



## **Cisco IronPort 邮件安全插件 7.1 管理员指南**

2010 年 12 月 6 日

**美洲总部**  
思科系统公司  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
电话: 408-526-4000  
800 553-NETS (6387)  
传真: 408-527-0883

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

Cisco 执行的 TCP 报头压缩是对加州大学伯克利分校 (UCB) 开发的程序的修改，它是 UNIX 操作系统的 UCB 公用版的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上述供应商不承诺所有明示或暗示的担保，包括（但不限于）对特定用途的适销性、适用性、非侵权性以及因交易、使用或商业惯例所衍生的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

CCDE、CCENT、CCSI、Cisco Eos、Cisco HealthPresence、Cisco IronPort、思科徽标、Cisco Nurse Connect、Cisco Pulse、Cisco SensorBase、Cisco StackPower、Cisco StadiumVision、Cisco TelePresence、Cisco Unified Computing System、Cisco WebEx、DCE、Flip Channels、Flip for Good、Flip Mino、Flipshare (Design)、Flip Ultra、Flip Video、Flip Video (Design)、Instant Broadband 和 Welcome to the Human Network 均为商标；Changing the Way We Work, Live, Play, and Learn、Cisco Capital、Cisco Capital (Design)、Cisco:Financed (Stylized)、Cisco Store、Flip Gift Card 和 One Million Acts of Green 是服务商标；Access Registrar、Aironet、AllTouch、AsyncOS、Bringing the Meeting To You、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、CCSP、CCVP、Cisco、Cisco Certified Internetwork Expert 徽标、Cisco IOS、Cisco Lumin、Cisco Nexus、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems 徽标、Cisco Unity、Collaboration Without Limitation、Continuum、EtherFast、EtherSwitch、Event Center、Explorer、Follow Me Browsing、GainMaker、iLYNX、IOS、iPhone、IronPort、IronPort 徽标、Laser Link、LightStream、Linksys、MeetingPlace、MeetingPlace Chime Sound、MGX、Networkers、Networking Academy、PCNow、PIX、PowerKEY、PowerPanels、PowerTV、PowerTV (Design)、PowerVu、Prisma、ProConnect、ROSA、SenderBase、SMARTnet、Spectrum Expert、StackWise、WebEx 和 WebEx 徽标均为思科系统公司和/或其附属公司在美国和其他特定国家/地区的注册商标。

本文档或网站中提及的所有其他商标均属于其各自所有者。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(0910R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

*Cisco IronPort 邮件安全插件 7.1 管理员指南*

© 2010 年思科系统公司。保留所有权利。



## 目录

<b>Cisco IronPort 邮件安全插件使用入门</b>	<b>1-1</b>
本版本中的新增内容	1-1
支持的配置	1-2
相关文档	1-2
如何使用本指南	1-3
本指南组织方式	1-3
排版规则	1-4
哪里可以获得详细信息	1-4
Cisco IronPort 欢迎您的评论	1-6
Cisco IronPort 邮件安全插件概述	1-7
<b>概述</b>	<b>2-9</b>
Cisco IronPort 邮件安全插件	2-9
安装此插件	2-10
配置 Cisco IronPort 邮件安全插件设置	2-11
<b>执行批量安装</b>	<b>3-13</b>
概述	3-13
创建响应文件	3-14
使用 SCCM 执行批量安装	3-15
更改插件配置文件	3-29
<b>配置和使用适用于 Outlook 的 Cisco IronPort 邮件安全插件</b>	<b>4-31</b>
适用于 Outlook 的 Cisco IronPort 邮件安全插件常规设置	4-32
启用/禁用	4-32

配置 Outlook 插件的基本设置	4-33
报告插件	4-35
使用适用于 Outlook 的报告插件	4-37
加密插件	4-39
选项	4-40
发送加密邮件	4-41
更改日志记录设置	4-42
使用诊断工具进行故障排除	4-43
Cisco IronPort 邮件安全诊断工具收集的数据	4-43
运行 Cisco IronPort 邮件安全诊断工具	4-44
卸载 Cisco IronPort 邮件安全插件	4-46
<b>配置和使用适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件</b>	<b>5-47</b>
适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件常规设置	5-47
报告插件	5-49
使用适用于 Lotus Notes 的报告插件	5-50
加密插件	5-51
配置加密选项	5-51
选项	5-51
使用加密插件	5-52
更改日志记录选项	5-54
故障排除和诊断	5-55
常见启动错误	5-55
思科邮件安全诊断工具	5-57
卸载	5-59
<b>IronPort 最终用户许可协议</b>	<b>A-61</b>
Cisco IronPort 系统有限责任公司软件许可协议	A-61



# 第 1 章

## Cisco IronPort 邮件安全插件使用入门

---

本章包含以下部分：

- [本版本中的新增内容](#)（第 1-1 页）
- [支持的配置](#)（第 1-2 页）
- [如何使用本指南](#)（第 1-3 页）
- [Cisco IronPort 邮件安全插件概述](#)（第 1-7 页）

### 本版本中的新增内容

本版本结合两种常用邮件安全插件 - 思科加密插件（允许用户对来自其邮件程序的邮件进行加密）和思科报告插件（允许用户报告垃圾邮件、病毒或错误分类的邮件）。通过结合这些插件，思科不仅使用户可以更轻松地访问和修改邮件安全插件，而且还简化了邮件安全插件的安装和更新过程。此外，Cisco IronPort 邮件安全插件还根据 Windows Installer 提供标准安装程序。该安装程序支持标准 Windows Installer 命令行选项，包括无提示安装响应文件。

## 支持的配置

支持下列配置：

Cisco IronPort 邮件安全插件 7.1.x	Outlook 2003	Outlook 2007	Outlook 2010	Notes 6.x	Notes 7.x	Notes 8.0.x	Notes 8.5.x
XP 32 位	通过认证	通过认证	通过认证	通过认证	通过认证	通过认证	通过认证
XP 64 位	兼容	兼容	兼容	兼容	兼容	兼容	兼容
Vista 32 位	通过认证	通过认证	通过认证	兼容	兼容	兼容	通过认证
Vista 64 位	兼容	通过认证	通过认证	兼容	兼容	通过认证	兼容
Win 7 32 位	通过认证	通过认证	通过认证	兼容	兼容	通过认证	通过认证
Win 7 64 位	兼容	通过认证	通过认证	兼容	兼容	兼容	通过认证
Citrix	不支持	不支持	不支持	不支持	不支持	不支持	不支持



备注

Cisco IronPort 邮件安全插件要求使用 Windows Installer 2.0 或更高版本。

## 相关文档

要使用加密插件，您需要运行 Cisco IronPort 加密设备并且将其正确配置为可与加密插件协同工作。要了解如何配置 Cisco IronPort 加密设备，您可以查看以下指南：

- *IronPort AsyncOS for Email Encryption 用户指南*。本指南提供配置邮件加密的说明，它还可以帮助您了解如何将您的加密设备设置配置为与您配置的插件设置协同工作。

要更好地了解 Cisco IronPort 邮件安全的工作方式，您可以查看有关邮件如何归类为垃圾邮件、病毒或非垃圾邮件方面的基本信息。有关这些主题的详情，您可以查看以下指南：

- *Cisco IronPort AsyncOS for Email 配置指南*。本指南包含垃圾邮件和病毒防护方面的信息。用户可以通过使用垃圾邮件和病毒插件提高 SenderBase 网络的效率。用户将邮件标记为“垃圾邮件”、“病毒”或“非垃圾邮件”时，他们可以使过滤器变得更高效并提升所有 Cisco IronPort 设备的性能。

# 如何使用本指南

将本指南作为了解有关 Cisco IronPort 邮件安全插件功能的资源进行使用。本指南的主题按照逻辑顺序组织，但是您可能无需阅读每个章节。查看目录和名为[本指南组织方式](#)（第 1-3 页）的部分以确定与您的具体配置相关的章节。

本指南以 PDF 电子版的形式发放。您可从 Cisco IronPort 客户支持门户上获取本指南的电子版。您也可以通过单击“帮助 (Help)”按钮访问设备 GUI 中的 HTML 在线帮助工具。

## 本指南组织方式

[第 1 章，“Cisco IronPort 邮件安全插件使用入门”](#) 提供了 IronPort 安全插件简介并阐明了它在网络安全配置中的重要功能和角色。本指南对当前版本的新功能与针对信息和支持联系信息的其他资源相关信息一同进行了描述。

[第 2 章，“概述”](#) 介绍了报告插件和加密插件。本部分提供了各个工具的概述。

[第 3 章，“执行批量安装”](#) 说明如何进行批量安装。该说明提供了创建响应文件、运行安装和安装之前可能修改的文件的步骤。

[第 4 章，“配置和使用适用于 Outlook 的 Cisco IronPort 邮件安全插件”](#) 提供有关配置适用于 Outlook 的 Cisco IronPort 邮件安全插件的说明。其中包括配置报告插件和加密插件的步骤。

[第 5 章，“配置和使用适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件”](#) 提供有关配置适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件的说明。其中包括配置报告插件和加密插件的步骤，以及使用 Lotus Notes 邮件程序插件的说明。

[附录 A，“Cisco IronPort 系统有限责任公司软件许可协议”](#) 包含有关 Cisco IronPort 产品许可协议的详细信息。

## 排版规则

字体	含义	示例
<b>AaBbCc123</b>	命令、文件和目录的名称；屏幕上的计算机输出。	请为此侦听器选择一个 IP 接口。  sethostname 命令设置 IronPort 设备的名称。
<b>AaBbCc123</b>	用户输入与屏幕上的计算机输出对应。	mail3.example.com> <b>commit</b> 请输入一些对您所作更改的描述： [ ]> <b>已更改系统主机名称</b>
<i>AaBbCc123</i>	书名、新术语、强调的单词以及命令行变量；对于命令行变量，斜体文本是实际名称或值的占位符。	请参阅 <i>IronPort 快速入门指南</i> 。  IronPort 设备 <b>必须</b> 能够独占选择一个接口来发送出站数据包。  开始之前，请将您的密码重置为一个新值。 旧密码： <b>ironport</b> 新密码： <i>您的新密码</i> 重新输入新密码： <b>您的新密码</b>

## 哪里可以获得详细信息

IronPort 提供以下资源用于了解 Cisco IronPort 邮件安全插件的更多信息。

### IronPort 技术培训

Cisco IronPort 系统技术培训服务可以帮您获得成功评估、集成、部署、维护和支持 Cisco IronPort 安全产品和解决方案的知识与技能。

使用以下方法之一联系 Cisco IronPort 技术培训服务：

培训。有关注册和常规培训的问题：

- <http://training.ironport.com>
- [training@ironport.com](mailto:training@ironport.com)



认证。有关证书和认证考试的问题：

- <http://training.ironport.com/certification.html>
- [certification@ironport.com](mailto:certification@ironport.com)

## 知识库

您可以在 Cisco IronPort 客户支持站点访问 Cisco IronPort 知识库，URL 如下：

<http://www.cisco.com/web/ironport/knowledgebase.html>



### 备注

您需要一个 Cisco.com 用户 ID 来访问该网站。如果您没有 Cisco.com 用户 ID，您可以点击以下链接进行注册：

<https://tools.cisco.com/RPF/register/register.do>

该知识库包含大量与 Cisco IronPort 产品相关的主题信息。

文章大致归为以下几类：

- **如何使用。** 这些文章介绍如何使用 Cisco IronPort 产品。例如，一篇如何使用文章可能会介绍备份并恢复某个设备数据库的步骤。
- **问题与解决方案。** 问题与解决方案文章可以处理您在使用 Cisco IronPort 产品时遇到的具体错误或问题。例如，一篇问题与解决方案文章可能介绍升级至新版本产品显示某具体错误消息时该怎么做。
- **参考。** 参考文章通常会提供信息列表，例如与特定硬件相关的错误代码。
- **故障排除。** 故障排除文章介绍如何分析并解决与 Cisco IronPort 产品相关的常见问题。例如，一篇故障排除文章可能提供 DNS 遇到问题时应遵循的步骤。

## 思科支持社区

思科支持社区是一个面向 Cisco 客户、合作伙伴和员工的在线论坛。它提供了一个讨论常规邮件和网络安全问题以及有关具体思科产品的技术信息的场合。您可以在论坛中发布主题咨询并与其他 Cisco 和 Cisco IronPort 用户分享信息。

您可以通过以下 URL 访问思科支持社区：

<https://supportforums.cisco.com>

## Cisco IronPort 客户支持

您可以随时通过电话、邮件或在线请求我们的支持。Cisco IronPort 客户支持服务等级协议详细信息可从支持门户上获取。

若要报告一个严重问题并且该问题需要在客户支持工作时间段外获得紧急协助，请通过以下方法之一联系 Cisco IronPort：

美国免费电话：1 (877) 646-4766

支持站点：<http://www.cisco.com/web/ironport/index.html>

如果您是通过经销商或另一个供应商购买了支持，请直接联系该供应商咨询您的产品支持问题。

## 第三方贡献者

IronPort AsyncOS 中包含的部分软件的分销遵守 FreeBSD, Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives, Inc. 和其他第三方贡献者的软件许可协议的条款、公告和条件，并且所有这些条款和条件已纳入 IronPort 许可协议。

这些协议的全文可通过以下网站查看：

[https://support.ironport.com/3rdparty/AsyncOS\\_User\\_Guide-1-1.html](https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html)。

IronPort AsyncOS 产品中的软件部分基于 RRDtool 并且得到 Tobi Oetiker 的明确书面许可。

本文档中部分相关内容的复制已取得 Dell Computer Corporation 的许可。本文档中部分相关内容的复制已取得 McAfee, Inc. 的许可。本文档中部分相关内容的复制已取得 Sophos Plc 的许可。

## Cisco IronPort 欢迎您的评论

Cisco IronPort 技术出版物团队乐于提高产品文档的质量。我们时刻欢迎您的评论和建议。您可以将评论发送至以下邮件地址：

[docfeedback@ironport.com](mailto:docfeedback@ironport.com)

# Cisco IronPort 邮件安全插件概述

Cisco IronPort 邮件安全插件在 Outlook 或 Lotus Notes 邮件程序上安装报告和加密菜单。通过报告插件，用户能够提交有关他们收到的邮件类型的反馈（例如，报告垃圾邮件、网络钓鱼和病毒邮件），加密插件会在工具栏上放入“加密邮件 (Encrypt Message)”按钮，这使得用户可以从自己的邮件程序发送加密邮件。

