Configuración de los Niveles de Seguridad en el Perfil de Cifrado ESA CRES

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Configuración desde la GUI](#)
[Configuración desde CLI](#)
[Verificación](#)
[Verificación desde la GUI](#)
[Verificación desde CLI](#)
[Troubleshoot](#)
[Errores más comunes:](#)
[Información Relacionada](#)

Introducción

Este documento describe la configuración de los perfiles Cisco Registered Envelope Service Encryption (CRES) dentro del dispositivo de seguridad Email Security Appliance (ESA) centrados en los diferentes niveles de seguridad permitidos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- configuración básica ESA
- Cifrado basado en la configuración del filtro de contenido
- Servicio de sobres registrados de Cisco

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

La creación del perfil CRES es una tarea central para la activación y el uso del servicio de cifrado a través del ESA. Antes de la creación de varios perfiles, asegúrese de haber completado la cuenta aprovisionada para un ESA con la creación de una cuenta CRES.

Puede haber más de un perfil y cada perfil se puede configurar con un nivel de seguridad diferente. Esto permite a la red mantener diferentes niveles de seguridad por dominio, usuario o grupo.

Configurar

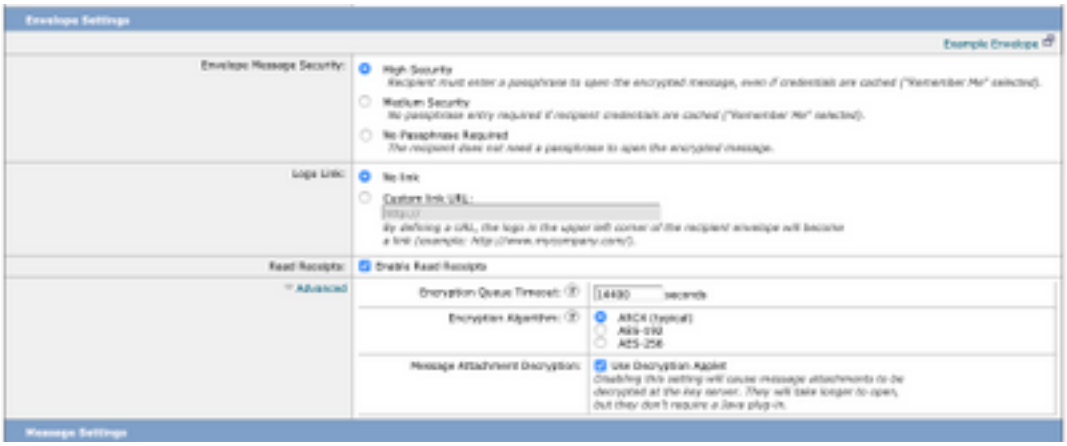
Puede habilitar y configurar un perfil de cifrado con el comando **encryptionconfig** CLI, o a través de **Servicios de Seguridad > Cisco IronPort Email Encryption** en la GUI.

Configuración desde la GUI

Desde ESA, vaya a **Servicios de seguridad > Cifrado de correo electrónico de Cisco IronPort > Agregar perfil de cifrado**.

Se muestra una pantalla con la configuración del perfil de cifrado. El nombre del perfil y el resto de la configuración se pueden personalizar y dependen de las etiquetas de identificación o de los métodos de la organización.

La configuración que define el nivel de seguridad por perfil es Envelope Settings (Configuración del sobre), como se muestra en la imagen:



Nota: Se sugiere que el nombre del perfil contenga: "Alto", "Bajo", etc, para coincidir con el nivel de seguridad configurado o el nombre del grupo con el que se asocia el perfil para una rápida identificación en la creación de filtros de contenido y verificación.

Los tres niveles de seguridad permitidos por la ESA son:

- Alta seguridad: El destinatario siempre debe introducir una frase de paso para abrir los mensajes cifrados.
- Seguridad media: El destinatario no necesita introducir credenciales para abrir el mensaje cifrado si las credenciales del destinatario están almacenadas en caché.

- No se requiere frase de paso: Este es el nivel más bajo de seguridad de mensajes cifrados. El destinatario no necesita introducir una frase de paso para abrir el mensaje cifrado. Todavía puede habilitar las funciones de confirmación de lectura, Respuesta segura para todos y Reenvío seguro de mensajes para los sobres que no estén protegidos con frase de paso.

Puede configurar los diferentes niveles de seguridad en estos objetos:

Sobra la Seguridad del Mensaje**:**

- Alta seguridad ·
- Seguridad media
- No se requiere frase de paso

Enlace del logotipo: Para que los usuarios puedan abrir la URL de su organización, haga clic en su logotipo, puede agregar un enlace al logotipo. Elija entre estas opciones:

- Sin link. No se agrega un enlace en directo al sobre del mensaje.
- URL de enlace personalizado. Introduzca la URL para agregar un enlace en directo al sobre del mensaje.

