

# Clearswift Secure Gateways

---

Implementing Encryption on the Clearswift Secure Email Gateways

Issue 1.3

September 2020

## Copyright

Version 1.3, September 2020

Published by Clearswift Ltd.

© 1995–2020 Clearswift Ltd.

All rights reserved.

All rights reserved. The intellectual property rights in the materials are the property of Clearswift Ltd and/or its licensors. The materials may not be reproduced or disseminated or transmitted in any form or by any means electronic, mechanical, photocopying, recording, or otherwise stored in any retrievable system or otherwise used in any manner whatsoever, in part or in whole, without the express permission of Clearswift Ltd.

The Clearswift Logo and Clearswift product names are trademarks of Clearswift Ltd. All other trademarks are the property of their respective owners. Clearswift Ltd. (registered number 3367495) is registered in Britain with registered offices at 1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA, England. Users should ensure that they comply with all national legislation regarding the export, import, and use of cryptography.

Clearswift reserves the right to change any part of this document at any time.

Click [here](#) to read Copyright, Trademark, and third party acknowledgments in full.

## Contents

1	Introduction .....	5
2	Encryption Options .....	6
3	Basics of Encryption.....	8
3.1	Public Key.....	8
3.2	Private Key .....	8
4	Encryption Components .....	9
4.1	Certificate/Key Storage.....	9
4.2	Decryption Policy .....	10
4.3	Encryption Policy .....	11
4.4	Encryption/Decryption Defaults .....	11
5	Implementing Encryption .....	13
5.1	Configuring the Encryption/Decryption Defaults .....	13
5.1.1	Password Encryption.....	14
5.1.2	PGP .....	14
5.1.3	S/MIME .....	15
5.1.4	Decryption Summary .....	16
5.1.5	Encryption/Decryption Logging .....	16
5.1.6	Original Encrypted Messages .....	17
5.2	Managing Certificates .....	18
5.2.1	Required Certificates .....	19
5.2.2	Managing the Partners Certificate Store .....	20
5.2.3	Managing the Corporate Certificate Store.....	21
5.2.4	Managing the Certificate Authorities Certificate Store .....	24
5.3	Configuring Encryption Endpoints.....	25
5.3.1	Defining a Mail Encryption Endpoint.....	25
5.4	Mail Policy Route Settings.....	26
5.5	Policy Based Encryption.....	28
6	Example Scenarios.....	28
6.1	How do I send an encrypted (secure) email to a partner? .....	29

- 6.2 How do I send an encrypted (secure) email to a recipient with no PGP or S/MIME capability?..... 31
- 6.3 How do I decrypt and content check email from a partner?..... 32
- 6.4 How do I content check secured emails entering my organization when going to one of the end users?..... 34
- 6.5 How do I encrypt email and content scan the message? ..... 36
- 6.6 How do I encrypt email and not content scan the message? ..... 37

## 1 Introduction

The Clearswift SECURE Email Gateway supports a number of modes of operation to facilitate SMTP messages being delivered over the Internet in an encrypted format, which can be decrypted at the Gateway or at the desktop of the recipient.

The Email Gateway offers encryption based on:

- Mail Policy Routes - Who the message is going to
- Content Rules - The detection of certain content being present in the message (e.g. confidential material, a particular file type, etc.)

Encrypting messages also provides authentication (proof of who you are) of who sent the message and also non-repudiation (proof that what you said in the message is what you wrote) because encrypted messages can't be modified in transit.

## 2 Encryption Options

The email itself can be encrypted using the following methods:

- Password encryption
- PGP
- S/MIME

The screenshot displays the Clearswift administration interface for a local administrator. The top navigation bar includes links for Home, Policy, Messages, Reports, System, Health, and Users. The main content area is titled "Encryption/Decryption Defaults" and contains several configuration sections, each with a "Click here to change these settings" link:

- Password Encryption:**
  - The password used will be automatically generated with a length of 16 characters
  - The subject line will not be protected
  - Automatically generated passwords will not be logged
  - The email containing the encrypted original and the password notification will be in English
- PGP:**
  - Messages will use the MIME format of PGP.
  - PGP attachments will use the pgp extension.
- S/MIME:**
  - Messages will be signed using the detached format.
- Decryption Summary:**
  - The decryption summary will be in English.
- Encryption/Decryption Logging:**
  - Logging information produced while encrypting and decrypting messages will be **disabled**.
- Original Encrypted Messages:**
  - When applying encryption endpoints prefer the original encrypted message to re-encryption.

The supported modes of operation are:

- Gateway to Gateway
  - S/MIME, PGP
- Gateway to Recipient
  - S/MIME, PGP, Password Protected
- Sender to Recipient
  - S/MIME, PGP
  - With content checking (assuming the appropriate key is available to decrypt the message)

The following examples demonstrate how encryption can be used:

- Outbound Email
  - User sends plain text message, Gateway encrypts message with user/company key or password mechanism
  - User sends encrypted message, Gateway decrypts, checks content and delivers encrypted original
  - User sends encrypted message, Gateway decrypts, checks content and delivers re-encrypted message
  - User sends encrypted message, Gateway delivers original message
  - User sends signed message, Gateway delivers original message
  - User sends plain message, Gateway delivers signed message
- Inbound Email
  - Receives signed message, verifies and delivers original
  - Receives signed message, verifies, strips the signature and delivers modified version
  - Receives encrypted message, delivers original
  - Receives encrypted message, decrypts and delivers original
  - Receives encrypted message, decrypts and delivers decrypted version
  - Receives encrypted message, decrypts and delivers re-encrypted version

## 3 Basics of Encryption

Encryption and digital signing rely on the principles of asymmetric cryptography better known as public key cryptography which relies on pairs of keys known as public and private keys.

### 3.1 Public Key

The public key of a person is used to encrypt email destined for that person. It is also used to verify the authenticity of any message that has been signed by the public key's owner.

As is suggested by the name, the public key can be widely distributed safely with no fear of loss of data or somebody forging the owner's identity.

### 3.2 Private Key

The private key of a person is used to decrypt email that has been sent to that person. It can also be used to digitally sign a message so that a recipient can prove that the message has not been tampered with by the time they receive it.

It is very important that the private key is protected and not widely distributed if at all. Any person that has access to the private key will be able to decrypt email destined for the key's owner and digitally impersonate them by signing messages and other types of data. For this reason, private keys are normally password protected so that even if you have access to the key, you also need to know the password in order to use it.

## 4 Encryption Components

In order to provide you with flexibility in the way you manage your encryption policy, the configuration options have been split across four distinct management areas:

- Certificate/key storage
- Decryption policy
- Encryption policy
- Encryption/decryption defaults

### 4.1 Certificate/Key Storage

The Email Gateway contains a certificate/key store that allows you to upload S/MIME and PGP keys to the Gateway so that they can be used to decrypt and/or encrypt email passing through the Gateway.

