Configurazione dei livelli di sicurezza nel profilo di crittografia CRES ESA

Sommario

Introduzione

Questo documento descrive la configurazione dei profili Cisco Registered Envelope Service Encryption (CRES) in Email Security Appliance (ESA) per i diversi livelli di sicurezza consentiti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di base ESA
- Crittografia basata sulla configurazione del filtro contenuti
- Cisco Registered Envelope Service

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La creazione del profilo CRES è un compito fondamentale per l'attivazione e l'uso del servizio di cifratura tramite l'ESA. Prima di creare più profili, accertarsi di disporre di un conto completo predisposto per un'ESA con la creazione di un conto CRES.

Èpossibile configurare più di un profilo e ogni profilo può essere configurato con un livello di protezione diverso. Ciò consente alla rete di mantenere diversi livelli di protezione per dominio, utente o gruppo.

Configurazione

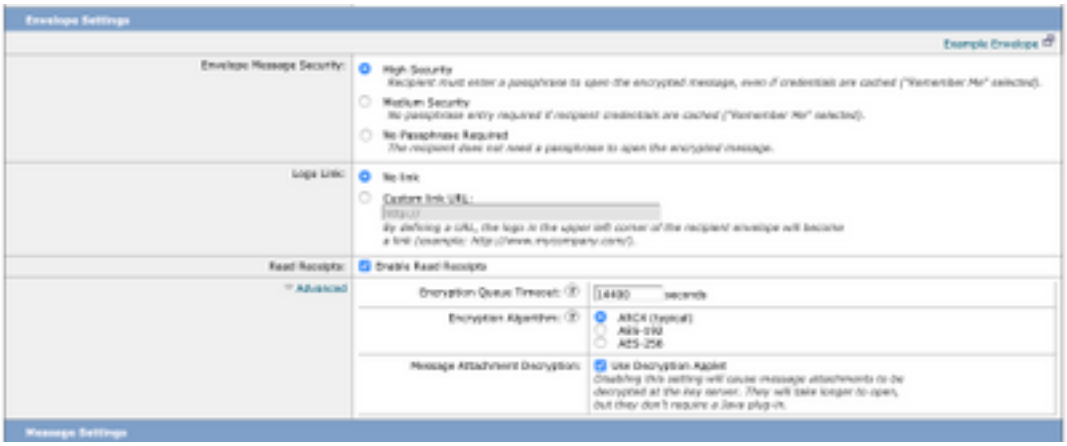
Èpossibile abilitare e configurare un profilo di crittografia con il comando **encryptionconfig** CLI o tramite **Security Services > Cisco IronPort Email Encryption** nella GUI.

Configurazione dalla GUI

Da ESA selezionare **Security Services > Cisco IronPort Email Encryption >** Add Encryption Profile (Servizi di sicurezza **>** Cisco IronPort Email Encryption **> Aggiungi profilo di crittografia)**.

Viene visualizzata una schermata con le impostazioni del profilo di crittografia. Il nome del profilo e il resto della configurazione possono essere personalizzati e dipendono dai tag di identificazione o dai metodi dell'organizzazione.

La configurazione che definisce il livello di protezione per profilo è Impostazioni involucro, come mostrato nell'immagine:



> **Nota:** Il nome del profilo dovrebbe contenere: "Alta", "Bassa", ecc., per corrispondere al livello di sicurezza configurato o al nome del gruppo a cui è associato il profilo, per una rapida identificazione nella creazione dei filtri contenuti e verifica.

I tre livelli di sicurezza consentiti dall'ESA sono:

- Sicurezza elevata: Il destinatario deve sempre immettere una passphrase per aprire i messaggi crittografati.
- Sicurezza media: Il destinatario non deve immettere credenziali per aprire il messaggio crittografato se le credenziali del destinatario sono memorizzate nella cache.

- Nessuna passphrase richiesta: Si tratta del livello più basso di protezione dei messaggi crittografati. Il destinatario non deve inserire una passphrase per aprire il messaggio crittografato. È comunque possibile attivare le funzionalità di conferma di lettura, Rispondi a tutti e Inoltro messaggi protetto per le buste non protette da passphrase.

Èpossibile configurare il diverso livello di protezione per questi oggetti:

Sicurezza messaggi buste**:**

- ·Elevata sicurezza
- Sicurezza media
- Nessuna passphrase richiesta

Collegamento logo: Per consentire agli utenti di aprire l'URL dell'organizzazione, fare clic sul logo, è possibile aggiungere un collegamento al logo. Selezionare una delle opzioni seguenti:

- Nessun collegamento. Nessun collegamento dinamico aggiunto alla busta del messaggio.
- URL collegamento personalizzato. Immettere l'URL per aggiungere un collegamento dinamico alla busta del messaggio.