Leer recepciones: Si activa esta opción, el remitente recibirá una confirmación cuando los destinatarios abran el sobre seguro. Esta es una selección opcional.

Avanzado:

Tiempo de espera de la cola de cifrado: Introduzca el tiempo (en segundos) que un mensaje puede estar en la cola de cifrado antes de que se agote el tiempo de espera. Una vez que se agota el tiempo de espera de un mensaje, el dispositivo rebota el mensaje y envía una notificación al remitente.

Algoritmo de encripción:

- ARC4. ARC4 es la opción más común, proporciona un cifrado sólido con retrasos mínimos de descifrado para los destinatarios de mensajes.
- AES. AES proporciona un cifrado más fiable, pero también tarda más en descifrarse, ya que introduce retrasos para los destinatarios. AES se suele utilizar en aplicaciones gubernamentales y bancarias.

Descifrado del adjunto del mensaje*:* Active o desactive el applet de descifrado. Después de activar esta opción, hace que el archivo adjunto del mensaje se abra en el entorno del explorador. Después de inhabilitar esta opción, se descifran los archivos adjuntos de los mensajes en el servidor de claves. De forma predeterminada, Java Applet está desactivado en el sobre.

Nota: Los exploradores más usados han desactivado Java Applet por razones de seguridad.

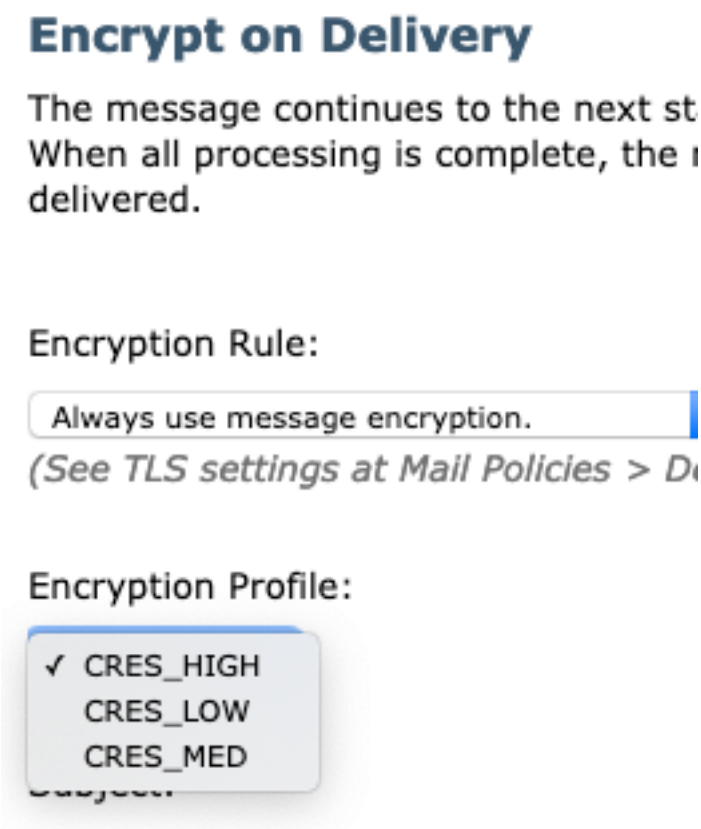
Una vez creados los perfiles de cifrado. Asegúrese de que esté aprovisionado, como se muestra en la imagen:

Cada uno de estos perfiles debe estar asociado a través de un filtro de contenido para poder ser aplicado.

Precaución: Si un filtro de contenido no llama al perfil, no se puede aplicar la configuración de cifrado.

Desde ESA, navegue hasta **Políticas de correo > Filtros de contenido saliente > Agregar un filtro**

Una vez configurada la condición de los usuarios, asunto, grupo, remitente, etc. dentro del filtro, defina el nivel de cifrado para el filtro saliente, como se muestra en la imagen:



Precaución: Todos los filtros de contenido deben estar asociados con las políticas de correo saliente para funcionar correctamente.

Nota: Puede configurar varios perfiles de cifrado para un servicio de clave alojada. Si su organización tiene varias marcas, esto le permite hacer referencia a diferentes logotipos almacenados en el servidor de claves para los sobres PXE.

