Guía de prácticas recomendadas para la prevención de la pérdida de datos y el cifrado

Contenido

Introducción

Este documento describe las prácticas recomendadas para la prevención de la pérdida de datos (DLP) y el cifrado para Cisco Email Security.

Este documento explica la configuración del cifrado de mensajes mediante Cisco Email Security Appliance (ESA) y el servicio Cisco Registered Envelope Service (RES) basado en la nube. Los clientes pueden utilizar el cifrado de mensajes para enviar mensajes individuales de forma segura a través de la Internet pública, utilizando diversos tipos de políticas, incluidos el filtrado de contenido y DLP. La creación de estas políticas se discutirá en otros documentos de esta serie. Este documento se centra en conseguir que el ESA esté preparado para enviar correo cifrado de modo que las políticas puedan utilizar el cifrado como acción.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En este documento se explican los siguientes pasos:

1. Habilitación de Cisco IronPort Email Encryption
2. Registre sus ESA y su organización con RES
3. Creación de perfiles de cifrado
4. Habilitación de DLP
5. Creación de acciones de mensaje DLP
6. Creación de políticas DLP
7. Aplicación de políticas DLP a una política de correo electrónico saliente

Una vez que estos pasos se hayan completado correctamente, el administrador ESA puede crear correctamente una política que utilice el cifrado como acción.

Cisco IronPort Email Encryption también se conoce como cifrado RES. RES es el nombre que utilizamos para los "servidores clave" en la nube de Cisco. La solución de cifrado RES utiliza cifrado de clave simétrica, lo que significa que la clave utilizada para cifrar el mensaje es la misma que se utiliza para descifrar el mensaje. Cada mensaje cifrado utiliza una clave única, que permite al remitente tener un control granular sobre un mensaje después de su envío (por ejemplo, bloquearlo o caducarlo para que el destinatario ya no pueda abrirlo) sin afectar a otros mensajes. Al cifrar un mensaje, el ESA almacena la clave de cifrado y los metadatos en CRES sobre cada mensaje cifrado.

El ESA puede decidir cifrar un mensaje de muchas maneras, por medio del "indicador" (como el contenido del asunto), a través de la coincidencia del filtro de contenido o a través de la política DLP, por ejemplo. Una vez que el ESA decide cifrar un mensaje, lo hace con un "perfil de cifrado" especificado creado en "Servicios de seguridad > Cifrado de correo electrónico de Cisco IronPort", la tabla denominada "Perfiles de cifrado de correo electrónico". De forma predeterminada, no hay perfiles de cifrado. Esto se debatirá en *3. Crear perfiles de cifrado*.

Guía de prácticas recomendadas para la prevención de la pérdida de datos y las prácticas recomendadas de cifrado

1. Habilitación de Cisco IronPort Email Encryption en los ESA

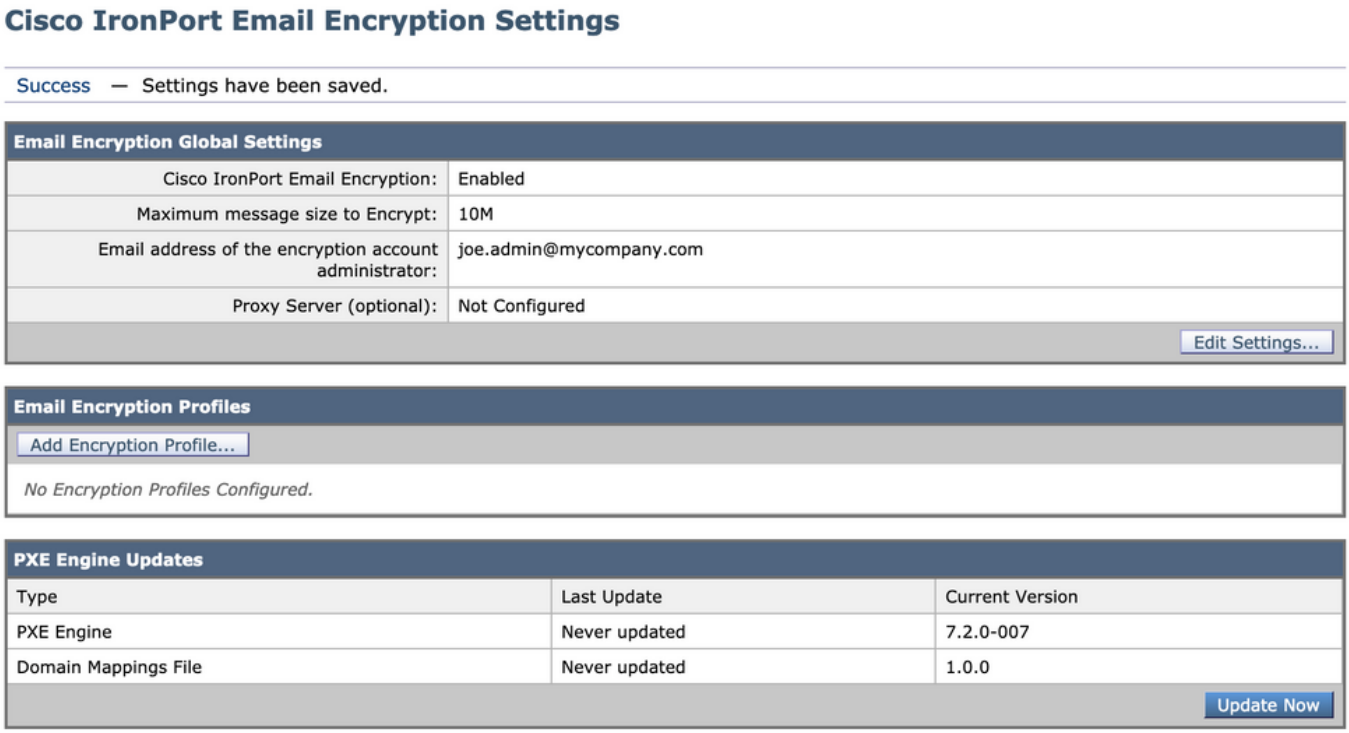
> **Nota:** Si tiene varios ESA en un clúster, el paso n.º 1 sólo debe realizarse una vez, ya que estos valores se administran normalmente en el nivel de clúster. Si tiene varias máquinas que no están agrupadas o si está administrando estas configuraciones en el nivel de máquina, el paso 1 se debe realizar en cada ESA.

