思科邮件加密

本章包含以下部分：

思科邮件加密概述

AsyncOS 支持使用加密技术保护入站和出站邮件的安全。要使用此功能，可以创建加密配置文件为密钥服务器指定加密邮件和连接信息的特征。密钥服务器可以是：

- 思科注册信封服务（托管服务），或
- 思科加密设备（本地托管的服务器）

接下来，创建内容过滤器、邮件过滤器和防数据丢失策略确定要加密的邮件。

1. 符合过滤器条件的外发邮件放置在用于加密处理的邮件网关上的队列中。
2. 对邮件进行加密后，用于加密的密钥会存储在在加密配置文件中指定的密钥服务器中，并且加密的邮件会排队等待传输。
3. 如果存在禁止加密队列中邮件的临时情况（例如，临时 C 系列正忙或思科安全邮件加密服务不可用），则会对邮件重新排队并稍后重试。

Note 还可以设置邮件网关以首先尝试在加密之前通过 TLS 连接发送邮件。有关详细信息，请参阅使用 TLS 连接作为加密备用项, on page 8。

如何通过本地密钥服务器加密邮件

Table 1: 如何通过本地密钥服务器加密邮件

步骤	操作	更多信息
第 1 步	设置网络中的思科 IronPort 加密设备。	请参阅设置和安装
第 2 步	启用邮件加密。	在邮件网关上启用邮件加密, on page 4。
第 3 步	通过创建加密配置文件，指定要使用的加密密钥服务器以及用于加密邮件的安全设置。	配置密钥服务如何处理加密邮件, on page 4。
第 4 步	定义要使邮件网关对邮件进行加密，邮件必须满足的条件。	确定要加密的邮件, on page 8。
第 5 步	确定什么时候对邮件工作流程中的邮件进行加密。	• 使用内容过滤器加密并立即传送邮件, on page 9。 或 • 在传送时使用内容过滤器加密邮件, on page 10。
第 6 步	（可选）标记进行额外安全保护的邮件。	将加密信头添加到邮件, on page 11。
第 7 步	定义要为其加密邮件的用户组。	创建邮件策略。 请参阅邮件策略
第 8 步	将您定义的加密操作与定义的用户组相关联。	将内容过滤器与邮件策略相关联。 请参阅邮件策略

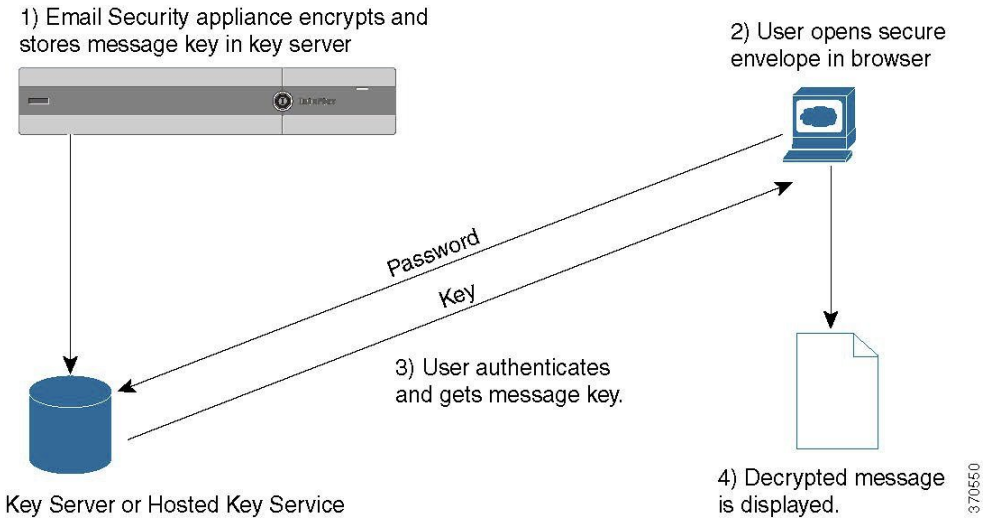
相关主题

- 加密工作流程, on page 2

加密工作流程

当使用邮件加密时，邮件网关会加密邮件，并将邮件密钥存储在本地密钥服务器或托管密钥服务中。当收件人打开加密邮件时，密钥服务会对收件人进行身份验证，并且解密的邮件将会显示。

