在ESA CRES加密配置文件中配置安全级别

目录

简介

本文档介绍在邮件安全设备(ESA)中配置思科注册信封服务加密(CRES)配置文件，重点是允许的不同安全级别。

先决条件

要求

Cisco 建议您了解以下主题：

- ESA基本配置
- 基于内容过滤器配置的加密
- 思科注册信封服务

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

创建CRES配置文件是通过ESA激活和使用加密服务的核心任务。在创建多个配置文件之前，请确保您已通过创建CRES帐户为ESA调配了完整的帐户。

可以有多个配置文件，并且每个配置文件都可以配置不同的安全级别。这使网络能够按域、用户或组维护不同的安全级别。

配置

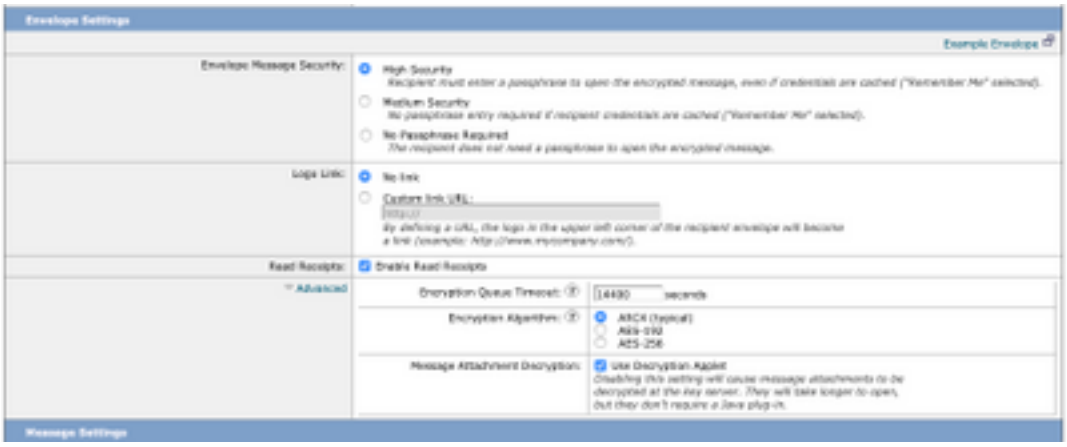
可以使用encryptionconfig CLI命令或通过GUI中的**Security Services > Cisco IronPort Email Encryption启用和配置加**密配置文件。

从GUI进行配置

从ESA导航至“安**全服务”>“Cisco IronPort邮件加密”>“添加加密配置文件”**。

屏幕上将显示加密配置文件设置。配置文件名称和配置的其余部分可以自定义，并取决于组织的标识标签或方法。

根据配置文件定义安全级别的配置是信封设置，如图所示：



> **注意：**建议配置文件名称包含：“高”、“低”等，以匹配配置的安全级别或配置文件与其关联的组的名称，以便在创建内容过滤器和验证时快速识别。

ESA允许的三个安全级别是：

- 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:如果缓存了收件人凭证，则收件人无需输入凭证即可打开加密邮件。
- 无需密码：这是加密邮件安全的最低级别。收件人无需输入密码即可打开加密邮件。您仍然可以为未受密码短语保护的信封启用读取回执、全部安全回复和安全邮件转发功能。

您可以在这些对象上配置不同的安全级别：

信封邮件安全:

- ·高度安全
- 中等安全
- 无需密码

徽标链接：要使用户能够打开您组织的URL，请点击其徽标，您可以添加徽标链接。从以下选项中进行选择：

- 没有链路。实时链接未添加到邮件信封。

- 自定义链接URL。输入URL，以向邮件信封添加实时链接。

读取回执：如果启用此选项，则收件人打开安全信封时，发件人会收到回执。这是可选选择。

高级：

加密队列超时：输入消息在超时之前可以在加密队列中的时间长度（以秒为单位）。消息超时后，设备会退回消息并向发件人发送通知。

加密算法:

- ARC4. ARC4是最常见的选择，它为邮件收件人提供强加密和最小的解密延迟。
- AES。AES提供更强的加密，但解密也需要更长的时间，它会给收件人带来延迟。AES通常用于政府和银行应用。

邮件附件解密:启用或禁用解密小程序。启用此选项后，会在浏览器环境中打开邮件附件。禁用此选项后，会导致邮件附件在密钥服务器上解密。默认情况下，信封中禁用Java小程序。

