Best Practices Guide for Data Loss Prevention and Encryption

Contents

Introduction

This document describes best practices for Data Loss Prevention (DLP) and encryption for Cisco Email Security.

This document discusses the setup of message encryption using the Cisco Email Security Appliance (ESA) and the cloud-based Cisco Registered Envelope Service (RES). Customers can use message encryption to send individual messages securely over the public Internet, using various types of policies including content filtering and 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.

Prerequisites

Requirements

There are no specific requirements for this document.

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

This document will discuss the following steps:

1. Enabling Cisco IronPort Email Encryption
2. Register your ESA(s) and your organization with RES
3. Creating Encryption Profiles
4. Enabling DLP
5. Creating DLP Message Actions
6. Creating DLP Policies
7. Applying DLP Policies to an Outgoing Email Policy

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

Cisco IronPort Email Encryption is also referred to as RES Encryption. RES is the name that we use for the “key servers” in the Cisco Cloud. The RES 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 *3. Creating Encryption Profiles*.

Best Practice Guide for Data Loss Prevention and Encryption Best Practices

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

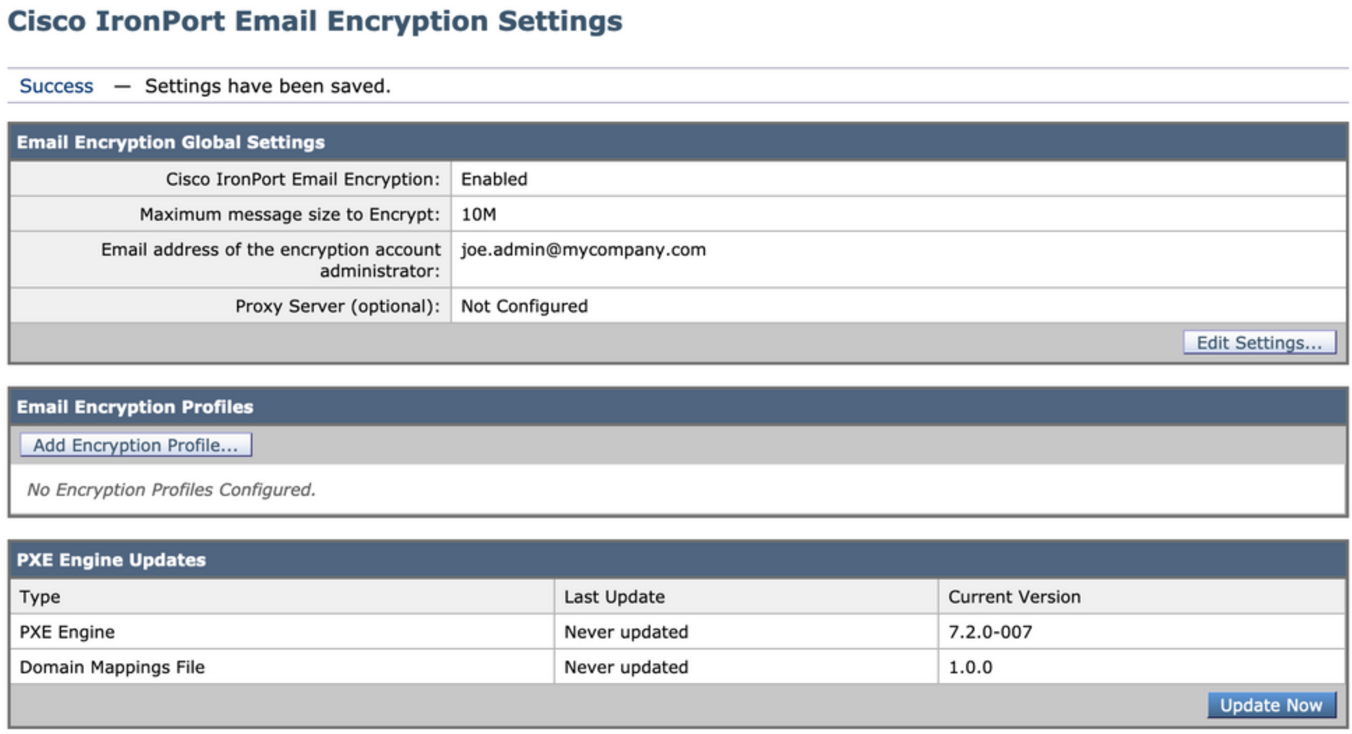
> **Note**: If you have multiple ESAs in a cluster, then Step #1 step should only need to be performed once since these settings are typically managed at the cluster level. If you have multiple machines that are not clustered, or if you are managing these settings at the machine level, then Step #1 should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

1. From the ESA UI, navigate to **Security Services > Cisco IronPort Email Encryption**.
2. Check the box to enable Cisco IronPort Email Encryption.
3. Accept the End User License Agreement (EULA), Cisco IronPort Email Encryption License Agreement.
4. In the *Email Encryption Global Settings*, click **Edit Settings...** Specify the email address for the administrator/person who is the primary RES Admin for the account. This email account will be associated with the administration of the RES environment for the company.Optional: The default maximum message size to encrypt is 10M. You may increase/decrease the size

at this time if you wish.Optional: If you have a proxy that the ESA will need to go through to connect to RES via HTTPS, add the necessary proxy and authentication settings for allowing it to go through the proxy.

5. Submit and Commit your configuration changes.

At this point you should see the “Email Encryption Global Settings” set to something like this, however with no profiles listed yet:



Cisco IronPort Email Encryption Settings

Success — Settings have been saved.