Figure 1: 加密工作流程



打开加密邮件的基本工作流程如下：

1. 当配置加密配置文件时，可以为邮件加密指定参数。对于加密的邮件，邮件网关会在本地密钥服务器或托管密钥服务（思科注册信封服务）上创建并存储邮件密钥。
2. 收件人可在浏览器中打开安全信封。
3. 当收件人在浏览器中打开加密的邮件时，可能需要输入密码以验证收件人的身份。密钥服务器会返回与邮件关联的加密密钥。

Note 当第一次打开加密的邮件时，收件人需要注册到密钥服务以打开安全信封。在注册后，收件人可以在不进行验证的情况下打开加密的邮件，具体取决于在加密配置文件配置的设置。加密配置文件可以指定不需要密码，但是某些功能将不可用。

4. 此时将显示解密的邮件。

使用邮件网关加密邮件

要使用邮件网关进行加密，必须配置加密配置文件。可以使用 encryptionconfig CLI 命令或通过 GUI 中的“安全服务”>“Cisco IronPort 邮件加密”启用并配置加密配置文件。

Note 如果在邮件网关上启用了 PXE 和 S/MIME 加密，AsyncOS 会首先使用 S/MIME 然后再使用 PXE 来加密邮件。

相关主题

- 在邮件网关上启用邮件加密, on page 4

在邮件网关上启用邮件加密

Procedure

步骤 1 依次单击**安全服务 (Security Services) > 思科 IronPort 邮件加密 (Cisco IronPort Email Encryption)**。

步骤 2 单击**启用 (Enable)**。

步骤 3 （可选）单击**编辑设置 (Edit Settings)** 配置以下选项：

- 要加密的最大邮件大小。思科建议的邮件大小为 10 MB。邮件网关将加密的最大邮件大小为 25 MB。

  Note 加密大于推荐的 10 MB 限制的邮件可能会降低邮件网关的性能。如果要使用思科注册信封服务，邮件收件人将无法回复包含超过 10 MB 的附件的加密邮件。

- 加密账户管理员的邮件地址。调配加密配置文件时，此邮件地址会自动注册到加密服务器。
- 配置代理服务器。

配置密钥服务如何处理加密邮件

如果使用密钥服务，则可以创建一个或多个加密配置文件。如果要为不同的邮件组使用不同的安全级别，则可能需要创建不同的加密配置文件。例如，您可能希望以高安全性发送包含敏感资料的邮件，但是以中等安全性发送其他邮件。在这种情况下，可创建高安全性加密配置文件以与包含某些关键字（例如“机密”）的邮件关联，并为其他外发邮件创建另一加密配置文件。

可以将加密配置文件分配给自定义用户角色，以允许分配给该角色的授权管理员将加密配置文件与其 DLP 策略和内容过滤器配合使用。当配置 DLP 策略和内容过滤器时，只有管理员、操作员和委派的用户可以使用加密配置文件。未分配给自定义角色的加密配置文件可供具有邮件或 DLP 策略权限的所有委派管理员使用。有关详细信息，请参阅分配管理任务。

Note 可以为托管密钥服务配置多个加密配置文件。如果贵组织有多个品牌，这样使您可以参考存储在PXE信封的密钥服务器中的不同徽标。

加密配置文件会存储以下设置：

- **密钥服务器设置**。指定密钥服务器和信息以用于连接到该密钥服务器。

- **信封设置**。指定有关邮件信封的详细信息，例如安全级别、是否返回已读回执、邮件在超时之前排队进行加密的时间长度、要使用的加密算法类型以及是否启用在浏览器中运行的解密小程序。
- **邮件设置**。指定有关邮件的详细信息，例如是否启用安全邮件转发和安全的全部回复。
- **通知设置**。指定要用于文本和 HTML 通知的通知模板，以及加密失败通知。在创建加密配置文件时，在文本资源中创建模板并选择模板。还可以本地化信封并为加密失败通知指定邮件主题。有关通知的详细信息，请参阅加密通知模板和退回和加密失败通知模板。

Procedure

步骤 1 在“邮件加密配置文件”(Email Encryption Profiles) 部分中，单击**添加加密配置文件 (Add Encryption Profile)**。

步骤 2 输入加密配置文件的名称。

步骤 3 单击**使用者（角色）(Used By [Roles])** 链接，选择要为其分配对加密配置文件访问权限的自定义用户角色，然后单击**确定 (OK)**。

