防数据丢失和加密的最佳实践指南

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

防数据丢失和加密最佳实践指南

- 1.在ESA上启用Cisco IronPort邮件加密
- 2.向RES注册您的ESA和组织
- 3.在ESA上创建加密配置文件
- 4.启用防数据丢失(DLP)
- 5.创建防数据丢失消息操作
- 6.制定防数据丢失策略
- 7.将DLP策略应用于传出邮件策略

结论

相关信息

简介

本文档介绍思科邮件安全防数据丢失(DLP)和加密的最佳实践。

本文档讨论使用思科邮件安全设备(ESA)和基于云的思科注册信封服务(RES)设置邮件加密。 客户可以使用各种类型的策略（包括内容过滤和DLP），通过公共Internet安全地发送单个邮件。 本系列中的其他文档将讨论这些策略的创建。 本文档重点介绍ESA准备发送加密邮件，以便策略可以将加密用作操作。

先决条件

要求

本文档没有任何特定的要求。

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

本文档将讨论以下步骤：

1. 启用Cisco IronPort邮件加密
2. 向RES注册您的ESA和组织
3. 创建加密配置文件
4. 启用DLP
5. 创建DLP邮件操作
6. 创建DLP策略
7. 将DLP策略应用于传出邮件策略

成功完成这些步骤后，ESA管理员可以成功创建将加密用作操作的策略。

Cisco IronPort邮件加密也称为RES加密。 RES是我们用于思科云中“关键服务器”的名称。 RES加密解决方案使用对称密钥加密 — 这意味着用于加密消息的密钥与用于解密消息的密钥相同。 每封加密邮件都使用唯一的密钥，这样发送者可以在邮件发送后对邮件进行精细控制，例如锁定邮件或使其过期，以便接收者不再能打开邮件，而不影响任何其他邮件。 当加密消息时，ESA将加密密钥和元数据存储在CRES中，以供每个加密消息使用。

ESA可以决定以多种方式加密邮件 — 例如，通过“标记”（如主题内容）、内容过滤器匹配或DLP策略。 ESA决定加密邮件后，会使用在“安全服务”(Security Services)>“Cisco IronPort邮件加密”(名为“邮件加密配置文件”(Email Encryption Profiles)的表中创建的指定“加密配置文件”(Encryption Profile)进行加密。 默认情况下，没有加密配置文件。 3.创建加密配置文件中将会讨论此问题。