Email Encryption Global Settings

Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	joe.admin@mycompany.com
Proxy Server (optional):	Not Configured

Email Encryption Profiles

No Encryption Profiles Configured.

PXE Engine Updates

Type	Last Update	Current Version
PXE Engine	Never updated	7.2.0-007
Domain Mappings File	Never updated	1.0.0

2. Register your ESA(s) and your organization with RES

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

> **Note**: ESA registration information is also found in the following TechNote: Cisco RES: Account Provisioning for Virtual, Hosted, and Hardware ESA Configuration Example

Please send an email direct to RES: stg-cres-provisioning@cisco.com.

In order to provision a CRES account for your ESA's Encryption Profile(s), please provide us with the following information:

1. Name of account **(Please specify the exact company name, as you require this to be listed.)** For Cloud Email Security(CES)/Hosted customer accounts, please notate your account name to end as "<Account Name> HOSTED"
2. Email address(es) to be used for the Account Admin **(Please specify the corresponding admin email address)**
3. Complete appliance serial number(s) An appliance serial number can be located from the ESA GUI (System Administration > Feature Keys), or ESA CLI via the 'version' command. Providing a virtual license number (VLN) or product activitation key (PAK) license is not acceptable, as a complete appliance serial number is required for CRES account

administration.
4. Domain names that should be mapped to the CRES account for administration purposes

Note: If you already have a CRES account, please provide the company name or existing CRES account number. This will assure that any new appliance serial numbers are added to the correct account, and avoid any duplication of company information and provisioning.

Please be assured, if you are emailing in regarding provisioning a CRES account, we will respond with-in one (1) business day. If you need immediate support and assistance, please open a support request with Cisco TAC. This can be done via Support Case Manager (https://mycase.cloudapps.cisco.com/case) or by calling by phone (https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html).

> **Note**: After you have emailed this request, it may take a day for your Company RES 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.

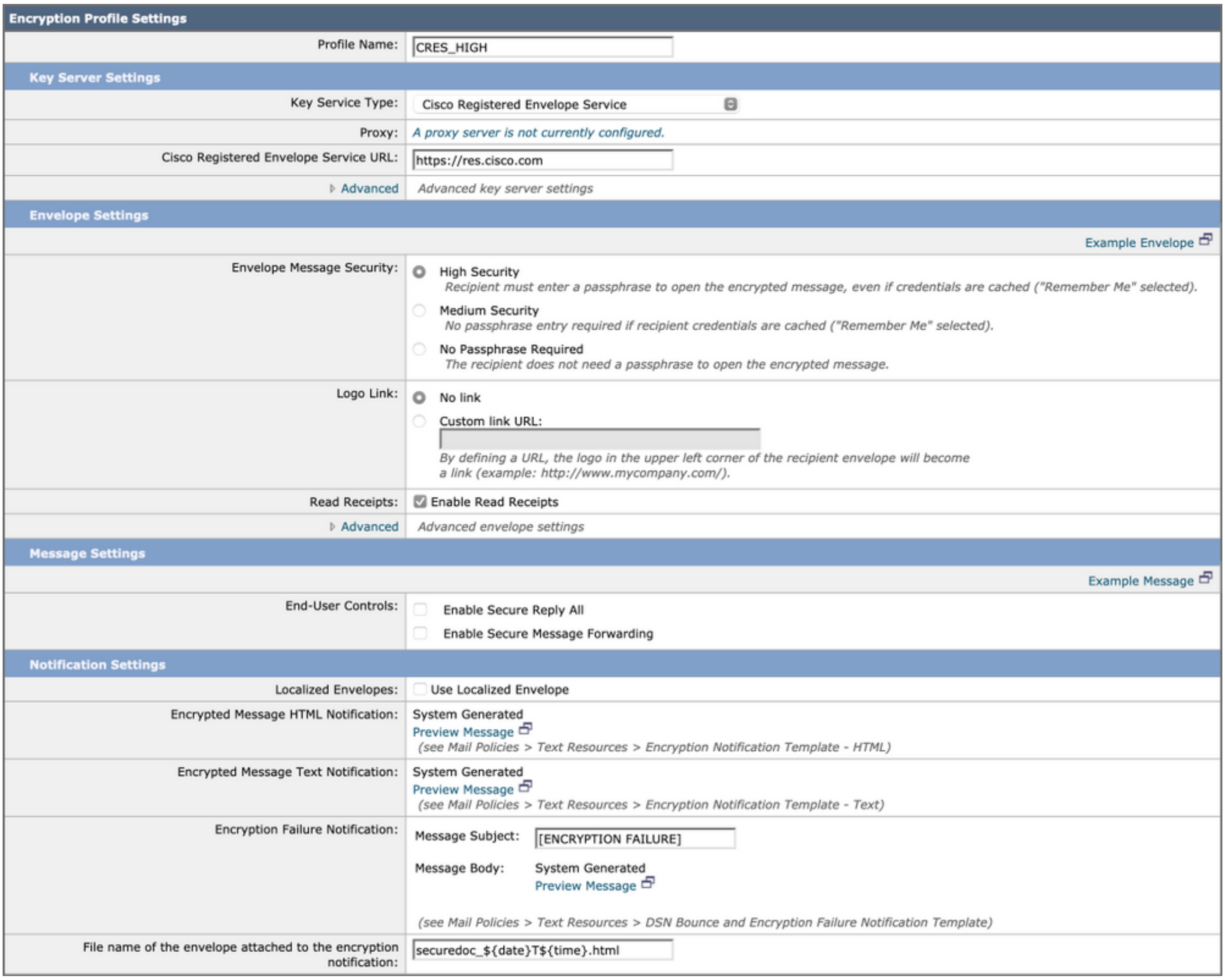
3. Create Encryption Profiles on the ESA(s)

> **Note**: 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.

