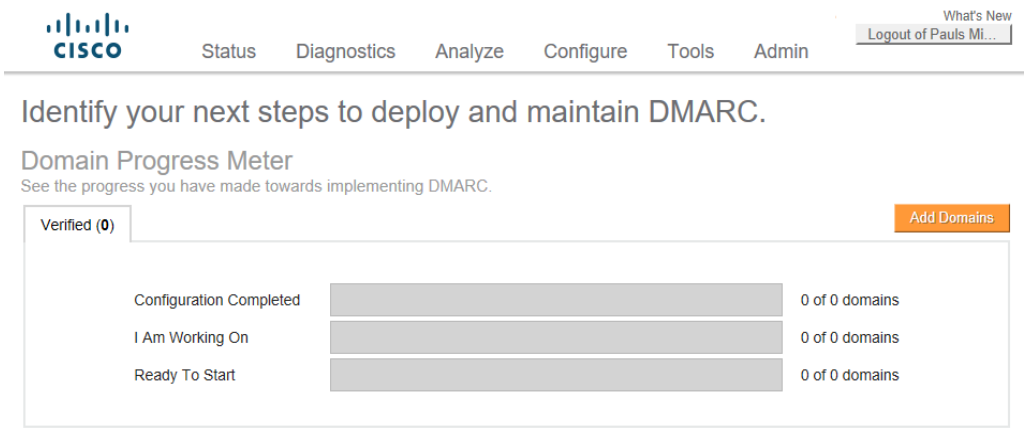
备注 如果您为计划要通过思科域保护保护的所有域发布了具有 `p=None` 策略的 DMARC 记录，则可跳过此步骤！思科会自动添加并验证这些域。如果您有没有为其发布 `p=None` 策略的其他域，请继续阅读：

您必须将域添加到门户；在思科域保护中，大多数活动都以*域*为中心。贵组织可能具有非常大的域列表，或者您可能具有更多可管理的域。

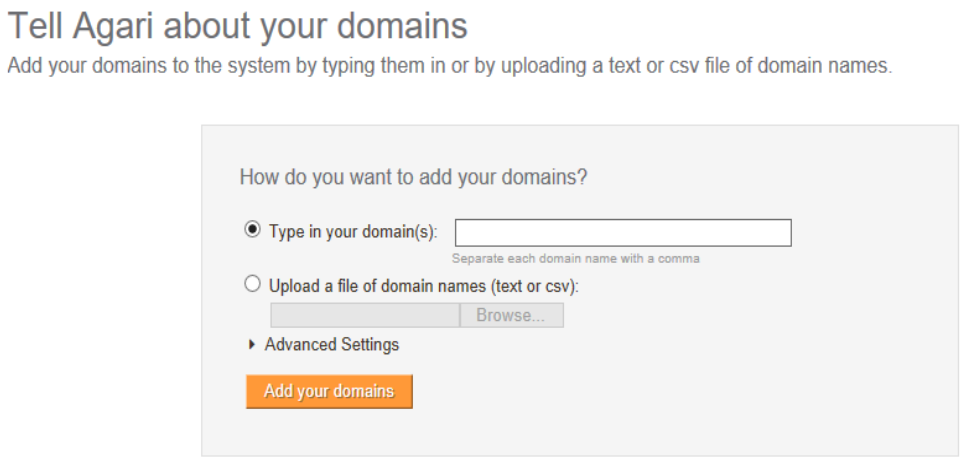
在任一情况下，您在此步骤中的活动都是让思科域保护知道哪些域与贵组织相关。

获得门户的访问权限后，在您进行身份验证后看到的第一个页面是“状态”>“保护”页面：

图 2-6　“状态”>“保护”页面上的“添加域”按钮



步骤 1　点击**添加域**按钮。



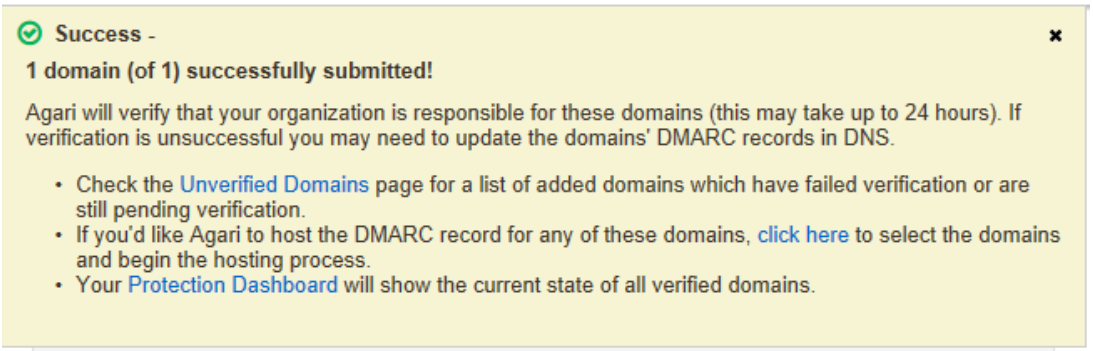
步骤 2　在对话框页面中，选择用于输入域的选项：

- 基本：文本字段：在提供的文本字段中输入一个域或多个域（用逗号隔开）。
- CSV 上传：浏览到包含域列表的本地文本或逗号分隔值文件。

高级主题：域组

此对话框的“高级”部分允许您为每个新上传的域指定域组和思科荣誉。请参阅以下部分了解对于域组的讨论。

步骤 3　点击“添加您的域”。将显示如下对话框：



什么是未验证的域？

您可以指定策略并仅查看已验证域的数据。

思科代表会采取相应措施来确保上传到系统域的所有域都已准备好进行管理，这一过程即为“验证”域。思科会定期检查所有未验证的域，以了解是否发生更改，从而允许其进行验证。您可以重新提交域进行验证，从而使其更快得到重新检查。

验证域的最快捷方法是为域发布 DMARC 记录，如上一部分中所述。思科强烈建议使用此方法。

为域发布 DMARC 记录需要您修改域的 DNS 条目，这是显示您对域具有授权的另一种方法。（通过验证输入到系统中的每个域，思科可以确保没有错误或无意中输入的域。）

有关 DNS 和验证的其他选项

为您的域更新 DNS 名称服务器记录（NS 记录），以便思科可以将其与贵组织相关联。如果您的域的 DNS 通过外部 DNS 提供商管理，则此方法可能不可行。

示例：您正在尝试在思科系统中注册 `cat.com`。如果思科已为贵组织批准 `dog.com`，而 `cat.com` 的 NS 记录是 `ns1.dog.com`，则思科会信任您拥有对 `cat.com` 的授权（因为 `cat.com` 的 DNS 由我们知道属于您的域控制）。

为您的域更新 DNS 邮件交换记录（MX 记录），以便思科可以将其与贵组织相关联。这并不总是可行；具体取决于如何为您的域托管邮件。

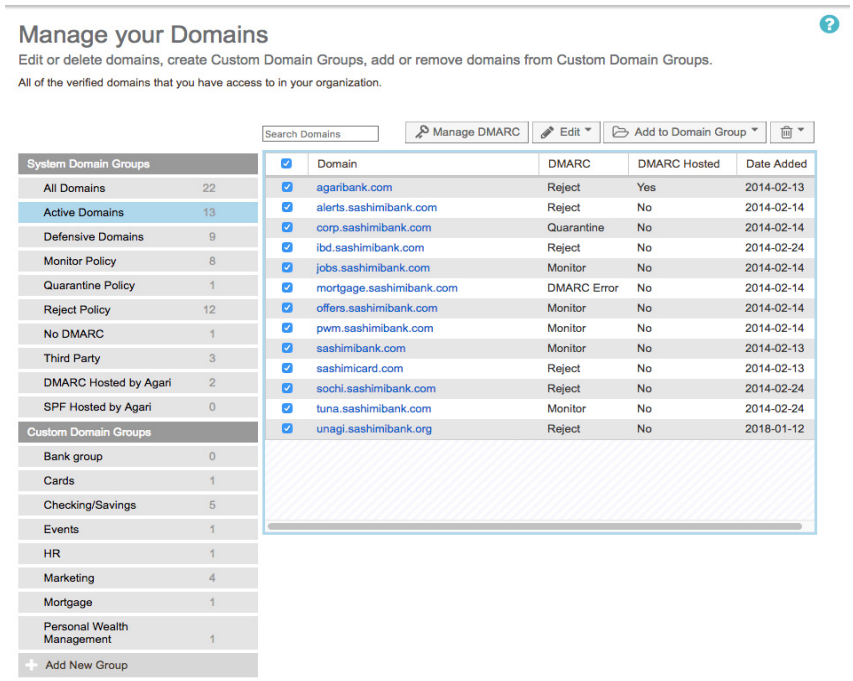
示例：您正在尝试在思科系统中注册 `cat.com`。如果思科已为贵组织批准 `dog.com`，而 `cat.com` 的 MX 记录是 `mail1.dog.com`，则思科会信任您拥有对 `cat.com` 的授权（因为发送到 `cat.com` 的所有邮件都定向到我们知道属于您的域）。

步骤 3a：将您的域组成组

思科域保护允许以任意方式对域分组，而且您可以在整个产品中使用这些域组。例如，您可以将由一个组织单位拥有且应在一起考虑的域分组在一起。按名称对域分组使用户可以更加轻松地查找要使用的已分组域，不必在一个很大的域列表中进行查找。域组是一种功能强大的分类工具，在您熟练掌握思科域保护后非常有用。

通过“管理”>“域”页面管理域和域组：

图 2-7　域组页面示例



在此页面上，您可以查看所有活动域和防御域，为域的分类创建自定义域组，以及管理用户的访问权限。

系统域组

系统域组是预定义的通用域类别，用于提供快速访问，以帮助您更好地管理您的域。系统还会动态填充系统域组。默认情况下，存在八 (8) 个系统级别，并且可以添加其他自定义组。例如，“拒绝策略”组将包含贵组织中具有 DMARC 拒绝策略的所有域。当思科发现一个域的 DMARC 拒绝策略时，该域将自动变成“拒绝策略”组的一部分。您无需执行任何操作以在此组中添加或删除域

备注　域可以属于多个唯一组。

“活动”与“防御”域：域将被视为“活动”，除非选择了“标记为防御”。防御域是没有与之关联的任何邮件流的域。

第三方：由非公司实体（例如合作伙伴或代理）管理的域

自定义域组

自定义域组使您可以创建域组以更好地组织工作流组。例如，在以上示例中，您可能有一个团队在使用“卡”域，而其他团队则使用“活期/储蓄：”域。对域分组使用户可以更加轻松地查找已分组域，不必在一个很大的域列表中进行查找。您还可以通过创建用户帐户来限制用户查看其他域。

创建新的自定义域组：

1. 从您的自定义域组列表中，点击“添加新的域组”。
2. 输入您的新域组的名称。键入“Return”以保存名称。
3. 创建完成后，从现有组中选择要添加的域。
4. 使用“添加到域组”按钮，将所选的域添加到新的自定义域组。

删除自定义域组

1. 将鼠标悬停在不再要使用的自定义域组上。
2. 点击垃圾桶图标可删除该组。
3. 确认您要从思科中删除该组。

请注意：一旦删除自定义域组，它将无法恢复。

监控

本章的步骤包含以下部分：

- 监控流量
- 识别目标域
- 识别所有发件人并对其进行分类（常见发件人和自定义发件人）

成功为域创建并发布 DMARC 记录后，思科域保护门户中将开始显示数据。

现在，您可以开始监控邮件流量，识别要保护的域，以及识别所有发件人并对其进行分类。

步骤 4：监控一段时间内的流量

开始向思科域保护发送 DMARC 报告数据（聚合和调查分析）时，接口开始监控流量。

在大多数情况下，思科建议**收集至少两周的数据**，这样才能获取有意义的数据集。

通过 DMARC 报告数据，可以查看哪些发件人正在代表您的域发送邮件，发送资产的源地址（IP 地址），以及这些邮件是否通过 SPF 和 DKIM 身份验证检查。

但第一步是监控流量一段时间。监控时间的长短取决于您组织的规模和复杂性。例如，您的组织可能会每天发送回执或订单确认邮件，但也可能会雇佣第三方发件人不太频繁地发送营销活动邮件，而有的部门可能只是偶尔通过另外的第三方发件人发送新闻稿。请注意，有些合法的第三方邮件新闻稿、活动或其他类型的事件可能一个月、一个季度甚至一年才会发送一次，因此可能无法在最初两周的时间段内捕获到。大多数公司都是等到开始通过 DMARC 报告获取聚合数据，才意识到自己的邮件生态系统的复杂性。

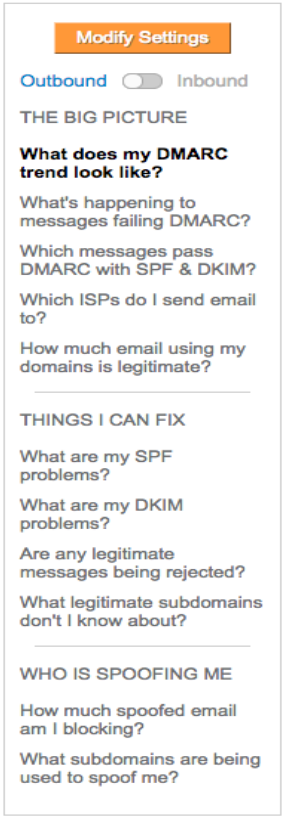
重点是：您需要监控数据一段时间，以确信收集了代表您的所有第三方发件人，从而为域的所有潜在发件人设置身份验证。

开始使用监控

导航至“分析”>“邮件流量”菜单，熟悉思科域保护中的可用报告。

“分析邮件流量”页面显示了常见问题列表，可为您提供查看邮件生态系统的有用视图。每个视图都是有关一份有关您的邮件生态系统的详细报告：

图 3-1　　邮件流量分析器报告



您可以调整每个报告的筛选器选项来帮助您获得所需的信息。这样，您可以快速找到并解决问题，以及正确配置邮件身份验证。

- 点击“修改设置”按钮可查看任何报告的可用筛选器选项。例如，您可以：
  - 面向单个域或域组筛选每个报告。
  - 增大或减小数据范围 2 周（默认值）。思科建议增加日期范围（例如 90 天），以查看发送过程中的趋势模式。（例如，每季度发送的新闻稿。）
  - 更改邮件分组的粒度（每日、每周或每月）
  - 修改某些报告的邮件来源；例如，在某些视图中，包括或排除某些类别的邮件可能会有所帮助。

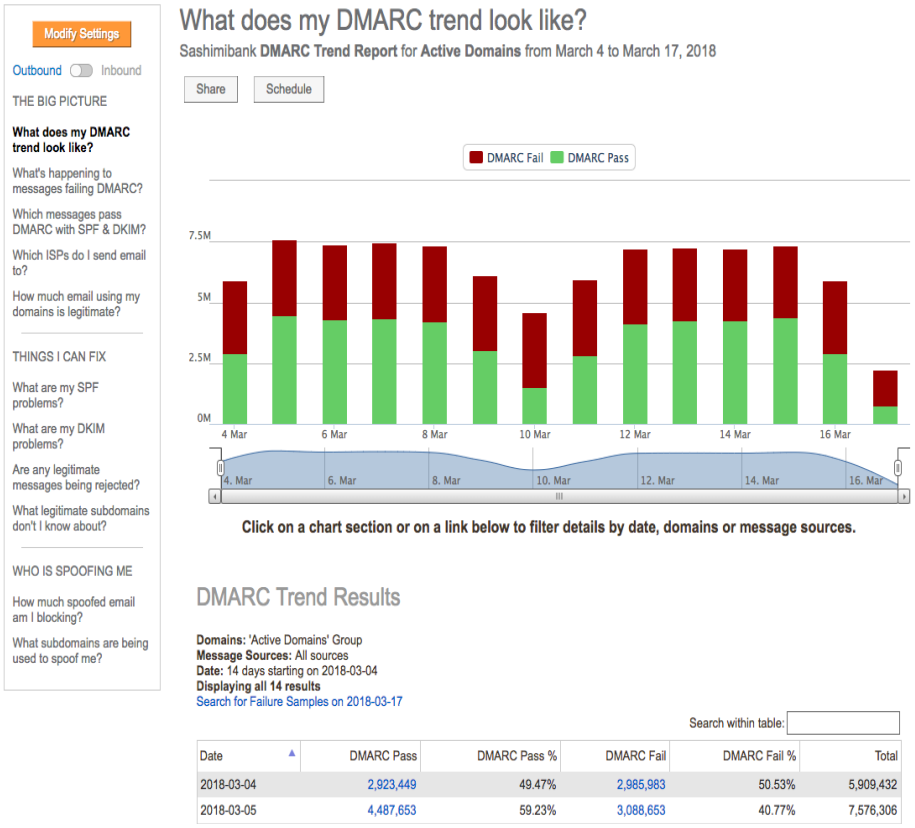
我的 DMARC 趋势

一个很好的用来开始监控数据的位置是默认视图：“我的 DMARC 趋势”报告。

在此处，您可能只有域会在思科域保护中生成数据，并且这些域可能没有进行任何身份验证。

- 点击“DMARC 通过”或“DMARC 未通过”列中的任意链接可深入了解特定数据。
- 在此视图中点击特定域的链接会生成报告，即在所选时间段代表该特定域发送邮件的所有 IP 地址。
- 您甚至可以通过点击此表中列出的任意 IP 地址的“DMARC 通过”链接，进一步进行深入分析。

图 3-2　“活动域”组的“我的 DMARC 趋势”视图



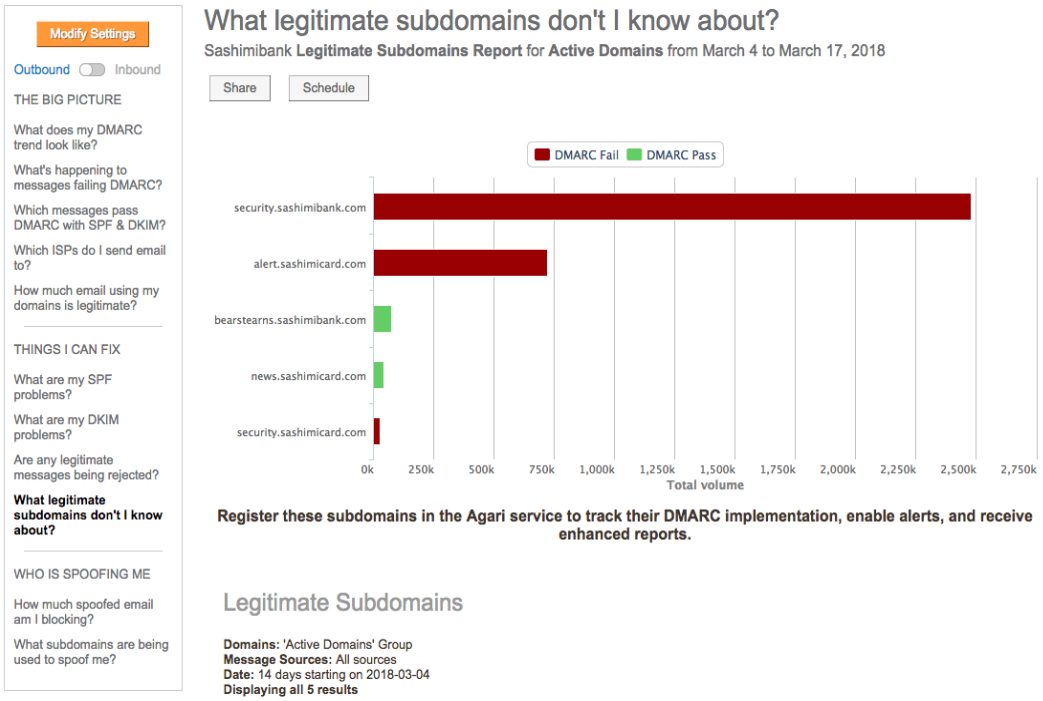
我不了解的合法子域

初始监控阶段的另一个有用视图是“我不了解的合法子域”视图。

- 在“我可以修复的问题”部分中，点击“我不了解的合法子域”对应的链接。

此视图的结果可能会清晰地列出可能会被用来发送邮件的主要域的子域。

图 3-3　“我不了解的合法子域”视图



备注　此报告中的合法子域仅针对*已批准*的域进行报告。

共享或订用报告

您可以将“我不了解的合法子域”报告发送给其他人，或定期接收报告的邮件版本。

点击视图顶部的“共享”或“订用”按钮可共享或订用报告。（请记住，所有计划的报告均保持为“修改设置”按钮中定义的范围。）思科建议您在开始监控时订用此报告的每周版本。