1. Desde la interfaz de usuario ESA, navegue hasta **Servicios de seguridad > Cisco IronPort Email Encryption**.
2. Marque la casilla para activar Cisco IronPort Email Encryption.
3. Acepte el Acuerdo de licencia de usuario final (EULA) y el Acuerdo de licencia de cifrado de

correo electrónico de Cisco IronPort.

4. En *Configuración global de cifrado de correo electrónico*, haga clic en **Editar configuración...** Especifique la dirección de correo electrónico del administrador/persona que es el administrador RES principal de la cuenta. Esta cuenta de correo electrónico se asociará con la administración del entorno RES para la empresa.Opcional: El tamaño máximo predeterminado del mensaje para cifrar es 10M. Puede aumentar/disminuir el tamaño en este momento si lo desea.Opcional: Si dispone de un proxy que el ESA tendrá que pasar para conectarse a RES a través de HTTPS, agregue los parámetros de proxy y autenticación necesarios para permitirle pasar por el proxy.
5. Envíe y confirme los cambios de configuración.

En este punto, debería ver la configuración global de "Email Encryption Global Settings" establecida en algo como esto, sin embargo, aún no aparece ningún perfil en la lista:



2. Registre sus ESA y su organización con RES

El paso 2 toma parte principalmente fuera de la consola de administración de ESA.

> **Nota:** La información de registro de ESA también se encuentra en la siguiente nota técnica: RES de Cisco: Ejemplo de Configuración de Aprovisionamiento de Cuenta para Virtual, Hosted y Hardware ESA

Envíe un correo electrónico directamente a RES: stg-cres-provisioning@cisco.com.

Para aprovisionar una cuenta CRES para los perfiles de cifrado de su ESA, proporciónenos la siguiente información:

1. Nombre de la cuenta **(especifique el nombre exacto de la empresa, ya que debe indicarlo).** En el caso de las cuentas de cliente de Cloud Email Security (CES)/Hosted, indique su

nombre de cuenta para finalizar como "<Account Name> HOSTED"
2. Direcciones de correo electrónico que se utilizarán para el administrador de cuentas **(especifique la dirección de correo electrónico administrativa correspondiente)**
3. Número(s) de serie completo del dispositivo Se puede encontrar un número de serie del dispositivo desde la GUI de ESA (Administración del sistema > Claves de funciones) o la CLI de ESA a través del comando 'version'. No es aceptable proporcionar una licencia con número de licencia virtual (VLN) o clave de actividad de productos (PAK), ya que se requiere un número de serie de dispositivo completo para la administración de cuentas de CRES.
4. Nombres de dominio que deben asignarse a la cuenta CRES para fines de administración

Nota: Si ya dispone de una cuenta de CRES, indique el nombre de la empresa o el número de cuenta de CRES existente. Esto garantizará que los nuevos números de serie del dispositivo se agreguen a la cuenta correcta y evitará cualquier duplicación de la información y el aprovisionamiento de la empresa.

Por favor, tenga la seguridad de que si envía un correo electrónico sobre el aprovisionamiento de una cuenta de CRES, responderemos con un (1) día laborable. Si necesita asistencia y asistencia inmediatas, abra una solicitud de asistencia con el TAC de Cisco. Esto se puede hacer a través de Support Case Manager (https://mycase.cloudapps.cisco.com/case) o llamando por teléfono (https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html).

> **Nota:** Después de enviar esta solicitud por correo electrónico, puede que le lleve un día crear la cuenta de RES de la empresa (si aún no se ha creado) y agregar los S/N. La tarea "Aprovisionamiento", en el paso 3, no funcionará hasta que se complete.

3. Crear perfiles de cifrado en los ESA

> **Nota:** Si tiene varios ESA en un clúster, el paso n.º 1 sólo debe realizarse una vez, ya que estos valores se administran normalmente en el nivel de clúster. Si tiene varias máquinas que no están agrupadas o si está administrando estas configuraciones en el nivel de máquina, el paso 1 se debe realizar en cada ESA.

