CISCO EMAIL SECURITY APPLIANCE

BEST PRACTICES:

CRES MESSAGE ENCRYPTION

September 2015
Version 1.0

Aaron Kuehn
Cisco Sales Engineer

The most current version of this document can be found here:
https://cisco.com/go/emailsecurity-customer

A. INTRODUCTION

This document discusses the setup of message encryption using the Cisco Email Security Appliance (ESA) and the cloud-based Cisco Registered Envelope Service (CRES). Customers can use message encryption to send individual messages securely over the public Internet, using various types of policy including content filtering and Data Loss Prevention (DLP). The creation of these policies will be discussed in other documents within this series. This document focuses on getting the ESA prepared to send encrypted mail, so that policies can use encryption as an action.

This document will discuss the following steps:

1. **Enabling Cisco IronPort Email Encryption**
2. **Registering the ESA appliance(s) with CRES**
3. **Creating Encryption Profiles**

Once these steps are completed successfully, the ESA administrator can successfully create policy that will use encryption as an action.

Cisco IronPort Email Encryption is also referred to as CRES Encryption. CRES (Cisco Registered Envelope Service) is the name that we use for the "Key Servers" in the Cisco Cloud. The CRES encryption solution uses symmetric key encryption — which means the key used to encrypt the message is the same key used to decrypt the message. Every encrypted message uses a unique key, which allows the sender to have granular control over a message after it is sent – for example, to lock or expire it so the recipient can no longer open it – without affecting any other messages. When encrypting a message, the ESA stores the encryption key and metadata in CRES about each encrypted message.

The ESA can decide to encrypt a message in many ways — via "flag" (like Subject content), via Content Filter matching, or via DLP Policy, for example. Once the ESA decides to encrypt a message, it does so with a specified "Encryption Profile" created in "Security Services > Cisco IronPort Email Encryption" — the table named "Email Encryption Profiles". By default, there are no Encryption Profiles. This will be discussed in Step #3.

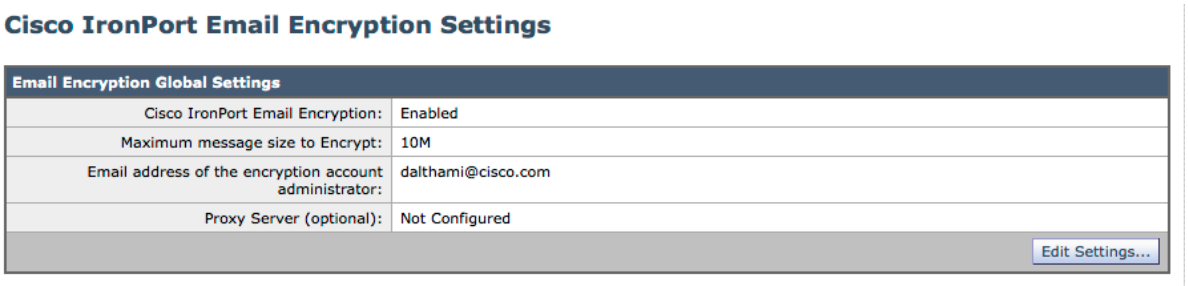
1. **Enable Cisco IronPort Email Encryption on the ESA(s)**

   Security Services > Cisco IronPort Email Encryption

   If you have multiple ESAs in a cluster, then Step #1 step should only need to be performed once, since these settings are typically managed at the cluster level. If you have multiple machines that are not clustered, or if you are managing these settings at the machine level, then Step #1 should be performed on each ESA. In the *Security Services > Cisco IronPort Email Encryption* menu, click 'Edit Settings'.

   - Check the box to enable Cisco IronPort Email Encryption.
   - Specify the Email Address for the person who is going to be the primary CRES Admin for the customer's account. This email account will be associated with administration of the CRES environment for the company.
   - If you have a proxy that the ESA will need to go through to connect to CRES via HTTPS, add the necessary proxy and authentication settings for allowing it to go through the proxy

   At this point you should see the "Email Encryption Global Settings" set to something like this:



   Be sure to submit and commit your changes.