请花些时间在“分析”>“邮件流量”部分中浏览所有视图和深入分析功能。

后续步骤

请不要被大量的报告功能和丰富的数据粒度吓倒！在此过程中，此刻您只是收集信息，以为项目的后续阶段*制定策略*：

- 确定要开始监控的一组目标域
- 确定这组目标域的发件人邮件传送身份验证要求（SPF、DKIM）
- 与您的邮件传送团队一起为这组目标域设置您自己的邮件基础设施身份验证
- 与第三方发件人和业务部门一起为这组目标域设置身份验证
- 为这组目标域修改 DNS SPF 和/或 DKIM 记录
- 观察并确认设置

步骤 5：确定一个目标域或一组目标域

监控思科域保护中的数据一段时间后，应考虑确定要开始保护的一组目标域。

例如，可以采用如下一些策略：

- 先保护您的主域，或是数量最多的域

  或许您的主域（不是特定子域）用于从您的公司发出的所有邮件通信；例如，地址为 joe@foo.com 的邮件就如同用于回执或订单确认、新闻稿、营销活动或从您的 CRM 系统进行邮件传送一样，很可能也会用于日常的公司通信。

  如果是这种情况，最好先阻止您的主域。

- 先保护防御域，然后再保护活动域

  防御域按定义来说不应当发送任何邮件，因此更易于通过严格的策略锁定。（未锁定且未受保护的防御域可能会遭到垃圾邮件发送者的滥用。）您可以使用思科域保护中的数据为防御域创建目录，并快速移至 DMARC 拒绝策略。

  为防御域制定策略后，您可以专注于处理那些旨在为您的组织发送合法邮件的域。

- 先保护具有一致或统一发送配置文件的关键业务或后端系统自动化域

  例如，如果贵组织从单个第三方发件人（例如 Zendesk） 通过单个子域（例如 `support.foo.com`）发送客户支持邮件，可能更加易于首先针对此域实施身份验证。

- 或者，先保护非关键业务域

  相反，如果您不希望中断业务关键邮件的传送性，请考虑保护先发送营销邮件的域，因为识别“切换”以从计划的邮件程序发送经过身份验证的邮件可能会更加容易。

无论选择哪种策略，都应使用“配置”>“管理域”视图来对域进行分组，如步骤 3a [HREF TBD] 中所述。

步骤 6：识别发件人并对其进行分类

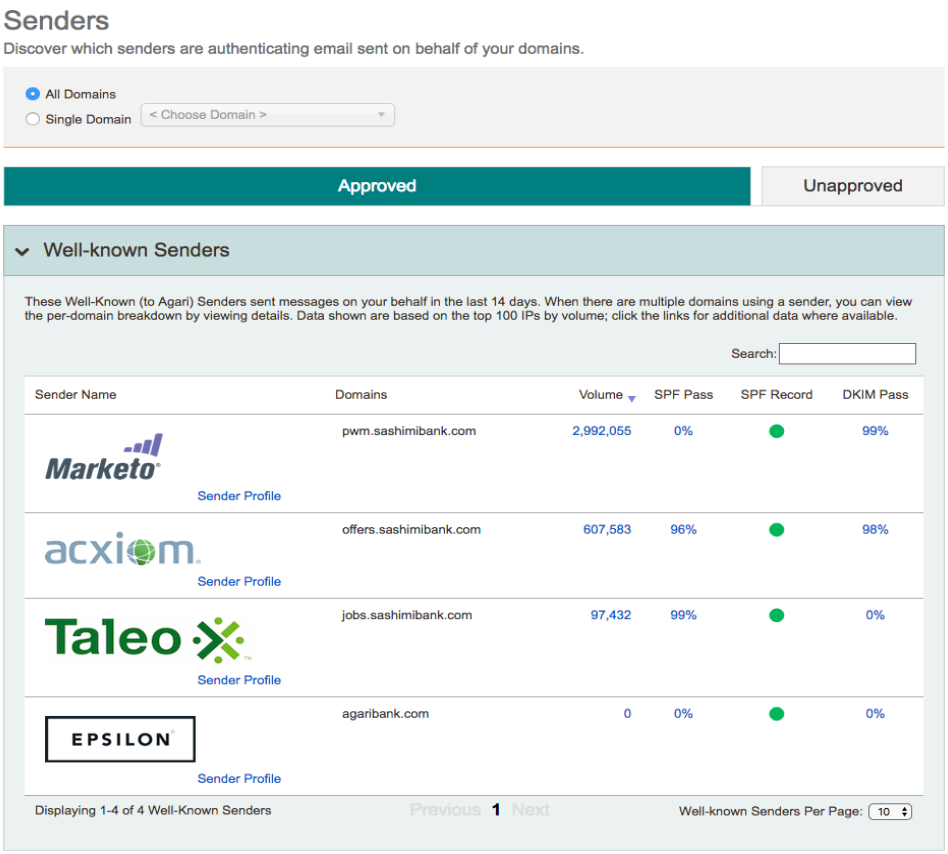
定义了为一组给定域实施邮件身份验证的策略之后，即可开始面向这些域（以及您的整个组织）识别发件人并对其进行分类。

“发件人”页面

步骤 1　导航至“诊断”>“发件人”页面。

默认情况下，思科域保护通过常见第三方发件人的发送基础设施来识别这些发件人。

图 3-4　“诊断”>“发件人”页面（常见发件人）



例如，在此视图中，组织已识别*并批准* Marketo、Acxiom、Taleo 和 Epsilon 为合法的第三方发件人。

如果您导航至此页面，并且没有看到批准的发件人或是未批准的发件人，请不要担心，这可能只是您尚未在 DNS 中发布正确身份验证信息的原因。

“发件人”页面工作原理

思科域保护会查看组织所有已注册域的 DNS 记录，以确定可能代表您的组织发送合法邮件的 IP 地址。您可以在此页面上查看思科认为对您的组织合法的常见发件人。此外，还可以查看用于发现这些 IP 地址的域以及发现这些地址所用的特定 DNS 记录源。

如果“已批准”选项卡中没有显示数据，请点击“未批准”选项卡以查看：

- 未批准的常见发件人
- 未批准的 IP 地址

选择特定域

从下拉列表中选择单个域，可查看已批准和未批准的常见发件人和 IP 地址。

“发件人”页面的作用

开始向思科域保护传输数据时，该产品会基于每个域来聚合整个组织的信息。您可以借助“发件人”页面来组织和跟踪系统中每个域的常见发件人和自定义发件人。

- 点击“批准”，将合法第三方常见发件人从“未批准”选项卡移至“已批准”选项卡。（相反，如果您知道您的组织**未**使用某个常见发件人，则可以点击“忽略”将该常见发件人移至已忽略发件人列表。）
- 将合法 IP 地址划分到自定义发件人中。思科无法对用于发送邮件的 IP 地址分类，这些 IP 地址可能属于您组织的发送基础设施。（例如，许多大型组织都拥有和管理着专用的邮件交换服务器，用于发送出站邮件。）如果您可以识别未批准的 IP 地址部分中给定域的 IP 地址，则可以通过将这些 IP 地址添加到自定义发件人对它们进行分类，也可以选择将它们添加到“已忽略”列表，不作处理。

备注　思科域保护中*授权*发件人的这种行为（将它们从“未批准”移至“已批准”）是您在下一章中为域管理 SPF 和 DKIM 策略的基础（会反映在这些策略中）！您将对来自您的域的已批准发件人的所有邮件*进行身份验证*，而且您的 DMARC 策略将指示接收者对未通过身份验证的邮件执行的操作。

发件人策略框架

本章的步骤包含以下部分：

- 推荐新的 SPF 记录
- 发布新的 SPF 记录
- 识别内部企业所有者

您在第 3 章“监控”（第 1 页）中了解的监控工具将在本章中为您提供有关所需操作的信息；也就是说，您将使用监控结果来识别某个域的第三方发件人并执行相关操作，以便对这些发件人启用身份验证方法（SPF 和/或 DKIM 身份验证）。

使用思科域保护，您可以深入了解邮件流以便启用 SPF。

发件人策略框架 (SPF)

发件人策略框架也称为 SPF，通过 RFC 7208 发布：（请参见 https://tools.ietf.org/html/rfc7208。）

该框架定义将“5321.from”地址（也称为发件人、邮寄地址或退回路径）关联到授权发送邮件的 IP 地址的身份验证过程。此授权发布在 DNS 的 TXT 记录中。

接收者可以检查 SMTP 事务开头的 SPF，并将 5321.from 域与连接 IP 地址进行比较，以确定是否授权连接 IP 为该域传输邮件。

通过发布某个域的 SPF 记录，您可以*断言*邮件仅应源自已发布记录中的 IP 地址。

SPF 记录语法

简单来说，SPF TXT 记录包含版本指示符、对域允许的 IP 地址以及授权类型。

例如，在以下简单的 SPF 记录中：

```
"v=spf1 ip4:198.51.1.137 -all"
```

- **v=spf1** 是版本指示符。
- **198.51.1.137** 是允许发送邮件的 IP 地址（IPv4 地址），
- **-all** 是授权类型，其断言仅授权 IP 地址 198.51.1.137 从该域发送邮件。

指定 IP 地址

有几种方法可用来定义 SPF 记录中的授权 IP 地址。

- 您可以通过在前面附加限定符来指定单个 IPv4 或 IPv6 地址，如 **ip4:191.51.1.137** 或 **ip6:7939:a348:460d:966f:a986:d0ba:1e9a:c67e**
- 您可以以 CIDR 格式指定 IP 地址范围，例如 **ip4:191.51.1.137/29**
- 您可以指定还作为发送域的 A 或 MX 记录的任何 IP。例如“**v=spf1 mx -all**”会授权还作为发送域的 MX 的任何 IP。
- 可以使用 **include:** 命令包含其他 SPF 记录；例如，**include:_spf.google.com** 会包含 Google 的 SPF 记录。

备注 有些机制和修饰符会导致在评估时进行 DNS 查询，有些则不会这样。“include”、“a”、“mx”、“ptr”和“exists”机制以及“redirect”修饰符需要 DNS 查询。单个 SPF 记录必须将 SPF 评估期间的查找总数限制为 **10 次查找**，以避免 DNS 出现不合理的负载。

授权类型

SPF 记录的结束语法允许您发布不同类型的授权方法。

表 4-1　SPF 记录授权类型

陈述	结果	含义
`+all`	传送	允许所有邮件。
`-all`	失败	仅允许匹配记录中的一个参数的邮件（例如，IPv4、IPv6、MX）。
`~all`	软失败	无论邮件是否与记录中的参数匹配，都允许邮件。
`?all`	不确定	没有策略陈述。

`~all` 与 `-all` 之间的区别在 DMARC 标准和 SPF 标准独立存在之前，软失败（'~'）授权可用于确保组织对声明在接受者以不同方式解说并按授权执行操作的环境中的出站 IP 空间的想法表示满意。

在实际使用 DMARC 和思科域保护时，在您监控数据时可以从不确定授权（`"?all"`）开始，然后快速转至软失败授权（`"~all"`），最终转至失败授权（"-all"）。

在您修改域的 SPF 记录时，可以使用“我有哪些 SPF 问题？”报告来持续监控数据。

SPF 一致

除了简单地在 SPF 记录中*断言*允许代表您的域发送邮件的 IP 地址列表之外，您将需要利用发件人来确保 SPF 正确地*一致*。

了解一致需要在很小的程度上了解 SMTP 协议。对于 SPF，当 RFC5321.MailFrom（也称为发件人、邮寄地址或退回路径）与邮件正文（或 DATA 部分）中显示的“发件人：”地址（也称为“友好发件人：”地址）相匹配时，域会被视为一致。

大多数情况下，“Return-Path”信头用于显示 RFC5321.MailFrom 域，而且通常在大多数邮件客户端中不可见。

下面显示了 SMTP 对话示例：

```
220 smtp.example.com ESMTP Postfix
HELO relay.example.com
250 smtp.example.com, I am glad to meet you
MAIL FROM:<bob@example.com>
250 Ok
RCPT TO:<alice@example.com>
250 Ok
RCPT TO:<theboss@example.com>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "Bob Example" <bob@example.com>
To: Alice Example <alice@example.com>
Cc: theboss@example.com
Date: Tue, 15 January 2008 16:02:43 -0500
Subject: Test message

Hello Alice.
This is a test message with 5 header fields and 4 lines in the message body.
Your friend,
Bob
.
250 Ok: queued as 12345
QUIT
221 Bye
{The server closes the connection}
```

在以上示例中，第 4 行是 RFC5321.MailFrom 地址，第 12 行是友好发件人地址（通常在邮件客户端中可见）。在此示例中，域部分被视为对于 SPF 目的*一致*。

第 7 步：构建和推荐新的 SPF 记录

推荐新 SPF 记录的过程对于您计划保护的所有域而言应是相同的。

步骤 1　使用思科域保护中的“发件人”页面识别给定域的发件人

步骤 2　查找该发件人的 SPF 说明并发布 SPF 记录：

- 为思科域保护中的常见发件人使用“发件人配置文件”链接，以了解供应商是否支持 SPF。
- 使用自定义发件人的数据枚举您控制的 IP 地址。

步骤 3　使用发件人（常见或自定义发件人）来确保实现 SPF 一致。

- 通过“发件人”页面和“分析”>“邮件流量”页面监控进度。

步骤 4　更新/修改域的 SPF 记录以考虑到所有潜在发件人。

备注　另请参阅对 SPF 记录使用 EasySPF™ 分析器，第 4-12 页。

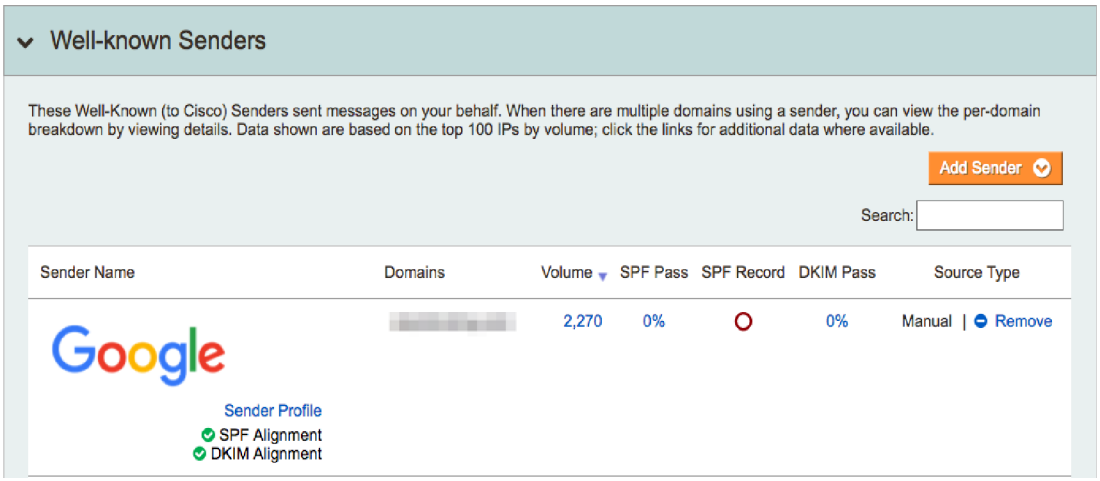
步骤 5　当您确信已在域的 SPF 记录中考虑到域的所有发件人时，将 SPF 记录更新为使用“`-all`”策略。

您将为计划保护的每个域重复上述每个步骤。

示例：常见发件人的 SPF

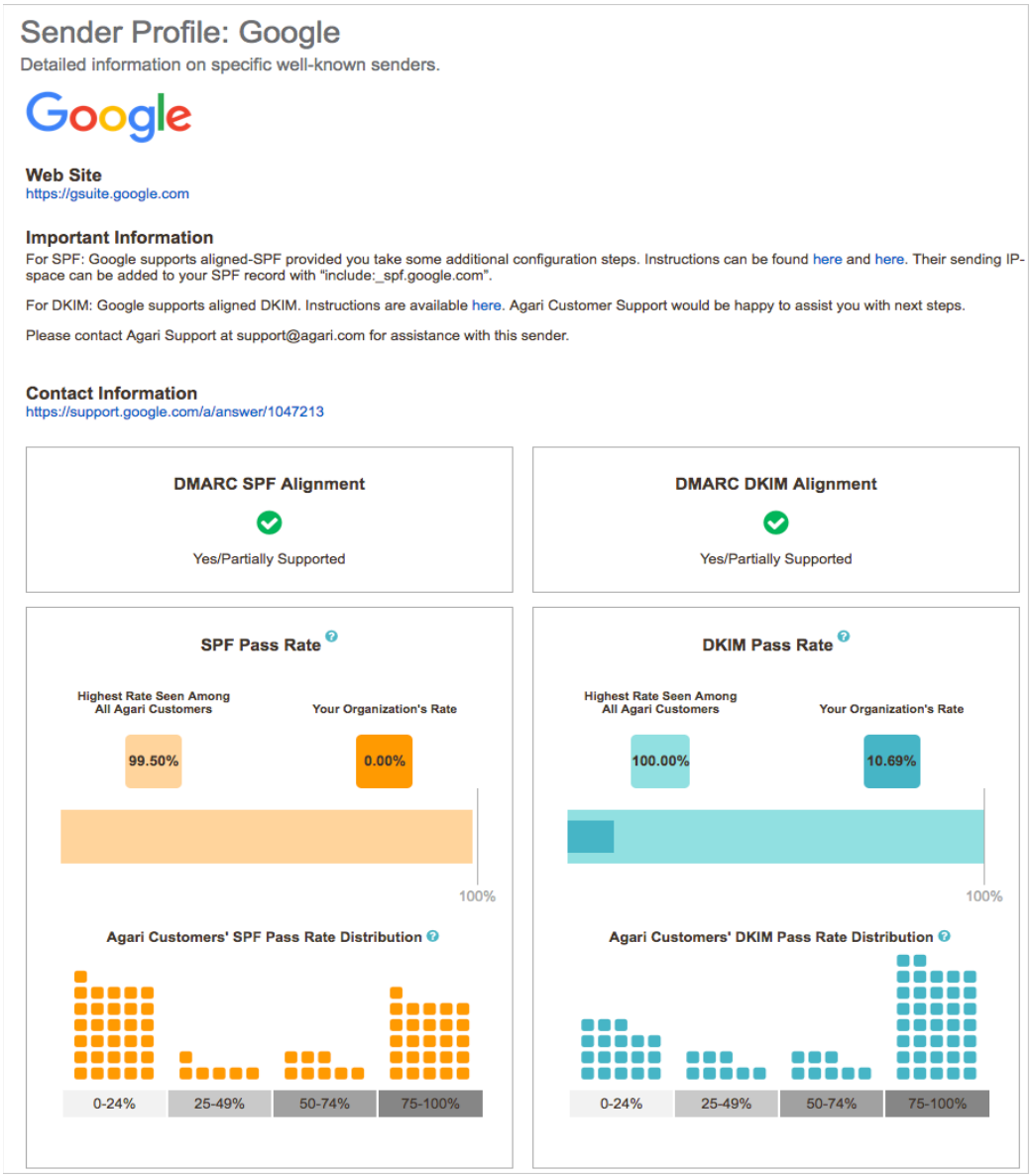
步骤 1　导航至“诊断”>“发件人”页面，然后从“单个域：”菜单中选择一个域以查看该域的发件人。