思科安全插件安装时会启用 Outlook 邮件客户端或 Lotus Notes 邮件客户端上的组件。这个单一接口允许最终用户无缝地从自己的邮件程序报告问题邮件或发送加密邮件。结合使用这些插件，可简化安装并提供单一接口供用户修改。

报告和加密插件提供了方便的接口，使您能够使用工具栏按钮和右键单击上下文菜单来提交反馈并发送加密邮件。如果您使用报告插件报告一封邮件，将出现一个对话框，说明该邮件已提交。加密插件会在邮件菜单栏中配置“加密邮件 (Encrypt Message)”按钮，以便发件人在将要加密和保护的邮件发送到组织外部之前，对其进行标记。加密插件的确切功能取决于有加密许可证的 Cisco IronPort 邮件安全设备的存在和合理配置。





## 第 2 章

# 概述

---

Cisco IronPort 邮件安全插件是一种支持多种 Cisco IronPort 邮件安全插件的框架，包括报告插件和加密插件。

本章包含以下部分：

- [Cisco IronPort 邮件安全插件（第 2-9 页）](#)
- [安装此插件（第 2-10 页）](#)
- [配置 Cisco IronPort 邮件安全插件设置（第 2-11 页）](#)

## Cisco IronPort 邮件安全插件

Cisco IronPort 邮件安全插件包含两个常用邮件安全插件：报告插件和加密插件。您可以在 Outlook 或 Lotus Notes 上部署思科邮件安全。部署 Cisco IronPort 邮件安全插件时，它会安装以下两个应用程序或其中一个：

- **报告插件。**报告插件使 Outlook 和 Lotus Notes 用户能够将有关未经索取或不需要的邮件（例如，垃圾邮件、病毒和网络钓鱼邮件）的反馈提交至 Cisco IronPort 系统。有关详细信息，请参阅[报告插件（第 2-10 页）](#)。
- **加密插件。**加密插件会在邮件菜单栏中放入“加密邮件 (Encrypt Message)”按钮，以便发件人在将要加密和保护的邮件发送到组织外部之前，对其进行标记。有关详细信息，请参阅[加密插件（第 2-10 页）](#)。

## 报告插件

报告插件使 Outlook 和 Lotus Notes 用户能够将有关未经索取或不需要的邮件（例如，垃圾邮件、病毒和网络钓鱼邮件）的反馈提交至 Cisco IronPort 系统。Cisco IronPort 系统使用此反馈更新其过滤器，从而阻止不需要的邮件发送至您的收件箱。

您也可以使用“**非垃圾邮件 (Not Spam)**”按钮将错误分类邮件（即正当的邮件被标记为垃圾邮件）报告至 Cisco IronPort 系统。Cisco IronPort 系统使用这些报告调整其垃圾邮件过滤器以提高效率。

此插件提供了便捷接口，使您能够使用工具栏按钮和右键单击上下文菜单来提交反馈。报告邮件时，将出现一个对话框，显示说明该邮件已提交。自动化系统会利用您提交的邮件数据改善 Cisco IronPort 过滤器。提交邮件数据有助于减少收件箱中未经索取的邮件的数量。

## 加密插件

加密插件会在邮件菜单栏中配置“**加密邮件 (Encrypt Message)**”按钮，以便发件人在将要加密和保护的邮件发送到组织外部之前，对其进行标记。加密插件旨在与正常运行且配置好的 Cisco IronPort 加密装置以及 Cisco IronPort 邮件安全设备（如果您的网络中有该设备）协同工作。加密插件使用的配置应与这些设备的设置相结合。如果这些设备使用的配置不同，发送加密邮件时可能会出现问題。

## 安装此插件

要针对多组用户安装 Cisco IronPort 邮件安全插件，您可能希望执行无提示安装。无提示安装允许您在不提示最终用户进行输入的情况下执行安装。要执行 Cisco IronPort 邮件安全插件的无提示安装，您需要创建一个响应文件（包含安装过程中遇到的所有问题答案的文本文件）。然后，您将使用该响应文件通过系统管理软件（例如 Systems Management Server (SMS) 或 System Center Configuration Manager (SCCM)）运行安装。有关执行无提示安装的说明，请参阅第 3 章，“[执行批量安装](#)”。

## 配置 Cisco IronPort 邮件安全插件设置

安装 Cisco IronPort 邮件安全插件之后，您可以从 Outlook 中的“工具 (Tools)” > “选项 (Options)” > “思科邮件安全 (Cisco Email Security)” 菜单以及 Lotus Notes 中的“操作 (Actions)” > “思科邮件安全 (Cisco Email Security)” 菜单进行配置更改。

您可以更改报告插件或加密插件的安装；或者更改影响两个插件安装的常规选项。例如，您希望加密和报告插件均启用日志记录，或者希望更改标记邮件以供加密的方式（这些设置必须与您的 Cisco IronPort 加密设备兼容）。

要更改 Outlook 安装的配置，请参阅第 4 章，“配置和使用适用于 Outlook 的 Cisco IronPort 邮件安全插件”。

要更改 Lotus Notes 安装的配置，请参阅第 5 章，“配置和使用适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件”。







## 第 3 章

# 执行批量安装

本章介绍如何在多台台式机上执行批量安装。本章包含以下部分：

- [概述（第 3-13 页）](#)
- [创建响应文件（第 3-14 页）](#)
- [使用 SCCM 执行批量安装（第 3-15 页）](#)
- [更改插件配置文件（第 3-29 页）](#)

## 概述

要为多组用户安装 Cisco IronPort 邮件安全插件，您需要执行本地无提示安装以生成要在安装过程中使用的响应文件，从而做好安装准备。无提示安装允许您在不提示最终用户进行输入的情况下执行安装。要执行 Cisco IronPort 邮件安全插件批量安装，您需要创建一个响应文件（包含安装过程中遇到的所有问题答案的文本文件）。然后，您将使用该响应文件通过系统管理软件（例如 Systems Management Server (SMS) 或 System Center Configuration Manager (SCCM)）运行安装。

执行批量安装的基本步骤包括：

1. 卸载安全插件包含的所有旧版本插件（包括适用于 Outlook 的桌面加密插件、适用于 Outlook 的桌面 Flag 插件、适用于 Outlook 的 IronPort 插件、适用于 Lotus Notes 的 IronPort 插件）。或者卸载 Cisco IronPort 邮件安全插件的当前运行版本。
2. 在安装之前请关闭 Outlook 或 Lotus Notes。
3. 运行本地版本的安装以创建响应文件，并验证响应文件是否已正确创建。请参阅[创建响应文件（第 3-14 页）](#)。

4. 创建响应文件后，卸载您在本地机器上安装的 Cisco IronPort 邮件安全插件。您将在下一步中重新安装此插件以测试响应文件。
5. 使用创建的响应文件在本地计算机上运行安装。验证程序是否已在 Outlook 或 Lotus Notes 中正确安装。
6. 验证安装之后，使用 System Center Configuration Manager (SCCM) 等系统管理软件在目标计算机上运行批量安装。要使用 SCCM 执行安装，请参阅[使用 SCCM 执行批量安装](#)（第 3-15 页）。

## 创建响应文件

要创建响应文件，您需要通过将响应记录到文件中的特殊选项运行插件安装。创建带有记录答案的响应文件之后，您可在安装过程中将其用于自动响应要安装 Cisco IronPort 邮件安全插件的所有计算机的安装序列问题。

- 步骤 1** 要创建响应文件，请从带有 **/r** 密钥选项的命令行执行安装。**/r** 密钥选项将指示 InstallShield，将结果记录到响应文件中。在默认情况下，InstallShield 使用以下名称和位置保存响应文件：

c:\windows\setup.iss。

- 步骤 2** 要为响应文件指定位置，请使用 **/f1** 选项。使用 **/f1** 选项可以指定备用响应文件名和路径。例如，从命令行运行以下命令可指示 InstallShield 将响应写入 C 盘上的 *install\_034.iss* 文件中：

```
C:\Users\user\\Desktop\CiscoEmailSecurity.7.1.0.34.exe /r
/f1"C:\install_034.iss "
```

其中 *C:\Users\user\Desktop\CiscoEmailSecurity.7.1.0.34.exe* 是 .exe 文件的路径。

确保密钥与密钥之间留有空格（在斜线之前）：*/s /v /qn /f1*

.exe 文件名和 .iss 文件名是示例文件名。如果您的 .exe 文件名与上面列出的文件名不同，安装性能也不会受到影响。

执行每个安装步骤时，会将您的响应保存至响应文件，此文件作为批量安装过程中的响应使用。

**提示**

如果使用 **/f1** 选项更改路径和文件名称，则 Cisco IronPort 建议您输入绝对路径。此外，如果在创建响应文件时使用 **/f1** 选项，请注意您需要在运行无提示安装（使用 **/s** 选项）时指定响应文件的路径。

**步骤 3** 验证 *install\_file.iss* 文件是否已创建。

**步骤 4** 验证 *install\_file.iss* 文件已创建之后，卸载插件（不使用任何命令行参数和密钥）。

**步骤 5** 通过在本地计算机上运行安装程序测试响应文件。为此，请从命令行运行以下命令：

```
C:\Users\user1\Desktop\CiscoEmailSecurity.7.1.0.34.exe /s /v /qn
/f1"C:\install_034.iss"
```

其中 **/s** - 可使 *setup.exe* 无提示，

**/v** - 可将参数传递到 MSI 数据包，

**/qn** - 可使除 *setup.exe* 以外的所有项无提示，

**/f1** - 可使程序使用位于此位置的响应文件。

**步骤 6** 打开邮件程序（Outlook 或 Lotus Notes），并验证 Cisco IronPort 邮件安全插件是否已正确安装。

**注意**

创建 *install\_file.iss* 文件之后，在更新 Cisco IronPort 邮件安全插件时也可使用该文件。

## 使用 SCCM 执行批量安装

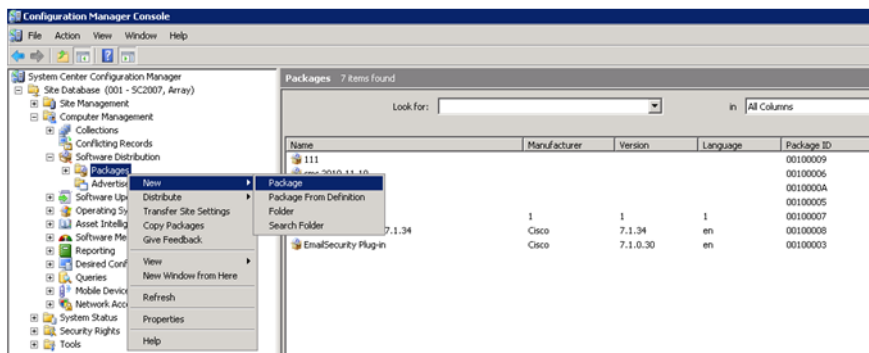
开始之前，请确保已在要安装 Cisco IronPort 邮件安全插件的客户端计算机上完成以下步骤：

- 在客户端计算机上安装 .Net 3.5（如果需要，安装进程将会下载并安装缺失的软件框架，但如果预先安装了 .Net 3.5，此安装过程将会运行得更快）。
- 关闭 Outlook 或 Lotus Notes。

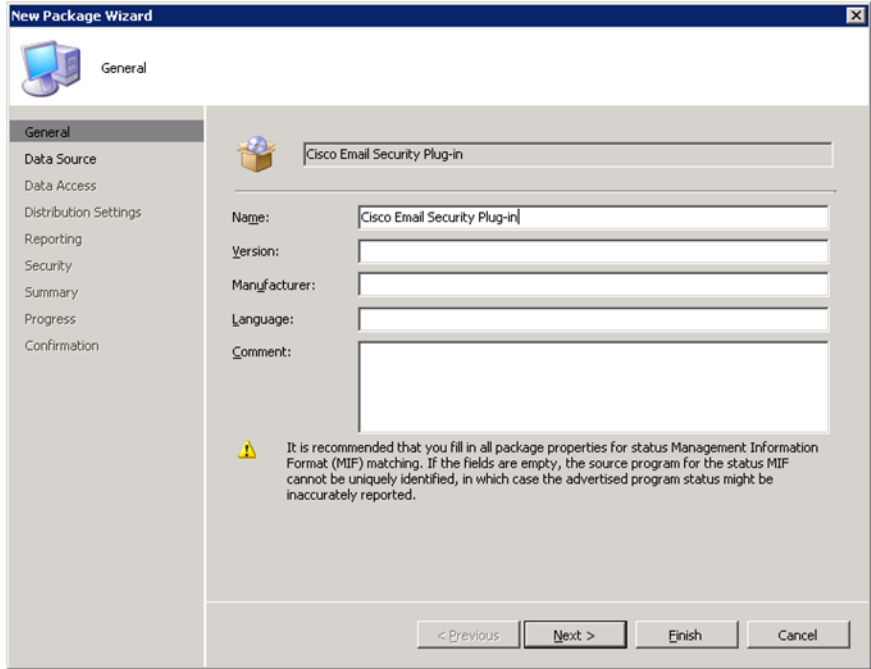
- 卸载当前版本的 Cisco IronPort 邮件安全插件（如已安装）。
  - 卸载安全插件包含的所有旧版本插件（包括适用于 Outlook 的桌面加密插件、适用于 Outlook 的桌面 Flag 插件、适用于 Outlook 的 IronPort 插件、适用于 Lotus Notes 的 IronPort 插件）。
  - 确保已创建 *install\_file.iss* 文件。请参阅[创建响应文件](#)（第 3-14 页）。
- 开始安装之前，请确保 SCCM 满足以下条件：
- 创建了应安装 Cisco IronPort 邮件安全插件的客户端列表集合。

## 要执行安装，请按照下列步骤操作：

- 步骤 1** 创建网络共享文件夹并为其指定用户访问权限。
- 步骤 2** 将安装程序和 *install\_file.iss* 文件放入该文件夹。
- 步骤 3** 打开 SCCM 管理工具。
- 步骤 4** 创建新的软件分发包。



**步骤 5** 为此包输入名称，然后点击“下一步 (Next)”。



The screenshot shows the 'New Package Wizard' dialog box with the 'General' tab selected. The 'Name' field contains the text 'Cisco Email Security Plug-in'. The 'Version', 'Manufacturer', and 'Language' fields are empty. A warning message is displayed at the bottom of the dialog box.

