思科邮件安全插件 7.5.1 管理员指南

2015 年 10 月 28 日

美洲总部
Cisco Systems,Inc.
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

思科邮件安全插件 7.5.1 管理员指南

目 录

第 1 章

思科邮件安全插件使用入门

本章包含以下各节：

本版本中的新增内容

本版本包含以下新功能：

- **安全回复和安全转发** (*7.5*) - 在此版本中，如果公司帐户配置允许，“注册信封”(Registered Envelopes) 收件人可以使用加密方式转发并回复加密邮件。过去，只有“桌面加密”(Desktop Encryption) 帐户才能使用安全转发和回复功能。现在，“仅解密”(Decrypt Only) 帐户和“标记加密”(Flag Encryption) 帐户也将可以使用此功能。
- **报告市场营销邮件** (*7.5*) - 在此版本中，在向思科提供反馈时，您除了可以报告垃圾邮件、病毒和网络钓鱼攻击，还可以报告“市场营销”(Marketing) 邮件。

- **本地化信封** (*7.5*) - 在此版本中，您为用户界面选择的区域设置也将决定注册信封内容所使用的语言。当用户向使用相同区域设置的收件人发送邮件时，根据所选的下列区域设置，收件人将会收到经过本地化的注册信封：
  - 英语
  - 法语
  - 德语
  - 西班牙语
  - 葡萄牙语
  - 日语
  - 意大利语
- **收集使用数据** (*7.5*) - 您可以使思科邮件安全插件收集用于改进产品的匿名数据。
- **发送使用数据** (*7.5.1*) - 您可以通过设置 CommonComponentsConfig.xml 文件中的 callHomeAdminEnabled 参数，来配置是否向思科发送使用数据（启用或禁用）。
- **跟踪垃圾邮件报告** (*7.5.1*) - 您可以通过设置 BCE_Config 文件中的 copyAddressInPlainFormat 参数，来配置是否跟踪标记为垃圾邮件、病毒、网络钓鱼或市场营销的已报告邮件。垃圾邮件报告的副本将以纯文本格式发送到客户的邮箱地址。

支持的配置

*思科加密兼容性列表*列出了支持的操作系统，可以通过以下 URL 访问：

http://www.cisco.com/en/US/docs/security/iea/Compatibility_Matrix/IEA_Compatibility_Matrix.pdf

符合安全配置指南

思科邮件安全插件 7.5.1 已进行了测试，来确认其可在以下强化指南描述的配置和环境中运行：

- Microsoft 强化指南，使用 Microsoft 安全合规管理器 3.0.60 配置，位于：http://www.microsoft.com/en-us/download/details.aspx?id=16776
- NSA 安全配置指南，位于：https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml#microsoft

相关文档

要使用加密插件，您需要运行 Cisco IronPort 加密设备 (IEA) 并对其进行正确配置，使其能够与加密插件协同工作；或者，您需要拥有一个思科注册信封服务 (CRES) 帐户。如需了解如何配置 Cisco IronPort 加密设备 (IEA)，您可以参阅以下指南：

- *IronPort 加密设备安装指南*。此指南提供安装和配置邮件加密的说明，也可以帮助您了解如何配置加密设备的设置，以便使其与您配置的插件设置协同工作。要查找适用于您的版本的指南，请参阅：http://www.cisco.com/en/US/products/ps10154/prod_installation_guides_list.html

要更好地了解思科邮件安全插件的工作方式，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 AsyncOS for Email Security 用户指南*。此指南包含与垃圾邮件和病毒防护相关的信息。用户可以使用垃圾邮件和病毒插件改善 SenderBase 网络的效果。用户将邮件标记为“垃圾邮件”、“病毒”或“非垃圾邮件”时，他们可以逐渐使过滤器变得更高效并提升所有思科邮件安全设备 (ESA) 的性能。要查找适用于您的版本的指南，请参阅：http://www.cisco.com/en/US/products/ps10154/products_user_guide_list.html

如何使用本指南

将本指南作为了解有关思科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。您可从思科客户支持门户上获取本指南的电子版。您也可以访问设备 GUI 中的 HTML 在线帮助工具。

- 在 Outlook 2010/2013 中，点击功能区中的**插件选项 (Plug-in Options)** 按钮，或转至**文件 (File) > 选项 (Options) > 加载选项 (Add-in Options) > 思科邮件安全 (Cisco Email Security)**。
- 在 Outlook 2003/2007 中，点击功能区中的**插件选项 (Plug-in Options)** 按钮，或转至**工具 (Tools) > 选项 (Options) > 思科邮件安全 (Cisco Email Security) > 帮助 (Help)**。

哪里可以获得详细信息

思科提供以下资源用于了解思科邮件安全插件的更多信息。

安全培训服务与认证

思科安全培训服务提供针对思科安全产品和解决方案的出色教育和培训。通过一套有针对性的技术培训课程体系，该培训计划向不同的受众传授最新的知识和技能。

使用以下方法之一联系思科安全培训服务：

培训。有关注册、常见培训、证书和认证考试的问题：

- http://www.cisco.com/web/learning/le31/email_sec/index.html
- stbu-trg@cisco.com

思科支持社区

思科支持社区是一个面向思科客户、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，以咨询问题并与其他用户分享信息。

您可以通过以下 URL 访问思科支持社区：

https://supportforums.cisco.com

思科客户支持

注意 对您来说，可用的支持等级取决于您的服务等级协议。有关思科客户支持服务级别协议的详情，可参阅支持门户。查看该页面获取有关您的支持等级详情。

您可以全天随时通过电话、邮件或在线客服寻求支持。您可以通过以下方法之一联系思科客户支持：

- 思科支持门户网址：http://www.cisco.com/support
- 支持电话：在美国和加拿大，思科技术支持中心 (TAC) 的联系电话为 800-553-2447；世界其他国家/地区请参阅当地的电话号码。
- 邮箱地址：tac@cisco.com

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：

思科内容安全欢迎您的评论

思科内容安全技术出版物团队乐于提高产品文档的质量。我们欢迎您随时提出意见和建议。您可以将评论发送至以下邮件地址：

contentsecuritydocs@cisco.com

思科邮件安全插件概述

思科邮件安全插件添加报告和加密菜单到 Microsoft Outlook GUI。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，用户可以报告垃圾邮件、网络钓鱼和病毒邮件），加密插件会在工具栏上放入“加密消息”按钮，这使得用户可以从自己的邮件程序发送加密邮件，也可以在将要加密的邮件发送到机构外部之前，对其进行标记。

思科邮件安全插件安装时会启用 Microsoft Outlook 邮件客户端上的组件。这个单一接口允许您无缝地报告邮件或发送加密邮件。您可以锁定或解锁加密的邮件，添加或修改锁定原因。您还可以设置过期日期和已加密邮件时间。结合使用这些插件，可简化安装并提供单一接口，以供最终用户和管理员安装并修改。

报告和加密插件提供了方便的界面，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放入**加密消息 (Encrypt Message)** 按钮，以便发件人以邮件方式发送加密消息。

注意　加密插件需要配备思科邮件安全设备 (ESA) 并对其进行适当配置或拥有思科注册信封服务 (CRES) 帐户。

第 2 章

部署思科邮件安全插件

思科邮件安全插件框架支持多种思科邮件安全插件，包括报告插件和加密插件。

本章包含以下各节：

思科邮件安全插件的组件

思科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 邮件程序上部署思科邮件安全插件。部署思科邮件安全插件时，它会安装以下两个应用或其中一个：

- **报告插件**。报告插件使 Outlook 用户能够将有关未经请求或不需要的邮件（例如，垃圾邮件、病毒、网络钓鱼和营销邮件）的反馈提交至思科系统公司。有关详细信息，请参阅报告插件（第 2-2 页）。
- **加密插件**。加密插件会在邮件菜单栏中放置一个“加密邮件”(Encrypt Message) 按钮，以便发件人标记要加密的邮件。有关详细信息，请参阅加密插件（第 2-2 页）。

注意　加密插件需要配备思科邮件安全设备 (ESA) 并对其进行适当配置，或拥有思科注册信封服务 (CRES) 帐户。

报告插件

报告插件使 Outlook 用户能够将有关未经请求或不需要的邮件（例如，垃圾邮件、病毒、网络钓鱼和营销邮件）的反馈提交给思科。思科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) 按钮将误报（即合法邮件被标记为垃圾邮件）报告给思科。合法邮件通常被称为“ham”。思科使用关于误报的报告调整垃圾邮件过滤器，从而避免未来再次将合法邮件误归类。任何有效的邮件均可报告为**非垃圾邮件**，并且有助于提高过滤器效果。

此插件提供了便捷的界面，使您能够使用工具栏按钮和右键点击上下文菜单来提交反馈。报告消息时，将出现一个对话框，显示说明该消息已提交。自动化系统会利用您提交的邮件数据改善思科过滤器。提交邮件数据有助于减少收件箱中未经请求的邮件的数量。

加密插件

加密插件会在邮件消息菜单栏中放入**加密邮件 (Encrypt Message)** 按钮，以便发件人标记要在发送到组织外部之前进行加密和保护的邮件。

加密变量有两种类型：Flag 加密和桌面加密。利用 Flag 加密选项，您可以将邮件标记为需要加密，所标记的邮件在发出网络之前会由思科邮件安全设备 (ESA) 进行加密。桌面加密使您能够使用思科加密技术加密来自邮件程序内部的邮件。然后，它会从您的桌面发送已加密的邮件。如果想确保在组织*内部*发送的邮件得到加密，则可以使用桌面加密。

加密插件旨在与正常运行且配置好的 Cisco IronPort 加密设备 (IEA) 或思科邮件安全设备 (ESA)（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题。

安装思科邮件安全插件

若要针对多组用户安装思科邮件安全插件，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。有关执行无提示安装的说明，请参阅第 3 章“执行批量安装”。

配置模式

思科邮件安全加密插件的部署提供三个不同的配置模式。默认配置模式为仅解密。

要启用其他配置模式，需使用从管理员处接收的更新附件文件对 Outlook 邮件帐户进行配置。管理员会向最终用户的邮件帐户发送一个 BCE 配置文件附件（文件的默认名称是 *BCE_Config_signed.xml*）。最终用户收到此文件的名称将为 *securedoc.html* 文件。当最终用户点击 *securedoc.html* 附件时，Outlook 应用会检测到邮件随附的配置信息并应用更新的配置。

注意　默认信封名称为 *securedoc.html*。管理员可更改附件名称值，信封将反映最新指定的名称。

三个配置模式为：

- **仅解密** - 允许对接收的安全邮件进行解密。
- **解密和标记** - 允许对安全邮件进行解密和标记。标记选项允许最终用户将邮件标记为需要加密，所标记邮件在发出网络之前会由思科邮件安全设备 (ESA) 进行加密。服务器必须配置为检测标记的邮件并在服务器端对邮件进行加密。

- **解密和加密** - 允许对安全邮件进行加密和解密。

下表说明每个配置模式支持哪些功能。

特性	仅解密	解密和标记	解密和加密
发送加密邮件			X
标记邮件以进行加密		X	
打开加密邮件	X	X	X
回复/回复全部/转发邮件	X	X	X
邮件锁定和解锁	X	X	X
邮件过期	X	X	X
邮件诊断 （用于报告和加密插件）	X	X	X
阅读回执			X
信封设置			X
设置	X	X	X

通过思科注册信封服务 (CRES) 密钥服务器部署思科邮件安全插件

请按照以下说明部署思科邮件安全插件，以便直接与思科注册信封服务 (CRES) 密钥服务器配合使用。

步骤 1　登录您的 CRES 帐户：https://res.cisco.com/admin 并转到**帐户 (Accounts)** 选项卡。

步骤 2　选择要启用邮件安全插件的帐户，然后转到 **BCE 配置 (BCE Config)** 选项卡。

步骤 3　选择要与配置模板一起使用的令牌：

- **CRES** - 如果您的密钥服务器是 CRES，请选择此项。

步骤 4　点击**下载模板 (Download Template)** 下载模板文件并对其进行编辑。文件名为 *BCE_Config.xml*。

步骤 5　编辑此配置文件。

BCE_Config.xml 文件包含有关需要根据您的特定环境进行编辑的字段的详细说明。在文本编辑器中打开该文件并按照备注中的说明进行必要修改。

注意　出于本地化目的，请勿更改或改述现有的邮件安全标签“低”(Low)、“中”(Medium) 和“高”(High)。

步骤 6　点击**浏览 (Browse)** 导航至已编辑的 *BCE_Config.xml* 文件，找到文件后点击**上传和签名 (Upload and Sign)**。

配置文件经过签名后，已签名版本将以 *BCE_Config_signed.xml* 名称下载，除非其经过重命名。将此文件保存到您的本地计算机。

步骤 7　要一次将配置文件部署到许多最终用户，请使用**将签名的配置分发到批量列表 (Distribute Signed Configuration to Bulk List)** 选项。为实现此目的，请：

a. 浏览至步骤 6 中创建的签名的 BCE 配置文件。

b. 浏览至包含最终用户邮件地址的逗号分隔文件。

c. 根据需要更改邮件主题。

d. 点击**分发配置 (Distribute Config)**。

注意　如果 xml 配置文件转发给另一个最终用户，而非从管理员处接收，自动配置将不起作用并收到错误消息。

注意　不要将签名的 BCE 配置文件发送到邮件列表。CRES 不支持邮件列表。

通过 Cisco IronPort 加密设备 (IEA) 密钥服务器部署思科邮件安全插件

下载 IEA 密钥服务器令牌

配置签名过程中需要使用 IEA 令牌。在签名配置文件之前，将令牌下载到本地计算机。

要从 IEA 密钥服务器下载令牌文件，请按照下列步骤操作：

步骤 1　登录您的 IEA 管理控制台：https://<IEA_hostname>/admin。系统随即会显示管理控制台。

步骤 2　转到**帐户 (Accounts)** 选项卡。转到您的插件安装要使用的帐户。通常是**用户 (Users)** 帐户。

步骤 3　转到**令牌 (Tokens)** 选项卡。点击令牌右侧的“保存令牌”(Save Token) 图标（类似于带向下箭头的圆圈）并将其保存到您的本地计算机。

自定义和签名配置文件

IEA 令牌文件下载完成后，便可以自定义和签名配置文件。思科注册信封服务 (CRES) 是一项为思科加密技术提供支持的托管服务。由于插件配置文件签名验证由 CRES 系统执行，使用 IEA 作为密钥服务器并想要部署思科邮件安全插件的用户也将需要 CRES 的管理员帐户。如果您需要帮助来创建 CRES 管理员帐户，请与思科客户支持联系：
http://www.cisco.com/web/ironport/index.html

要创建与 IEA 密钥服务器一同使用的签名配置文件，请按照下列步骤操作：

步骤 1　登录您的 CRES 帐户：https://res.cisco.com/admin。系统随即会显示管理控制台。

步骤 2　转到**帐户 (Accounts)** 选项卡并选择要启用邮件安全插件的帐户。然后，转到 **BCE 配置 (BCE Config)** 选项卡。

步骤 3　选择 **IEA** 作为令牌类型，然后上传您之前从 IEA 下载的 IEA 令牌。

步骤 4　点击**下载模板 (Download Template)** 下载模板文件并对其进行编辑。文件名为 *BCE_Config.xml*。

步骤 5　编辑此配置文件。

BCE_Config.xml 文件包含有关需要根据您的特定环境进行编辑的字段的详细说明。在文本编辑器中打开该文件并按照备注中的说明进行必要修改。

注意　出于本地化目的，请勿更改或改述现有的邮件安全标签“低”(Low)、“中”(Medium) 和“高”(High)。

步骤 6　点击**浏览 (Browse)** 导航至已编辑的 *BCE_Config.xml* 文件，找到文件后点击**上传和签名 (Upload and Sign)**。

配置文件经过签名后，已签名版本将以 *BCE_Config_signed.xml* 名称下载，除非其经过重命名。将此文件保存到您的本地计算机。

将配置文件部署到最终用户

要将配置文件部署到最终用户，请将在 IEA 上加密的邮件中的签名配置文件发送给每个最终用户。发出邮件的邮件地址必须在 IEA 和 CRES 帐户上列为管理员。

注意　如果 xml 配置文件转发给另一个最终用户，而非从管理员处接收，自动配置将不起作用并收到错误消息。

注意　不要将签名的 BCE 配置文件发送到邮件列表。CRES 不支持邮件列表。

要使用签名的 BCE 配置文件执行批量安装，请参阅使用 BCE_Config.xml 文件进行批量安装（第 3-18 页）。

配置思科邮件安全插件的设置

安装思科邮件安全插件之后，您可以从 Outlook 中的“思科邮件安全” (Cisco Email Security) 选项卡执行配置更改操作。

- 在 Outlook 2010/2013 中，点击功能区中的**插件选项 (Plug-in Options)** 按钮，或转到**文件 (File) > 选项 (Options) > 加载项 (Add-ins) > 加载选项 (Add-in Options) > 思科邮件安全 (Cisco Email Security)**。
- 在 Outlook 2007 中，点击工具栏上的**插件选项 (Plug-in Options)** 按钮，或转到**工具 (Tools) > 选项 (Options) > 思科邮件安全 (Cisco Email Security)**。

您可以更改报告插件或加密插件的安装。或者，您也可以更改影响两个插件安装的常规选项。例如，您可以启用或禁用思科邮件安全加密插件的日志记录或修改特定加密模式的选项。

要更改标记邮件以进行加密的方式，您需要更改 *BCE_Config.xml* 文件并执行自动配置。任何指定的设置都必须与您的思科邮件安全设备 (ESA) 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 的思科邮件安全插件”。

思科邮件安全插件所需的系统进程

思科邮件安全插件只需要基本系统进程，例如 TCP/IP DNS、DHCP 等，这些进程无法禁用。但是，可以禁用任何非基础的系统进程，例如数据库管理器、HTTP 服务器和硬件配置守护程序，这不会影响思科邮件安全插件的功能。

思科邮件安全插件所需的 TCP 服务

思科邮件安全插件需要使用以下 TCP/IP 服务及其相关端口。这些端口必须保留为可用，以供 TCP/IP 服务使用。

- DNS（域名系统）。

  DNS 服务可以将互联网域名和主机名转换为 IP 地址。DNS 会自动将我们输入 Web 浏览器地址栏的名称转换为托管这些站点的 Web 服务器的 IP 地址。

  端口号：53 (TCP/UDP)

有关详细信息，请参阅：
http://en.wikipedia.org/wiki/Domain_Name_System

影响：高

解析：此服务必须允许所有最终用户访问。

- SMTP（简单邮件传输协议）

  简单邮件传输协议 (SMTP) 是一种互联网标准，用于跨互联网协议 (IP) 网络的邮件传输。

  端口号：SIP25、587、465、475、2525 (TCP)

  有关详细信息，请参阅：
  http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

  影响：高

  解析：此服务必须允许所有最终用户访问。

- DHCP（动态主机配置协议）

  DHCP 是一种网络协议，用于配置连接到网络（称为主机）的设备，以使它们使用互联网协议 (IP) 在网络上通信

  端口号：67、68 (TCP/UDP)

  有关详细信息，请参阅：
  http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

  影响：高

  解析：此服务必须允许所有自动从 DHCP 服务器获取 IP 地址的最终用户访问。

- Net BIOS over TCP/IP

  Net BIOS over TCP/IP（NBT，有时称为 NetBT）是一种网络协议，允许在现代 TCP/IP 网络上使用依赖 NetBIOS API 的传统计算机应用。

  端口号：137(UDP)（名称服务）、138(UDP)（数据报服务）、139(TCP)（会话服务）

  有关详细信息，请参阅：
  http://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP

  影响：高

  解析：此服务必须允许所有最终用户访问。

- HTTP（超文本传输协议）

  超文本传输协议 (HTTP) 是一种应用于分发、协作、超媒体信息系统的应用协议。

  端口号：SIP80、8080 (TCP)

  有关详细信息，请参阅：
  http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

  影响：高

  解析：此服务必须允许所有最终用户访问。

- HTTPS（安全超文本传输协议）

  HTTPS 是一种计算机网络安全通信协议，在互联网上的部署尤为广泛。

  端口号：443 (TCP)