2. Register the ESA Appliances and the organization with CRES

Step #2 primarily takes part outside of the ESA administration console.

First, send an email either to their Cisco Web and Email Security team, or to the Cisco partner assisting with the deployment, or for even faster turnaround, directly to CRES at stg-cres-provisioning@cisco.com. The email should contain the following information:

- Company Name
- CRES Admin Name and Email (as added in the ESA when enabling encryption, above)
- List of ESA S/Ns. In the case of virtual appliances, also please include the VLN. This can be found in the CLI using the 'showlicense' command.
- Indicate whether an existing CRES Company account exists for this customer.

Note: After you have emailed this detail, it may take a day for your Company CRES account to be created (if it was not already created) and the S/Ns to be added. The "Provision" task, in Step #3, will not work until this is completed.

3. Create Encryption Profiles on the ESA(s)

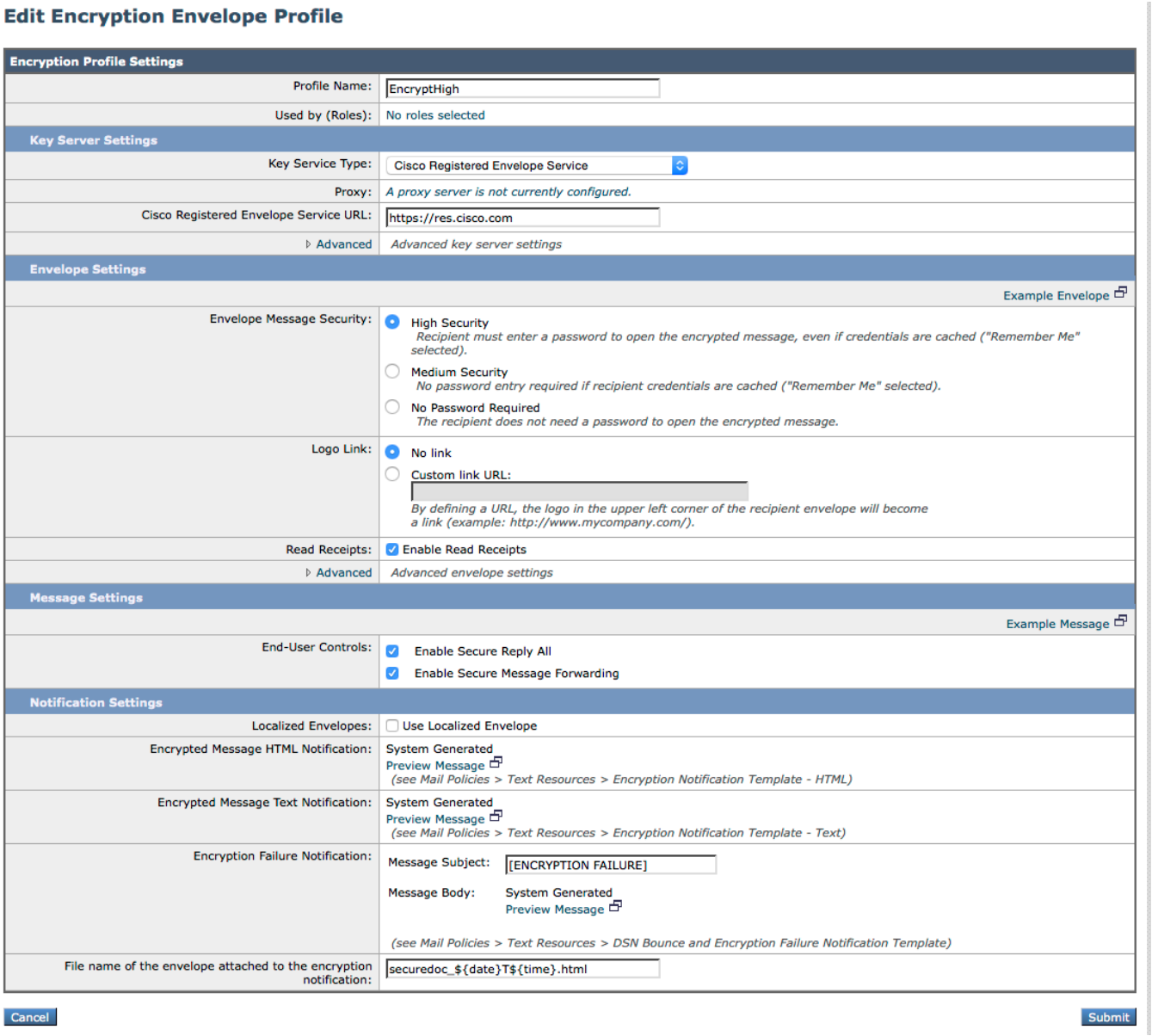
If you have multiple ESAs in a cluster, then Step #1 step should only need to be performed once, since these settings are typically managed at the cluster level. If you have multiple machines that are not clustered, or if you are managing these settings at the machine level, then Step #1 should be performed on each ESA.