**General**

Data Source: Cisco Email Security Plug-in


Name: Cisco Email Security Plug-in

Version:

Manufacturer:

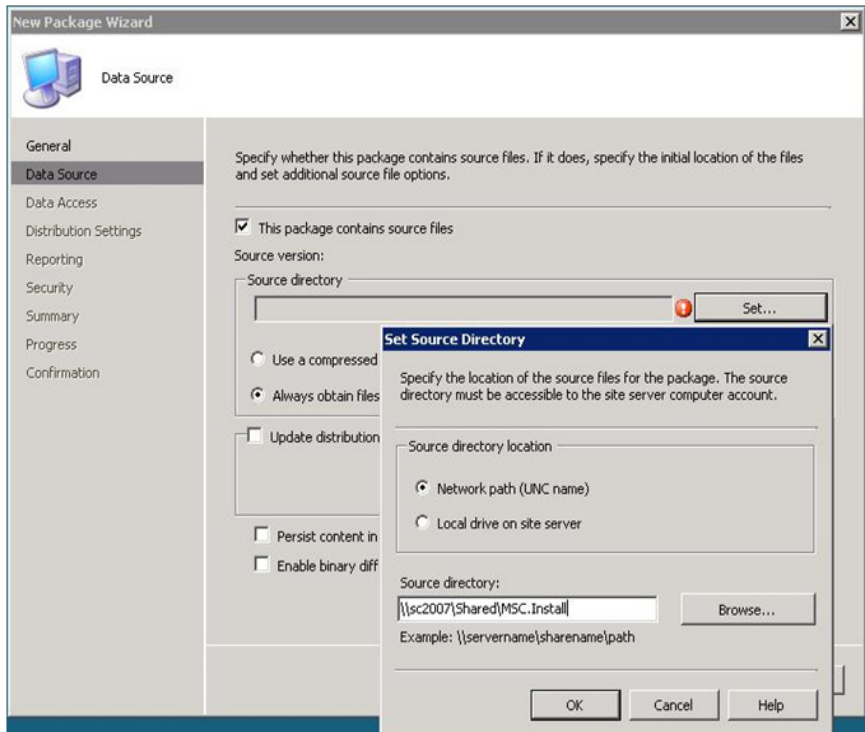
Language:

Comment:

 It is recommended that you fill in all package properties for status Management Information Format (MIF) matching. If the fields are empty, the source program for the status MIF cannot be uniquely identified, in which case the advertised program status might be inaccurately reported.

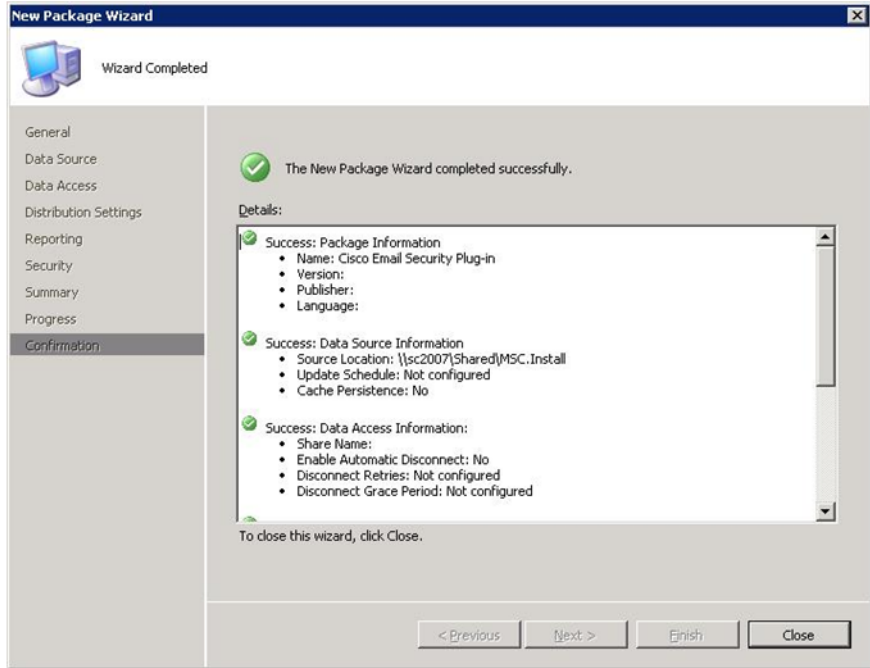
< Previous   Next >   Finish   Cancel

**步骤 6** 输入指向网络共享文件夹的路径，以指定在**步骤 1**中创建的网络源目录。您可以输入路径或浏览该文件夹。点击“**下一步 (Next)**”。

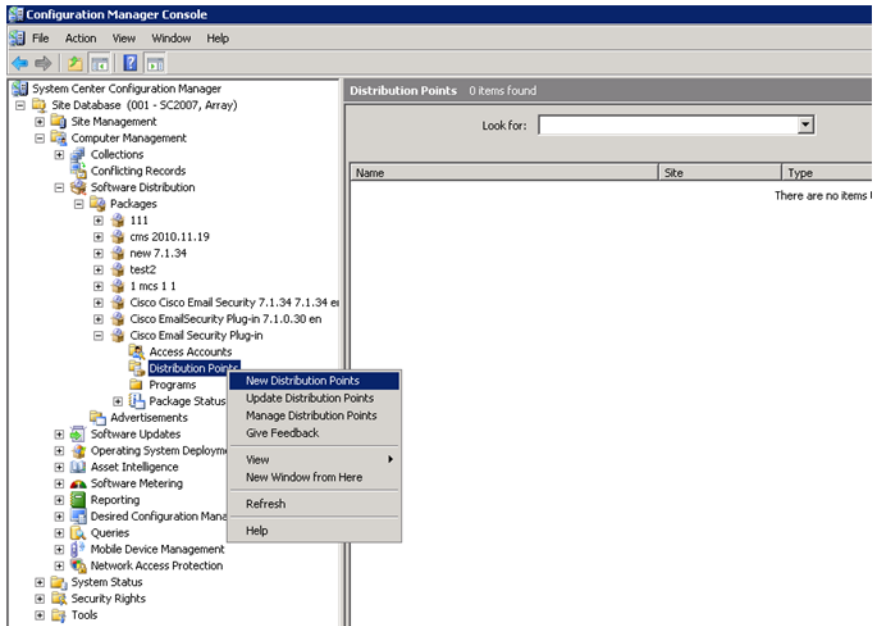


**步骤 7** 继续执行新建包向导中的下一步，并点击“**下一步 (Next)**”。

**步骤 8** 查看新建包向导已成功完成确认消息，然后点击“关闭 (Close)”。

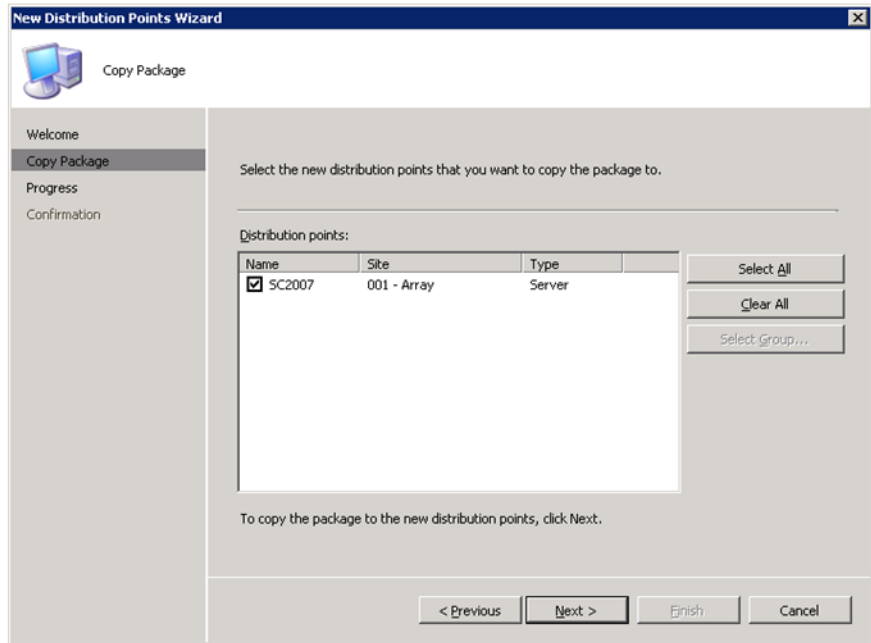


**步骤 9** 创建新的分发点，然后单击欢迎页面上的“下一步 (Next)”。

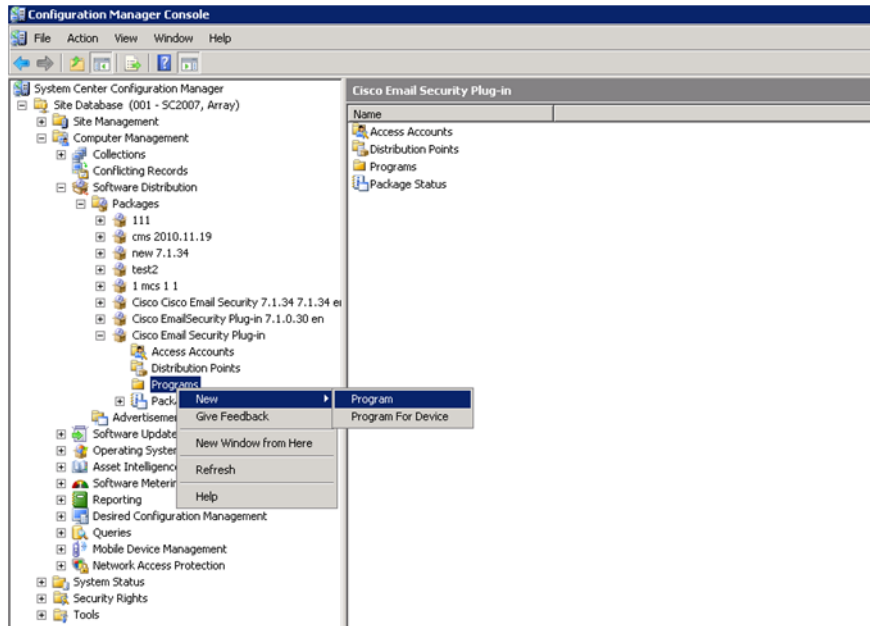




**步骤 10** 选择新的分发点。点击浏览新分发点向导上的后续页，然后点击“关闭(Close)”。



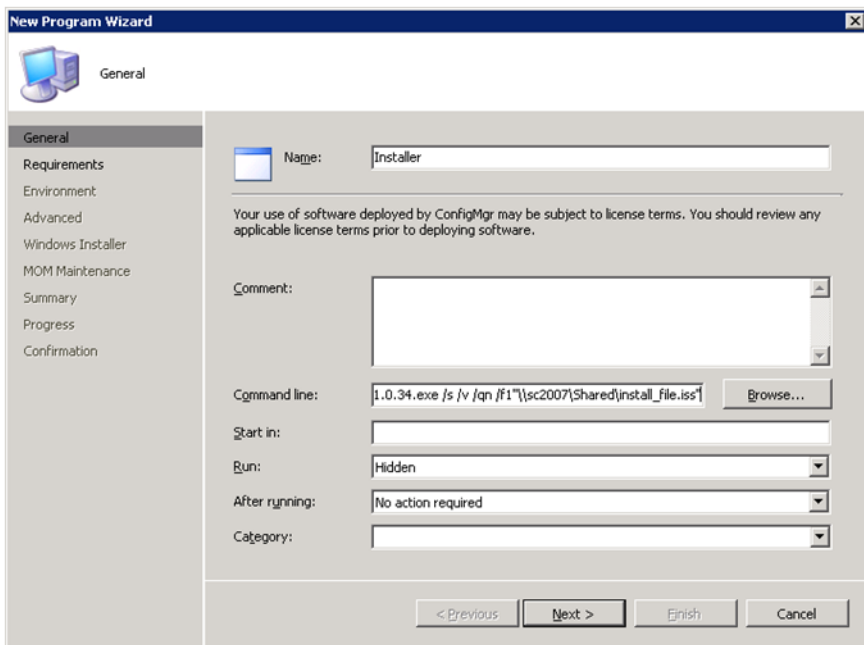
## 步骤 11 创建新程序。



**步骤 12** 在命令行输入程序名称和以下命令：

```
\sc2007\Shared\CiscoEmailSecurity.7.1.0.34.exe /s /v /qn
/f1 "\sc2007\Shared\install_file.iss"
```

其中 `\sc2007\Shared\CiscoEmailSecurity.7.1.0.34.exe` 是网络共享文件夹 `"\sc2007\Shared\install_file.iss"` 中 `.exe` 文件的完整网络路径。



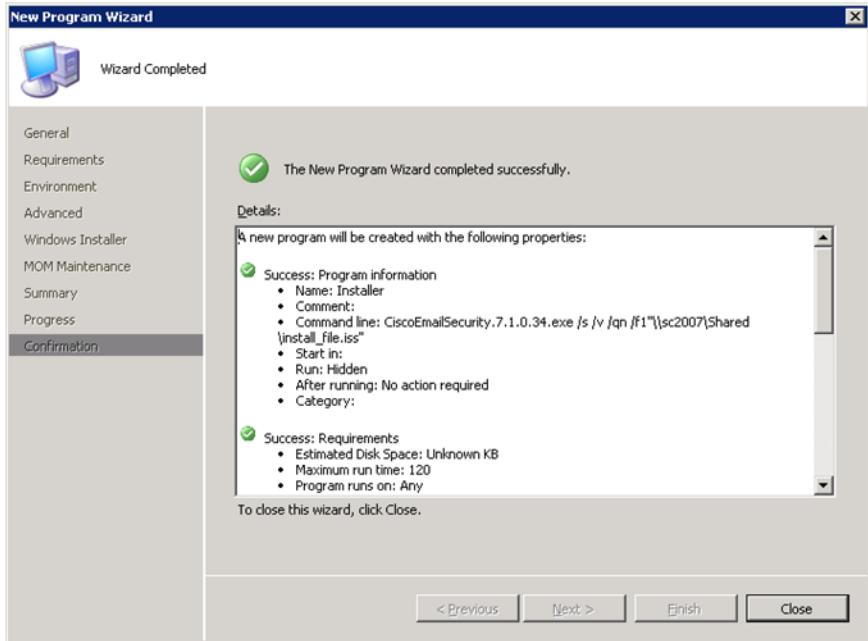
**步骤 13** 在“运行 (Run)”字段中输入“隐藏 (Hidden)”，然后点击“下一步 (Next)”。