The screenshot displays the 'Certificate Store' management interface. On the left, there is a sidebar with 'What would you like to do?' options such as 'Generate certificate/key', 'Import certificate authority', and 'Run checks'. The main area shows a table of certificates with the following columns: Type, Details, Email, and Expires. The table contains 20 entries, showing a mix of S/MIME certificates from various issuers like AC Camerfirma, Actalis, and Agencia Notarial de Certificación.

Type	Details	Email	Expires
S/MIME	AC Camerfirma S.A., Chambers of Commerce Root - 2008		July 31, 2038
S/MIME	AC Camerfirma S.A., Global Chambersign Root - 2008		July 31, 2038
S/MIME	AC Camerfirma SA CIF A82743287, http://www.chambersig...	chambersroot@chambersign.org	September 30, 2037
S/MIME	AC Camerfirma SA CIF A82743287, http://www.chambersig...	chambersignroot@chambersign.org	September 30, 2037
S/MIME	AC Camerfirma SA CIF A82743287, http://www.chambersig...	publicnotaryroot@chambersign.org	September 30, 2037
S/MIME	ACCV, PKIACCV, ACCVRAIZ1	accv@accv.es	December 31, 2030
S/MIME	ACNLB		May 15, 2023
S/MIME	Actalis S.p.A./03358520967, Actalis Authentication CA G1		June 25, 2022
S/MIME	Actalis S.p.A./03358520967, Actalis Authentication Root CA		September 22, 2030
S/MIME	AddTrust AB, AddTrust External TTP Network, AddTrust Exter...		May 30, 2020
S/MIME	admin, Services, Admin-Root-CA		November 10, 2021
S/MIME	ADMINISTRACION NACIONAL DE CORREOS, SERVICIOS ELE...		December 31, 2030
S/MIME	AffirmTrust, AffirmTrust Commercial		December 31, 2030
S/MIME	AffirmTrust, AffirmTrust Networking		December 31, 2030
S/MIME	AffirmTrust, AffirmTrust Premium		December 31, 2040
S/MIME	AffirmTrust, AffirmTrust Premium ECC		December 31, 2040
S/MIME	Agencia Catalana de Certificacio (NIF Q-0801176-1), Serveis...	ec_acc@catcert.net	January 7, 2031
S/MIME	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B833...	ancert@ancert.com	February 11, 2024
S/MIME	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B833...	ancert@ancert.com	February 11, 2024
S/MIME	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B833...	ancert@ancert.com	February 11, 2024

The certificate store is split into three separate sections based on the use of the certificates/keys.

- **Certificate Authorities**  
This store contains the Certificate Authorities used for TLS and the Certificate Authorities used to verify the other certificates/keys that will be used to encrypt/decrypt and sign email messages. The certificates contained in this part of the store are never used to encrypt or decrypt email messages.
- **Corporate Certificate/Keys**  
You should upload certificates/keys that belong to your organization into this section of the store. These keys will be used to decrypt and sign email messages on behalf of people within your organization.  
This part of the store will contain a large number of private keys because of the nature of the operations performed using them.
- **Partner Certificate/Keys**  
The partner section of the store contains the public keys of people and organizations you do business with. These keys are used to encrypt email being sent to those people and verify the digital signatures of email being received from those people.  
This part of the store will contain a large number of public keys.

## 4.2 Decryption Policy

By default the Email Gateway will not decrypt messages or validate their digital signatures unless these features have been enabled on a Mail Policy Route. This enables you to control which routes you wish to decrypt and content inspect encrypted email on.

### 4.3 Encryption Policy

Whether the Email Gateway encrypts messages is a facet of the delivery disposal action for each processed message. Once it has been decided that a message should be encrypted, the Gateway will use the Mail Encryption Endpoints to decide how this encryption is performed.

The screenshot displays the 'Mail Encryption Endpoints' configuration page in the Clearswift SECURE Email Gateway. The interface includes a navigation menu with options like Home, Policy, Messages, Reports, System, Health, and Users. A sidebar on the left offers 'What would you like to do?' (New encryption endpoint) and 'Help' (Clearswift SECURE Email Gateway, Mail Encryption Endpoints). The main content area shows a table of encryption endpoints with columns for From, To, Method, Encryption, and Signing.

	From	To	Method	Encryption	Signing
<input type="checkbox"/>	HR - Department	Clearswift	PGP	Red.com (UK)	
<input type="checkbox"/>	My Company	Payroll	Password	Password	
<input type="checkbox"/>	My Company	Legal - External	S/MIME , Automatic	Legal - External	Automatic

The Mail Encryption Endpoints define:

- Who you may be encrypting messages to:
  - An email address
  - An email domain
  - Address list(s)
- What method of encryption you will be using:
  - S/MIME
  - PGP
  - Password
- How the encryption will be configured
  - If this particular encryption policy is for S/MIME or PGP, then the endpoint will be defined with the correct certificate for that endpoint.
  - If this endpoint will be communicated with via the Password scheme, then these parameters are related to the password and its strength.

### 4.4 Encryption/Decryption Defaults

You can use the Encryption/Decryption Defaults page to configure the default settings for encryption and decryption.

The screenshot shows the Clearswift SECURE Email Gateway administration interface. The page title is "Encryption/Decryption Defaults". The navigation menu includes Home, Policy, Messages, Reports, System, Health, and Users. The page content is organized into several sections, each with a list of settings and a "Click here to change these settings" button:

- Password Encryption**
  - The password used will be automatically generated with a minimum length of 16 characters
  - When encrypting the body, the subject line will not be protected
  - Automatically generated passwords will be shared by split messages
  - Passwords will not be logged
  - The email containing the encrypted original and the password notification will be in English
  - All of the message will be encrypted
  - The Zip file format used will be Windows-compatible
  - Exchange 2007 Compatibility Mode is not enabled
- PGP**
  - Messages will use the MIME format of PGP
  - All of the message will be used for encryption and signing.
  - PGP attachments will use the pgp extension
- S/MIME**
  - Messages will be signed using the detached format
  - Messages will not be signed using RSA/PSS
  - Messages will not be encrypted using RSA/OAEP
  - Message headers will not be protected
  - If message headers are protected, the subject will not be changed
- Decryption Summary**
  - The decryption summary will be in English.
- Encryption/Decryption Logging**
  - Logging information produced while encrypting and decrypting messages will be **disabled**.
- Original Encrypted Messages**
  - When applying encryption endpoints prefer the original encrypted message to re-encryption.
- Key Resolution**
  - Prefer S/MIME keys
- Automatic Encryption**
  - Do not query key servers for encryption keys
  - If an encryption key can not be found then trigger the cryptographic failure rule
- Automatic Signing**
  - If a signing key can not be found then trigger the cryptographic failure rule.
- Online Certificate Status Protocol**
  - S/MIME certificate revocation checking via OCSP is enabled.
- Key Extraction**
  - When added to the Certificate Store, extracted PGP and S/MIME user keys will not be enabled for encryption.

