防数据丢失和加密最佳实践指南

目录

简介

本文档介绍思科邮件安全的防数据丢失(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。 客户可以使用邮件加密，通过公共互联网安全地发送单个邮件，使用包括内容过滤和DLP在内的各种策略。 这些策略的创建将在此系列中的其他文档中讨论。 本文档重点介绍如何让ESA准备好发送加密邮件，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密钥，这样发送方就可以在邮件发送后对邮件进行精细控制，例如，锁定或过期，这样收件人就无法再打开邮件，而不会影响任何其他邮件。 加密消息时，ESA将加密密钥和元数据存储在CRES中，以了解每条加密消息。

ESA可以决定以多种方式加密邮件，例如通过“标志”（如主题内容）、内容过滤器匹配或通过DLP策略。 一旦ESA决定加密邮件，它会使用在“安全服务> Cisco IronPort邮件加密”（表名为“邮件加密配置文件”）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。 这将在3.创建加*密配置文件中讨论*。

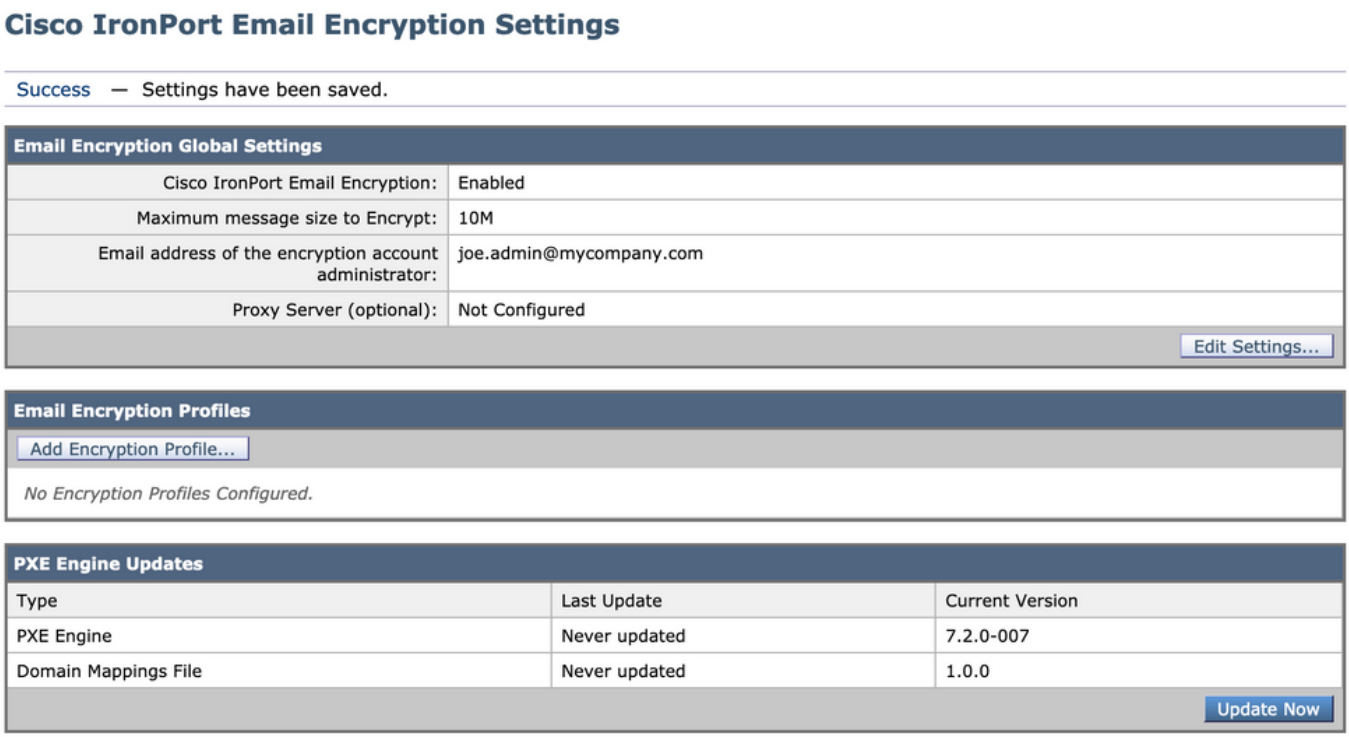
防数据丢失和加密最佳实践最佳实践指南

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步骤，因为这些设置通常在集群级别进行管理。 如果您有多台未群集的计算机，或者如果您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……** 指定管理员/人员的电子邮件地址，该管理员/人员是帐户的主要RES管理员。 此电子邮件帐户将与公司的RES环境管理相关联。可选：要加密的默认最大邮件大小为10M。 如果您愿意，您现在可以增加/减小尺寸。可选：如果您有ESA需要通过的代理通过HTTPS连接到RES，请添加必要的代理和身份验证设置以允许其通过代理。
5. 提交并提交配置更改。