An encryption profile specifies how encrypted messages should be sent. For example, an organization may need to send High-Security envelopes for one segment of its 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 user id 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 "CRES_HIGH", "CRES_MED", and "CRES_LOW".

1. From the ESA UI, navigate to **Security Services > Cisco IronPort Email Encryption**.
2. Click "Add Encryption Profile..."
3. The Encryption Profile menu will open, and you can name your first encryption profile "CRES_HIGH".
4. Select "High Security" for the Envelope Message Security, if not already selected.
5. Click **Submit** to save this profile.



Encryption Profile Settings	
Profile Name:	CRES_HIGH
Key Server Settings	
Key Service Type:	Cisco Registered Envelope Service
Proxy:	*A proxy server is not currently configured.*
Cisco Registered Envelope Service URL:	https://res.cisco.com
▹ Advanced	*Advanced key server settings*
Envelope Settings	
	Example Envelope
Envelope Message Security:	● High Security *Recipient must enter a passphrase to open the encrypted message, even if credentials are cached ("Remember Me" selected).* ○ Medium Security *No passphrase entry required if recipient credentials are cached ("Remember Me" selected).* ○ No Passphrase Required *The recipient does not need a passphrase to open the encrypted message.*
Logo Link:	● No link ○ Custom link URL: *By defining a URL, the logo in the upper left corner of the recipient envelope will become a link (example: http://www.mycompany.com/).*
Read Receipts:	☑ Enable Read Receipts
▹ Advanced	*Advanced envelope settings*
Message Settings	
	Example Message
End-User Controls:	□ Enable Secure Reply All □ Enable Secure Message Forwarding
Notification Settings	
Localized Envelopes:	□ Use Localized Envelope
Encrypted Message HTML Notification:	System Generated Preview Message *(see Mail Policies > Text Resources > Encryption Notification Template - HTML)*
Encrypted Message Text Notification:	System Generated Preview Message *(see Mail Policies > Text Resources > Encryption Notification Template - Text)*
Encryption Failure Notification:	Message Subject: [ENCRYPTION FAILURE] Message Body: System Generated Preview Message *(see Mail Policies > Text Resources > DSN Bounce and Encryption Failure Notification Template)*
File name of the envelope attached to the encryption notification:	securedoc_${date}T${time}.html

Next, repeat steps 2-5 to create "CRES_MED" and "CRES_LOW" — just change the radio button for the Envelope Message Security for each profile.

- For the CRES_HIGH profile, choose the “High Security” radio button.
- For the CRES_MED profile, choose the “Medium Security” radio button.
- For the CRES_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. In Envelope Settings, if you click the “Advanced” link, you can select one of three symmetric encryption algorithms, as well as specify that the envelope is sent without the Java encryption applet.

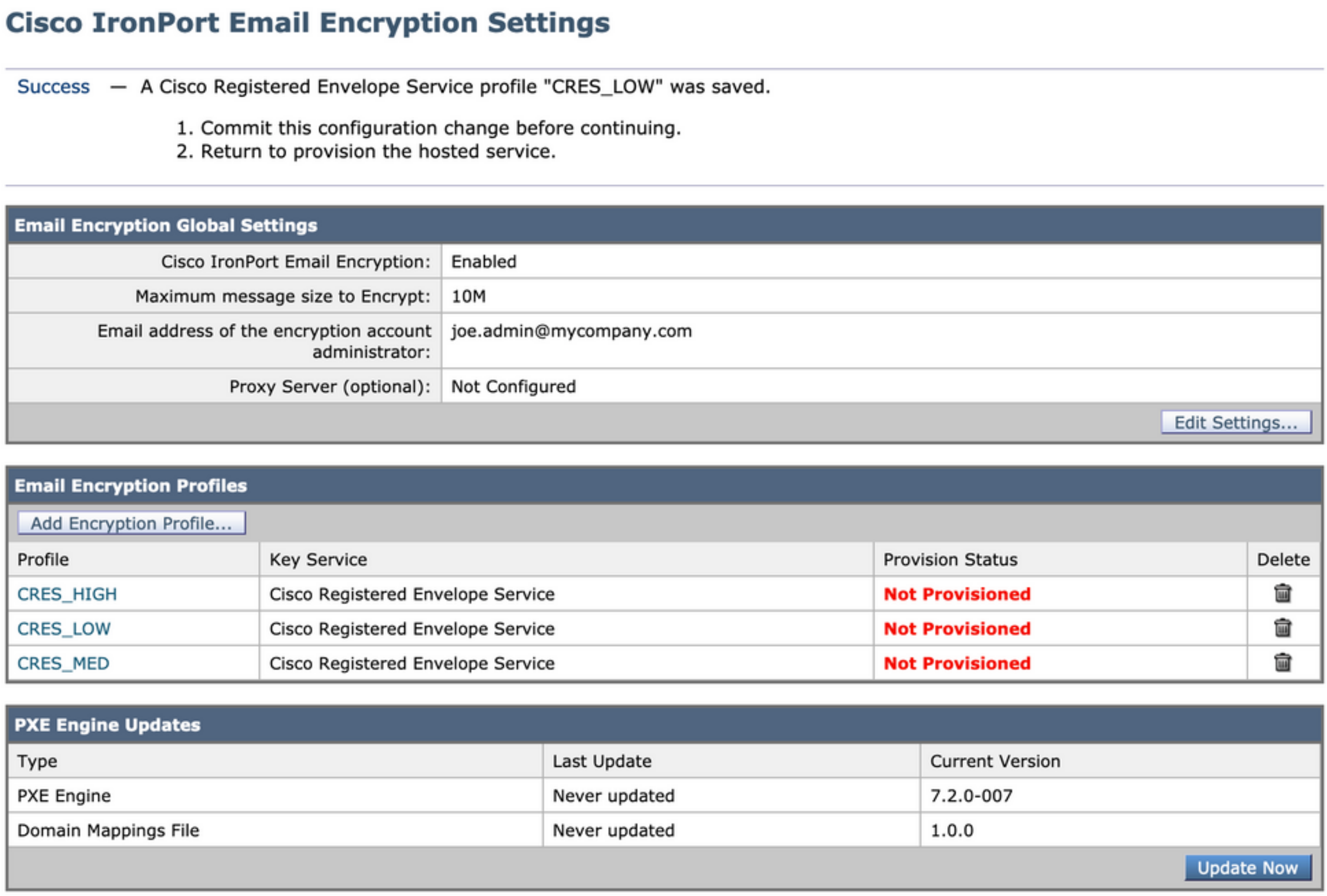
To the right of Envelope Settings, you will see the “Example Message” hypertext link. If clicked, this will show you an example of the Secure Message Envelope — what the recipient will see in their email after they open the HTML attachment.