防数据丢失和加密最佳实践指南

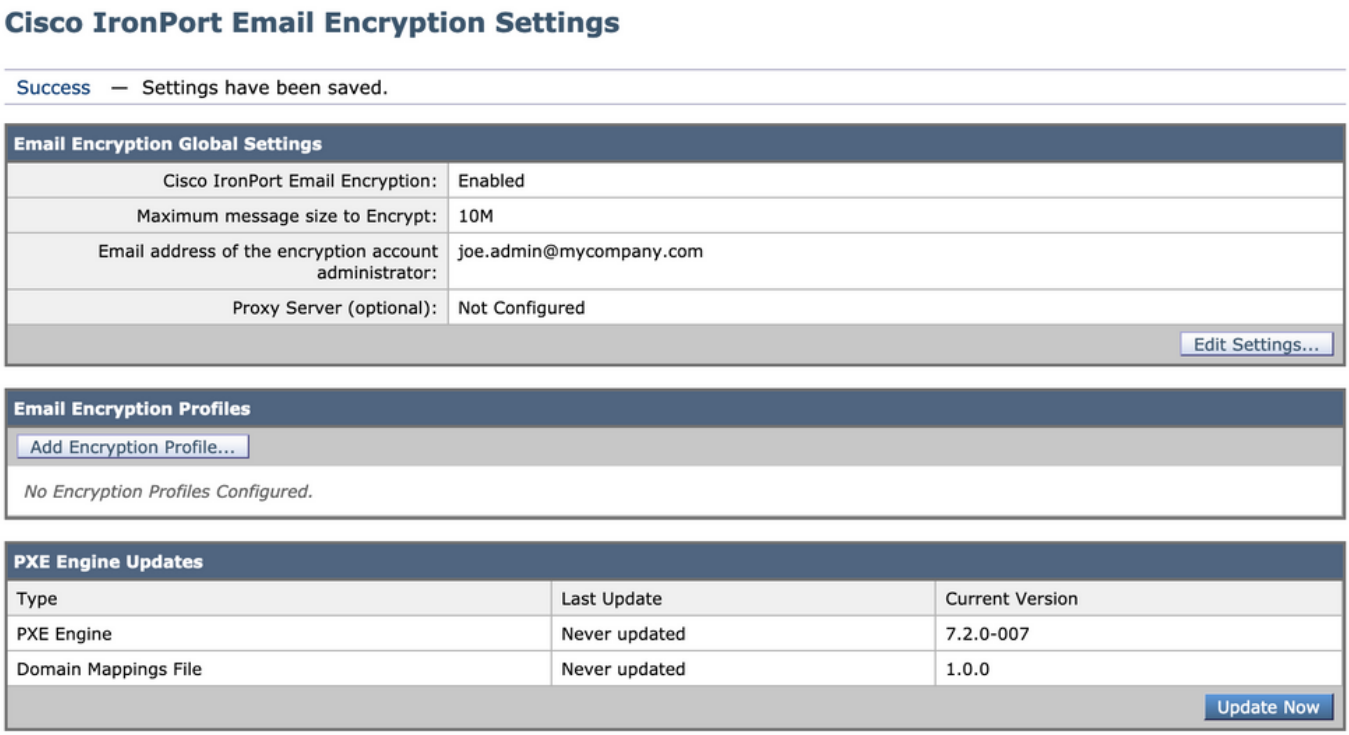
1.在ESA上启用Cisco IronPort邮件加密

注意：如果集群中有多个ESA，则只需执行一次步骤#1，因为这些设置通常在集群级别进行管理。 如果您有多台计算机未进行群集，或者您正在计算机级别管理这些设置，则应在每个ESA上执行步骤#1。

---

1. 从ESA UI导航至安全服务> Cisco IronPort邮件加密。
2. 选中此框可启用Cisco IronPort邮件加密。
3. 接受最终用户许可协议(EULA)、Cisco IronPort邮件加密许可协议。
4. 在邮件加密全局设置中，单击编辑设置……
    - 指定作为帐户的主要RES管理员的管理员/人员的邮件地址。 此电子邮件帐户将关联到公司的RES环境管理。
    - 可选：要加密的默认最大邮件大小为10M。 如果愿意，可以增加/减少此时的尺寸。
    - 可选：如果您有通过HTTPS连接到RES时需要经过ESA的代理，请添加必要的代理和身份验证设置，以便其通过代理。
5. 提交并确认配置更改。

此时，您应该看到“Email Encryption Global Settings”（邮件加密全局设置）设置为类似的设置，但是尚未列出配置文件：



2.向RES注册您的ESA和组织

第#2步主要参与ESA管理控制台外部。

注意：ESA注册信息也可在以下TechNote中找到：思科RES:虚拟、托管和硬件ESA帐户调配配置示例

请直接发送电邮至RES:stg-cres-provisioning@cisco.com。

为了为您的ESA加密配置文件设置CRES帐户，请向我们提供以下信息：

1. 帐户名称（请根据您的要求指定确切的公司名称。）
    1. 对于云邮件安全(CES)/托管客户帐户，请将您的帐户名称以“<Account Name> HOSTED”结尾
2. 用于帐户管理员的邮件地址（请指定相应的管理员邮件地址）
3. 完整的设备序列号
    1. 通过“version”命令，可以从ESA GUI（系统管理>功能密钥）或ESA CLI找到设备序列号。 提供虚拟许可证编号(VLN)或产品激活密钥(PAK)许可证是不可接受的，因为CRES帐户管理需要完整的设备序列号。
4. 出于管理目的应映射到CRES帐户的域名

注意：如果您已经拥有CRES帐户，请提供公司名称或现有CRES帐号。这将确保任何新的设备序列号都添加到正确的帐户中，并避免公司信息和调配的任何重复。

请放心，如果您通过电邮与调配CRES帐户有关，我们将在一(1)个工作日内做出响应。如果您需要

即时支持和帮助，请向思科TAC提交支持请求。这可以通过支持案例管理器(https://mycase.cloudapps.cisco.com/case)或通过电话(https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html)来完成。