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



2.在RES中注册ESA和组织

第#2步主要参与ESA管理控制台之外。

> **注意**：ESA注册信息也可在以下技术说明中找到：思科RES:虚拟、托管和硬件的帐户调配ESA配置示例

请直接向RES发送电子邮件:stg-cres-provisioning@cisco.com。

要为ESA的加密配置文件调配CRES帐户，请提供以下信息：

1. 帐户名称（**请指定确切的公司名称，因为您需要列出此名称。**）对于云邮件安全(CES)/托管客户帐户，请注明您的帐户名称以“<帐户名称>托管”结尾
2. 要用于帐户管理员的电子邮件地址(请**指定相应的管理员电子邮件地址)**
3. 完整的设备序列号 设备序列号可以通过ESA GUI（系统管理>功能密钥）或ESA CLI（通过“version”命令）找到。 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. 应映射到CRES帐户以用于管理的域名

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。这将确保将任何新设备序列号添加到正确的帐户，并避免公司信息和调配的重复。

请确保，如果您正在发送有关调配CRES帐户的电子邮件，我们将在一(1)个工作日内回复。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)完成。

> **注意**：在您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。 步骤#3中的“调配”任务在完成之前将无法工作。

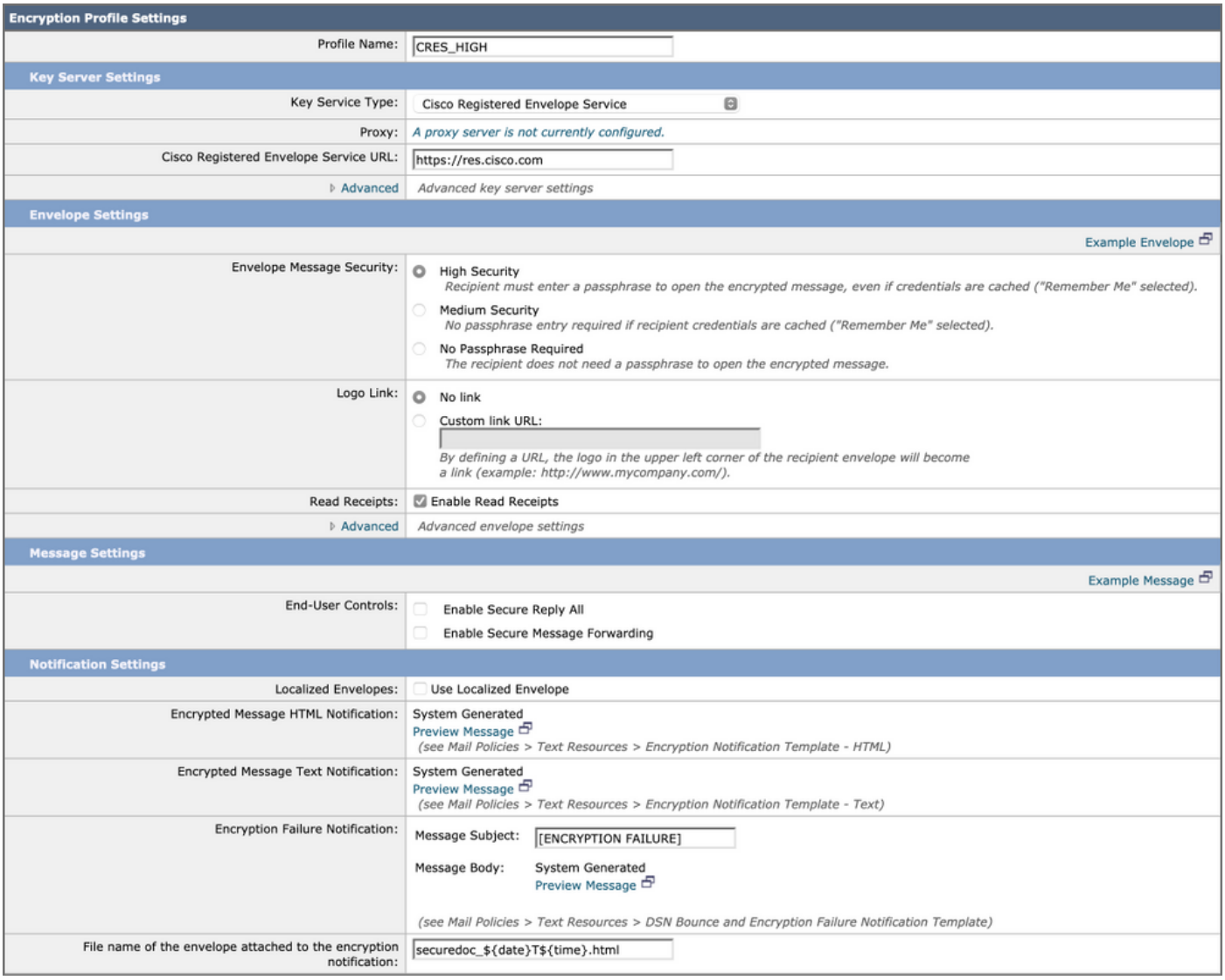
3.在ESA上创建加密配置文件

注意：如果集群中有多个ESA，则只需执行一次步骤#1步骤，因为这些设置通常在集群级别进行管理。 如果您有多台未群集的计算机，或者如果您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，组织可能需要为其某一段收件人发送高安全性信封，例如他们知道经常向其发送高度敏感数据的收件人。 同一组织可能有接收者社区中其他部分的接收者不太敏感的信息，而且可能没有那么耐心地提供用户ID和密码来接收加密邮件。 这些收件人是低安全性信封的好候选者。 拥有多个加密配置文件使组织能够为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就行。

在本文档中，我们将显示创建三个加密配置文件的示例，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“添加加密配置文件……”"
3. 将会打开“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. 为信封邮件安全选择“高安全性”(High Security)（如果尚未选择）。
5. 单击**Submit**以保存此配置文件。



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，选择“无密码要求”单选按钮

您会注意到，有以下选项可供选择：启用读取回执、启用全部安全回复和启用安全邮件转发。 在信封设置中，如果单击“高级”链接，可以选择三种对称加密算法之一，并指定信封在不使用Java加密小程序的情况下发送。