  有关详细信息，请参阅：
  http://en.wikipedia.org/wiki/HTTP_Secure

  影响：高

  解析：此服务必须允许所有最终用户访问。

- IMAP（互联网消息访问协议）

  互联网消息访问协议允许邮件客户端在远程邮件服务器上访问邮件。

  端口号：143、993 (TCP)

  有关详细信息，请参阅：
  http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

  影响：高

  解析：此服务必须允许所有最终用户访问。

- POP3（邮局协议）

  邮局协议是本地邮件客户端用于通过 TCP/IP 连接从远程服务器检索邮件的协议。

  端口号：110、995 (TCP)

  有关详细信息，请参阅：
  http://en.wikipedia.org/wiki/Post_Office_Protocol

  影响：高

  解析：此服务必须允许所有最终用户访问。

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，包含以下部分：

执行安装

要执行安装，请完成以下步骤以创建网络共享文件夹、分发软件包、新建软件包向导和新建程序向导。

要执行安装，请按照下列步骤操作：

步骤 1 下载安装程序包并验证校验和。

a. 使用以下 URL 的 Quick Hash GUI 和 SHA512 散列算法为您的安装程序包生成校验和：

http://sourceforge.net/projects/quickhash/

b. 验证生成的校验和是否与以下内容匹配：

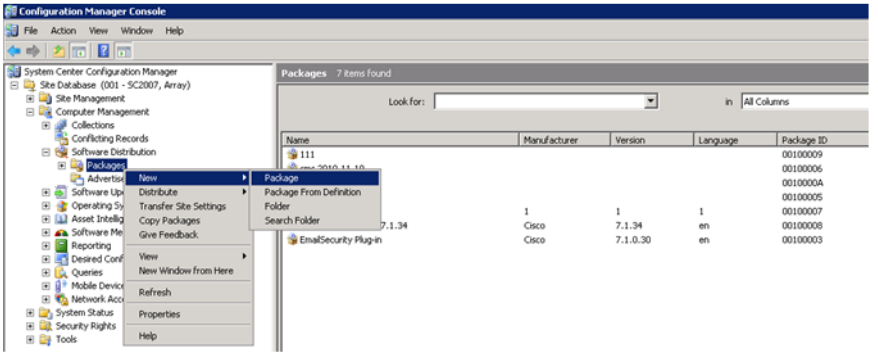
29CC5346F59592866CADCFE3E6DE455C3E95849CBF7C3FE83D78C3E0ED409B2620DC35E8DE01D809CA4B4D8AF698B3BC4468058B54339EF554B4C844852191ED

步骤 2　创建包含安装程序包的网络共享文件夹，并向用户提供该共享文件夹的访问权限。

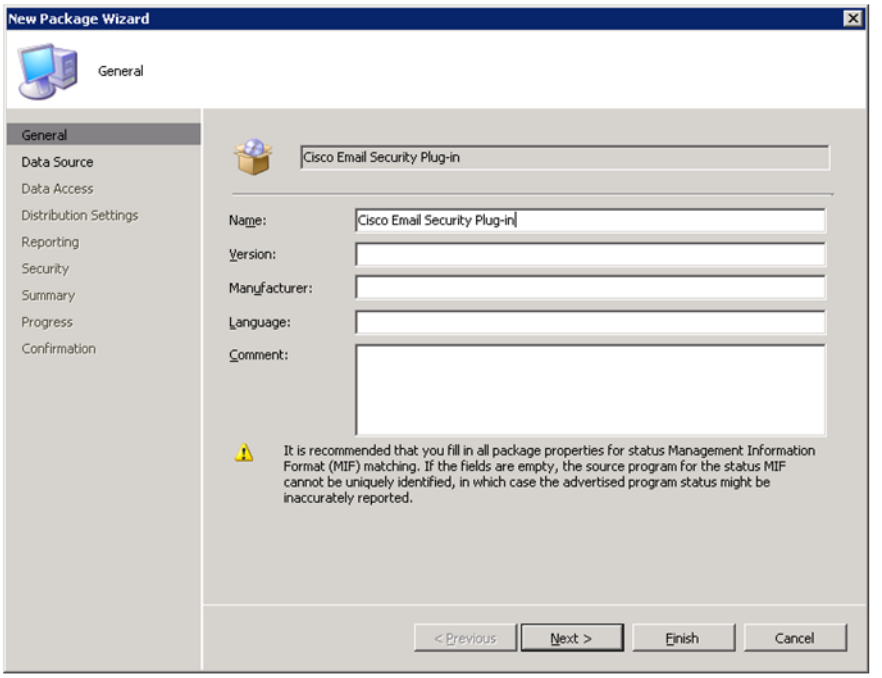
注意　您无法从 Dropbox、网络驱动器或共享系统文件夹执行安装。

步骤 3　打开 SCCM 管理工具。

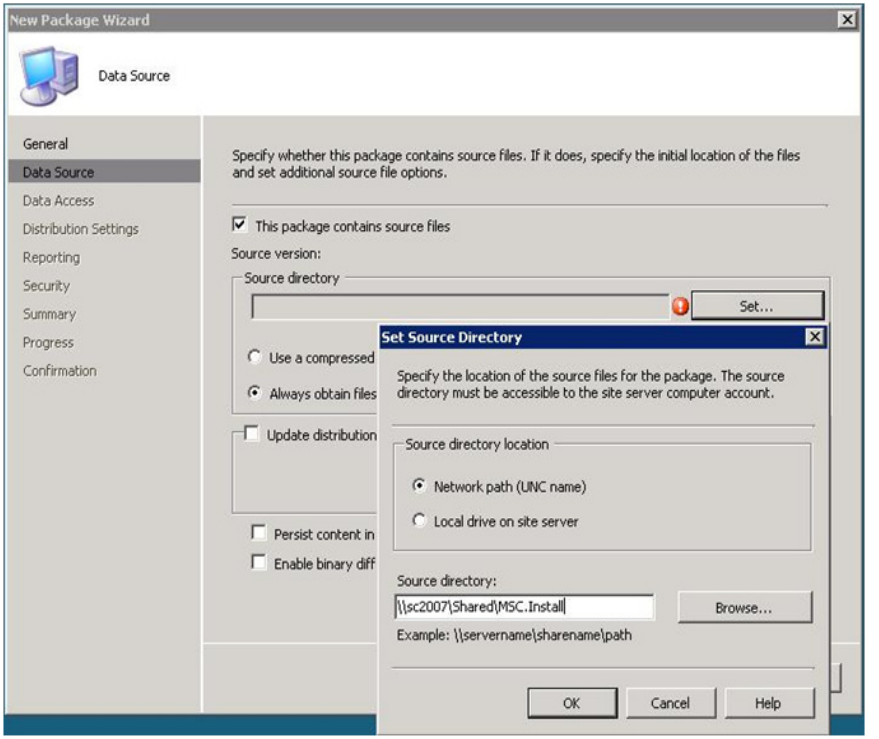
步骤 4　创建新的软件分发包。



步骤 5　为此包输入名称，并点击**下一步 (Next)**。

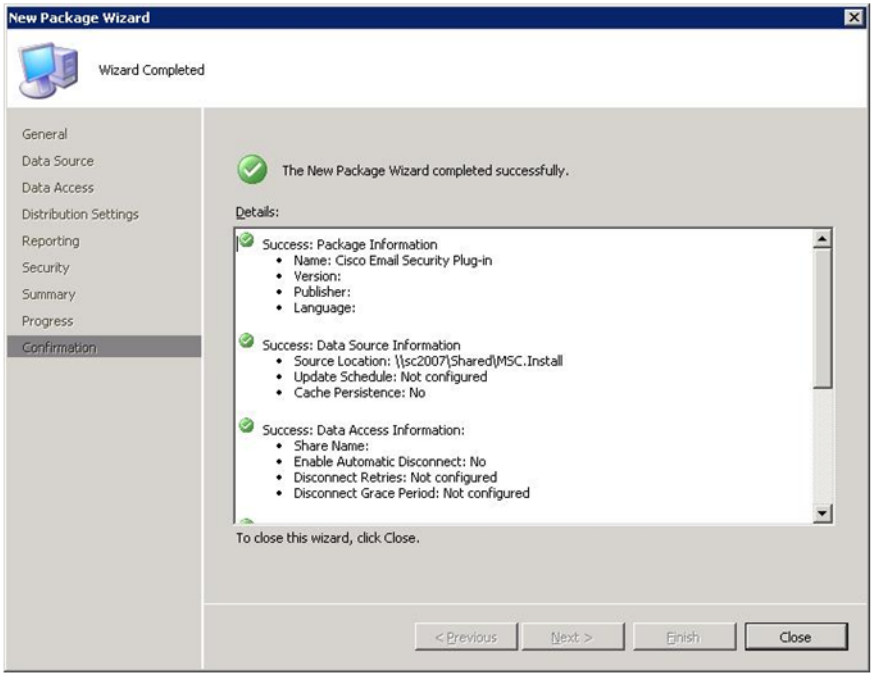


步骤 6　输入指向网络共享文件夹的路径，以指定在步骤 2 中创建的网络源目录。您可以输入路径或浏览该文件夹。点击**下一步 (Next)**。

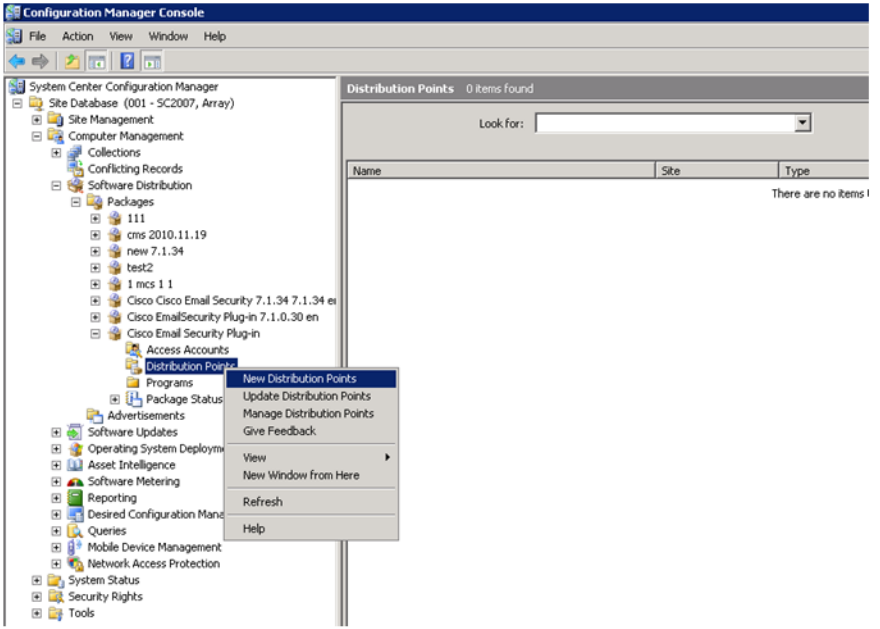


步骤 7　继续执行新建软件包向导中的下一步，并点击**下一步 (Next)**。

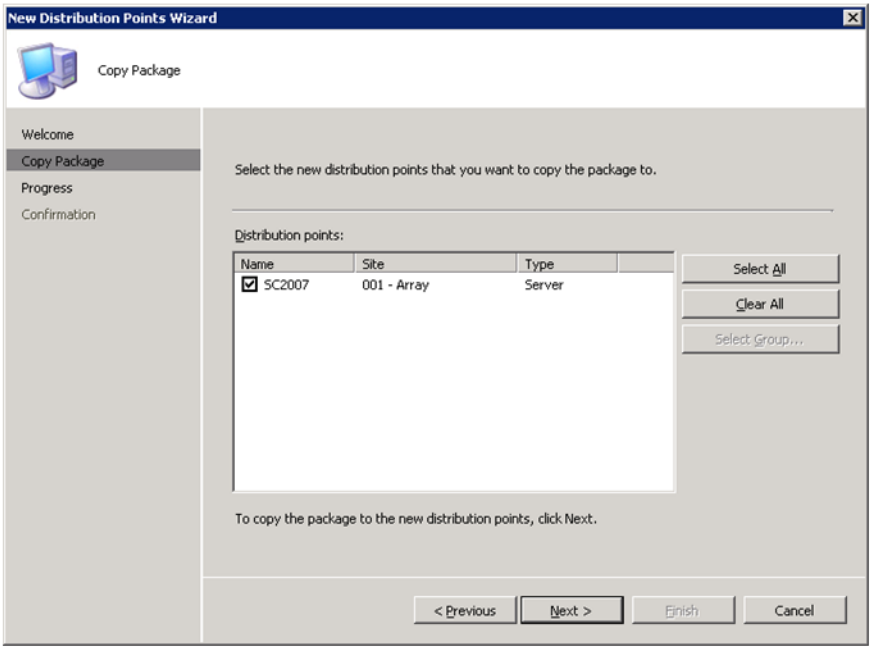
步骤 8　查看显示新建软件包向导已成功完成的确认消息，然后点击**关闭 (Close)**。



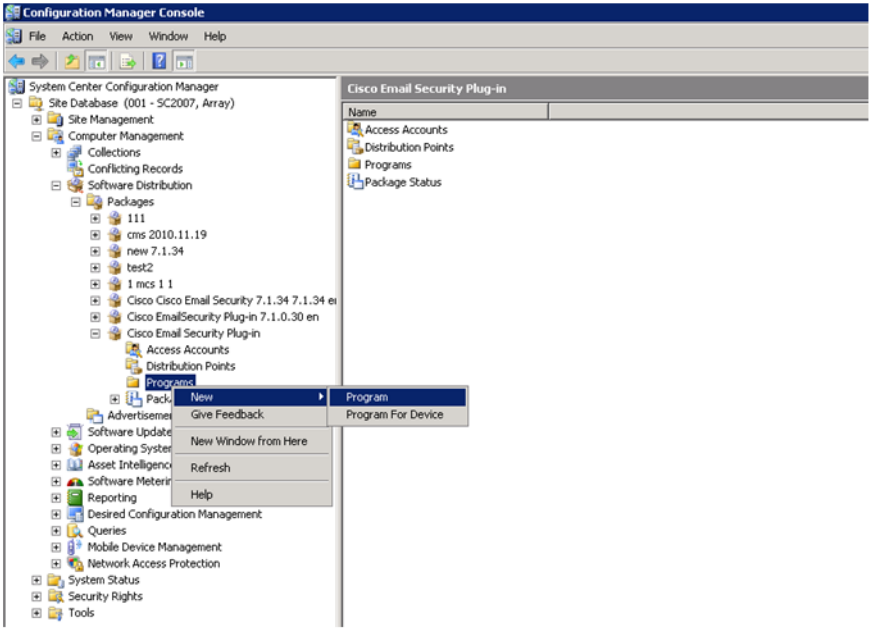
步骤 9　创建新的分发点，并点击“欢迎”(Welcome) 页面上的**下一步 (Next)**。



步骤 10　选择新的分发点。点击浏览新建分发点向导中的后续页，然后点击**关闭 (Close)**。

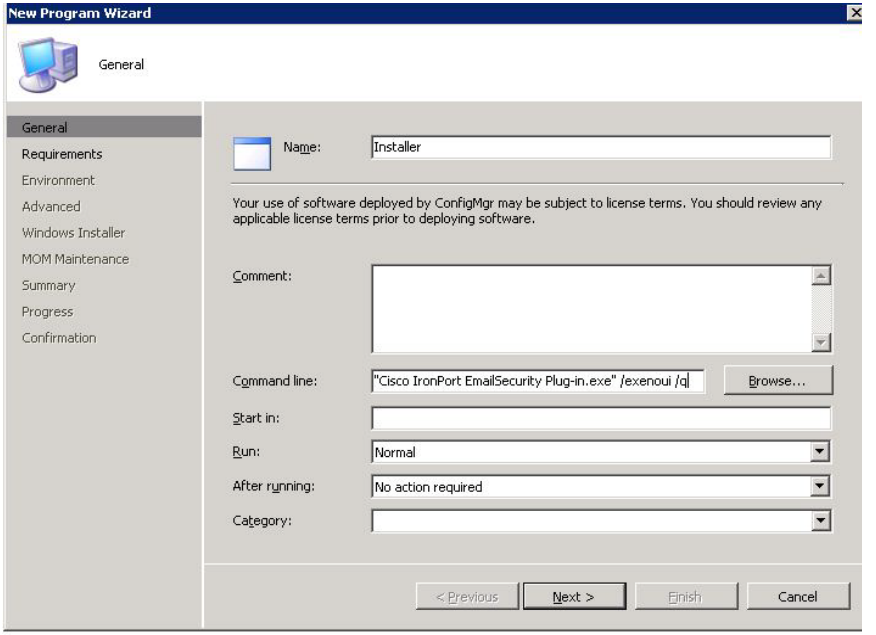


步骤 11　创建新程序。



步骤 12　在命令行字段中，输入以下命令：*{共享网络路径}\Cisco Email Security Plug-in.exe /exenoui /qn*

例如：*\\sc2007\Shared\Cisco Email Security Plug-in.exe /exenoui /qn*，其中 *\\sc2007\Shared\Cisco Email Security Plug-in.exe* 是网络共享文件夹中的 .exe 文件的完整网络路径。



注意　如果您希望使用自定义配置文件，则需要在此步骤中添加一个使安装使用该自定义文件的特殊值。您可以使用以下语法从命令行添加该特殊值（在 = 符号后指定自定义配置文件位置）：

Cisco Email Security Plug-in.exe /exenoui /qn UseCustomConfig="||sc2007|Shared|config|"

有关自定义配置文件的详细信息，请参阅使用自定义配置文件，第 3-16 页。

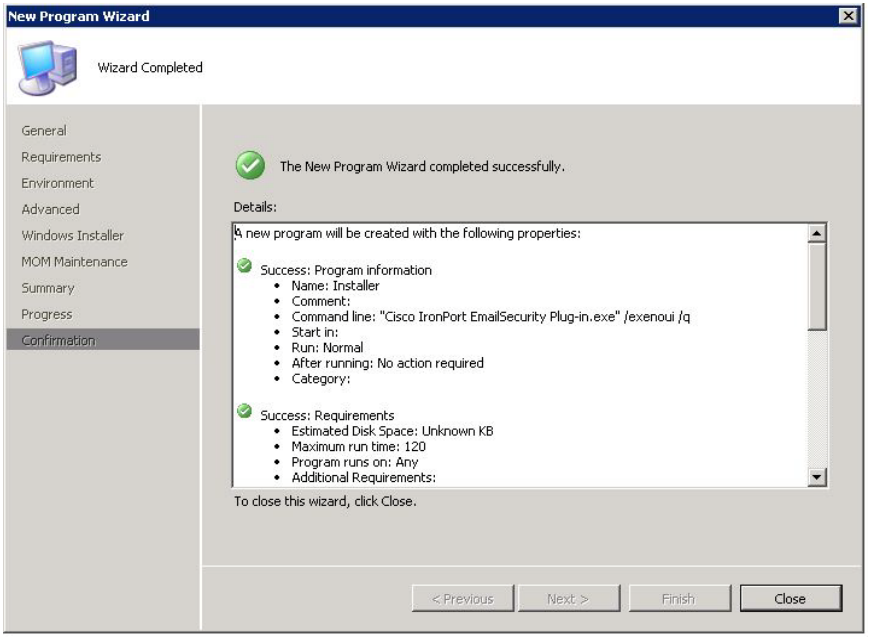
步骤 13　在**运行 (Run)** 字段中，输入 **Hidden**，然后点击**下一步 (Next)**。

