



S/MIME 安全服务

本章包含以下部分：

- [S/MIME 安全服务概述, on page 1](#)
- [邮件网关中的 S/MIME 安全服务, on page 1](#)
- [使用 S/MIME 签名并/或加密传出邮件, on page 4](#)
- [使用 S/MIME 验证、解密或解密并验证传入的邮件, on page 14](#)
- [S/MIME 证书要求, on page 20](#)
- [管理公钥, on page 21](#)

S/MIME 安全服务概述

安全/多用途互联网邮件扩展 (S/MIME) 是一种基于标准的用于发送和接收经过验证的安全邮件的方法。S/MIME 使用公钥/私钥对来对邮件加密或签名。这样，

- 如果邮件进行了加密，则只有邮件收件人才能打开加密的邮件。
- 如果邮件进行了签名，则邮件收件人可验证发件人的域的身份，并可确保邮件在传输过程中未被修改。

有关 S/MIME 的详细信息，请查看以下 RFC：

- RFC 5750：安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 证书处理
- RFC 5751：安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 邮件规范
- RFC 3369：邮件语法加密

邮件网关中的 S/MIME 安全服务

组织可能希望使用 S/MIME 安全地通信，而无需所有最终用户都拥有自己的证书。对于此类组织，邮件网关支持使用标识组织（而不是个人用户）的证书在网关级别执行 S/MIME 安全服务（签名、加密、验证和解密）。

邮件网关为企业到企业 (B2B) 和企业到消费者 (B2C) 场景提供以下 S/MIME 安全服务：

- 使用 S/MIME 对邮件签名、加密或签名并加密。请参阅[使用 S/MIME 签名并/或加密传出邮件, on page 4](#)。
- 使用 S/MIME 验证、解密邮件或解密并验证邮件。请参阅[使用 S/MIME 验证、解密或解密并验证传入的邮件, on page 14](#)。

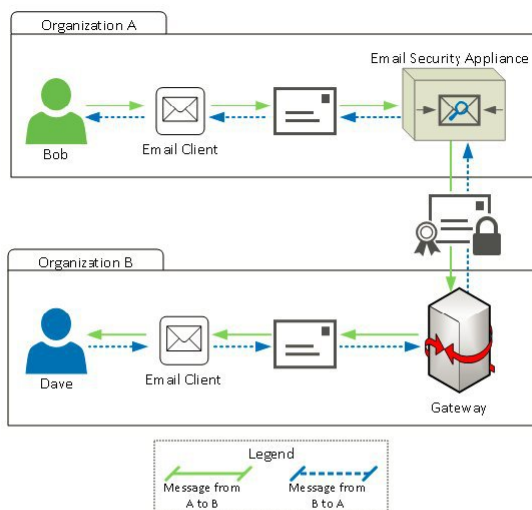
相关主题

- [了解 S/MIME 安全服务的工作方式, on page 2](#)

了解 S/MIME 安全服务的工作方式

- [场景：企业到企业, on page 2](#)
- [场景：企业到消费者, on page 3](#)

场景：企业到企业



组织 A 和 B 希望它们之间传输的所有邮件都使用 S/MIME 签名和加密。组织 A 配置了思科安全邮件网关，在网关级别执行 S/MIME 安全服务。组织 B 配置了第三方应用，在网关级别执行 S/MIME 安全服务。

**Note**

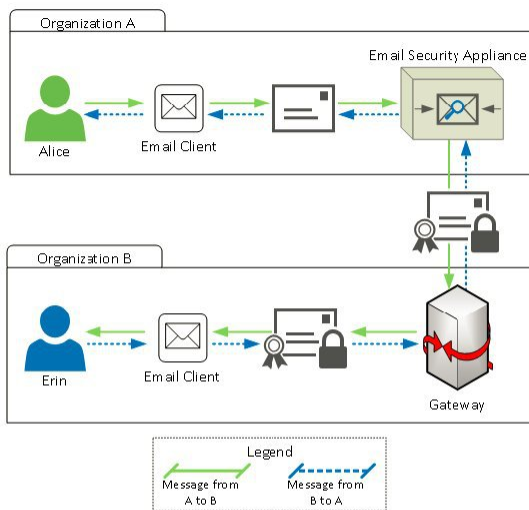
当前示例假设组织 B 使用第三方应用来执行 S/MIME 安全服务。实际上，可以使用能在网关级别执行 S/MIME 安全服务的任何应用或邮件网关（包括思科安全邮件网关）。

组织 A 向组织 B 发送邮件：

1. Bob（组织 A）使用邮件客户端向 Dave（组织 B）发送未签名和加密的邮件。
2. 组织 A 中的思科安全邮件网关对邮件签名并加密，然后将其发送到组织 B。
3. 组织 B 网关的第三方应用解密并验证该邮件。
4. Dave 收到未加密但已签名的邮件。