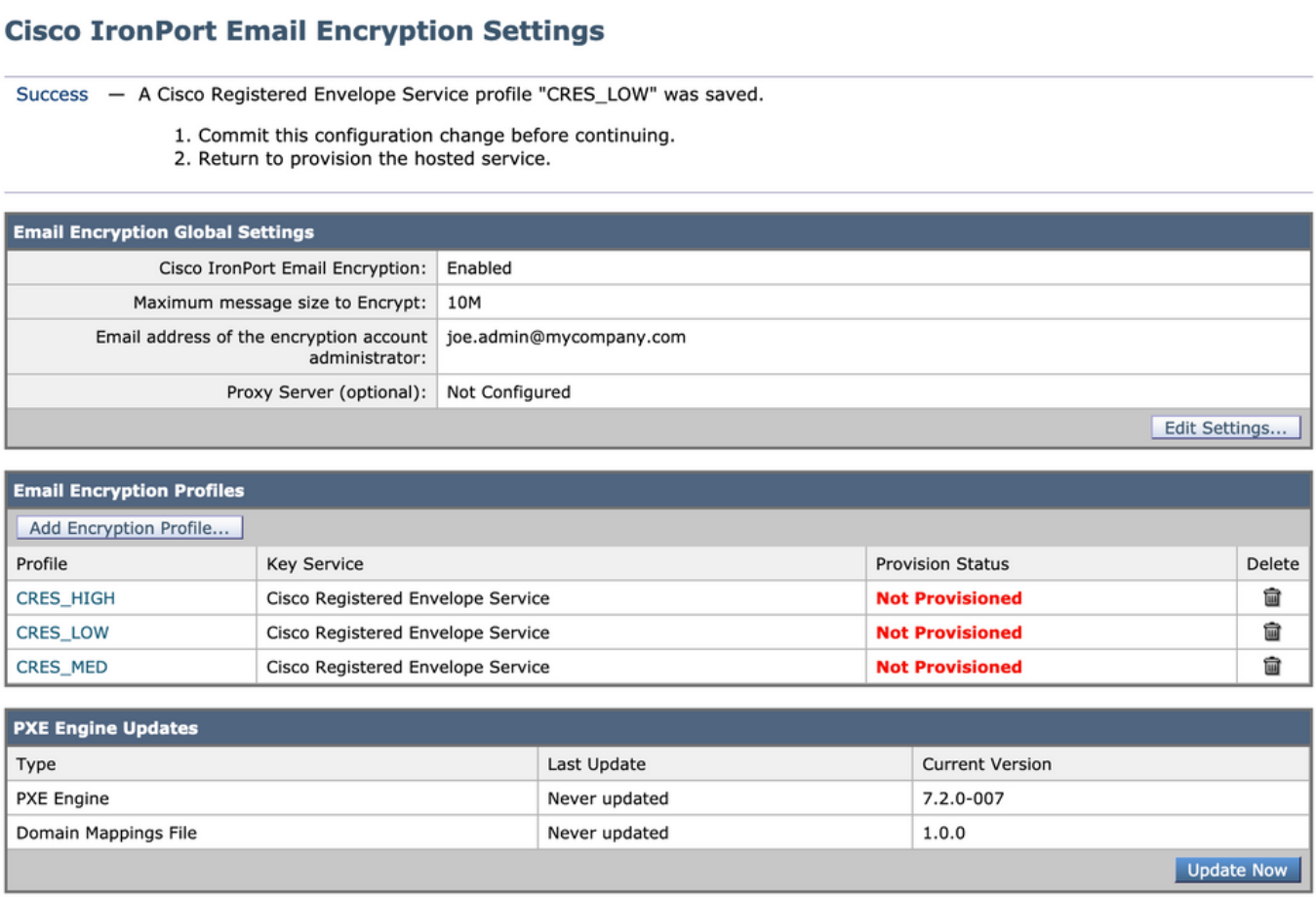
在“信封设置”(Envelope Settings)右侧，您会看到“示例消息”(Example Message)超文本链接。 如果单击，这将显示一个安全邮件信封示例 — 收件人打开HTML附件后在邮件中将看到的内容。

“读取回执”(Read Receipts)表示当收件人打开安全邮件时，加密邮件的发件人将收到来自CRES的电子邮件（这表示收件人拉下对称密钥并解密邮件）。

在“消息设置”(Message Settings)右侧，您将看到“示例消息”超文本链接。 如果单击，这将显示打开的邮件的样式 — 收件人在信封中提供必要信息并打开加密邮件后，将看到什么。

请务必单击“提**交”**并提交更改。

然后，表中的行将显示“调配”按钮。 “提交”更改后，“调配”按钮才会显示。

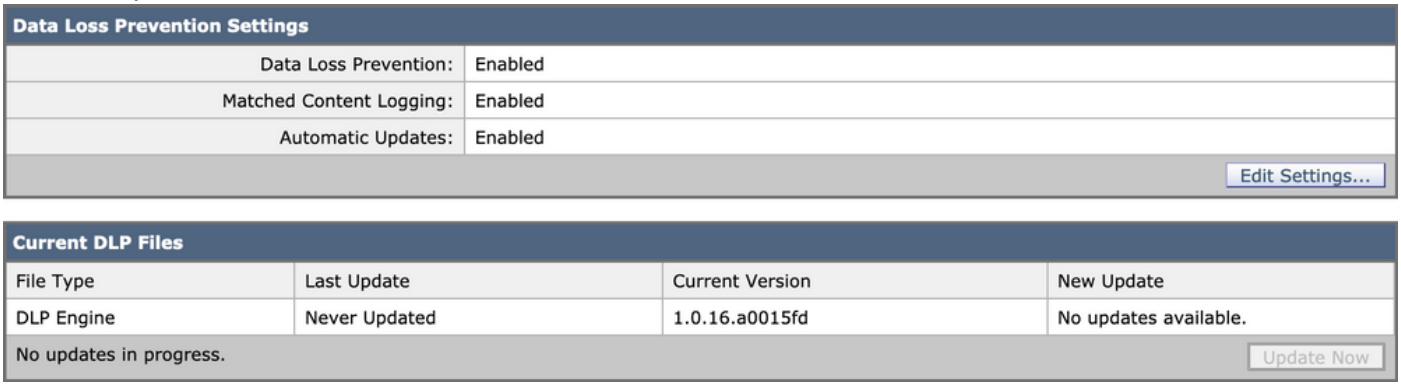


再次单击“调配”按钮，此操作仅在您的公司RES帐户已创建且设备S/N已添加到您的帐户后才可用。 如果RES帐户链接到ESA，调配过程将相对快速。 否则，该过程必须先完成。