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 the "Example Message" hypertext link. If clicked, this will show you what the opened message will look like — what the recipient will see once they have provided the necessary information in the envelope, and have opened the encrypted message.

Always remember to click **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.



Cisco IronPort Email Encryption Settings

Success — A Cisco Registered Envelope Service profile "CRES_LOW" was saved.

1. Commit this configuration change before continuing.
2. Return to provision the hosted service.

Email Encryption Global Settings

Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	joe.admin@mycompany.com
Proxy Server (optional):	Not Configured

Email Encryption Profiles

Profile	Key Service	Provision Status	Delete
CRES_HIGH	Cisco Registered Envelope Service	Not Provisioned	🗑
CRES_LOW	Cisco Registered Envelope Service	Not Provisioned	🗑
CRES_MED	Cisco Registered Envelope Service	Not Provisioned	🗑

PXE Engine Updates

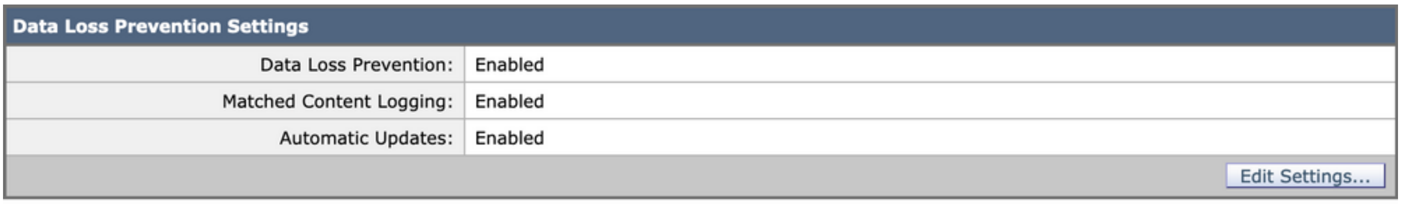
Type	Last Update	Current Version
PXE Engine	Never updated	7.2.0-007
Domain Mappings File	Never updated	1.0.0

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

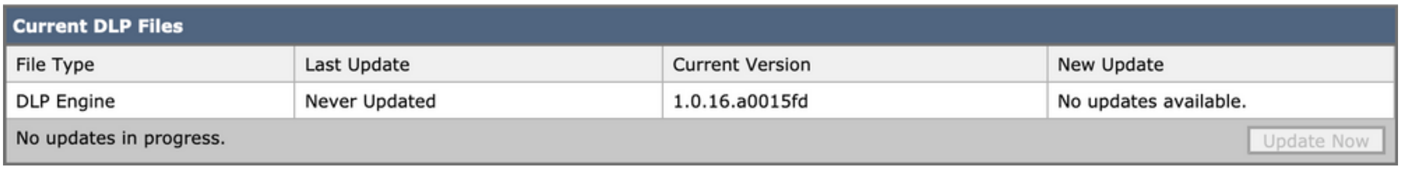
Once provisioning is completed, your Cisco IronPort Email Encryption page will show the profile as provisioned.

4. Enabling Data Loss Prevention (DLP)

1. From the ESA UI, navigate to **Security Services > Data Loss Prevention**.
2. Click **Enable...** to enable DLP.
3. Accept the EULA, Data Loss Prevention License Agreement.
4. Click the checkbox for Enable matched content logging.
5. Click the checkbox for Enable automatic updates.
6. Click **Submit**.



Data Loss Prevention Settings	
Data Loss Prevention:	Enabled
Matched Content Logging:	Enabled
Automatic Updates:	Enabled