组织 B 向组织 A 发送邮件：

1. Dave（组织 B）使用邮件客户端向 Bob（组织 A）发送未签名和加密的邮件。
2. 组织 B 网关的第三方应用对邮件签名并加密，然后将其发送到组织 A。
3. 组织 A 中的思科安全邮件网关解密并验证该邮件。
4. Bob 收到未加密但已签名的邮件。

场景：企业到消费者

组织 A 和 B 希望它们之间传输的所有邮件都使用 S/MIME 签名和加密。组织 A 配置了思科安全邮件网关，在网关级别执行 S/MIME 安全服务。组织 B 配置了所有用户的邮件客户端来执行 S/MIME 安全服务。

组织 A 向组织 B 发送邮件：

1. Alice（组织 A）使用邮件客户端向 Erin（组织 B）发送未签名和加密的邮件。
2. 组织 A 中的安全邮件网关对邮件签名并加密，然后将其发送到组织 B。
3. 组织 B 的邮件客户端解密并验证该邮件，然后为 Erin 显示邮件内容。

组织 B 向组织 A 发送邮件：

1. Erin（组织 B）使用邮件客户端对邮件签名并加密，然后将其发送给 Alice（组织 A）。
2. 组织 A 中的安全邮件网关解密并验证该邮件。
3. Alice 收到未加密和签名的邮件。

使用 S/MIME 签名并/或加密传出邮件

- [邮件网关中的 S/MIME 签名和加密工作流程, on page 4](#)
- [如何使用 S/MIME 签名、加密或签名并加密传出邮件, on page 5](#)
- [设置用于 S/MIME 签名的证书, on page 6](#)
- [设置用于 S/MIME 加密的公钥, on page 8](#)
- [管理 S/MIME 发送配置文件, on page 10](#)
- [确定要签名、加密或签名并加密的邮件, on page 13](#)
- [使用内容过滤器签名、加密或签名并加密及立即传送邮件, on page 13](#)
- [传送时使用内容过滤器签名并/或加密邮件, on page 13](#)



Note

您可以使用邮件网关签名、加密及签名并加密传出和传入的邮件。

邮件网关中的 S/MIME 签名和加密工作流程

- [S/MIME 签名工作流程, on page 4](#)
- [S/MIME 加密工作流程, on page 5](#)

S/MIME 签名工作流程

以下过程介绍邮件网关如何执行 S/MIME 签名。

1. 对邮件应用散列算法，以创建邮件摘要。
2. 利用邮件网关的 S/MIME 证书私钥对邮件摘要加密。
3. 利用加密的邮件摘要和邮件网关的 S/MIME 证书公共密钥创建 PKCS7 签名。
4. 通过将 PKCS7 签名附加到邮件中，对邮件签名。

5. 将签名的邮件发送给收件人。

S/MIME 加密工作流程

以下过程介绍邮件网关如何执行 S/MIME 加密。

1. 创建一个伪随机的会话密钥。
2. 使用该会话密钥对邮件正文加密。
3. 使用收件人（网关或消费者）的 S/MIME 证书公钥对该会话密钥加密。
4. 将加密的会话密钥附加到邮件中。
5. 将加密的邮件发送给收件人。



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

如何使用 S/MIME 签名、加密或签名并加密传出邮件

步骤	操作	更多信息
第 1 步	了解 S/MIME 证书要求。	请参阅 S/MIME 证书要求, on page 20 。
第 2 步	根据您的要求，执行以下操作之一： <ul style="list-style-type: none"> • 要执行 S/MIME 签名，请设置 S/MIME 签名证书。 • 要执行 S/MIME 加密，请设置收件人 S/MIME 证书的公钥。 • 要执行 S/MIME 签名并加密，请分别设置 S/MIME 签名证书和收件人 S/MIME 证书的公钥。 	请参阅： <ul style="list-style-type: none"> • 设置用于 S/MIME 签名的证书, on page 6 • 设置用于 S/MIME 加密的公钥, on page 8
第 3 步	创建一个配置文件用于签名、加密或签名并加密邮件。	请参阅 创建签名、加密或签名和加密邮件的 S/MIME 发送配置文件, on page 11 。
第 4 步	定义邮件网关要对邮件签名、加密或签名并加密，邮件所必须满足的条件。	请参阅 确定要签名、加密或签名并加密的邮件, on page 13 。
第 5 步	确定在邮件工作流程中对邮件签名、加密或签名并加密的时间。	请参阅： <ul style="list-style-type: none"> • 使用内容过滤器签名、加密或签名并加密及立即传送邮件, on page 13 • 传送时使用内容过滤器签名并/或加密邮件, on page 13

步骤	操作	更多信息
第 6 步	定义要对其邮件签名或加密的用户组。	创建邮件策略。 请参阅 邮件策略
第 7 步	将定义的签名或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



Note 如果要使用 CLI 执行 S/MIME 签名、加密或签名并加密，请使用 `smimeconfig` 命令。请参阅《适用于思科安全邮件网关的 *AsyncOS CLI* 参考指南》。