Encryption Profiles specify how encrypted messages should be sent. For example, an organization may need to send High Security envelopes for one segment of their recipients, such as those that they know they will frequently be sending highly sensitive data to. The same organization may have other segments of their recipient community who receive less sensitive information, and who are also perhaps less patient with having to provide userid and password to receive encrypted mail. Those recipients would be good candidates for a Low Security type of envelope. Having multiple encryption profiles allows the organization to tailor the encrypted message format to the audience. On the other hand, many organizations may be fine with just one Encryption Profile.

For this document, we will show an example of creating three Encryption Profiles named "EncryptHigh", "EncryptMedium", and "EncryptLow". In the *Security Services > Cisco IronPort Email Encryption* menu, click the button to "Add Encryption Profile". The

Encryption Profile menu will open, and you can name your first encryption profile "EncryptHigh".

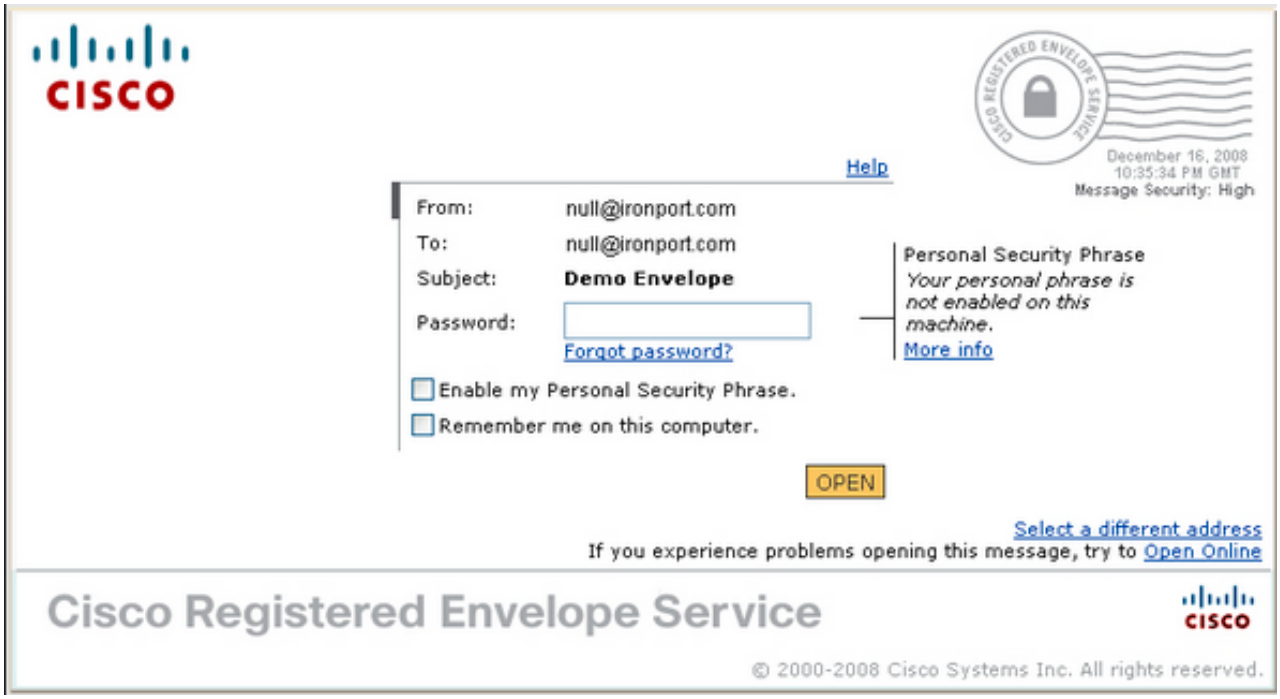
In the *Security Services* > *Cisco IronPort Email Encryption* menu, click 'Add Encryption Profile'. Below is a screenshot providing an example encryption profile — in this case it is for "Encrypt High". Use this same example to create all three profiles — just change the radio button for each profile.