Configuración desde CLI

Desde el comando ESA CLI type **encryptionconfig**:

```
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]>
```

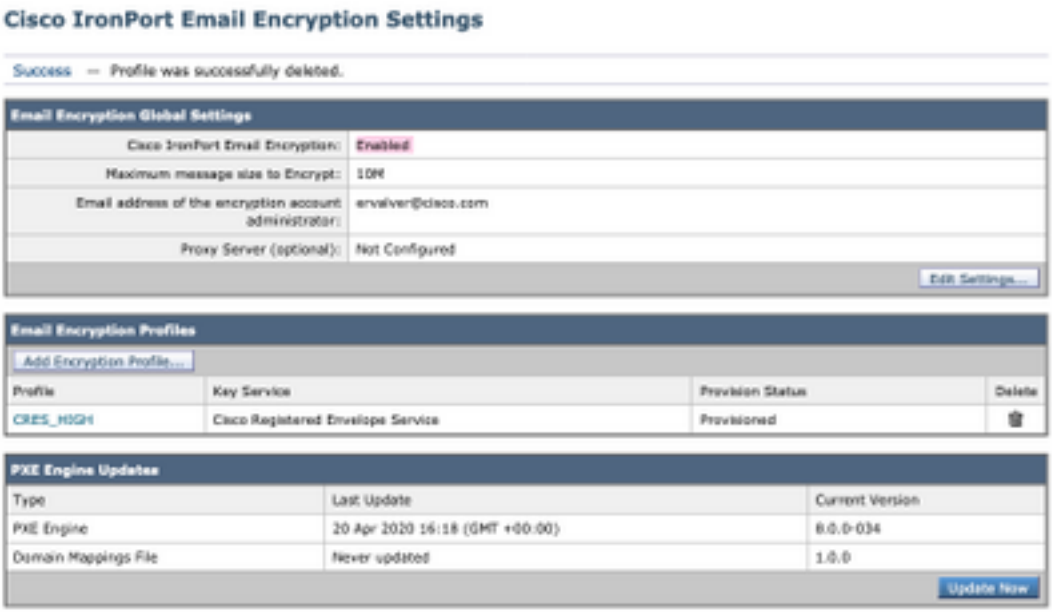
```
Enter the subject to use for failure notifications:
[[ENCRYPTION FAILURE]]>

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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Verificación desde la GUI

Desde ESA vaya a **Servicios de seguridad > Cifrado de correo electrónico de Cisco IronPort**, como se muestra en la imagen:



Nota: Asegúrese de que el cifrado esté habilitado y que el perfil configurado esté

aprovisionado. Como se muestra en la imagen.

Verificación desde CLI

Desde el comando CLI type **encryptconfig** y type profiles.

```
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
```

Nota: Asegúrese de que el cifrado esté habilitado y que el perfil configurado esté aprovisionado. Como se muestra en la imagen.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Desde ESA, vaya a **Administración del sistema > teclas de función**

Verifique que la clave de característica esté aplicada y activa. La clave: El cifrado de correo electrónico de IronPort debe estar activo.

Desde ESA vaya a **Servicios de seguridad > Cifrado de correo electrónico de Cisco IronPort**

Verifique que el servicio de cifrado esté habilitado correctamente.

Verifique que el perfil de cifrado no esté en estado No aprovisionado, como se muestra en la imagen:

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**

Verifique la última actualización del motor, como se muestra en la imagen:

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

En los detalles de Rastreo de mensajes, verifique si se muestra un error.

Errores más comunes:

`5.x.3 - Temporary PXE Encryption failure`
Solución: El servicio actualmente no está disponible o es inalcanzable. Verifique la conectividad y los problemas de red.

`5.x.3 - PXE Encryption failure. (Message could not be encrypted due to a system configuration issue. Please contact your administrator`
Solución: Este error está asociado con:

- Problemas de licencia. Verifique las claves de característica
- El perfil utilizado no está aprovisionado. Identifique desde el mensaje que rastrea el perfil configurado en el filtro de contenido y el aprovisionamiento
- No hay ningún perfil asociado a un filtro de contenido. A veces se eliminan los perfiles de cifrado, se modifican con nombres diferentes, etc. Y el filtro de contenido configurado no puede encontrar el perfil asociado

`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.)`
Solución: Regularmente, este problema es causado por el relleno automático de la dirección de correo electrónico del cliente de correo electrónico interno (por ejemplo, Outlook) del destinatario que contiene una dirección de correo electrónico "De"/"A" no válida.

Normalmente, esto se debe a las comillas que rodean la dirección de correo electrónico u otros caracteres ilegales en la dirección de correo electrónico.

Información Relacionada

- Guía de administración de CRES
- Guía del usuario final
- Soporte Técnico y Documentación - Cisco Systems