注意：通过电子邮件发送此请求后，可能需要一天时间创建您的公司RES帐户（如果尚未创建）和添加S/N。 在此步骤完成之前，第#3步中的“调配”任务将无法工作。

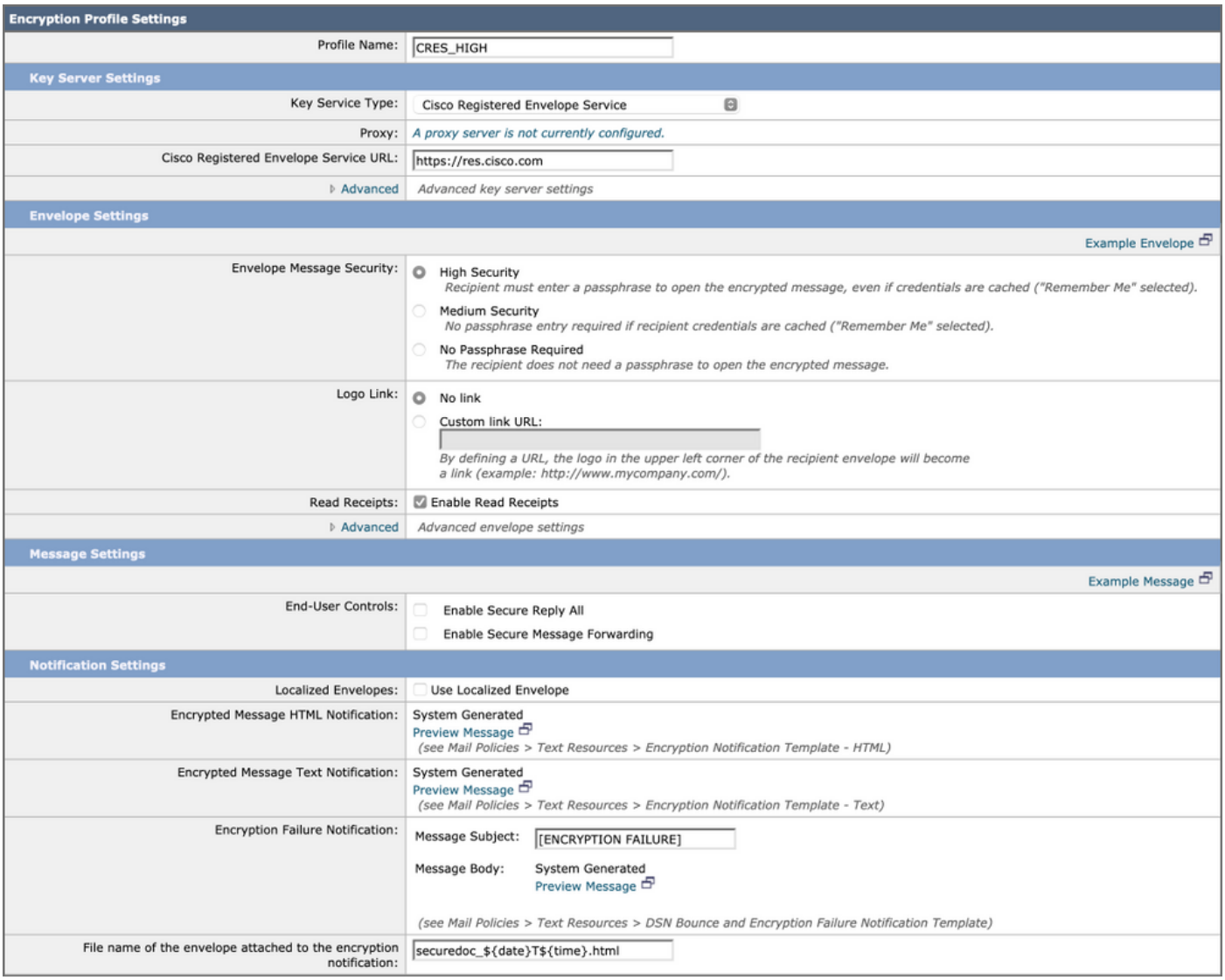
3.在ESA上创建加密配置文件

注意：如果集群中有多个ESA，则只需执行一次步骤#1，因为这些设置通常在集群级别进行管理。 如果您有多台计算机未进行群集，或者您正在计算机级别管理这些设置，则应在每个ESA上执行步骤#1。

加密配置文件指定应如何发送加密邮件。 例如，组织可能需要为其收件人的一个分段发送高安全性信封，例如知道将经常向其发送高度敏感数据的收件人。 同一组织可能拥有其收件人社区的其他部分，这些部分接收不太敏感的信息，并且可能对于必须提供用户ID和密码才能接收加密邮件不太耐心。 这些收件人非常适合使用低安全性信封类型。 拥有多个加密配置文件后，组织可以针对受众定制加密消息格式。 另一方面，许多组织可能只使用一个加密配置文件。

对于本文档，我们将展示一个创建三个加密配置文件的示例，分别名为“CRES_HIGH”、“CRES_MED”和“CRES_LOW”。

1. 从ESA UI导航至安全服务> Cisco IronPort邮件加密。
2. 点击“Add Encryption Profile...”"
3. 系统将打开“加密配置文件”(Encryption Profile)菜单，您可以将第一个加密配置文件命名为“CRES_HIGH”。
4. 如果尚未选择“信封邮件安全”，请选择“高安全性”。
5. 单击Submit保存此配置文件。



接下来，重复步骤2-5以创建“CRES_MED”和“CRES_LOW” — 只需更改每个配置文件的“信封邮件安全”单选按钮。

- 对于CRES_HIGH配置文件，选择“High Security”单选按钮。
- 对于CRES_MED配置文件，选择“Medium Security”单选按钮。
- 对于CRES_LOW配置文件，请选择“无需密码”单选按钮