- For the Encrypt High profile, choose the “High Security” radio button.
- For the Encrypt Medium profile, choose the “Medium Security” radio button.
- For the Encrypt Low profile, choose the “No Password Required” radio button

You will notice there are options to Enable Read Receipts, Enable Secure Reply All, and Enable Secure Message Forwarding. If you click on the envelope settings “Advanced” link under Read Receipts, you can select one of three symmetric encryption algorithms, as well as specify that the envelope be sent without the Java encryption applet.

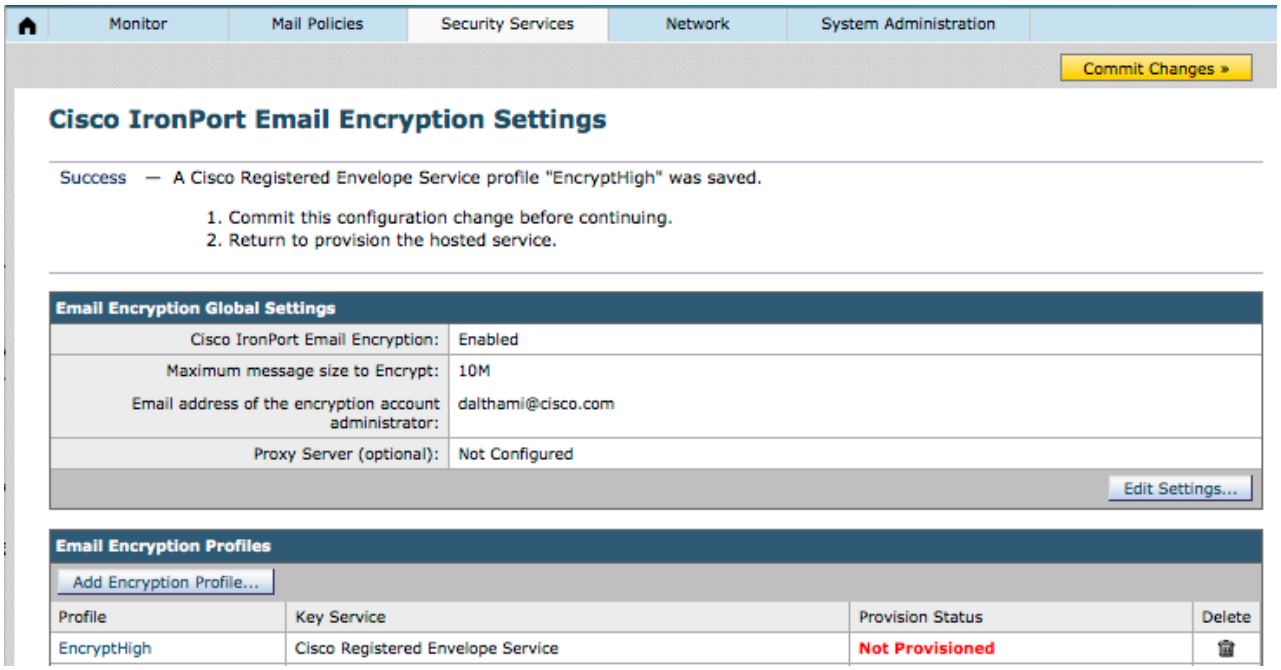
To the right of Envelope Settings, you will see “Example Message” hypertext link which, if clicked, will show you an example of the Secure Message Envelope — what the recipient will see in their email after they open the HTML attachment.