Conferme di lettura: Se si abilita questa opzione, il mittente riceverà una conferma quando i destinatari apriranno la busta protetta. Questa è una selezione facoltativa.

Avanzate:

Timeout coda di crittografia: Immettere il periodo di tempo (in secondi) durante il quale un messaggio può trovarsi nella coda di crittografia prima del timeout. Quando si verifica il timeout di un messaggio, l'accessorio lo rifiuta e invia una notifica al mittente.

Algoritmo di crittografia*:*

- ARC4. ARC4 è la scelta più comune e fornisce una crittografia efficace con ritardi di decrittografia minimi per i destinatari dei messaggi.
- AES. AES offre una crittografia più avanzata ma richiede più tempo per la decrittografia; inoltre, comporta dei ritardi per i destinatari. L'AES è generalmente utilizzato nelle applicazioni governative e bancarie.

Decrittografia allegati messaggio*:* Attivare o disattivare l'applet di decrittografia. Se si attiva questa opzione, l'allegato del messaggio verrà aperto nell'ambiente del browser. Se si disattiva questa opzione, gli allegati dei messaggi verranno decrittografati nel server delle chiavi. Per impostazione predefinita, l'applet Java è disabilitata nella busta.

> **Nota:** Per motivi di sicurezza, i browser più utilizzati hanno disabilitato l'applet Java.

Una volta creati i profili di crittografia. Assicurarsi che sia stato eseguito il provisioning, come mostrato nell'immagine:

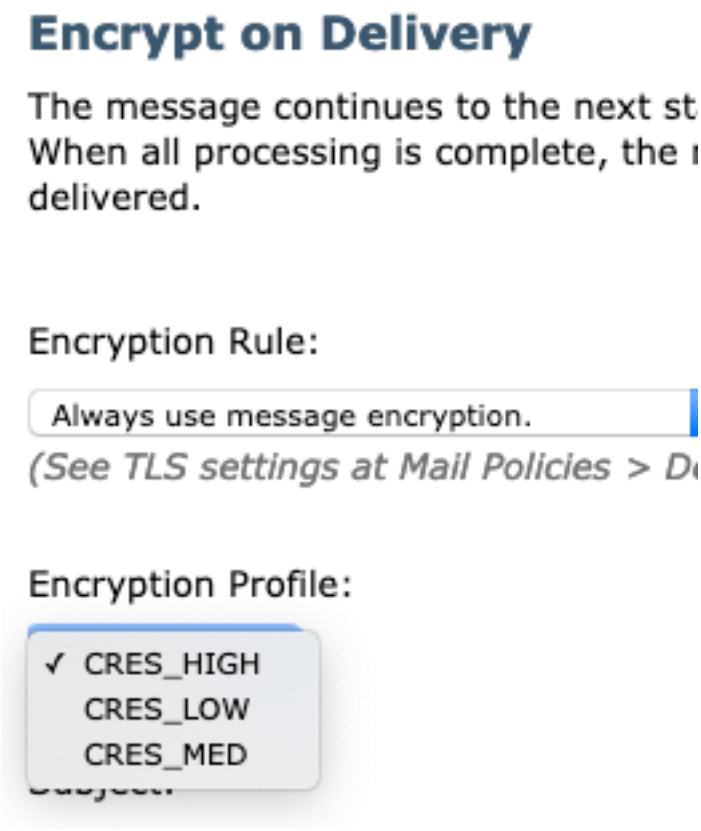
Per essere applicati, questi profili devono essere associati tramite un filtro contenuti.

> **Attenzione:** Se il profilo non viene chiamato da un filtro contenuti, le impostazioni di

crittografia non possono essere applicate.

Da ESA, selezionare **Mail Policies > Outgoing Content Filters >** Add a filter (Policy di posta **>** Filtri contenuti in uscita **> Aggiungi filtro)**

Una volta configurata la condizione di utenti, oggetto, gruppo, mittente e così via all'interno del filtro, definire il livello di crittografia per il filtro in uscita, come mostrato nell'immagine:



Attenzione: Per funzionare correttamente, tutti i filtri contenuti devono essere associati ai criteri di posta in uscita.

Nota: È possibile configurare più profili di crittografia per un servizio con chiave ospitata. Se l'organizzazione dispone di più marchi, è possibile fare riferimento a diversi logo memorizzati sul server principale per le buste PXE.