设置用于 S/MIME 签名的证书

要对邮件签名，必须设置 S/MIME 证书。邮件网关允许您使用以下方法之一设置 S/MIME 签名证书。

- 使用邮件网关创建自签名 S/MIME 证书。请参阅[创建自签名 S/MIME 证书, on page 6](#)。
- 将现有的 S/MIME 证书导入到邮件网关。请参阅[导入 S/MIME 签名证书, on page 8](#)。



Note 要将签名邮件发送给组织内或测试环境中的用户，思科建议使用自签名 S/MIME 证书。要将签名邮件发送给外部用户或生产环境中的用户，请使用从可信颁发机构获取的有效 S/MIME 证书。

要了解 S/MIME 的证书要求，请参阅[S/MIME 证书要求, on page 20](#)。

创建自签名 S/MIME 证书

您可以使用 Web 界面或 CLI 生成符合 RFC 5750（安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 证书处理）要求的自签名 S/MIME 证书。



Note 要将签名邮件发送给组织内或测试环境中的用户，思科建议使用自签名 S/MIME 证书。

Procedure

- 步骤 1** 依次单击网络 (Network) > 证书 (Certificates)。
- 步骤 2** 单击添加证书 (Add Certificate)。
- 步骤 3** 选择创建自签名 S/MIME 证书 (Create Self-Signed S/MIME Certificate)。
- 步骤 4** 为自签名证书输入以下信息：

公共名称	完全限定域名。
组织	组织精确的法定名称。
组织单位	组织的部门。
城市（地区）	组织法定所在的城市。
省/市/自治区	组织法定所在的省/市/自治区、县或区域。
国家/地区	组织法定所在国家/地区的双字母 ISO 缩写。
过期前的持续时间	证书到期之前的天数。
主题备用名称(域)	如果配置了此字段，则来自指定域的所有用户均可发送签名邮件。 计划从中发送签名邮件的域的名称。示例包括 domain.com 和 *.domain.net。对于多个条目，请使用逗号分隔值列表。
主题备用名称(邮件)	如果配置了此字段，则只有指定用户可以发送签名邮件。 计划发送签名邮件的用户的邮件地址，例如 user@somedomain.com。对于多个条目，请使用逗号分隔值列表。
私钥大小	生成证书签名请求 (CSR) 的私钥大小。

Note S/MIME 签名证书可能包含“主题备用名称(域)” (Subject Alternative Name (Domains)) 和“主题备用名称(邮件)” (Subject Alternative Name (Email))。

步骤 5 单击下一步 (Next) 查看证书和签名信息。

步骤 6 根据您的要求，执行以下操作：

- 选中 **FQDN 验证 (FQDN Validation)** 复选框，以便允许邮件网关检查证书中是否存在“公共名称” (Common Name)、“SAN: DNS 名称” (SAN: DNS Name) 字段或两者同时存在，以及是否为 FQDN 格式。
- 为证书输入一个名称。
- 如果您要将自签名证书的 CSR 提交给证书颁发机构，请单击**下载证书签名请求 (Download Certificate Signing Request)**，以将 PEM 格式的 CSR 保存到本地或网络计算机。

步骤 7 提交并确认更改。

What to do next



Note 在 CLI 中，使用 `certconfig` 命令可生成自签名 S/MIME 证书。

导入 S/MIME 签名证书

如果已有用来签名邮件的 S/MIME 证书，可以通过导入将其添加到邮件网关中。

准备工作

请确保计划导入的 S/MIME 证书符合[S/MIME 证书要求, on page 20](#)中所述的要求。

Procedure

步骤 1 依次单击网络 (Network) > 证书 (Certificates)。

步骤 2 单击添加证书 (Add Certificate)。

步骤 3 选择导入证书 (Import Certificate)。

步骤 4 输入指向网络或本地计算机中的证书文件的路径。

步骤 5 输入该文件的密码。

步骤 6 单击下一步 (Next) 查看证书的信息。

步骤 7 [可选] 选中 **FQDN 验证 (FQND Validation)** 复选框，以便允许邮件网关检查证书中是否存在“公共名称” (Common Name)、“SAN: DNS 名称” (SAN: DNS Name) 字段或两者同时存在，以及是否为 FQDN 格式。

步骤 8 为证书输入一个名称。

步骤 9 提交并确认更改。

What to do next



Note 在 CLI 中，使用 `certconfig` 命令可导入 S/MIME 证书。

设置用于 S/MIME 加密的公钥

只有将收件人 S/MIME 证书的公共密钥添加到邮件网关中，才能对邮件加密。根据组织的策略和流程，可以使用下列方法之一将公共密钥添加到邮件网关：

- 请求收件人使用电子通道（例如邮件）发送公钥。然后，可以使用 Web 界面或 CLI 添加公钥。有关添加公钥的说明，请参阅[添加用于 S/MIME 加密的公钥, on page 9](#)。
- 使用 Web 界面或 CLI 启用公钥搜集，并请求收件人发送签名的邮件。邮件安全邮件网关可从签名邮件中搜集公共密钥。有关从传入的签名邮件中搜集公钥的说明，请参阅[搜集公钥, on page 9](#)。