**步骤 14** 点击浏览要求页面，然后点击“下一步 (Next)”。

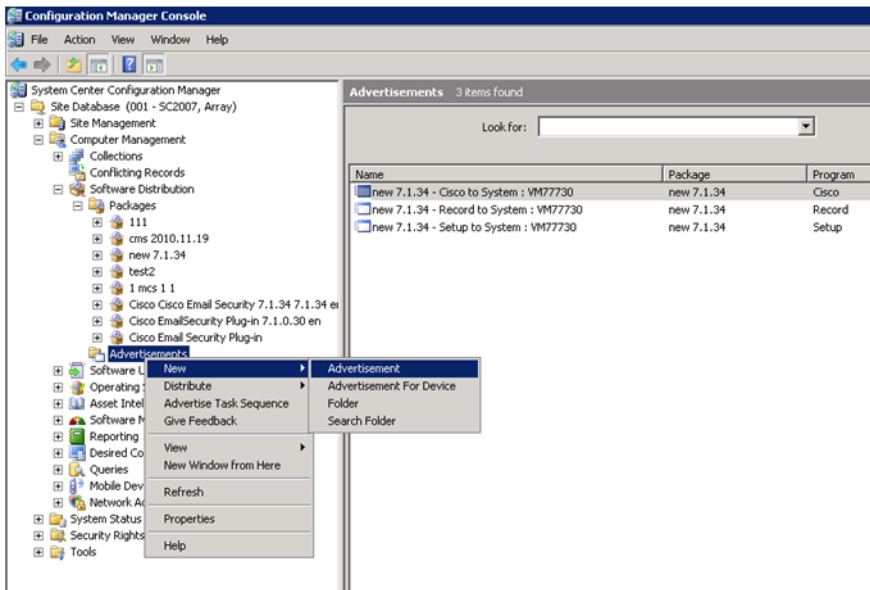
**步骤 15** 选择以下环境选项：

- **程序可运行：**仅限于用户登录时。
- **运行模式：**使用用户权限运行，如果用户没有足够的权限安装新软件，则使用管理权限运行。

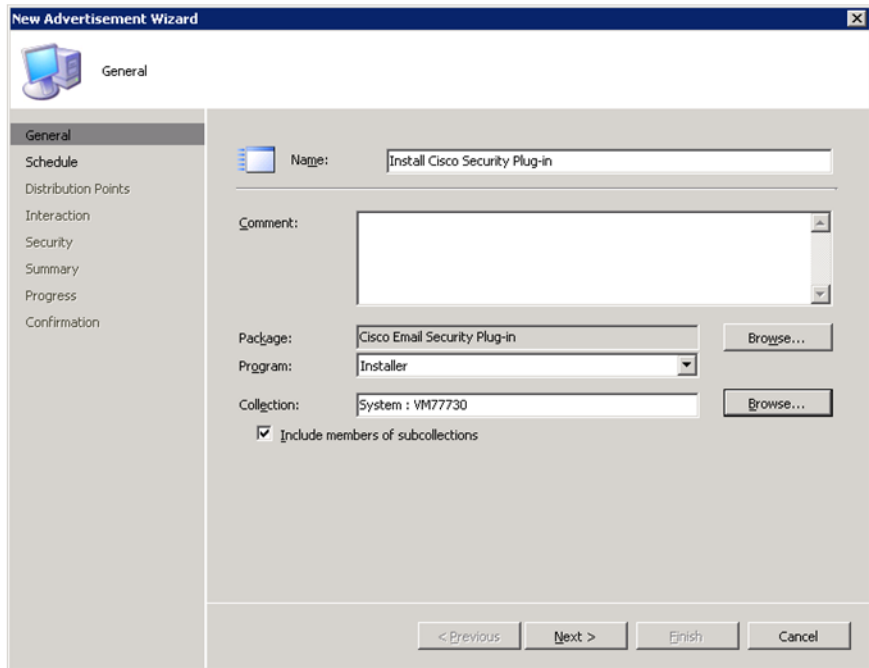
**步骤 16** 确认新程序向导已成功完成，然后点击“关闭 (Close)”。



## 步骤 17 创建新通告。



**步骤 18** 输入名称，选择已创建的数据包和程序。选择含有您希望安装插件的客户端组集合。点击“**下一步 (Next)**”。

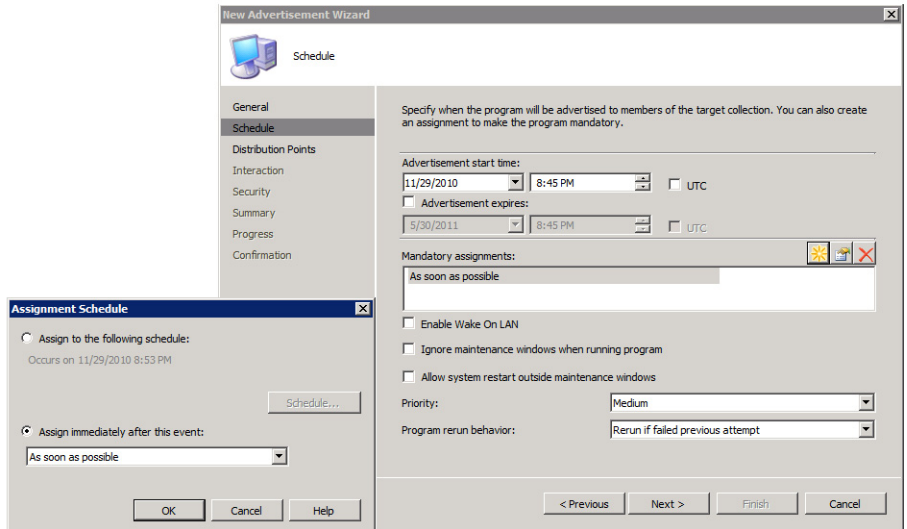


The screenshot shows the 'New Advertisement Wizard' dialog box with the 'General' tab selected. The dialog has a sidebar on the left with the following options: General, Schedule, Distribution Points, Interaction, Security, Summary, Progress, and Confirmation. The main area contains the following fields and controls:

- Name:** A text box containing 'Install Cisco Security Plug-in'.
- Comment:** A large empty text area.
- Package:** A dropdown menu showing 'Cisco Email Security Plug-in' with a 'Browse...' button to its right.
- Program:** A dropdown menu showing 'Installer'.
- Collection:** A text box containing 'System : VM77730' with a 'Browse...' button to its right.
- Include members of subcollections**

At the bottom of the dialog, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

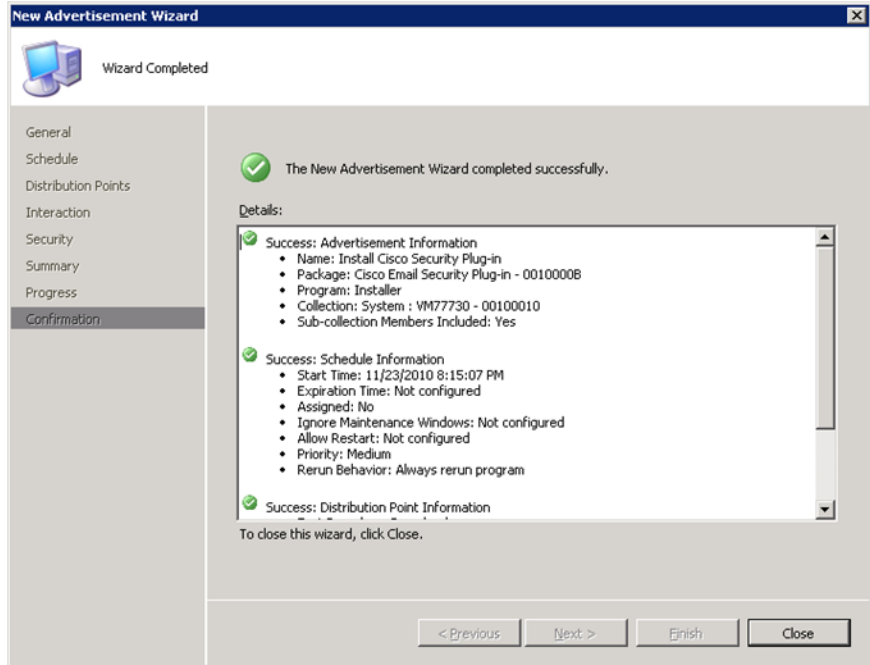
**步骤 19** 设置强制分配。点击“**下一步 (Next)**”。



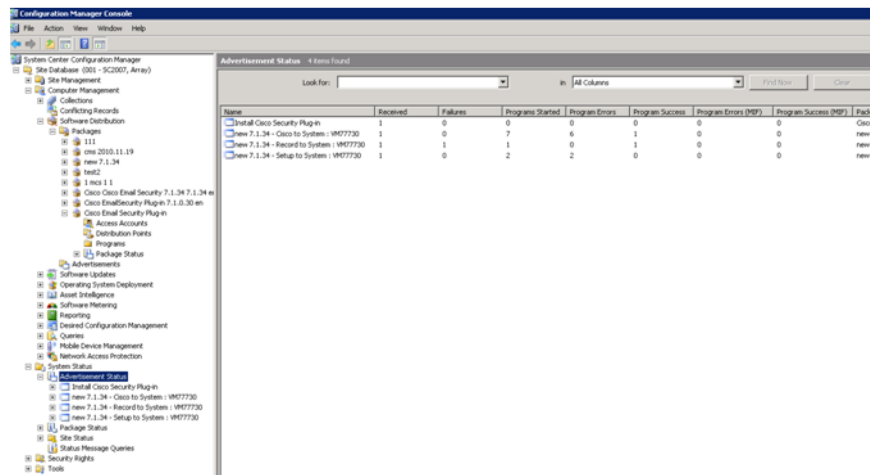
**步骤 20** 根据您的偏好选择选项，但不要选择“**不运行程序 (Do Not Run Program)**”，因为如果连接速度慢，程序将不会启动。点击“**下一步 (Next)**”。

**步骤 21** 点击浏览新通告向导，然后点击“**下一步 (Next)**”。

**步骤 22** 查看新通告向导已成功完成确认消息，然后单击“关闭 (Close)”。

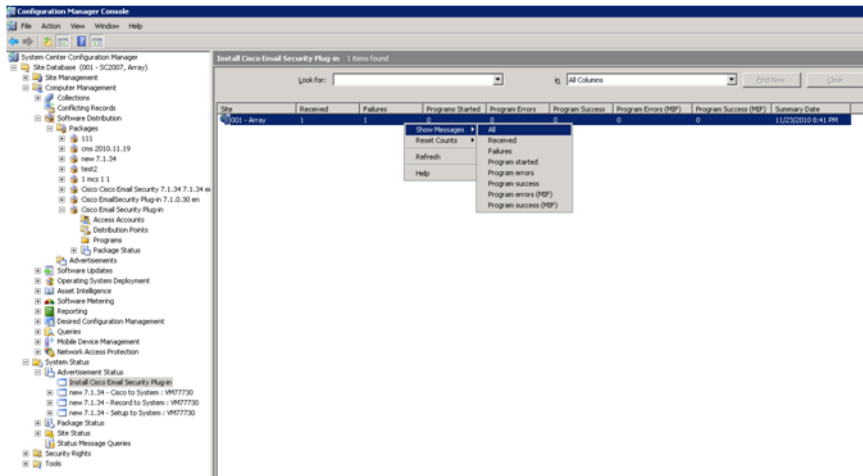


**步骤 23** 在通告状态窗口查看通告状态。





**步骤 24** 您可以通过从上下文菜单选择“显示消息 (Show message)” > “全部 (All)”创建通告报告，以查看详细信息。如果出现错误，您可以核查该报告以了解出现错误的位置。



## 更改插件配置文件

安装 Cisco IronPort 邮件安全插件时，系统会创建配置数据并将其保存在以下 XML 文件中：

- **CommonConfig.xml**。包含报告插件和加密插件共有的基础配置数据，例如日志记录信息。
- **Reporting.xml**。包含与报告插件相关的配置数据，例如可报告的邮件大小最大值。
- **Encryption.xml**。包含与加密插件相关的配置数据，例如标记方法（例如主题字符串或 x 标头）。

Cisco IronPort 邮件安全插件安装程序允许您更改默认配置文件。您可能希望使用不同的配置文件来更改安装的基础功能。例如，在加密配置文件中，您可能会更改文件标记方法（仅在能够更改加密设备上的该方法的情况下进行此更改）。在报告配置文件中，您可能更改部分默认选项，如报告邮件大小最大值或者是否在文件报告后保留文件副本。并且在主配置文件中，您可以启用或禁用日志记录或修改日志记录级别。

如果您希望使用自定义配置文件，则需要使用以下语法从命令行添加一个特殊密钥：

```
CiscoEmailSecurity-7.0.0.005.exe /s  
/v"UseCustomConfigs="\smsarray\SMSClient\config\" /qn  
/f1CiscoEmailSecurity.7.0.0.005.iss"
```

**UseCustomConfigs** 命令行参数可用于使用自定义配置文件和指定指向含有安装期间应使用的配置文件的文件夹的路径。

在默认情况下，插件将配置文件安装在以下 Outlook 和 Lotus Notes 位置的 %appdata% 目录中：

```
%appdata%\Cisco\Cisco IronPort Email Security Plug In\Outlook\  
%appdata%\Cisco\Cisco IronPort Email Security Plug In\LotusNotes\  

```

使用 **UseCustomConfigs** 命令行参数，您可以指定您自己的安装配置文件的名称和位置。但必须保持原始文件的目录结构以保证有效性。默认配置文件位于 config.zip 文件中。如果创建一个文件夹，请确保保持文件结构并包括带配置文件的 Outlook 或 Lotus Notes 子文件夹（如果只安装 Outlook 插件，则可以省略 LotusNotes 文件夹，反之亦然）。



## 第 4 章

# 配置和使用适用于 Outlook 的 Cisco IronPort 邮件安全插件

---

本章介绍适用于 Outlook 的 Cisco IronPort 邮件安全插件中的可用功能。Cisco IronPort 邮件安全插件包括多种与 Outlook 邮件程序配合使用的安全插件。本章包含以下部分：