您会发现有“启用读回执”、“启用安全回复全部”和“启用安全消息转发”的选项。 在“信封设置”(Envelope Settings)中，如果单击“高级”(Advanced)链接，您可以选择三种对称加密算法之一，并指定发送不带Java加密小程序的信封。

在“Envelope Settings”（信封设置）的右侧，您将看到“Example Message”（示例消息）超文本链接。 如果单击此按钮，将会显示一个安全邮件信封示例 — 收件人打开HTML附件后在邮件中看到的内容。

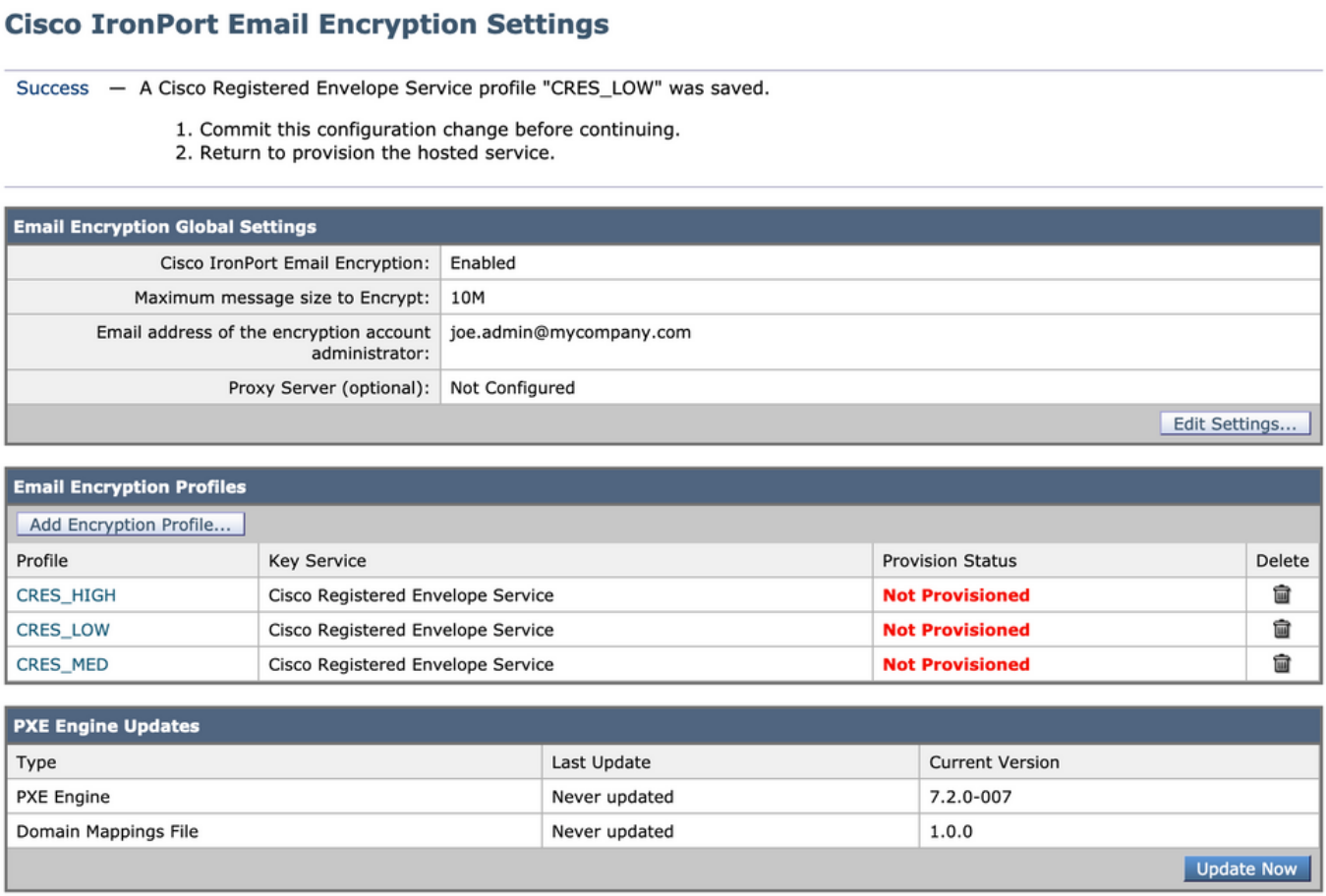
“读取回执”(Read Receipts)表示当收件人打开安全邮件（表示收件人提取对称密钥并解密邮件）时，加密邮件的发件人将收到CRES发送的邮件。

在Message Settings（消息设置）的右侧，您将看到“Example Message”（示例消息）超文本链接。 如果单击此按钮，则会向您显示打开邮件的外观 — 收件人已在信封中提供必要信息并打开加密