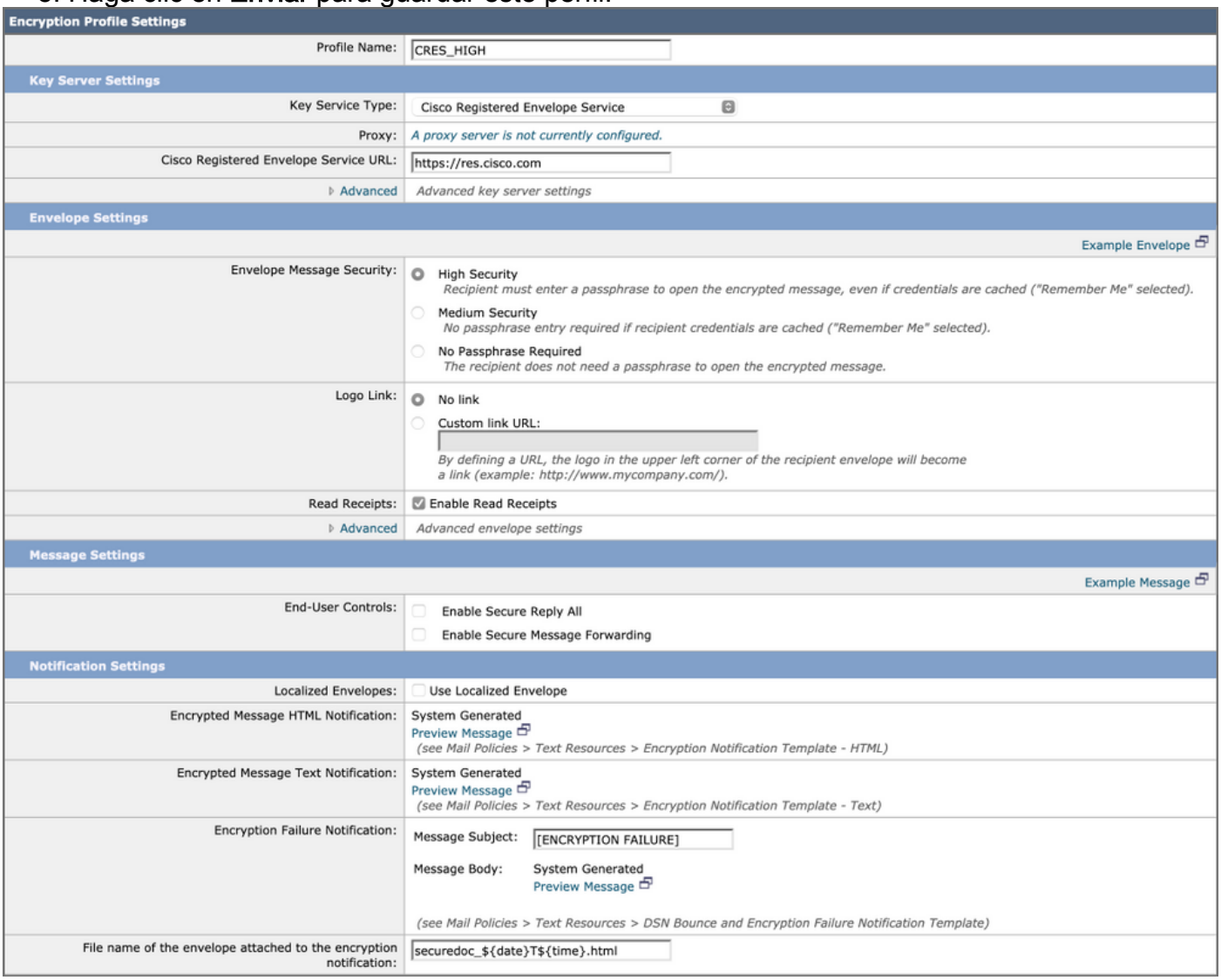
Un perfil de cifrado especifica cómo se deben enviar los mensajes cifrados. Por ejemplo, una organización puede necesitar enviar sobres de alta seguridad para un segmento de sus destinatarios, como aquellos a los que saben que con frecuencia enviarán datos altamente confidenciales. La misma organización puede tener otros segmentos de su comunidad receptora que reciben información menos confidencial y que quizás tengan menos pacientes al tener que proporcionar ID de usuario y contraseña para recibir correo cifrado. Esos destinatarios serían buenos candidatos para un tipo de sobre de baja seguridad. La existencia de varios perfiles de cifrado permite a la organización adaptar el formato de mensaje cifrado al público. Por otra parte, muchas organizaciones pueden estar bien con un solo perfil de cifrado.

Para este documento, mostraremos un ejemplo de creación de tres perfiles de cifrado denominados "CRES_HIGH", "CRES_MED" y "CRES_LOW".

1. Desde la interfaz de usuario ESA, navegue hasta **Servicios de seguridad > Cisco IronPort Email Encryption**.
2. Haga clic en "Agregar perfil de cifrado..."
3. Se abrirá el menú Encryption Profile (Perfil de cifrado) y podrá asignar el nombre de su

primer perfil de cifrado "CRES_HIGH".

4. Seleccione "High Security" (Alta seguridad) para la seguridad del mensaje del sobre, si aún no está seleccionada.
5. Haga clic en **Enviar** para guardar este perfil.



A continuación, repita los pasos 2-5 para crear "CRES_MED" y "CRES_LOW"; basta con cambiar el botón de opción de Envelope Message Security para cada perfil.

- Para el perfil CRES_HIGH, seleccione el botón de opción "Alta seguridad".
- Para el perfil CRES_MED, seleccione el botón de opción "Seguridad media".
- Para el perfil CRES_LOW, seleccione el botón de opción "No se requiere contraseña"

Observará que hay opciones para activar los recibos de lectura, habilitar la respuesta segura a todos y habilitar el reenvío seguro de mensajes. En Configuración de sobre, si hace clic en el enlace "Avanzado", puede seleccionar uno de los tres algoritmos de cifrado simétrico, así como especificar que el sobre se envíe sin el applet de cifrado Java.