From this page, you can edit the default settings for:

- Password Encryption
- PGP
- S/MIME
- Decryption Summary
- Encryption/Decryption Logging
- Original Encrypted Messages

## 5 Implementing Encryption

Implementing encryption on the Clearswift SECURE Email Gateway can be split into a number of stages:

- Use the Encryption settings in the System Center to:
  - Configure the Encryption/Decryption Defaults.
  - Create new Certificates or load existing Certificates into the Certificate Store.
  - Configure Mail Encryption Endpoints.
- Use the Mail Policy Route settings in the Policy Center to:
  - Enable encryption/decryption on a Mail Policy Route by applying the Mail Encryption Endpoints defined above.
- Use the Policy Rule settings in the Policy Center to:
  - Configure policy based encryption.

### 5.1 Configuring the Encryption/Decryption Defaults

To configure the Encryption/Decryption Defaults:

1. From the System Center Home page, click **Encryption**.
2. Click **Encryption/Decryption Defaults**.
3. On the Encryption/Decryption Defaults page you can configure the following:
  - Password Encryption
  - PGP
  - S/MIME
  - Decryption Summary
  - Encryption/Decryption Logging
  - Original Encrypted Messages

### 5.1.1 Password Encryption

#### Password Encryption

- The password used will be  with a minimum length of  characters
- When encrypting the body, the subject line will
- Automatically generated passwords will
- Passwords will
- The email containing the encrypted original and the password notification will be in
- 
- The Zip file format used will be
- Exchange 2007 Compatibility Mode is

In the Password Encryption area of the Encryption/Decryption Defaults page you can specify whether:

- The password will be automatically generated or a specific phrase.
- The subject line will be protected or not be protected.
- Automatically generated passwords will be logged or not be logged.

### 5.1.2 PGP

#### PGP

- Messages will use the  of PGP
- 
- PGP attachments will use the  extension

In the PGP area of the Encryption/Decryption Defaults page you can specify whether:

- The messages will use the MIME format or inline format of PGP.
- PGP attachments will use the pgp, gpg or asc extension.

### 5.1.3 S/MIME

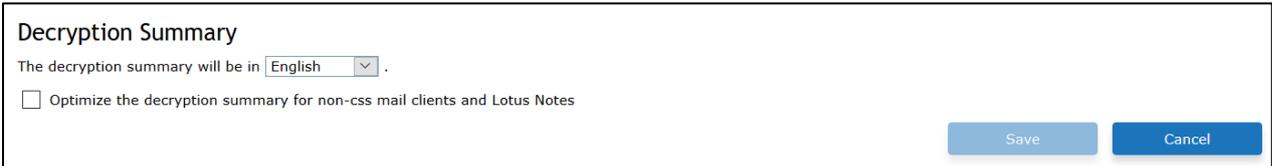
**S/MIME**

- Messages will be signed using the
- Signing using RSA/PSS is
- Encryption using RSA/OAEP is
- Message header protection is
- If message headers are protected, replace the subject with this string:

In the S/MIME area of the Encryption/Decryption Defaults page you can specify whether the messages will be signed using the detached format or opaque format.

- **Detached format**  
S/MIME signatures are usually detached signatures where the signature information is separate from the text being signed. The MIME type for this is multipart/signed with the second part having a MIME subtype of application/(x-)pkcs7-signature. However, it is possible for mailing list software to change the textual part and invalidate the signature.
- **Opaque format**  
The secured content in S/MIME messages is actually made up of Multipurpose Internet Mail Extension (MIME) body parts. A plain text message can, therefore, contain an attached signature. This is called a clear-signed message because the message can be read without verifying the signature.  
An opaque-signed message contains the message and signature combined in a single part that cannot be read except by verifying the signature.

### 5.1.4 Decryption Summary



**Decryption Summary**

The decryption summary will be in English .

Optimize the decryption summary for non-css mail clients and Lotus Notes

Save Cancel

In the Decryption Summary area of the Encryption/Decryption Defaults page you can specify:

- The language of the decryption summary:
  - English
  - German
  - French
  - Polish
  - Japanese
- Whether to optimize the decryption summary for non-css mail clients and Lotus Notes.

### 5.1.5 Encryption/Decryption Logging



**Encryption/Decryption Logging**

• When encrypting and decrypting messages the log level should be : disabled

disabled  
summary  
detailed  
debug

Save Cancel

In the Encryption/Decryption Logging area of the Encryption/Decryption Defaults page you can specify:

- The log level to be used when encrypting and decrypting messages:
  - Disabled
  - Summary
  - Detailed
  - Debug

### 5.1.6 Original Encrypted Messages

In the Original Encrypted Messages area of the Encryption/Decryption Defaults page you can specify whether the Gateway acts transparently by content inspecting a digitally signed or encrypted message and then delivering the original message.

If a message meets the following criteria and the **When applying encryption endpoints prefer the original encrypted message to re-encryption** checkbox is selected, the original unmodified encrypted message will be delivered, rather than apply the Encryption Endpoint:

- It was decrypted by the Gateway.
- A delivery disposal action for the message specifies that the message should be encrypted.
- The message has not been modified by policy (e.g. the addition of a disclaimer).

## 5.2 Managing Certificates

The Email Gateway contains a certificate/key store that allows you to upload S/MIME and PGP keys to the Gateway so that they can be used to decrypt and/or encrypt email passing through the Gateway.

**SECURE Email Gateway** Local administrator (admin) | Logout

Home Policy Messages Reports System Health Users

Apply Configuration Now | Backup & Restore | System Center | Mail Encryption Endpoints | Encryption/Decryption Defaults | Certificate Store

**Certificate Store**

Certificate Authorities Corporate Partners Configuration

Search Criteria [Click here to change these settings](#)