步骤 14　点击浏览要求页面，然后点击**下一步 (Next)**。

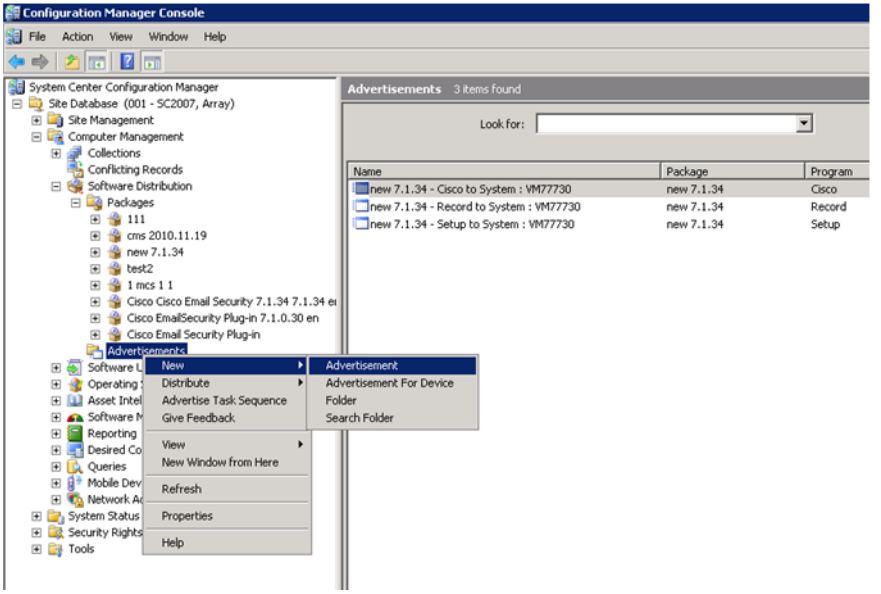
步骤 15　选择以下环境选项：

- **程序可运行　(Program can run)**：仅限于用户登录时。如果“运行模式”(Run mode) 设置为管理权限，则可将**程序可运行 (Program can run)** 设置为**每当用户登录时 (Whenever the user is logged on)**。
- **运行模式 (Run mode)**：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。

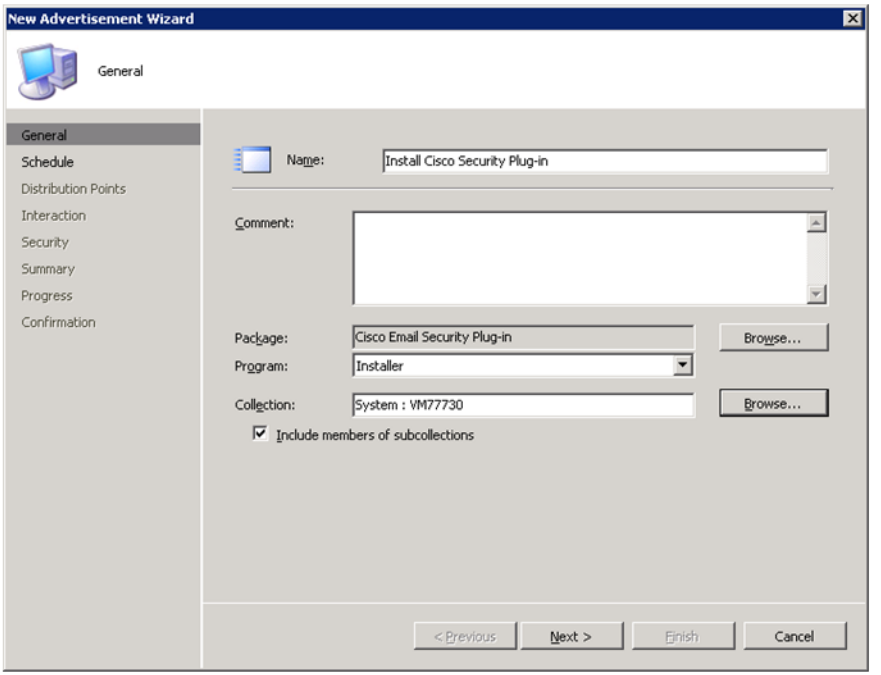
步骤 16　确认新建程序向导已成功完成，然后点击**关闭 (Close)**。



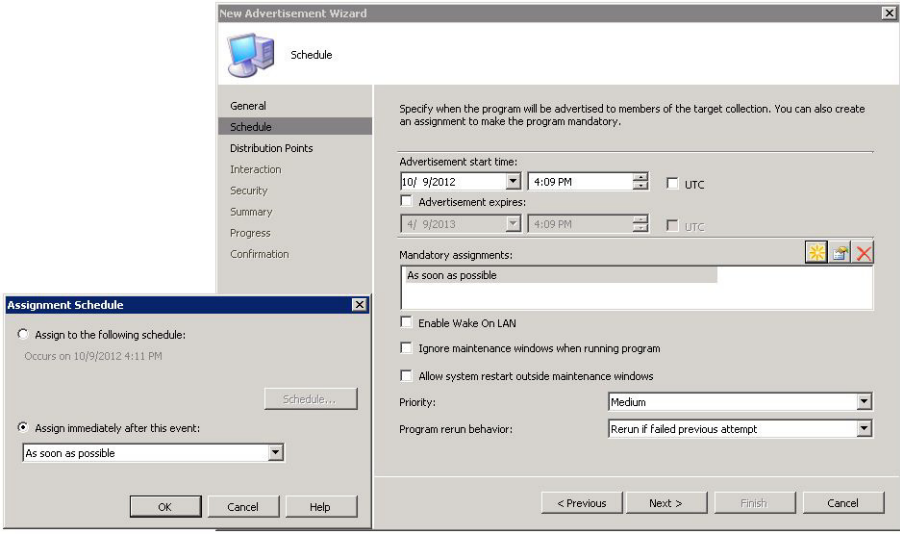
步骤 17　创建新通告。


Configuration Manager Console
File Action View Window Help
System Center Configuration Manager
Site Database (001 - SC2007, Array)
Site Management
Computer Management
Collections
Conflicting Records
Software Distribution
Packages
111
cms 2010.11.19
new 7.1.34
test2
1 mcs 1 1
Cisco Cisco Email Security 7.1.34 7.1.34 en
Cisco EmailSecurity Plug-in 7.1.0.30 en
Cisco Email Security Plug-in
Advertisements
Reporting
Queries
System Status
Security Rights
Tools
New
Distribute
Advertise Task Sequence
Give Feedback
View
New Window from Here
Refresh
Properties
Help
Advertisement
Advertisement For Device
Folder
Search Folder
Advertisements 3 items found
Look for:
Name
Package
Program
new 7.1.34 - Cisco to System : VM77730
new 7.1.34 - Record to System : VM77730
new 7.1.34 - Setup to System : VM77730
new 7.1.34
Cisco
Record
Setup

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)**。



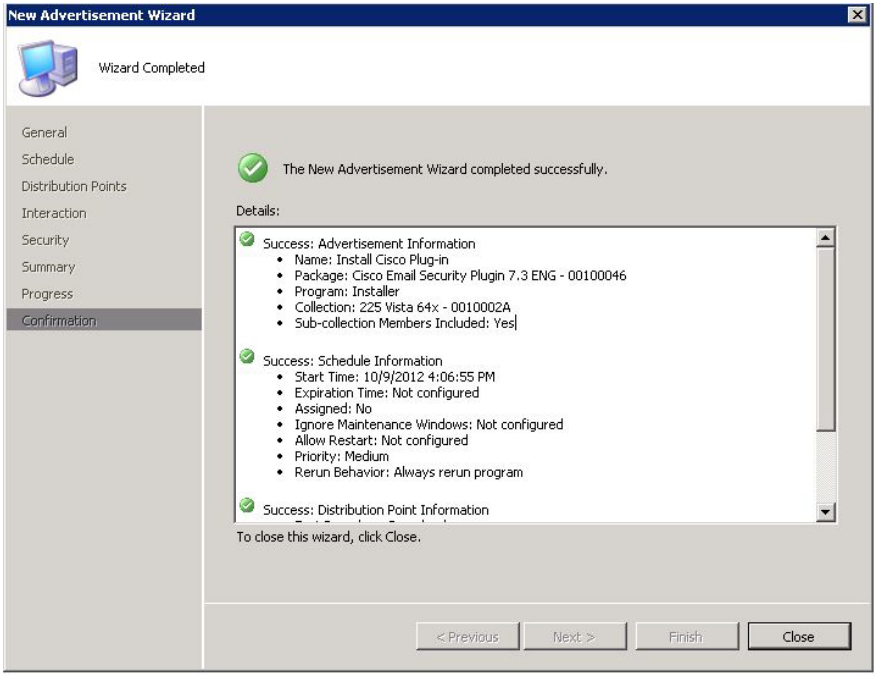
步骤 19　设置强制分配。点击**下一步 (Next)**。



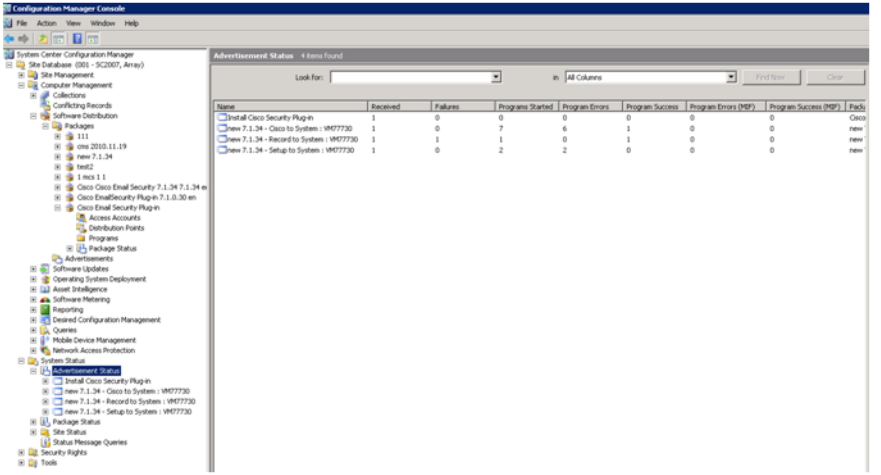
步骤 20　根据您的偏好选择选项。至少应设置一个强制分配。但不要选择**不运行程序 (Do Not Run Program)**，因为如果连接速度较慢，程序将不会启动。点击**下一步 (Next)**。

步骤 21　点击浏览新建通告向导，然后点击**下一步 (Next)**。

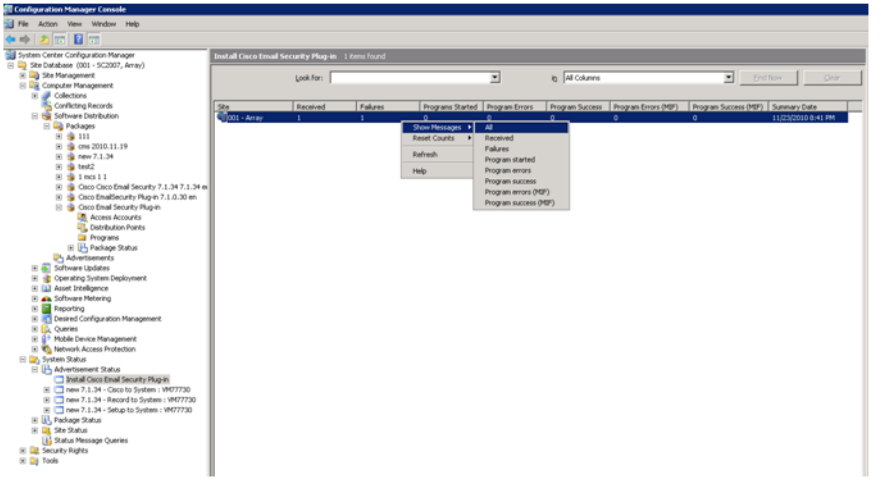
步骤 22　查看显示新建通告向导已成功完成的确认消息，然后点击**关闭 (Close)**。



步骤 23　在“通告状态”(Advertisement Status) 窗口中查看通告状态。



步骤 24　您可以通过从上下文菜单依次选择**显示邮件 (Show Message) > 全部 (All)** 创建通告报告，以查看更多详细信息。如果出现错误，您可以核查该报告以了解出现错误的位置。



使用自定义配置文件

思科邮件安全插件允许通过编辑包含在安装中的 XML 文件集来修改默认配置。您可能希望使用不同的配置文件更改部分安装。例如，在 config_1.xml 配置文件中，您可以更改一些加密选项，例如文件标记方法（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 config_1.xml 配置文件的报告组件部分，您可以更改部分默认选项，例如报告的邮件大小最大值或者是否在报告文件后保留文件副本。此外，您可能还希望自定义按钮名称，甚至可能希望本地化用户界面中的文本。

概述

要修改并部署自定义配置文件，请完成以下步骤：

步骤 1　复制 **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In** 目录。必须包含“常见”(Common) 文件夹。

注意　必须保持原始文件的目录结构以保证有效性。确保从 **Cisco IronPort 邮件安全插件 (Cisco IronPort Email Security Plug-in)** 目录开始的结构得到保持并包含所有带配置文件的文件。

步骤 2　编辑 XML 配置文件。思科建议您不要创建新文件，而是修改包含在安装文件中的 XML 文件。有关修改这些文件的说明，请参阅编辑 XML 配置文件，第 3-17 页。

步骤 3　按照执行安装，第 3-1 页所述运行批量安装，并按照部署自定义配置文件，第 3-20 页所述部署自定义 XML 文件。

编辑 XML 配置文件

安装 思科邮件安全插件时，会创建配置数据并保存在 XML 文件中。您可以编辑字符串值以自定义参数值。但是，思科建议您不要删除值或修改文件结构。

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

%allusersprofile%|Cisco|Cisco IronPort Email Security Plug In

XML 文件位于以下默认位置：

- **\\%allusersprofile%\Cisco\Cisco IronPort Email SecurityPlug-In\Common\config_1.xml, config_{N}.xml。** 这些数字取决于用户帐户的计数。包含与桌面加密插件和报告插件相关的配置数据，例如可报告的邮件大小最大值。思科建议您不要修改报告设置。
- **\\%allusersprofile%\Cisco\Cisco IronPort Email SecurityPlug-In\Common\CommonComponentsConfig.xml。** 包含报告和加密插件常用的基本配置数据，例如日志文件位置和本地化文件名称（*en.xml* 是默认的本地化文件）。您可以使用邮件程序设置更改日志文件位置，并与批量安装程序一起部署。如果您希望创建不同于可用本地化文件语言的本地化文件，则需要在此处引用新 XML 文件名称。
- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\Localization\en.xml**。包含与本地语言相关的数据。默认语言为英语。但是，还有其他几个本地化文件，包括 *de.xml*、*es.xml*、*fr.xml*、*it.xml*、*zh.xml*、*pt.xml* 和 *ja.xml*。如果您希望使用除以上 xml 文件之外的语言，可以创建自定义 xml 文件并将其引用在 CommonConfig.xml 文件中。

注意 请勿更改 < 或 > 符号内的任何字符串 ID，因为这样做会使插件运行不正常。

示例

以下是 *en-US.xml* 文件的更改示例。

要更改报告工具栏中的文本，请找到 *en-US.xml* 文件的以下部分并编辑粗体文本：

```
<group name="Mso.Report.Button.Cations">
 <string id="blockSender">Block Sender</string>
 <string id="spam">Spam</string>
```

```
 <string id="ham">Not Spam</string>
 <string id="virus">Virus</string>
 <string id="phish">Phish</string>
</group>
```

例如，如果您希望添加更多说明性标题，可以更改如下显示的文本。

```
<group name="Mso.Report.Button.Cations">
 <string id="blockSender">Block Sender using Outlook</string>
 <string id="spam">Report Spam</string>
 <string id="ham">Report Not Spam</string>
 <string id="virus">Report Virus</string>
 <string id="phish">Report Phishing Attacks</string>
</group>
```

使用 BCE_Config.xml 文件进行批量安装

要使用 BCE_Config.xml 文件执行批量安装，请按照下列步骤操作：

步骤 1　导航至 **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common** directory。

步骤 2　删除 *config_1.xml 文件*（如果存在）。

步骤 3　将 BCE 配置文件（默认名称为 *BCE_Config_signed.xml*）复制到此目录并将该文件重命名为 *config_1.xml*。

步骤 4　导航至 **\\%allusersprofile%\Cisco\Cisco IronPort Email SecurityPlug-In\CommonComponentsConfig.xml** 文件。

步骤 5　验证 *CommonComponentsConfig.xml* 文件是否包含以下标签：

```
 <accountFileNames>
    <accountFileName filePath="config_1.xml"
emailAddressAndKeyServer="*" />
  </accountFileNames>
```

提示　确保 `accountFileName` 标签不包括 `profileName` 属性。如果该属性存在，请将其删除。

注意　要仅配置特定域中选定的用户，您需要指定该域为邮件地址，以此修改 *CommonComponentsConfig.xml* 文件。

例如，要将 BCE 配置文件仅应用到思科用户，请将：

```
<accountFileName filePath="config_1.xml"
emailAddressAndKeyServer="*" />
```

更改为：

```
<accountFileName filePath="config_1.xml"
emailAddressAndKeyServer="@cisco.com" />
```

如果有多个 `accountFileName` 标签，则 `filePath` 将为 config_2.xml、config_3.xml 等。

例如：

```
<accountFileName filePath="config_2.xml"
emailAddressAndKeyServer="@cisco.com" />
```

步骤 6　按照执行安装，第 3-1 页所述运行批量安装，并按照部署自定义配置文件，第 3-20 页所述部署自定义 XML 文件。

注意　必须将 **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common** 目录内容复制到 **\\{SHARED_DIR}\{CONFIG_FOLDER}**。{CONFIG_FOLDER} 中必须存在“常用”(Common) 文件夹。UseCustomConfig 命令参数可以使安装使用您已修改的自定义配置文件。

部署自定义配置文件

完成编辑配置文件后，您将需要在部署期间添加一个特殊值，以确保安装程序使用经修改的自定义配置文件。**UseCustomConfig** 命令行参数可以使安装使用自定义配置文件，并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。

您可以使用以下语法，在执行批量安装的步骤 12 期间（请参阅执行安装，第 3-1 页）从命令行添加 **UseCustomConfig** 值：

```
Cisco Email Security Plugin.exe /exenoui /qn
UseCustomConfig="\\{SHARED_DIR}\{CONFIG_FOLDER}
```

其中，= 后面的路径指定指向自定义配置文件的路径。

其他命令

除 UseCustomConfig 外，您还可以使用以下命令：

- AppDir="C:\CustomInstallDir" - 指定自定义目标目录。
- SkipReporting="TRUE" - 禁用即将开始的安装的报告插件。
- SkipEncryption="TRUE" - 禁用即将开始的安装的加密插件。

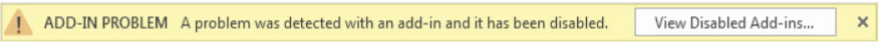
第 4 章

配置和使用适用于 Outlook 的思科邮件安全插件

本章介绍适用于 Outlook 的思科邮件安全插件中的可用功能。思科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。本章包含以下各节：

启用思科邮件安全插件

您在安装后首次启动思科邮件安全插件时，它可能被 Outlook 禁用。如果是这种情况，您会看到以下消息：



要启用思科邮件安全插件，请点击通知栏上的**查看禁用的加载项 (View Disabled Add-ins)** 按钮，以显示“禁用的加载项”(Disabled Add-ins) 对话框。要将 Outlook 配置为始终允许该加载项运行而无论其启动时需要多长时间，请点击**始终启用此加载项 (Always enable this add-in)** 按钮。

配置使用情况数据的发送

当思科邮件安全插件首次启动时，系统会询问您是否要允许将匿名数据发送到思科以帮助改进产品。如果您选择**向思科发送匿名使用情况数据 (Send anonymous usage data to Cisco)** 复选框，系统将收集以下两种类型的信息并将其存储在思科服务器上供分析使用：

- 关于正在运行插件的计算机的一般信息
- 特定于帐户的信息

此信息的详情如下所述。

在启动后，您可以通过选择**插件选项 (Plug-in Options) > 其他选项 (Additional Options) > 发送使用情况数据 (Sending usage data)** 选项卡，启用或禁用发送使用情况数据。

要启用或禁用将使用情况数据发送到思科，请在 CommonComponentsConfig.xml 文件中设置以下参数：

- callHomeAdminEnabled - 设置为 true 或 false 以在 Outlook 启动时启用或禁用发送使用情况数据。默认值为 true。若设置为 false，用户将不会收到有关使用情况数据收集的通知，并不能将匿名使用情况数据发送到思科。

一般信息

收集的信息包括：

- 标识符 (UUID) - 首次安装插件时生成的非永久标识符。它只用于关联使用情况报告，以便可以跟踪一段时间内的使用情况数据。您可以重置标识符，方法是选择**插件选项 (Plug-in Options) > 其他选项 (Additional Options) > 隐私 (Privacy)** 选项卡。
- 操作系统的版本
- Microsoft Outlook 的版本
- 思科 Outlook 插件的版本
- 思科加密 SDK 的版本 - 此 SDK 是插件在内部使用的库，用于对安全邮件进行加密和解密。
- 操作系统使用的语言
- 所有已安装的 Outlook 插件的名称