添加用于 S/MIME 加密的公钥

准备工作

- 确保公钥符合[S/MIME 证书要求, on page 20](#)中所述的要求。
- 确保公钥为 PEM 格式。

Procedure

步骤 1 依次单击邮件策略 (Mail Policies) > 公钥 (Public Keys)。

步骤 2 单击添加公钥 (Add Public Key)。

步骤 3 输入公钥的名称。

步骤 4 输入公钥。

步骤 5 提交并确认更改。

What to do next



Note 在 CLI 中，使用 `smimeconfig` 命令可添加公钥。

S/MIME 搜集的公钥

您可以将邮件网关配置为从传入的 S/MIME 签名邮件中检索（搜集）公共密钥，并利用搜集到的密钥将加密邮件发送给其所有者（企业或消费者）。

在“邮件流策略” (Mail Flow Policies) 中可以启用公钥搜集。“S/MIME 搜集的公钥” (S/MIME Harvested Public Keys) 页面将列出搜集的所有公钥。

相关主题

- [搜集公钥, on page 9](#)

搜集公钥

您可以将邮件网关配置为从传入的 S/MIME 签名邮件中检索（搜集）公共密钥，并利用搜集到的密钥将加密邮件发送给其所有者（企业或消费者）。



Note 默认情况下，不会从过期或自签名 S/MIME 证书中搜集公钥。

准备工作

确保发件人 S/MIME 证书的公钥符合[S/MIME 证书要求, on page 20](#)中所述的要求。

Procedure

- 步骤 1** 依次单击邮件策略 (Mail Policies) > 邮件流策略 (Mail Flow Policies)。
- 步骤 2** 创建新的邮件流策略或修改现有的邮件流策略。
- 步骤 3** 向下滚动至安全功能 (Features) 部分。
- 步骤 4** 在“S/MIME 公钥搜集” (S/MIME Public Key Harvesting) 下，执行以下操作：
- 启用 S/MIME 公钥搜集。
 - (可选) 选择传入的签名邮件验证失败时是否搜集公钥。
 - (可选) 选择是否搜集更新的公钥。

Note 如果邮件网关在 48 小时内收到来自同一个域或邮件的多个更新公共密钥，将发出风险通告。

- 步骤 5** 提交并确认更改。
-

What to do next



Note 邮件网关中搜集的公共密钥存储库的大小为 512MB。如果存储库已满，邮件网关将自动删除未使用的公共密钥。

在 CLI 中，使用 `listenerconfig` 命令可启用密钥搜集。

下一步

请求收件人将签名邮件发送给邮件网关管理员。邮件网关将从签名的邮件中搜集公共密钥，并在“邮件策略” (Mail Policies) > “搜集的公共密钥” (Harvested Public Keys) 页面显示它们。

相关主题

- [S/MIME 搜集的公钥, on page 9](#)

管理 S/MIME 发送配置文件

S/MIME 发送配置文件允许您定义参数，例如：

- 要使用的 S/MIME 模式，例如签名、加密等。
- 适用于签名的 S/MIME 证书
- 要使用的 S/MIME 签名模式，例如不透明或独立。
- 邮件网关中收件人 S/MIME 证书的公共密钥不可用时采取的操作。

例如，一家组织要求发送给它们的所有邮件都进行签名，另一家组织要求发送给它们的所有邮件都进行签名并加密。在此情况下，必须创建两个发送配置文件，一个用于仅签名，另一个用于签名并加密。

您也可以使用 Web 界面或 CLI 创建、编辑、删除、导入、导出和搜索 `export` 搜索配置文件。

相关主题

- [创建签名、加密或签名和加密邮件的 S/MIME 发送配置文件, on page 11](#)
- [编辑 S/MIME 发送配置文件, on page 12](#)