邮件后会看到的内容。

请始终记得单击Submit并提交更改。

然后，表中的行将显示“调配”按钮。 提交更改后才会显示Provision按钮。



再次点击Provision（调配）按钮，此操作仅在您公司的RES帐户已创建且设备S/N已添加到您的帐户后才能生效。 如果RES帐户链接到ESA，调配过程将相对较快地完成。 如果没有，那么这个过程必须首先完成。

调配完成后，您的Cisco IronPort邮件加密页面将显示已调配的配置文件。

4.启用防数据丢失(DLP)

1. 从ESA UI导航到安全服务>数据丢失保护。
2. 单击启用……以启用DLP。
3. 接受EULA、防数据丢失许可协议。
4. 点击“启用匹配的内容日志记录”复选框。
5. 点击启用自动更新(Enable automatic updates)复选框。
6. 单击 submit。

Data Loss Prevention Settings

Data Loss Prevention:	Enabled
Matched Content Logging:	Enabled
Automatic Updates:	Enabled

Edit Settings...

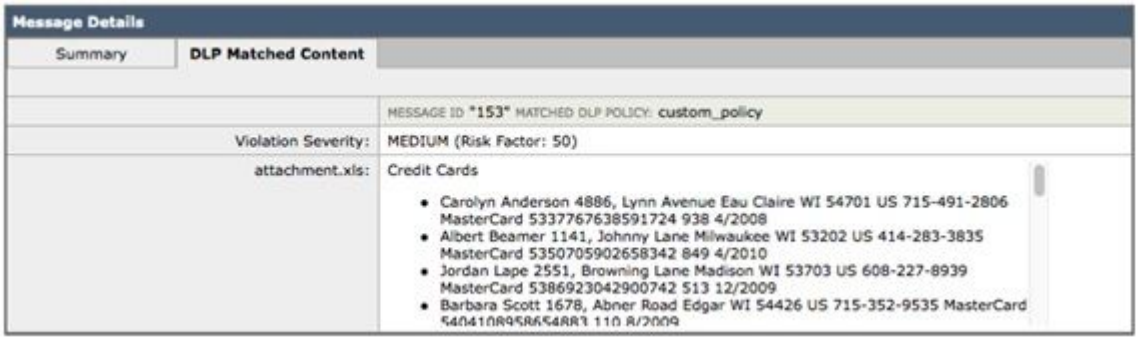
Current DLP Files

File Type	Last Update	Current Version	New Update
DLP Engine	Never Updated	1.0.16.a0015fd	No updates available.

No updates in progress. Update Now

DLP引擎和设备上的预定义内容匹配分类器的更新独立于其他安全服务的更新。3-5分钟的常规Talos签名更新不同，不包括更新DLP策略和词典。必须在此处启用更新。

当“匹配的内容记录”处于启用状态时，它允许邮件跟踪显示导致违规的邮件的内容。以下是显示导致DLP违规的邮件内容的邮件跟踪示例。 这样，管理员就可以确切知道哪些数据触发了特定DLP策略。