- [适用于 Outlook 的 Cisco IronPort 邮件安全插件常规设置（第 4-32 页）](#)
- [配置 Outlook 插件的基本设置（第 4-33 页）](#)
- [报告插件（第 4-35 页）](#)
- [加密插件（第 4-39 页）](#)
- [更改日志记录设置（第 4-42 页）](#)
- [使用诊断工具进行故障排除（第 4-43 页）](#)
- [卸载 Cisco IronPort 邮件安全插件（第 4-46 页）](#)

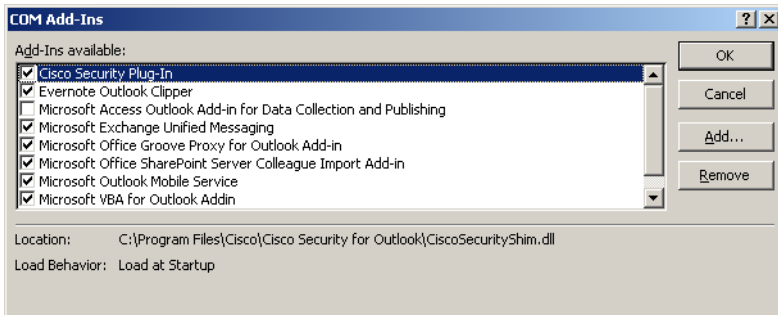
# 适用于 Outlook 的 Cisco IronPort 邮件安全插件常规设置

Cisco IronPort 邮件安全插件是一个支持多个思科插件（包括加密插件和报告插件）的平台。您可以从选项页配置 Cisco IronPort 邮件安全插件的常规设置。

## 启用/禁用

在默认情况下，Cisco IronPort 邮件安全插件会在安装时启用。如果您希望禁用 Cisco IronPort 邮件安全插件，可以从以下位置执行禁用操作：

- 从 Outlook2003/2007：转到“工具 (Tools)” > “选项 (Options)” > “思科邮件安全 (Cisco Email Security)”。
- 从 Outlook 2010：转到“文件 (File)” > “选项 (Options)” > “加载项 (Add-ins)”。然后选中“管理 (Manage)”下拉列表中的 COM 插件，并点击“前往 (Go)”。



从 COM 加载项窗口，取消选中 Cisco IronPort 邮件安全插件复选框，然后点击“确定 (OK)”。

## 配置 Outlook 插件的基本设置

您可以从“思科邮件安全 (Cisco Email Security)”选项卡配置基本设置。要在 Outlook 2003/2007 中打开思科邮件安全选项卡，请转到“工具 (Tools)” > “选项 (Options)” > “思科邮件安全 (Cisco Email Security)”。

-或-

从 Outlook 2010：转到“文件 (File)” > “选项 (Options)” > “加载项 (Add-ins)” > “加载项选项 (Add-in Options)” > “思科邮件安全 (Cisco Email Security)”。

思科邮件安全选项卡：



您可以通过选中该选项卡中报告、加密和日志记录的“启用 (Enable)”复选框启用这些选项。要进一步配置设置，可点击“报告选项...(Reporting Options...)”、“加密选项...(Encryption Options...)”或“日志记录选项...(Logging Options...)”按钮。此外，您还可以在解决问题时使用诊断工具运行有关 Cisco IronPort 邮件安全插件的报告，并发送至思科支持部门。

# 报告插件

报告设置允许您启用或禁用报告插件。报告插件允许您向思科报告您收到的邮件为垃圾邮件、网络钓鱼攻击邮件、病毒邮件或错误分类为垃圾邮件的邮件（有时也称为“ham”）。

您可以通过 Outlook 中的“选项”页配置适用于 Outlook 的 Cisco IronPort 邮件安全报告插件。

要启用适用于 Outlook 2003/2007 的报告插件，请转到“工具 (Tools)” > “选项 (Options)” > “思科邮件安全 (Cisco Email Security)”选项卡，然后选中“思科邮件安全 (Cisco Email Security)”选项卡“报告 (Reporting)”区域中的“启用 (Enable)”复选框。

-或-

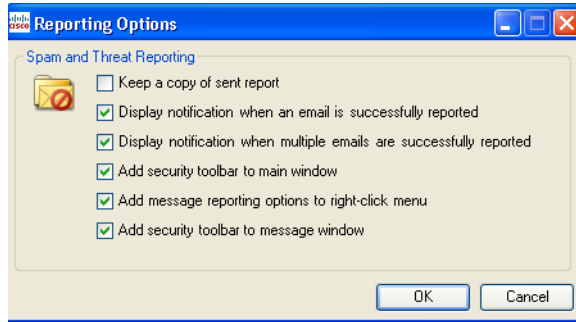
要启用适用于 Outlook 2010 的报告插件，请转到“文件 (File)” > “选项 (Options)” > “加载项 (Add-ins)” > “加载项选项 (Add-in Options)” > “思科邮件安全 (Cisco Email Security)”选项卡，然后选中“思科邮件安全 (Cisco Email Security)”选项卡“报告 (Reporting)”区域中的“启用 (Enable)”复选框。

## 报告选项

要访问 Outlook 2003/2007 中的报告选项页，请转到“工具 (Tools)” > “选项 (Options)” > “思科邮件安全 (Cisco Email Security)”选项卡，然后点击“报告选项 (Reporting Options)”按钮。

要修改 Outlook 2010 中的加密设置，请转到“文件 (File)” > “选项 (Options)” > “加载项 (Add-ins)” > “加载项选项 (Add-in Options)” > “思科邮件安全 (Cisco Email Security)”，然后点击“报告选项 (Reporting Options)”按钮。

报告选项页：



## 选项

本部分介绍您可以配置的报告选项。

- **保存已发送报告的副本。**在默认情况下，当您向思科报告邮件为垃圾邮件、病毒、错误分类的垃圾邮件时，发送的报告邮件会被删除。选择此选项可防止邮件被删除。
- **成功报告邮件时显示通知。**成功将一封邮件报告为垃圾邮件或病毒时，可将 Outlook 设置为在对话框中显示成功消息。清除此选项可防止显示此对话框。
- **成功报告多封邮件时显示通知。**当多封邮件报告成功时（报告为垃圾邮件、病毒、网络钓鱼或非垃圾邮件），可将 Outlook 设置为在对话框中显示成功消息。清除此选项可防止显示此对话框。
- **在主窗口添加安全工具栏。**在默认情况下，安装 Cisco IronPort 邮件安全插件时，将向 Outlook 主窗口添加插件工具栏。清除此选项可防止向 Outlook 主窗口添加此工具栏。
- **在右键单击窗口添加邮件报告选项。**在默认情况下，安装 Cisco IronPort 邮件安全插件时，将向 Outlook 右键单击上下文菜单添加“报告”插件菜单项。清除此选项可防止向右键单击上下文菜单添加此菜单项。
- **在邮件窗口添加安全工具栏。**在默认情况下，安装 Cisco IronPort 邮件安全插件时，将向邮件窗口添加插件工具栏。清除此选项可防止向邮件窗口添加此工具栏。



## 使用适用于 Outlook 的报告插件

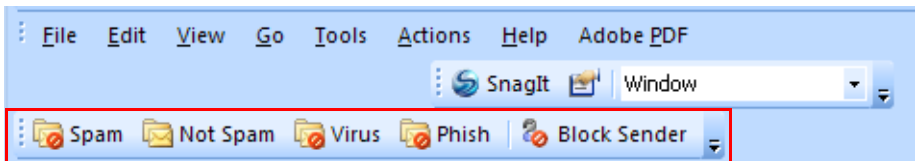
### 概述

适用于 Outlook 的 Cisco IronPort 邮件安全插件允许向思科提交有关在收件箱中收到的垃圾邮件、病毒或网络钓鱼邮件的反馈。例如，如果邮件被错误分类或邮件应被分类为垃圾邮件，您可以告知思科。思科将使用该反馈更新邮件过滤器，此过滤器可防止将不需要的邮件发送至您的收件箱。

此插件通过 Outlook 菜单栏和右键单击邮件菜单提供便捷接口，以报告垃圾邮件、病毒、网络钓鱼和错误分类邮件。报告邮件后，系统将显示报告已提交消息。您报告的邮件用于改进思科邮件过滤器，帮助降低发送至收件箱的未经索取的邮件总量。

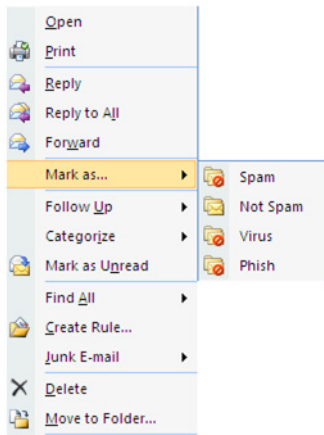
### 向思科提供反馈

此插件在 Outlook 中提供新的工具栏，包括以下按钮：垃圾邮件、非垃圾邮件、病毒、网络钓鱼和阻止发件人（“阻止发件人”不阻止垃圾邮件箱中的邮件）。

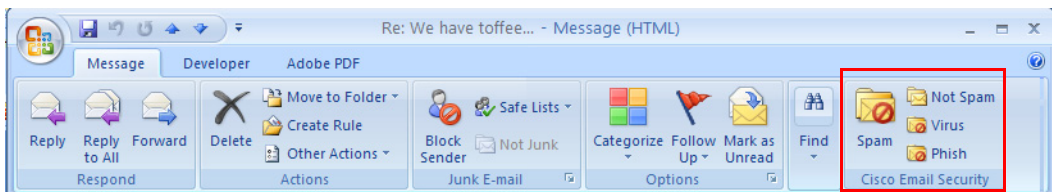


这些按钮用于报告垃圾邮件、病毒和网络钓鱼邮件。（网络钓鱼攻击指链接至欺骗收件人泄露信用卡帐号、帐户用户名和密码、身份证号等个人财务数据的欺诈网站的邮件。例如，您可能会收到来自 *infos@paypals.com* 的邮件，此邮件意在骗取您的个人银行信息）。

您还可以使用右键单击上下文菜单报告垃圾邮件、错误分类邮件、病毒和网络钓鱼邮件。

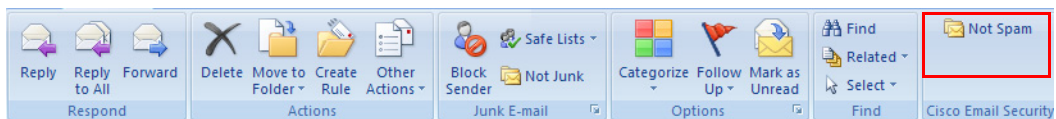


您可以使用邮件窗口中的按钮报告垃圾邮件、病毒、网络钓鱼和错误分类邮件（错误分类邮件指被错误标记为垃圾邮件、病毒或网络钓鱼的邮件）。

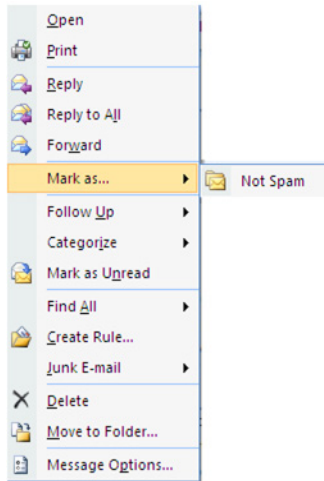


如果您收到的邮件被错误分类为垃圾邮件（即经过过滤并发送至垃圾邮件文件夹），您可以点击“**非垃圾邮件 (Not Spam)**”按钮将此邮件报告为错误分类邮件。这样可确保以后来自此发件人的邮件不再被归类为垃圾邮件。

此外，从垃圾邮件文件夹可点击邮件窗口中的“**非垃圾邮件 (Not Spam)**”按钮，将邮件标记为错误分类邮件。



还可以从右键单击上下文菜单标记错误分类邮件。



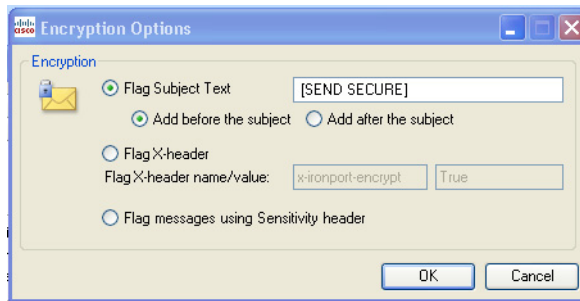
## 加密插件

加密设置位于思科邮件安全页。要修改 Outlook 2003/2007 中的加密设置，请转到“工具 (Tools)” > “选项 (Options)” > “思科邮件安全 (Cisco Email Security)”选项卡，然后单击“加密选项 (Encryption Options)”。

要修改 Outlook 2010 中的加密设置，请转到“文件 (File)” > “选项 (Options)” > “加载项 (Add-ins)” > “加载项选项 (Add-in Options)” > “思科邮件安全 (Cisco Email Security)”，然后单击“加密选项 (Encryption Options)”按钮。

选中或清除“思科邮件安全 (Cisco Email Security)”选项卡中“加密 (Encryption)”区域中的“启用 (Enable)”复选框可启用或禁用加密插件。

加密选项：



## 选项

### 发送加密邮件选项

希望加密发送邮件时，需要“标记”邮件进行加密。这样可允许系统管理员创建的过滤器识别需要加密的邮件。



警告

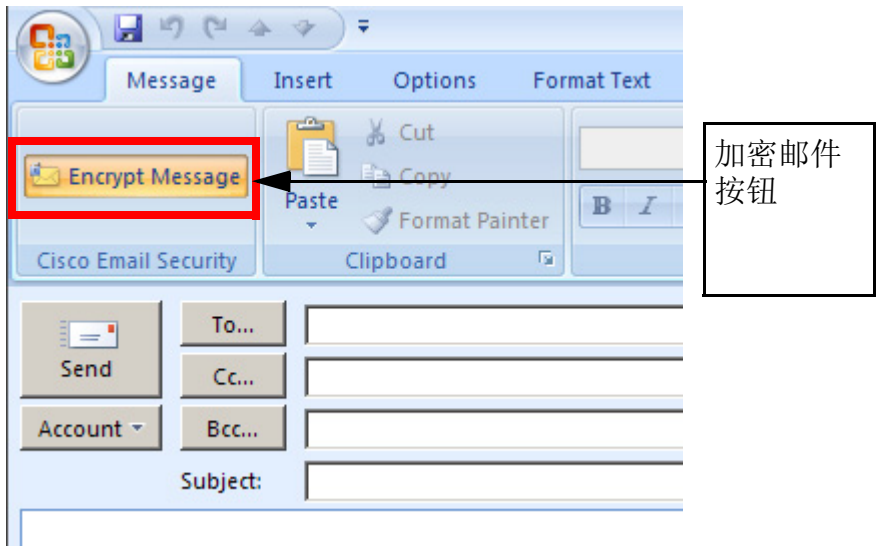
**在未与系统管理员联系的情况下，请勿更改标记加密邮件的方法。这些方法需要在 Cisco IronPort 加密装置中进行设置更改才能正常使用，并且只有您的系统管理员才能进行这些更改。**