创建签名、加密或签名和加密邮件的 S/MIME 发送配置文件

Procedure

步骤 1 依次单击邮件策略 (Mail Policies) > 发送配置文件 (Sending Profiles)。

步骤 2 单击添加配置文件 (Add Profile)。

步骤 3 配置以下字段：

S/MIME 配置文件名称 (S/MIME Profile Name)	输入发送配置文件的名称。
S/MIME 模式 (S/MIME Mode)	<p>选择 S/MIME 模式。可能的值包括：</p> <ul style="list-style-type: none"> • 签名 (Sign) • 加密 (Encrypt) • 签名/加密 (Sign/Encrypt)。签名，然后加密 • 三重 (Triple)。登录，加密，然后再签名 <p>Note 如果使用以下 S/MIME 模式之一，当签名失败时，邮件将退回给发件人：签名 (Sign)、签名/加密 (Sign/Encrypt) 或三重 (Triple)。</p>
签名证书 (Signing Certificate)	<p>选择要使用的签名证书。</p> <p>Note 只有在选择以下 S/MIME 模式之一时，才需要设置此字段：签名 (Sign)、签名/加密 (Sign/Encrypt) 或三重 (Triple)。</p>
S/MIME 签名模式 (S/MIME Sign Mode)	<p>选择 S/MIME 签名的模式。可能的值包括：</p> <ul style="list-style-type: none"> • 不透明 (Opaque)。不透明签名的邮件包含组合成单一部分的邮件和签名，并且只能通过验证签名阅读。 • 独立 (Detached)。签名信息与签名的文本分开。这种 MIME 类型是多部分签名/签名的第二部分包含应用程序/(x-)pkcs7 签名的 MIME 子类型。 <p>Note 只有在选择以下 S/MIME 模式之一时，才需要设置此字段：签名 (Sign)、签名/加密 (Sign/Encrypt) 或三重 (Triple)。</p>

S/MIME 配置文件名称 (S/MIME Profile Name)	输入发送配置文件的名称。
S/MIME 操作 (S/MIME Action)	<p>选择收件人的公共密钥不可用时邮件网关必须采取的行动。可能的值包括：</p> <ul style="list-style-type: none"> • 退回 (Bounce)。如果其中任意收件人的公钥不可用，则将该邮件退回给发件人。 • 丢弃 (Drop)。如果其中任意收件人的公钥不可用，则丢弃该邮件。 • 拆分 (Split)。拆分邮件。如果邮件发往的收件人的公钥不可用，将以不加密形式传送邮件；如果邮件发往的收件人的公钥可用，将以加密形式传送邮件。 <p>示例：假设您要将邮件发送到 bob@example1.com 和 dave@example2.com，且 dave@example2.com 的公钥不可用。在此情况下，如果您选择了拆分 (Split)，邮件网关将：</p> <ul style="list-style-type: none"> • 加密该邮件后，将其传送到 bob@example1.com。 • 将该邮件传送到 dave@example2.com，但不对其加密。 <p>Note 只有在选择以下 S/MIME 模式之一时，才需要设置此字段：加密 (Encrypt)、签名/加密 (Sign/Encrypt) 或三重 (Triple)。</p>

步骤 4 提交并确认更改。

What to do next



Note 在 CLI 中，使用 `smimeconfig` 命令可创建发送配置文件。

编辑 S/MIME 发送配置文件

Procedure

步骤 1 依次单击邮件策略 (Mail Policies) > 发送配置文件 (Sending Profiles)。

步骤 2 单击要修改的发送配置文件。

步骤 3 编辑创建签名、加密或签名和加密邮件的 S/MIME 发送配置文件, on page 11 中所述的字段。

步骤 4 提交并确认更改。

确定要签名、加密或签名并加密的邮件

创建发送配置文件后，您需要创建一个传出内容过滤器，用于确定应该对哪些邮件执行签名、加密或者签名和加密操作。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。一旦内容过滤器确定邮件与条件匹配，邮件网关将对该邮件签名、加密或签名并加密。

相关主题

- [根据内容过滤邮件的方法](#)

使用内容过滤器签名、加密或签名并加密及立即传送邮件

准备工作

了解构建内容过滤器条件的概念。请参阅[内容过滤器的工作原理](#)。

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，以过滤要签名、加密或签名并加密的邮件。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** 在“操作” (Actions) 部分，单击添加操作 (Add Action)。
- 步骤 7** 从添加操作 (Add Action) 列表中选择 S/MIME 签名/加密 (最终操作) (S/MIME Sign/Encrypt (Final Action))。
- 步骤 8** 选择要与内容过滤器关联的发送配置文件。
- 步骤 9** 单击确定 (OK)。
- 步骤 10** 提交并确认更改。

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](#)。

传送时使用内容过滤器签名并/或加密邮件

创建传送邮件时要对其签名、加密或签名加密的内容过滤器，也就是说，该邮件将进入下一个处理阶段，并且在所有处理完成后，该邮件已得到签名、加密或签名并加密，并被传送。

准备工作

- 了解构建内容过滤器条件的概念。请参阅[内容过滤器概述](#)。

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，以过滤要签名、加密或签名并加密的邮件。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** 在“操作” (Actions) 部分，单击添加操作 (Add Action)。
 - 步骤 7** 从添加操作 (Add Action) 列表中选择传送时 S/MIME 签名/加密 (S/MIME Sign/Encrypt on Delivery)。
 - 步骤 8** 选择要与内容过滤器关联的发送配置文件。
 - 步骤 9** 单击确定 (OK)。
 - 步骤 10** 提交并确认更改。
-

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](#)。

使用 S/MIME 验证、解密或解密并验证传入的邮件

- [邮件网关中的 S/MIME 验证和解密工作流程, on page 14](#)
- [如何使用 S/MIME 验证、解密或解密并验证传入的邮件, on page 15](#)
- [设置解密邮件的证书, on page 16](#)
- [设置验证签名邮件的公钥, on page 17](#)
- [启用 S/MIME 解密和验证, on page 19](#)
- [配置针对 S/MIME 解密或验证的邮件的操作, on page 19](#)