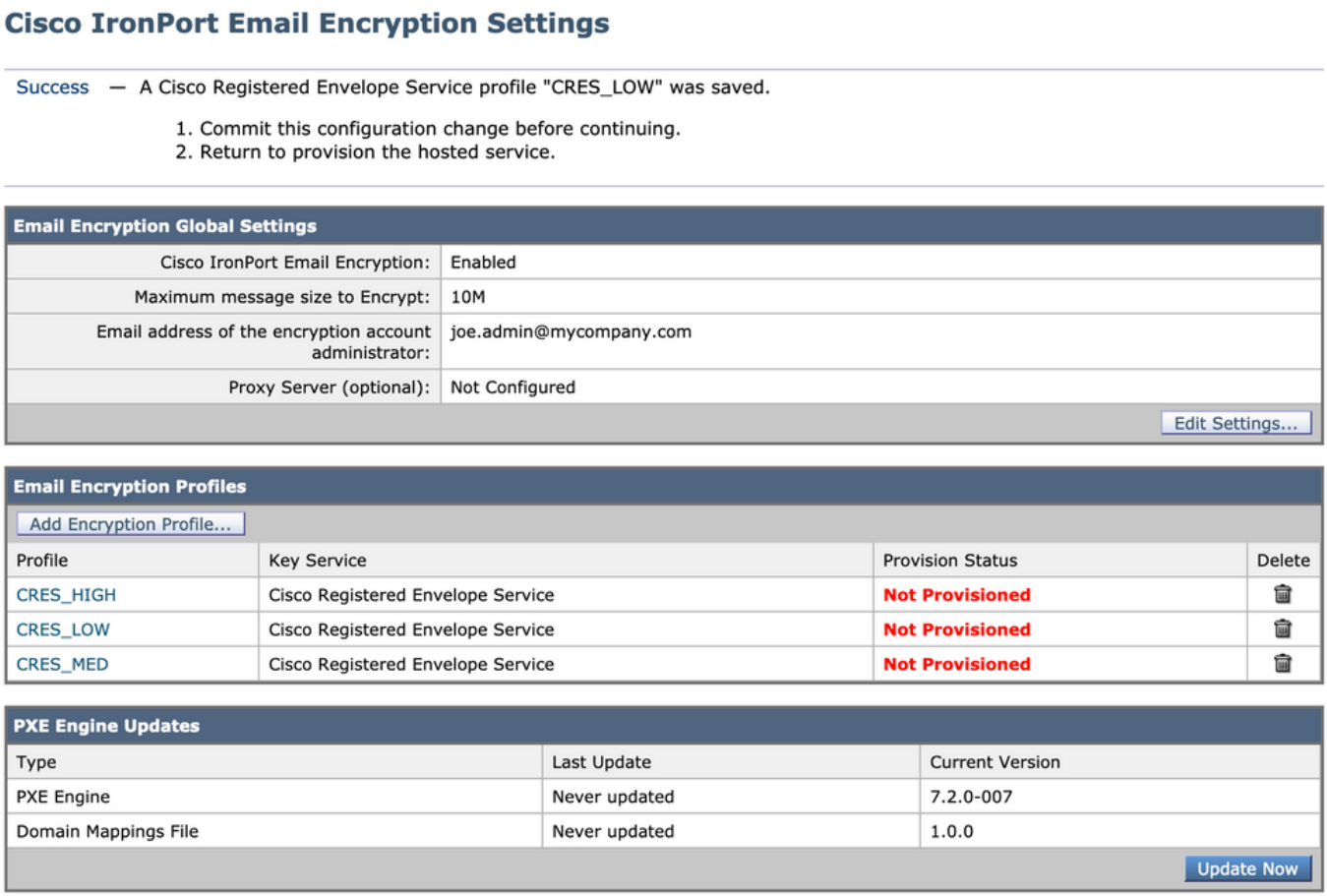
A la derecha de Configuración del sobre, verá el enlace de hipertexto "Mensaje de ejemplo". Si se hace clic en esta opción, se mostrará un ejemplo del sobre de mensaje seguro: lo que el destinatario verá en su correo electrónico después de abrir el archivo adjunto HTML.

Leer confirmación significa que el remitente del mensaje cifrado recibirá un correo electrónico de CRES cuando el destinatario abra el mensaje seguro (lo que significa que el destinatario retiró la clave simétrica y descifró el mensaje).

A la derecha de Message Settings (Configuración de mensajes), verá el enlace de hipertexto "Ejemplo de mensaje". Si se hace clic en esta opción, se mostrará cómo se verá el mensaje abierto: qué verá el destinatario una vez que haya proporcionado la información necesaria en el sobre y haya abierto el mensaje cifrado.

Recuerde siempre hacer clic en **Enviar** y registrar cambios.

A continuación, la fila de la tabla mostrará el botón "Provisión". El botón Aprovisionamiento no aparecerá hasta después de realizar cambios.



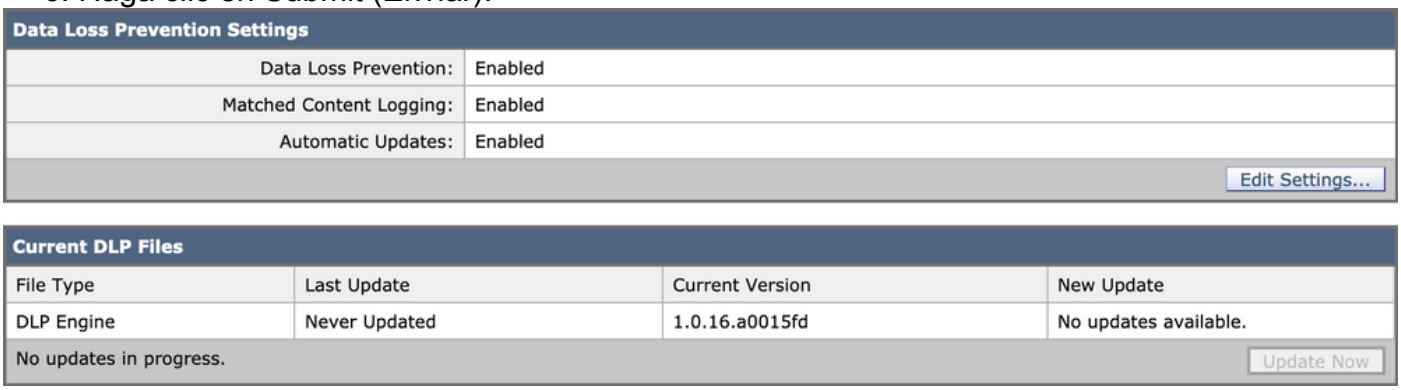
Vuelva a hacer clic en el botón Aprovisionamiento. Esto sólo funcionará después de que se haya creado su cuenta RES de la empresa y de que se hayan agregado los S/N del dispositivo a su cuenta. Si la cuenta RES está vinculada al ESA, el proceso de aprovisionamiento se llevará a cabo con relativa rapidez. Si no lo es, ese proceso tendrá que completarse primero.