如果您使用 Google 作为邮件提供商（例如，您具有 G Suite 环境），将会发现 Google 列出在“发件人”中：



请注意，“SPF 记录”列指示对于选定域未找到任何 SPF 记录。

步骤 2　点击 Google 的发件人配置文件链接可查看思科的关于发件人的信息：



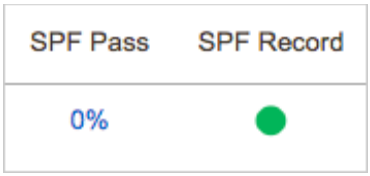
“发件人配置文件”页面包含有关发件人是否支持一致 SPF 的信息和实现一致的说明。（您还可以查看 SPF 通过率，以及其他思科客户是否已对此发件人成功实现 SPF 身份验证。）

访问“发件人配置文件”页面中的链接，您将学习如何向选定域的 SPF 记录添加以下内容：

```
include:_spf.google.com
```

....将为该域授权 Google 的 IP 地址。

新 SPF 记录可能最多需要 48 小时才能生效，但通常会更快生效。然后，您会看到“SPF 记录”指示符更改，以显示您已在所选域的 SPF 记录中包含发件人：



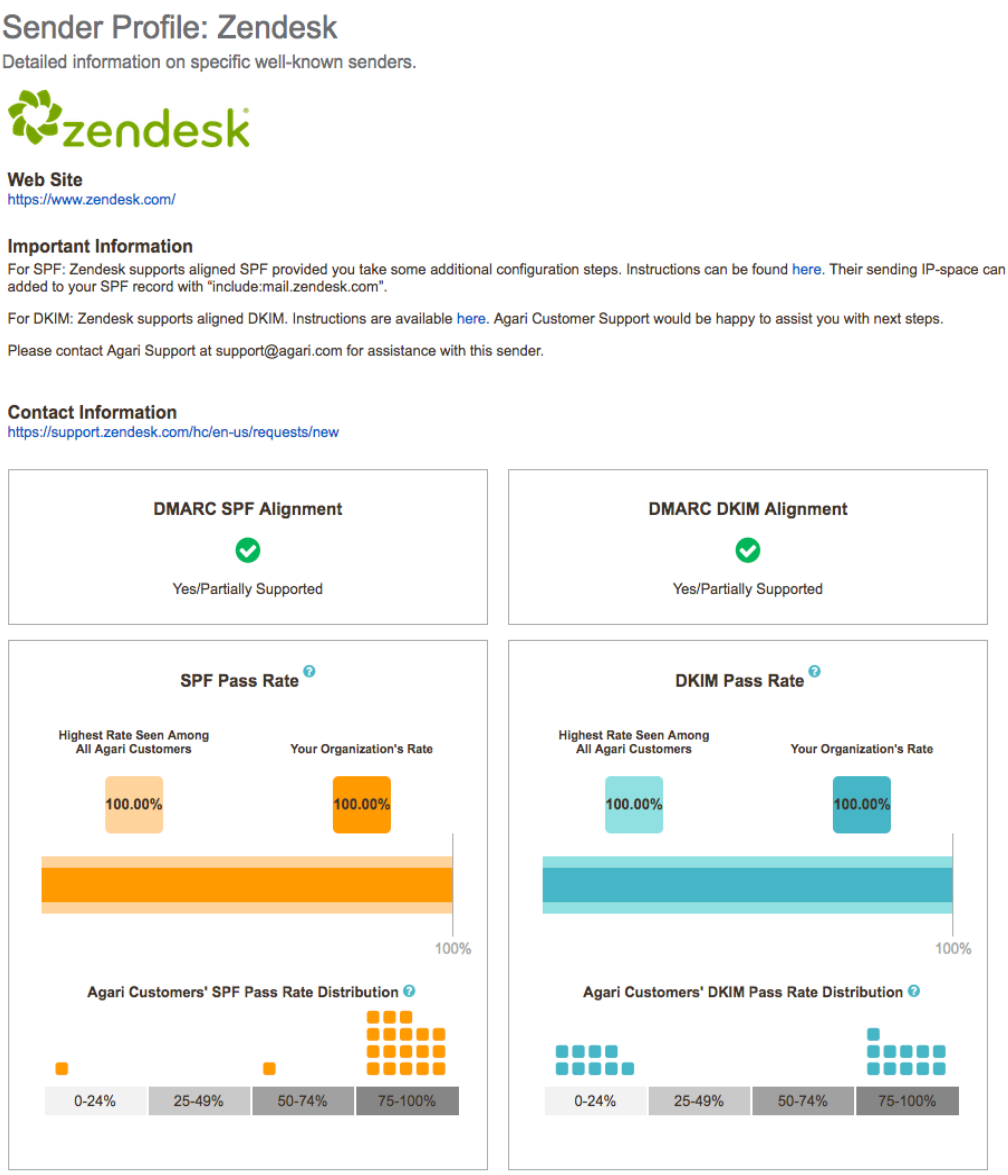
“SPF 通过”列将显示来自该发件人且通过该域的 SPF 一致检查的邮件。

（对于 G Suite，可使用 G Suite Postmaster 工具来添加和验证域，以实现 SPF 一致。有关更多详细信息，请访问 https://support.google.com/mail/answer/6227174。）

步骤 3　重复该过程，您可能会在“发件人”页面上看到贵组织将 Zendesk 用于所选的域：

步骤 4　点击 Zendesk 的发件人配置文件链接可查看思科的关于发件人的信息：

访问“发件人配置文件”页面中的链接，您将学习如何向选定域的 SPF 记录添加以下内容：




```
include:mail.zendesk.com
```

....将为该域授权 Zendesk 的 IP 地址。

此时，您建议的 SPF 记录将对两个发件人（Google 和 Zendesk）的授权：

```
v=spf1 include:spf.google.com include:mail.zendesk.com ~all
```

备注　将已批准的发件人添加到域的单个 SPF 记录，以对其进行授权。请*勿*为每个发件人创建单独的 SPF 记录。相反，增加 SPF 记录（但请注意上述 10 次 DNS 机制查找的限制。）

示例：自定义发件人的 SPF

在“发件人”页面的下半部分会显示自定义发件人。

什么是自定义发件人？

可以使用自定义发件人来组织不属于思科常见发件人的发件人或服务器。或许贵组织具有为旧系统发生出站邮件的内部旧邮件网关。默认情况下，思科域保护将其无法与常见发件人关联的 IP 地址分组在“未分配”自定义发件人组中。

您可以使用自定义发件人作为各种视图和报告中的筛选器。例如，您可以将您基础实施中拥有的服务器分类为自定义发件人。

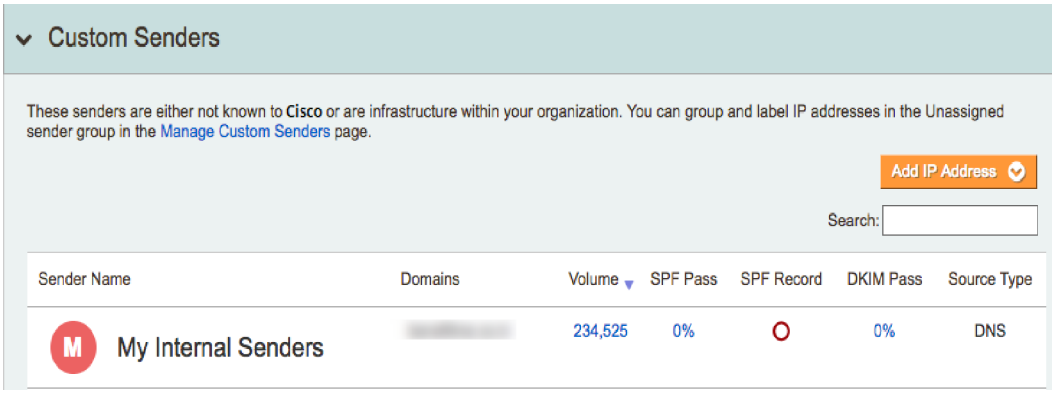
创建新的自定义发件人：

步骤 1　导航至“配置”>“管理自定义发件人”页面。

步骤 2　在“自定义发件人”下的左侧，点击“添加新发件人”：

步骤 3　输入新自定义发件人的名称并进行保存。
创建完成后，从“未分配”组中选择要添加的 IP 地址/范围。

例如，假设您已将您基础设施中的内部 IP 地址分组在名为“我的内部发件人：”的自定义发件人中



对于上面的常见发件人，页面的“自定义发件人”部分会确认看到来自此自定义发件人的邮件流量，而且 SPF 记录指示符会注明该域的 SPF 记录中尚未显示发件人。

导航至“配置”>“管理自定义发件人”页面，您可以看到为该自定义发件人定义的 IP 地址的列表。

要将 IP 地址添加到 SPF 记录，请将 SPF 记录修改为包括这些 IPv4 或 IPv6 地址。例如：

```
ip4:192.168.1.67
```

（此处以 RFC 1918 地址为例。）

所选域的 SPF 记录现在将修改为包含 Google、Zendesk 以及“我的内部发件人”自定义发件人组中的特定 IP 地址：

```
v=spf1 include:spf.google.com include:mail.zendesk.com ip4:192.168.1.67 ~all
```

备注　可以指定 CIDR 格式的 IP 地址范围。

您也可以使用其他机制在 SPF 记录中指定地址（例如“a”、“mx”、“exists”），但这些机制较为高级，本文不做讨论。（例如，建议不要在 SPF RFC 规范中使用“ptr”机制。）有关这些机制的详细信息，请访问 http://www.openspf.org/RFC_4408#mechanisms。

不要忘了一致

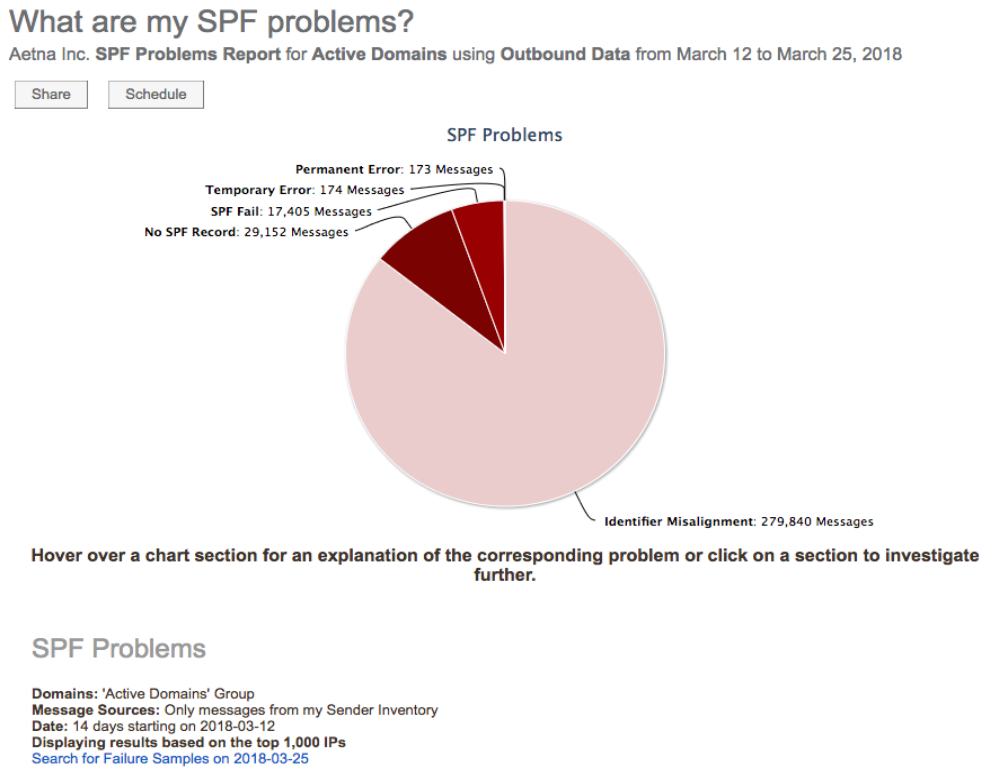
同样，添加来自自定义发件人的 IP 地址不能保证实现一致。您必须使用从该基础设施发送邮件的系统，以确保 RFC5321.MailFrom（也称为发件人、邮寄地址或退回路径）与邮件正文（或 DATA 部分）中显示的“发件人：”地址（也称为“友好发件人：”地址）相匹配。

使用“SPF 问题”报告

使用此报告，您通常可以识别在进行身份验证和为给定域中的每个发件人创建全面 SPF 记录时要解决的问题所在的域和所属类别。

步骤 1　导航至“分析”>“邮件流量”>“我的 SPF 问题是什么”以查看初始报告。

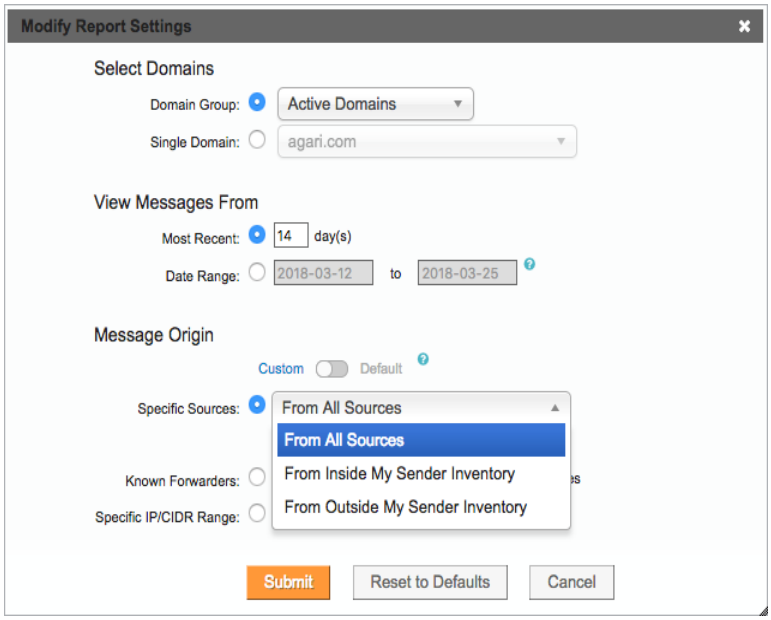
图 4-1　　SPF 问题报告的最高级别



通常，标识符不一致是最大的问题。

请注意，可以使用左上角的“修改设置”按钮缩小范围或筛选此报告（例如，仅显示单个域在最近 2 周的 SPF 问题）。

图 4-2　“修改设置”窗口



例如，您可能想要增加范围以查找“来自所有来源”的邮件。发件人清单外部的发件人将显示在“诊断”>“发件人”页面的“未批准”选项卡上。

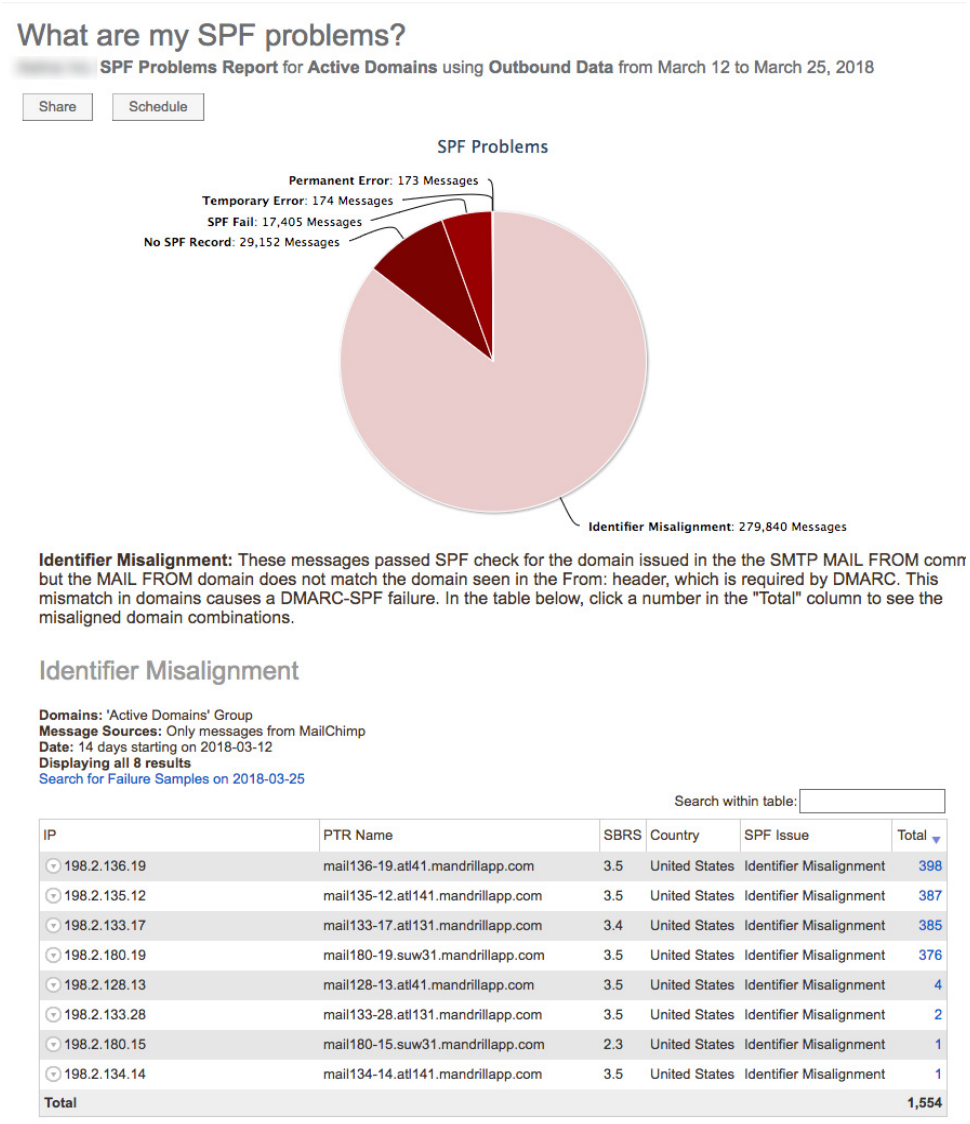
检查此报告下半部分中的发件人列表可了解问题。例如，您可能会注意到选定域从发件人 MailChimp 发送的邮件存在“标识符不一致”问题：

图 4-3　MailChimp 标识符不一致问题

MailChimp	All Issues	1,546
	Identifier Misalignment	1,546

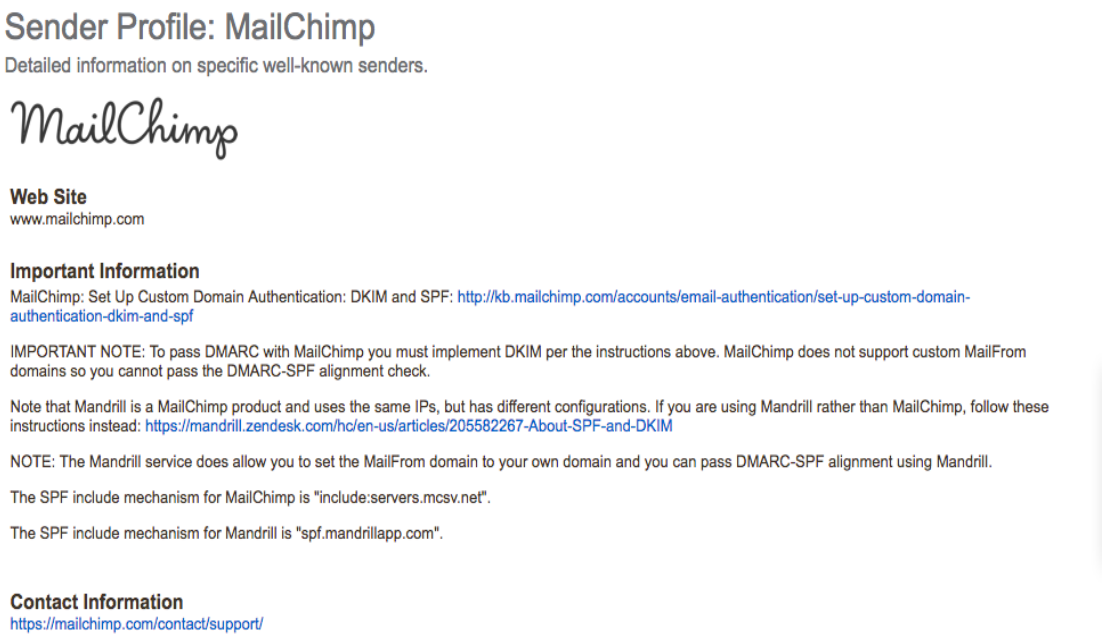
步骤 2　点击从发件人 MailChimp 发送的邮件链接可深入了解该发件人的详细信息：

图 4-4　　MailChimp 不一致问题：详细信息视图



该视图显示从 MailChimp 发送的邮件不一致（假定您已将发件人 MailChimp 的 IP 地址添加到域的 SPF 记录）。

MailChimp 的“发件人配置文件”页面具有关于为 MailChimp 和 Mandrill（MailChimp 产品，使用相同的 IP 地址，但具有不同的 SPF 配置）启用 SPF 身份验证的具体说明：


Sender Profile: MailChimp

Detailed information on specific well-known senders.