Import Reset Filter

Showing 1 - 20 of 319

	Type	Details	Email	Expires
<input type="checkbox"/>	S/MIME	AC Camerfirma S.A., Chambers of Commerce Root - 2008		July 31, 2038
<input type="checkbox"/>	S/MIME	AC Camerfirma S.A., Global Chambersign Root - 2008		July 31, 2038
<input type="checkbox"/>	S/MIME	AC Camerfirma SA CIF A82743287, http://www.chambersig...	chambersroot@chambersign.org	September 30, 2037
<input type="checkbox"/>	S/MIME	AC Camerfirma SA CIF A82743287, http://www.chambersig...	chambersignroot@chambersign.org	September 30, 2037
<input type="checkbox"/>	S/MIME	AC Camerfirma SA CIF A82743287, http://www.chambersig...	publicnotaryroot@chambersign.org	September 30, 2037
<input type="checkbox"/>	S/MIME	ACCV, PKIACCV, ACCVRAIZ1	accv@accv.es	December 31, 2030
<input type="checkbox"/>	S/MIME	ACNLB		May 15, 2023
<input type="checkbox"/>	S/MIME	Actalis S.p.A./03358520967, Actalis Authentication CA G1		June 25, 2022
<input type="checkbox"/>	S/MIME	Actalis S.p.A./03358520967, Actalis Authentication Root CA		September 22, 2030
<input type="checkbox"/>	S/MIME	AddTrust AB, AddTrust External TTP Network, AddTrust Exter...		May 30, 2020
<input type="checkbox"/>	S/MIME	admin, Services, Admin-Root-CA		November 10, 2021
<input type="checkbox"/>	S/MIME	ADMINISTRACION NACIONAL DE CORREOS, SERVICIOS ELE...		December 31, 2030
<input type="checkbox"/>	S/MIME	AffirmTrust, AffirmTrust Commercial		December 31, 2030
<input type="checkbox"/>	S/MIME	AffirmTrust, AffirmTrust Networking		December 31, 2030
<input type="checkbox"/>	S/MIME	AffirmTrust, AffirmTrust Premium		December 31, 2040
<input type="checkbox"/>	S/MIME	AffirmTrust, AffirmTrust Premium ECC		December 31, 2040
<input type="checkbox"/>	S/MIME	Agencia Catalana de Certificacio (NIF Q-0801176-1), Serveis...	ec_acc@catcert.net	January 7, 2031
<input type="checkbox"/>	S/MIME	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B833...	ancert@ancert.com	February 11, 2024
<input type="checkbox"/>	S/MIME	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B833...	ancert@ancert.com	February 11, 2024
<input type="checkbox"/>	S/MIME	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B833...	ancert@ancert.com	February 11, 2024

**What would you like to do?**

- Generate certificate/key
- Import certificate authority
- Import corporate certificate/key
- Import partner certificate/key
- Run checks
- Copy to Partners
- Copy to Corporate
- Use as default decryption key
- Do not use as default decryption key

**Help**

- Clearswift SECURE Email Gateway
- Certificate Store

### 5.2.1 Required Certificates

To use S/MIME or PGP, you must have the correct certificates in the appropriate Certificate Store of the encrypting or decrypting Gateway. You can import existing certificates into the Gateway, or create new certificates using the key generation functionality.

The Gateway mode, Encrypting or Decrypting, is dependent on the direction of the email. For example, with an inbound message, the Gateway will be in Decrypting mode and needs a Private Key to decrypt the message.

#### 5.2.1.1 Encryption

Use the following guidelines for encryption:

- S/MIME
  - Encrypting Gateway - Public Key of the Recipient must be in the Partners Certificate Store.
  - Decrypting Gateway - Private Key of the Recipient must be in the Corporate Certificate Store (Configured as a Default Decryption Key)
  - Any message can be decrypted by the Default Decryption key.
- PGP
  - Encrypting Gateway - Public Key of the Recipient must be in the Partners Certificate Store.
  - Decrypting Gateway - Private Key of the Recipient must be in the Corporate Certificate Store.
  - The Default Decryption Key is not used by PGP.

#### 5.2.1.2 Signing

Use the following guidelines for signing:

- S/MIME
  - Sender End - Sign with the Private Key of the sender.
  - Recipient End - Sender CA Certificate (Public Key version) or a self-signed CA.
- PGP
  - Sender End - Private Key of the Sender must be in the Corporate Certificate Store.
  - Recipient End - Public Key of the Sender must be in the Partners Certificate Store.

Please note that you cannot encrypt with S/MIME and sign with PGP, or vice versa.

## 5.2.2 Managing the Partners Certificate Store

To view the certificates currently stored in the Partners Certificate Store:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page.
3. Click the **Partners** tab. The issuer of each stored certificate is listed in the information pane in its Distinguished Name (DN) format.
4. Select a certificate from the list and click **View** to display the Certificate Details.

To import a certificate to the Certificate Store:

1. Obtain the certificate and place it on a file system that you can access from the Clearswift SECURE Email Gateway web interface.
2. From the System Center page, click **Encryption**. The Encryption page appears.
3. Click **Certificate Store** to display the Certificate Store page.
4. Click the **Partners** tab to display the Partners Certificate Store.
5. Click **Import** at the top of the list of stored certificates.
6. In the Upload Certificate or Key dialog, click **Browse** and select the certificate .PEM file you wish to add. Enter a password, if required.
7. Click **Import**.
8. If the upload is successful, the Clearswift Gateway will display a Certificate Imported dialog.

To export a certificate from the Certificate Store:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page.
3. Click the **Partners** tab to display the Partners Certificate Store.
4. Select a certificate from the list and click **Export**.
5. Specify the filename and location to which the certificate should be saved and click **Save**.

To copy a certificate to the Corporate Certificate Store:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page.
3. Click the **Partners** tab.
4. Select the certificate(s) from the list and click **Copy to Corporate** in the Task Pane.

### 5.2.3 Managing the Corporate Certificate Store

To view the certificates currently stored in the Corporate Certificate Store:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page.
3. Click the **Corporate** tab. The issuer of each stored certificate is listed in the information pane in its Distinguished Name (DN) format.
4. Select a certificate from the list and click **View** to display the Certificate Details.

To import a certificate to the Certificate Store:

1. Obtain the certificate and place it on a file system that you can access from the Clearswift SECURE Email Gateway web interface.
2. From the System Center page, click **Encryption**. The Encryption page appears.
3. Click **Certificate Store** to display the Certificate Store page.
4. Click the **Corporate** tab to display the Corporate Certificate Store.
5. Click **Import** at the top of the list of stored certificates.
6. In the Upload Certificate or Key dialog, click **Browse** and select the certificate .PEM file you wish to add. Enter a password, if required.
7. Click **Import**.
8. If the upload is successful, the Clearswift Gateway displays a Certificate Imported dialog.

To export a certificate from the Certificate Store:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page.
3. Click the **Corporate** tab to display the Corporate Certificate Store.
4. Select a certificate from the list and click **Export**.
5. Specify the filename and location to which the certificate should be saved and click **Save**.