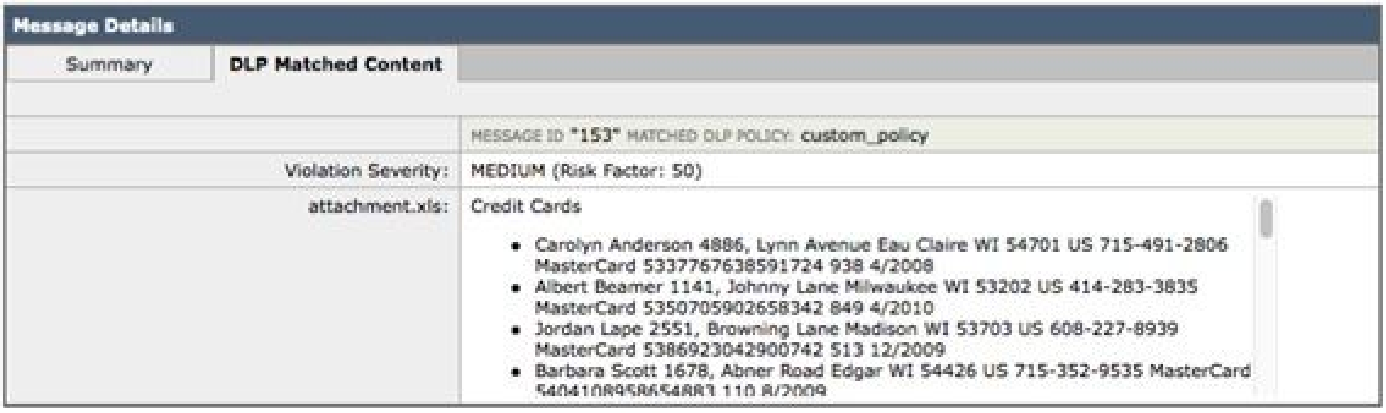
Current DLP Files

File Type	Last Update	Current Version	New Update
DLP Engine	Never Updated	1.0.16.a0015fd	No updates available.

No updates in progress.

Updates for the DLP engine and predefined content matching classifiers on your appliance are independent of updates for other security services. The 3-5 minute regular Talos signature updates are different and do not include updating DLP policies and dictionaries. Updates must be enabled here.

When “Matched Content Logging” is Enabled, it allows Message Tracking to show the content of the email that caused the violation. Here is an example of Message Tracking showing the email content that caused the DLP violation. In this way, an admin can know exactly which data triggered a specific DLP policy.



MESSAGE ID "153" MATCHED DLP POLICY: custom_policy

Violation Severity: MEDIUM (Risk Factor: 50)

attachment.xls: Credit Cards

- Carolyn Anderson 4886, Lynn Avenue Eau Claire WI 54701 US 715-491-2806 MasterCard 5337767638591724 938 4/2008
- Albert Beamer 1141, Johnny Lane Milwaukee WI 53202 US 414-283-3835 MasterCard 5350705902658342 849 4/2010
- Jordan Lape 2551, Browning Lane Madison WI 53703 US 608-227-8939 MasterCard 5386923042900742 513 12/2009
- Barbara Scott 1678, Abner Road Edgar WI 54426 US 715-352-9535 MasterCard 5404108958654883 110 8/2009

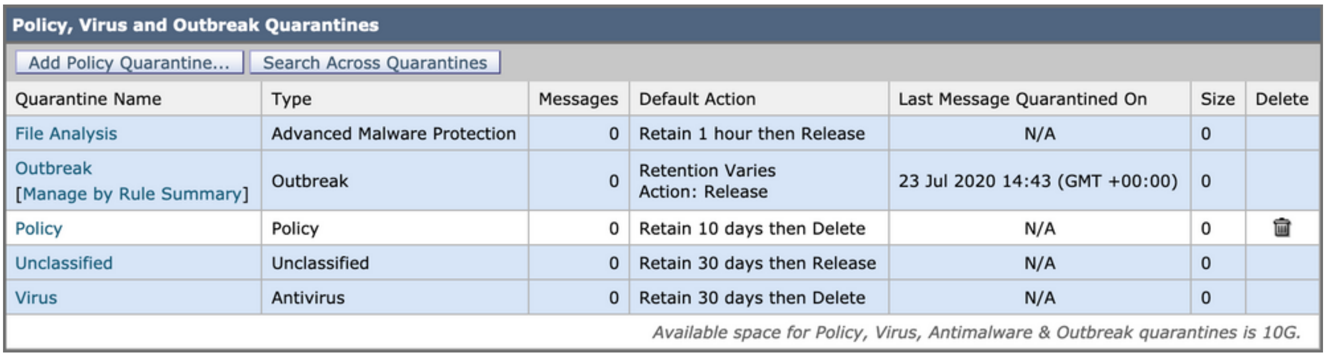
Data Loss Prevention Violation

5. Creating Data Loss Prevention Message Actions

Create DLP Quarantines

If you’d like to keep a copy of messages violating DLP policies you can create individual Policy quarantines for each type of policy violation. This is especially useful when running a ‘transparent’ POV, where Outbound messages violating DLP policies are logged and delivered but no action is taken on the messages.

1. On the SMA, navigate to **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**
2. This is what the Quarantines table should look like before we start:



Policy, Virus and Outbreak Quarantines

Add Policy Quarantine... | Search Across Quarantines

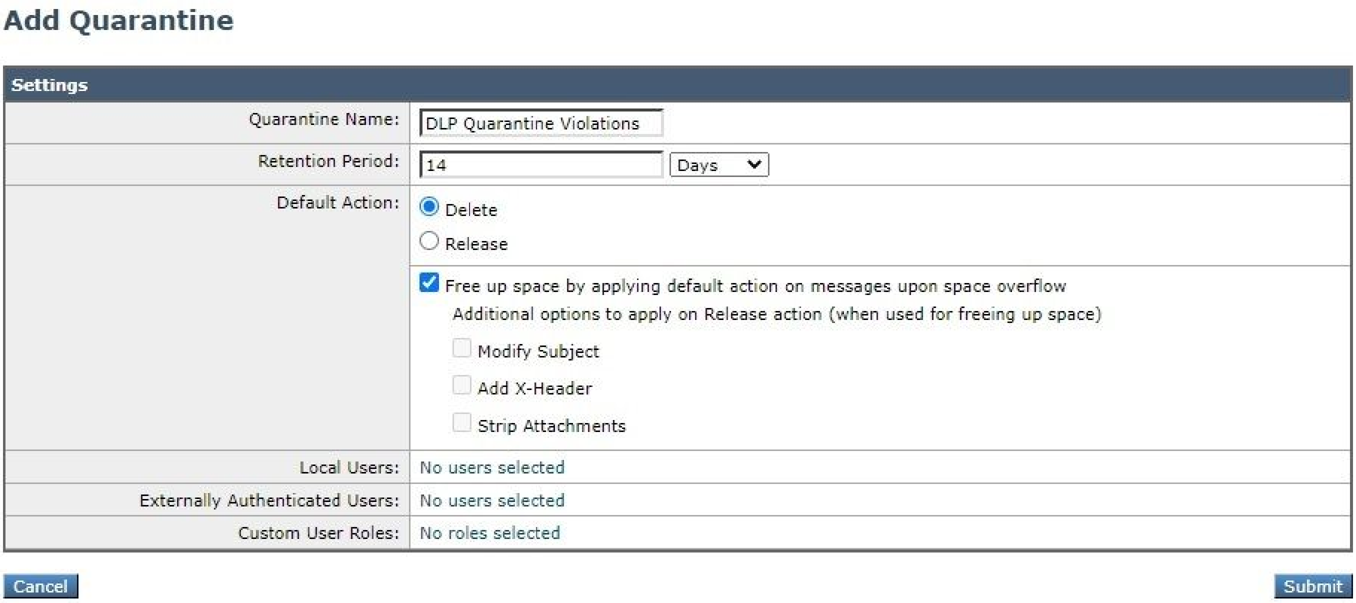
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	N/A	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	23 Jul 2020 14:43 (GMT +00:00)	0	
Policy	Policy	0	Retain 10 days then Delete	N/A	0	🗑
Unclassified	Unclassified	0	Retain 30 days then Release	N/A	0	
Virus	Antivirus	0	Retain 30 days then Delete	N/A	0	

Available space for Policy, Virus, Antimalware & Outbreak quarantines is 10G.

Policy Virus and Outbreak Quarantine

3. Click the “Add Policy Quarantine” button and create a quarantine to be used by the DLP policies.

Below is an example quarantine made for a medium DLP violation. Segmentation of quarantines is possible and may be desired for multiple DLP rules:



Add Quarantine

Settings

Quarantine Name:	DLP Quarantine Violations
Retention Period:	14 Days
Default Action:	● Delete ○ Release ☑ Free up space by applying default action on messages upon space overflow Additional options to apply on Release action (when used for freeing up space) □ Modify Subject □ Add X-Header □ Strip Attachments
Local Users:	No users selected
Externally Authenticated Users:	No users selected
Custom User Roles:	No roles selected

Cancel | Submit

Example DLP Quarantine

About DLP Message Actions

DLP message actions describe what actions that the ESA will take when it detects a DLP violation in an outgoing email. You can specify primary and secondary DLP Actions and different actions can be assigned for different violation types and severities.

Primary actions include:

- Deliver
- Drop
- Quarantine

For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used.

Secondary actions include:

- Sending a copy to any custom quarantine or the ‘Policy’ quarantine.
- **Encrypt the message.** The appliance only encrypts the message body. It does not encrypt

the message headers.
- Altering the Subject header.
- Adding disclaimer text/HTML to the message.
- Sending the message to an alternate destination mailhost.
- Sending bcc copies of the message.
- Sending DLP violation notification to the sender and/or other contacts.

These actions are not mutually exclusive — you can combine some of them within different DLP policies for various processing needs for different user groups.

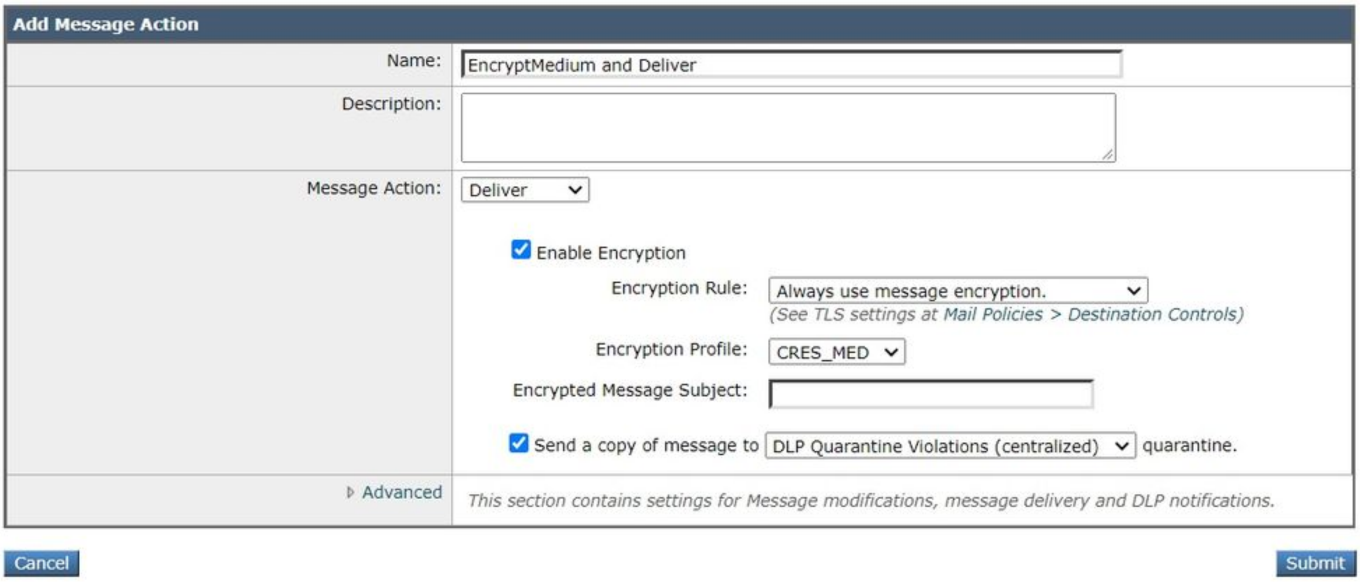
We are going to implement the following DLP Actions: **Encrypt**