特定于帐户的信息

收集的信息包括：

- 帐户类型 - 类型为加密、解密或标记。
- 服务器
- 收件人数量 - 自安装以来在加密期间添加的收件人数量，包括在标记期间添加的收件人。
- 已解密的数量 - 已使用插件解密的邮件数量。
- 已加密的数量 - 自安装以来已在设备上加密的邮件数量，包括已标记的邮件数量。
- 管理邮件次数 - 已访问“管理邮件”(Manage Messages) 屏幕的次数。
- 管理邮件使用计数 - 使用“管理邮件”(Manage Messages) 屏幕更新的邮件数量。
- 是否正在使用非标准的报告地址。

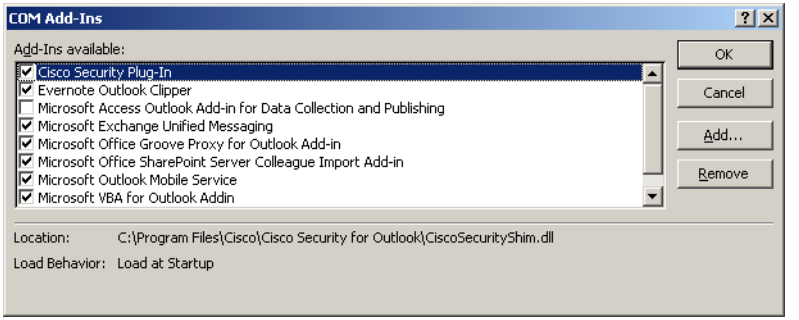
适用于 Outlook 的思科邮件安全插件常规设置

思科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。可从“选项”(Options) 页配置思科邮件安全插件的常规设置。

启用或禁用

在默认情况下，思科邮件安全插件会在安装时启用。可从以下位置禁用思科邮件安全插件：

- 在 Outlook 2010/2013 中，转到**文件 (File) > 选项 (Options)**，然后从左侧导航栏选择**加载项 (Add-ins)**。然后，从页面底部的“管理”(Manage) 下拉菜单选择 **COM 加载项 (COM Add-ins)**，并点击**转到 (Go)**...
- 在 Outlook 2007 中，转到**文件 (File) > 信任中心 (Trust Center)**，然后从左侧导航栏选择**加载项 (Add-ins)**。然后，从页面底部的**管理 (Manage)** 下拉菜单选择 **COM 加载项 (COM Add-ins)**，并点击**转到 (Go)**。



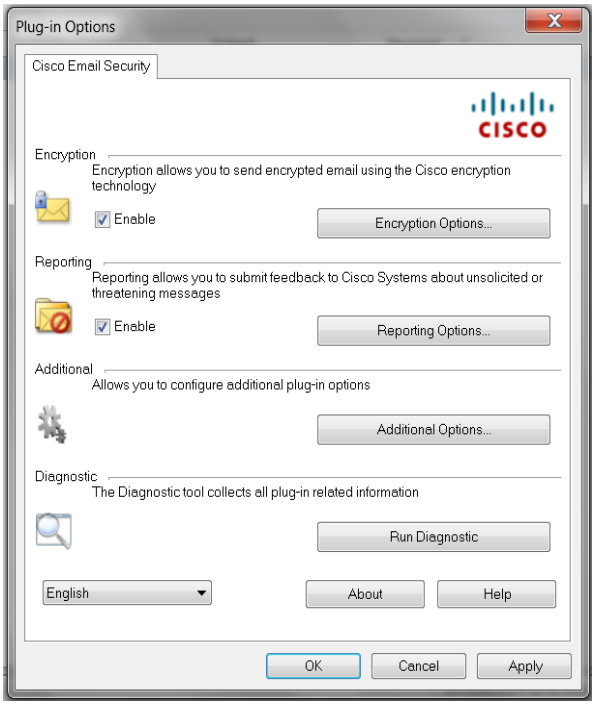
从“COM 加载项”(COM Add-Ins) 窗口，清除“思科邮件安全插件”(Cisco Email Security Plug-in) 复选框，然后点击**确定 (OK)**。

配置 Outlook 插件的基本设置

最终用户可以从“思科邮件安全”(Cisco Email Security) 选项卡配置基本设置。

- 在 Outlook 2010/2013 中，点击功能区中的**插件选项 (Plug-in Options)** 按钮，或转到**文件 (File) > 选项 (Options) > 加载项 (Add-ins) > 加载选项 (Add-in Options) > 思科邮件安全 (Cisco Email Security)**。
- 在 Outlook 2007 中，点击工具栏上的**插件选项 (Plug-in Options)** 按钮，或转到**工具 (Tools) > 选项 (Options) > 思科邮件安全 (Cisco Email Security)**。

“思科邮件安全”(Cisco Email Security) 选项卡：



从此选项卡中，最终用户可选择合适的**启用 (Enable)** 复选框，启用加密和报告选项。最终用户也可以选择**其他选项...(Additional Options...)** 按钮来启用其他选项。要进一步配置设置，请点击**加密选项...(Encryption Options...)**、

报告选项...(Reporting Options...) 或**其他选项...(Additional Options...)** 按钮。最终用户还可以在解决问题时使用诊断工具运行有关思科邮件安全插件的报告，并发送至思科支持部门。您还可以将插件配置为在 Outlook 启动时将匿名使用信息（有关插件使用的一般信息）发送到服务器。

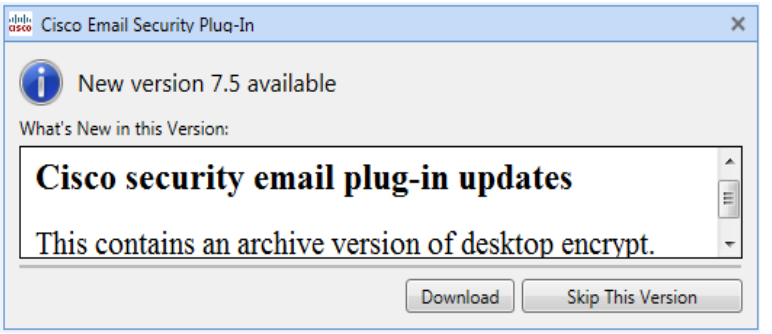
将 Outlook 插件配置为检查更新

要将插件配置为自动检查更新，请设置 CommonComponentsConfig.xml 文件的 checkForUpdates 部分中的以下参数：

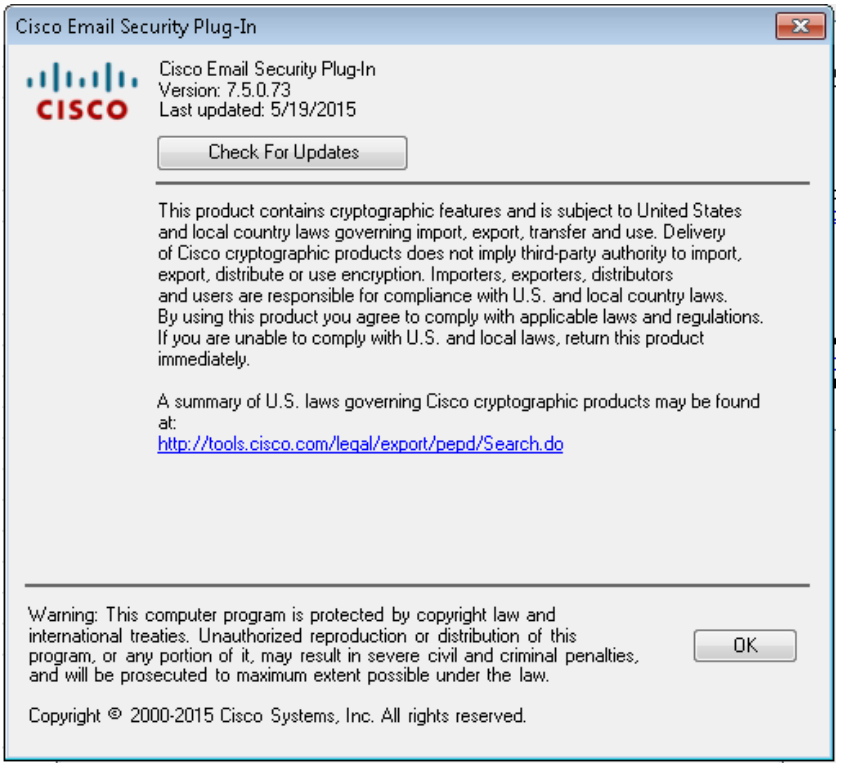
- checkAutomatically - 设置为 true 或 false 以在 Outlook 启动时启用或禁用自动检查更新。默认值为 true。
- serverURL - 设置为插件将用于检查是否有新版本可用的 URL。
- ignoredVersion - 设置为您希望插件在查找更新时忽略的版本号。

更新通知

如果桌面加密插件配置为自动检查更新，而且桌面加密插件当前不是最新版本，则 Outlook 启动时会显示以下对话框：



要在 Outlook 启动后检查更新，请在“插件选项”(Plug-in Options) 窗口中点击“关于”(About) 按钮，然后在以下对话框中点击“检查更新”(Check for updates) 按钮：



使用 BCE_Config 文件配置常用选项

所有 Outlook 帐户和整个插件的常见选项均包含在 CommonComponentsConfig.xml 文件中。这些选项包括：

- diagnosticSupportAddress - 指定诊断工具运行时所发送消息的收件人邮件地址。该消息包含诊断工具的输出。
- diagnosticReportSubject - 指定诊断工具运行时所发送消息的主题。
- showPluginOptions - 指定发现更新时是否显示对话框，从而让您选择是否应用一般设置。
- checkAutomatically - 设置为 true 或 false 以在 Outlook 启动时启用或禁用自动检查更新。默认值为 true。有关详细信息，请参阅“将 Outlook 插件配置为检查更新”一节，第 4-6 页。
- serverURL - 设置为插件将用于检查是否有新版本可用的 URL。
- callHomeAdminEnabled - 设置为 true 或 false 以在 Outlook 启动时启用或禁用发送使用情况数据。默认值为 true。有关详细信息，请参阅“配置使用情况数据的发送”一节，第 4-2 页。

在插件应用 BCE_Config.xml 的情况下，如果这些选项在 BCE_Config.xml 文件中进行了配置，这些配置会复制到 CommonComponentsConfig.xml 中。否则，要在用户环境中修改**这些选项**，您必须使用 UseCustomConfig 选项执行批量安装。有关详细信息，请参阅“使用 BCE_Config.xml 文件进行批量安装”一节，第 3-18 页。

按同样的方式，您也可通过应用 BCE_Config 来配置帐户特定文件（config_1.xml、config_2.xml 等）中的选项。但是，您无法使用 BCE_Config.xml 文件配置日志记录设置或插件本地化。

报告不需要的垃圾邮件、营销邮件、病毒和网络钓鱼攻击

报告插件允许最终用户向思科报告收到的邮件是垃圾邮件、营销邮件、网络钓鱼攻击还是病毒。最终用户还可以报告被错误分类为垃圾邮件的邮件（有时也称为“ham”）。

最终用户可以通过 Outlook 中的“选项”(Options) 页启用适用于 Outlook 的思科邮件安全报告插件。要启用报告，请执行以下操作：

- 在 Outlook 2010/2013 中，点击功能区中的**插件选项 (Plug-in Options)** 按钮，或转到**文件 (File) > 选项 (Options) > 加载项 (Add-ins) > 加载选项 (Add-in Options) > 思科邮件安全 (Cisco Email Security)**。 选择“思科邮件安全”(Cisco Email Security) 选项卡的“报告”(Reporting) 字段中的**启用 (Enable)** 复选框。
- 在 Outlook 2007 中，点击工具栏上的**插件选项 (Plug-in Options)** 按钮，或转到**工具 (Tools) > 选项 (Options) > 思科邮件安全 (Cisco Email Security)** 选项卡。选择“思科邮件安全”(Cisco Email Security) 选项卡的“报告”(Reporting) 字段中的**启用 (Enable)** 复选框。

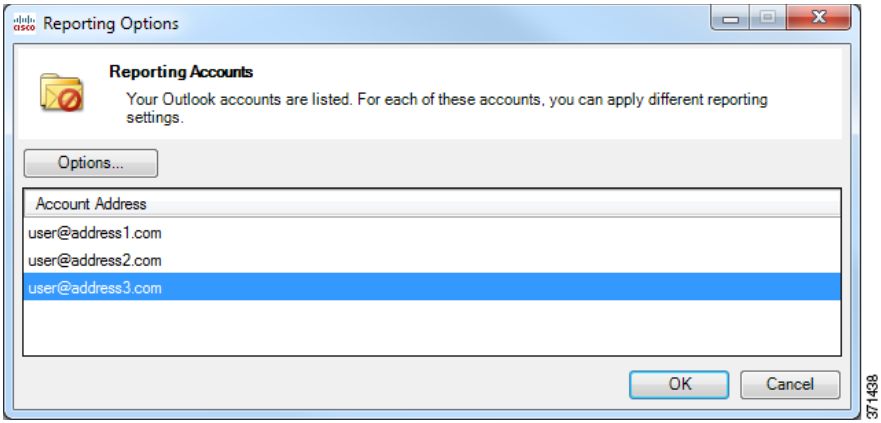
报告选项

报告设置位于“思科邮件安全”(Cisco Email Security) 页。要修改报告设置，请执行以下操作：

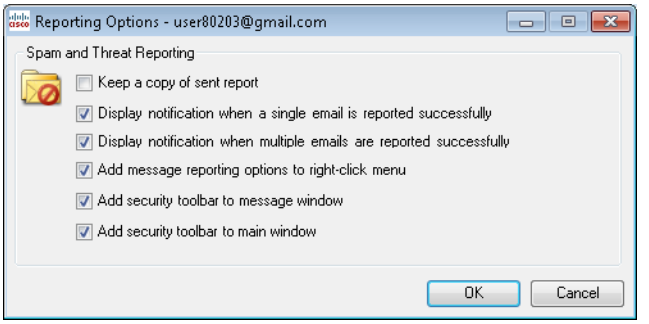
- 在 Outlook 2010/2013 中，点击功能区中的**插件选项 (Plug-in Options)** 或转到**文件 (File) > 选项 (Options) > 加载项 (Add-ins) > 加载选项 (Add-in Options) > 思科邮件安全 (Cisco Email Security)**，然后点击**报告选项 (Reporting Options)** 按钮。
- 在 Outlook 2007 中，点击工具栏上的**插件选项 (Plug-in Options)** 按钮，或转到**工具 (Tools) > 选项 (Options) > 思科邮件安全 (Cisco Email Security)** 选项卡，然后点击**报告选项 (Reporting Options)** 按钮。

还有一些必须在 BCE_Confg 文件中进行配置的报告选项。有关详细信息，请参阅“配置垃圾邮件报告的加密”一节，第 4-14 页。

以下“报告帐户”(Reporting Accounts) 页面显示了在 Outlook 中配置的所有帐户。要为某个帐户配置报告选项，请选择相应帐户并点击“选项”(Options) 按钮。该帐户的报告选项随即会显示出来。



以下特定于帐户的“报告选项”(Reporting Options) 页面显示了所选帐户的报告选项，并允许您启用或禁用它们的功能。有关详细信息，请参阅下表。



该表介绍了最终用户可配置的报告选项。

选项	说明
保留已发送报告副本 (Keep a copy of sent report)	在默认情况下，当最终用户向思科报告邮件为垃圾邮件、病毒或错误分类的垃圾邮件时，最终用户发送的报告邮件会被删除。选择此选项可防止邮件被删除。
成功报告一封邮件时显示通知 (Display notification when a single email is successfully reported)	当最终用户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 (Display notification when multiple emails are successfully reported)	当最终用户成功将一组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。
为主窗口添加安全工具栏 (Add security toolbar to the main window)	在默认情况下，当最终用户安装思科邮件安全插件时，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。
为右键单击菜单添加邮件报告选项 (Add message reporting options to the right-click menu)	在默认情况下，当最终用户安装思科邮件安全插件时，将向 Outlook 右键单击上下文菜单添加“报告”(Reporting) 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。
为邮件窗口添加安全工具栏 (Add security toolbar to the message window)	在默认情况下，当最终用户安装思科邮件安全插件时，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

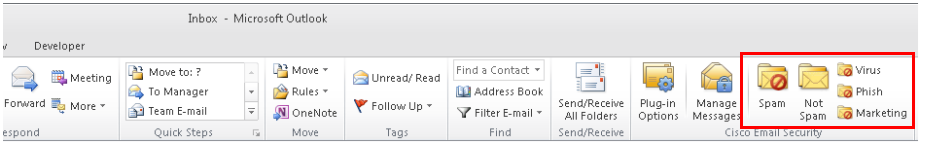
概述

适用于 Outlook 的思科邮件安全插件允许最终用户向思科提交有关在收件箱中收到的垃圾邮件、病毒、网络钓鱼或营销邮件的反馈。如果邮件被错误分类或邮件应被分类为垃圾邮件，最终用户可以向思科报告。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他们的收件箱。

此插件通过 Outlook 菜单栏和右键单击邮件菜单提供便捷界面，以报告垃圾邮件、病毒、网络钓鱼、营销邮件和错误分类邮件。报告邮件后，将显示报告已提交消息。最终用户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。

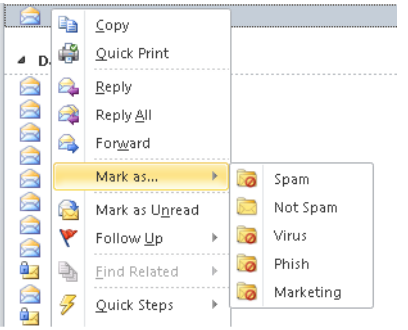
向思科提供反馈

此插件在 Outlook 中提供新的工具栏，包括以下按钮：垃圾邮件 (Spam)、非垃圾邮件 (Not Spam)、病毒 (Virus)、网络钓鱼 (Phish)、营销邮件 (Marketing) 和阻止发件人 (Block Sender)（“阻止发件人”[Block Sender] 不阻止最终用户垃圾邮件箱中的邮件）。

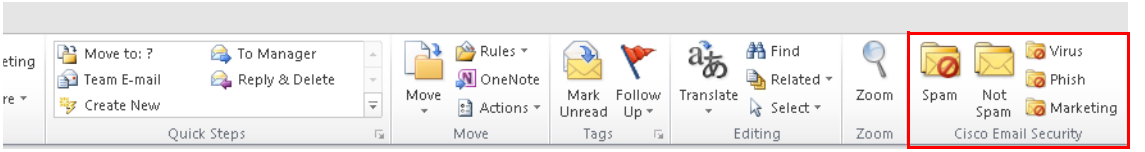


这些按钮用于报告垃圾邮件、病毒、网络钓鱼和营销邮件（网络钓鱼攻击指链接至欺骗收件人泄露信用卡帐号、帐户用户名和口令、身份证号等个人财务数据的欺诈网站的邮件。例如，最终用户可能会收到来自 *infos@paypals.com* 的邮件，此邮件意在骗取他们的个人银行信息）。此外，最终用户还可以点击“阻止发件人”(Block Sender) 按钮。点击此按钮可执行 Outlook 垃圾邮件操作“将发件人添加至‘已阻止发件人列表’”(Add Sender to Blocked Senders List)。请参阅 Microsoft 文档获取此功能的详细信息。