Una vez completado el aprovisionamiento, la página Cisco IronPort Email Encryption (Cifrado de correo electrónico de Cisco IronPort) mostrará el perfil tal como se ha aprovisionado.

4. Habilitación de la prevención de la pérdida de datos (DLP)

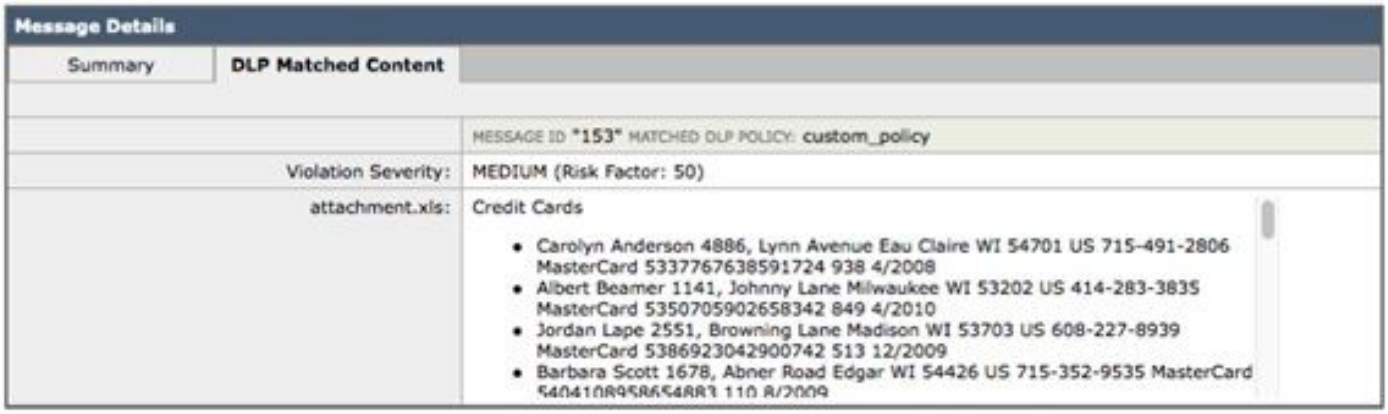
1. Desde la interfaz de usuario de ESA, navegue hasta **Servicios de seguridad > Prevención de pérdida de datos**.
2. Haga clic en **Habilitar...** para activar DLP.
3. Acepte el EULA, Acuerdo de licencia de prevención de pérdida de datos.
4. Haga clic en la casilla de verificación Habilitar registro de contenido coincidente.

5. Haga clic en la casilla de verificación Habilitar actualizaciones automáticas.
6. Haga clic en Submit (Enviar).



Las actualizaciones para el motor DLP y los clasificadores predefinidos de coincidencia de contenido en su dispositivo son independientes de las actualizaciones para otros servicios de seguridad. Las actualizaciones regulares de la firma Talos de entre 3 y 5 minutos son diferentes y no incluyen la actualización de las políticas y diccionarios de DLP. Las actualizaciones deben estar habilitadas aquí.

Cuando se habilita "Registro de contenido coincidente", permite que el rastreo de mensajes muestre el contenido del correo electrónico que causó la violación. Este es un ejemplo de Rastreo de mensajes que muestra el contenido de correo electrónico que causó la violación de DLP. De esta manera, un administrador puede saber exactamente qué datos desencadenaron una política de DLP específica.



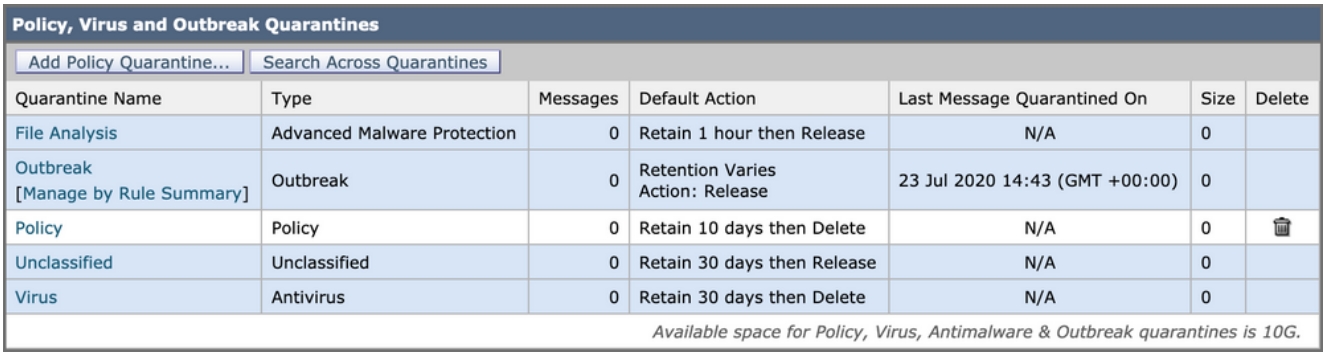
Violación de prevención de pérdida de datos

5. Creación de Acciones de Mensaje de Prevención de Pérdida de Datos

Crear cuarentenas DLP

Si desea conservar una copia de los mensajes que infringen las políticas de DLP, puede crear cuarentenas de políticas individuales para cada tipo de violación de políticas. Esto es especialmente útil cuando se ejecuta un POV "transparente", donde los mensajes salientes que violan las políticas de DLP se registran y envían pero no se realiza ninguna acción en los mensajes.