您可以使用以下方法之一标记邮件进行加密：

- **标记主题文本。**可通过向发出邮件的“主题 (Subject)”字段添加文本标记邮件进行加密。输入文本，将“主题 (Subject)”字段预置为表示应对邮件进行加密（默认值为 *[SEND SECURE]*）。
- **标记 X 标头名称/值。**可为发出邮件添加标记邮件以供加密的 x 标头。在第一个字段输入 x 标头（默认值为 *x-ironport-encrypt*）。在第二个字段中，输入一个 *True* 值或 *False* 值。如果输入 *true*，则带有指定的 x 标头的邮件将被加密（默认值为 *true*）。
- **Outlook 敏感标头。**Outlook 可添加敏感标头标记邮件进行加密。选择此方法允许使用 Outlook 敏感标头标记邮件进行加密。

## 发送加密邮件

编写邮件时，您可以通过点击“加密邮件 (Encrypt Message)”按钮发送安全邮件。在发送安全邮件前，请先验证“加密邮件 (Encrypt message)”按钮是否已选中，如下所示：

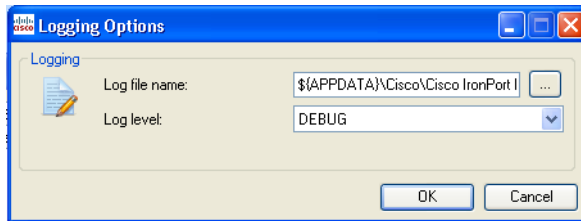


编写邮件时，“加密邮件”按钮可用。

## 更改日志记录设置

点击“日志记录选项...(Logging Options...)”打开“日志记录选项 (Logging Options)”页。

日志记录选项：



### 选项

您可以从日志记录菜单配置以下选项：

#### 日志文件名称

允许指定将存储在 %appdata%\Cisco 中的日志文件名称。日志文件名的扩展名必须是 .log。

#### 日志级别

日志级别指定将哪些信息记录在日志文件中。您可以选择以下日志记录级别之一：

- **错误。**记录错误消息和异常情况。
- **警告。**记录警告消息和错误消息。
- **信息。**记录基本信息和其他状态消息。记录自动更新进程状态消息。还记录全部警告和错误消息。
- **调试。**记录有关配置设置的详细信息。记录所有“错误 (ERROR)”、“警告 (WARN)”和“信息 (INFO)”错误消息，并且还记录对解决问题可能有帮助的信息。

您可能希望根据特定情况所需的故障排除级别更改日志记录级别。例如，如果您遇到了 Cisco IronPort 邮件安全插件问题，可能将日志记录级别设置为“调试”，从而向开发人员提供尽可能多的信息，使开发人员能够重现问题并运行诊断。

## 使用诊断工具进行故障排除

Cisco IronPort 邮件安全插件包括帮助思科支持进行故障排除的诊断工具。此诊断工具从插件工具收集重要数据，之后将数据发送至思科支持以协助开发人员解决问题。

如果您收到错误或遇到修复过程无法解决的 Cisco IronPort 邮件安全插件问题，您可能希望使用此诊断工具。报告错误时，您还可以使用此诊断工具与思科工程师共享重要信息。

注意：如果遇到错误，请查看“诊断”部分获取故障排除提示。

## Cisco IronPort 邮件安全诊断工具收集的数据

此诊断工具从您的计算机收集以下信息：

- 部分 COM 组件的注册信息
- 环境变量
- Cisco IronPort 邮件安全插件输出文件
- 有关 Windows 和 Outlook 的信息
- 系统用户名和 PC 名称
- 有关其他 Outlook 插件的信息

## 运行 Cisco IronPort 邮件安全诊断工具

您可以从以下位置之一运行思科邮件安全诊断工具：

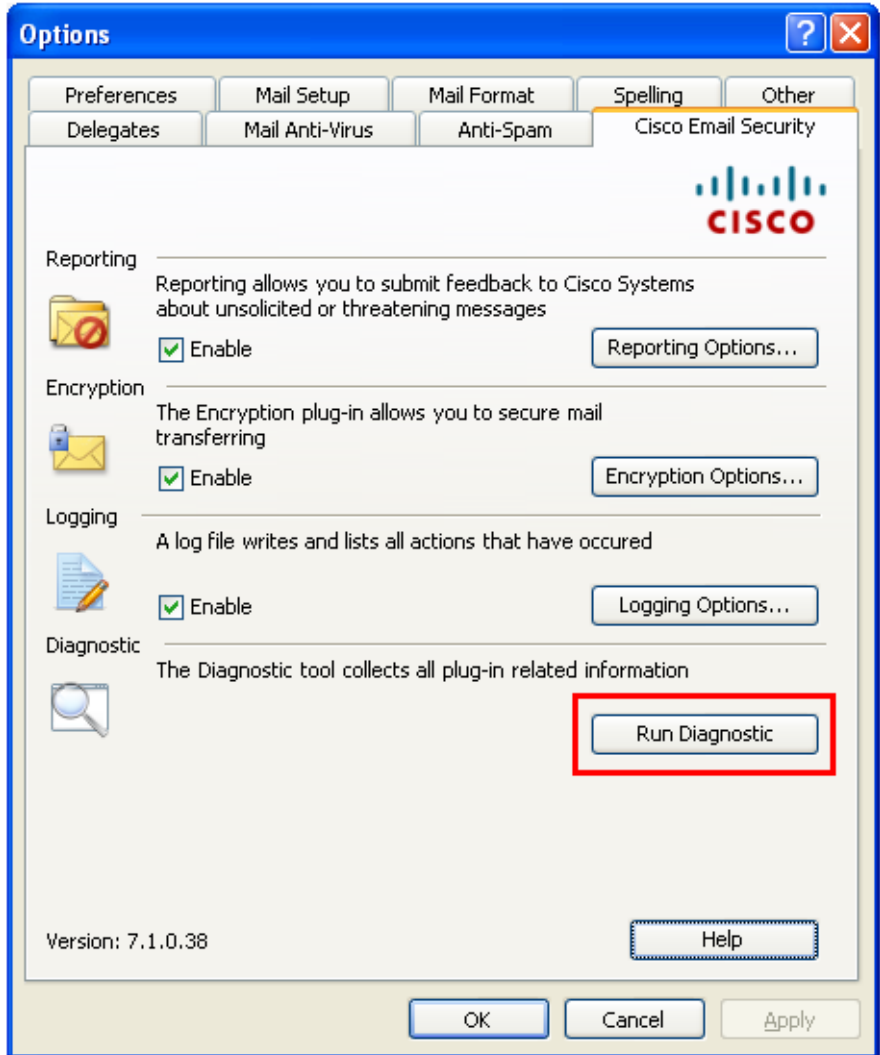
- 从“思科邮件安全选项 (Cisco Email Security options)”选项卡运行诊断工具。通常，您可以从“思科邮件安全选项 (Cisco Email Security options)”选项卡运行诊断工具。
- 从“Program Files\Cisco IronPort 邮件安全插件”文件夹（通常为 C:\Program Files\Cisco\Cisco IronPort 邮件安全插件）运行诊断工具。此文件夹为安装 Cisco IronPort 邮件安全插件的文件夹。
- 从“开始菜单 (Start Menu)” > “所有程序 (All Programs)” > “Cisco IronPort 邮件安全插件” > “诊断工具 (Diagnostic Tool)”运行诊断工具。

### 从“Outlook 选项 (Outlook Options)”选项卡运行诊断工具

从 Outlook 2003/2007：转到“工具 (Tools)” > “选项 (Options)” > “思科邮件安全 (Cisco Email Security)”选项卡，然后点击“运行诊断 (Run Diagnostics)”。或者，从 Outlook 2010：转到“文件 (File)” >



“选项 (Options)” > “加载项 (Add-ins)” > “加载项选项 (Add-in Options)” > “思科邮件安全 (Cisco Email Security)”，然后点击“运行诊断 (Run Diagnostics)”：



1. 等待几秒钟，使诊断工具收集数据。
2. 当诊断工具完成数据收集时，它将显示一个表示已成功收集数据的消息。

您可以转到 *CiscoDiagnosticReport.zip* 文件，并将其手动发送给您的系统管理员或思科支持代表。

## 从“程序文件 (Program Files)”运行诊断工具

找到安装 Cisco IronPort 邮件安全插件的文件夹（通常为 C:\Program Files\Cisco\Cisco IronPort 邮件安全插件），然后双击 *Cisco.EmailSecurity.Framework.Diagnostic.exe* 文件。

## 从开始菜单运行诊断工具

从“开始 (Start)” > “程序 (Programs)” > “Cisco IronPort 邮件安全插件”运行诊断工具。点击“诊断工具 (Diagnostic Tool)”。要查看报告，请点击“转到报告 (Go to Report)”。报告保存为压缩文件 *CiscoDiagnosticsReport.zip*。

# 卸载 Cisco IronPort 邮件安全插件

您可以通过“控制面板 (Control Panel)” > “添加/删除程序 (Add/Remove Program)”选项或运行 *setup.exe* 程序卸载 Cisco IronPort 邮件安全插件。

卸载期间，将删除以下项：

- 插件生成的所有注册表项。
- 添加/删除程序列表中的插件项。
- 与插件相关的文件。
- 插件工具栏（从 Outlook 删除）。



### 注意

卸载该插件不会影响 Outlook 性能。

## 卸载适用于 Outlook 的 Cisco IronPort 邮件安全插件

要卸载适用于 Outlook 的 Cisco IronPort 邮件安全插件，有两种可行的方法：

- 点击“开始 (Start)” > “控制面板 (Control Panel)” > “添加/删除程序 (Add/Remove Programs)”。选中 Cisco IronPort 邮件安全插件，然后点击“删除 (Remove)”。
- 或-
- 双击插件设置文件（用于安装此插件的文件），并选择“删除 (Remove)”选项卸载 Cisco IronPort 邮件安全插件。



## 第 5 章

# 配置和使用适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件

---

本章介绍适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件中的可用功能。Cisco IronPort 邮件安全插件包含多个常用邮件安全插件。本章包含以下部分：

- [适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件常规设置（第 5-47 页）](#)
- [报告插件（第 5-49 页）](#)
- [加密插件（第 5-51 页）](#)
- [更改日志记录选项（第 5-54 页）](#)
- [故障排除和诊断（第 5-55 页）](#)
- [卸载（第 5-59 页）](#)

## 适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件常规设置

适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件是一个支持多个 Cisco IronPort 邮件安全插件的框架：

- 报告插件。使用此插件可报告属于垃圾邮件、病毒、网络钓鱼攻击或错误分类为垃圾邮件的邮件。
- 加密插件。使用此插件可发送安全加密的邮件。

您可以从“选项 (Options)”页配置 Cisco IronPort 邮件安全插件。要访问“选项 (Options)”页，请转到“操作 (Actions)” > “思科邮件安全 (Cisco Email Security)”。

思科邮件安全选项页：



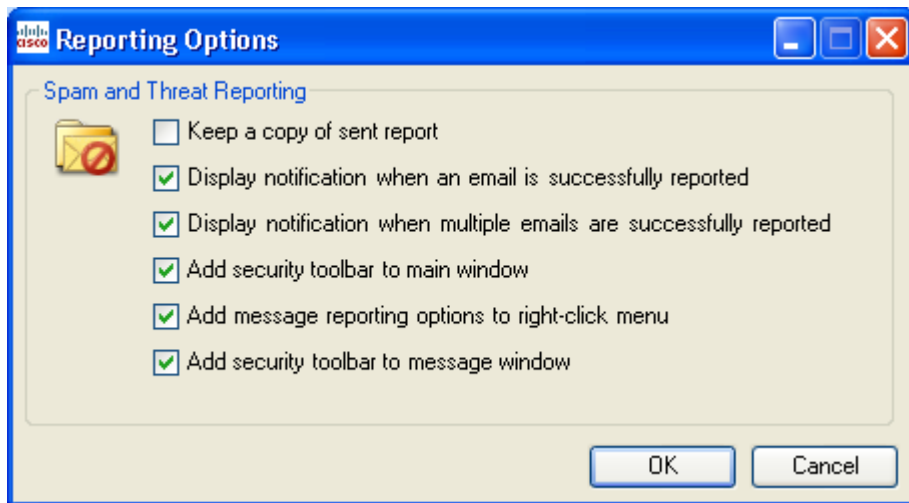
您可以通过选中该选项卡中报告、加密和日志记录的“启用 (Enable)”复选框启用这些选项。要进一步配置设置，可点击“报告选项...(Reporting Options...)”、“加密选项...(Encryption Options...)”或“日志记录选项...(Logging Options...)”按钮。此外，您还可以在解决问题时使用诊断工具运行有关 Cisco IronPort 邮件安全插件的报告，并发送至思科支持部门。

## 报告插件

### 选项对话框

报告插件允许您向思科报告您收到的属于垃圾邮件、网络钓鱼攻击、病毒或错误分类为垃圾邮件的邮件。

您可以通过“选项 (Options)”对话框配置适用于 Lotus Notes 的思科邮件安全报告插件。要访问报告选项页，请转到“操作 (Actions)” > “思科邮件安全选项 (Cisco Email Security Options)”，然后选择对话框中的“报告 (Reporting)”选项卡。