Read Receipts means that the Sender of the encrypted message will receive an email from CRES when the Recipient opens the Secure Message (meaning the recipient pulled down the symmetric key and decrypted the message).

To the right of the Message Settings you will see Example Message hypertext link that will show you what the opened message will look like with and without Enable Secure Reply All and Enable Secure Message Forwarding checked. This is an example of what the recipient will see once they have provided the necessary information in the envelope, and have opened the encrypted message.

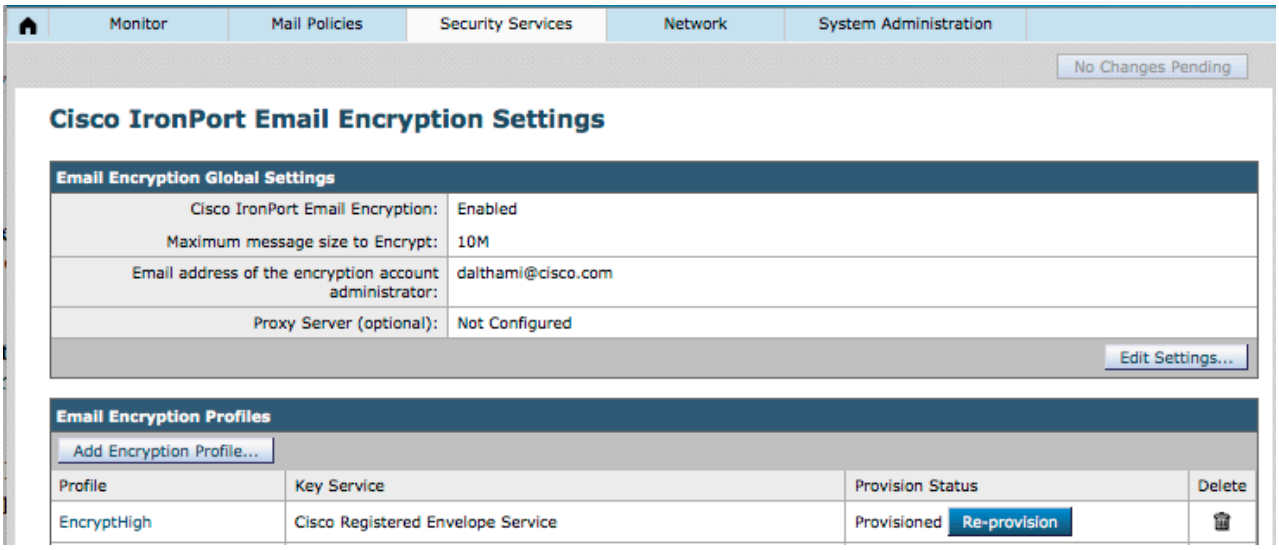
After you submit and commit the Encryption Profile, you will see the profile in the Cisco IronPort Email Encryption menu, similar to the below.



Submit and commit changes. The row in the table will then show a "Provision" button. The Provision button will not appear until after you Commit changes.

Click the Provision button Again, this will only work after your company CRES account has been created and the appliance S/Ns have been added to your account. If the CRES account is linked to the ESA, the provisioning process will happen relatively quickly. If it is not, that process will have to complete first.

Once provisioning is completed, your Cisco IronPort Email Encryption page will show the profile as provisioned. At this stage, you are ready to create policy that uses encryption.



CONCLUSION

In summary, we have shown the three steps necessary to prepare a Cisco Email Security Appliance for sending encrypted email.

1. **Enabling Cisco IronPort Email Encryption**
2. **Registering the ESA appliance(s) with CRES**
3. **Creating Encryption Profiles**

Additional detail is available in the ESA User Guide corresponding to your ESA software release. User guides are available at the following link:

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**