1. En el SMA, navegue hasta **Correo electrónico > Cuarentena de mensajes > Cuarentenas de brotes, virus y políticas**
2. Así debe ser la tabla de cuarentenas antes de comenzar:



Policy, Virus and Outbreak Quarantines

Add Policy Quarantine... | Search Across Quarantines

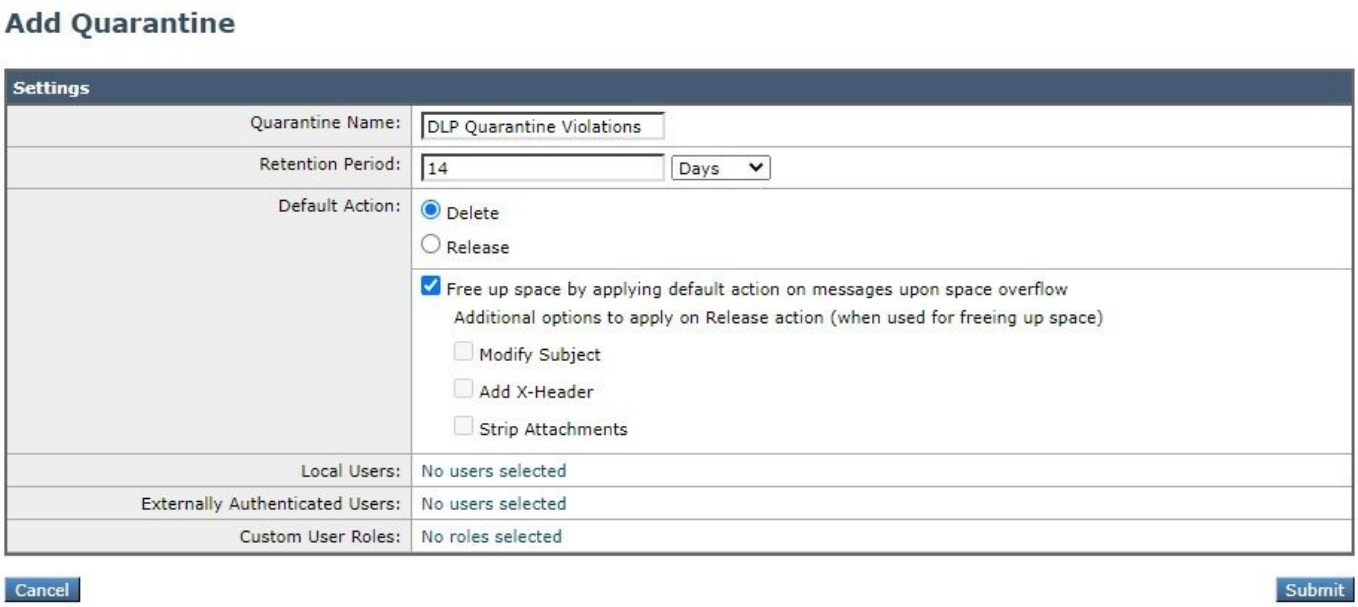
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	N/A	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	23 Jul 2020 14:43 (GMT +00:00)	0	
Policy	Policy	0	Retain 10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

Cuarentena de brotes y virus de políticas

3. Haga clic en el botón "Agregar cuarentena de política" y cree una cuarentena que utilizará la política de DLP.

A continuación se muestra un ejemplo de cuarentena realizada para una violación DLP de medio. La segmentación de cuarentenas es posible y se puede desear para varias reglas DLP:



Add Quarantine

Settings

Quarantine Name:	DLP Quarantine Violations
Retention Period:	14 Days
Default Action:	(•) Delete ( ) Release
	[x] Free up space by applying default action on messages upon space overflow Additional options to apply on Release action (when used for freeing up space) [ ] Modify Subject [ ] Add X-Header [ ] Strip Attachments
Local Users:	No users selected
Externally Authenticated Users:	No users selected
Custom User Roles:	No roles selected

Cancel | Submit

Ejemplo de cuarentena DLP

Acerca de las acciones de mensaje DLP

Las acciones de mensajes DLP describen las acciones que realizará el ESA cuando detecte una violación de DLP en un correo electrónico saliente. Puede especificar acciones DLP primarias y secundarias y se pueden asignar diferentes acciones para diferentes tipos de infracciones y gravedad.

Las acciones principales incluyen:

- Entregar
- Desplegar
- Cuarentena

En el caso de un estado de sólo lectura en el que se registran y notifican las violaciones de DLP, pero los mensajes no se detienen/ponen en cuarentena ni se cifran, la acción Entregar se utiliza con mayor frecuencia.

Las acciones secundarias incluyen:

- Enviar una copia a cualquier cuarentena personalizada o a la cuarentena de "política".

- **Cifrar el mensaje.** El dispositivo solo cifra el cuerpo del mensaje. No cifra los encabezados de los mensajes.
- Alteración del encabezado Asunto.
- Agregar texto/HTML de advertencia al mensaje.
- Enviando el mensaje a un host de correo de destino alternativo.
- Enviando copias bcc del mensaje.
- Enviando notificación de violación de DLP al remitente y/u otros contactos.

Estas acciones no se excluyen mutuamente: puede combinar algunas de ellas dentro de diferentes políticas de DLP para diversas necesidades de procesamiento de diferentes grupos de usuarios.