MailChimp

Web Site

www.mailchimp.com

Important Information

MailChimp: Set Up Custom Domain Authentication: DKIM and SPF: http://kb.mailchimp.com/accounts/email-authentication/set-up-custom-domain-authentication-dkim-and-spf

IMPORTANT NOTE: To pass DMARC with MailChimp you must implement DKIM per the instructions above. MailChimp does not support custom MailFrom domains so you cannot pass the DMARC-SPF alignment check.

Note that Mandrill is a MailChimp product and uses the same IPs, but has different configurations. If you are using Mandrill rather than MailChimp, follow these instructions instead: https://mandrill.zendesk.com/hc/en-us/articles/205582267-About-SPF-and-DKIM

NOTE: The Mandrill service does allow you to set the MailFrom domain to your own domain and you can pass DMARC-SPF alignment using Mandrill.

The SPF include mechanism for MailChimp is "include:servers.mcsv.net".

The SPF include mechanism for Mandrill is "spf.mandrillapp.com".

Contact Information

https://mailchimp.com/contact/support/

通过这种方式，您可以缩小问题类别的范围：

- 按域
- 按常见发件人
- 按自定义发件人

对于每个域，您可以使用“发件人”页面以及“我的 SPF 问题是什么？”报告视图来获得您每个域的发件人及其在 SPF 记录中的对应条目的全面列表。

共享或订用报告

您可以将“我的 SPF 问题是什么？”报告发送给其他人，或定期接收报告的邮件版本。

点击视图顶部的“共享”或“订用”按钮可共享或订用报告。

请记住，所有计划的报告均保持在“修改设置”按钮中定义的范围。例如，您可能想要将缩小范围版本的报告（单个域的单个发件人）定期发送给企业所有者，但是在为域构建全面的 SPF 记录时收到了范围更广版本的报告（所有域的所有发件人）。

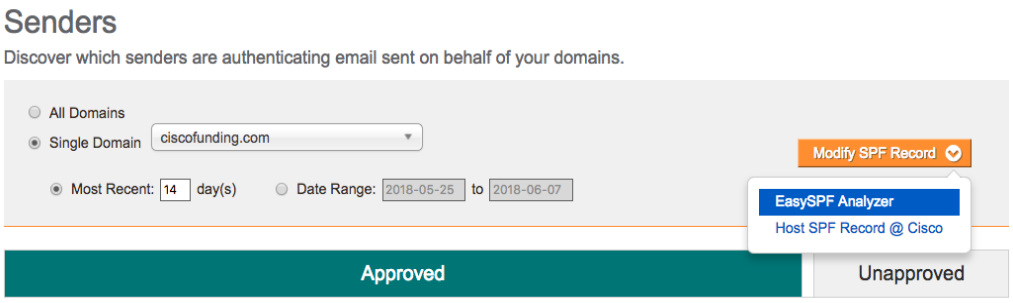
对 SPF 记录使用 EasySPF™ 分析器

您还可以使用最近推出的 EasySPF 分析器来分析现有 SPF 记录或基于已批准发件人创建新的 SPF 记录。

步骤 1　导航到“诊断”>“发件人”页面，并选择一个域以查看该域的已批准发件人。

步骤 2　选择“修改 SPF 记录”>“EasySPF 分析器”以进入“EasySPF 分析器”视图。

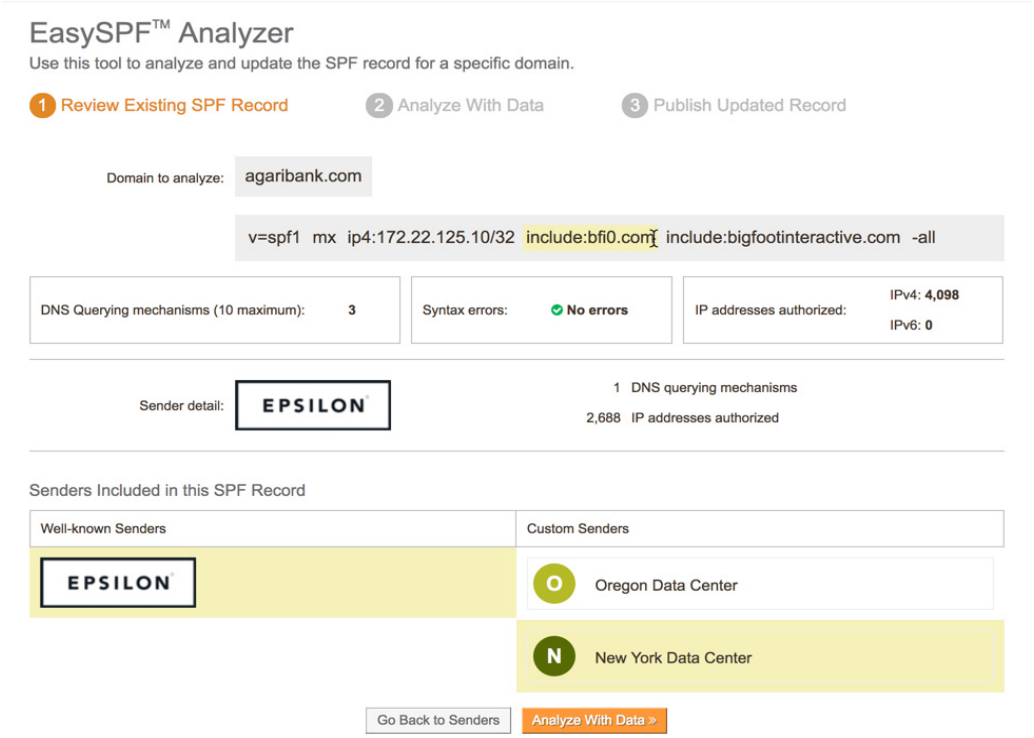
图 4-5　“修改 SPF 记录”按钮



在 EasySPF 分析器的第一步，查看现有 SPF 记录。请记下：在 SPF 记录中识别的发件人，授权的 IP 地址数，DNS 查询机制数以及现有记录中的任何语法错误。

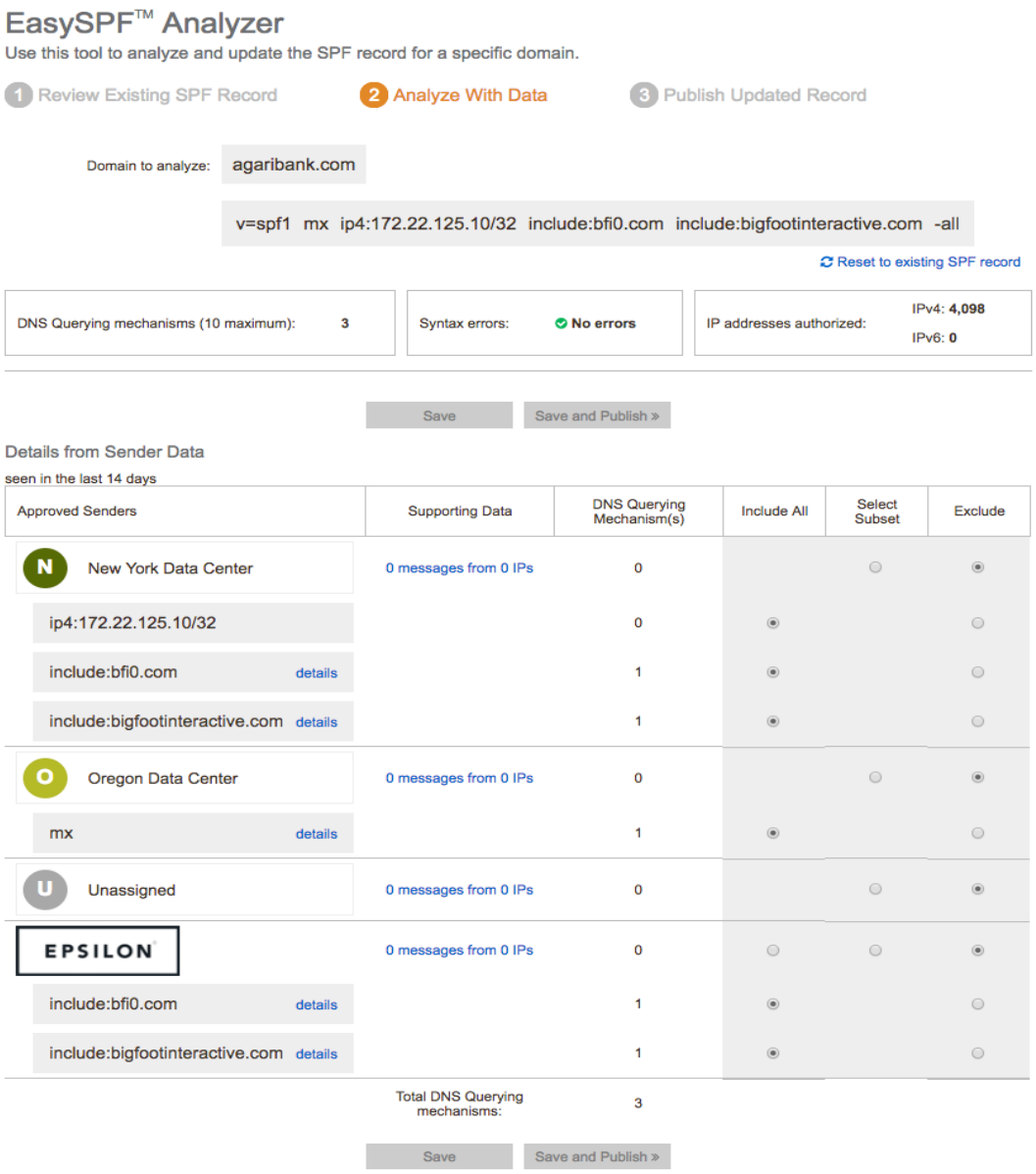
您可以将光标悬停在 SPF 记录组件上以显示详细信息，并了解机制组件之间的连接以及与所选域的已批准发件人的关系。

图 4-6　EasySPF 分析器：步骤 1



步骤 3　选择“通过数据分析”以修改当前 SPF 记录

图 4-7　EasySPF 分析器：步骤 2



EasySPF 分析器选项的步骤 2

在此视图中，您可执行以下操作：

- 点击支持数据链接可查看该发件人为域发送的邮件。

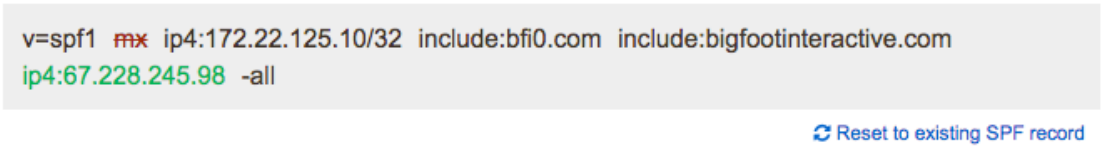
  或许您从第三方发件人那里购买了专用 IP 地址。您可能希望将 SPF 记录中的发件人定义（在此例中）缩小到更小的一组 IP 地址。您可以在支持数据视图中查看用于从该发件人发送邮件的 IP 地址数（甚至进一步进行深入分析）

  对于某个域的每个常见和自定义发件人，支持数据链接将显示：

  - IP 地址：邮件的源 IP 地址
  - 发件人的任何包含机制引用的 IP 地址

  - PTR 名称（指针记录）：IP 地址的主机名
  - 基于发件人的信誉得分 (SBRS)
  - 国家/地区：IP 地址的地理位置
  - SPF 通过率 (%)
  - DMARC 通过率 (%)
  - DMARC 通过量
  - 邮件总量
- 点击“包含”、“包含子集”、或“排除”可修改域的 SPF 记录中表示的每个发件人的定义。在进行更改时，页面顶部显示的已修改 SPF 记录中会更新添加和删除的内容：

图 4-8　　对 SPF 记录的更改

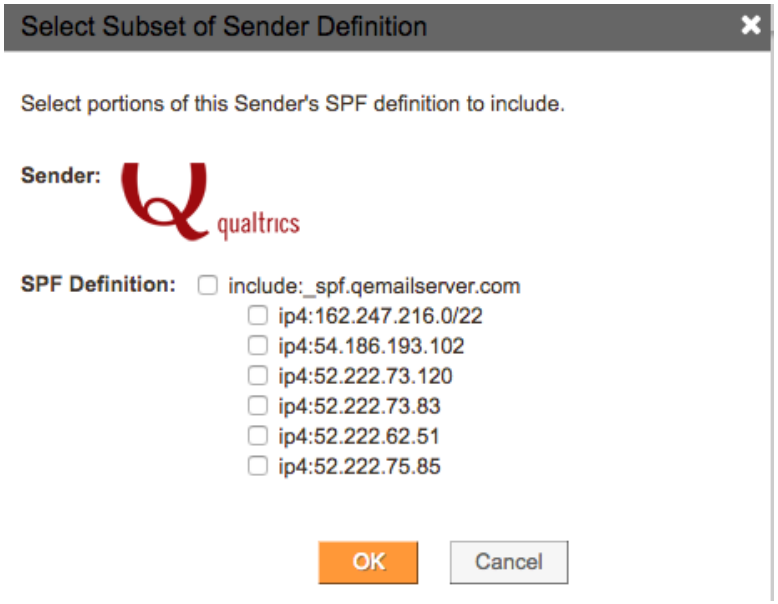


在您将包含机制更改为显式 IP 地址或范围时，DNS 查询机制也会更新。

您可以随时重置现有 SPF 记录（如当前在 DNS 中所找到）以删除您所做的任何更改。

编辑常见发件人定义的特定子集会将包含语句“展平”为一系列 IP 地址。

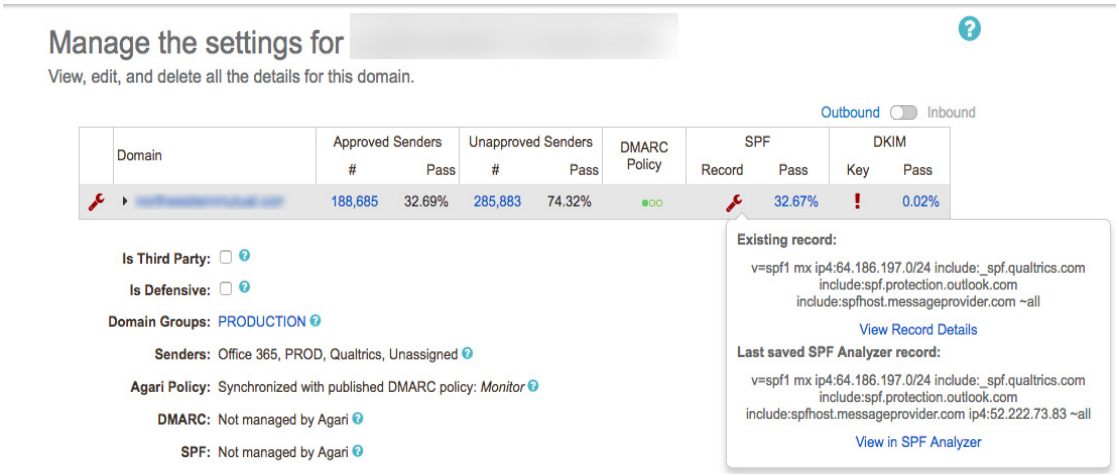
图 4-9　　选择常见发件人定义的子集



- 选择“保存”以停留在步骤 2，并继续修改 SPF 记录，或选择“保存并发布”前进到步骤 3“发布更新的记录”。

备注　如果您正在保存修改的记录，可以通过点击“分析”>“域”>“域详细信息”页面中的链接返回到已修改的视图：

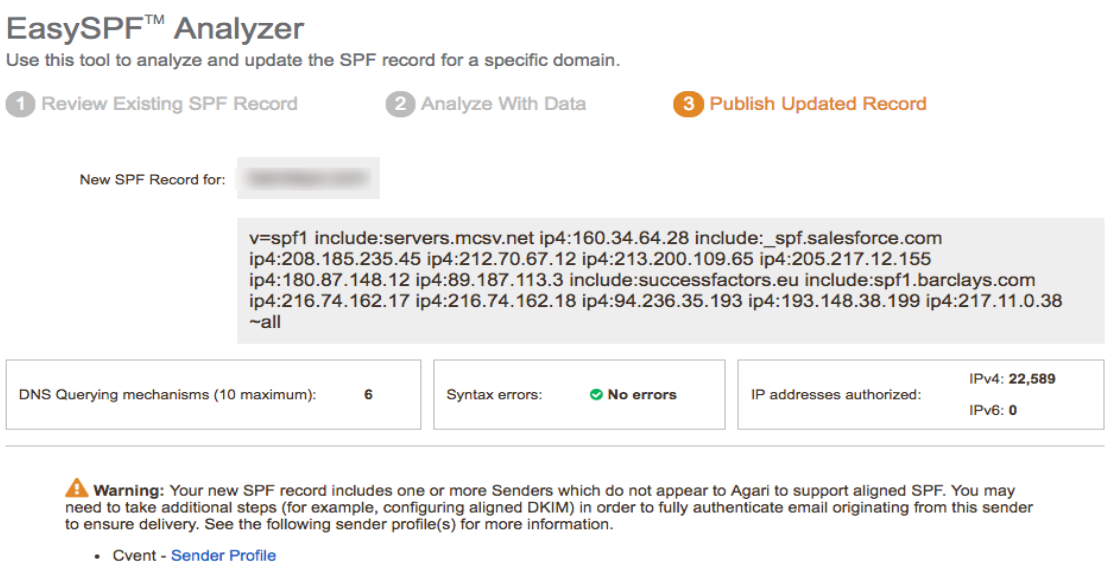
图 4-10　域的已保存 EasySPF 分析器记录



如果您点击“发布”按钮，EasySPF 分析器的步骤 3 将向您显示已修改的 SPF 记录。

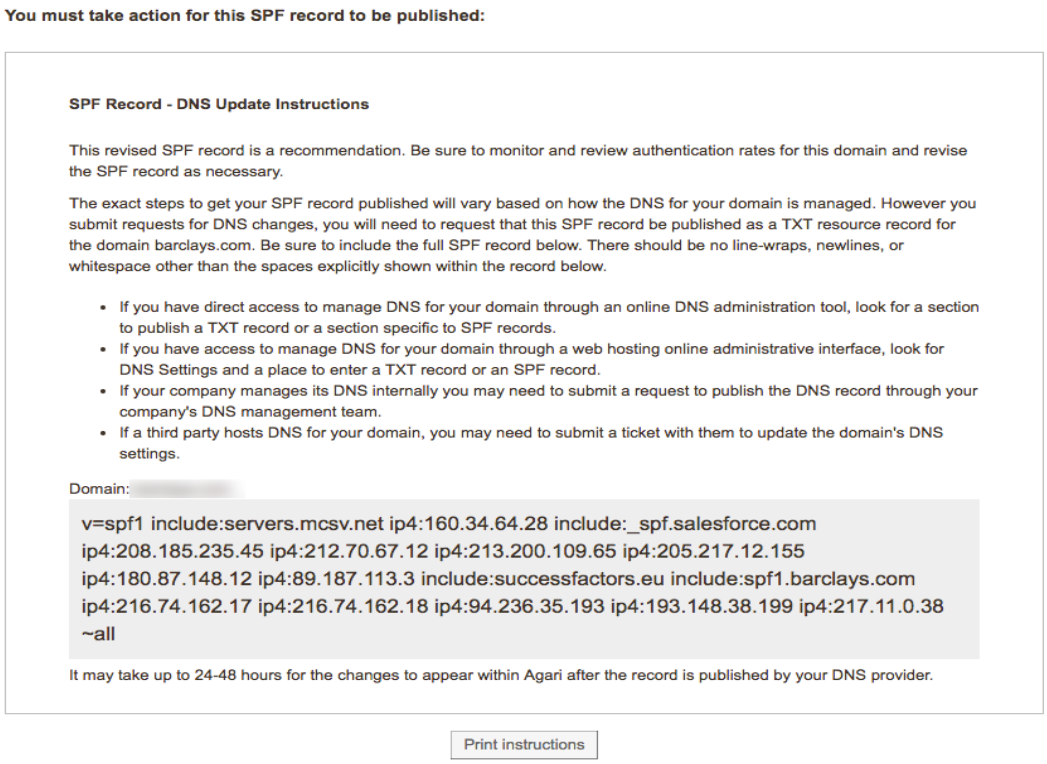
如果您有为思科知道其无法发送一致 SPF 邮件的发件人包含了一种机制，则可能需要查看“不一致发件人警告”。在这种情况下，您应访问该发件人的“发件人配置文件”页面以确定是否需要其他操作对来自该发件人的邮件进行完全身份验证。