Configurazione dalla CLI

Dal 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:
```

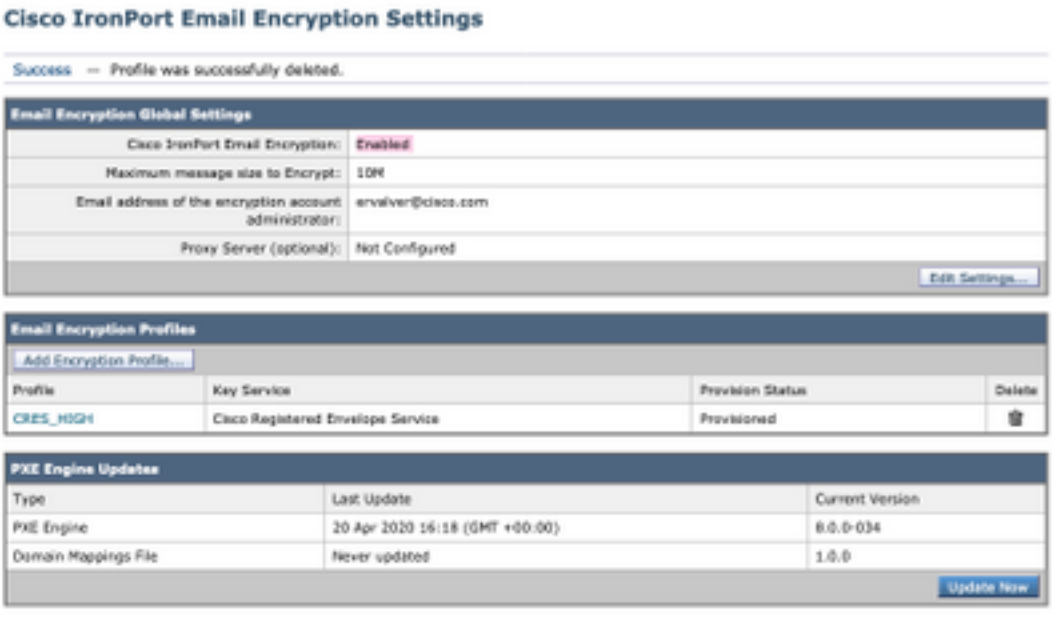
```
[[ENCRYPTION FAILURE]]>

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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Verifica dalla GUI

Da ESA passare a **Security Services > Cisco IronPort Email Encryption**, come mostrato nell'immagine:



Nota: Verificare che la crittografia sia abilitata e che sia stato eseguito il provisioning del profilo configurato. Come mostrato nell'immagine.

Verifica dalla CLI

Dalla CLI, digitare **encryptconfig** e il comando 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:** Verificare che la crittografia sia abilitata e che sia stato eseguito il provisioning del profilo configurato. Come mostrato nell'immagine.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Da ESA passare a **Amministrazione sistema > tasti funzione**

Verificate che la chiave di feature sia applicata e attiva. La chiave: IronPort Email Encryption deve essere attivo.

Da ESA passare a **Security Services > Cisco IronPort Email Encryption**

Verificare che il servizio di crittografia sia abilitato correttamente.

Verificare che lo stato del profilo di crittografia non sia Nessun provisioning, come mostrato nell'immagine:

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**

Verificare l'ultimo aggiornamento del motore, come mostrato nell'immagine:

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

In Dettagli verifica messaggi verificare se è visualizzato un errore.

Errori più comuni:

`5.x.3 - Temporary PXE Encryption failure`
Soluzione*:* Servizio attualmente non disponibile o non raggiungibile. Verificare i problemi di connettività e di rete.

`5.x.3 - PXE Encryption failure. (Message could not be encrypted due to a system configuration issue. Please contact your administrator`
Soluzione: Questo errore è associato a:

- Problemi di licenza. Verificare i tasti funzione
- Il provisioning del profilo utilizzato non è stato eseguito. Identificare dal messaggio il profilo configurato sul filtro contenuti e il provisioning
- Nessun profilo associato a un filtro contenuti. Talvolta i profili di crittografia vengono eliminati, modificati con nomi diversi, ecc. Il filtro contenuti configurato non è in grado di trovare il profilo associato

`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.)`
Soluzione: Il problema è causato regolarmente dal riempimento automatico dell'indirizzo di posta elettronica del destinatario da parte del client di posta elettronica del mittente interno (ad esempio, Outlook) che contiene un indirizzo "Da"/"A" non valido.

In genere, ciò è causato dalle virgolette che racchiudono l'indirizzo e-mail o da altri caratteri non validi nell'indirizzo.

Informazioni correlate

- Guida per l'amministratore di CRES
- Guida per l'utente finale
- Documentazione e supporto tecnico – Cisco Systems