Configure Security Levels in the ESA CRES Encryption Profile

Contents

Introduction

This document describes the configuration of the Cisco Registered Envelope Service Encryption (CRES) profiles within the Email Security Appliance (ESA) focused on the different security levels allowed.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ESA basic configuration
- Encryption based on the content filter configuration
- Cisco Registered Envelope Service

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The creation of the CRES profile is a core task for the activation and use of the encryption service through the ESA. Before multiple profiles creation ensure that you have complete account provisioned for an ESA with the creation of a CRES account.

There can be more than one profile and each profile can be configured with a different security level. This allows the network to maintain different levels of security by domain, user, or group.

Configure

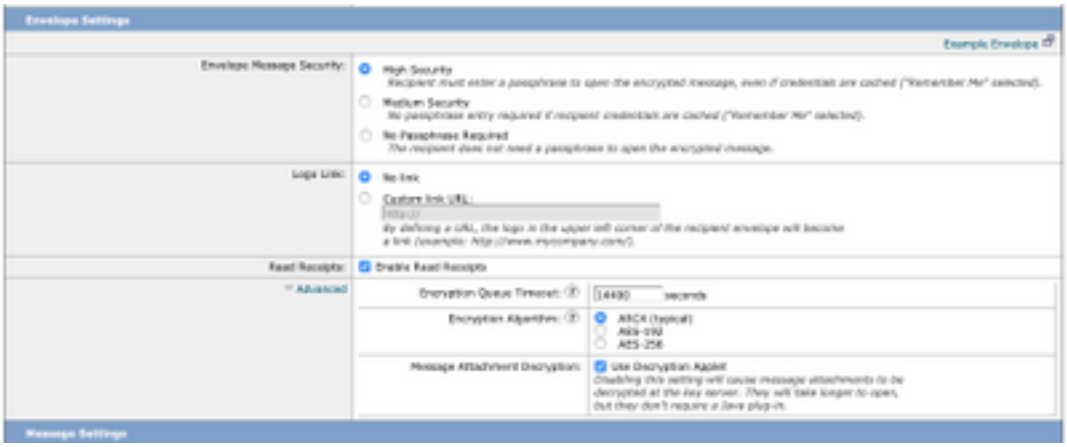
You can enable and configure an encryption profile with the **encryptionconfig** CLI command, or via **Security Services > Cisco IronPort Email Encryption** in the GUI.

Configuration from GUI

From ESA navigate to **Security Services > Cisco IronPort Email Encryption > Add Encryption Profile**.

A screen with the Encryption Profile Settings is displayed. The profile name and the rest of the configuration can be customized and depends on identification tags or methods of the organization.

The configuration that defines security level per profile is Envelope Settings, as shown in the image:



> **Note**: It is suggested that the profile name contains: "High", "Low", etc, in order to match the configured security level or the name of the group with which the profile is associated with for quick identification in the creation of content filters and verification.

The three levels of security allowed by the ESA are:

- High Securit: The recipient must always enter a passphrase in order to open encrypted messages.
- Medium Security: The recipient does not need to enter credentials to open the encrypted message if the recipient credentials are cached.
- No Passphrase Required: This is the lowest level of encrypted message security. The

recipient does not need to enter a passphrase to open the encrypted message. You can still enable the read receipts, Secure Reply All, and Secure Message Forwarding features for envelopes that are not passphrase-protected.

You can configure the different level of security on these objects:

Envelopes Message Security**:**

- ·High Security
- Medium Security
- No Passphrase Required

Logo Link: In order to enable users to open your organization's URL, click its logo, you can add a link to the logo. Choose from these options:

- No link. A live link is not added to the message envelope.
- Custom link URL. Enter the URL to add a live link to the message envelope.

Read Receipts: If you enable this option, the sender receives a receipt when recipients open the secure envelope. This is an optional selection.

Advanced:

Encryption Queue Timeout: Enter the length of time (in seconds) that a message can be in the encryption queue before it times out. Once a message times out, the appliance bounces the message and sends a notification to the sender.

Encryption Algorithm*:*

- ARC4. ARC4 is the most common choice, it provides strong encryption with minimal decryption delays for message recipients.
- AES. AES provides stronger encryption but also takes longer to decrypt, it introduces delays for recipients. AES is typically used in government and bank applications.

Message Attachment Decryption*:* Enable or disable the decryption applet. After you enable this option, it causes the message attachment to be opened in the browser environment. After you disable this option, it causes message attachments to be decrypted at the key server. By default, Java Applet is disabled in the envelope.

> **Note**: The most used browsers have disabled Java Applet because of security reasons.

