

Exemplo da configuração de criptografia do email ESA

Índice

[Introdução](#)

[Pré-requisitos](#)

[Configurar](#)

[Permita a criptografia do email no ESA](#)

[Crie um filtro satisfeito que parte](#)

[Verificar](#)

[Valide o filtro da criptografia que processa no Mail logs](#)

[Troubleshooting](#)

Introdução

Este documento descreve como estabelecer a criptografia do email na ferramenta de segurança do email (ESA).

Pré-requisitos

As informações neste documento são baseadas nestas versões de software e hardware:

- Modelo: Toda a série C e X-séries
- Característica da criptografia do envelope (PostX) instalada

Configurar

Permita a criptografia do email no ESA

Termine estas etapas do GUI:

1. Sob Serviços de segurança, escolha a **criptografia do email de Cisco IronPort > permitem a criptografia do email**, e o clique **edita ajustes**.
2. O clique **adiciona o perfil da criptografia** a fim criar um perfil novo da criptografia.
3. Escolha o **serviço registrado Cisco do envelope** ou o **dispositivo da criptografia de Cisco IronPort** (se o dispositivo da criptografia é comprado) para o tipo de serviço chave.

4. O clique **submete e compromete mudanças**.
5. Depois que o perfil da criptografia foi criado, você está dado a opção para provision o ao server registrado do serviço do envelope de Cisco (CRE). Um botão da disposição deve indicar ao lado do perfil novo. **Disposição do clique**.

Crie um filtro satisfeito que parte

Termine estas etapas do GUI a fim criar um filtro satisfeito que parte para executar o perfil da criptografia. No exemplo seguinte, o filtro provocará a criptografia para todo o mensagem enviada com a corda "fixa-se: " no encabeçamento sujeito:

1. Sob políticas do correio, escolha os filtros satisfeitos que parte, e o clique **adiciona o filtro**.
2. Adicionar um filtro novo com condição do encabeçamento sujeito como o == sujeito "fixam-se: " e a ação Encrypt e entrega agora (ação final). Clique em Submit.
3. Sob políticas do correio, escolha as políticas que parte do correio, e permita este filtro novo na política do correio do padrão ou nas políticas apropriadas do correio.
4. Comprometa mudanças.

Verificar

Esta seção descreve como verificar que a criptografia trabalha.

1. A fim verificar, gerencia um correio novo com **seguro**: no assunto e envie o email a uma conta da Web (Hotmail, Yahoo, Gmail) a fim determinar se é cifrada.
2. Verifique os logs do correio como descrito na próxima seção a fim assegurar-se de que a mensagem esteja cifrada através do filtro satisfeito que parte.

Valide o filtro da criptografia que processa no Mail_logs

Estas entradas do mail_log mostram que as mensagens combinaram o filtro da criptografia chamado Encrypt_Message.

```
Wed Oct 22 17:06:46 2008 Info: MID 116 was generated based on MID 115 by encrypt filter 'Encrypt_Message'  
Wed Oct 22 17:07:22 2008 Info: MID 118 was generated based on MID 117 by encrypt filter 'Encrypt_Message'  
Wed Oct 22 17:31:21 2008 Info: MID 120 was generated based on MID 119 by encrypt filter ''Encrypt_Message'
```

Refira a [determinação da disposição da mensagem ESA](#) para a instrução em como usar o **grep** ou os comandos **findevent** a fim recolher a informação dos logs segundo as indicações desta seção.

Troubleshooting

Se o filtro da criptografia não provoca, verifique os logs do correio para ver se há a política que do correio o mensagem de teste se usa. Certifique-se que o filtro está permitido nesta política do correio, e igualmente aquele lá não é nenhum filtro precedente permitido nesta política com uma **ação restante dos filtros do índice da faixa clara**.

Assegure-se de que as mensagens no rastreamento de mensagem usem a corda correta ou o assunto designado que etiquetam a fim provocar a criptografia através do filtro satisfeito.