分配给此自定义角色的委派管理员可以将该加密配置文件用于任何 DLP 策略以及它们负责的内容过滤器。

步骤 4 在“密钥服务器设置”(Key Server Settings) 部分中，从以下密钥服务器中进行选择：

- 思科加密设备（网内）
- 思科注册信封服务（托管密钥服务）

步骤 5 如果选择思科加密设备（本地密钥服务），请输入以下设置：

- **内部 URL**。此 URL 由邮件网关用于联系网络中的思科加密设备。
- **外部 URL**。当收件人的邮件访问思科加密设备上的密钥和其他服务时，会使用该 URL。收件人使用此 URL 提出入站 HTTP 或 HTTPS 请求。

步骤 6 如果选择思科注册信封服务，请为托管密钥服务输入该 URL。密钥服务 URL 为 https://res.cisco.com。

步骤 7 在“密钥服务器设置”(Key Server Settings) 下单击**高级 (Advanced)**，以指定在收件人打开信封时是使用 HTTP 还是 HTTPS 来传输信封的加密负载。选择以下其中一项：

- **将密钥服务与 HTTP 配合使用**。当收件人打开信封时，使用 HTTP 从密钥服务传输加密的负载。如果您使用的是思科注册信封服务，这是在第 6 步中指定的 URL。如果您使用的是思科加密设备，这是在第 5 步中指定的外部 URL。
- 由于已加密负载，因此通过 HTTP 传输它是安全的，而且比通过 HTTPS 传输更加快速。这会提供比通过 HTTPS 发送图像请求更好的性能。
- **将密钥服务与 HTTPS 配合使用**。当收件人打开信封时，使用 HTTPS 从密钥服务传输加密的负载。如果您使用的是思科注册信封服务，这是在第 6 步中指定的 URL。如果您使用的是思科加密设备，这是在第 5 步中指定的外部 URL。

- **为负载传输指定一个单独的URL**。如果不希望将密钥服务器用于加密的负荷，则可以使用另一个 URL 并指定是使用 HTTP 或还是 HTTPS 进行负载传输。

步骤 8 在“信封设置”(Envelope Settings) 部分中，选择邮件安全级别：

- **高安全性**。收件人必须始终输入密码才能打开加密邮件。
- **中等安全性**。如果已缓存收件人凭证，则收件人不需要输入凭证便可打开加密邮件。
- **不需要密码**。这是最低级别的加密邮件安全性。收件人不需要输入密码就能打开加密的邮件。您仍可为不受密码保护的信封启用阅读回执、安全的全部回复和安全邮件转发功能。

步骤 9 要允许用户通过单击其徽标来打开贵组织的 URL，可以添加指向徽标的链接。从以下选项中选择：

- **无链接**。未向邮件信封添加有效链接。
- **自定义链接 URL**。输入 URL，将有效链接添加到邮件信封。

步骤 10 （可选）启用阅读回执。如果启用该选项，则收件人打开安全信封时，发件人将收到回执。

步骤 11 （可选）在“信封设置”(Envelope Settings) 下单击**高级 (Advanced)** 以配置以下设置：

- 输入邮件超时之前，可以在加密队列中存在的时间长度（以秒为单位）。邮件超时后，邮件网关将退回该邮件并向发件人发送通知。
- 选择加密算法 - 'AES 192' 或 'AES 256'。

  Note AES 提供更强大的加密，但是还需要更长时间进行解密，为收件人产生延迟。AES 通常用于政府和银行应用。

- 启用或禁用解密小序。启用此选项可导致在浏览器环境中打开邮件附件。禁用此选项会导致在密钥服务器中解密邮件附件。如果禁用此选项，则打开邮件可能需要更长时间，但是不依赖于浏览器环境。

步骤 12 在“邮件设置”(Message Settings) 部分中，执行以下操作：

- 要启用安全的全部回复功能，请选中**启用安全的全部回复 (Enable Secure Reply All)** 复选框。
- 要启用安全邮件转发功能，请选中**启用安全邮件转发 (Enable Secure Message Forwarding)** 复选框。

步骤 13 （可选）如果选择了思科注册信封服务并且此服务支持信封本地化，可启用信封的本地化。在“通知设置”(Notification Settings) 部分中，选中**使用本地化信封 (Use Localized Envelope)** 复选框。