Note 可以使用邮件网关 S/MIME 安全服务验证、解密或解密并验证传出和传入的邮件。

邮件网关中的 S/MIME 验证和解密工作流程

- [S/MIME 验证工作流程, on page 15](#)

- [S/MIME 解密工作流程, on page 15](#)

S/MIME 验证工作流程

以下过程介绍邮件网关如何执行 S/MIME 验证。

1. 对签名邮件应用散列算法，以创建邮件摘要。
2. 使用发件人 S/MIME 证书的公钥解密附加到签名邮件的 PKCS7 签名，并获得邮件摘要。
3. 对比生成的邮件摘要与从该签名邮件中检索到的邮件摘要。如果邮件摘要匹配，该邮件将通过验证。
4. 使用证书颁发机构验证发件人域的 S/MIME 证书。

S/MIME 解密工作流程

以下过程介绍邮件网关如何执行 S/MIME 解密。

1. 使用邮件网关 S/MIME 证书的私钥解密会话密钥
2. 使用会话密钥解密邮件正文。

如何使用 S/MIME 验证、解密或解密并验证传入的邮件

步骤	操作	更多信息
第 1 步	了解 S/MIME 证书要求。	请参阅 S/MIME 证书要求, on page 20 。
第 2 步	根据您的要求，执行以下操作之一： <ul style="list-style-type: none"> • 要执行 S/MIME 解密，请将组织的 S/MIME 证书（包含执行解密所需的私钥）添加到邮件网关中。 • 要执行 S/MIME 验证，请将执行验证所需的发件人 S/MIME 证书的公共密钥添加到邮件网关中。 • 要执行 S/MIME 解密和验证，请将以下信息添加到邮件网关中： <ul style="list-style-type: none"> • 将组织的 S/MIME 证书（包含执行解密所需的私钥）添加到邮件网关。 • 发件人域的证书颁发机构。 • 执行验证所需的发件人 S/MIME 证书的公钥。 	请参阅 <ul style="list-style-type: none"> • 设置解密邮件的证书, on page 16 • 设置验证签名邮件的公钥, on page 17 • 导入自定义证书颁发机构列表
第 3 步	使用 S/MIME 配置验证、解密、解密和验证传入邮件的邮件流策略。	请参阅 启用 S/MIME 解密和验证, on page 19 。

步骤	操作	更多信息
第 4 步	(可选) 定义邮件网关将对解密或验证的邮件采取的操作。	请参阅 配置针对 S/MIME 解密或验证的邮件的操作, on page 19 。



Note 如果要使用 CLI 执行 S/MIME 验证、解密或解密并验证，请依次使用 `listenerconfig>hostaccess` 命令。有关更多详细信息，请参阅 CLI 在线帮助。

设置解密邮件的证书

您必须将组织的 S/MIME 证书（包含执行解密所需的私钥）添加到邮件网关。

准备工作

- 通过下列方式之一，与发件人（企业或消费者）共享邮件网关 S/MIME 证书的公共密钥：
 - 使用电子通道（例如邮件）发送公钥。
 - 请求发件人通过密钥搜集检索公钥。

发件人可以使用此公共密钥将加密的邮件发送到您的邮件网关。



Note 在 B2C 场景下，如果组织的 S/MIME 证书是域证书，则某些邮件客户端（例如 Microsoft Outlook）可能无法使用组织的 S/MIME 证书公钥发送加密的邮件。这是因为，这些邮件客户端不支持使用域证书的公钥进行加密。

- 请确保计划导入的 S/MIME 证书符合[S/MIME 证书要求, on page 20](#)中所述的要求。

Procedure

- 步骤 1** 依次单击网络 (Network) > 证书 (Certificates)。
- 步骤 2** 单击添加证书 (Add Certificate)。
- 步骤 3** 选择导入证书 (Import Certificate)。
- 步骤 4** 输入指向网络或本地计算机中的证书文件的路径。
- 步骤 5** 输入该文件的密码。
- 步骤 6** 单击下一步 (Next) 查看证书的信息。
- 步骤 7** 为证书输入一个名称。
- 步骤 8** 提交并确认更改。

What to do next



Note 在 CLI 中，使用 `certconfig` 命令可添加 S/MIME 证书。

设置验证签名邮件的公钥

只有将发件人 S/MIME 证书的公共密钥添加到邮件网关中，才能验证签名的邮件。根据组织的策略和流程，可以使用下列方法之一将公共密钥添加到邮件网关：

- 请求发件人使用电子通道（例如邮件）发送其公钥。然后，可以使用 Web 界面或 CLI 添加公钥。
- 有关添加公钥的说明，请参阅[添加用于 S/MIME 加密的公钥, on page 9](#)。
- 通过密钥搜集检索公钥。请参阅[搜集公钥, on page 9](#)。