To generate a new certificate:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page.
3. Click the **Corporate** tab to display the Corporate Certificate Store.
4. Click **New** at the top of the list of stored certificates.
5. In the Generate New Certificate or Key dialog:
  - Specify the Type of Certificate, **S/MIME** or **PGP**, using the drop-down list.
  - Enter a **Name** for the certificate.
  - Enter an **Email address** for the certificate.
  - Optionally, enter the **Company**, **Department** and **Location**.
  - Specify the **Country** using the drop-down list.
  - Enter the **Days Valid**.
  - If an S/MIME certificate is being generated, you can select the signature to **Sign With** using the drop-down list.
  - Specify the **Key Strength** (1024, 2048, 3072 or 4096) using the drop-down list.
  - Optionally, enter a **Password**.
  - If an S/MIME certificate is being generated, optionally, click the checkbox to select the **Certificate Authority**, **Include certificate revocation list** or **Limit to email usage**.
6. Click **Generate**.

To copy a certificate to the Partners Certificate Store:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page.
3. Click the **Corporate** tab.
4. Select the certificate(s) from the list and click **Copy to Partners** in the Task Pane.

### 5.2.3.1 Default Decryption S/MIME Keys

When using S/MIME encryption, a number of default decryption keys can be specified. A company that has multiple domains is likely to have one default key per domain. In addition, a company may issue a default decryption key on a partner by partner basis as well.

An S/MIME certificate that has a private key component can be marked as being a default decryption key. Only certificates in the Corporate store can be marked as default decryption certificates.

There is no imposed limit to the number of certificate/key pairs that can be marked. However there will be a gradual impact on performance depending on the number of keys that need to be tried before a message can be decrypted.

To indicate that a certificate/key pair has been marked as a default decryption key a mail envelope with a small padlock overlaid is displayed. If the key pair has been marked, the icon will be in colour and will have a tool tip, otherwise it will be greyed out. If the certificate dialog is opened for the key pair, the default decryption state is noted towards the bottom of the dialog.

To specify the Corporate Key that, by default, should be used to attempt to decrypt an S/MIME message:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page and click the **Corporate** tab.
3. Select the S/MIME Certificate to be used and click **Use as default decryption key** in the task pane.

## 5.2.4 Managing the Certificate Authorities Certificate Store

To view the certificates currently stored:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page. The issuer of each stored certificate is listed in the information pane in its Distinguished Name (DN) format.
3. To view the key algorithm and the dates for which any certificate is valid, select that certificate from the list.

To import a certificate to the Certificate Store:

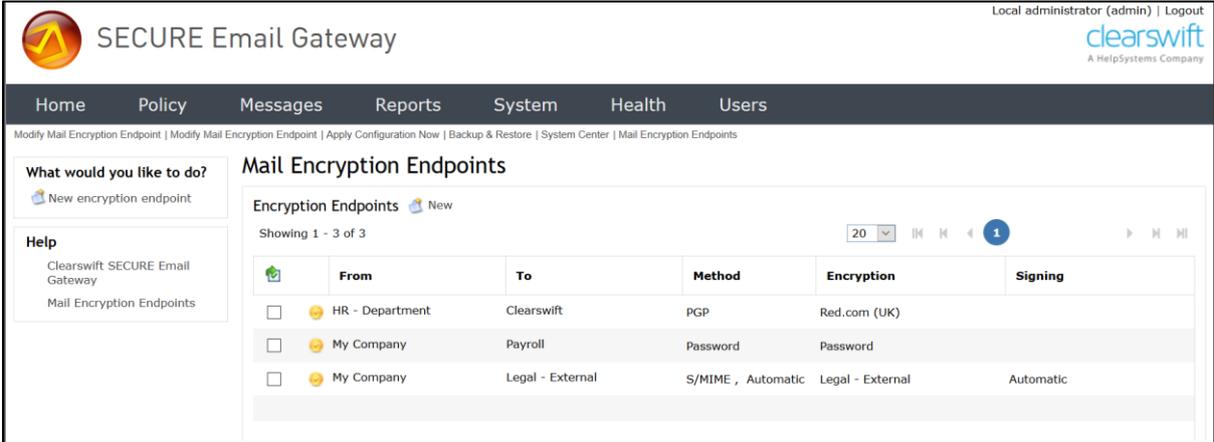
1. Obtain the CA signing certificate from the owner of the TLS client system and place it on a file system that you can access from the Clearswift Gateway web interface.
2. From the System Center page, click **Encryption**. The Encryption page appears.
3. Click **Certificate Store** to display the Certificate Store page.
4. Click the **Certificate Authorities** tab to display the Certificate Authorities Store.
5. Click **Import** at the top of the list of stored certificates.
6. In the Upload Certificate or Key dialog, click **Browse** and select the certificate .PEM file you wish to add. Enter a password, if required.
7. Click **Import**.
8. If the upload is successful, Clearswift Gateway displays a Certificate Imported dialog.

To export a certificate from the Certificate Store:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Certificate Store** to display the Certificate Store page.
3. Click the **Certificate Authorities** tab to display the Certificate Authorities Store.
4. Select a certificate from the list and click **Export**.
5. Specify the filename and location to which the certificate should be saved and click **Save**.

## 5.3 Configuring Encryption Endpoints

A Mail Encryption Endpoint defines a profile of encryption settings for the Clearswift SECURE Email Gateway to use when establishing an encrypted conversation.



The screenshot shows the 'Mail Encryption Endpoints' configuration page in the Clearswift SECURE Email Gateway administration interface. The page includes a navigation menu with options like Home, Policy, Messages, Reports, System, Health, and Users. The main content area displays a table of encryption endpoints. The table has columns for 'From', 'To', 'Method', 'Encryption', and 'Signing'. There are three rows of endpoints listed, each with a checkbox in the 'From' column.

	From	To	Method	Encryption	Signing
<input type="checkbox"/>	HR - Department	Clearswift	PGP	Red.com (UK)	
<input type="checkbox"/>	My Company	Payroll	Password	Password	
<input type="checkbox"/>	My Company	Legal - External	S/MIME , Automatic	Legal - External	Automatic

The Mail Encryption Endpoint specifies:

- The Email address, Domain or Address List(s) with which these settings are to be used.
- Whether encryption is required and, if so, what level of encryption to enforce.

### 5.3.1 Defining a Mail Encryption Endpoint

To define a Mail Encryption Endpoint:

1. From the System Center page, click **Encryption**. The Encryption page appears.
2. Click **Mail Encryption Endpoints** to display the Mail Encryption Endpoints page. The page lists any previously defined Mail Encryption Endpoints.
3. Click **New** adjacent to the **Encryption Endpoints** heading. The Modify Mail Encryption Endpoint page appears.
4. Edit the Overview information as required:
  - Move the pointer over the Overview area and click on **Click here to change these settings**.
  - Edit the **Name** of the Mail Encryption Endpoint, to provide a meaningful name.
  - Enter any **Notes** you want to add to describe the Mail Encryption Endpoint.
  - Click **Save**.