Note 如果启用信封的本地化，则不能选择加密邮件 HTML 或文本通知。

如果要设置信封的默认区域设置，请参阅配置信封的默认区域设置, on page 7。

步骤 14 选择 HTML 和文本通知模板。

Note 密钥服务器基于收件人的邮件应用使用 HTML 或文本通知。必须为两者都配置通知。

执行以下操作：

a) 选择一个 HTML 通知模板。从在文本资源中配置的 HTML 通知中进行选择。如果没有配置模板，系统将使用默认模板。
b) 选择一个文本通知模板。从在文本资源中配置的文本通知中进行选择。如果没有配置模板，系统将使用默认模板。

Note 如果使用本地化信封，这些选项将不可用。

步骤 15 输入加密失败通知的主题信头。如果加密过程超时，则邮件网关会发送通知。

步骤 16 为邮件正文选择加密失败通知模板。从在文本资源中配置的加密失败通知模板中进行选择。如果没有配置模板，系统将使用默认模板。

步骤 17 提交并确认更改。

步骤 18 如果使用思科注册信封服务，则必须执行额外的调配邮件网关步骤。调配邮件网关会通过托管密钥服务注册加密配置文件。要调配邮件网关，请单击要注册的加密配置文件的**调配 (Provision)** 按钮。

配置信封的默认区域设置

信封的默认区域设置为“英语”(English)。如果选择了思科注册信封服务且该服务支持信封的本地化，则可以将信封的区域设置更改为下列任一项：

- 英语
- 法语
- 德语
- 日语
- 葡萄牙语
- 西班牙语
- 意大利语
- 韩语
- 荷兰语
- 波兰语
- 俄文
- 中文

准备工作

- 在思科注册信封服务作为密钥服务类型且启用了信封本地化的情况下，创建加密配置文件。请参阅配置密钥服务如何处理加密邮件, on page 4。
- 确保思科注册信封服务支持信封的本地化。

Procedure

步骤 1 依次单击**安全服务 (Security Services)** > **思科 IronPort 邮件加密 (Cisco IronPort Email Encryption)**。

步骤 2 打开现有的加密配置文件。

步骤 3 在**通知设置 (Notification Settings)** 部分中，从**本地化信封 (Localized Envelopes)** 下拉列表中选择区域设置。

步骤 4 单击**提交 (Submit)**。

步骤 5 单击**确认更改 (Commit Changes)**。

更新为 PXE 引擎的最新版本

思科邮件加密设置页面会显示 PXE 引擎的最新版本以及邮件网关使用的域映射文件。您可以使用**安全服务 (Security Services)** > **服务更新 (Service Updates)**页面（或 CLI 中的 updateconfig 命令）将邮件网关配置为自动更新 PXE 引擎。有关详细信息，请参阅服务更新。

还可以使用“IronPort 邮件加密设置”(IronPort Email Encryption Settings) 页面中“PXE 引擎更新”(PXE Engine Updates) 部分的**立即更新 (Update Now)** 按钮（或 CLI 中的 **`encryptionupdate`** 命令）手动更新引擎。

确定要加密的邮件

创建加密配置文件后，需要创建确定应加密哪些邮件的传出邮件内容过滤器。内容过滤器扫描传出的邮件，并确定邮件是否与指定的条件匹配。内容过滤器确定邮件与相应条件匹配后，邮件网关会加密邮件并将生成的密钥发送到密钥服务器。它会使用在加密配置文件中指定的设置来确定要使用的密钥服务器和其他加密设置。

还可以在防数据丢失扫描后放行了邮件时，对邮件进行加密。有关详细信息，请参阅定义要针对 DLP 违规采取的操作（邮件操作）。

相关主题

- 使用 TLS 连接作为加密备用项, on page 8
- 使用内容过滤器加密并立即传送邮件, on page 9
- 在传送时使用内容过滤器加密邮件, on page 10

使用 TLS 连接作为加密备用项

根据为域指定的目标控制，如果 TLS 连接可用，则邮件网关可以安全地通过 TLS 连接中继邮件而不是加密它。邮件网关会根据目标控制中的 TLS 设置（“必需”(Required)、“首选”(Preferred) 或“无”(None)）以及在加密内容过滤器中定义的操作，确定是加密邮件还是通过 TLS 连接发送邮件。