添加用于 S/MIME 验证的公钥

准备工作

- 确保公钥符合[S/MIME 证书要求, on page 20](#)中所述的要求。
- 确保公钥为 PEM 格式。

Procedure

步骤 1 依次单击邮件策略 (Mail Policies) > 公钥 (Public Keys)。

步骤 2 单击添加公钥 (Add Public Key)。

步骤 3 输入公钥的名称。

步骤 4 输入公钥。

步骤 5 提交并确认更改。

What to do next



Note 在 CLI 中，使用 `smimeconfig` 命令可添加公钥。

搜集用于 S/MIME 验证的公钥

您可以将邮件网关配置为从传入的 S/MIME 签名邮件中检索（搜集）公共密钥，并利用搜集到的密钥来验证其所有者（企业或消费者）的签名邮件。



Note 默认情况下，不会从过期或自签名 S/MIME 证书中搜集公钥。

1. 使用 Web 界面或 CLI 启用公钥搜集。请参阅 [启用公钥搜集, on page 18](#)。
2. 请求发件人发送签名邮件。
3. 搜集完成后，将搜集的公共密钥添加到邮件网关。请参阅 [添加用于 S/MIME 验证的搜集公钥, on page 18](#)。

此步骤是为了确保邮件在网关级别进行验证。

启用公钥搜集

Procedure

步骤 1 依次单击 **邮件策略 (Mail Policies)** > **邮件流策略 (Mail Flow Policies)**。

步骤 2 创建新的邮件流策略或修改现有的邮件流策略。

步骤 3 向下滚动至 **安全功能 (Features)** 部分。

步骤 4 在“S/MIME 公钥搜集” (S/MIME Public Key Harvesting) 下，执行以下操作：

- 启用 S/MIME 公钥搜集。
- (可选) 选择传入的签名邮件验证失败时是否搜集公钥。
- (可选) 选择是否搜集更新的公钥。

Note 如果邮件网关在 48 小时内收到来自同一个域或邮件的多个更新公共密钥，将发出风险通告。

步骤 5 提交并确认更改。

What to do next



Note 邮件网关中搜集的公共密钥存储库的大小为 512MB。如果使用的存储库已满，邮件网关将自动删除未使用的公共密钥。

在 CLI 中，使用 `listenerconfig` 命令可启用密钥搜集。

添加用于 S/MIME 验证的搜集公钥

Procedure

步骤 1 依次单击 **邮件策略 (Mail Policies)** > **搜集的公钥 (Harvested Public Keys)**。

步骤 2 单击搜集的目标用途的公钥，并复制该公钥。

步骤 3 将该公共密钥添加到邮件网关。请参阅[添加用于 S/MIME 验证的公钥](#), on page 17。

步骤 4 提交并确认更改。

启用 S/MIME 解密和验证

Procedure

步骤 1 依次单击邮件策略 (Mail Policies) > 邮件流策略 (Mail Flow Policies)。

步骤 2 创建新的邮件流策略或修改现有的邮件流策略。

步骤 3 向下滚动至安全功能 (Features) 部分。

步骤 4 在“S/MIME 验证/解密” (S/MIME Decryption/Verification) 下，执行以下操作：

- 启用 S/MIME 解密和验证。
- 选择在 S/MIME 验证后是保留还是删除邮件中的数字签名。如果不希望最终用户了解 S/MIME 网关验证，请选择删除 (Remove)。

对于三重封装的邮件，仅保留或删除内部签名。

步骤 5 提交并确认更改。

What to do next



Tip 如果在邮件流策略中启用了 S/MIME 解密和验证，则传送所有 S/MIME 邮件，不考虑解密和验证的状态。如果要配置处理 S/MIME 解密或验证的邮件的操作，可以使用邮件过滤器规则 smime-gateway-verified 和 smime-gateway。有关详细信息，请参阅[配置针对 S/MIME 解密或验证的邮件的操作](#), on page 19。

配置针对 S/MIME 解密或验证的邮件的操作

在邮件网关执行 S/MIME 解密、验证或两者后，您可能希望根据结果采取不同的操作。您可以使用邮件过滤器规则 smime-gateway-verified 和 smime-gateway，基于解密和/或验证的结果对邮件执行操作。有关详细信息，请参阅[使用邮件过滤器实施邮件策略](#)



Note 此外，还可以使用内容过滤器条件 - S/MIME 网关邮件 (S/MIME Gateway Message) 和 S/MIME 网关已验证 (S/MIME Gateway Verified)，基于解密、验证或两者的结果对邮件执行操作。有关详细信息，请参阅[内容过滤器](#)

示例：隔离验证、解密（或两者）失败的 S/MIME 邮件

下列邮件过滤器检查邮件是否为 S/MIME 邮件，并在使用 S/MIME 的验证或解密失败时对邮件进行隔离。

```
quarantine_smime_messages:if (smime-gateway-message and not smime-gateway-verified)
{ quarantine("Policy"); }
```

S/MIME 证书要求

- [签名的证书要求, on page 20](#)
- [加密的证书要求, on page 21](#)