5. Edit the **For mail sent to the** information to define who the endpoint is associated with:
  - Move the pointer over the **For mail sent to the** area and click on **Click here to change these settings**.
  - Select from:
    - **Email address**
      - The Email address can be a maximum of 160 characters.
    - **Domain**
      - The Domain must not exceed 160 characters and be a fully qualified domain name.
    - **Address List(s)**
      - Select the Address List(s) from the displayed list.
  - Click **Save**.
6. Edit the **Messages will be encrypted** information to define the encryption details:
  - Move the pointer over the **Messages will be encrypted** area and click on **Click here to change these settings**.
  - Click the checkbox to encrypt the messages and use the drop-down list to select one of the following options:
    - **Encrypt body and attachments**
    - **Encrypt attachments**
  - Use the drop-down list to select the encryption method:
    - **Password**
    - **PGP certificate**
    - **S/MIME certificate**
  - If the selected certificate is signed, you can click the checkbox to **Sign the messages using** and specify the signature using the drop-down list.
  - Click **Save**.
7. Depending on the Encryption method selected above, the Password Options, PGP Options or S/MIME Options panel will be displayed:
  - The Password Options allow you to specify whether:
    - The password will be automatically generated or a specific phrase.
    - The subject line will be protected or not be protected.
    - Automatically generated passwords will be logged or not be logged.
  - The PGP Options allow you to specify whether:
    - The messages will use the MIME format or inline format of PGP.
    - PGP attachments will use the pgp, gpg or asc extension.
  - The S/MIME Options allow you to specify whether the messages will be signed using the:
    - a. Detached format
    - b. Opaque format

## 5.4 Mail Policy Route Settings

Once you have all of the components in place, you can configure your encryption/decryption policy on a Mail Policy Route.

To do this:

1. Click on the **Policy** tab.
2. Click on **Mail Policy Routes**.
3. Create a new Policy Route or modify an existing Policy Route.
4. Use the **For Mail Sent** area to specify a mail route between the **For** and **To** Address Lists.
5. In the **Do NOT Decrypt or Apply Encryption Endpoints** area click on **Click here to change these settings**.
6. Select the checkbox to **Decrypt and apply content rules to PGP and S/MIME messages**.
7. You can select to include with the message a description of the decryption and/or signature verification, if required.
8. Select the **By default apply encryption endpoint delivery policy** checkbox.
9. Click on **Save**.

**Do NOT Decrypt or Apply Encryption Endpoints**

 When encrypted message inspection is enabled, we recommend that you check the policy rules assigned to this route to ensure that they will not leak sensitive information via informs.  
Please consult the documentation for more information.

Decrypt and apply content rules to PGP and S/MIME messages.

Extract the following types of key from the message: S/MIME

**Include with the message a description of the**

Decryption.

Signature verification.

By default apply encryption endpoint delivery policy.

Save Cancel

10. Add the appropriate Content Rules.
11. Note that you need to add a Content Rule to define the actions if encryption or decryption fails.

**Unless One Of These Content Rules Triggers**

 New  Show rule action

1 Rule on route

		Rules	Rule Type
1.	<input type="checkbox"/>	Encryption or decryption fails <small>Hold in <b>Encryption or decryption failures</b> area</small>	Error

## 5.5 Policy Based Encryption

You can also configure the Clearswift SECURE Email Gateway to apply encryption based upon your message policy. For example, you may wish to encrypt emails containing a specific word or phrase.

The screenshot displays the Clearswift SECURE Email Gateway administration console. The main configuration area is titled "Content Rule Usage" and shows a rule named "Mail Policy Routes : 'My Company' to 'Payroll'". The rule is configured to detect lexical expressions. The "What To Look For?" section includes a "Lexical Expression" rule with a list of conditions: "Content - the attachments matching the conditions in the other clauses", "Scan body", "Scan header and footer", and "Scan properties". Other conditions include "And Which Media Types", "And Size Restriction Of", and "And Scan text extracted from images (OCR)". The "What To Do?" section includes a "Disposal Action" to "Deliver the message applying encryption endpoint policy".

To do this:

1. Create a new Lexical Expression List that contains the words/phrases you wish to search for.
2. Create a Content Rule that references the above Lexical Expression List and contains the Disposal Action **Deliver the message applying encryption endpoint policy**.
3. Apply the new Content Rule to the appropriate Mail Policy Routes.

## 6 Example Scenarios

This section contains a number of examples of how you can implement encryption on the Clearswift SECURE Email Gateway.

- How do I send an encrypted (secure) email to a partner?
- How do I send an encrypted (secure) email to a recipient with no PGP or S/MIME capability?
- How do I decrypt and content check email from a partner?
- How do I content check secured emails entering my organization when going to one of the end users?
- How do I encrypt email and content scan the message?
- How do I encrypt email and not content scan the message?

## 6.1 How do I send an encrypted (secure) email to a partner?

You can send an encrypted (secure) email to a partner using S/MIME, PGP or Password encryption.

The screenshot displays the 'SECURE Email Gateway' web interface. The top navigation bar includes 'Home', 'Policy', 'Messages', 'Reports', 'System', 'Health', and 'Users'. The current page is 'Modify Mail Encryption Endpoint'. On the left, there are sections for 'Changes Made', 'What would you like to do?', and 'Help'. The main content area is divided into several sections:

- Overview:** A lightbulb icon indicates that the endpoint name is automatically maintained. A link 'Click here to change these settings' is present.
- For Mail Sent:** A 'New' button and a list of endpoints. The selected endpoint is 'Legal - External'.
- Encryption and Signing Options:**
  - Encrypt the message using:
    - a password
    - the recipient's key
    - the following certificate: Legal - External (SMIME) [Search]
  - Sign the messages using:
    - the sender's key
    - the following certificate: [Search]
- Automatic Signing:** A link 'Click here to change these settings' and a note: 'If a signing key can not be found then trigger the cryptographic failure rule. (Default Setting)'
- S/MIME Options:** A link 'Click here to change these settings' and a list of default settings:
  - Messages will be signed using the detached format (Default Setting)
  - Messages will not be signed using RSA/PSS (Default Setting)
  - Messages will not be encrypted using RSA/OAEP (Default Setting)
  - Message headers will not be protected (Default Setting)
  - If message headers are protected, the subject will not be changed (Default Setting)

## To do this:

1. If appropriate, use the System Center, Encryption, Certificate Store page to ensure that at least one valid PGP or S/MIME certificate is loaded into the store.
2. Use the Mail Encryption Endpoints page to configure the settings for the partner.
  - a. Add the email address of the partner to the **For mail sent to the** area.
  - b. In the **Messages will be encrypted** area:
    - i. Specify whether to **encrypt body and attachments** or **encrypt attachments**.
    - ii. Specify whether to use a **password, PGP certificate** or **S/MIME certificate** using the drop-down list.
    - iii. You can also choose to sign a message by clicking the **Sign the messages using** checkbox and selecting a certificate from the drop-down list.
3. Use the Mail Policy Route settings in the Policy Center to enable encryption/decryption on a route by applying the Encryption Endpoint defined above.
  - a. Create a new Policy Route or modify an existing Policy Route.
  - b. Specify the Default Delivery Action of the Route to use Encryption Endpoints.
  - c. Specify the Default Decryption Action of the Route to decrypt and apply content rules to PGP and S/MIME messages.
  - d. Then add a Content Rule to define the actions if Encryption or Decryption fails.