These actions assume that Encryption is licensed and configured on the ESA and three profiles have been created for High, Medium, and Low security as was done in the earlier sections:

- CRES_HIGH
- CRES_MED
- CRES_LOW

Create the DLP Message Actions

1. Go to *Mail Policies > DLP Message Customizations.*
2. Click the “Add Message Action” button and add the following DLP Actions. Make sure to commit the change after submitting your message action



Add Message Action

Name:	EncryptMedium and Deliver
Description:	
Message Action:	Deliver ☑ Enable Encryption Encryption Rule: Always use message encryption. (See TLS settings at Mail Policies > Destination Controls) Encryption Profile: CRES_MED Encrypted Message Subject: ☑ Send a copy of message to DLP Quarantine Violations (centralized) quarantine.
Advanced	This section contains settings for Message modifications, message delivery and DLP notifications.

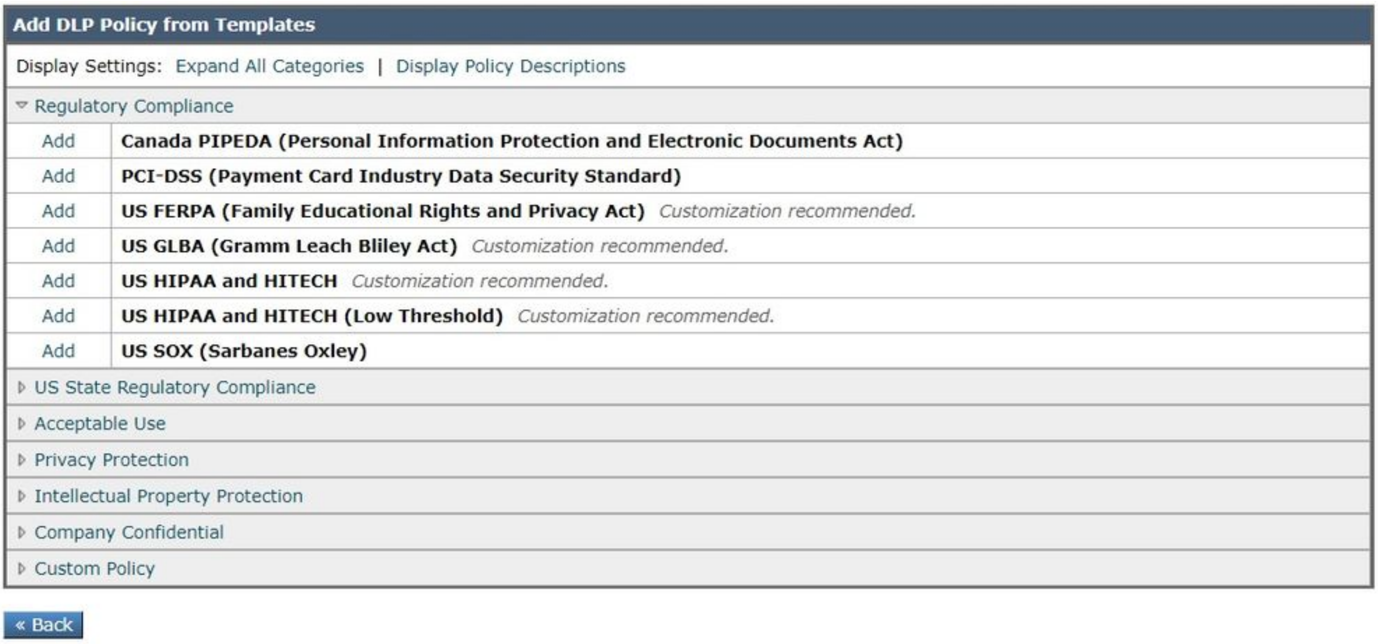
Message Action

6. Creating Data Loss Prevention Policies

A DLP policy includes:

- A set of conditions that determine whether an outgoing message contains sensitive data
- The actions to be taken when a message contains such data.

1. Navigate to: *Mail Policies > DLP Policy Manager*
2. Click *‘Add DLP Policy’*
3. Open the “Regulatory Compliance” disclosure triangle.



Add DLP Policy from Templates

Display Settings: Expand All Categories | Display Policy Descriptions

▽ Regulatory Compliance

Add	**Canada PIPEDA (Personal Information Protection and Electronic Documents Act)**
Add	**PCI-DSS (Payment Card Industry Data Security Standard)**
Add	**US FERPA (Family Educational Rights and Privacy Act)** *Customization recommended.*
Add	**US GLBA (Gramm Leach Bliley Act)** *Customization recommended.*
Add	**US HIPAA and HITECH** *Customization recommended.*
Add	**US HIPAA and HITECH (Low Threshold)** *Customization recommended.*
Add	**US SOX (Sarbanes Oxley)**