最终用户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、网络钓鱼和营销邮件。



最终用户还可以使用邮件窗口中的按钮报告垃圾邮件、病毒、网络钓鱼、营销和错误分类邮件（错误分类邮件指被错误标记为垃圾邮件、病毒、网络钓鱼或营销的邮件）。



报告的垃圾邮件、病毒、网络钓鱼或营销邮件的消息轮换

当邮件报告为垃圾邮件、错误分类邮件、病毒、网络钓鱼或营销邮件时，邮件将被如下处理。

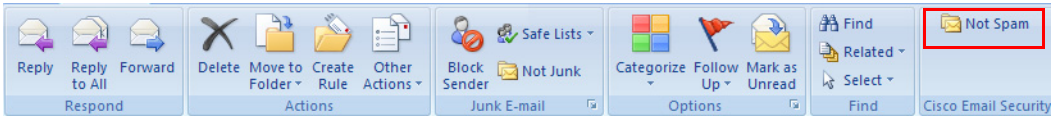
收件箱：

- 收件箱内报告为垃圾邮件、病毒、网络钓鱼或营销邮件的邮件被转入垃圾邮件文件夹。
- 收件箱内报告为非垃圾邮件的邮件留在收件箱文件夹。

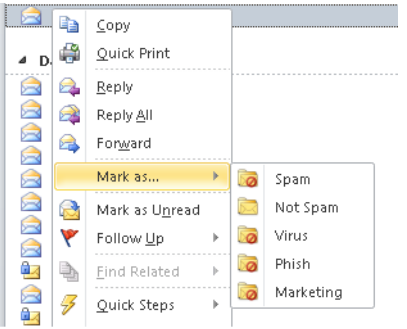
垃圾邮件箱：

- 垃圾邮件箱内报告为垃圾邮件、病毒、网络钓鱼或营销邮件的邮件留在垃圾邮件文件夹内。
- 垃圾邮件箱内报告为非垃圾邮件的邮件转入收件箱文件夹。

如果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），最终用户可以点击**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。



最终用户还可以从右键单击上下文菜单标记错误分类邮件。



配置单个 Outlook 帐户的报告

BCE_Config 文件现包含一个 reportingComponent 部分，将对每个帐户分别应用。

配置垃圾邮件报告的加密

要启用或禁用垃圾邮件报告的加密，请在 BCE_Config 文件的“报告”部分配置以下两个选项：

- 格式 - 定义报告的格式。支持的值包括：
  - 加密 - 指定发送前将对报告进行加密。
  - 无格式 - 指定报告发送时不加密。

  默认值为加密。
- 主题 - 定义报告的主题。您可通过包含字符串“${reportType}”，在主题中包含报告类型（垃圾邮件、Ham、病毒、网络钓鱼、营销）。

配置垃圾邮件报告的跟踪

要启用标记为垃圾邮件、病毒、网络钓鱼或营销邮件的报告邮件的跟踪，请在 BCE_Config 文件中设置以下参数：

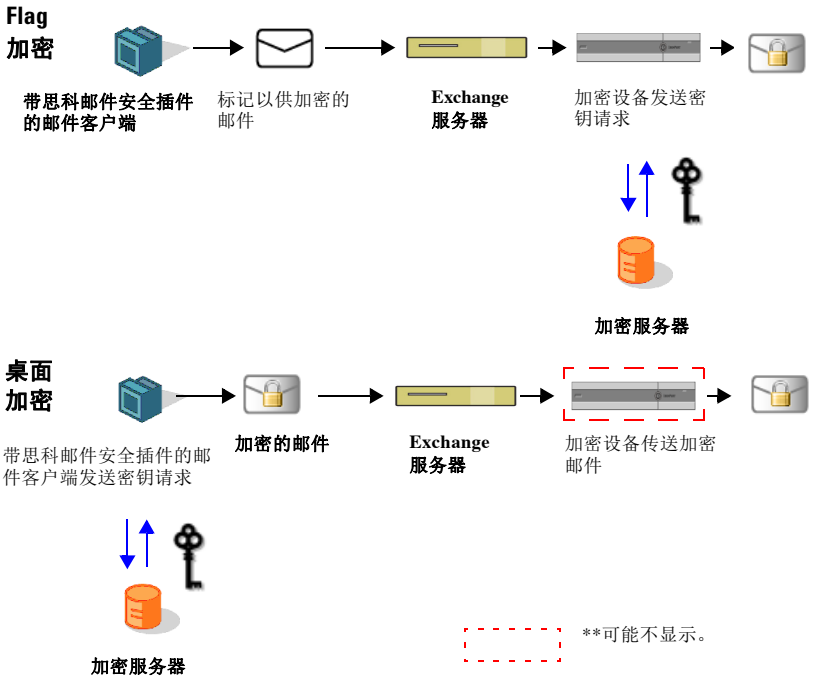
- copyAddressInPlainFormat - 指定将垃圾邮件报告的副本以无格式 (.raw) 的自定义邮件地址。

加密邮件

加密插件允许最终用户从桌面加密邮件或将邮件标记为要在从公司网络发出之前进行加密。选择以下其中一个加密选项：

- **Flag 加密 (Flag Encryption)**。“Flag 加密”(Flag Encryption) 选项允许最终用户标记出要加密的邮件，并使邮件在从网络中发出前使用思科邮件安全设备 (ESA) 进行加密。如果最终用户只需要对发送到组织之外的邮件进行加密，而不需要对在组织之内发送的邮件进行加密，可以使用 Flag 加密实现目的。例如，他们的组织负责处理一些敏感的医疗文档，这些文档在发送给患者之前，需要进行加密。
- **桌面加密 (Desktop Encryption)**。“桌面加密”(Desktop Encryption) 允许最终用户使用思科加密技术从 Outlook 内部加密邮件。然后，它会从他们的桌面发送已加密的邮件。如果最终用户想确保在组织*内部*发送的邮件得到加密，那么可以使用桌面加密。例如，他们的组织要求对在组织内外发送的所有敏感财务数据进行加密。

图 4-1　　Flag 加密工作流与桌面加密工作流



注意　加密方法通过解密来自 Outlook 邮件帐户的签名 BCE 配置文件附件来确定。默认情况下启用“仅解密”(Decrypt Only) 模式。最终用户可以选择通过从您（即管理员）那里接收和解密更新的签名 BCE 配置文件，来修改安装以更改加密方法。

Flag 加密和桌面加密配置

最终用户 Outlook 邮件帐户的默认配置模式为“仅解密”(Decrypt Only)。要启用 Flag 或加密功能，最终用户邮件帐户要通过从管理员接收的更新附件文件进行配置。另外，如果直接将一组配置文件提供给用户的配置文件夹，也可以通过批量安装实现 Flag 和加密功能。如果已解密的邮件包含一个签名 BCE 配置文件附件，当最终用户启动此配置文件时会自动配置 Outlook 的加密插件。Cisco IronPort 加密设备 (IEA) 或思科注册信封服务 (CRES) 用作密钥服务器。如果最终用户没有帐户，系统会提示他们注册帐户。

有三种配置模式可供选择：

- **仅解密 (Decrypt Only)**。允许对收到的加密邮件进行解密。
- **解密和标记 (Decrypt and Flag)**。允许对安全邮件进行解密和标记。标记选项使最终用户能够标记要加密的邮件，所标记的邮件在发出网络之前会由思科邮件安全设备进行加密。服务器必须配置为检测标记的邮件并在服务器端对邮件进行加密。
- **解密和加密 (Decrypt and Encrypt)**。允许对安全邮件加密和解密。

启动邮件安全插件配置文件

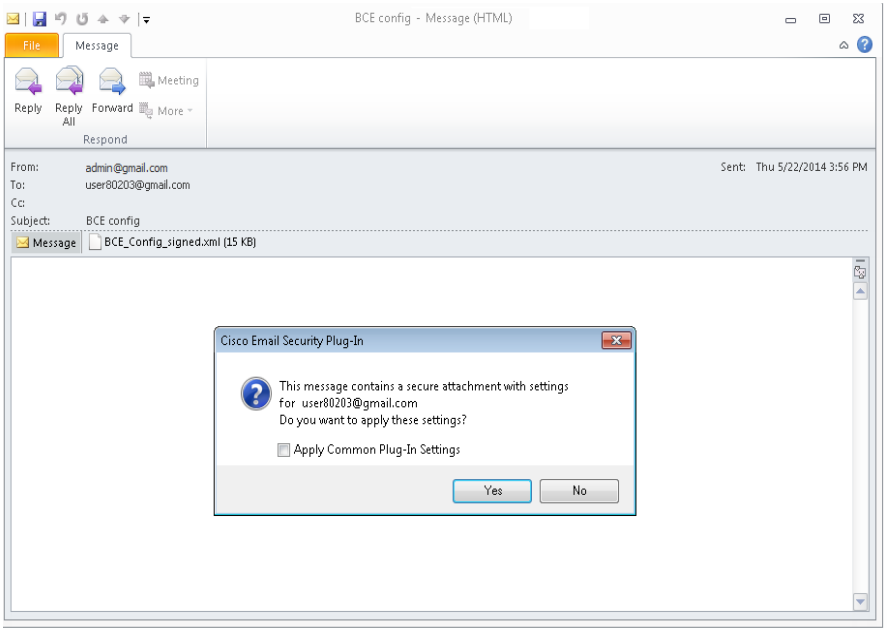
最终用户可以通过解密来自其 Outlook 邮件帐户的签名 BCE 配置文件附件，启用并配置 Outlook 邮件帐户的加密。如果最终用户的收件箱中没有带附件的通知邮件，可检查垃圾邮箱或垃圾邮件文件夹。

启动配置文件时，系统会为接收通知邮件（带有签名 BCE 文件附件）的邮件帐户配置插件。

注意　通常，Java 运行时环境 (JRE) 在插件安装时自动安装。但是，如果未自动安装，请至少安装 1.6 版本与插件搭配使用。

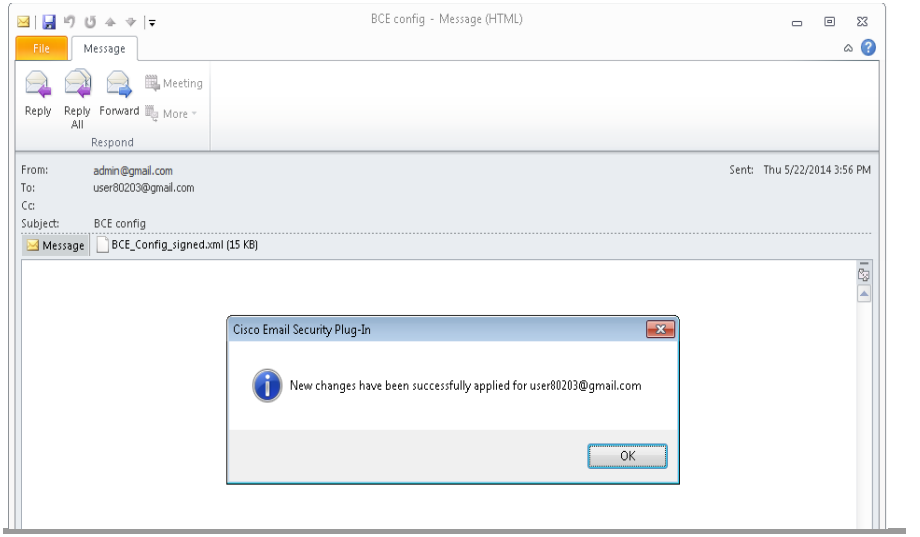
要启用和配置 Outlook 邮件帐户的安全插件：

步骤 1　打开随附签名 BCE 配置文件的通知邮件。系统会询问最终用户是否要应用设置。



步骤 2　点击**是 (Yes)** 自动配置思科邮件安全插件。成功应用配置后，屏幕上会显示一条消息。

如果您选择**应用一般插件设置 (Apply Common Plug-in Setting)** 复选框，将应用一般插件设置。有关一般插件设置的详细信息，请参阅“使用 BCE_Config 文件配置常用选项”一节，第 4-8 页。



Flag 加密

“Flag 加密”(Flag Encryption) 使最终用户能够标记要加密的邮件，所标记的邮件在发出网络之前会由思科邮件安全设备 (ESA) 进行加密。如果离开公司网络的邮件需要扫描垃圾邮件或病毒，应使用“Flag 加密”方法。

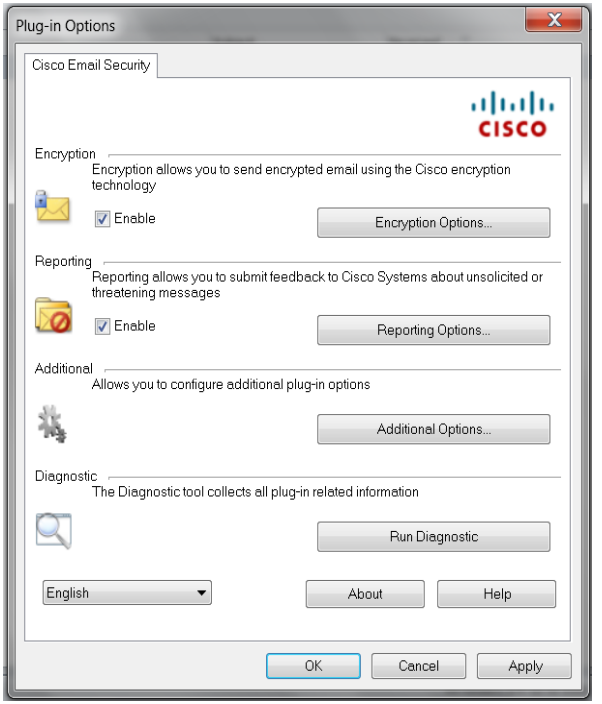
Flag 加密设置位于“思科邮件安全”(Cisco Email Security) 页上。要修改 Flag 加密设置，请执行以下操作：

- 在 Outlook 2010/2013 中，点击功能区中的**插件选项 (Plug-in Options)** 按钮，或转到**文件 (File) > 选项 (Options) > 加载项 (Add-ins) > 加载选项 (Add-in Options) > 思科邮件安全 (Cisco Email Security) > 加密选项 (Encryption Options)**。
- 在 Outlook 2007 中，点击工具栏上的**插件选项 (Plug-in Options)** 按钮，或转到**工具 (Tools) > 选项 (Options) > 思科邮件安全 (Cisco Email Security) > 加密选项 (Encryption Options)** 选项卡。

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

选择**启用 (Enable)** 以允许邮件程序通过安全信封发送敏感邮件。

思科邮件安全“加载项选项”(Add-in Options) 页：

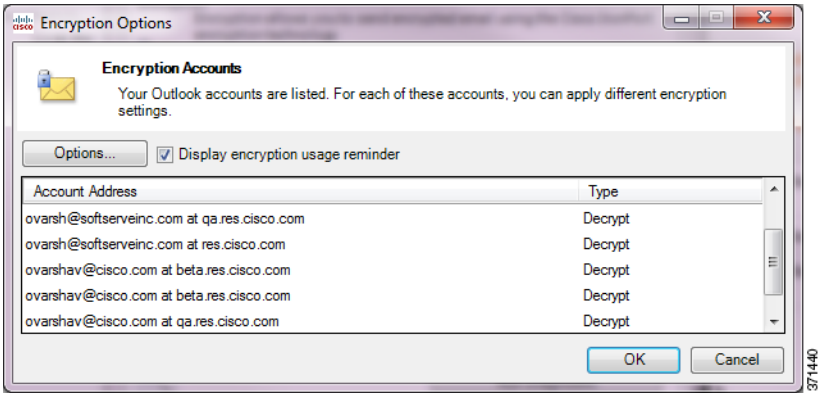


Flag 加密选项

当您点击**加密选项 (Encryption Options)** 时，将出现“加密帐户”(Encryption Accounts) 页。

“加密帐户”(Encryption Accounts) 页会显示 Flag 加密插件的所有邮件用户帐户。每行显示一个 Outlook 帐户邮件地址及相关的密钥服务器和加密类型（Flag 或加密）。点击**选项 (Options)** 或双击帐户地址将打开帐户“加密选项”(Encryption Options) 页。

“加密帐户”(Encryption Accounts) 页：



注意　Outlook 中的新帐户将自动添加到加密帐户列表中。删除 Outlook 帐户后，该帐户也将自动从加密帐户列表中删除。

发送 Flag 加密邮件的选项

当最终用户希望加密发送邮件时，需要“标记”邮件进行加密。这样可允许您创建的过滤器识别需要加密的邮件。

注意　这些标记邮件以供加密的方法要求对邮件过滤器进行更改才能正常使用，并且只有管理员才能进行这些更改。

编写邮件时“加密邮件”(Encrypt Message) 按钮可用。您可以使用以下方法之一标记邮件进行加密：

“常规”(General) 选项卡

您可以从以下常规选项中进行选择：

常规选项	值
Flag 主题文本 (Flag Subject Text)	可添加到发送邮件“主题”(Subject) 字段，以标记要加密邮件的文本。输入要添加到“主题”(Subject) 字段，表示该邮件应该加密的文本（默认值为 *[SEND SECURE]*）。
Flag X 标头名称/值 (Flag X-header name/value)	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，输入值 *true* 或 *false*。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）。
Flag 敏感性标头 (Flag Sensitivity header)	Outlook 可添加敏感标头标记邮件以供加密。选择此方法允许使用 Outlook 敏感标头标记邮件以供加密。

“连接”(Connection) 选项卡

您可以从以下连接选项中进行选择：

连接选项	值
无代理 (No proxy)	选择是否不使用代理。
使用系统代理设置 (Use system proxy settings)	选择此项以使用默认系统代理设置。
手动代理配置 (Manual proxy configuration)	选择此项以输入特定代理的设置。
协议 (Protocol)	如果选择不使用默认连接设置，请选择以下协议之一：HTTP、SOCKS4、SOCKS4a 或 SOCKS5。
主机 (Host)	为系统或代理服务器指定主机名称或 IP 地址。
端口 (Port)	为系统或代理服务器指定端口。
用户名 (Username)	如果服务器用户名为必填，请输入用户名。
口令 (Passphrase)	输入与为系统或代理服务器输入的用户名相关联的口令。

“记住口令”(Remember Passphrase) 选项卡

从以下记住口令选项中进行选择：

口令选项	值
从不 (Never)	若选择此项，系统每次在解密和加密邮件时都将要求输入加密口令。
始终 (Always)	若选择此项，系统只会在首次对加密的邮件进行解密时要求输入加密口令。然后口令就会存入缓存。
分钟数 (Minutes)	选择此选项可确保加密口令存入缓存。键入记忆口令的分钟数或使用箭头修改条目。指定的持续时间过后，最终用户再对加密的邮件解密时必须重新输入加密口令。默认值为 1440 分钟。

桌面加密

“桌面加密”(Desktop Encrypt) 选项允许最终用户从 Outlook 内部加密邮件以及从桌面发送加密的邮件。

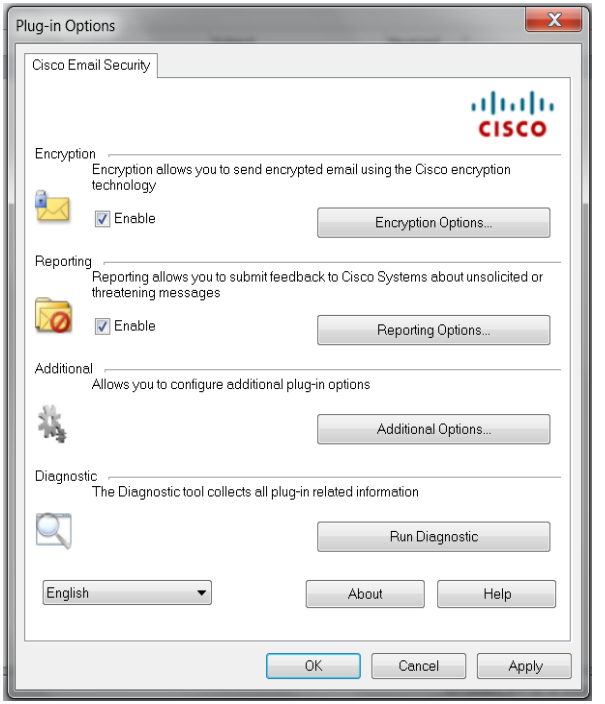
桌面加密设置位于“思科邮件安全”(Cisco Email Security) 页。要修改桌面加密设置，请执行以下操作：

- 在 Outlook 2010/2013 中，点击功能区中的**插件选项 (Plug-in Options)** 按钮，或转到**文件 (File) > 选项 (Options) > 加载项 (Add-ins) > 加载选项 (Add-in Options) > 思科邮件安全 (Cisco Email Security) > 加密选项 (Encryption Options)**。
- 在 Outlook 2007 中，点击工具栏上的**插件选项 (Plug-in Options)** 按钮，或转到**工具 (Tools) > 选项 (Options) > 思科邮件安全 (Cisco Email Security) > 加密选项 (Encryption Options)** 选项卡。