## 6.2 How do I send an encrypted (secure) email to a recipient with no PGP or S/MIME capability?

You can send an encrypted (secure) email to a partner with no PGP or S/MIME capability.

The screenshot displays the 'Modify Mail Encryption Endpoint' configuration page in the Clearswift SECURE Email Gateway. The page is titled 'Modify Mail Encryption Endpoint' and includes a navigation menu with options like Home, Policy, Messages, Reports, System, Health, and Users. The main content area is divided into several sections:

- Changes Made:** A notification box indicating that configuration changes have been made and need to be applied. It includes buttons for 'Apply Configuration' and 'Discard Configuration'.
- What would you like to do?:** A section with options to 'Delete the endpoint' or 'Change default settings'.
- Help:** A section with links to 'Clearswift SECURE Email Gateway' and 'Mail Encryption Endpoints'.
- Overview:** A section with a lightbulb icon and the text: 'The name for this endpoint is automatically maintained. Edit this panel if you would like to supply your own name.' A button 'Click here to change these settings' is present.
- For Mail Sent:** A section with a 'New' button and a list of recipients. The list shows 'My Company' under the 'From' column and 'Payroll' under the 'To' column. A 'Showing 1 - 1 of 1' indicator is visible.
- Encryption and Signing Options:** A section with two main options:
  - Encrypt the message using:** This is checked. It includes radio buttons for 'a password' (selected), 'the recipient's key', and 'the following certificate' (with a search button).
  - Sign the messages using:** This is unchecked. It includes radio buttons for 'the sender's key' and 'the following certificate' (with a search button).
- Password Options:** A section with a 'Click here to change these settings' button and a list of default settings:
  - The password used will be automatically generated with a minimum length of 16 characters (Default Setting)
  - When encrypting the body, the subject line will not be protected (Default Setting)
  - Automatically generated passwords will be shared by split messages (Default Setting)
  - Passwords will not be logged (Default Setting)
  - The email containing the encrypted original will be in English (Default Setting)
  - All of the message will be encrypted (Default Setting)
  - The Zip file format used will be Windows-compatible (Default Setting)

1. Use the Mail Encryption Endpoints page to configure the settings for the partner.
  - a. Add the email address of the partner to the **For mail sent to the** area.
  - b. In the **Messages will be encrypted** area:
    - i. Specify whether to **encrypt body and attachments** or **encrypt attachments**.
    - ii. Select **password** from the drop-down list.
2. Use the Mail Policy Route settings in the Policy Center to enable encryption/decryption on a route by applying the Encryption Endpoint defined above.
  - a. Create a new Policy Route or modify an existing Policy Route.

- b. Specify the Default Delivery Action of the Route to use Encryption Endpoints.
- c. Then add a Content Rule to define the actions if Encryption or Decryption fails.

### 6.3 How do I decrypt and content check email from a partner?

You can decrypt and content check email from a partner that has been encrypted using S/MIME or PGP.

The screenshot shows the 'Modify Policy Route' configuration page in the Clearswift Secure Email Gateway. The page is divided into several sections:

- Changes Made:** A notification box indicating that configuration changes have been made and need to be applied to take effect. It includes buttons for 'Apply Configuration' and 'Discard Configuration'.
- What would you like to do?:** A list of actions such as 'Copy rules from route', 'Delete the route', 'New 'From' LDAP address list', 'New 'From' static address list', 'New 'To' LDAP address list', 'New 'To' static address list', 'Create encryption endpoint', 'Manage Content Rules', and 'Manage Disposal Actions'.
- Help:** Links to 'Clearswift SECURE Email Gateway', 'Content security policy FAQ', and 'Edit a policy route'.
- Overview:** A section with a lightbulb icon stating 'The name for this route is automatically maintained. Edit this panel if you would like to supply your own name.' and a 'Click here to change these settings' button.
- For Mail Sent:** A table showing the 'From' and 'To' fields. The 'From' field is 'Partner Companies' and the 'To' field is 'My Company'. There is a 'New' button and a 'Showing 1 - 1 of 1' indicator.
- Decrypt and Apply Encryption Endpoints:** A section with a green checkmark icon. It includes the text 'Decrypt and apply content rules to PGP and S/MIME messages.' and 'Include with the message a description of the decryption and signature verification.' Below this, there is a checked checkbox for 'By default apply encryption endpoint delivery policy.' and a 'Click here to change these settings' button.
- By Default Perform This Disposal Action:** A section with a green checkmark icon. It shows 'Deliver the message' as the default action and a 'Click here to change these settings' button.
- Unless One Of These Content Rules Triggers:** A section with a green checkmark icon and a 'Show rule action' checkbox. It lists '3 Rules on route (applied in the order shown)'. The rules are:
 

Rules	Rule Type
1. <input type="checkbox"/> Drop Messages Containing a Virus Drop the message	Virus
2. <input type="checkbox"/> Encryption or decryption fails Hold in Encryption or decryption failures area	Error
3. <input type="checkbox"/> Hold Messages Containing Executables Hold in Executables area	Media Types

To do this:

1. Use the System Center, Encryption, Certificate Store page to ensure that at least one valid PGP or S/MIME certificate is loaded into the store.

2. Use the Mail Encryption Endpoints page to configure the settings for your organization.
  - a. Add the email address of your organization to the **For mail sent to the** area.
  - b. In the **Messages will be encrypted** area:
    - i. Specify whether to **encrypt body and attachments** or **encrypt attachments**.
    - ii. Specify whether to use a **PGP certificate** or **S/MIME certificate** using the drop-down list.
    - iii. You can also choose to sign a message by clicking the **Sign the messages using** checkbox and selecting a certificate from the drop-down list.
3. Use the Mail Policy Route settings in the Policy Center to enable encryption/decryption on a route by applying the Encryption Endpoint defined above.
  - a. Create a new Policy Route or modify an existing Policy Route between the partner and your organization.
  - b. Specify the Default Delivery Action of the Route to use Encryption Endpoints.
  - c. Specify the Default Decryption Action of the Route to decrypt and apply content rules to PGP and S/MIME messages.
  - d. Then add a Content Rule to define the actions if Encryption or Decryption fails.