## 选项

本部分介绍您可以修改的报告选项。

### 保留已发送报告副本

在默认情况下，当您向思科报告邮件为垃圾邮件、病毒、错误分类的垃圾邮件时，发送的报告邮件会被删除。选择此选项可防止邮件被删除。

### 成功报告邮件时显示通知

报告邮件时，您可以选择此选项，以显示向您提示已成功报告邮件的通知。

### 成功报告多封邮件时显示通知

报告一组邮件时，您可以选择此选项，以显示向您提示已成功报告邮件的通知。

### 在主窗口添加安全工具栏

使用此选项可在主窗口添加安全工具栏。

### 在右键单击窗口添加邮件报告选项

使用此选项可在右键单击窗口添加邮件报告选项。

### 在邮件窗口添加安全工具栏

使用此选项可在邮件窗口添加安全工具栏。

## 使用适用于 Lotus Notes 的报告插件

适用于 Lotus Notes 的思科邮件安全报告插件允许您向思科提交有关在收件箱中收到的垃圾邮件、病毒或网络钓鱼邮件的反馈。思科将使用该反馈更新邮件过滤器，此过滤器可防止将不需要的邮件发送至您的收件箱。

您可以通过主菜单栏配置设置，以使 Lotus Notes 报告垃圾邮件、病毒、网络钓鱼和错误分类的邮件。报告邮件后，系统将显示报告已提交消息。您报告的邮件用于改进思科邮件过滤器，帮助降低发送至收件箱的未经索取的邮件总量。

# 加密插件

## 配置加密选项

您可以从“思科邮件安全选项 (Cisco Email Security Options)”对话框修改加密插件设置。要修改您的加密设置，请转到“**操作 (Actions)**” > “**思科邮件安全选项 (Cisco Email Security Options)**”，然后点击“**加密选项 (Encryption Options)**”。

## 选项

### 发送加密邮件选项

希望加密发送邮件时，需要“标记”邮件进行加密。这样可允许系统管理员创建的过滤器识别需要加密的邮件。



#### 警告

---

**在未与系统管理员联系的情况下，请勿更改标记加密邮件的方法。这些方法的更改需要在 Cisco IronPort 加密设备上进行，并且只有您的系统管理员才能进行这些更改。**

---

您可以使用以下方法之一标记邮件进行加密：

- **标记主题文本。**可通过向发出邮件的“主题 (Subject)”字段添加文本标记邮件进行加密。输入文本，将“主题 (Subject)”字段预置为表示应对邮件进行加密（默认值为 *[SEND SECURE]*）。
- **标记 X 标头名称/值。**可为发出邮件添加标记邮件以供加密的 x 标头。在第一个字段输入 x 标头（默认值为 *x-ironport-encrypt*）。在第二个字段中，输入一个 **true** 值或 **false** 值。如果输入 *true*，则带有指定的 x 标头的邮件将被加密（默认值为 *true*）。

## 使用加密插件

### 概述

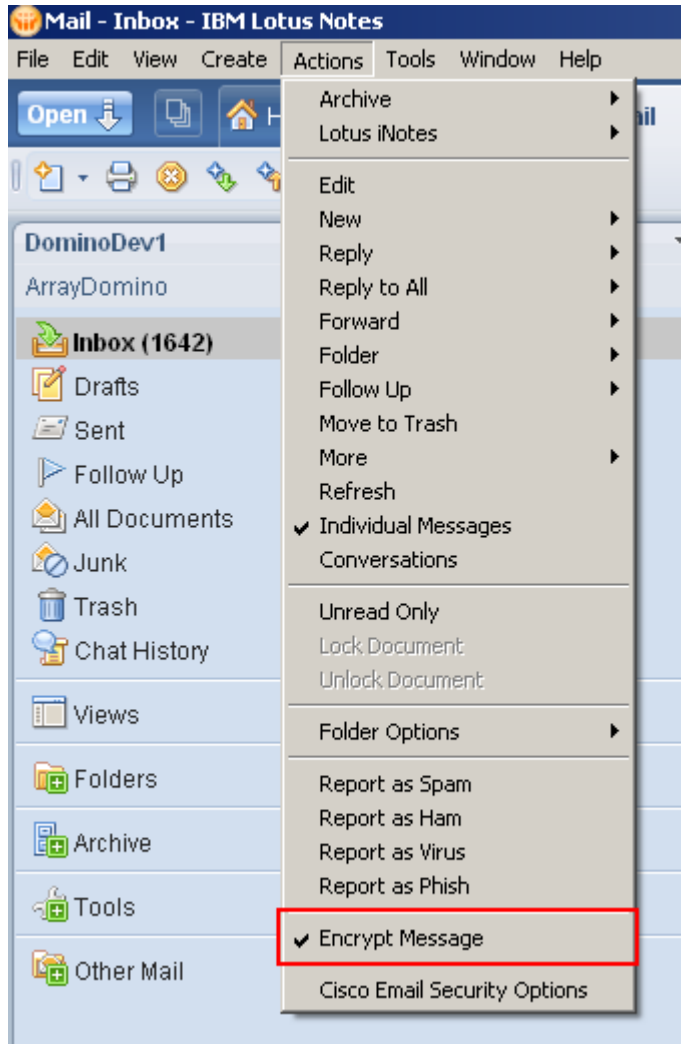
加密插件允许您从 Lotus Notes 邮件程序发送加密邮件。发送安全邮件时，思科邮件安全加密插件会安全地发送标记进行加密的邮件，确保只有目标收件人能够阅读您的邮件。

### 发送安全邮件

您可以通过选中“操作 (Actions)”菜单中的“**加密邮件 (Encrypt message)**”按钮，使您的邮件系统发送安全邮件。



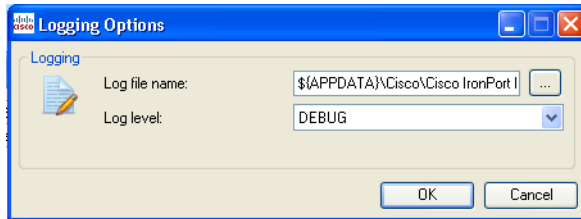
要发送安全邮件，请先验证“加密邮件 (Encrypt message)”按钮是否选中，如下所示：



## 更改日志记录选项

点击“日志记录选项...(Logging Options...)”打开“日志记录选项 (Logging Options)”页。

日志记录选项：



### 选项

您可以从日志记录菜单配置以下选项：

#### 日志文件名称

允许指定将存储在 %appdata%\Cisco 中的日志文件名称。日志文件名的扩展名必须是 .log。

#### 日志级别

日志级别指定将哪些信息记录在日志文件中。您可以选择以下日志记录级别之一：

- **错误。**记录错误消息和异常情况。
- **警告。**记录警告消息和错误消息。
- **信息。**记录基本信息和其他状态消息。记录自动更新进程状态消息。还记录全部警告和错误消息。
- **调试。**记录有关配置设置的详细信息。记录所有“错误 (ERROR)”、“警告 (WARN)”和“信息 (INFO)”错误消息，并且还记录对解决问题可能有帮助的信息。

您可能希望根据特定情况所需的故障排除级别更改日志记录级别。例如，如果您遇到了 Cisco IronPort 邮件安全插件问题，可能将日志记录级别设置为“调试”，从而向开发人员提供尽可能多的信息，使开发人员能够重现问题并运行诊断。

## 故障排除和诊断

本部分列出了使用适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件时可能出现的一些常见错误以及修复这些错误的故障排除提示。



### 注意

如果多次收到相同的错误消息，并且该错误干扰适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件的功能，请运行修复过程。如果您在运行修复过程后遇到相同的错误，请根据相关步骤向思科提供[思科邮件安全诊断工具](#)反馈。

## 常见启动错误

### 配置文件初始化时出错

启动 Outlook 时可能会出现以下消息：

- Cisco IronPort 邮件安全插件配置文件初始化时出错。将有些设置设置为默认值。
- 读取报告组件的配置时出错。将有些设置设置为默认值。
- 读取加密组件的配置时出错。将有些设置设置为默认值。

如果配置文件 (*%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes\CommonConfig.xml*) 中的某些值损坏了，则会出现这些错误消息。

### 解决方案

插件将会恢复损坏的配置文件中的默认值。但是，如果您继续收到错误消息，则请运行修复过程以修复配置文件。

## 找不到配置文件。将设置设置为默认值

启动 Outlook 时可能会显示以下错误消息之一：

- 找不到 Cisco IronPort 邮件安全插件配置文件。将设置设置为默认值。
- 未找到加密组件的配置文件。将设置设置为默认值。
- 未找到报告组件的配置文件。将设置设置为默认值。

## 解决方案

插件将会恢复损坏的配置文件中的默认值。但是，如果您继续收到此错误消息，则请运行修复过程以修复配置文件。

## 邮件报告错误

### 无效的邮件地址

点击 Lotus Notes 中的“报告为垃圾邮件 (Report as Spam)”、“报告为病毒 (Report as Virus)”、“报告为网络钓鱼 (Report as Phish)”或“报告为非垃圾邮件 (Report as Not Spam)”按钮时，可能会出现以下消息：

无效的报地址类型。请更新配置文件。

如果您在使用报告插件且您试图报告的邮件格式不正确，则会出现此错误消息。您需要修复报告插件文件，以确保您可以报告垃圾邮件和网络钓鱼邮件（以及报告合法邮件为“非垃圾邮件”）。

## 解决方案

检查 `%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes` 文件夹中的报告配置。删除配置，然后运行修复过程以恢复默认值。

## 修复适用于 Lotus Notes 的 Cisco IronPort 邮件安全插件文件

1. 转到“控制面板 (Control Panel)” > “添加 (Add)”或“删除程序 (Remove Programs)”。
2. 从程序列表中找到 Cisco IronPort 邮件安全插件，然后点击“更改 (Change)”。
3. 确保 Lotus Notes 已关闭。

4. 选择 Cisco IronPort 邮件安全插件安装程序，然后单击“**修复 (Repair)**”单选按钮。
5. 单击“**下一步 (Next)**”。系统运行安装程序修复过程。
6. 执行导致错误的操作。如果运行修复过程后仍出现相同的错误，请根据相应步骤向思科提供诊断工具反馈。

## 思科邮件安全诊断工具

思科提供适用于 Cisco IronPort 邮件安全插件的诊断工具，该工具允许您向思科发送全面分析问题所需的详细信息。如果您收到错误或遇到修复过程无法解决的 Cisco IronPort 邮件安全插件问题，您可能希望使用此诊断工具。报告错误时，您还可以使用此诊断工具与思科工程师共享重要信息。

如果遇到错误，请查看“诊断”部分获取故障排除提示。

## 思科邮件安全诊断工具收集的数据

此诊断工具从您的计算机收集以下信息：

- 部分 COM 组件的注册信息
- 环境变量
- 思科邮件安全输出文件
- 有关 Windows 和 Lotus Notes 的信息
- 系统用户名和 PC 名称
- 有关其他 Lotus Notes 插件的信息

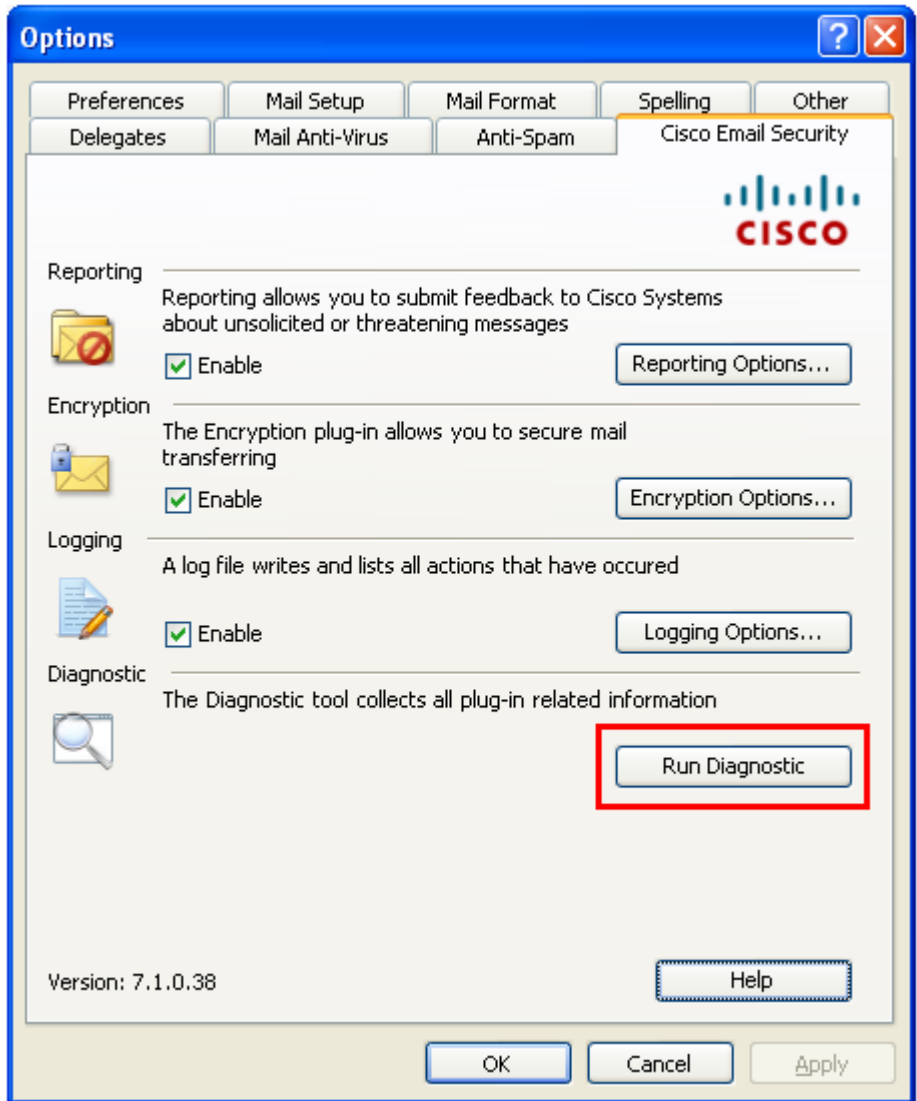
## 运行思科邮件安全诊断工具

您可以从以下位置之一运行思科邮件安全诊断工具：

- 从“**思科邮件安全选项 (Cisco Email Security options)**”对话框运行**诊断工具**。通常，您可以从“思科邮件安全选项 (Cisco Email Security options)”对话框运行诊断工具。您可以从“**操作 (Actions)**” > “**思科选项 (Cisco Options)**”访问诊断工具。
- 从“**Program Files\Cisco IronPort 邮件安全插件**”文件夹（通常为 C:\Program Files\Cisco\Cisco IronPort 邮件安全插件）运行诊断工具。此文件夹为安装 Cisco IronPort 邮件安全插件的文件夹。