调配完成后，您的Cisco IronPort邮件加密页面将显示配置文件为已调配。

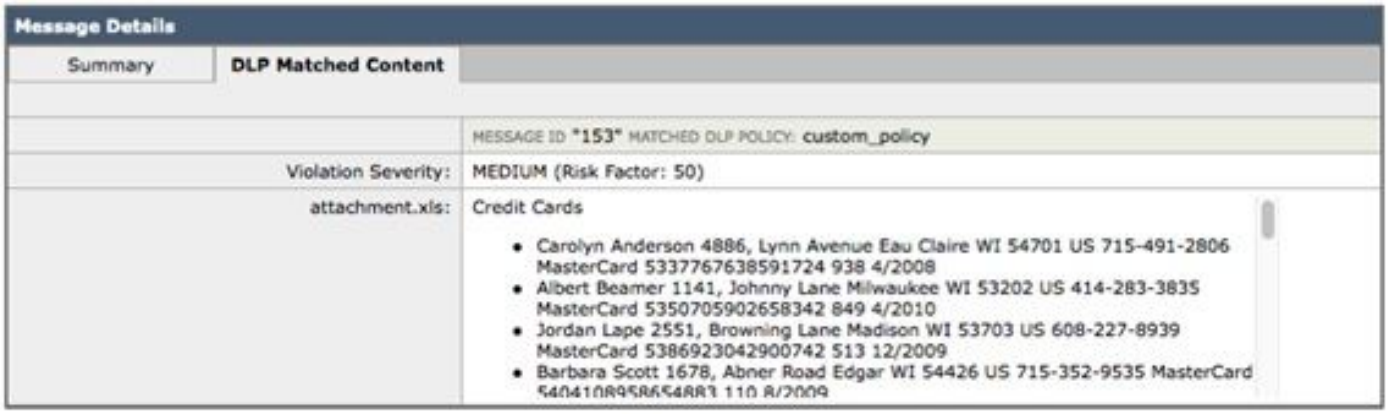
4.启用防数据丢失(DLP)

1. 从ESA UI导航至Security Services **> Data Loss Prevention**。
2. 单**击启用。**..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. 点击启用自动更新复选框。
6. 单击“Submit”。



DLP引擎和设备上预定义的内容匹配分类器的更新与其他安全服务的更新无关。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。

启用“匹配内容日志记录”时，它允许邮件跟踪显示导致违规的邮件内容。以下是邮件跟踪示例，显示导致DLP违规的邮件内容。 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，可以为每种策略违规类型创建单独的策略隔离区。当运行“透明”POV时，这尤其有用，在该POV中，违反DLP策略的出站邮件会被记录和传送，但对邮件不执行任何操作。

1. 在SMA上，导航至**Email > Message Quarantine > Policy， Virus， and Outbreak Quarantines**
2. 这是“隔离区”(Quarantines)表在我们开始之前应显示的内容
   ：