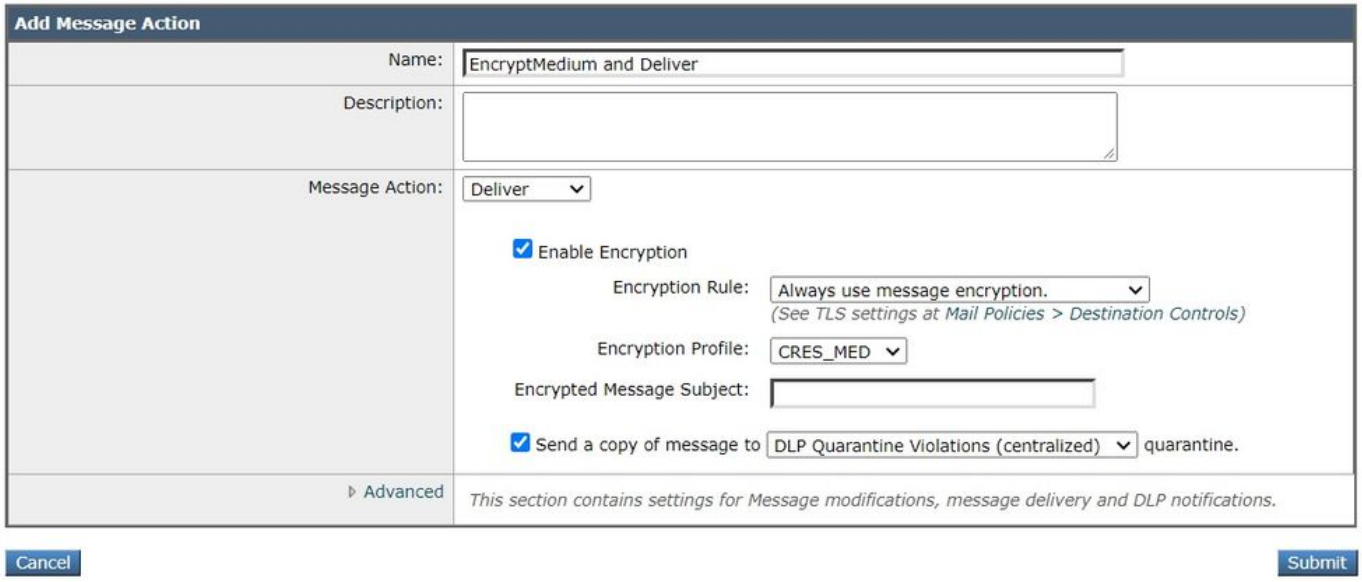
Vamos a implementar las siguientes acciones de DLP: **Cifrar**

Estas acciones asumen que la licencia de cifrado se otorga y se configura en el ESA y se han creado tres perfiles para alta, media y baja seguridad, como se hizo en las secciones anteriores:

- CRES_HIGH
- CRES_MED
- CRES_LOW

Crear las acciones de mensaje DLP

1. Vaya a *Políticas de correo > Personalizaciones de mensajes DLP.*
2. Haga clic en el botón "Agregar acción de mensaje" y agregue las siguientes acciones de DLP. Asegúrese de confirmar el cambio después de enviar la acción del mensaje



Acción de mensaje

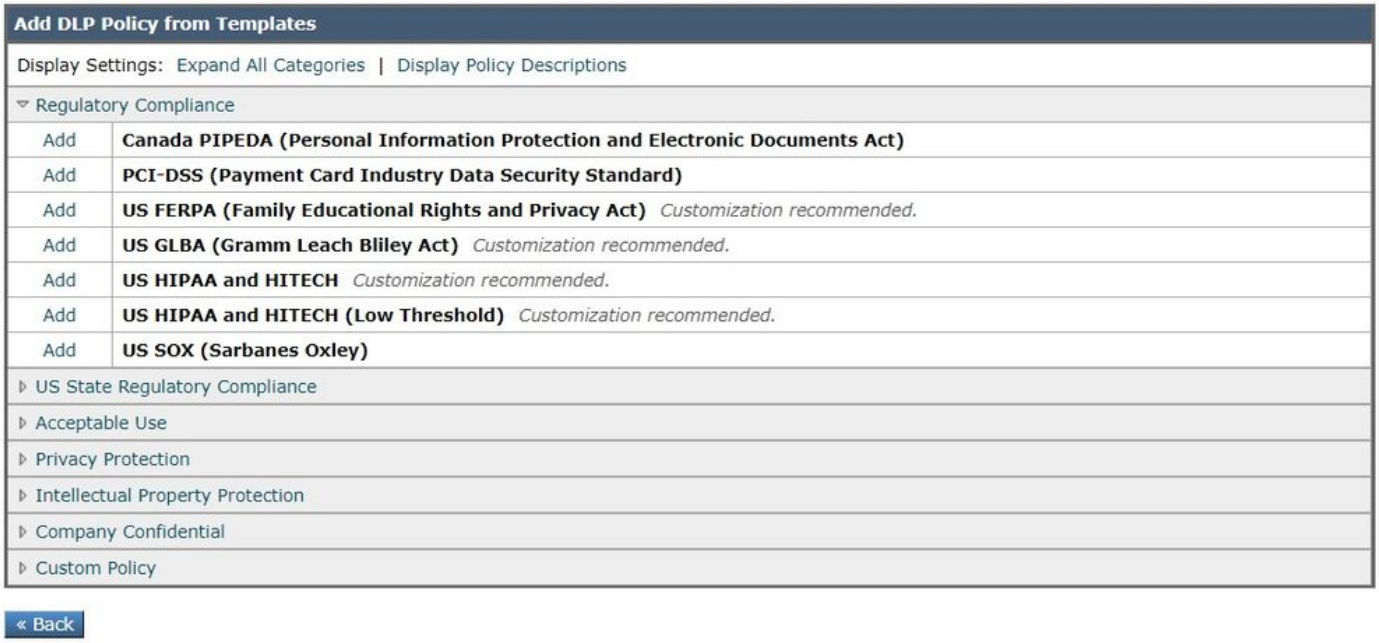
6. Creación de Políticas de Prevención de Pérdida de Datos

Una política de DLP incluye:

- Conjunto de condiciones que determinan si un mensaje saliente contiene datos confidenciales
- Las acciones que se deben realizar cuando un mensaje contiene dichos datos.