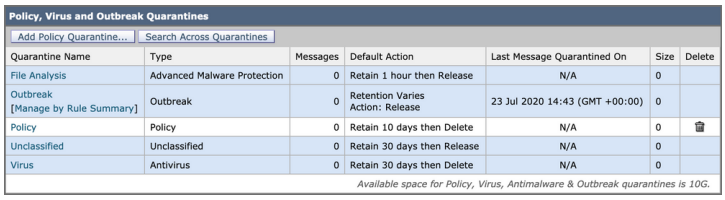
防数据丢失违规

5.创建防数据丢失消息操作

创建DLP隔离区

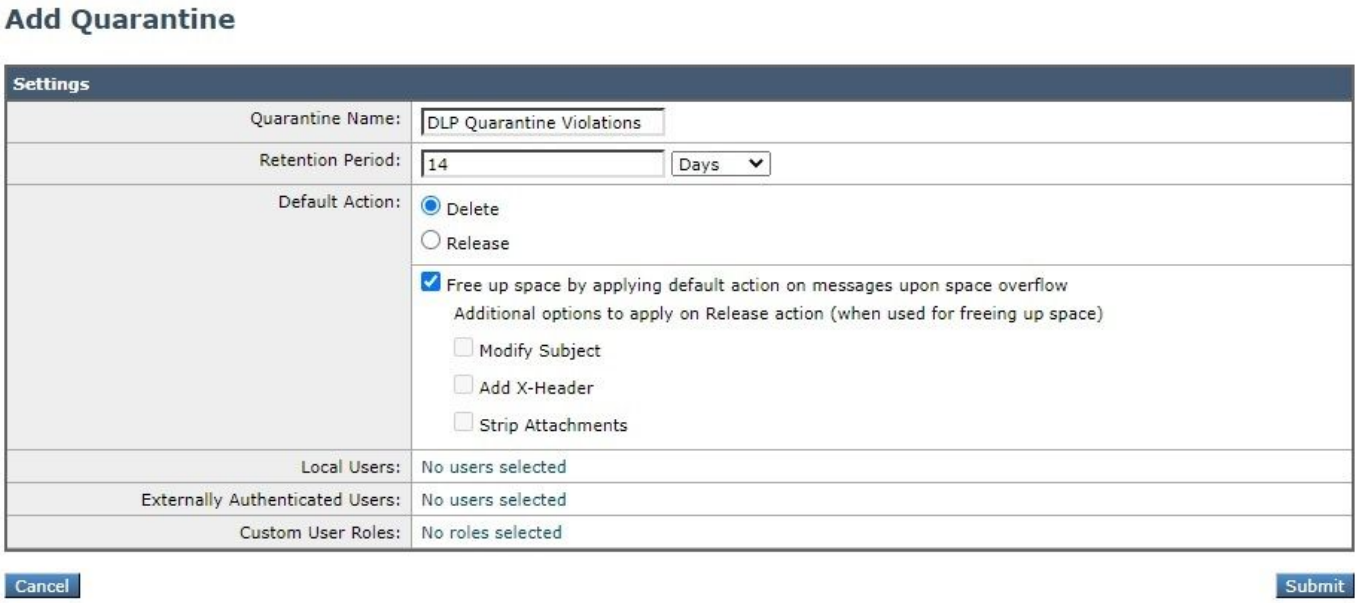
如果要保留违反DLP策略的邮件副本，可以为每种类型的策略违规创建单独的策略隔离区。当运行“透明”POV时，这尤其有用，在该处，违背DLP策略的出站邮件被记录并传送，但不会对这些邮件执行任何操作。

1. 在SMA上，导航到邮件>邮件隔离>策略、病毒和爆发隔离区



2. 下面是开始之前“隔离区”表应显示的内容：策略病毒和爆发隔离区
3. 点击“Add Policy Quarantine”（添加策略隔离区）按钮，创建要由DLP策略使用的隔离区。

以下是针对中型DLP违规建立的隔离示例。隔离区分段是可能的，并且可能适用于多个DLP规则：



DLP隔离示例

关于DLP邮件操作

DLP邮件操作描述了ESA在检测到外发邮件中的DLP违规时会采取的操作。您可以指定主要和辅助DLP操作，并且可以为不同的违规类型和严重性分配不同的操作。

主要操作包括：

- 交付
- 丢弃
- 隔离

对于只读状态，其中会记录并报告DLP违规，但邮件不会停止/隔离或加密，通常使用“传送”(Deliver)操作。

辅助操作包括：

- 将副本发送到任何自定义隔离区或“策略”隔离区。
- 加密邮件。设备仅加密邮件正文。它不会加密邮件报头。
- 更改主题信头。
- 向邮件添加免责声明文本/HTML。
- 将邮件发送到备用目标邮件主机。
- 正在发送邮件的密件抄送副本。
- 向发件人和/或其他联系人发送DLP违规通知。