创建内容过滤器时，可以指定是始终加密邮件还是首先尝试通过 TLS 连接发送邮件，并且如果 TLS 连接不可用，则对邮件进行加密。下表显示了当加密控制过滤器首先尝试通过 TLS 连接发送邮件时，邮件网关如何基于域目标控制的 TLS 设置发送邮件。

Table 2: 邮件网关上的 ***TLS*** 支持

目标控制 TLS 设置	TLS 连接可用时的操作	TLS 连接不可用时的操作
无	加密信封并发送	加密信封并发送
首选 TLS	通过 TLS 发送	加密信封并发送
需要 TLS	通过 TLS 发送	重试/退回邮件

有关在目标控制中启用 TLS 的详细信息，请参阅配置网关以接收邮件。

使用内容过滤器加密并立即传送邮件

准备工作

- 要了解为内容过滤器构建条件的概念，请参阅内容过滤器概述。
- （可选）请参阅将加密信头添加到邮件, on page 11。

Procedure

步骤 1 依次转到**邮件策略 (Mail Policies) > 传出邮件内容过滤器 (Outgoing Content Filters)**。

步骤 2 在“过滤器”(Filters) 部分，单击**添加过滤器 (Add Filter)**。

步骤 3 在“条件”(Conditions) 部分，单击**添加条件 (Add Condition)**。

步骤 4 添加一个条件以过滤要加密的邮件。例如，要加密敏感材料，可以添加一个条件来识别主题或正文中包含特定字词或短语（例如“机密”）的邮件。

步骤 5 单击**确定 (OK)**。

步骤 6 或者，单击**添加操作 (Add Action)**，然后选择**添加信头 (Add Header)** 将加密信头插入邮件以指定一个额外的加密设置。

步骤 7 在“操作”(Actions) 部分，单击**添加操作 (Add Action)**。

步骤 8 从**添加操作 (Add Action)** 列表中选择**立即加密并发送（最终操作）(Encrypt and Deliver Now [Final Action])**。

步骤 9 选择是始终加密符合条件的邮件还是仅在尝试通过 TLS 连接发送邮件失败时加密邮件。

步骤 10 选择加密配置文件以与内容过滤器相关联。

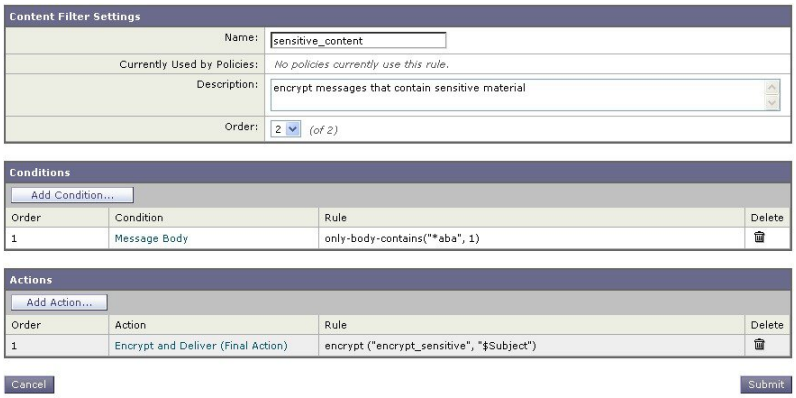
加密配置文件会指定有关要使用的密钥服务器、安全性级别、邮件信封格式的设置，以及其他邮件设置。将加密配置文件与内容过滤器相关联时，内容过滤器会使用存储的设置来加密邮件。

步骤 11 输入邮件的主题。

步骤 12 单击**确定 (OK)**。

下图中的内容过滤器显示了在邮件正文中搜索 ABA 内容的内容过滤器。为内容过滤器定义的操作指定将加密并传送邮件。

Figure 2: 加密内容过滤器



步骤 13 添加加密操作后，单击**提交 (Submit)**。

步骤 14 确认更改。

What to do next

添加内容过滤器后，需要将该过滤器添加到传出邮件策略中。您可能希望在默认策略中启用该内容过滤器，也可以选择将该过滤器应用到特定邮件策略，具体取决于组织的需求。有关使用邮件策略的信息，请参阅邮件策略概述。