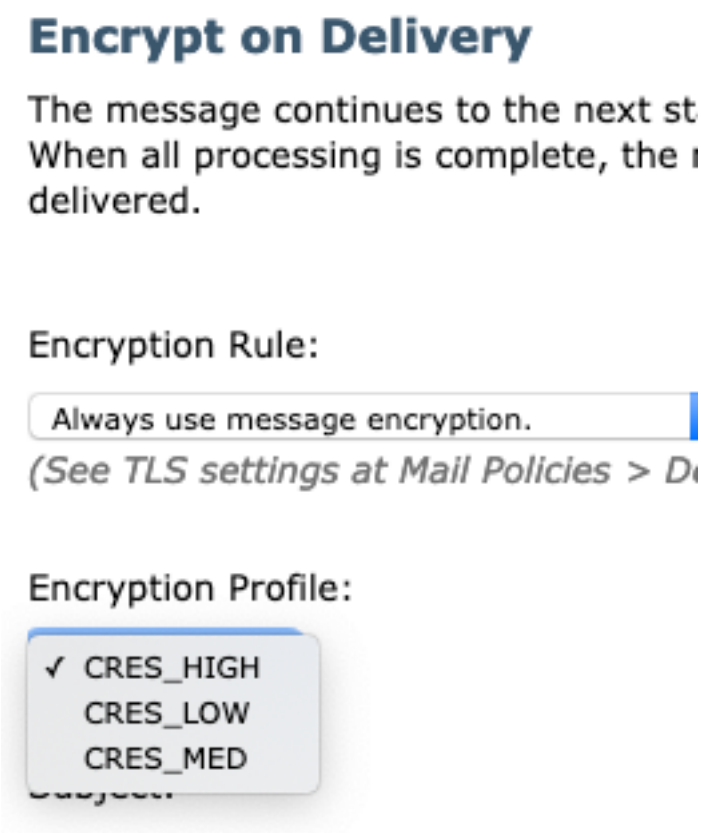
Once the encryption profiles have been created. Ensure it is provisioned, as shown in the image:

Each of these profiles must be associated through a content filter in order to be applied.

> **Caution**: If the profile is not called by a content filter, the encryption settings cannot be applied.

From ESA, navigate to **Mail Policies > Outgoing Content Filters > Add a filter**

Once the condition of users, subject, group, sender, etc. has been configured inside the filter, define the encryption level for the outgoing filter, as shown in the image:



Caution: All content filters must be associated with outgoing mail policies in order to function properly.

Note: You can configure multiple encryption profiles for a hosted key service. If your organization has multiple brands, this allows you to reference different logos stored on the key server for the PXE envelopes.

Configuration from CLI

From ESA CLI type **encryptionconfig** command:

```
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]>
```

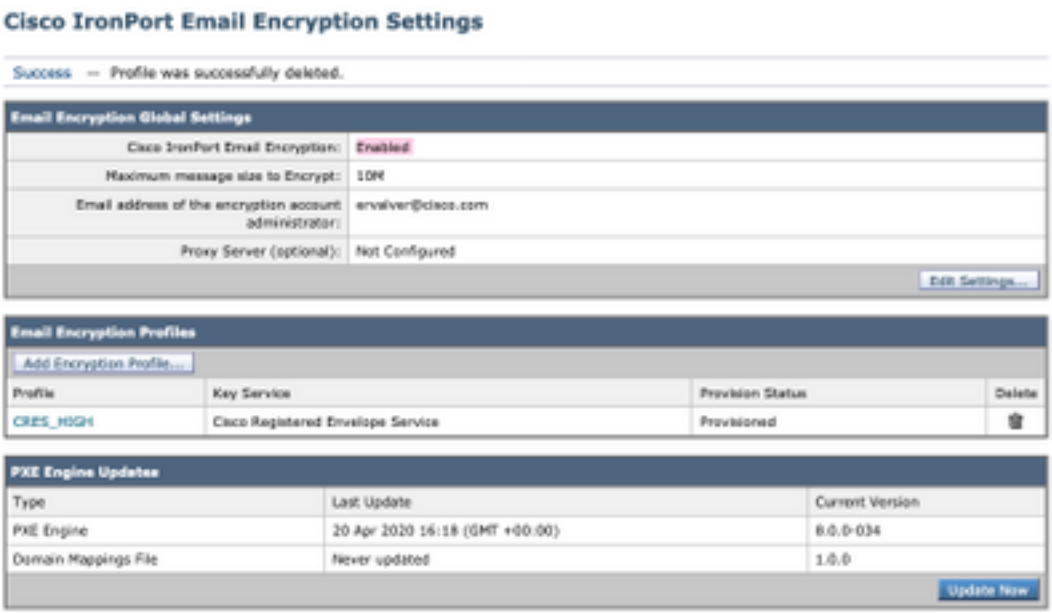
```
A Cisco Registered Envelope Service profile "HIGH" was added.

   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
```

Verify

Use this section to confirm that your configuration works properly.

Verification from GUI

From ESA navigate to **Security Services > Cisco IronPort Email Encryption**, as shown in the image:



> **Note**: Ensure that the encryption is enabled and the profile configured is provisioned. As shown in the image.

Verification from CLI

From CLI type **encryptconfig** and type profiles command.

```
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
```

> **Note**: Ensure that the encryption is enabled and the profile configured is provisioned. As shown in the image.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

From ESA navigate to **System Administration > feature keys**

Verify the feature key is applied and active. The key: IronPort Email Encryption must be active.

From ESA navigate to **Security Services > Cisco IronPort Email Encryption**

Verify that the encryption service is properly enabled.

Verify that the encryption profile is not in a Not Provisioned status, as shown in the image:

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**

Verify engine last update, as shown in the image:

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

From Message Tracking details, verify if an error is displayed.

Most common errors:

`5.x.3 - Temporary PXE Encryption failure`

Solution: The service is currently unavailable or unreachable. Verify connectivity and network issues.

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

Solution: This error is associated with:

- License issues. Please verify feature keys
- The profile used is not provisioned. Identify from message tracking the profile configured on content filter and provision
- There is no profile associated with a content filter. Sometimes the encryption profiles are deleted, modified with different names, etc. And the content filter configured is not able to find the profile associated

`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.)`

Solution: Regularly, this issue is caused by the internal sender's email client's (e.g. Outlook) autofill of the recipient's email address which contains an invalid “From”/"To" address.

Typically, this is caused by quotation marks around the email address or other illegal characters in the email address.

Related Information

- **CRES Admin Guide**
- **End User Guide**
- **Technical Support & Documentation - Cisco Systems**