## 6.4 How do I content check secured emails entering my organization when going to one of the end users?

You can content check secured emails entering your organization when going to one of the end users.

The screenshot shows the 'Modify Policy Route' configuration page in the Clearswift Secure Email Gateway management console. The page is titled 'Modify Policy Route' and includes a navigation menu with options like Home, Policy, Messages, Reports, System, Health, and Users. The main content area is divided into several sections:

- Overview:** A lightbulb icon indicates that the route name is automatically maintained. A button 'Click here to change these settings' is present.
- For Mail Sent:** A table with columns 'From' and 'To'. One entry is visible: 'Legal - External' to 'Legal - Internal'. A 'New' button and pagination controls are also shown.
- Decrypt and Apply Encryption Endpoints:** Two green checkmarks indicate that content rules for PGP and S/MIME messages are applied, and that the default encryption endpoint delivery policy is used. A 'Click here to change these settings' button is present.
- By Default Perform This Disposal Action:** The action is set to 'Deliver the message'. A 'Click here to change these settings' button is present.
- Unless One Of These Content Rules Triggers:** A table lists three rules:
 

Rules	Rule Type
1. <input type="checkbox"/> Drop Messages Containing a Virus Drop the message	Virus
2. <input type="checkbox"/> Encryption or decryption fails Hold in Encryption or decryption failures area	Error
3. <input type="checkbox"/> Hold Messages Containing Executables Hold in Executables area	Media Types

To do this:

1. Use the System Center, Encryption, Certificate Store page to ensure that at least one valid PGP or S/MIME certificate is loaded into the store.
2. Use the Mail Encryption Endpoints page to configure the settings for the end user.
  - a. Add the email address of the end user to the For mail sent to the area.
  - b. In the Messages will be encrypted area:

- i. Specify whether to **encrypt body and attachments** or **encrypt attachments**.
  - ii. Specify whether to use a **PGP certificate** or **S/MIME certificate** using the drop-down list.
  - iii. You can also choose to sign a message by clicking the **Sign the messages using** checkbox and selecting a certificate from the drop-down list.
3. Use the Mail Policy Route settings in the Policy Center to enable encryption/decryption on a route by applying the Encryption Endpoint defined above.
  - a. Create a new Policy Route or modify an existing Policy Route between the external address and the end user.
  - b. Specify the Default Delivery Action of the Route to use Encryption Endpoints.
  - c. Specify the Default Decryption Action of the Route to decrypt and apply content rules to PGP and S/MIME messages.
  - d. Then add a Content Rule to define the actions if Encryption or Decryption fails.

## 6.5 How do I encrypt email and content scan the message?

You can encrypt email at the desktop and content scan the message at the Gateway.

Content scanning is always available if the Clearswift Gateway, alone, does the encryption/decryption. If encryption/decryption is required at the desktop/endpoint, then the appropriate private key(s) need to be installed in the Certificate Store first.

To do this:

1. If appropriate, use the System Center, Encryption, Certificate Store page to ensure that at least one valid PGP or S/MIME certificate is loaded into the store.
  - a. To decrypt messages sent to an internal user you must have their Private Key in the Certificate Store.
2. Use the Mail Encryption Endpoints page to configure the settings for the recipient.
  - a. Add the email address of the recipient to the **For mail sent to the** area.
  - b. In the **Messages will be encrypted** area:
    - i. Specify whether to **encrypt body and attachments** or **encrypt attachments**.
    - ii. Specify whether to use a **password, PGP certificate** or **S/MIME certificate** using the drop-down list.
    - iii. You can also choose to sign a message by clicking the **Sign the messages using** checkbox and selecting a certificate from the drop-down list.
3. Use the Mail Policy Route settings in the Policy Center to enable encryption/decryption on a route by applying the Encryption Endpoint defined above.
  - a. Create a new Policy Route or modify an existing Policy Route.
  - b. Specify the Default Delivery Action of the Route to use Encryption Endpoints.
  - c. Specify the Default Decryption Action of the Route to decrypt and apply content rules to PGP and S/MIME messages.
  - d. Then add a Content Rule to define the actions if Encryption or Decryption fails.

## 6.6 How do I encrypt email and not content scan the message?

You can choose to encrypt email and not content scan the message.

The screenshot shows the 'Modify Policy Route' configuration page in the Clearswift SECURE Email Gateway. The page is titled 'Modify Policy Route' and includes the following sections:

- Overview:** A lightbulb icon and text stating 'The name for this route is automatically maintained. Edit this panel if you would like to supply your own name.' A button 'Click here to change these settings' is present.
- For Mail Sent:** A 'New' button and a table with columns 'From' and 'To'. The table contains one row: 'Legal - External' under 'From' and 'Legal - Internal' under 'To'. A 'Showing 1 - 1 of 1' indicator is visible.
- Apply Encryption Endpoints:** A 'New' button and two checkboxes: 'Do NOT decrypt PGP and S/MIME messages.' (unchecked) and 'By default apply encryption endpoint delivery policy.' (checked). A button 'Click here to change these settings' is present.
- By Default Perform This Disposal Action:** A 'New' button and the text 'Deliver the message'. A button 'Click here to change these settings' is present.
- Unless One Of These Content Rules Triggers:** A 'New' button, a 'Show rule action' checkbox (checked), and a table with 3 rules on route (applied in the order shown):
 

Rules	Rule Type
1. <input type="checkbox"/> Drop Messages Containing a Virus Drop the message	Virus
2. <input type="checkbox"/> Encryption or decryption fails Hold in Encryption or decryption failures area	Error
3. <input type="checkbox"/> Hold Messages Containing Executables Hold in Executables area	Media Types

1. If appropriate, use the System Center, Encryption, Certificate Store page to ensure that at least one valid PGP or S/MIME certificate is loaded into the store.
2. Use the Mail Encryption Endpoints page to configure the settings for the recipient.
  - a. Add the email address of the recipient to the **For mail sent to the** area.
  - b. In the **Messages will be encrypted** area:
    - i. Specify whether to **encrypt body and attachments** or **encrypt attachments**.
    - ii. Specify whether to use a **password, PGP certificate** or **S/MIME certificate** using the drop-down list.

- iii. You can also choose to sign a message by clicking the **Sign the messages using** checkbox and selecting a certificate from the drop-down list.
3. Use the Mail Policy Route settings in the Policy Center to enable encryption/decryption on a route by applying the Encryption Endpoint defined above.
  - a. Create a new Policy Route or modify an existing Policy Route.
  - b. Specify the Default Delivery Action of the Route to use Encryption Endpoints.
  - c. Then add a Content Rule to define the actions if Encryption or Decryption fails.