签名的证书要求

签名的 S/MIME 证书必须包含以下信息：

公共名称	完全限定域名。
组织	组织精确的法定名称。
组织单位	组织的部门。
城市（地区）	组织法定所在的城市。
省/市/自治区	组织法定所在的省/市/自治区、县或区域。
国家/地区	组织法定所在国家/地区的双字母 ISO 缩写。
过期前的持续时间	证书到期之前的天数。
主题备用名称(域)	计划从中发送签名邮件的域的名称。示例包括 <code>domain.com</code> 和 <code>*.domain.net</code> 。对于多个条目，请使用逗号分隔值列表。
主题备用名称(邮件)	计划发送签名邮件的用户的邮件地址，例如 <code>user@somedomain.com</code> 。对于多个条目，请使用逗号分隔值列表。
私钥大小	为 CSR 生成的私钥的大小。
密钥使用	主要用作决定证书用途的限制方法。如果指定了密钥使用延长期，则必须设置以下位： <code>digitalSignature</code> 和 <code>nonRepudiation</code> 。 如果未指定密钥使用延长期，则接收客户端必须假定已设置 <code>digitalSignature</code> 和 <code>nonRepudiation</code> 位。

有关 S/MIME 证书的详细信息，请参阅“RFC 5750：安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 证书处理”。

加密的证书要求

加密的 S/MIME 证书必须包含以下信息：

公共名称	完全限定域名。
组织	组织精确的法定名称。
组织单位	组织的部门。
城市（地区）	组织法定所在的城市。
省/市/自治区	组织法定所在的省/市/自治区、县或区域。
国家/地区	组织法定所在国家/地区的双字母 ISO 缩写。
过期前的持续时间	证书到期之前的天数。
主题备用名称(域)	计划将加密邮件发送到的域的名称。示例包括 <code>domain.com</code> 和 <code>*.domain.net</code> 。对于多个条目，请使用逗号分隔值列表。 如果计划将加密邮件发送给域中的所有用户，则公钥应包括 SAN 域。
主题备用名称(邮件)	计划作为加密邮件收件人的用户的邮件地址，例如， <code>user@somedomain.com</code> 。对于多个条目，请使用逗号分隔值列表。
私钥大小	为 CSR 生成的私钥的大小。
密钥使用	主要用作决定证书用途的限制方法。必须指定密钥使用延长期，并且必须设置以下位： <code>keyEncipherment</code> 。

有关 S/MIME 证书的详细信息，请参阅“RFC 5750：安全/多用途互联网邮件扩展 (S/MIME) 版本 3.2 - 证书处理”。

管理公钥

邮件网关要求：

- 收件人的 S/MIME 加密证书的公钥，用于加密传出邮件。
- 发件人的 S/MIME 签名证书的公钥，用于验证传入的签名邮件。

您可以通过以下方式向邮件网关添加公共密钥：

- 如果您有 PEM 格式的目标公钥，可以使用 Web 界面或 CLI 进行添加。请参阅[添加公钥](#), on page 22。

- 如果您的目标公钥包含在导出文件中，可以将导出文件复制到 /configuration 目录，再使用 Web 界面或 CLI 将其导入。请参阅[从现有导出文件中导入公钥, on page 22](#)。

此外，邮件网关还支持密钥搜集（自动从传入的签名邮件中检索公共密钥）。有关详细信息，请参阅[S/MIME 搜集的公钥, on page 9](#)。

添加公钥

准备工作

- 确保公钥符合[S/MIME 证书要求, on page 20](#)中所述的要求。
- 确保公钥为 PEM 格式。

Procedure

步骤 1 依次单击邮件策略 (Mail Policies) > 公钥 (Public Keys)。

步骤 2 单击添加公钥 (Add Public Key)。

步骤 3 输入公钥的名称。

步骤 4 输入公钥。

步骤 5 提交并确认更改。

What to do next



Note 在 CLI 中，使用 `smimeconfig` 命令可添加公钥。

从现有导出文件中导入公钥

准备工作

将导出文件复制到邮件网关的 /configuration 目录。有关创建导出文件的说明，请参阅[导出公钥, on page 23](#)。

Procedure

步骤 1 依次单击邮件策略 (Mail Policies) > 公钥 (Public Keys)。

步骤 2 单击导入公钥 (Import Public Keys)。

步骤 3 选择导出文件，然后单击提交 (Submit)。

Note 如果要导入包含大量公钥的文件，则导入过程可能需要较长的时间。确保相应地调整 Web 界面或 CLI 的不活动超时时间。

步骤 4 确认您的更改。

导出公钥

将邮件网关中的所有公共密钥一起导出到一个文本文件中，存储在 /configuration 目录中。

Procedure

步骤 1 依次选择邮件策略 (Mail Policies) > 公钥 (Public Keys)。

步骤 2 单击导出公钥 (Export Public Keys)。

步骤 3 输入文件名称并单击提交 (Submit)。