在传送时使用内容过滤器加密邮件

在传送时创建内容过滤器来加密邮件，这表示邮件继续下一阶段的处理，而且当所有处理完成后，将加密并传送邮件。

准备工作

- 要了解为内容过滤器构建条件的概念，请参阅内容过滤器概述。
- （可选）请参阅将加密信头添加到邮件, on page 11。

Procedure

步骤 1 依次转到**邮件策略 (Mail Policies)** > **传出邮件内容过滤器 (Outgoing Content Filters)**。

步骤 2 在“过滤器”(Filters) 部分，单击**添加过滤器 (Add Filter)**。

步骤 3 在“条件”(Conditions) 部分，单击**添加条件 (Add Condition)**。

步骤 4 添加一个条件以过滤要加密的邮件。例如，要加密敏感材料，可以添加一个条件来识别主题或正文中包含特定字词或短语（例如“机密”）的邮件。

步骤 5 单击**确定 (OK)**。

步骤 6 或者，单击**添加操作 (Add Action)**，然后选择**添加信头 (Add Header)** 将加密信头插入邮件以指定一个额外的加密设置。

步骤 7 在“操作”(Actions) 部分，单击**添加操作 (Add Action)**。

步骤 8 从**添加操作 (Add Action)** 列表中选择**传送时加密 (Encrypt on Delivery)**。

步骤 9 选择是始终加密符合条件的邮件还是仅在尝试通过 TLS 连接发送邮件失败时加密邮件。

步骤 10 选择加密配置文件以与内容过滤器相关联。

加密配置文件会指定有关要使用的密钥服务器、安全性级别、邮件信封格式的设置，以及其他邮件设置。将加密配置文件与内容过滤器相关联时，内容过滤器会使用存储的设置来加密邮件。

步骤 11 输入邮件的主题。

步骤 12 单击**确定 (OK)**。

步骤 13 添加加密操作后，单击**提交 (Submit)**。

步骤 14 确认更改。

What to do next

添加内容过滤器后，需要将该过滤器添加到传出邮件策略中。您可能希望在默认策略中启用该内容过滤器，也可以选择将该过滤器应用到特定邮件策略，具体取决于组织的需求。有关使用邮件策略的信息，请参阅邮件策略概述。

将加密信头添加到邮件

AsyncOS 支持使用内容过滤器或邮件过滤器将 SMTP 信头插入邮件，从而将加密设置添加到邮件。加密信头可以覆盖在关联的加密配置文件中定义的加密设置，而且它可以将指定的加密功能应用到邮件。

Note 必须设置思科 Ironport 设备来处理标记的邮件。

Procedure

步骤 1 依次转到**邮件策略 (Mail Policies)** > **传出邮件内容过滤器 (Outgoing Content Filters)** 或**传入内容过滤器 (Incoming Content Filters)**。

步骤 2 在“过滤器”(Filters) 部分，单击**添加过滤器 (Add Filter)**。

步骤 3 在“操作”(Actions) 部分，单击**添加操作 (Add Action)**，然后选择**添加/编辑信头 (Add/Edit Header)** 将加密信头插入邮件以指定一个额外的加密设置。

例如，如果希望注册的信封在发送后的 24 小时内过期，请键入 X-PostX-ExpirationDate 作为信头名称，并且键入 +24:00:00 作为信头值。

What to do next

相关主题

- 加密信头, on page 12
- 加密信头示例, on page 13
- 有关创建加密内容过滤器的详细信息，请参阅使用内容过滤器加密并立即传送邮件, on page 9。
- 有关使用邮件过滤器插入信头的信息，请参阅使用邮件过滤器实施邮件策略。

加密信头

下表显示可以添加到邮件的加密信头。

Table 3: 邮件加密信头

MIME 信头	说明	值
X-PostX-Reply- Enabled	指示是否为邮件启用安全回复，并在邮件栏中显示“回复”(Reply) 按钮。此信头会将加密设置添加到邮件。	有关是否显示“回复”(Reply) 按钮的布尔值。设置为 true 可显示该按钮。默认值为 false。
X-PostX-Reply-All-Enabled	指示是否为邮件启用安全的“全部回复”，并在邮件栏中显示“全部回复”(Reply All) 按钮。此信头会覆盖默认配置文件设置。	有关是否显示“全部回复”(Reply All) 按钮的布尔值。设置为 true 可显示该按钮。默认值为 false。
X-PostX-Forward-Enabled	指示是否启用安全邮件转发，并在邮件栏中显示“转发”(Forward) 按钮。此信头会覆盖默认配置文件设置。	有关是否显示“转发”(Forward) 按钮的布尔值。设置为 true 可显示该按钮。默认值为 false。
X-PostX-Send-Return-Receipt	指示是否启用阅读回执。当收件人打开安全信封时，发件人将收到回执。此信头会覆盖默认配置文件设置。	有关是否发送阅读回执的布尔值。设置为 true 可显示该按钮。默认值为 false。
X-PostX-Expiration Date	在发送之前定义注册信封的到期日期。密钥服务器会在到期日期之后限制对注册信封的访问。注册信封会显示消息指明邮件已过期。此信头会将加密设置添加到邮件。 如果使用思科注册信封服务，则可以登录到网站 http://res.cisco.com 并使用邮件管理功能设置、调整或消除发送邮件后的邮件到期日期。	包含相对日期或时间的字符串值。将 +HH:MM:SS 格式用于相对小时、分钟和秒，将 +D 格式用于相对日期。默认情况下，没有到期日期。