Policy, Virus and Outbreak Quarantines

Add Policy Quarantine... | Search Across Quarantines

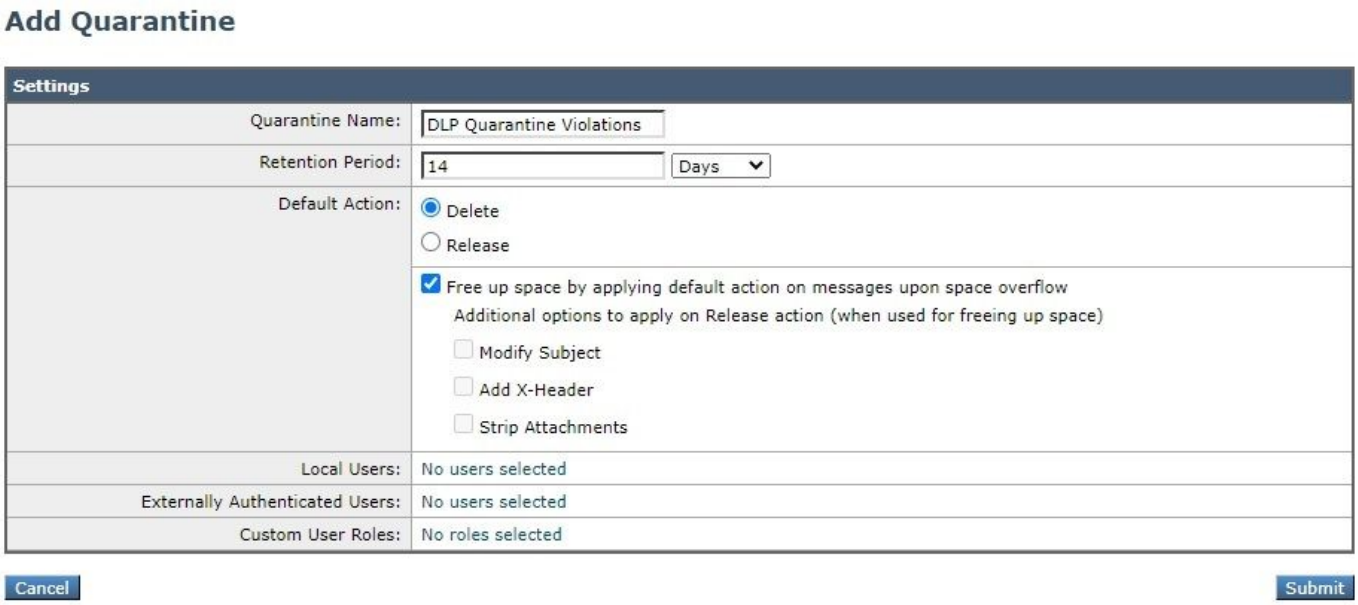
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	N/A	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	23 Jul 2020 14:43 (GMT +00:00)	0	
Policy	Policy	0	Retain 10 days then Delete	N/A	0	
Unclassified	Unclassified	0	Retain 30 days then Release	N/A	0	
Virus	Antivirus	0	Retain 30 days then Delete	N/A	0	

Available space for Policy, Virus, Antimalware & Outbreak quarantines is 10G.

策略病毒和爆发隔离区

3. 点击“添加策略隔离”(Add Policy Quarantine)按钮，创建要由DLP策略使用的隔离区。

下面是为中型DLP违规进行的隔离示例。可以对隔离区进行分段，并且可能需要对多个DLP规则进行分段：



DLP隔离示例

关于DLP邮件操作

DLP邮件操作描述ESA在检测传出邮件中的DLP违规时将采取哪些操作。您可以指定主DLP操作和辅助DLP操作，并且可以为不同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

对于记录和报告DLP违规但邮件未停止/隔离或加密的只读状态，最常使用“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。它不加密邮件报头。
- 更改主题标题。
- 将免责声明文本/HTML添加到邮件。
- 将邮件发送到备用目的邮件主机。
- 正在发送密件抄送邮件副本。
- 向发件人和/或其他联系人发送DLP违规通知。