这些操作并不互相排斥 — 您可以根据不同用户组的不同处理需求，将其中一些操作组合到不同的DLP策略中。

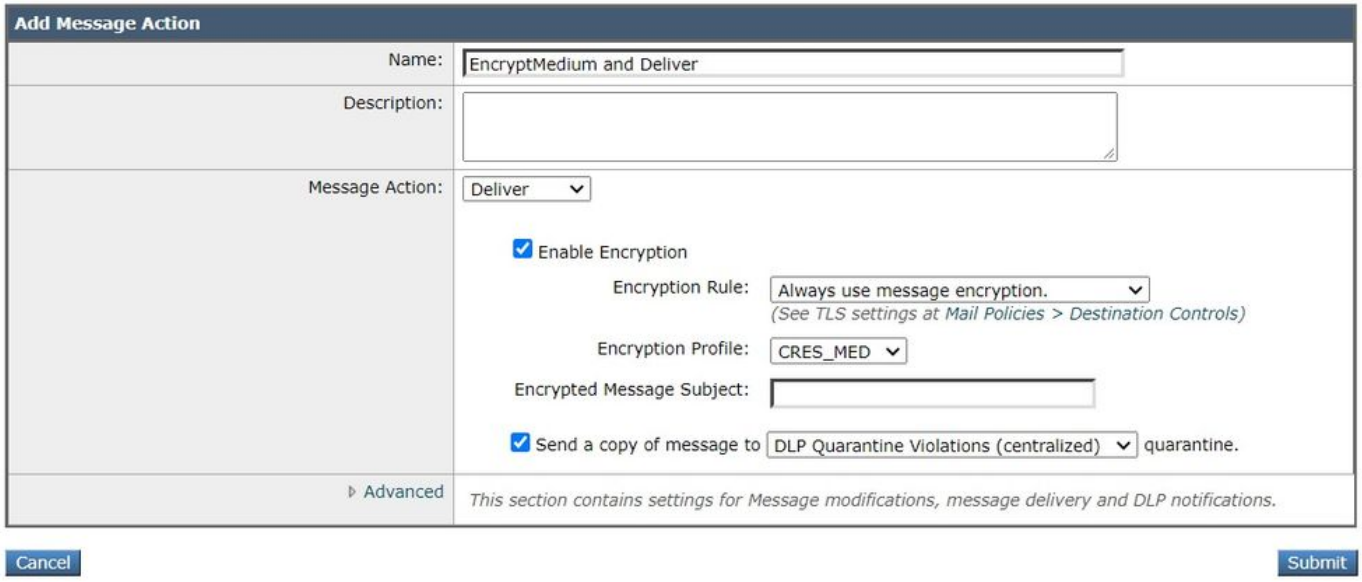
我们将实施以下DLP操作：加密

这些操作假设加密已在ESA上许可和配置，并且已按照前面部分中的步骤为高、中和低安全性创建了三个配置文件：

- CRES_HIGH
- CRES_MED
- CRES_LOW

创建DLP邮件操作

1. 转至邮件策略> DLP邮件自定义。
2. 点击“添加邮件操作”(Add Message Action)按钮并添加以下DLP操作。 确保在提交邮件操作后提交更改