注意：由于安全原因，最常用的浏览器已禁用Java小程序。

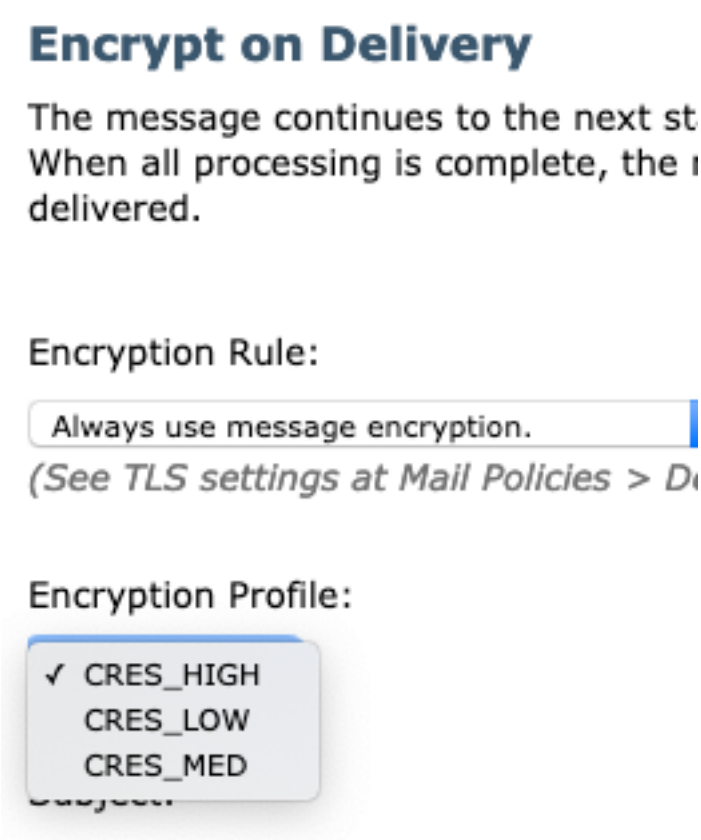
创建加密配置文件后。 确保已调配，如图所示：

必须通过内容过滤器关联每个配置文件才能应用。

警告：如果内容过滤器未调用配置文件，则无法应用加密设置。

从ESA导航至“邮件策**略”>“传出内容过滤器”>“添加过滤器”**

在过滤器内配置用户、主题、组、发件人等条件后，定义传出过滤器的加密级别，如图所示：



警告：所有内容过滤器必须与外发邮件策略相关联才能正常运行。

注意：可以为托管密钥服务配置多个加密配置文件。如果您的组织有多个品牌，这允许您引用存储在PXE信封的关键服务器上的不同徽标。

从CLI进行配置

从ESA CLI键入encryptionconfig命令：

```
ESA.com> encryptionconfig

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service

[]> profiles

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIGH-CRES              Hosted Service         No          Not Provisioned
Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
```

```
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[]> new

1. Cisco Registered Envelope Service
2. IronPort Encryption Appliance (in network)
Choose a key service:
[1]>

Enter a name for this encryption profile:
[]> HIGH

Current Cisco Registered Key Service URL: https://res.cisco.com
Do you wish to alter the Cisco Registered Envelope Service URL? [N]> N

1. ARC4
2. AES-192
3. AES-256
Please enter the encryption algorithm to use when encrypting envelopes:
[1]>

1. Use envelope service URL with HTTP (Recommended). Improves performance for opening envelopes.
2. Use the envelope service URL with HTTPS.
3. Specify a separate URL for payload transport.
Configure the Payload Transport URL
[1]>

1. High Security (Recipient must enter a passphrase to open the encrypted message, even if
credentials are cached ("Remember Me" selected).)
2. Medium Security (No passphrase entry required if recipient credentials are cached ("Remember
Me" selected).)
3. No Passphrase Required (The recipient does not need a passphrase to open the encrypted
message.)
Please enter the envelope security level:
[1]>

Would you like to enable read receipts? [Y]>

Would you like to enable "Secure Reply All"? [N]> y

Would you like to enable "Secure Forward"? [N]> y

Enter a URL to serve as a link for the envelope logo image (may be blank):
[]>

Would you like envelopes to be displayed in a language other than English ? [N]>

Enter the maximum number of seconds for which a message could remain queued waiting to be
encrypted. Delays could be caused by key server outages or resource limitations:
[14400]>

Enter the subject to use for failure notifications:
[[ENCRYPTION FAILURE]]>

Please enter file name of the envelope attached to the encryption notification:
[securedoc_${date}T${time}.html]>


A Cisco Registered Envelope Service profile "HIGH" was added.

   1. Commit this configuration change before continuing.
   2. Return to the encryptionconfig menu and select PROVISION to complete
the configuration.
```