这些操作不是互斥的 — 您可以将其中一些操作组合到不同的DLP策略中，以满足不同用户组的各种处理需求。

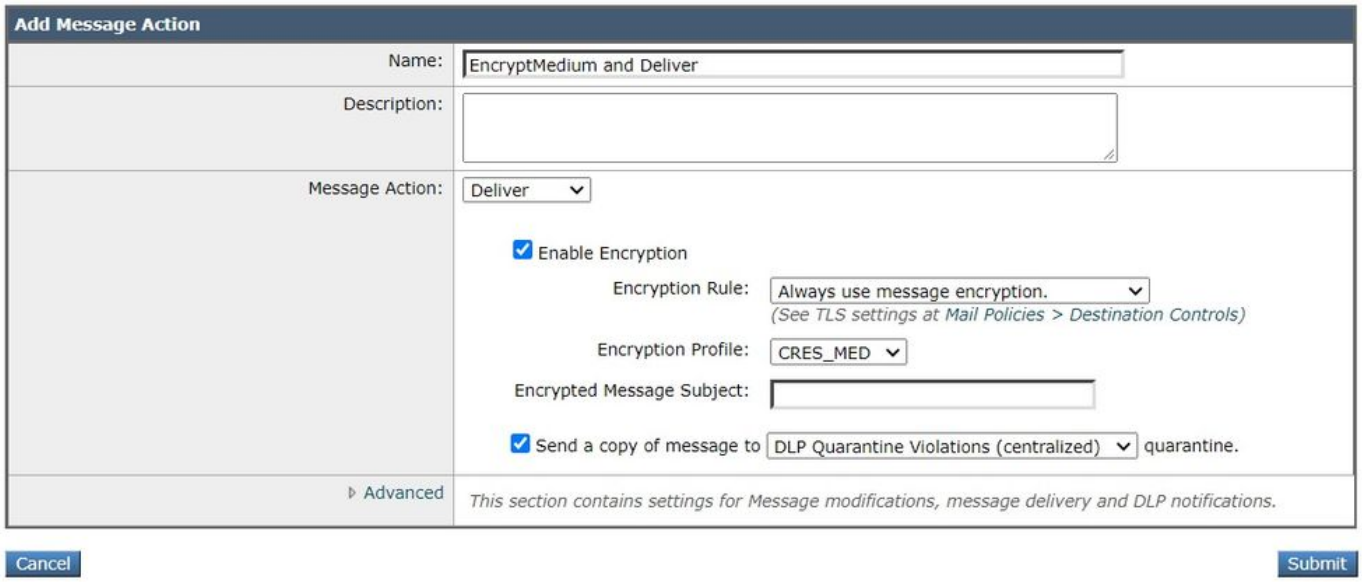
我们将实施以下DLP操作：加**密**

这些操作假设加密已在ESA上许可并配置，并且已为高安全性、中安全性和低安全性创建了三个配置文件，如前几节所述：

- 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，然后添加以下DLP操作。 确保提交邮件操作后提交更改