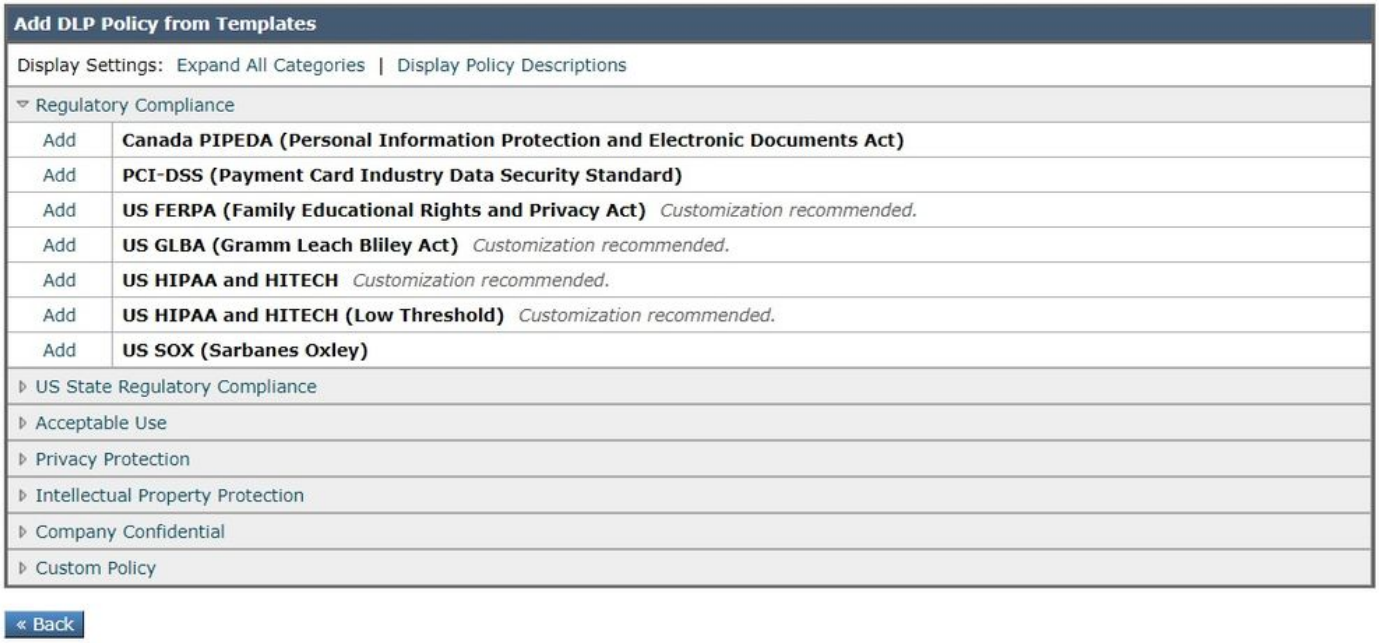
邮件操作

6.制定防数据丢失策略

DLP策略包括：

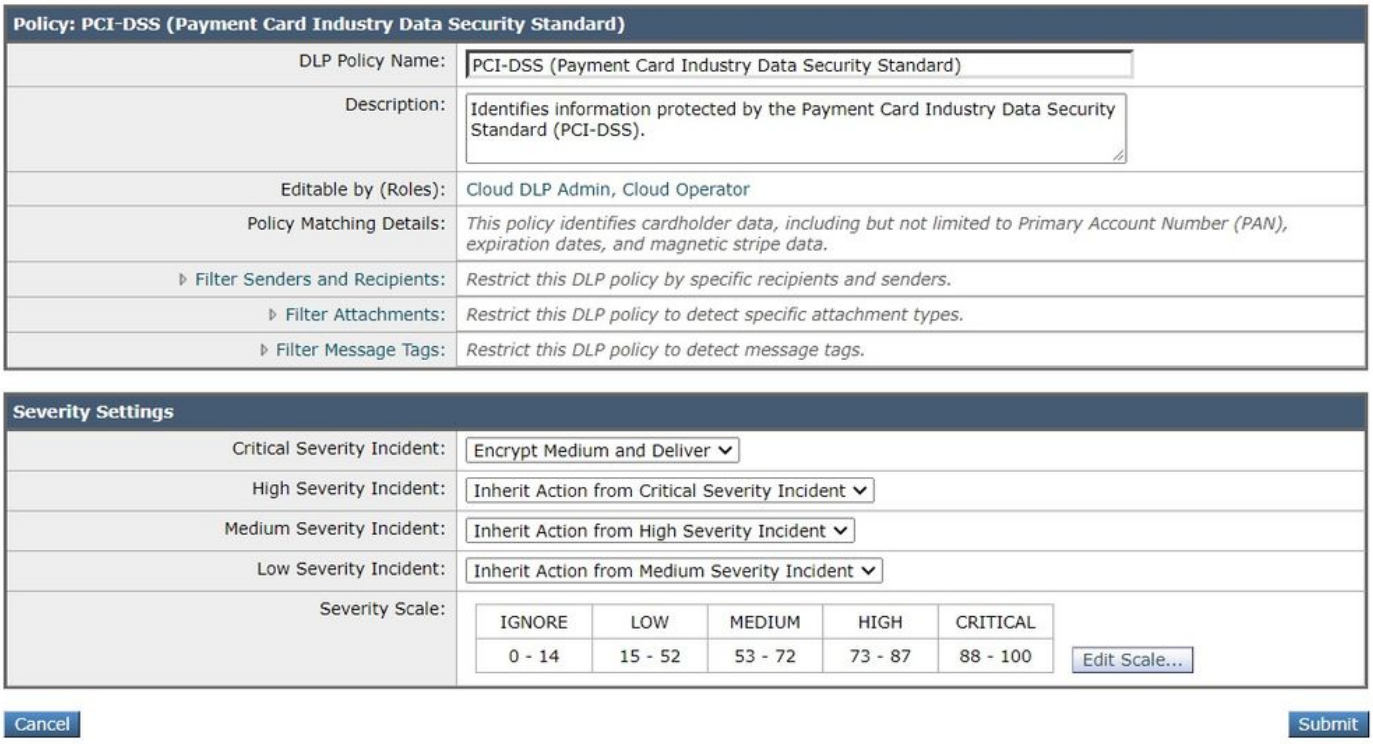
- 确定传出邮件是否包含敏感数据的一组条件
- 邮件包含此类数据时要执行的操作。

1. 导航至：邮件策略> DLP策略管理器
2. 单击“添加DLP策略”
3. 打开“合规性”信息披露三角框。



DLP策略模板

4.对于PCI策略，点击PCI-DSS左侧的“添加”按钮。



PCI-DSS DLP规则示例

5.对于“严重性严重性事件”，请选择我们之前配置的“加密介质并传送”操作。我们可以更改较低严重性事件，但现在，让我们使这些事件继承我们的严重性事件。提交，然后确认更改。

7.将DLP策略应用于传出邮件策略

1. 导航至：邮件策略>外发邮件策略
2. 点击默认策略的DLP的控制信元。如果尚未启用，它将显示为“已禁用”。
3. 将Disable DLP下拉按钮更改为Enable DLP，您将立即看到刚刚创建的DLP策略。

4. 点击“全部启用”复选框。提交，然后确认更改。

结论

总之，我们展示了准备思科邮件安全设备以发送加密邮件的必要步骤：

1. 启用Cisco IronPort邮件加密
2. 向RES注册您的ESA和组织
3. 创建加密配置文件
4. 启用DLP
5. 创建DLP邮件操作
6. 创建DLP策略
7. 将DLP策略应用于传出邮件策略

与您的ESA软件版本对应的《ESA用户指南》提供了更多详细信息。 用户指南位于以下链接：

http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html

相关信息

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。