MIME 信头	说明	值
X-PostX-ReadNotification Date	在发送前定义注册信封的“阅读”日期。如果注册信封未在此日期之前阅读，则本地密钥服务器生成通知。具有此信头的注册信封不使用思科注册信封服务，只有使用一个本地密钥服务器。此信头会将加密设置添加到邮件。	包含相对日期或时间的字符串值。将 +HH:MM:SS 格式用于相对小时、分钟和秒，将 +D 格式用于相对日期。默认情况下，没有到期日期。
X-PostX-Suppress-Applet-For-Open	指示是否禁用解密小程序。解密小应用程序会导致在浏览器环境中打开邮件附件。禁用此小应用程序会导致在密钥服务器中解密邮件附件。如果禁用此选项，则打开邮件可能需要更长时间，但是它们不依赖于浏览器环境。此信头会覆盖默认配置文件设置。	指示是否禁用解密小程序的布尔值。设置为 true 可禁用小程序。默认值为 false。
X-PostX-Use-Script	指示是否发送无 JavaScript 的信封。无 JavaScript 的信封是不包括用于在收件人计算机本地打开信封的 JavaScript 的注册信封。收件人必须使用在线打开方法或通过转发打开方法查看邮件。如果收件人域的网关剥离 JavaScript 并使加密消息不可打开，可使用此信头。此信头会将加密设置添加到邮件。	用于指明是否包含 JavaScript 小程序的布尔值。设置为 false 可发送无 JavaScript 的信封。默认值为 true。
X-PostX-Remember-Envelope-Key-Checkbox	指示是否允许通过信封特定的密钥缓存来离线打开信封。通过信封密钥缓存，当收件人输入正确的密码并选中“记住此信封的密码”复选框时，会在收件人计算机上缓存特定信封的解密密钥。随后，收件人不需要重新输入密码，便可在计算机上重新打开信封。此信头会将加密设置添加到邮件。	用于指明是否启用密钥缓存并显示“记住此信封的密码”(Remember the password for this envelope) 复选框的布尔值。默认值为 false。

加密信头示例

本部分提供 XML 信头的示例。

相关主题

- 启用无 JavaScript 的信封, on page 14
- 启用信封密钥缓存进行离线打开, on page 13
- 启用邮件到期, on page 14
- 禁用解密小程序, on page 14

启用信封密钥缓存进行离线打开

要在启用了信封密钥缓存的情况下发送注册信封，请将以下信头插入邮件中：

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

“记住此信封的密码”(Remember the password for this envelope) 复选框会在显示注册信封中。

启用无 JavaScript 的信封

要发送无 JavaScript 的注册信封，请将以下信头插入邮件中：

```
X-PostX-Use-Script: false
```

当收件人打开 securedoc.html 附件时，会显示具有“在线打开”(Open Online) 链接的注册信封，并且“打开”(Open) 按钮已禁用。

启用邮件到期

要配置邮件，以便其在发送后的 24 小时过期，请将以下信头插入邮件中：

```
X-PostX-ExpirationDate: +24:00:00
```

在发送后的24小时内，收件人可以打开并查看加密邮件的内容。随后，注册信封会显示消息指明信封已过期。

禁用解密小程序

要禁用解密小程序并在密钥服务器中解密邮件附件，请将以下信头插入邮件中：

```
X-PostX-Suppress-Applet-For-Open: true
```

Note 当禁用了解密小程序时，可能需要更长时间打开邮件，但是这不依赖于浏览器环境。