图 4-11　便捷的 SPF 分析器：步骤 3（上半部分）



页面的下半部分将包含新的 SPF 记录和有关在 DNS 中创建 SPF 记录的说明。点击“打印说明”按钮以创建说明的打印友好版本。

图 4-12　EasySPF 分析器：步骤 3（下半部分）



托管的 SPF

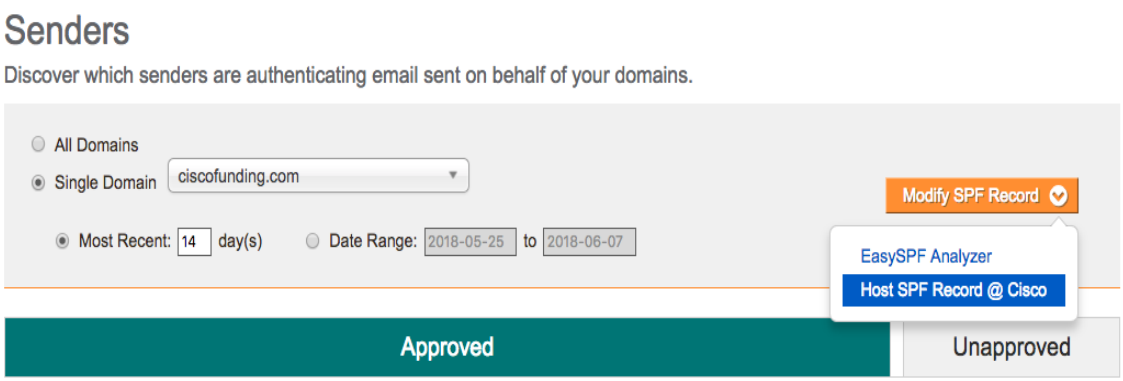
您可能希望思科代表您托管 SPF 记录。当您选择在思科托管 SPF 记录时，可以通过在批准发件人时快速准确地发布 SPF 记录来加快身份验证工作，而且不会在贵组织中导致手动 DNS 更改延迟。使用托管的 SPF，您可以放心地利用思科域保护的邮件云身份，只需点击几下便可对域的邮件进行身份验证。

要开始为域使用托管 SPF，请首先：

步骤 1　导航至“诊断”>“发件人”页面，并选择一个域以查看该域的已批准发件人。

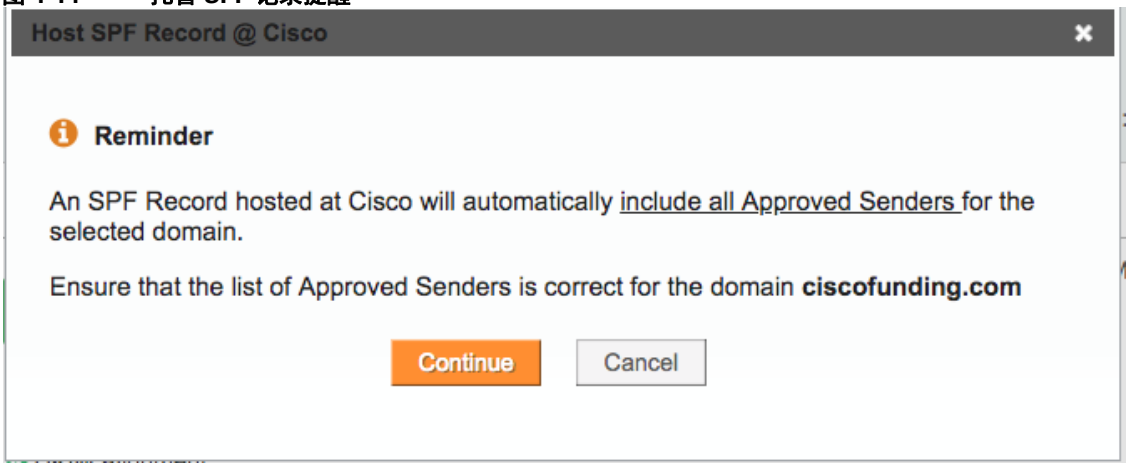
步骤 2　选择“修改 SPF 记录”>“在思科托管的 SPF 记录”。

图 4-13　在思科托管 SPF 记录选项



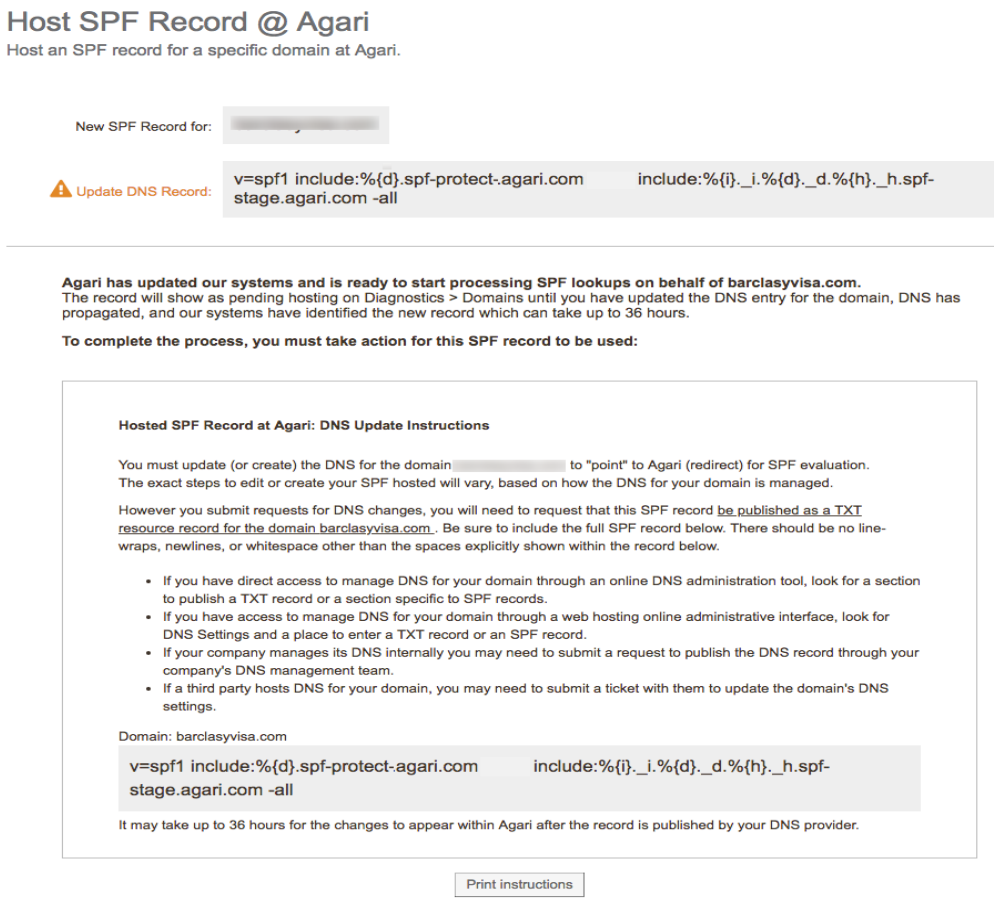
系统会显示提醒，通知您思科将包含所选域的所有已批准发件人：

图 4-14　托管 SPF 记录提醒



步骤 3　点击“继续”以开始为域托管 SPF 记录。

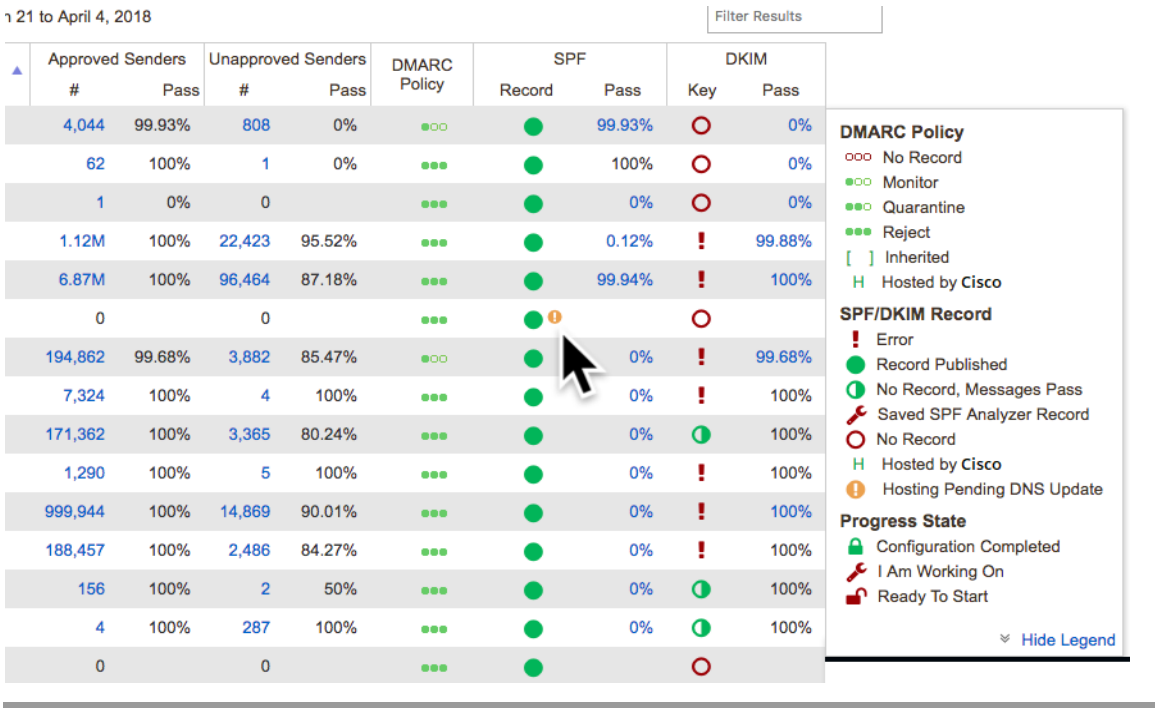
图 4-15　　托管的 SPF 说明



备注　您必须对要使用的 SPF 记录执行操作。您需要将 DNS 更新为“指向”思科（重定向）以进行 SPF 评估。

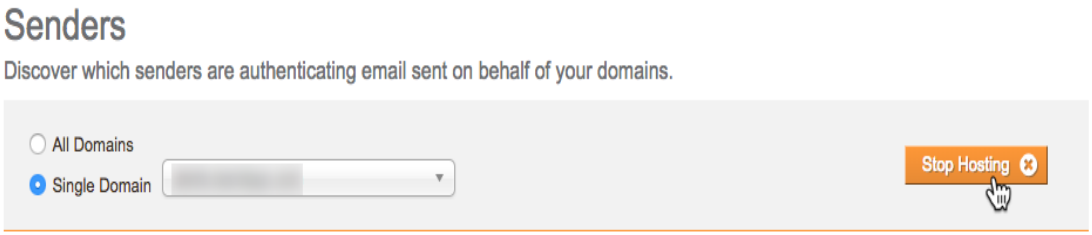
选择通过思科托管 SPF 记录后，相应状态会反映在“诊断”>“域”页面中：

图 4-16　托管待处理 DNS 更新



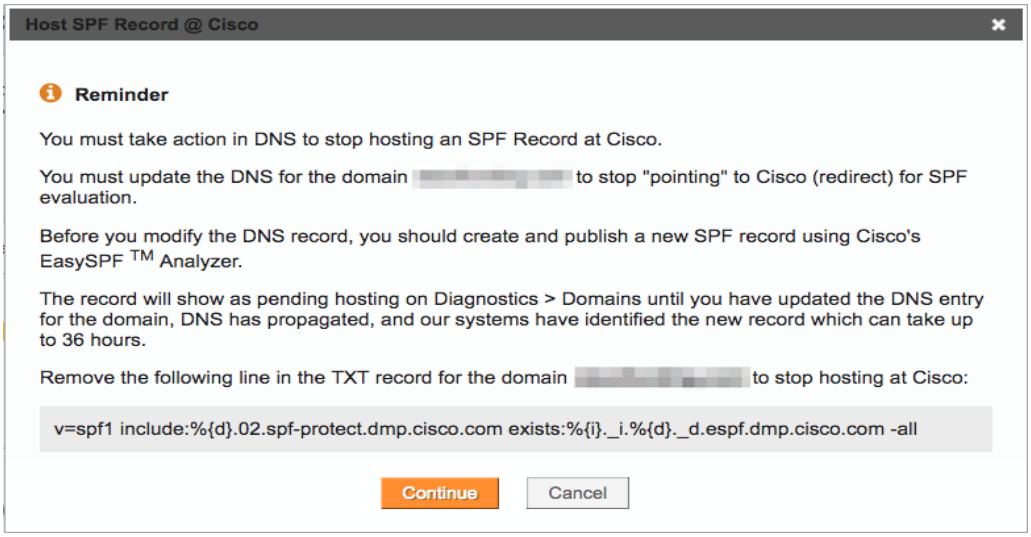
停止在思科托管

要停止托管一个托管的 SPF 记录，只需从所选域的“分析”>“发件人”页面选择“停止托管”：



系统将显示一条警告，提醒您需要哪些步骤以开始在您自己的 DNS 基础设施内托管 SPF 记录：

图 4-17　停止在思科托管 SPF 记录



步骤 8 和 9：发布 SPF 记录并识别企业所有者

此过程中的步骤 9 和 10 是迭代式的：您很可能在与贵组织中的企业所有者合作时为您的域发布和更新 SPF 记录，并在域记录的全面性方面收获信心。

同样，当您信心大增时，将在以下情况下更新 SPF 记录：开始进行不确定授权（`"?all"`），然后转至软失败授权（`"~all"`），最终转至失败授权（"-all"），然后继续监控数据。

如果我的发件人不支持 SPF 该怎么办？

某些发件人可能仅支持来自专用 IP 地址的一致 SPF。（例如，发件人 Marketo。）

在这种情况下，要通过没有专用 IP 选项的 DMARC，您必须使用 DKIM 通过一致的 DKIM 签名域对邮件签名。

请记住 DMARC 规范指出，如果 SPF *和/或* DKIM 检查成功且仍与 DMARC 设置的策略一致，则检查被视为成功；否则，DMARC 检查会设置为失败。

请查看下一章了解设置一致的 DKIM。

参考资料

以下是附加的一些参考资料，可帮助您了解为域启用 SPF 身份验证的过程。

Google G Suite 管理员帮助，“通过 SPF 授权发件人：”

https://support.google.com/a/answer/33786

Microsoft Office365 帮助，“在 Office 365 中设置 SPF 以帮助防止欺骗：”

https://technet.microsoft.com/en-us/library/dn789058(v=exchg.150).aspx

OpenSPF：

http://www.openspf.org/

SPF 维基百科条目：

https://en.wikipedia.org/wiki/Sender_Policy_Framework

RFC 7208，“发件人策略框架：”

https://tools.ietf.org/html/rfc7208

Word to the Wise 博客，“使用 SPF 进行身份验证：-all 或 ~all”

https://wordtothewise.com/2014/06/authenticating-spf/

全球网络联盟，“发件人策略框架 (SPF) 简介：深入了解”

https://www.youtube.com/watch?v=oEpU-iqBerI

第 5 章

DomainKey 识别的邮件

本章的步骤包含以下部分：

- 对邮件网关启用 DKIM 签名
- 验证 DKIM 在邮件网关上的运行情况
- 从第三方所有者请求 DKIM 签名
- 对所有第三方发件人实施 DKIM 密钥
- 对所有第三方发件人验证 DKIM 运行情况

您在第 3 章“监控”（第 1 页）中了解的监控工具将在本章中为您提供有关所需操作的信息；也就是说，您将使用监控结果来识别某个域的第三方发件人并执行相关操作，以便对这些发件人启用身份验证方法（SPF 和/或 DKIM 身份验证）。

您通过思科域保护获得的对邮件流的洞察力有助于您启用 DKIM。

Domainkey 识别的邮件 (DKIM)

Domainkey 识别的邮件也称为 DKIM，通过 RFC 6376 发布：（请参阅 https://tools.ietf.org/html/rfc6376。）

DKIM 为发送数字签名邮件的发件人定义了标准化方法。这样，收件人将可以非常有把握地确认邮件的实际发件人的身份，以及邮件在传输过程中是否被更改。DKIM 可为邮件发件人提供一种对其域的所有外发邮件进行数字签名的方式，从而补对 SPF 进行了有益的补充。DKIM 受到全球主要邮箱提供商的广泛支持，是并入 DMARC 中的两种基本身份验证方法之一。

DomainKey 识别的邮件 (DKIM) 通过将签名域和邮件关联，允许拥有该域的人员、角色或组织对邮件承担某些责任。DKIM 解决了将邮件签名者的身份与声称的邮件编写者分离开来的问题。责任断言的验证方式如下：通过加密签名以及直接查询签名者的域（在 DNS 中）来检索正确的公钥。

概述：DKIM 涉及加密

通过 DKIM 签名邮件涉及创建一个公共密钥/私钥对。

- 创建密钥对后，在 DNS 中发布公钥，然后使用私钥创建邮件的散列（或“签名”）部分。
- 接收者收到 DKIM 签名的邮件时，会根据您的公钥检查其签名。如果没有匹配，则将该邮件视为 PASS DKIM 签名。

DMARC 需要 DKIM 标识符一致

DMARC 规范扩展了 DKIM PASS 概念。

要通过 DMARC-DKIM，邮件需符合以下条件：

- 邮件必须使用有效的 DKIM 签名进行签名

  且

- 邮件的签名内容不得更改

  且

- 根据 DMARC 要求，DKIM 签名域必须与“发件人”域相匹配。

*标识符不一致*定义为邮件通过 DKIM 签名域的 DKIM 检查，但 DKIM 签名域未根据 DMARC 需要与“发件人”域相匹配。这种域的不匹配会导致 DMARC-DKIM 失败。

步骤 10-11：对网关启用 DKIM

您需要重复以下过程，对每个用于给定域的邮件网关启用 DKIM。

您自己基础设施中的邮件网关通常在“诊断”>“发件人”页面上显示为自定义发件人。

如果是您托管的邮件网关发送出站邮件，则您需要执行以下 4 个步骤来实施 DKIM：

步骤 1　确定域

确定允许从邮件网关发送出站邮件的所有域。“诊断”>“域”页面（和自定义域组）可帮助您确定全面的一组域。

步骤 2　创建密钥对

接下来，您将使用工具来创建 DKIM 公钥/私钥配对和策略记录。“公钥”是您将其与 DKIM“策略记录”一起放置在面向公众的 DNS 记录中的密钥。

“私钥”是安装在邮件网关（MTA/邮件发送系统）上的长密钥。当您发送外发邮件时，外发邮件网关会添加 DKIM 签名。

有多个在线工具可帮助您创建密钥对。一些可用于创建密钥对的在线工具包括：

https://port25.com/dkim-wizard/

http://dkimcore.org/tools/keys.html

https://www.dnswatch.info/dkim/create-dns-record

搜索“DKIM 密钥生成器”或“DKIM 密钥向导”将提供更多结果。

步骤 3　发布包含 DKIM 信息的 DNS 记录

创建 DNS 文本记录，其中包含用于发送邮件的每个域的 DKIM 信息。这些记录将插入每个发送域的面向公众的 DNS 记录中。请注意，您将创建

步骤 4　对网关启用 DKIM 签名

有关启用 DKIM 签名的说明因您的网关而异。以下提供了常用网关型号对应文档的一些链接：

思科邮件安全网关

https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide/b_ESA_Admin_Guide/b_ESA_Admin_Guide_chapter_010101.html

Symantec

https://support.symantec.com/en_US/article.HOWTO126432.html

Postfix

https://petermolnar.net/howto-spf-dkim-dmarc-postfix/

步骤 12 至 14 - 为第三方发件人启用 DKIM

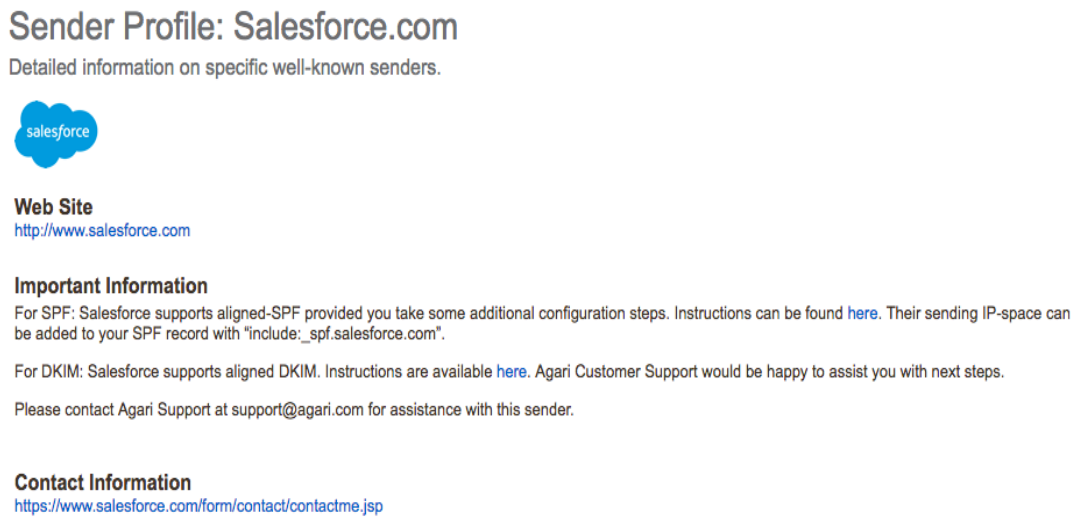
从第三方所有者请求 DKIM 签名

您将需要重复以下过程，对每个用于给定域的第三方发件人启用 DKIM。

步骤 1　转至“诊断”>“发件人”页面。

点击“常见发件人”列表中发件人的“发件人配置文件”链接，了解有关该发件人 DKIM 功能的信息：

图 5-1　有关“发件人配置文件”页面的 DKIM 说明的链接



点击 DKIM 说明链接会将您重定向到以下说明：为 Salesforce 代表您位于 https://help.salesforce.com/articleView?id=emailadmin_create_dkim_key.htm 的域发送的邮件启用 DKIM 签名。

为第三方发件人实施 DKIM 密钥

阅读针对每个发件人的文档（如上面的 Salesforce 示例中所示），该过程通常包括：

- 生成密钥对
- 选择域选择器
- 在 DNS 中发布公钥

对于 DKIM 密钥，相应规范定义：

- TXT 文件的名称根据选择器构建，后跟“._”，随后是域密钥，后跟“.”，最后是域名。例如：`selector._domainkey.domain.com`。
- TXT 文件中的值采用如下格式：`v=DKIM1; k=rsa; p=MHww...`，其中 p= 后的值是公钥的内容。

您现在可以移至所选域的下一个已批准的常见发件人。对下一个已批准的常见发件人重复上述步骤，从而相应地更新 DNS TXT 记录。

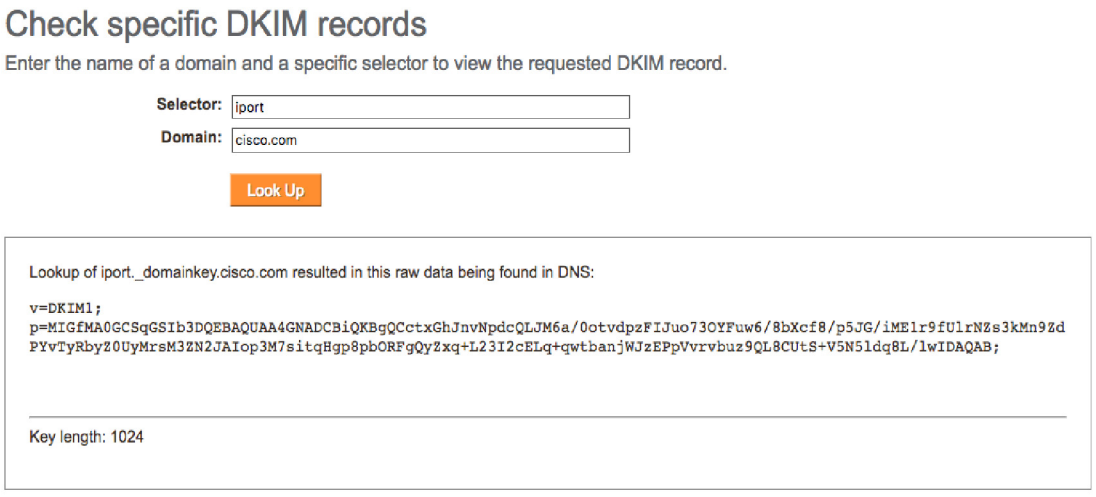
备注　*默认情况下*，许多第三方发件人会启用 DKIM 签名。例如，Microsoft Office365 和 Google G Suite 会自动为外发邮件启用 DKIM 签名。

对所有第三方发件人验证 DKIM

您可以使用 思科域保护（甚至公开可用的工具，例如 MX 工具箱：https://mxtoolbox.com/dkim.aspx）来验证是否在 DNS 中正确发布了 DKIM 记录。

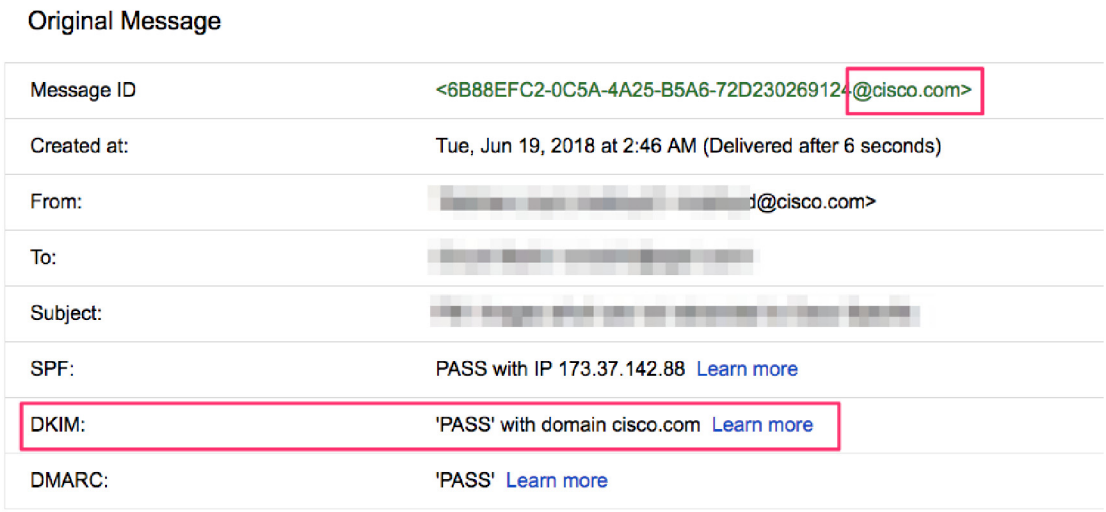
在 思科域保护 中，导航至“工具”>“DKIM”菜单，然后输入域名和选择器。例如：

图 5-2　检查 DKIM 记录



您可以通过检查收到的邮件的信头来验证第三方签名是否正确。例如，在 Gmail 客户端中，选择邮件上的“原始显示邮件”将显示 SPF、DKIM 和 DMARC 的身份验证结果。

此示例邮件从 Salesforce.com 的发送基础设施中发出。请注意，Gmail 客户端显示 DKIM PASS 的身份验证结果：



检查邮件的信头，您可以看到 Salesforce 插入适当的 DKIM 信头中：

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
  d=cisco.com; i=@cisco.com; l=5289592; q=dns/txt;
  s=iport; t=1529401619; x=1530611219;
  h=from:to:subject:date:message-id:references:in-reply-to:
   mime-version;
  bh=wwnGqrNevIbPG97FceJsWcspPFmLJJludpJAODKqgzM=;
  b=Cr5VTd6UKKVC8ixQr4G/FwA3gOWTezZNM8YYUpDf/06uxRm1lepYH9XF
   exxCsMcmhtauyH7CUXFfl2csTgWOnutzrhWhIU3p01U2fX821e8VXH1eI
   bDnRiQb9C+gaVVgv27MRcpmaJZCnxOaBjJUC/Ubs5Go+vZE+tfADyXX/0
   o=;
```

d=cisco.com - 域为 cisco.com

s=s1024 - 选择器为“s1024”

h=... - 用于确定散列的信头。

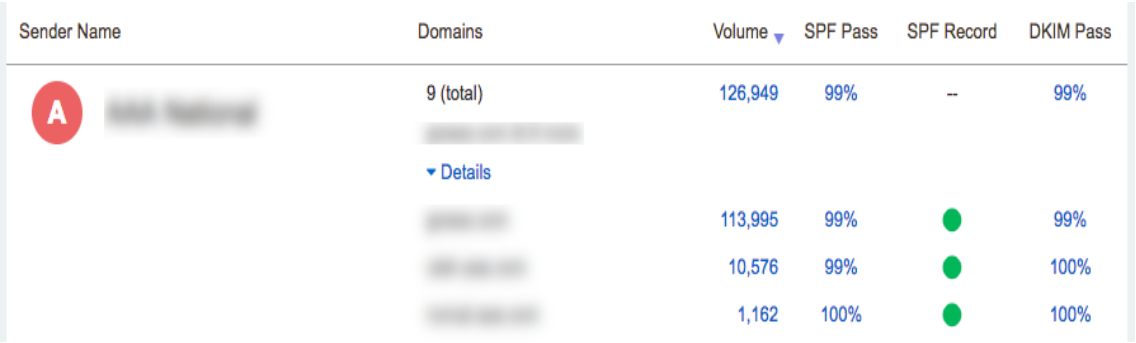
bh=... 邮件的正文散列。

b=... - 邮件内容的实际数字签名。

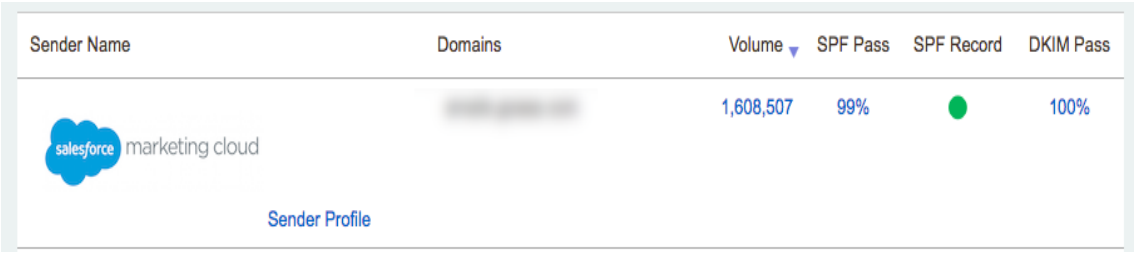
有关发送代理标记的 DKIM 信头的内容和结构的更多详细信息，请参阅 https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail#Technical_details。

DKIM 结果思科域保护

为域启用了 DKIM 签名时，您将在“发件人”页面中看到结果。在以下示例中，DKIM Pass 列已更新，以显示从自定义发件人 A 发送的邮件的域的 DKIM PASS 结果：



还会显示常见发件人的结果；以下示例显示从发件人 Salesforce 营销云发送的邮件的 DKIM PASS 结果：



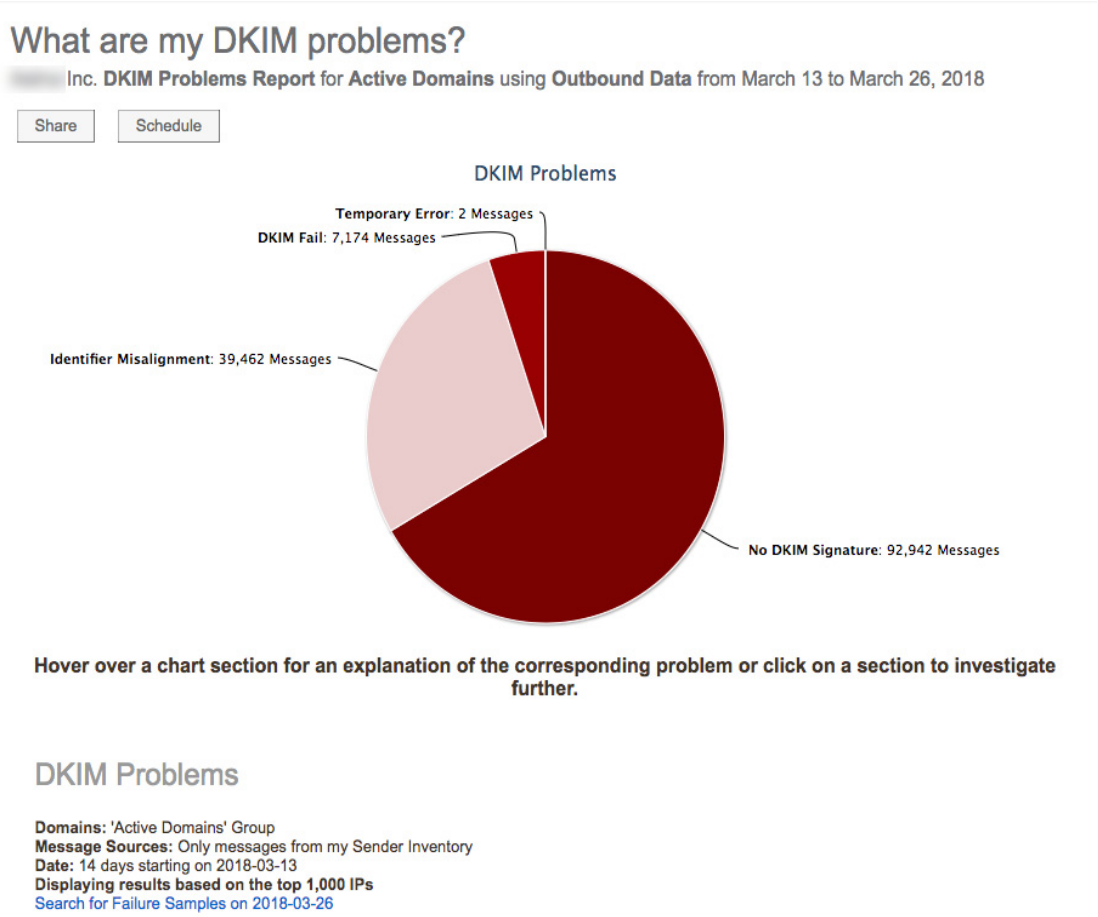
点击 DKIM Pass 列任何结果的链接将显示“我的 DKIM 问题是什么？”报告，具体在下一部分中介绍。

使用“DKIM 问题”报告查找问题

使用此报告，您通常可以识别在进行身份验证和为给定域中的每个发件人创建 DKIM 签名时要解决的问题所在的域和所属类别。

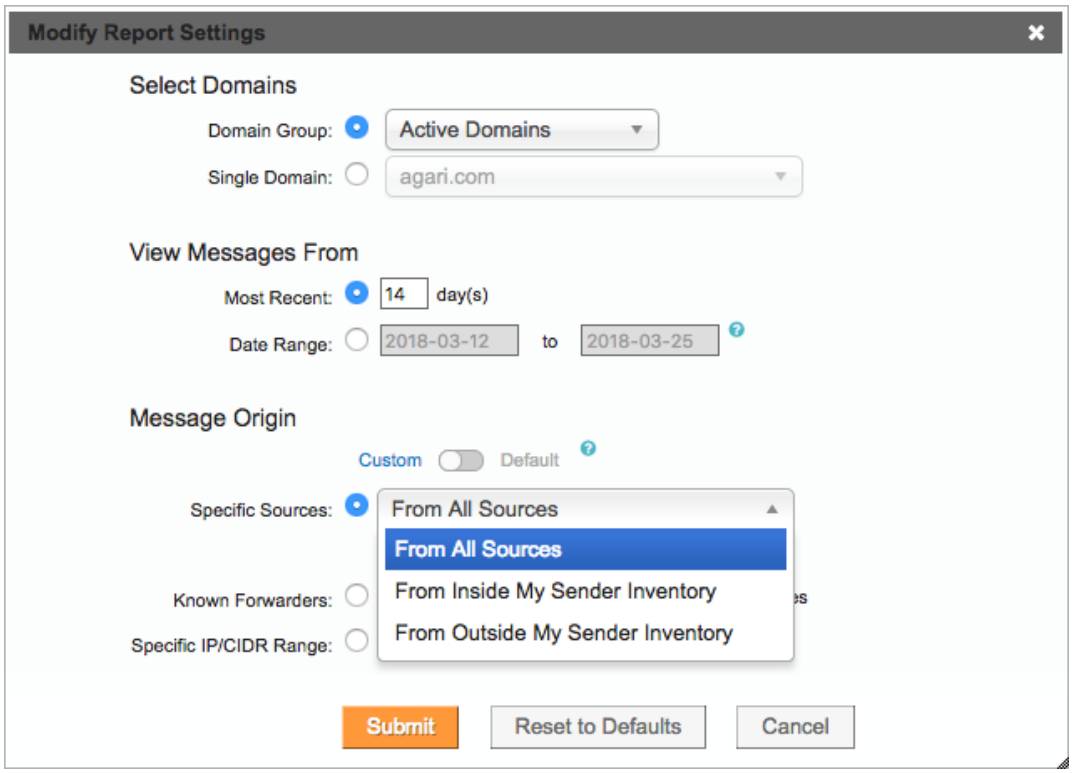
步骤 1　导航至“分析”>“邮件流量”>“我的 SPF 问题是什么？”以查看初始报告。

图 5-3　　DKIM 问题报告的最高级别



通常情况下，标识符不一致是“没有 DKIM 签名”（即：邮件根本未进行 DKIM 签名）之后的最大问题。请注意，可以使用左上角的“修改设置”按钮缩小范围或筛选此报告（例如，仅显示单个域在最近 2 周的 DKIM 问题）。

图 5-4　“修改设置”窗口



例如，您可能想要增加范围以查找“来自所有来源”的邮件。发件人清单外部的发件人将显示在“诊断”>“发件人”页面的“未批准”选项卡上。

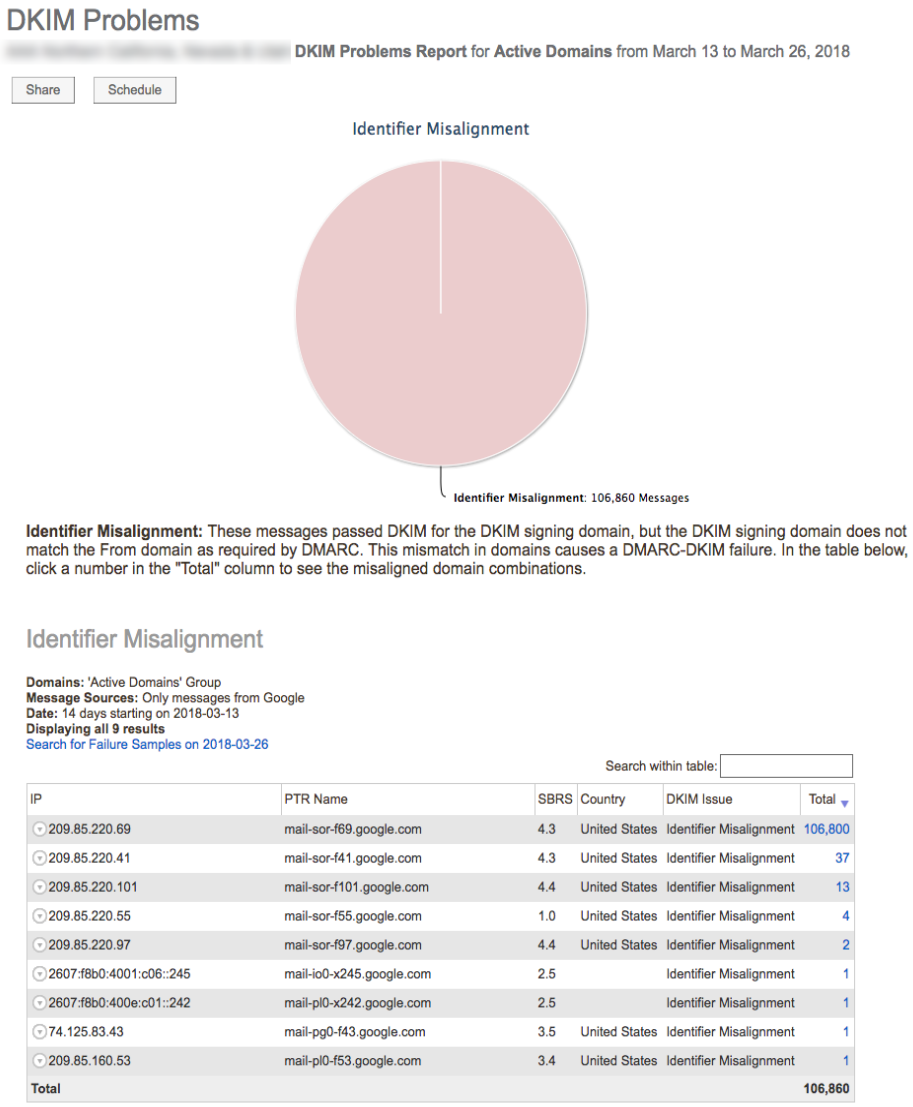
检查此报告下半部分中的发件人列表可了解问题。例如，您可能会注意到选定域从发件人 Google 发送的邮件存在“标识符不一致”和“无 DKIM 签名”问题：

图 5-5　Google 标识符不一致问题

Sender	DKIM Issues	Total
Google	All Issues	107,981
	Identifier Misalignment	106,858
	No DKIM Signature	1,057
	DKIM Fail	66

步骤 2　点击从发件人 Google 发送的邮件以深入了解该发件人的详细信息：

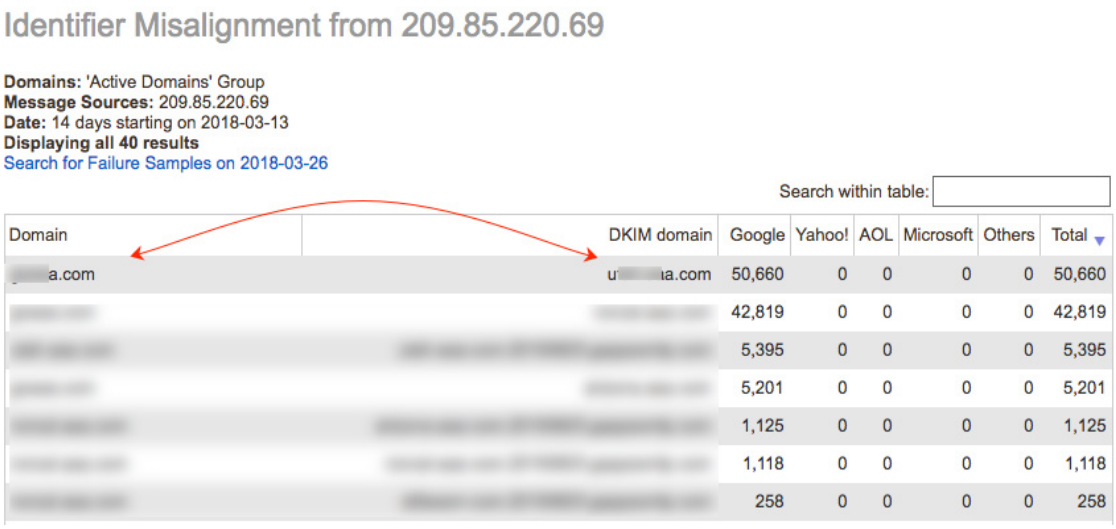
图 5-6　Google 不一致详细信息视图



该视图显示从 Google 发送的邮件不一致。事实上，大多数一致性失败都来自单个 IP 地址：209.85.220.69，mail-sor-f69.google.com。

步骤 3　点击该 IP 地址对应的链接以深入了解更详细级别的信息。

在此示例中，大多数失败（超过 50,000 个）来自与 DKIM 密钥不一致的单个域：



通过这种方式，您可以缩小问题类别的范围：

- 无 DKIM 签名（含义：您需要针对特定域为发件人实施 DKIM 签名）
- 标识符不一致（含义：您需要将“发件人:”域与用于特定域的签名密钥保持一致）。

对于每个域，您可以使用“发件人”页面以及“我的 DKIM 问题是什么？”报告视图来系统地对每个域的发件人进行 DKIM 签名。

共享或订用报告

您可以将“我的 DKIM 问题是什么？”报告发送给其他人，或定期接收报告的邮件版本。

点击视图顶部的“共享”或“订用”按钮可共享或订用报告。

请记住，所有计划的报告均保持在“修改设置”按钮中定义的范围。例如，您可能想要将缩小范围版本的报告（单个域的单个发件人）定期发送给企业所有者，但是在为域构建全面的 SPF 记录时收到了范围更广版本的报告（所有域的所有发件人）。

参考资料

以下是附加的一些参考资料，可帮助您了解为域启用 DKIM 签名的过程。

Google G Suite 管理员帮助，“关于 DKIM：”

https://support.google.com/a/answer/174124?hl=en

Microsoft Office365 帮助，“使用 DKIM 验证从 Office365 中的自定义域发送的出站邮件：”

https://technet.microsoft.com/en-us/library/mt695945

OpenDKIM：

http://opendkim.org/

DKIM 维基百科条目：
https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail

RFC 6376，“DomainKey 识别的邮件 (DKIM) 签名”
https://tools.ietf.org/html/rfc6376

Word to Wise 博客，“DA DKIM Primer Resurrected:”
https://wordtothewise.com/2016/04/a-dkim-primer-resurrected/

F-Zero,“如何通过 3 个步骤设置 DKIM - 设置 DNS 和邮件：”
https://www.youtube.com/watch?v=q4SNXHhIIJw

转为使用拒绝策略

本章的步骤包含以下部分：

- 获取所有企业所有者的签名
- 将 DMARC 记录移动到拒绝策略

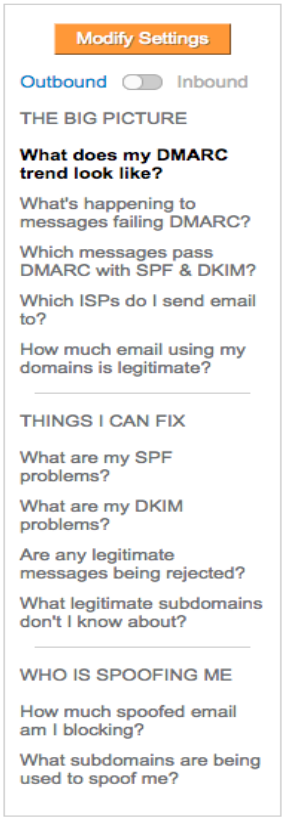
使用 DMARC 实施

在前面几章中，您了解了对您域中的邮件进行身份验证需要执行的步骤。在对每个域重复执行各个步骤时，您可以使用思科域保护中的工具和报告来组织和跟踪进度。

通过报告监控

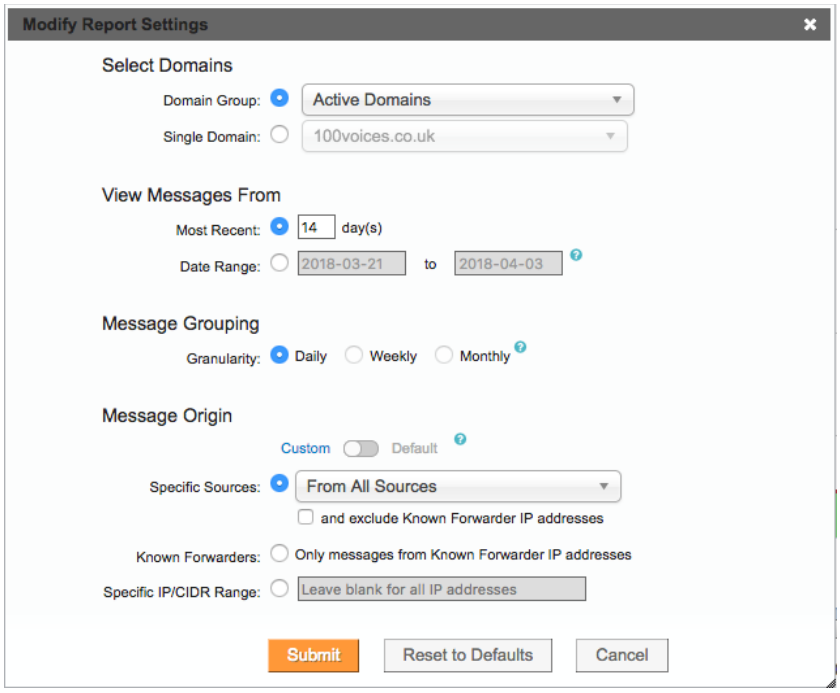
您在前面几章中了解了一些报告。在重复执行步骤时，请抽时间查看“分析”>“邮件流量”视图中为您提供的其余所有报告。

图 6-1　　邮件流量分析器报告



该类型的报告均提供源于 DMARC 聚合和调查分析数据的重要信息，而且展示了 思科域保护 解决方案的强大功能。请记住，对于任何报告，您都可以使用“修改设置”按钮以多种方式编辑参数：

图 6-2　修改所有邮件流量分析器报告的报告设置



大多数报告都有多个“深入分析”视图，允许您关注要处理的特定邮件流和区域。

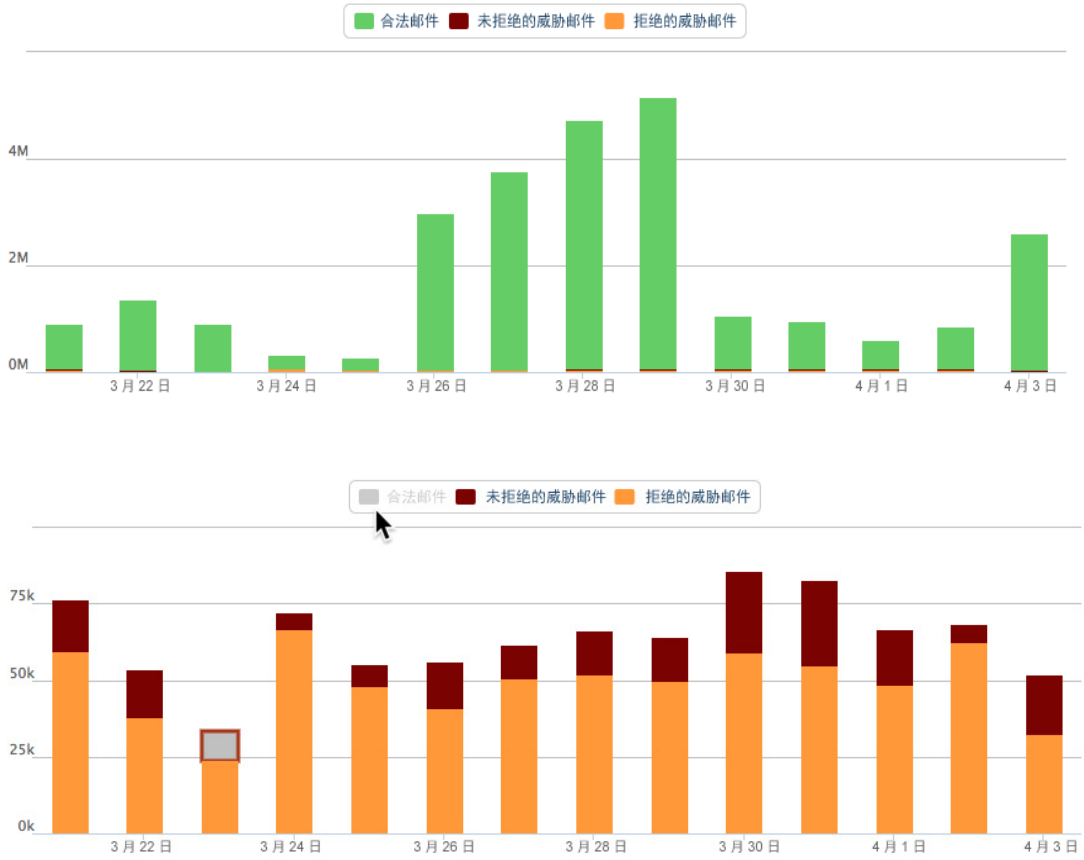
报告交互性

备注　视图中的许多报告具有交互式图表选项；也就是说，您可以点击某个时间段对应的条形图部分以缩小结果范围。

报告视图中的大多数表格列均可排序；点击列标题可按该列对表格进行排序，或再次点击可反向排序。

同样，您可以通过启用和禁用要显示的图表部分来筛选视图（即点击条形图顶部的键可启用或禁用该部分的显示）。

图 6-3　交互式条形图示例



共享和计划

最后，所有报告视图都能够进行共享或计划。点击报告视图顶部的按钮可使用您在“修改设置”按钮中选择的参数来共享和/或计划报告。

报告如下所示：

概述

- 我的 DMARC 趋势如何？

  此报告显示邮件通过和未通过 DMARC 检查的的总体趋势。随着您对来自所有域的所有发件人身份验证的增加，您可以确定何时有足够多的邮件通过 DMARC 检查，以便放心地转为使用拒绝策略。

- 未通过 DMARC 的邮件发生了什么情况？

  可对未通过 DMARC 检查的邮件执行不同的操作，具体取决于：a) 您的策略和 b) 接收者的操作。使用此视图可检查未通过的邮件，了解各种大型接收者（Google、Yahoo、AOL、Microsoft 等）对它们的处理方式。深入分析详细信息以逐个域检查未通过的邮件。

- 哪些邮件通过了 DMARC 以及 SPF 和 DKIM？

  相反，此视图按域显示通过的邮件（通过 DMARC 和/或 SPF 检查）。您可以使用此视图深入分析详细信息，查看每个域在身份验证检查方面的执行情况。

- 我将邮件发送至哪个 ISP？

  此透视视图显示了对应于以下各类身份验证失败的 ISP 明细：已通过 DKIM 和 SPF 检查、两者均未通过，或只通过其中一个。

- 使用我的域的邮件有多少是合法的？

  在另一个透视视图中，您可以查看合法邮件和威胁邮件，它们按域以总量的形式显示。

  *合法邮件*包括源自发件人清单中的 IP 地址的任何邮件（即已批准的发件人列表），无论它们已通过还是未通过 DMARC 身份验证。此外，还包括来自发件人清单之外的已通过 DMARC 身份验证的邮件，例如保留原始 DKIM 签名的自动转发邮件。

  *威胁邮件*是未通过 DMARC 身份验证且源自 IP 空间外部的邮件。

我可以解决的问题

- 我有哪些 SPF 问题？
- 我有哪些 DKIM 问题？