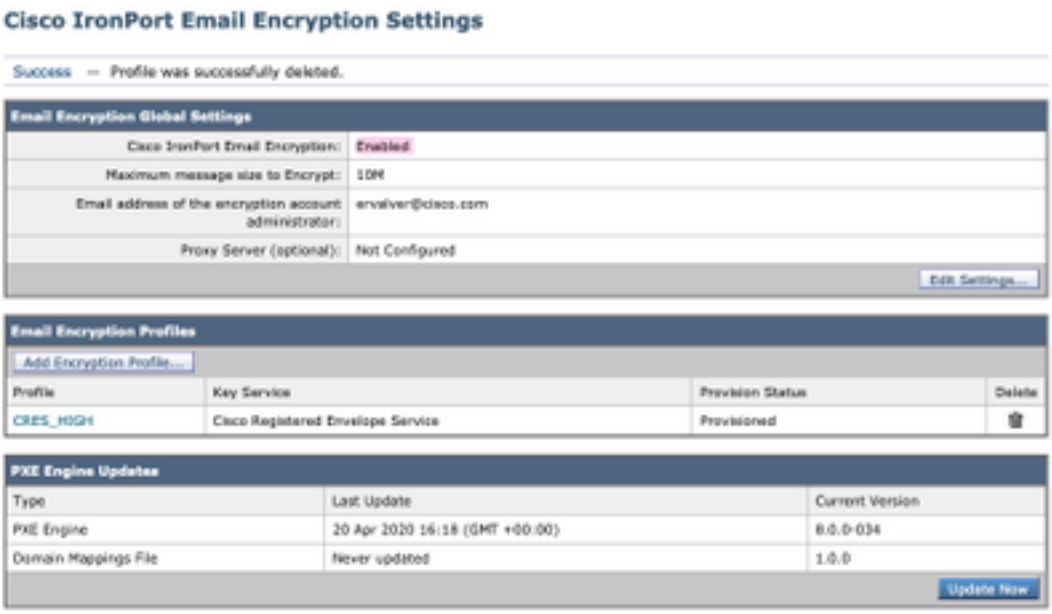
```
Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIGH-CRES            Hosted Service         No          Not Provisioned
LOW-CRES             Hosted Service         No          Not Provisioned

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service

[]> provision
```

验证

使用本部分可确认配置能否正常运行。

从GUI验证

从ESA导航至**Security Services > Cisco IronPort Email Encryption**，如图所示：



注意：确保已启用加密并调配配置文件。如图所示.

从CLI验证

在CLI中键入**encryptconfig** 和type profiles命令。

```
ESA.com> encryptionconfig

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
```

```
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]> profiles

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
CRES_HIGH             Hosted Service         No          Provisioned
```

注意：确保已启用加密并调配配置文件。如图所示.

故障排除

本部分提供了可用于对配置进行故障排除的信息。

从ESA导航至“系统**管理”>“功能键”**

验证功能密钥是否已应用且处于活动状态。关键：IronPort邮件加密必须处于活动状态。

从ESA导航至**安全服务> Cisco IronPort邮件加密**

验证加密服务是否已正确启用。

验证加密配置文件是否未处于未调配状态，如图所示：

Profile	Key Service	Provision Status
HIGH	Cisco Registered Envelope Service	**Not Provisioned**
LOW	Cisco Registered Envelope Service	**Not Provisioned**
MEDIUM	Cisco Registered Envelope Service	**Not Provisioned**

验证引擎上次更新，如图所示：

PXE Engine Updates

Type	Last Update	Current Version
PXE Engine	21 Jan 2020 16:01 (GMT +00:00)	7.2.1-015

从邮件跟踪详细信息中，验证是否显示错误。

最常见的错误：

```
5.x.3 - Temporary PXE Encryption failure
```

解决方案：服务当前不可用或无法访问。检验连通性和网络问题。

```
5.x.3 - PXE Encryption failure. (Message could not be encrypted due to a system configuration
issue. Please contact your administrator
```

解决方案：此错误与：

- 许可问题.请验证功能密钥
- 未调配使用的配置文件。从邮件跟踪中识别在内容过滤器和调配上配置的配置文件
- 没有与内容过滤器关联的配置文件。有时，加密配置文件会被删除、修改为不同的名称等。配

置的内容过滤器无法找到关联的配置文件

```
5.x.3 - PXE Encryption failure. (Error 30 - The message has an invalid "From" address.)
```

```
5.x.3 - PXE Encryption failure. (Error 102 - The message has an invalid "To" address.)
```

解决方案：通常，此问题是由内部发件人的电子邮件客户端（如Outlook）自动填写收件人的电子邮件地址（包含无效的“发件人”/“收件人”地址）引起的。

通常，这是由电子邮件地址周围的引号或电子邮件地址中的其他非法字符引起的。

相关信息

- CRES管理指南
- 最终用户指南
- 技术支持和文档 - Cisco Systems