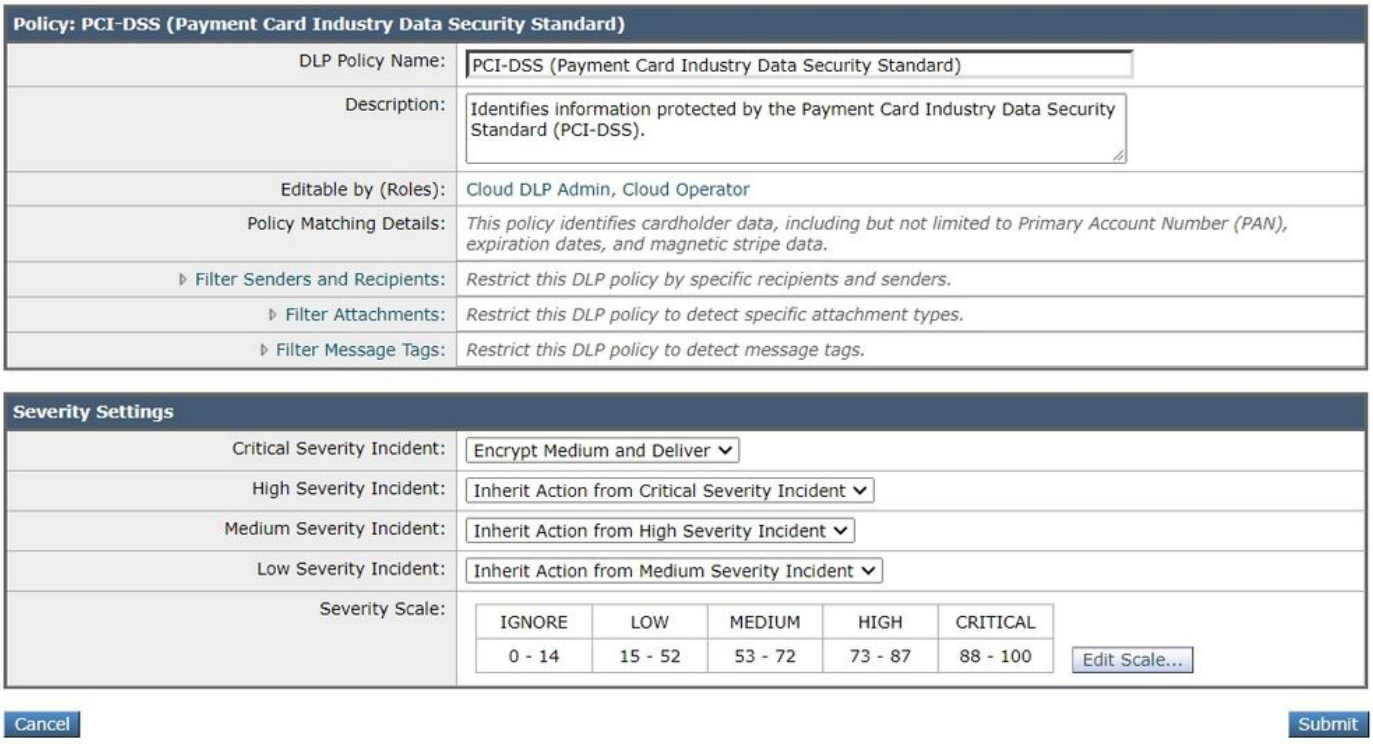
1. Vaya a: *Políticas de correo > Gestor de políticas DLP*

2. Haga clic en *'Agregar política DLP'*
3. Abra el triángulo de divulgación "Cumplimiento de Normas Regulatorias".



Plantilla de política DLP

4. Para la política PCI, haga clic en el botón "Agregar" situado a la izquierda de PCI-DSS.



Ejemplo de regla DLP de PCI-DSS

5. Para el incidente de gravedad crítica, seleccione la acción "Cifrar medio y entregar" que hemos configurado anteriormente. Podríamos cambiar los incidentes de menor gravedad pero por ahora, hagamos que hereden nuestro incidente de gravedad crítica. Envíe y confirme el cambio.

7. Aplicación de políticas DLP a una política de correo electrónico saliente

1. Vaya a: Políticas de correo > Políticas de correo saliente

2. Haga clic en la celda de control de DLP para la política predeterminada. Se leerá "Desactivado" si aún no lo ha habilitado.
3. Cambie el botón desplegable Desactivar DLP para activar DLP y se le presentará inmediatamente la política de DLP que acaba de crear.
4. Haga clic en la casilla de verificación "Habilitar todo". Envíe y, a continuación, confirme los cambios.

Conclusión

En resumen, hemos mostrado los pasos necesarios para preparar un dispositivo de seguridad Cisco Email Security Appliance para enviar un correo electrónico cifrado:

1. Habilitación de Cisco IronPort Email Encryption
2. Registre sus ESA y su organización con RES
3. Creación de perfiles de cifrado
4. Habilitación de DLP
5. Creación de acciones de mensaje DLP
6. Creación de políticas DLP
7. Aplicación de políticas DLP a una política de correo electrónico saliente

Encontrará más detalles en la Guía del usuario ESA correspondiente a su versión de software ESA. Las guías de usuario están disponibles en el siguiente enlace:

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems