

报告垃圾邮件、分类错误、病毒邮件

目录

[简介](#)

[邮件提交类型](#)

[为什么向思科报告电子邮件？](#)

[电子邮件状态门户](#)

[如何向思科报告电子邮件](#)

[思科安全电邮提交插件](#)

[思科电邮安全插件](#)

[直接电邮提交](#)

[Microsoft Outlook](#)

[Microsoft Outlook Web App、Microsoft Office 365](#)

[Microsoft Outlook 2011和Microsoft Outlook 2016 for Mac\(OS X、macOS\)](#)

[邮件\(OS X、macOS\)](#)

[Mozilla Thunderbird](#)

[移动平台 \(iPhone、Android或其他 \)](#)

[如何验证向思科提交的文件](#)

[直接电邮提交](#)

[电子邮件状态门户](#)

[其他信息](#)

[思科安全电邮网关文档](#)

[安全电邮云网关文档](#)

[思科安全电邮和Web Manager文档](#)

[思科安全产品文档](#)

简介

本文档介绍向思科报告垃圾邮件、误分类、病毒或其他电子邮件以获得支持或检查。

邮件提交类型

垃圾邮件、火腿和营销邮件包括：

- **垃圾邮件**:与收件人无关或不适当的电子邮件。
- **火腿**:非垃圾邮件的电子邮件。或者“非垃圾邮件”、“好邮件”。
- **营销**:直接营销商业电子邮件。

思科接受对任何分类不正确的电子邮件的提交：

- **误报** (漏报垃圾邮件)

- 误报 (或“Ham”)
- 虚假的营销信息
- 误报营销信息
- 怀疑网络钓鱼的邮件，怀疑网络钓鱼的邮件
- 怀疑病毒的病毒阳性邮件

为什么向思科报告电子邮件？

报告给思科帮助的电子邮件消息有漏报或标记错误，包括内容确认、整体效力以及相关规则和分数。向思科报告电子邮件后，您可以通过电子邮件状态门户查看其他可观察的附件和嵌入的附件。

电子邮件状态门户

使用有效的CCO ID，您可以登录https://talosintelligence.com/tickets/email_submissions。电邮状态门户是查看您向思科提交电邮的状态的工具。思科鼓励提交绕过当前检测内容的垃圾邮件/网络钓鱼邮件和错误过滤出的Ham（理想邮件），以提高整体效力。电子邮件状态门户提供了一种跟踪这些提交的状态的方法。您可以监控您的提交，而域管理员或域查看器可以监控来自您的域的所有提交。

注意：从2020年9月1日起，旧版邮件提交和跟踪门户(ESTP)已替换为托管于Talosintelligence.com的邮件状态门户。

如何向思科报告电子邮件

支持的方法包括：

1. 思科安全电邮提交插件
支持Outlook (Windows、Mac和Web)
2. 思科电邮安全插件 支持Outlook (仅Windows)
3. 直接从最终用户提交电子邮件

思科安全电邮提交插件

思科安全邮件提交插件支持Microsoft Outlook for Windows、Mac和Web。请参阅[Compatibility Matrix for Cisco Secure Email Encryption Service Add-In and Cisco Secure Email Submission Add-in](#) (思科安全邮件加密服务兼容性矩阵) 中的“Supported Configurations for Cisco Secure Email Encryption Service Add-in”，以确保Outlook版本的兼容性。

有关下载和安装文档，请参阅[思科安全邮件提交插件](#)。

思科电邮安全插件

思科邮件安全插件仅支持Windows上的Microsoft Outlook。请参阅《思科安全邮件加密服务兼容性矩阵》中的“思科邮件报告插件的[支持配置](#)”，以确保Outlook版本的兼容性。

注意：旧版本的插件名为“IronPort邮件安全插件”或“Encryption Plug-in for Outlook”。此版本的插件同时包含报告和加密。2017年，思科分离了这些服务，并发布了两个新版本的插件“Email Reporting Plugin for Outlook”和“Email Encryption Plugin for Outlook”。1.0.0.x版本提供这些功能。

直接电邮提交

请按照提供的电子邮件客户端说明将电子邮件附加为[RFC 822多功能互联网邮件扩展\(MIME\)](#)编码附件。如果其中一个示例未反映您的电子邮件客户端，请直接参阅您的电子邮件客户端用户指南或产品支持，并确认电子邮件客户端支持“作为附件转发”。

请将提交的电子邮件发送到相应的电子邮件地址：

spam@access.ironport.com

最终用户认为电子邮件垃圾邮件或主题行包含[SUSPECTED SPAM]。

ham@access.ironport.com

最终用户不会将电子邮件视为垃圾邮件。主题行包含[可疑垃圾邮件]，或者主题行包含标记。

ads@access.ironport.com

最终用户认为电子邮件是或包含营销内容或灰色邮件，或者主题行包括[MARKETING]、[SOCIAL NETWORK]或[BULK]。

not_ads@access.ironport.com

最终用户不认为电子邮件是营销邮件或灰色邮件，或者主题行包含[MARKETING]、[SOCIAL NETWORK]或[BULK]。

phish@access.ironport.com

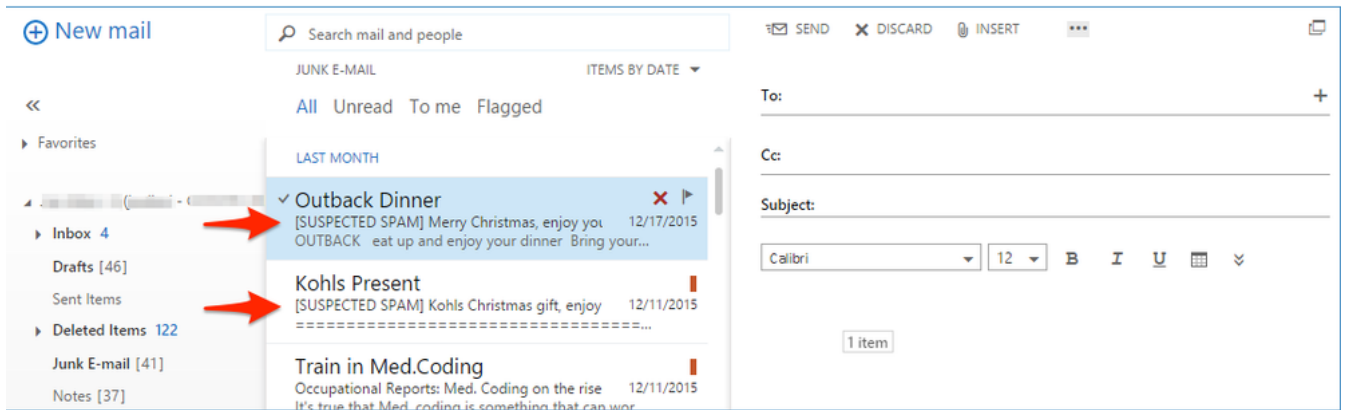
电子邮件似乎是网络钓鱼（旨在获取用户名、密码、信用卡信息或其他个人信息者电子邮件包含恶意软件附件（同样，也是为了获取用户名或密码）。主题行前缀为垃圾邮件]、[可能的\$threat_category欺诈]或类似内容。

virus@access.ironport.com

最终用户将电子邮件或附件视为病毒邮件，或主题行包含[警告：病毒检测]。

并非所有主题行都包含其他文本和标记。有关您的设置，请咨询思科安全邮件网关或云网关的反垃圾邮件、防病毒、灰色邮件和爆发过滤器配置，或者如有任何疑问，请与电子邮件管理员联系。

标记主题行示例：



警告：不要将电子邮件作为提交文件“转发”。此操作不会保留邮件路由报头的顺序，并会删除对邮件来源进行属性所必需的邮件路由报头。相反，请始终确保您通过“转发为附件”选项发送有问题的电子邮件。

您可以直接从以下位置提交电子邮件：

- Microsoft Outlook
- Microsoft Outlook Web App、Microsoft Office 365
- Microsoft Outlook 2011和Microsoft Outlook 2016 for Mac(OS X、macOS)
- 邮件(OS X、macOS)
- Mozilla Thunderbird
- 移动平台 (iPhone、Android或其他)

Microsoft Outlook

- Microsoft Outlook的首选提交方法是使用思科安全邮件提交插件。
- 向思科提交邮件，以获取未经请求和不需要的电子邮件，如垃圾邮件、病毒和网络钓鱼。
- “非垃圾邮件”按钮可以快速对标记为垃圾邮件的合法邮件重新分类。

注意：如果您不能或不想安装思科邮件安全插件，请按照下一说明操作。

Microsoft Outlook Web App、Microsoft Office 365

1. 在Microsoft Outlook Web App中打开您的邮箱。
2. 选择要提交的邮件。
3. 单击左上角的“新邮件”。
4. 将邮件拖放到新邮件的附件中。
5. 将电子邮件发送到本文档中提供的相应地址。

Microsoft Outlook 2011和Microsoft Outlook 2016 for Mac(OS X、macOS)

1. 在消息窗格中选择消息。
2. 单击“附件”按钮。
3. 将邮件转发到本文档中提供的相应地址。

邮件(OS X、macOS)

1. 请右键单击电子邮件本身，然后选择“转发为附件”。
2. 将电子邮件转发到本文档中提供的相应地址。

Mozilla Thunderbird

1. 右键单击电子邮件本身，然后选择“转发为”>“附件”。
2. 将电子邮件转发到本文档中提供的相应地址。

注意： [MailSentry IronPort Spam Reporter](#)是Mozilla Thunderbird的第三方插件，它采取与描述相同的操作，但提供“垃圾邮件/火腿”按钮。**MailSentry IronPort Spam Reporter不是Cisco支持的插件。**

移动平台 (iPhone、Android或其他)

- 如果您的移动平台没有将原始电子邮件作为附件转发的方法，请在您有权访问所提供的其他方法之一后提交。

如何验证向思科提交的文件

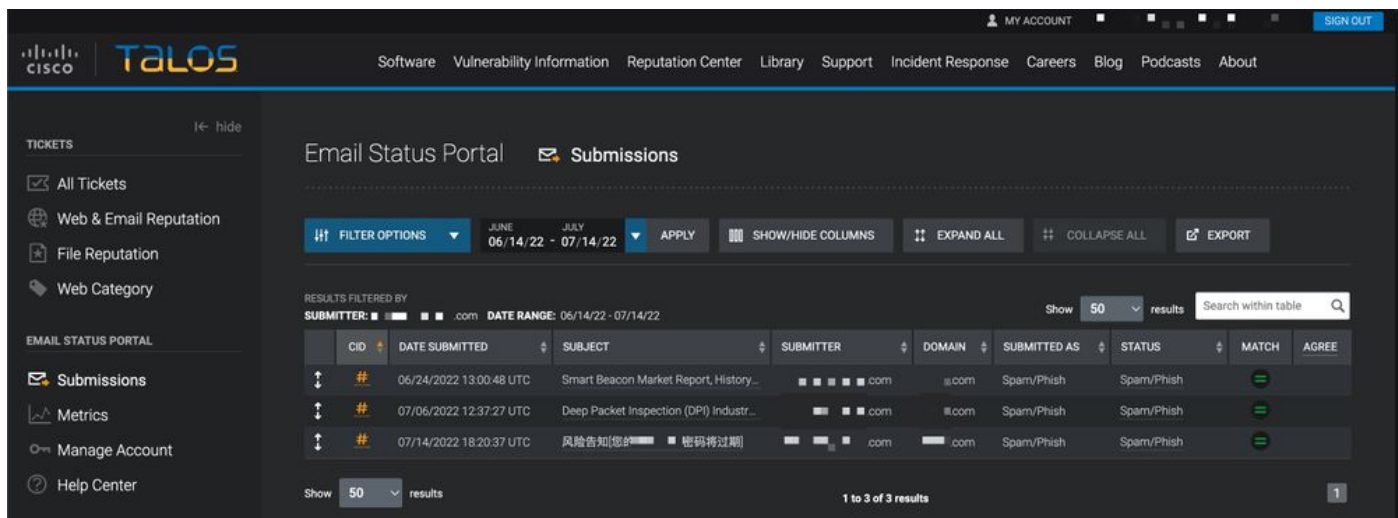
直接电邮提交

思科不提供确认电邮或电邮提交的接收通知。相反，请通过Talosintelligence.com上托管的邮件状态门户查看您的提交文件。

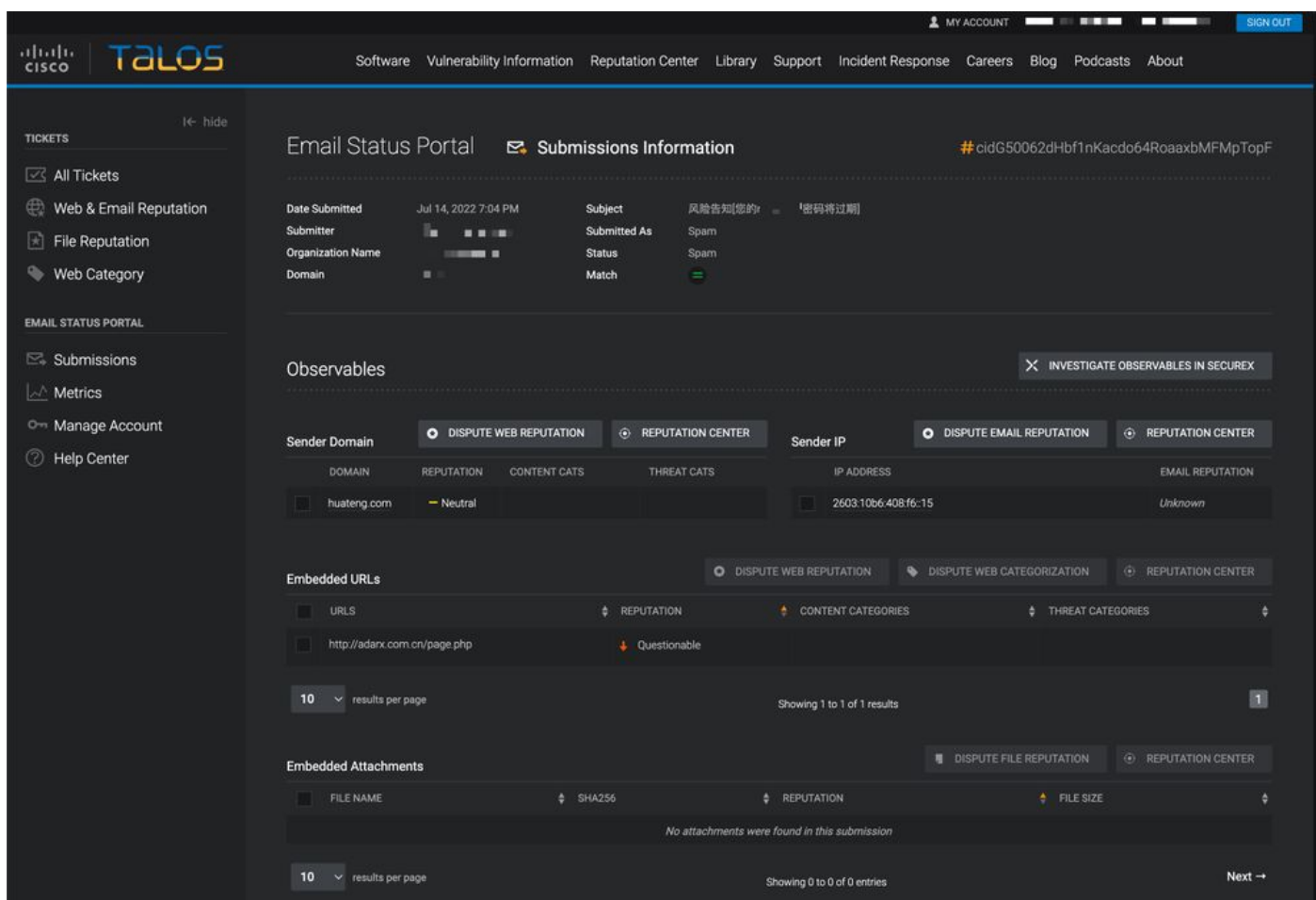
电子邮件状态门户

请从邮件状态门户验证您的提交。登录后，系统将为您提供指定日期/时间范围内所有提交文件的列表。

示例：



如果点击唯一CID“#”，您可以看到与报告的电子邮件相关的更多详细信息。



您将看到与报告的电子邮件关联的发件人域、发件人IP、嵌入的URL和嵌入的附件。您可以对争议Web信誉、**争议电子邮件信誉**和**争议文件信誉**采取进一步的操作。

每个嵌套信息行最多显示5个可观察的嵌入URL和嵌入附件。如果电子邮件提交具有更多可观察项，用户可以点击“转至电子邮件提交详细信息页面”查看提取的可观察项的完整列表。

您可以使用所需的可观察信息查看单个可观察信息的进一步信誉详细信息，然后单击“信誉中心”按钮。

您还可以通过SecureX调查多个可**观察项**。此控制面板根据您的思科产品组合将思科安全产品整套产品的信誉数据组合在一起。您可以从单个提交文件中选择最多20个可观察项，以在SecureX中同时使用“在SecureX中调查可观察项”按钮进行调查。

用户可以提交单个信誉争议（Web、电子邮件或文件），或批量应用争议，以便提交一份或多份可观察数据。URL和域也可以针对它们提交Web分类争议。

有关电子邮件状态门户的详细信息，请访问
https://talosintelligence.com/tickets/email_submissions/help

其他信息

思科安全电邮网关文档

- [版本说明](#)
- [用户指南](#)
- [CLI参考指南](#)
- [思科安全电邮网关API编程指南](#)
- [思科安全电子邮件网关中使用的开源](#)
- [思科内容安全虚拟设备安装指南（包括虚拟云网关）](#)

安全电邮云网关文档

- [版本说明](#)
- [用户指南](#)

思科安全电邮和Web Manager文档

- [版本说明和兼容性列表](#)
- [用户指南](#)
- [思科安全电邮和Web Manager的API编程指南](#)
- [思科内容安全虚拟设备安装指南](#) (包括虚拟邮件和Web Manager)

思科安全产品文档

- [思科安全产品组合命名架构](#)