  如之前各章所述，您可以使用这些报告来深入了解有关任何域的 SPF 和 DKIM 身份验证进度及问题的详细信息。有关更多详细信息，请访问使用“SPF 问题”报告，第 4-9 页和使用“DKIM 问题”报告查找问题，第 5-6 页。

- 是否拒绝了任何合法邮件？

  使用此报告可确定是否由于您的 DMARC 策略导致收件人*错误*地拒绝了邮件。

- 有哪些我不了解的合法子域？

  使用此报告可发现您的组织正用于发送邮件的子域。请参阅我不了解的合法子域，第 3-3 页。

谁在欺骗我

- 我阻止了多少欺骗邮件？

  在实施拒绝策略时，您可以在此报告视图中查看实施策略的优势。

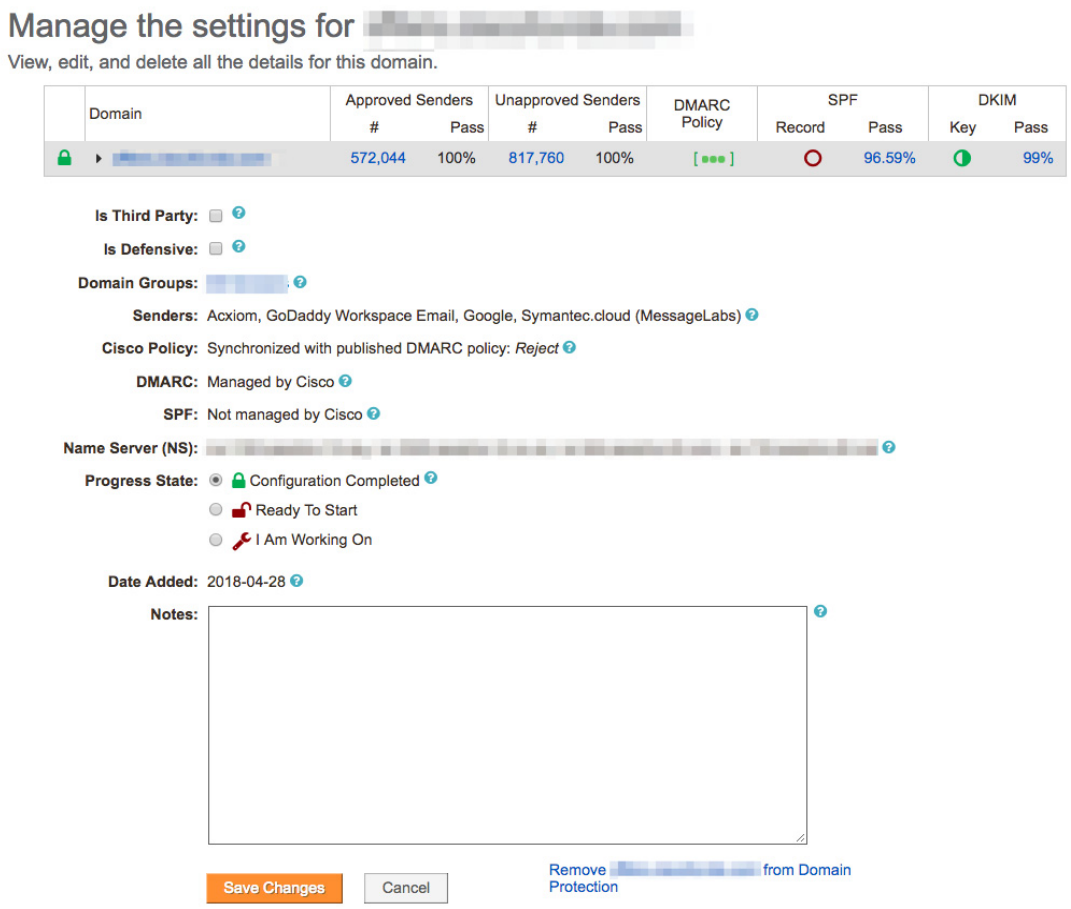
- 哪些子域正被用来欺骗我？

  与上面的子域报告一样，您可以使用此视图来发现当前未经过您授权发送邮件的子域。在 思科域保护 中将子域注册为*防御域*以实施 DMARC 拒绝策略。

组织域

“分析”>“域”页面包含每个域的详细视图。点击域可查看其状态：

图 6-4　　域的详细信息页面



域详细信息会显示注册到您的组织的域的相关数据和特征摘要。您还可以编辑某些特征并存储有关域的备注。

第三方

此域是否由第三方发件人用于代表您发送邮件？域可以专门由第三方使用，也可以只是混入第三方流量。如果思科已自动检测到第三方发件人，则会选中此框。

防御

防御域是已注册但不用于发送任何合法邮件的域。思科建议通过 DMARC 拒绝策略保护防御域以避免滥用。如果思科已自动检测到某个域为防御域，则会选中此框。防御域会添加到“防御域”系统组。

域组

此域所属的域组的列表。

域保护策略

为此域发布的思科专用信道策略。如果域具有已发布的 DMARC 记录，则域保护策略会自动同步为相同的情况。如果未发布任何 DMARC 策略，则可以在此处设置域保护策略。

名称服务器 (NS)

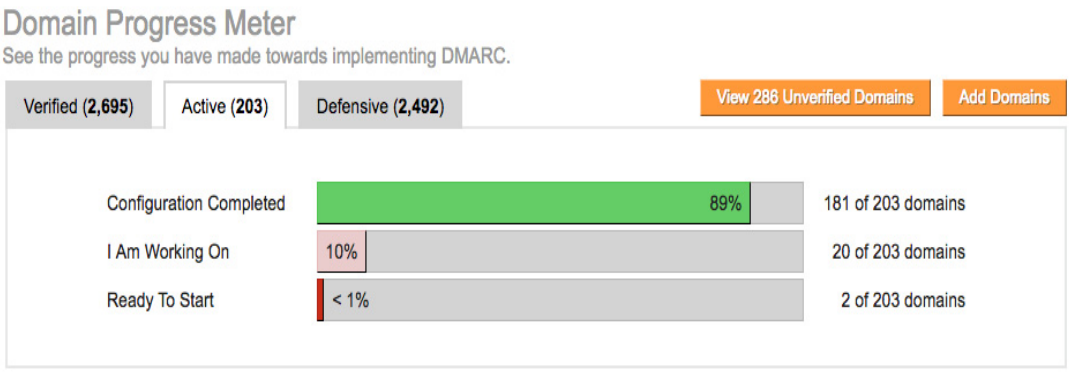
为域托管 DNS 记录的服务器。

进度状态

域的进度状态将帮助您跟踪当前正在处理的域、已完成处理的域以及需要注意的域。您可以通过点击域名旁边的星形将域设置为“我正在处理中”、“已完成配置”或“已准备好开始”。

备注　使用进度状态会影响“状态”>“保护”页面上反映总体进度的域进度指示器的状态：

图 6-5　域进度指示器



- 已完成配置

  域完全受保护且思科未检测到任何其他问题时，思科域保护 会自动将其标记为“已完成配置”。当没有计划进一步的工作来保护某个域时，也可以将该域标记为“已完成配置”。如果您手动将某个域标记为“已完成配置”，即表示您确认该域具有无需或无计划予以解决的待解决问题。

- 我正在处理中

  如果您解决某个域的问题，请将其标记为“我正在处理中”，以使其进入完全受保护状态。例如，您已提交 DNS 变更申请来更新 SPF 记录或将 DMARC 策略更改为拒绝，并且您正在等待更改生效。

- 已准备好开始

  大多数域在开始时将处于此状态。思科建议您执行一些操作以便完全保护域。您可以通过手动更改域的进度状态，将域从“我正在处理中”或“已完成配置”恢复为“已准备好开始”状态。

添加日期

在 思科域保护 中批准域并将其添加到您的组织的日期。

说明

自由文本字段，您可以在其中存储有关域的备注。只需添加或附加新文本，或者删除不再相关的现有文本。

步骤 15 和 16：实施

使用上面的监控视图，希望您对于为域实施更加严格的策略来执行身份验证充满信心。

如果您在移至拒绝策略之前需要帮助解释相关数据，可以随时安排思科客户支持团队进行检查。

思科建议您：

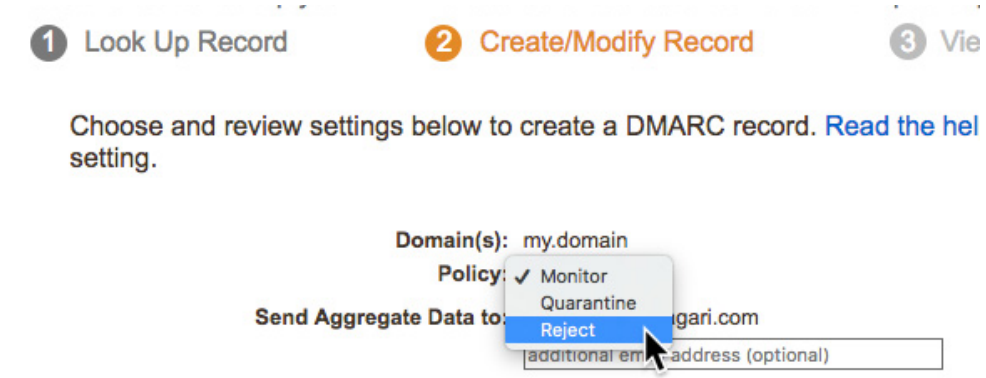
- 从企业所有者获取签字。

  在启用实施策略之前，请确保您已与域的所有内部企业所有者进行沟通。如上述报告所示，您应该能够预测从单个域、发件人、ISP 接收者等方面出现的任何传送性问题。

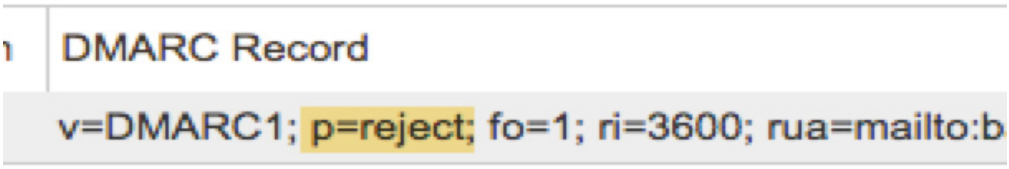
- 将所选域的 DMARC 记录移至拒绝。

  更新和发布策略的过程与您在步骤 2：在监控策略中发布 DMARC 记录，第 2-3 页中使用的过程相同；但是，现在您已获得可视性，可以将策略设置为拒绝：

图 6-6　　将 DMARC 策略修改为拒绝



已修改的策略将包含 **p=Reject** 注释：



您已成功完成所有步骤！

使用本指南，您已成功管理为组织中的某个域或一组域应用实施 (p=Reject) 策略的步骤。

使用 DMARC，您可以充满信心地保护您的品牌，避免受到欺骗并在您的客户之中建立信任。

监控更改

本章的步骤包含以下部分：

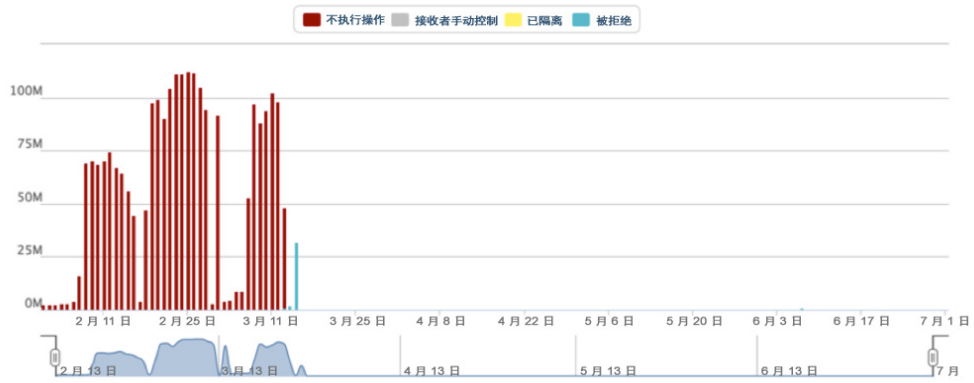
- 查看警报和报告

监控过去的拒绝策略

启用了带有拒绝策略的一个或多个域后，即可发现身份验证的优势。

例如，对于此思科域保护客户，“我的 DMARC 趋势如何”报告会显示，将域转为使用拒绝策略后，垃圾邮件发送者就离开了，且已停止尝试欺骗该域：

图 7-1　　转为使用拒绝策略的优势

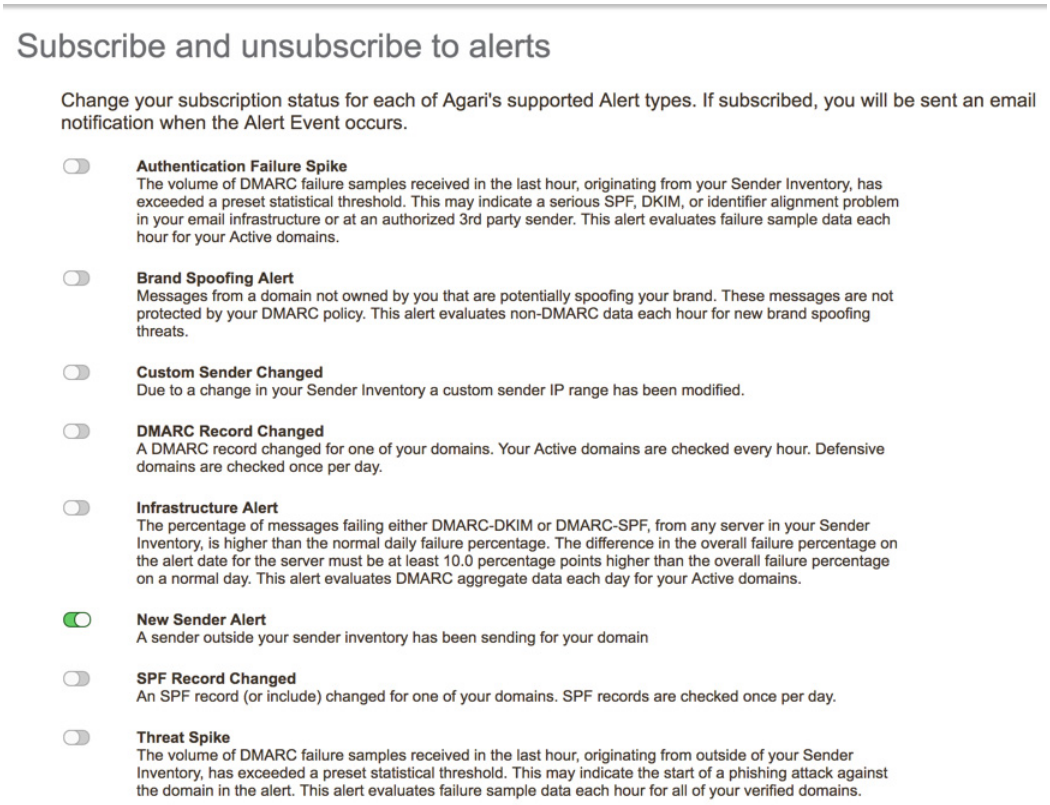


警报

思科域保护定义了您可以订用的警报。在监控您计划保护的所有域的身份验证时，请考虑订用相关的警报。

步骤 1　可通过导航到“状态”>“警报”并点击“管理我的订用”来开始订用。

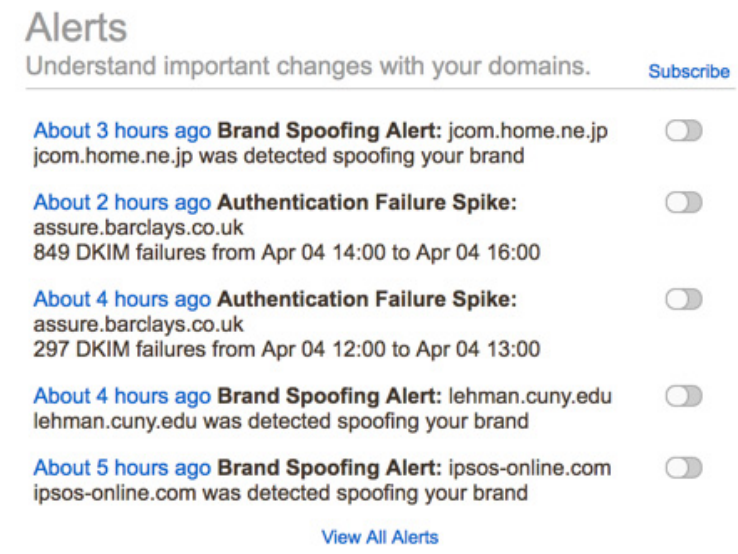
图 7-2　　警报订用



步骤 2　点击“管理组织警报设置”来管理各种警报类型的阈值和例外情况。

最近的警报也会显示在“状态”>“保护”概述页面中：

图 7-3　　概述页面上的最近的警报



后续内容...

本入门指南仅涉及为组织实施 DMARC 策略的基础知识。

请联系思科支持部门，详细了解思科域保护的一些高级功能，包括：

品牌欺骗检测

每当出现问题的 DMARC 邮件中显示特定品牌标识字符串时，都会发出相应警报。

类似域

了解与您的域类似的域，客户可能使用这些域来损害您的品牌形象。

威胁源

了解如何结合使用思科的威胁源与信息清除方案供应商，以快速应对恶意欺骗。

API 访问

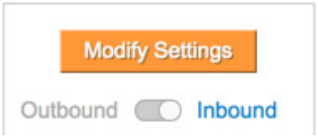
通过应用程序编程接口 (API) 访问思科域保护中的信息，以与其他安全工具配合使用。

SSO 访问

支持通过单点登录 (SSO) 功能登录到思科域保护。

入站洞察力（“反映”）

您可以安装其他软件以获得对发送*到*您组织的邮件的 DMARC 可视性。



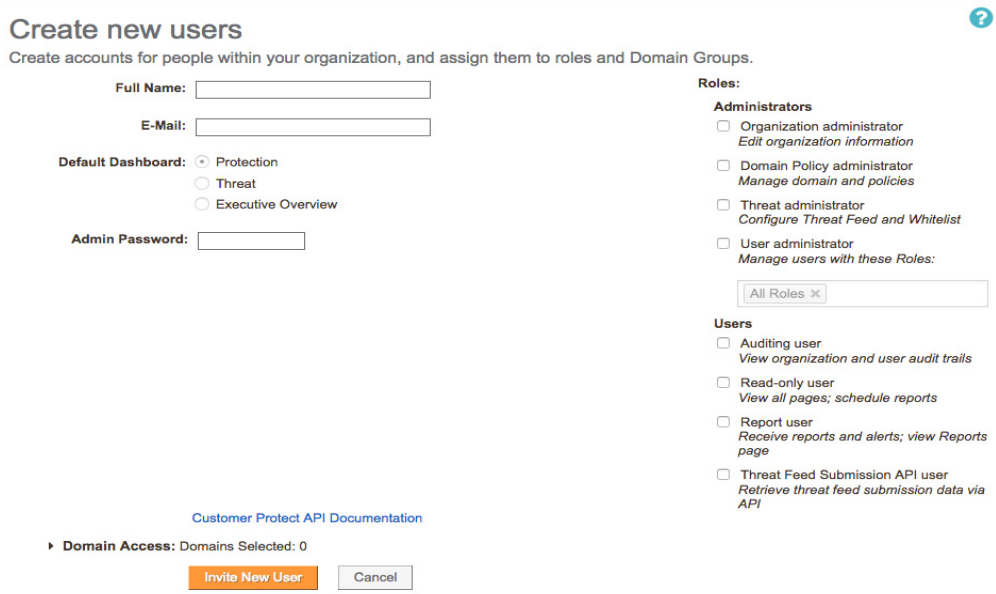
后续内容...

用户帐户

添加用户

思科域保护支持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用于访问思科域保护功能。

通过导航至“管理”>“用户”页面并点击“创建新用户”，将新用户添加到系统。



在页面左侧，输入以下项的值：

- 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。

- 邮件

  用户的邮件地址，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，此邮件地址用于具有初始激活令牌的邀请邮件。

- 默认控制面板

  选择在用户登录时显示的控制面板。

激活新用户

思科会向每个新创建的用户发送邀请邮件（有效期为 30 天），用于激活其新的思科帐户。如果您已分配警报和报告，则新用户将在此 30 天期限内收到报告和警报，即使他们没有激活其帐户也是如此。如果在此 30 天的期限内未激活用户，则系统会停止所有报告和警报。

用户角色

有两种类型的用户角色：

- 管理员角色 - 可以对您组织中的设置进行更改。
- 只读角色 - 用于接收警报和/或查看数据/信息

您可以单独分配角色，或将其与另一个角色一起分配（例如具有日志审核者用户权限的组织管理员。角色权限没有分层继承）。请谨慎选择角色；系统会自动选择低于您为用户选择的最高级别角色的角色。您可以取消选择角色，但取消选择某些组合可能会导致异常 UI 行为。下面提供设置用户角色的一些示例。

管理员角色

以下是可用的管理员角色：

- 组织管理员

  管理组织级别设置。这包括为您的组织设置密码规则、设置会话到期时间、设置数据收集策略，以及为访问思科域保护 Web 门户的用户设置基于 IP 的访问控制列表限制。

- 域策略管理员

  管理域级别设置。这包括从您的组织添加、编辑或删除域或自定义域组，以及为您的组织编辑发件人清单。

- 威胁管理员

  管理威胁级别设置。这包括配置您组织的威胁源以及编辑您组织的 URI 白名单。

- 用户管理员

  管理用户，包括在您的组织中添加、编辑或删除用户。

当您创建用户管理员时，必须分配此管理员可以提供给用户的角色类型（请参阅下面的“角色使用示例”）。

只读角色

以下是可用的只读角色：

- 日志审核者

  查看您的组织和组织中的用户的审核日志。

- 只读

  在 Web 门户中查看数据和计划报告。

- 报告收件人

  接收已计划的报告和警报。

备注　顾名思义，此角色无法直接在门户中查看数据。它仅可以接收由其他用户计划的通过邮件发送的报告，接收其他用户订用的通过邮件发送的警报，以及从 UI 中查看订用的报告的列表。

要创建帐户用于将报告和/或通知发送到邮件列表而不是个人，请照常创建并邀请用户，然后在“用户”列表中，点击用户的名称以编辑该用户，添加强密码，点击“更新”，该虚构用户现已激活并可用于接收报告。

域特定的访问权限

默认情况下，将为新用户分配对所有域的访问权限。

您可以通过分配对自定义域组的用户访问权限，将用户访问权限限制到特定域：

- 点击“邀请新用户”按钮上方的“域访问权限”旁边的箭头。
- 查看可用的域组，然后从列表中选择一个或多个自定义域组。

  您创建的用户仅可在门户和报告中查看属于这些组的域，而且仅会收到针对此组域的警报。

具有域特定访问权限的用户只能查看与其具有访问权限的域相关的数据，因此在其访问“我的 DMARC 趋势如何？”的邮件流量分析时会看到的视图不同于对有权访问所有域的用户可用的视图。

角色使用示例

- 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。

- 创建可以更改域设置但无法创建或编辑用户的用户

  为您要创建的用户选择域策略管理员角色。默认情况下，系统将选择域策略管理员下的所有角色。如果您不希望此用户能够创建或编辑其他用户，请取消选择“用户管理员”角色。