▷ US State Regulatory Compliance

▷ Acceptable Use

▷ Privacy Protection

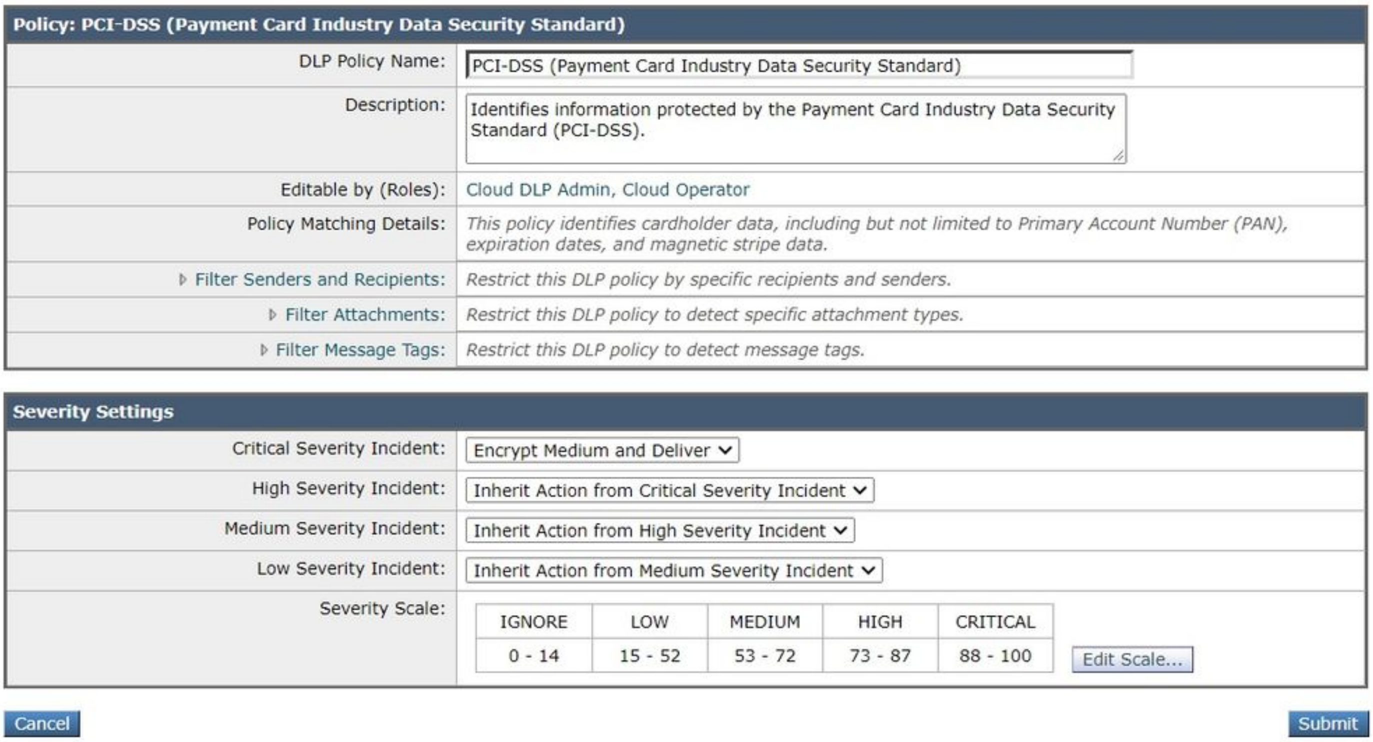
▷ Intellectual Property Protection

▷ Company Confidential

▷ Custom Policy

DLP Policy Template

4. For PCI policy click the "Add" button to the left of PCI-DSS.



Policy: PCI-DSS (Payment Card Industry Data Security Standard)

DLP Policy Name:	PCI-DSS (Payment Card Industry Data Security Standard)
Description:	Identifies information protected by the Payment Card Industry Data Security Standard (PCI-DSS).
Editable by (Roles):	Cloud DLP Admin, Cloud Operator
Policy Matching Details:	*This policy identifies cardholder data, including but not limited to Primary Account Number (PAN), expiration dates, and magnetic stripe data.*
▷ Filter Senders and Recipients:	*Restrict this DLP policy by specific recipients and senders.*
▷ Filter Attachments:	*Restrict this DLP policy to detect specific attachment types.*
▷ Filter Message Tags:	*Restrict this DLP policy to detect message tags.*

Severity Settings

Critical Severity Incident:	Encrypt Medium and Deliver
High Severity Incident:	Inherit Action from Critical Severity Incident
Medium Severity Incident:	Inherit Action from High Severity Incident
Low Severity Incident:	Inherit Action from Medium Severity Incident

Severity Scale:

IGNORE	LOW	MEDIUM	HIGH	CRITICAL
0 - 14	15 - 52	53 - 72	73 - 87	88 - 100

PCI-DSS Example DLP rule

5. For the Critical Severity Incident select "Encrypt Medium and Deliver" action we previously configured. We could change the lower severity incidents but for now, let's have them inherit our critical severity incident. Submit and then commit the change.

7. Applying DLP Policies to an Outgoing Email Policy

1. Navigate to: Mail Policies > Outgoing Mail Policies
2. Click on the control cell for DLP for the Default Policy. It will read “Disabled” if you have not enabled it yet.
3. Change the pulldown button from Disable DLP to Enable DLP and you will immediately be

presented with the DLP policy you just created.
4. Click the “Enable All” checkbox. Submit and then Commit the changes.

Conclusion

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

1. Enabling Cisco IronPort Email Encryption
2. Register your ESA(s) and your organization with RES
3. Creating Encryption Profiles
4. Enabling DLP
5. Creating DLP Message Actions
6. Creating DLP Policies
7. Applying DLP Policies to an Outgoing Email Policy

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

Related Information

- **Technical Support & Documentation - Cisco Systems**