最终用户选择或清除“思科邮件安全”(Cisco Email Security) 选项卡中“加密”(Encryption) 字段的**启用 (Enable)** 复选框可启用或禁用加密插件。选择**启用 (Enable)** 以允许邮件程序通过安全信封发送敏感邮件。

注意　最终用户可从思科邮件安全页启用或禁用加密插件，但是加密模式的任何变更都需要由管理员在 *BCE_config.xml* 文件中执行。

思科邮件安全“加载项选项”(Add-in Options) 页：

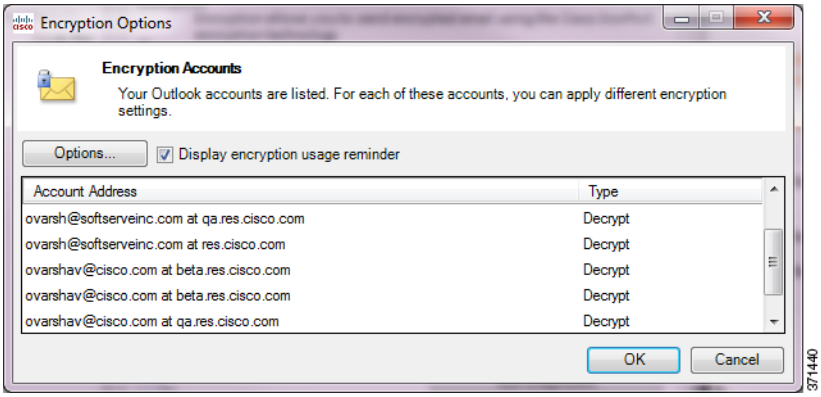


桌面加密选项

当您点击**加密选项 (Encryption Options)** 时，将出现“加密帐户”(Encryption Accounts) 页。

“加密帐户”(Encryption Accounts) 页会显示 Flag 加密插件的所有邮件用户帐户。每行显示一个 Outlook 帐户邮件地址及相关的密钥服务器和加密类型（Flag 或加密）。点击**选项 (Options)** 或双击帐户地址将打开帐户“加密选项”(Encryption Options) 页。

“加密帐户”(Encryption Accounts) 页：



注意　Outlook 中的新帐户将自动添加到加密帐户列表中。删除 Outlook 帐户后，该帐户也将自动从加密帐户列表中删除。

“常规”(General) 选项卡

注意　下表显示了“常规”(General) 选项卡中的所有可能选项。根据您的 *BCE_config.xml* 文件的设置，某些选项可能不可见或不可用。

您可以从以下常规选项中进行选择：

常规选项	值
用作默认加密帐户 (Use as default encryption account)	选择此项以将当前帐户设为默认加密帐户。
默认加密 (Encrypt by default)	选择此设置后，所有已发送的邮件在默认情况下均会加密。
服务器 URL (Server URL)	输入加密服务器的 URL。
始终使用来自密钥服务器的邮件正文 (Always use message body from key server)	使插件能够根据每个收件人的区域设置来确定要用于邮件正文的语言。如果您要将加密的邮件发送给具有相同区域设置的收件人，请使用此选项。如果您禁用此选项，邮件正文将始终使用您为下列选项选择的默认语言。
外发邮件的默认语言 (Default language for outgoing messages)	指定当您将邮件发送给具有不同区域设置的收件人时，将用于外发邮件的语言（正上方的复选框处于选中状态）。 指定将用于所有外发邮件的语言（正上方的复选框处于未选中状态）
令牌文件名 (Token File Name)	令牌是数据在邮件客户端和加密服务器之间加密所要使用的客户专用密钥。目前，只有客户支持团队可以使用此信息，而且此信息无法进行更改。
默认过期期限（天）(Default Expiration [days])	指定加密邮件有效期限（天）。达到过期天数后，邮件将过期，并且在此阶段之后收件人将无法将其打开。
默认阅读截止日期（天）(Default read-by [days])	指定期望收件人阅读加密邮件的持续时间（按天数计算）。如果邮件在指定时间内未被阅读，那么发件人将收到通知。
附件名称 (Attachment name)	默认信封名称为 *securedoc.html*。可以更改附件名称，且信封将显示新指定的名称。

常规选项	值
邮件安全 (Message security)	设置加密邮件的安全级别。默认值在 *BCE_Config.xml* 文件中进行了定义。 **注意**　在此处更改安全级别只会影响正在撰写的邮件。 • **高 (High)**。如果邮件的安全级别为“高”(High)，则每次对加密邮件进行解密时都需要输入口令进行身份验证。 • **中 (Medium)**。如果收件人口令存入缓存且邮件安全级别设置为“中”(Medium)，则对邮件进行解密时不需要输入口令。 • **低 (Low)**。如果将邮件安全级别设置为“低”(Low)，邮件会以安全方式传输，不过对加密邮件进行解密时不需要输入口令。
发送回执 (Send return receipt)	选择此项后，系统会在收件人打开发送的邮件时要求回执。
在邮件加密期间显示对话框 (Show dialog during message encryption)	选择此选项可显示每个加密邮件的加密选项对话框。

“连接”(Connection) 选项卡

您可以从以下连接选项中进行选择：

连接选项	值
无代理 (No proxy)	选择是否不使用代理。
使用系统代理设置 (Use system proxy settings)	选择此项以使用默认系统代理设置。
手动代理配置 (Manual proxy configuration)	选择此项以输入特定代理的设置。

连接选项	值
协议 (Protocol)	如果选择不使用默认连接设置，请选择以下协议之一：HTTP、SOCKS4、SOCKS4a 或 SOCKS5。
主机 (Host)	为系统或代理服务器指定主机名称或 IP 地址。
端口 (Port)	为系统或代理服务器指定端口。
用户名	如果服务器用户名为必填，请输入用户名。
口令 (Passphrase)	输入与为系统或代理服务器输入的用户名相关联的口令。

“记住口令”(Remember Passphrase) 选项卡

从以下记住口令选项中进行选择：

口令选项	值
从不 (Never)	若选择此项，系统每次在解密和加密邮件时都将要求输入加密口令。
始终 (Always)	若选择此项，系统只会在首次对加密的邮件进行解密时要求输入加密口令。然后口令就会存入缓存。
分钟数 (Minutes)	选择此选项可确保加密口令存入缓存。从下拉列表中选择缓存持续时间（以分钟为单位）。指定的持续时间过后，最终用户再解密和加密邮件时必须重新输入加密口令。默认值为 1440 分钟。

“高级”(Advanced) 选项卡

注意　下表显示了“常规”(General) 选项卡中的所有可能选项。根据您的 *BCE_config.xml* 文件的设置，某些选项可能不可见或不可用。

您可以从以下高级选项中进行选择：

高级选项	值
未受安全保护的服务器 URL (Unsecure server URL)	为邮件栏帮助使用未受安全保护的基本 URL。如果忽略此项设置，则系统会使用外部安全 URL，例如 http://res.cisco.com。
连接超时 (Connection timeout)	与密钥服务器建立连接所需等待的时长。
套接字超时 (Socket timeout)	接收密钥服务器数据所需等待的时长。
显示“离线打开”复选框 (Display “Open offline” check box)	选择此项后，信封上会显示“离线打开” (Open offline) 复选框。
显示“记住信封密钥” (Display “Remember envelope key”)	选择此项后，信封上会显示“记住信封密钥”(Remember envelope key) 复选框。
显示“启用个人安全短语”	选择此项后，信封上会显示“启用个人安全口令”(Enable personal security phrase) 复选框。
添加邮件栏 (Add message bar)	选择此项可在安全邮件中添加邮件栏。
在邮件栏中显示“回复”按钮 (Show “Reply” button in the message bar)	启用邮件栏时，在邮件栏中显示“回复” (Reply)。
在邮件栏中显示“转发”按钮 (Show “Forward” button in the message bar)	启用邮件栏时，在邮件栏中显示“转发” (Forward)。
在邮件栏中显示“回复全部”按钮 (Show “Reply to All” button in the message bar)	启用邮件栏时，在邮件栏中显示“回复全部”(Reply to All)。
阻止打开小应用程序 (Suppress applet from opening)	选择此项可阻止使用小应用程序打开信封。
显示“记住我”(Display “Remember me”)	选择此项后，信封上会显示“记住我” (Remember me) 复选框。

高级选项	值
显示“自动打开”(Display “Auto open”)	选择此项后，信封上会显示“自动打开”(Auto open) 复选框。
在同一个窗口中打开 (Open in the same window)	选择此项可在信封所在窗口中打开安全邮件。
显示“加密使用情况提醒”(Display “Encryption usage reminder”)	选择此项后，用户每次执行加密时，都显示加密应当只用于商业目的提醒。

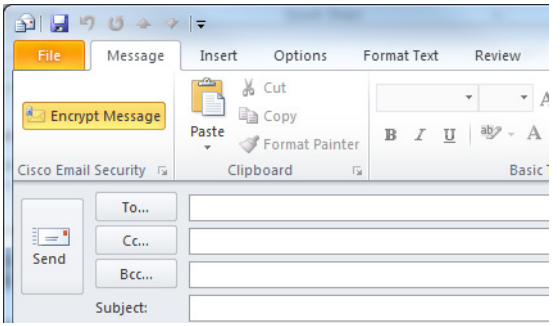
发送加密邮件

注意　加密邮件在添加附件前的默认最大大小为 7 MB，但管理员可在 *BCE_Config.xml* 文件中更改此值。

编写邮件时，最终用户可以通过点击**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。

编写邮件时“加密邮件”(Encrypt Message) 按钮可用。

以下显示了“邮件撰写”(Mail Compose) 页的“加密邮件”(Encrypt Message) 按钮及“加密邮件选项”(Encryption Mail Options) 切换按钮：



要发送加密邮件，请选择一个密钥服务器并输入您的口令。

要配置加密选项，请点击右下角的**思科邮件安全 (Cisco Email Security)** 启动程序，会出现如下“加密邮件选项”(Encryption Mail Options) 页。

注意　以下截图和表列出了加密邮件选项中所有可能的选项，但是显示的选项很大程度上取决于 *BCE_config.xml 文件*的配置。

注意　修改加密邮件选项时，所做更改只会影响正在撰写的邮件。

从以下邮件选项中进行选择：

加密邮件选项	说明
允许回复 (Allow Reply)	若选择此选项，收件人将可以回复加密邮件的发件人，并且回复邮件会自动加密。
允许回复全部 (Allow Reply All)	若选择此选项，收件人将可以回复加密邮件的所有收件人，并回复邮件会自动加密。
允许转发 (Allow Forward)	若选择此选项，收件人将可以转发加密邮件，并且转发邮件会自动加密。

加密邮件选项	说明
邮件安全 (Message security)	利用下拉菜单设置加密邮件的安全级别。默认值为 *BCE_Config.xml* 文件中设置的值。 **注意**　在此处更改安全级别只会影响正在撰写的邮件。 • **高 (High)**。如果邮件的安全级别为“高”(High)，则每次对加密邮件进行解密时都需要输入口令进行身份验证。 • **中 (Medium)**。如果收件人口令存入缓存且邮件安全级别设置为“中”(Medium)，则对邮件进行解密时不需要输入口令。 • **低 (Low)**。如果将邮件安全级别设置为“低”(Low)，邮件会以安全方式传输，不过对加密邮件进行解密时不需要输入口令。
到期 (Expiration)	通过下拉菜单指定加密邮件的有效期是多长时间（日期和时间）。指定的到期日期和时间过后，邮件就会到期，收件人将无法再打开此邮件。
阅读期限 (Read By)	在下拉菜单中选择日期和时间，指定收件人应当在多长时间之内阅读加密的邮件。如果邮件在指定时间内未被阅读，那么发件人将收到通知。

当最终用户点击**发送 (Send)** 时，安全信封选项页会出现，如“配置安全信封选项”一节，第 4-35 页中所示，除非此选项被禁用。

配置错误会导致错误。有关详细信息，请参阅错误和故障排除，第 4-51 页。

继承回复选项

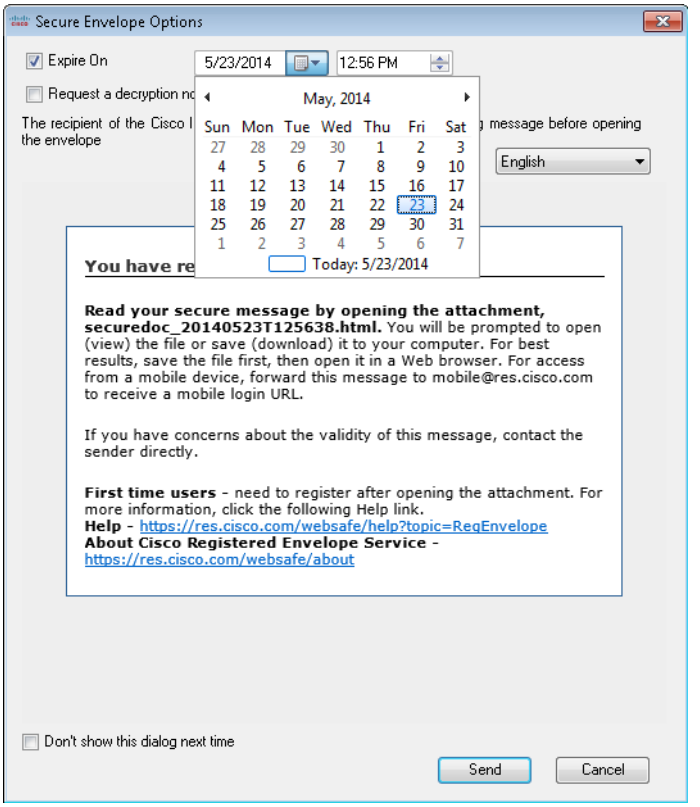
邮件解密时，回复、回复全部或转发选项及邮件敏感性选项的所有设置都将从原始邮件中继承，不可更改。例如：

- 默认情况下，邮件在回复或转发时会加密。
- 若原始邮件不允许回复、回复全部或转发选项，将无法发送回复或转发邮件，最终用户在点击**发送 (Send)** 时会收到通知。
- 当最终用户执行回复、回复全部或转发选项时，无法删除原始邮件中包含的收件人。
- 当最终用户执行回复、回复全部或转发选项时，无法添加原始邮件中未包含的收件人。
- 当最终用户执行回复、回复全部或转发选项时，无法在收件人、抄送或密件抄送之间混合或移动收件人。
- 如果帐户配置为仅解密或 Flag 加密，将无法发送回复或转发邮件，最终用户在点击**发送 (Send)** 时会收到通知。
- 如果帐户的邮件敏感性设置为“高”(High)，回复、回复全部或转发的邮件将具有高敏感性。
- 如果帐户的邮件敏感性设置为“中”(Medium)，回复、回复全部或转发的邮件将具有中度敏感性。
- 如果帐户的邮件敏感性设置为“低”(Low)，回复、回复全部或转发的邮件将具有低敏感性。
- 回复、回复全部或转发邮件将保存在已发送邮件文件夹内，且发件人可解密。
- 如果邮件包含签名 BCE 配置文件并转发给另一个最终用户，相比直接从管理员处接收，自动配置将不起作用并会收到错误消息。

配置安全信封选项

最终用户可以配置下表中所介绍的安全信封选项，如下面的截图所示：

注意　根据您的配置设置，语言选项可能不会显示在此屏幕上，并且将根据收件人的首选项选择通知的语言。



最终用户可以从以下安全信封选项中选择：

安全信封选项	说明
到期日期 (Expire on)	选择启用此选项。指定加密邮件的到期日期和时间。指定的到期日期和时间过后，邮件就会到期，收件人将无法再打开此邮件。日期和时间以发件人所在时区显示。
请求解密通知 (Request a Decryption Notification)	允许发件人请求邮件加密通知。打开加密邮件时，发件人将收到通知。
语言 (Language)	选择通知文本要使用的语言。从下拉菜单选择语言后，收件人通知将以所选语言显示。

如果最终用户的帐户配置为 Flag 加密，则从组织发送邮件之前，将会标记邮件以进行加密。如果最终用户的帐户配置为桌面加密，则在邮件发送至 Exchange 服务器之前，邮件会在桌面进行加密。

管理安全邮件

最终用户可以通过以下两种方式管理安全邮件：

- 使用管理安全邮件对话框管理选定的邮件。使用此对话框锁定、解锁或更新您发送加密邮件的到期日期。
- 使用“管理邮件”(Manage Messages) 对话框管理从所选帐户发送的所有邮件。使用此对话框搜索特定邮件。

这两种管理安全邮件的方式在以下部分中进行了说明。无论使用哪一种方式，最终用户都可以对他们发送的加密邮件执行以下操作：

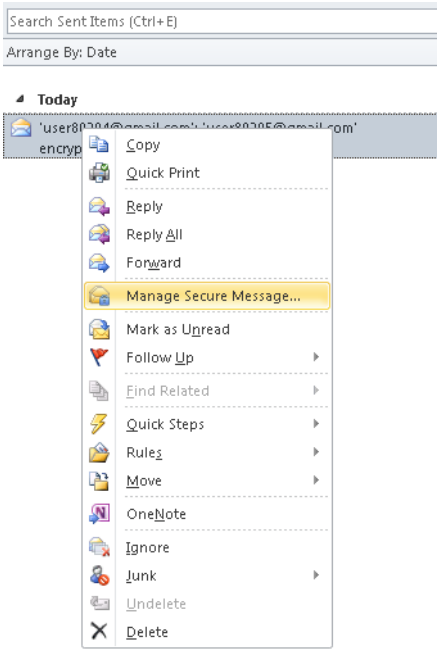
- **锁定邮件**。最终用户可以锁定之前发送的加密邮件。如果邮件已锁定，他们也可以设置锁定原因或更新锁定原因。收件人无法打开锁定的邮件。
- **解锁邮件**。最终用户可以解锁他们之前发送的加密邮件，允许收件人解密邮件。
- **更新到期日期**。最终用户可以设置、更新或清除已发送的加密邮件的到期日期。加密邮件到期后，收件人将无法解密邮件。

使用“管理安全邮件”(Manage Secure Messages) 对话框

步骤 1　选择您已发送且想要修改的加密邮件，然后右键单击该邮件以显示“管理安全邮件”(Manage Secure Messages) 菜单选项。

注意　最终用户也可以在对邮件进行解密和加密时访问“管理安全邮件”(Manage Secure Messages) 菜单。如果最终用户是当前邮件的发件人，则他们可以在工具栏中看到“管理安全邮件”(Manage Secure Messages) 按钮。当从工具栏访问“管理安全邮件”(Manage Secure Messages) 菜单时，到期设置每次只能应用于一封邮件。

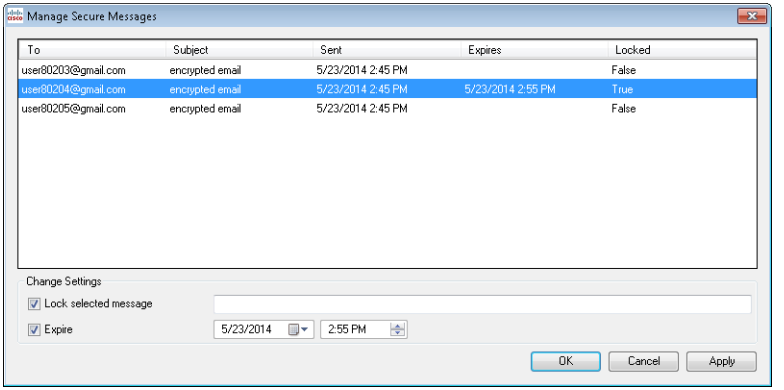
管理安全邮件菜单选项：



步骤 2　选择**管理安全邮件 (Manage Secure Messages)**。

如果您的口令未缓存，系统会要求您输入口令。

然后会显示“管理安全邮件”(Manage Secure Messages) 页面：



步骤 3　要设置每个收件人的锁定或到期选项，请先选择您已发送的一封或多封加密邮件，选中**锁定 (Lock)** 或 **到期 (Expire)** 复选框，并输入适当的信息。

注意　当从工具栏或功能区访问管理安全邮件菜单时，如下一部分所述，到期设置每次只能应用于一封邮件。

使用“管理邮件”(Manage Messages) 对话框

步骤 1　点击功能区（在 Outlook 2010/13 中）或工具栏（在 Outlook 2007 中）中的**管理邮件 (Manage Messages)** 按钮。