## 从“选项 (Options)”对话框运行诊断工具

转到“操作 (Actions)” > “思科邮件安全选项 (Cisco Email Security Options)”，然后点击“运行诊断 (Run Diagnostics)”。等待几秒钟，使诊断工具收集数据。



当诊断工具完成数据收集时，它将显示一个表示已成功收集数据的消息。该工具将数据存储在名为 *CiscoDiagnosticReport.zip* 的压缩文件中。

您可以通过点击“**转至报告 (Go to Report)**”访问 *CiscoDiagnosticReport.zip* 文件，并将其手动发送给系统管理员或思科安全管理员。

## 从“程序文件 (Program Files)”运行诊断工具

从“开始 (Start)” > “程序 (Programs)” > “适用于 Lotus Notes 的思科邮件安全 (Cisco Email Security for Lotus Notes)”运行诊断工具。或者，找到安装思科邮件安全的文件夹（通常为 C:\Program Files\Cisco\Cisco IronPort 邮件安全插件），然后双击 *Cisco.EmailSecurity.Framework.Diagnostic.exe* 文件。

## 卸载

您可以通过“控制面板 (Control Panel)” > “添加/删除程序 (Add/Remove Program)”或运行 *setup.exe* 程序卸载 Cisco IronPort 邮件安全插件。

卸载期间，将删除以下项：

- 插件生成的所有注册表项。
- 添加/删除程序列表中的插件项。
- 与插件相关的文件。



**注意**

卸载该插件不会影响 Lotus Notes 的性能。

## 卸载该插件

要卸载 Cisco IronPort 邮件安全插件，有两种可行的方法：

- 点击“开始 (Start)” > “控制面板 (Control Panel)” > “添加/删除程序 (Add/Remove Programs)”。选中 Cisco IronPort 邮件安全插件，然后点击“**删除 (Remove)**”。
- 或-
- 双击插件设置文件（用于安装此插件的文件），并选择“**删除 (Remove)**”选项卸载 Cisco IronPort 邮件安全插件。







## 附录 **A**

# IronPort 最终用户许可协议

---

本附录包含以下部分：

- [Cisco IronPort 系统有限责任公司软件许可协议（第 A-61 页）](#)

## Cisco IronPort 系统有限责任公司软件许可协议

全体用户须知：请仔细阅读以下软件（如下文定义）许可法律协议（“协议”）。您在收到提示时点击“接受 (Accept)”按钮或输入“Y”，即表示您（个人或单一实体，统称为“公司”）同意成为特拉华州 CISCO IRONPORT 系统有限责任公司（以下简称“IRONPORT”）和公司（统称为“双方”）之间签订的协议的一方并受此协议约束。您在收到提示时点击“接受 (Accept)”按钮或输入“Y”，即表示您 (A) 经正式授权代表您的公司并且 (B) 您代表您的公司同意本协议中的条款和条件，因此形成协议。如果您或者您所代表的公司（统称为“公司”）不同意本协议中的条款和条件，请在收到提示时点击“取消 (Cancel)”按钮或输入“N”并立即（自下文定义的交付日期起三十 (30) 天之内）通知 IRONPORT 或通知向您提供该软件的经销商，以获得已为软件支付的款项的全额退款。

### 1. 定义

1.1 “公司服务”指公司向最终用户提供的用于经营公司内部业务的邮件服务或互联网服务，通过由公司和 IronPort 或其经销商签订的购买协议、评估协议、测试或预发行版本协议、采购订单、销售报价或其他类似协议（“协议”）中所描述的公司产品，以及概述了系统架构及其接口的可用程序接口和 IronPort 标准系统指南文档（统称为“许可文档”）实现这些服务。

1.2 “最终用户”指经公司授权通过公司服务接入互联网或使用邮件服务的员工、承包商或其他代理。

1.3 “服务”是指 (i) 提供软件功能，例如更新和升级，和 (ii) 由 IronPort 或其经销商（视情况而定）提供的支持。

1.4 “软件”是指：(i) 连同 IronPort 硬件产品一起经 IronPort 授权给公司的 IronPort 专有软件；(ii) 任何由 IronPort 第三方许可者提供的授权给公司以实现与 IronPort 硬件产品共同使用的软件；(iii) 任何连同 IronPort 硬件产品一起由 IronPort 授权给公司的其他 IronPort 软件模块；(iv) 所有随附的任何更新与升级。

1.5 “更新”是指不会添加重要新功能至软件的并且由 IronPort 或其第三方许可者发行的微小更新、错误更正或漏洞修补程序。更新通过软件版本号小数点右面的数字增加进行命名（例如，软件 1.0 到软件 1.1）。具体而言，更新不包括由 IronPort 或其第三方许可者作为单独产品销售及授权的升级或新软件版本。

1.6 “升级”是指由 IronPort 或其第三方许可者全权决定是否发行或何时发行的软件修订版，该修订版会对当前功能添加新增强功能。思科通过增加软件版本号小数点左面的数字对升级进行命名（例如，软件 1.x 到软件 2.0）。任何情况下，升级均不包括由 IronPort 或其第三方许可者作为单独产品销售及授权的新软件版本。

## 2. 许可证授予并同意数据收集条款

2.1 软件许可证。公司使用该软件和授权文件，即代表公司同意遵守本协议中的条款。只要公司遵守本协议，IronPort 特此授予公司在本软件使用期限内非独占、不可再授权、不可转让的全球许可证，前提是软件只能用于 IronPort 的硬件产品且只能与最终用户的公司服务关联使用。该许可的持续时间和范围在许可文档中详细定义。除非本文另外明示说明，否则 IronPort、IronPort 的经销商或其对应许可者并未授予公司任何软件拥有权利、所有权或利益。此许可证与所有服务拥有相同的期限。

2.2 同意并许可使用数据。依照本文第 8 部分和 <http://www.IronPort.com/privacy.html> 网站上的 IronPort 隐私声明，IronPort 可能不定期对该隐私声明进行修正并通知公司，公司据此同意并许可 IronPort 收集和使用权文档所述的来自公司的数据，并且 IronPort 也可能不定期更新隐私声明（“数据”）。鉴于报告或统计是通过使用数据生成的，应仅以汇聚的形式进行披露，并且应无法根据数据推测出最终用户识别信息，包括（但不限于）用户名、电话号码、明确的文件名、邮件地址、实际地址和文件内容。尽管受到上述限制，但如果该权利被终止，公司可能无法使用软件或其组件，则公司可以事先书面或电子通知的形式随时终止 IronPort 收集并使用数据的权利。

3. 机密性。各方同意以保护自身类似机密信息的同等谨慎程度保密另一方的所有机密信息（并且任何情况下均不得低于合理的谨慎程度）并仅在本协议允许的情况下使用此类机密信息。鉴于本协议的目的，“机密信息”指一方标记为“机密”的信息或披露方合理认为具有所有权或机密性质的信息；数据、软件、设计评审披露的信息和任何 IronPort 提供的软件前期制作版本均明确指定为机密信息，不管它们是否被标记为此类信息。

4. 专有权；所有权。对软件和其他材料的拥有权和所有权以及与 IronPort 或其经销商提供给公司的上述服务相关的所有知识产权（如下文定义）将仍是 IronPort 和/或其高级许可者的专有财产。公司与其员工和代理不会删除或更改 IronPort 或其经销商提供给公司的软件或其他材料（或其副本）上出现的任何商标或者其他所有权公告、图例、符号或标签。公司将不会修改、传输、转售以获取利润、散布、复制、加强、改编、翻译、反编译、逆向开发、拆卸，或者确定或试图获取任何软件的源代码或软件生成的任何内部数据文件，或者基于软件或许可文档创建任何衍生产品，并且公司同意不允许或授权他人进行此类操作。除非经过书面同意，否则 IronPort 或其高级许可者在协议执行期间创建或开发的任何程序、发明、理念、文档、规格或其他书面或图形材料和媒体，或者任何相关的咨询或专业服务协议，包括所有版权、数据库权利、专利、交易秘密、商标、道德权利或与此类相关的其他知识产权（“知识产权”）应为 IronPort 或其高级许可者独家所有，并且不可在《美国法典》第 17 条（1976 年的版权法）的意义内将此类产品视为公司雇佣作品。

#### 5. 有限保修和保修声明

5.1 有限保修。IronPort 向公司担保在正确安装并使用的前提下，软件自交付日期起九十 (90) 天或在许可文档中阐述的时间段（以较长者为准）（“保修期”）内将基本遵守许可文档中的规范。对于本节中包含的任何保修违例，如果不合规已经由公司于保修期内报告至 IRONPORT 或其经销商，则公司的独自补救和 IRONPORT 的全权负责将是对错误或不合规的迅速矫正。此保修仅面向公司，不可转让给任何最终用户或其他第三方。对于出现本节所述的保修违例或者通过以下方式直接或间接出现或者与其相关的协议违例，IronPort 不应承担责任：(i) 公司或任何第三方对软件进行任何未经授权的、不正确的、不完整的或不当的维护或校准；(ii) 任何第三方硬件的软件、服务或系统；(iii) 任何未经授权对软件或服务的修改或更改；(iv) 任何对软件未经授权或不正确的使用或操作，或者公司未遵守任何适用环境规范；或者 (v) 未能适时安装和/或使用 IronPort 或其经销商提供的更新、升级、修补程序或修正。

5.2 保修声明。本协议第 5.1 部分明确阐述的保修构成与软件或服务相关的唯一性能保修。在适用法律最大程度允许的情况下，IRONPORT 依本协议按“原样”对软件和服务进行许可。除了本文明确阐明之外，IronPort 和其高级许可者不做任何明示、暗示或者法定（基于事实或法律的实施）的陈述或担保，并且明确声明不承诺所有其他担保，包括但不限于对特定用途的适销性或适用性的暗示担保。IronPort 与其第三方许可者均不会担保软件或服务 (1) 无缺陷、错误或漏洞，(2) 软件的操作不受干扰，或 (3) 使用软件得出或可能得出的结果和信息均是准确、完整、可靠和/或安全的。

6. 责任限制。在适用法律最大程度允许的情况下，任何一方将不会关于以下方面对另一方负责，包括任何利润的损失、替代物品或服务的采购开销、业务损失、使用或数据损失、业务中断或者任何形式的间接、特殊、偶发性或相应而生损坏，即使一方事先已经收到可能产生此类损坏的通知。对于超出在引起此责任的事件发生之前十二 (12) 个月之内为软件或服务已支付总额的索赔，无论此类损坏索赔是基于合同、侵权或其他法律理论，双方均不会根据本协议的任何条款负有责任。

7. 期限和终止。本协议中的期限应如许可文档中所述（“期限”）。如果 IronPort 违反本协议或许可文档中任何材料条款的履行，并且如果违反行为未在三十 (30) 天的时间期限内得到纠正，则公司可基于此三十 (30) 天的书面通知终止本协议。如果公司违反本协议或许可文档中任何材料条款的履行，并且如果违反行为未在三十 (30) 天的书面通知内得到纠正，IronPort 可基于此三十 (30) 天的书面通知终止本协议并且不予退款。若出现下列情况，一方可在不进行通知的情况下随时终止本协议：(i) 另一方为偿还债务而破产、进行破产管理或破产程序或其他任何程序的情况，(ii) 此另一方将资产全部移交给债权人，或 (iii) 此另一方解散。第 2 部分中授予的许可证将根据本协议的终止或期满立即终止。在本协议终止或期满后三十 (30) 个日历天数内，公司将 IronPort 或其经销商依据本协议提供给公司的所有版本的软件或其他任何材料或文档递交至 IronPort 或其经销商，或者销毁所有这些软件、材料或文档。

8. 美国政府限制的权利；出口管制。软件和随附的许可文档分别被视为“商业计算机软件”和“商业计算机软件文档”，并且分别遵守 DFAR Section 227.7202 和 FAR Section 12.212 适用部分的条款。软件及随附美国政府批准的许可文档的任何使用、修改、复制、发行、性能、显示或披露应仅受本协议条款的监管并受到禁止，除非受到本协议条款的明确允许。公司认同软件和许可文档必须遵循美国出口管理条例，禁止违反美国法律的转运。公司阐明美国出口管理局和其他联邦机构均没有中止、撤销或拒绝公司出口特权。公司阐明公司将不会针对与任何核武器、生化武器或导弹技术相关的最终用途而使用或转移该软件，除非美国政府通过法规或具体许可授权。公司认同遵守美国或其他国家/地区所有任何进出口限制和其他适用法律是公司的最终责任，并且认同 IronPort 或其经销商在原始销售国家/地区首次将产品售给公司之后将不再负有其他责任。

9. 附则。本协议受美国和加利福尼亚州法律监管，不涉及任何法律原则冲突。明示排除《联合国国际货物销售合同公约》的适用性。本协议包含内容不应视为在各方之间建立代理、合作关系或其他形式的合营企业。依据本协议，任一方均不对由于下列原因而引起的任何未履行或推迟履行本协议义务（付费问题除外）负有责任：(i) 适用于本协议标的的当前或未来美国法律或法规或任何适用法律的任何条款，及 (ii) 电力中断、互联网故障、罢工、短缺、暴动、叛乱、火灾、洪水、暴风雨、爆炸、天灾、战争、恐怖行动、政府行为、劳动条件、地震或其他任何超出此方合理控制范围的因素。本协议和许可文档阐明了软件用户的所有权利并且是各方之间的完整协议，并取代其他任何与软件和许可文档有关的通信。当许可文档或任何购买订单或一方提交的其他书面文书与本协议中的条款和条件出现不一致时，以本协议为准，而不管是否受到另一方正式拒绝。除了经 IronPort 正当授权的公开发行的书面补遗外，本协议不可修改，但 IronPort 可随时自行修改 IronPort 隐私声明，此类修改会通知公司并在 <http://www.IronPort.com/privacy.html> 上公布。本协议任何条款均不可放弃，除非该放弃得到 IronPort 或其经正当授权的代表的书面签署认可。如果本协议中的任何条款失效，协议中的其他条款应继续保持完全有效。各方确定他们希望本协议仅以英文形式书写。

10. IRONPORT 联系信息。如果公司出于任何原因想要联系 IronPort，请写信至 IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066，或者拨打电话：650.989.6500，或者发传真至：650.989.6543。