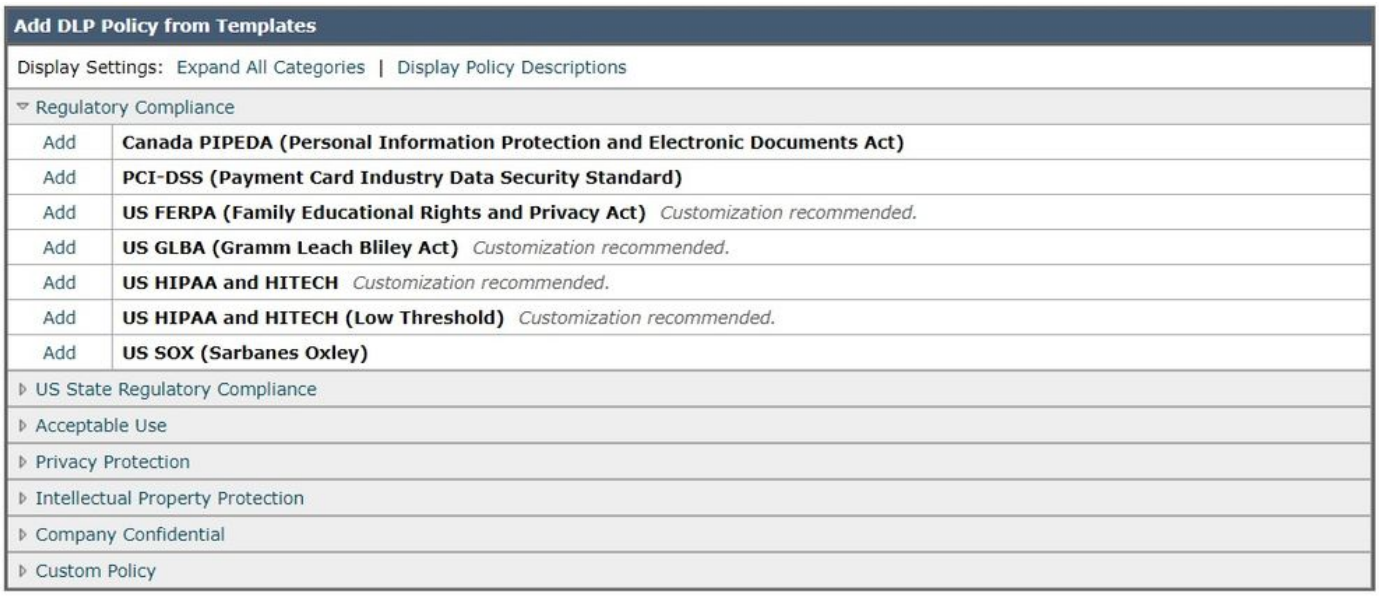
消息操作

6.制定防数据丢失政策

DLP策略包括：

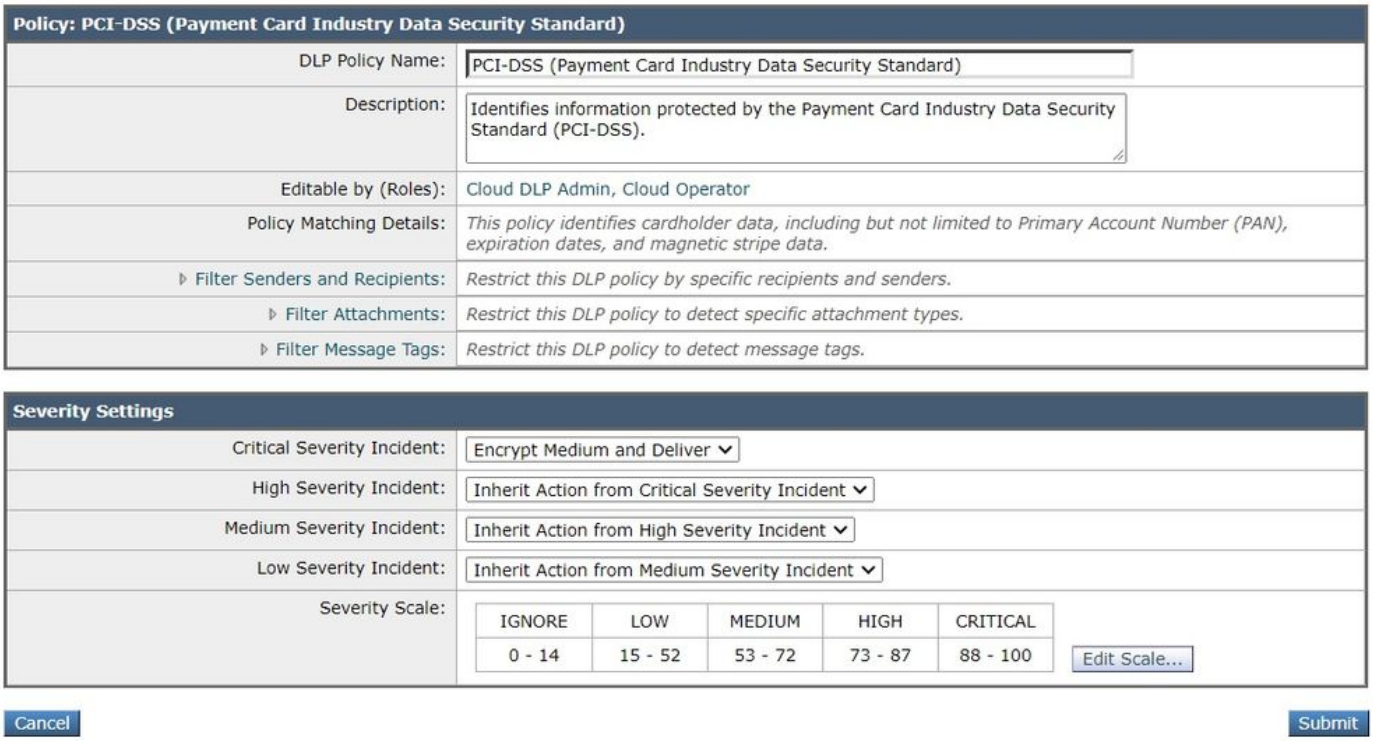
- 确定传出消息是否包含敏感数据的一组条件
- 当邮件包含此类数据时要采取的操作。

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”披露三角。



DLP策略模板

4.对于PCI策略，单击PCI-DSS左侧的“添加”按钮。



PCI-DSS示例DLP规则

5.对于严重性事故，请选择“加密介质并传送”操作，我们之前已配置。我们可以更改严重性较低的事故，但是现在，让我们让它们继承我们的严重事故。提交，然后提交更改。

7.将DLP策略应用于传出邮件策略

1. 导航至：邮件策略>传出邮件策略
2. 点击默认策略的DLP控制单元。如果您尚未启用它，它将显示为“已禁用”。
3. 将下拉按钮从“禁用DLP”(Disable DLP)更改为“启用DLP”(Enable DLP)，系统会立即显示您刚创建的DLP策略。
4. 单击“全部启用”复选框。提交，然后提交更改。

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ESA软件版本对应的《ESA用户指南》中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