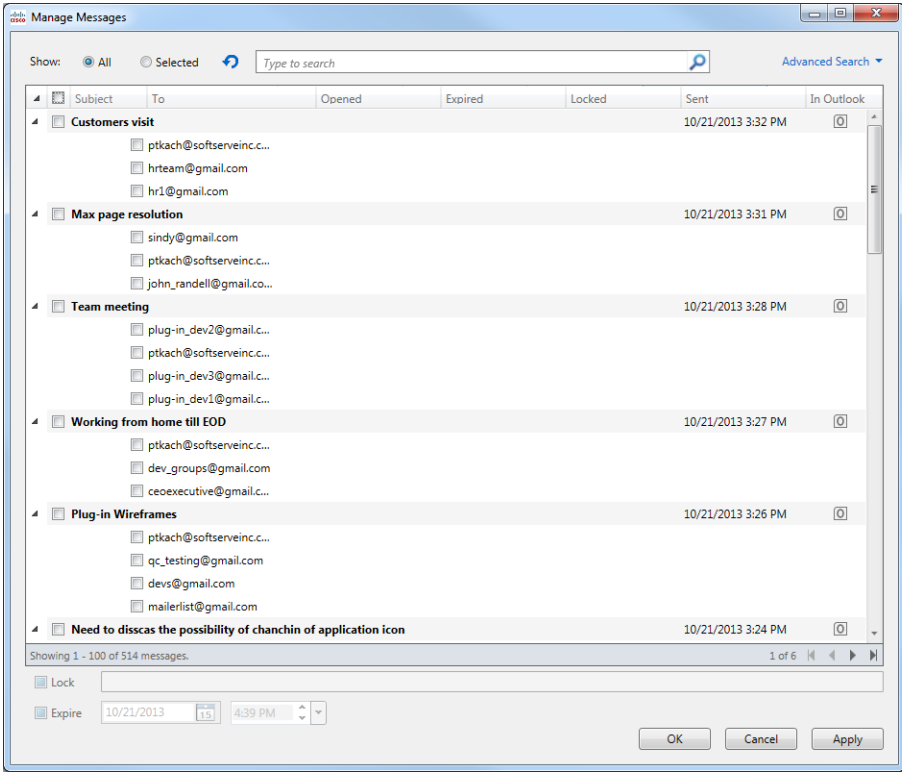
系统随即会打开“管理邮件”(Manage Messages) 对话框。

注意　最终用户可以使用此界面管理他们已发送的所有加密邮件。如果网络连接速度较慢且加密邮件很多，加载过程可能需要几分钟。

步骤 2　要查找特定邮件，请点击**基本搜索 (Basic Search)** 或**高级搜索 (Advanced Search)**。

步骤 3　要执行基本搜索，请在以下屏幕的“收件人”(To) 和“主题”(Subject) 字段中输入要搜索的关键字。

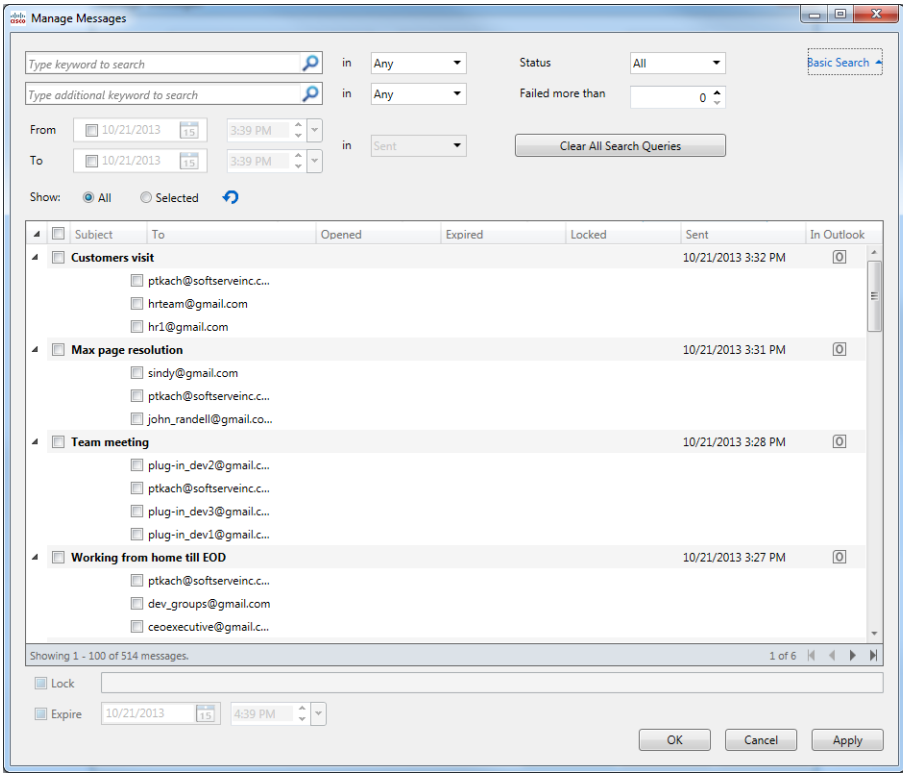
最大字符串长度为 500 个字符。



步骤 4　要执行高级搜索，请在以下屏幕中输入以下一个或多个搜索参数：

- 关键字 1 - 用于搜索在“收件人”(To) 或“主题”(Subject) 字段中包含该关键字的邮件。关键字的最大字符串长度为 500 个字符。
- 关键字 2 - 用法与关键字 1 相同。如果同时指定两个关键字，则所执行的搜索会寻找同时包含这两个关键字的邮件。
- 搜索范围（适用于关键字搜索）- 指定关键字搜索范围是否包含“收件人”(To)、“主题”(Subject) 或“锁定原因”(Locked Reason) 字段。
- 失败次数超过 (Failed more than) - 用于根据失败尝试次数进行搜索。搜索结果会显示失败尝试次数大于指定值的所有邮件。最大值为 10。

- 状态 (Status) - 用于根据以下某项状态设置进行搜索：“所有”(All)、“未打开”(Unopened)、“已打开”(Opened)、“已锁定”(Locked) 和“已到期”(Expired)。
- 从 (From)/ 到 (To) - 用于根据日期和时间间隔进行搜索。如果仅设置“从”(From) 日期，系统将仅搜索在所选日期之后发送的所有邮件。如果仅设置“到”(To) 日期，系统将仅搜索在所选日期之前发送的所有邮件。如果您既设置“从”(From) 日期又设置“到”(To) 日期，系统会搜索在所选日期之间发送的所有邮件。您可以使用下拉日历也可以手动输入日期来设置日期。默认日期是当前日期和时间，不过默认情况下按日期搜索功能处于禁用状态。
- 搜索范围 (In)（适用于日期搜索）- 指定与日期相关的搜索的条件。系统提供以下选项：“已发送”(Sent)、“已打开”(Opened) 和“已到期”(Expired)。



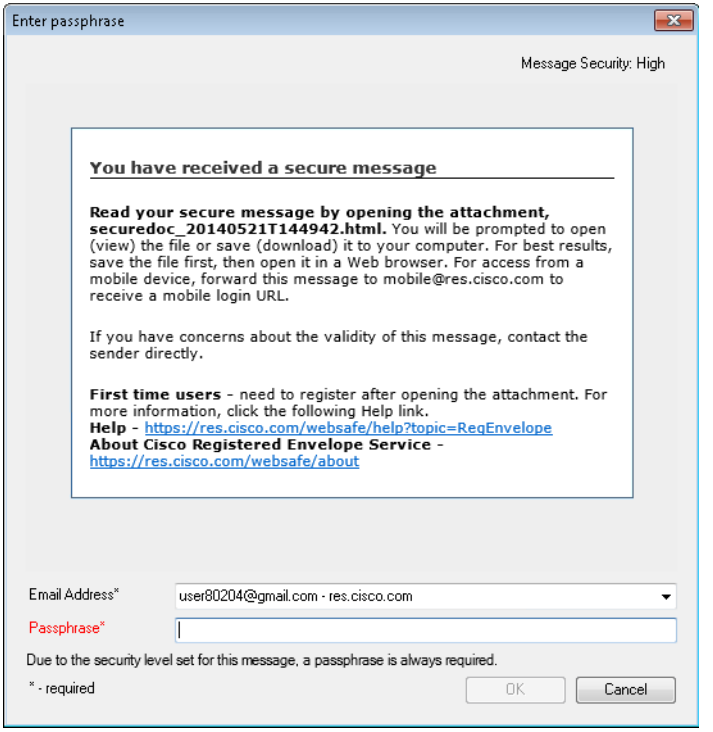
步骤 5　点击**确定 (OK)**。

接收和回复安全邮件

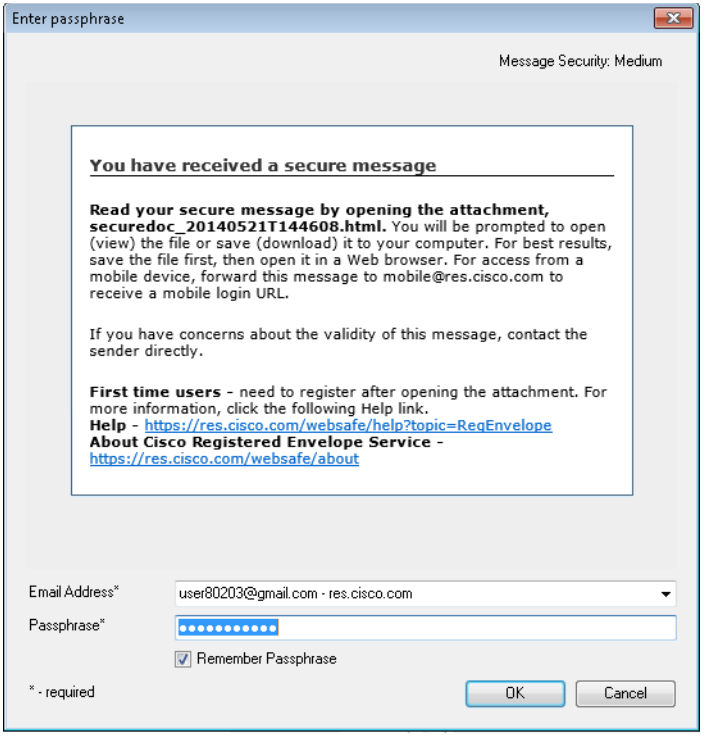
桌面加密插件会自动检测安全邮件，并尝试在 Outlook 中进行解密。当最终用户收到加密邮件，通常需要输入加密口令才能打开信封。发送安全邮件的安全等级可以为“高”(High)、“中”(Medium) 或“低”(Low)。

注意　如果最终用户收到受口令保护的安全邮件，必须使用思科注册信封服务 (CRES) 注册和建立一个用户帐户才能打开加密邮件。最终用户在注册服务后，就可以使用他们的帐户口令打开收到的所有注册信封。有关详细信息，请参阅打开您的首封加密安全邮件，第 4-45 页。

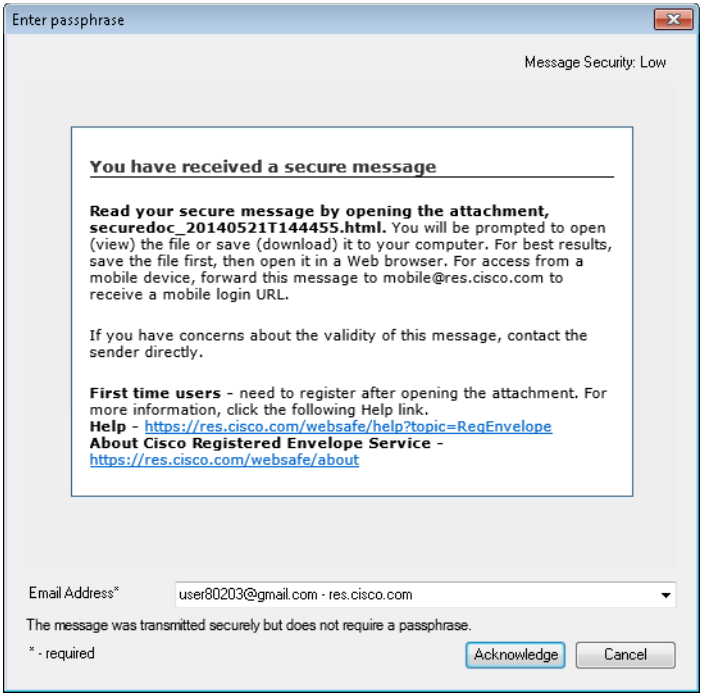
邮件安全等级为高的页面：



邮件安全等级为中的页面：



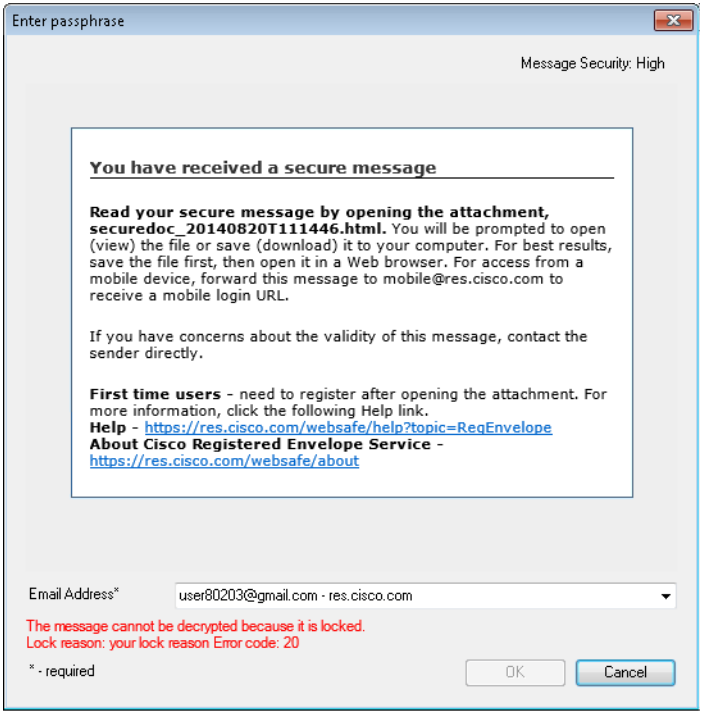
邮件安全等级为低的页面：



以下部分介绍了邮件安全等级选项：

邮件安全等级选项	说明
高 (High)	如果邮件的安全级别为“高”(High)，则每次对加密邮件进行解密时都需要输入口令进行身份验证。
中 (Medium)	如果收件人口令存入缓存且邮件安全级别设置为“中”(Medium)，则对邮件进行解密时不需要输入口令。
低 (Low)	如果将邮件安全级别设置为“低”(Low)，邮件会以安全方式传输，不过对加密邮件进行解密时不需要输入口令。

如果最终用户接收的安全邮件已被锁定或已到期，“邮件安全”(Message Security) 页面中会以红色字体显示一条通知消息。



安全回复/回复全部/转发

当您回复或转发加密的邮件时，如果您正在使用桌面加密或仅解密模式，默认情况下回复邮件会自动加密。如果您正在使用 Flag 加密，则回复邮件将由思科邮件安全设备 (ESA) 加密。安全邮件的设置将决定是否允许您执行以下任何一种操作：

- 安全回复
- 安全回复全部
- 安全转发

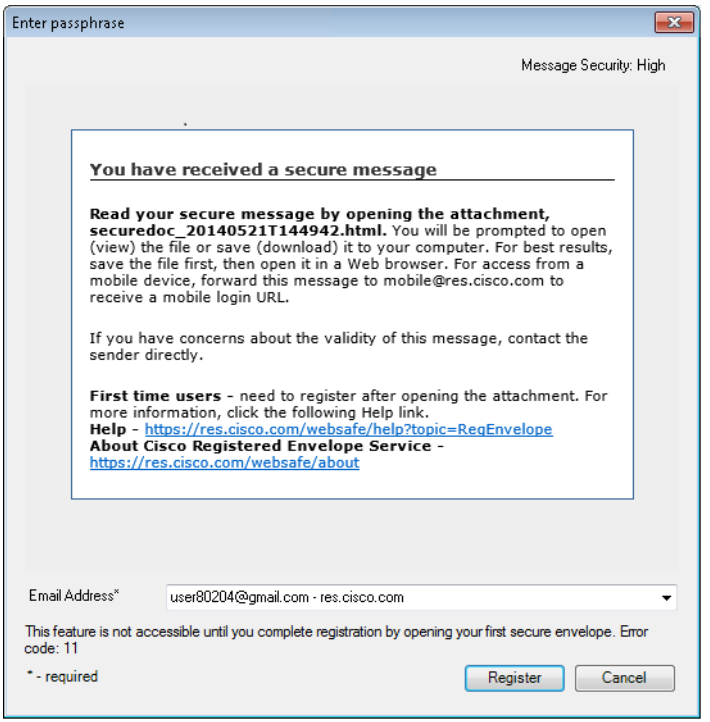
打开您的首封加密安全邮件

如果最终用户收到加密安全邮件，必须使用思科注册信封服务 (CRES) 注册和建立一个用户帐户才能打开加密邮件。最终用户在注册服务后，就可以使用他们的帐户密码打开收到的所有加密安全邮件。

要打开您的首封加密安全邮件，请执行以下操作：

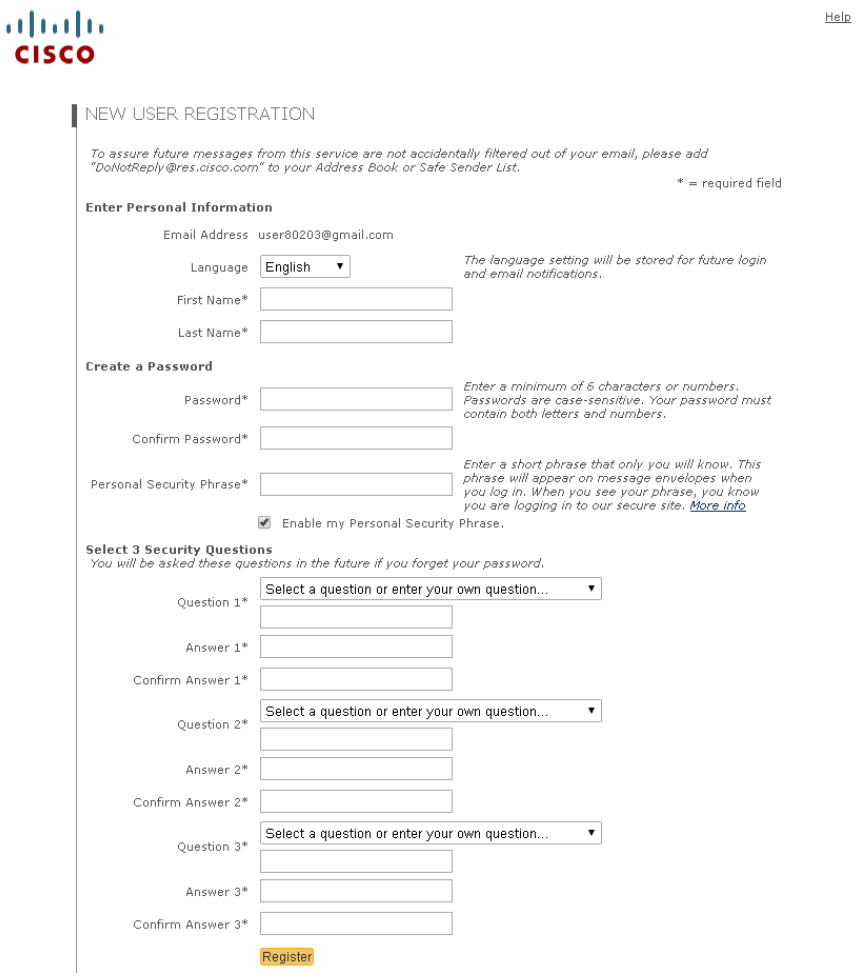
步骤 1　在邮箱中双击安全邮件。屏幕上会显示“解密”(Decryption) 对话框，并且其中包含注册按钮。

步骤 2　点击**注册 (Register)**，以注册思科注册信封服务 (CRES)。



步骤 3　在“CRES 新用户注册”(CRES New User Registration) 页面中输入信息，填写在线注册表。

“CRES 新用户注册”(CRES New User Registration) 页面：



新用户注册选项：

字段	说明
语言 (Language)	（可选）。从下拉菜单中为您的 CRES 帐户选择一种语言。注册页面默认以英语显示，但最终用户可选的语言包括英语、法语、德语、西班牙语、葡萄牙语和日语。
名字 (First Name)	必填。输入 CRES 用户帐户的名字。
姓氏 (Last Name)	必填。输入 CRES 用户帐户的姓氏。
密码 (Password)	必填。为帐户输入密码。密码最少包含六个字符，且应由数字和字母混合组成。 **注意**　如果最终用户忘记密码，可以通过正确回答安全提示问题来重置密码。
个人安全口令 (Personal Security Phrase)	必填。输入个人安全口令。个人安全口令可以帮助最终用户抵御密码网络钓鱼威胁。最终用户可以在注册期间指定一个只有其自己和服务系统知道的简短个人安全口令。最终用户在收到的注册信封上点击密码字段，就能看到其个人安全口令。如果最终用户没有看到个人安全口令，可点击链接了解详情。 **注意**　如果最终用户没有选择“在此计算机上记住我”(Remember me on this computer)，则安全口令将不会显示。
启用个人安全口令 (Enable Personal Security Phrase)	（可选）。选中此复选框以启用个人安全口令。
安全提示问题 (Security Questions)	必填。最终用户可以选择三个安全提示问题，且必须输入并确认问题的答案。最终用户可在忘记密码时使用这些问题重置密码。

步骤 4　点击表单底部的**注册 (Register)**，创建用户帐户。

注意　如果最终用户收到的注册信封来自多个邮件地址，则可能需要创建多个用户帐户。每个邮件地址需要一个单独的用户帐户。

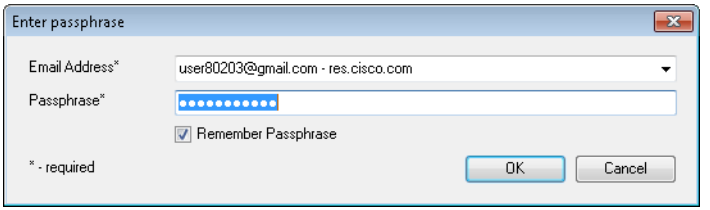
步骤 5　在您的收件箱中查收帐户激活邮件。在激活邮件中，点击**点击此处激活此帐户 (Click here to activate this account)** 链接。最终用户会收到一封邮件，表明帐户激活已得到确认，最终用户现在可以查看发送到所注册邮件地址的加密邮件。

步骤 6　返回原始邮件并点击 *securedoc_date_time.html* 文件附件。

步骤 7　点击**打开 (Open)**。安全邮件会进行解密并显示邮件内容。

注意　根据最终用户的配置文件设置，某些功能可能不可用。例如，可能无法回复邮件、无法回复全部或无法转发邮件。

密码将在 Outlook 会话期间保存。但是，在重新启动 Outlook 时，最终用户需要再次输入密码。



更改其他设置

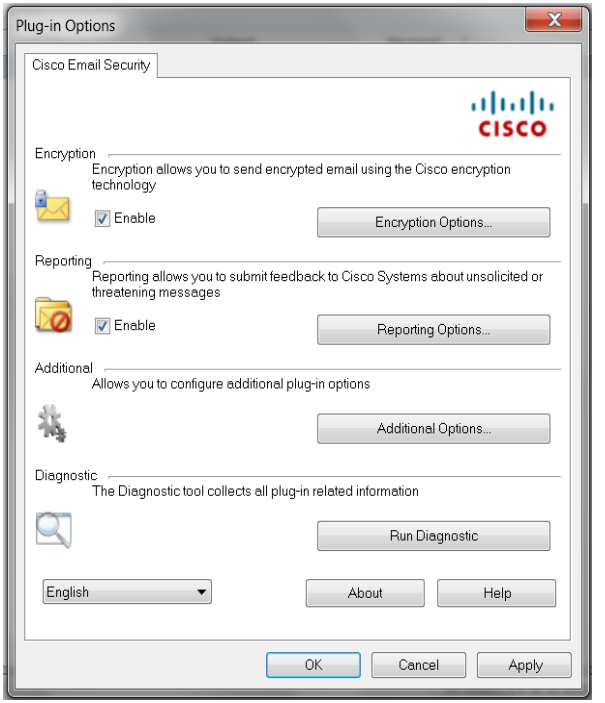
日志文件会记录并列出所有已发生的操作。

“其他选项”(Additional Options) 位于“思科邮件安全”(Cisco Email Security) 页。要修改其他选项，请执行以下操作：

- 在 Outlook 2010/2013 中，点击功能区中的**插件选项 (Plug-in Options)** 按钮，或转到**文件 (File) > 选项 (Options) > 加载项 (Add-ins) > 加载选项 (Add-in Options) > 思科邮件安全 (Cisco Email Security) > 其他选项 (Additional Options)**。

- 在 Outlook 2007 中，点击工具栏上的**插件选项 (Plug-in Options)** 按钮，或转到**工具 (Tools) > 选项 (Options) > 思科邮件安全 (Cisco Email Security) > 其他选项 (Encryption Options)**。

思科邮件安全“加载项选项”(Add-in Options) 页：



通过“加密其他选项”(Encryption Additional Option) 页面，您可以配置以下选项类型，如以下部分所介绍：

- 日志记录 (Logging)
- 发送使用情况数据 (Sending Usage Data)
- 隐私声明 (Privacy)

“日志记录”(Logging) 选项卡

最终用户可以从“日志记录”(Logging) 选项卡配置以下选项。

选项	说明
启用日志记录 (Enable Logging)	选择此选项即可启用思科邮件安全插件的日志记录功能。
日志文件名称 (Log file name)	指定将存储在 %ALLUSERSPROFILE%\Cisco\Cisco Email Security Plug-in\<*username*> 中的日志文件的名称。日志文件的扩展名必须是 .log。
日志级别 (Log level)	选择以下一个选项： • **普通 (Normal)** - 系统默认启用此选项。普通日志记录包括严重错误、可恢复错误、警告和有用信息。 • **扩展 (Extended)** - 扩展日志记录中除了普通日志消息外，还包括调试日志消息。 您可能希望根据特定情况所需的故障排除级别更改日志级别。例如，如果您遇到了思科邮件安全插件方面的问题，可以将日志记录级别设置为**扩展 (Extended)**，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。

“发送使用情况数据”(Sending Usage Data) 选项卡

最终用户可以从“发送使用情况数据”(Sending Usage Data) 选项卡配置以下选项。

选项	说明
向思科发送匿名使用情况数据 (Send anonymous usage data to Cisco)	使思科邮件安全插件能够收集将用于改进产品的数据。将收集以下两种类型的信息并将其存储在思科服务器上以便进行分析： • 关于正在运行插件的计算机的一般信息 • 特定于帐户的信息

“隐私”(Privacy) 选项卡

最终用户可以从“隐私”(Privacy) 选项卡配置以下选项。

选项	说明
重置标识符 (Resets Identifier)	重置用于关联使用情况报告的标识符。
清除所有口令 (Clear All Passphrases)	清除所有帐户缓存的所有口令。

错误和故障排除

本部分列出了使用适用于 Outlook 的思科邮件安全插件时可能会遇到的常见错误，并提供了用于修复这些错误的一些故障排除提示。

注意　如果相同的错误反复出现，并且此错误导致适用于 Outlook 的思科邮件安全插件功能无法正常运行，最终用户可以尝试运行修复程序。请参阅修复适用于 Outlook 的思科邮件安全插件文件，第 4-56 页。如果运行修复过程后仍出现相同的错误，最终用户可根据相应步骤使用诊断工具向思科提供反馈。请参阅运行思科邮件安全诊断工具，第 4-57 页。

Outlook 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：

- *<file_name> 配置文件初始化时出错。部分设置已被设为默认值。(An error occurred during <file_name> configuration file initialization. Some settings have been set to the default values.)*
- *对帐户 <account_address> 的配置验证失败。请选择正确的配置值，或与管理员联系。(Config validation for account <account_address> has failed. Please set the correct configuration values or contact your administrator.)*

当 %ALLUSERSPROFILE%\Cisco\Cisco IronPort Email Security Plug-In\<*username*> 文件夹中的某些配置值无效或某些配置文件损坏时，会出现这些错误消息。

解决方案

思科邮件安全插件不会恢复受损配置文件中的某些加密选项的默认值，而是会关闭某些加密功能。如果最终用户重复收到错误消息，可运行维修程序对配置文件进行修复。请参阅修复适用于 Outlook 的思科邮件安全插件文件，第 4-56 页。

找不到配置文件

启动 Outlook 时可能会显示以下错误消息：

- *未找到 <file_name> 配置文件。设置已被设为默认值。(<file_name> configuration file was not found. Settings have been set to the default values.)*

解决方案

思科邮件安全插件不会恢复受损配置文件中的某些加密选项的默认值，而是会设置解密模式。如果最终用户重复收到错误消息，可运行维修程序对配置文件进行修复。请参阅修复适用于 Outlook 的思科邮件安全插件文件，第 4-56 页。

邮件报告错误

Outlook 无法识别一个或多个名称

最终用户点击 Outlook 中的**垃圾邮件 (Spam)**、**病毒 (Virus)**、**网络钓鱼 (Phish)**、**营销邮件 (Marketing)** 或**非垃圾邮件 (Not Spam)** 按钮时，可能会出现以下消息：

- *邮件报告过程中出现错误。说明：Outlook 无法识别一个或多个名称。(There was error during email reporting. Description: Outlook does not recognize one or more names.)*

当最终用户使用报告插件，而 Outlook 无法识别其尝试报告的邮件的格式时会出现此错误。最终用户将需要修复报告插件文件，以确保其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

运行修复程序。请参阅修复适用于 Outlook 的思科邮件安全插件文件，第 4-56 页。

无法连接服务器

最终用户点击 Outlook 中的**垃圾邮件 (Spam)**、**病毒 (Virus)**、**网络钓鱼 (Phish)**、**营销邮件 (Marketing)** 或**非垃圾邮件 (Not Spam)** 插件按钮和使用 IMAP 协议或“仅邮件头”(headers only) Outlook 属性时，可能会出现以下消息：

- *错误：无法连接服务器。Outlook 必须处于在线或连接状态才能完成此操作。(Error: The connection to the server is unavailable. Outlook must be online or connected to complete this action.)*

当最终用户尝试报告只下载了一部分（仅邮件头）的邮件并且与邮件服务器的连接中断时，会出现此错误。报告插件无法报告只下载了一部分的邮件，它会尝试连接邮件服务器，直到将要报告的邮件的完整副本下载下来。

解决方案

在报告仅包含邮件头的邮件时，确保 Outlook 与邮件服务器之间的连接正常。

连接服务器时出错

如果 Outlook 在线但您的网络连接丢失或服务器暂时不可用时，会出现以下错误。

- *连接服务器时出现 HTTP 错误 (An HTTP error occurred during connection to server)*。

解决方案

检查网络设置或联系本地管理员。

解密和加密错误

点击**发送 (Send)** 时，如果没有禁用安全信封选项，将显示“安全信封选项”(Secure Envelope Options) 页。邮件帐户会收到以下状态消息：

您的帐户已锁定

- *您的帐户已锁定。请联系您的帐户管理员，了解更多信息。(Your account has been locked. Please contact your account administrator for more information.)*

解决方案

联系系统管理员，以解锁邮件帐户。

您的帐户已被阻止

- *您的帐户已被阻止，您必须重置密码。请使用忘记密码链接重新激活您的帐户。(Your account has been blocked and you must reset your password. Please use the forgot password link to reactivate your account.) 忘记密码？(Forgot password?)*

解决方案

点击密码链接并输入密码安全提示问题的正确答案，以重置密码。

您的帐户已被暂停

- *您的尝试次数已用尽。您的帐户在接下来的 15 分钟处于锁定状态。(You have no attempts remaining. Your account is locked for the next 15 minutes.)*

解决方案

您可以尝试稍后登录 https://res.cisco.com/websafe 或访问 https://res.cisco.com/websafe/help?topic=ContactSupport 联系支持人员获取帮助。

无收件人

如果您未在正在发送的邮件中列出收件人，您会收到以下消息：

- *加密期间出现错误：未指定收件人 (An error occurred during encryption: no recipients specified)*。

解密期间出现错误

邮件解密期间出现意外错误。例如，SDK 返回一个未知错误代码或插件报告一个异常情况。

- *解密期间出现错误 (An error occurred during decryption)*。

解决方案

运行诊断工具并将诊断报告发送给支持团队。请参阅运行思科邮件安全诊断工具，第 4-57 页。

加密期间出现错误

邮件加密期间出现意外错误。例如，SDK 返回一个未知错误代码或插件报告一个异常情况。

- *加密期间出现错误 (An error occurred during encryption)*。

解决方案

运行诊断工具并将诊断报告发送给支持团队。请参阅运行思科邮件安全诊断工具，第 4-57 页。

超出允许的限制

加密邮件在添加附件前的默认最大大小为 7 MB，但管理员可在 *BCE_Config.xml* 文件中更改此值。如果加密邮件超过最大限制，您可能会收到以下消息之一：

- *此邮件超过了规定的限制，因此无法解密。(This message exceeds the allowable limit and cannot be decrypted.)*
- *此邮件超过了规定的限制，因此无法加密。(This message exceeds the allowable limit and cannot be encrypted.)*

- *加密期间出现错误：发现无效的附件。(An error occurred during encryption: an invalid attachment found.)*
- *无法报告此邮件。邮件过大。(Failed to report this message. This message is too large.)*
- *无法报告{0}封邮件。{0}封邮件过大。(Failed to report {0} messages. {0} messages are too large.)*

注意　*无法报告... (Failed to report ...)*的最后两条消息 目前只有英文版本。

修复适用于 Outlook 的思科邮件安全插件文件

要修复思科邮件安全插件：

步骤 1　确保已关闭 Outlook。

步骤 2　转到**控制面板 (Control Panel) > 添加或删除程序 (Add or Remove Programs)**。

步骤 3　在程序列表中找到思科邮件安全插件，然后点击**卸载/更改 (Uninstall/Change)**。

步骤 4　点击**修复 (Repair)**。系统运行安装程序修复过程。

注意　您无法恢复或修复加密配置。加密配置仅由管理员在 *BCE_Config.xml* 文件中发送。

步骤 5　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。请参阅运行思科邮件安全诊断工具，第 4-57 页。

使用诊断工具进行故障排除

思科邮件安全插件包括帮助思科支持部门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部门以协助开发人员解决问题。

如果最终用户收到错误或遇到修复过程无法解决的思科邮件安全插件问题，他们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。

请参阅修复适用于 Outlook 的思科邮件安全插件文件，第 4-56 页或运行思科邮件安全诊断工具，第 4-57 页。

注意　如果遇到错误，请查看错误和故障排除，第 4-51 页获取故障排除提示。

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
- 与 Outlook 相关的 Windows 事件日志条目

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：

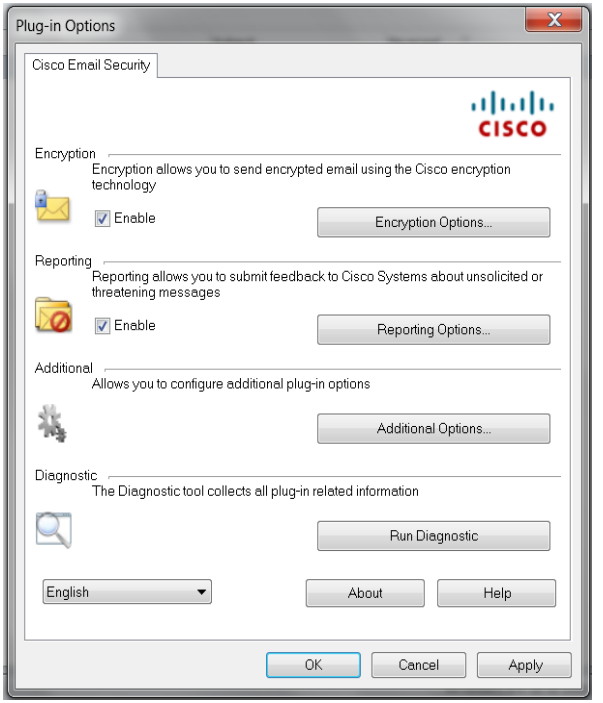
- **从“思科邮件安全选项”(Cisco Email Security options) 选项卡**。通常，您可以从“思科邮件安全选项”(Cisco Email Security options) 选项卡运行诊断工具。
- **从“Program Files\Cisco Email Security Plug-in”文件夹**（通常为 C:\Program Files\Cisco\Cisco Email Security Plug-in）。此文件夹为安装思科邮件安全插件的文件夹。
- **从“开始”(Start) 菜单 >“所有程序”(All Programs) >“思科邮件安全插件”(Cisco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

从“Outlook 选项”(Outlook Options) 页面运行诊断工具

步骤 1　按以下操作运行诊断工具：

- 在 Outlook 2010/2013 中，点击功能区中的**插件选项 (Plug-in Options)** 按钮，或转到**文件 (File) > 选项 (Options) > 加载项 (Add-ins) > 加载选项 (Add-in Options) > 思科邮件安全 (Cisco Email Security) > 运行诊断 (Run Diagnostic)**。
- 在 Outlook 2007 中，点击工具栏上的**插件选项 (Plug-in Options)** 按钮，或转到**工具 (Tools) > 选项 (Options) > 思科邮件安全 (Cisco Email Security) > 运行诊断 (Run Diagnostic)**。

思科邮件安全“加载项选项”(Add-in Options) 页：



步骤 2　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。

诊断工具将生成 *CiscoDiagnosticReport.zip* 文件并将其保存至当前用户的**我的文档 (My Documents)** 文件夹。最终用户可将此文件发送给系统管理员，或管理员可以将其发送给思科支持代表。要查看报告，请双击 *CiscoDiagnosticsReport.zip* 文件。

从 Program Files 运行诊断工具

有两种方式可以从程序文件运行诊断工具。

- 从**“开始”(Start)>“程序”(Programs) >“思科邮件安全插件”(Cisco Email Security Plug-in) > 思科邮件安全插件诊断 (Cisco Email Security Plug-in Diagnostic)** 运行诊断工具。

-或-

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

在信封中禁用 JavaScript

如果收到的邮件在信封中使用 JavaScript，会导致错误或会使信封无法打开。要避免这些问题，您可以执行以下步骤，在生成的信封中禁用 JavaScript：

步骤 1　从密钥服务器下载 BCE 配置文件模板。

以管理员身份登录密钥服务器，然后选择“帐户”(Accounts) >“管理帐户”(Manage Accounts) >“BCE 配置”(BCE Config) >“步骤 2：下载模板”(Step2: Download Template)。

步骤 2　编辑 BCE 配置文件，然后在 <encryption> 部分下的任何地方添加 <usescript>false<usescript>，或如果 <usescript> 标签已存在，将值设置为 false。

步骤 3　保存 BCE 配置文件，并在密钥服务器上进行签名。

步骤 4　将签名 BCE 配置文件发送给您的用户。

卸载思科邮件安全插件

您可以通过**控制面板 (Control Panel) > 添加/删除程序 (Add/Remove Programs)** 选项或运行 setup.exe 程序卸载思科邮件安全插件。

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。
- 某些文件与插件相关。注意并非所有文件都会删除。
- 插件工具栏（从 Outlook 删除）。

注意　卸载该插件不会影响 Outlook 性能。在卸载期间，Outlook 必须处于关闭状态。

要卸载适用于 Outlook 的思科邮件安全插件，请执行以下操作：

要卸载适用于 Outlook 的思科邮件安全插件，有两种可行的方法：

步骤 1　点击**开始 (Start) > 控制面板 (Control Panel) > 添加/删除程序 (Add/Remove Programs)**。

步骤 2　选择**思科邮件安全插件 (Cisco Email Security Plug-In)** 并点击**卸载/更改 (Uninstall/Change) > 下一步 (Next) > 删除 (Remove)**。

第二种卸载方法是

- 双击插件设置文件（用于安装此插件的文件），并选择**删除 (Remove)** 选项卸载思科邮件安全插件。

附 录 A

思科最终用户许可协议

有关 Cisco IronPort 最终用户许可协议的信息，请参阅 http://www.cisco.com/web/products/software_licensing_center.html。