



# **Implementing the Clearswift SECURE Encryption Portal**

---

Technical Guide

Version 2.0

February 2016

## Implementing the Clearswift SECURE Encryption Portal

## Contents

1	Introduction .....	3
2	How it Works.....	4
3	Configuration Overview .....	5
4	Obtaining a Digital Certificate for Your Email Gateway.....	6
4.1	Creating a Private Key and CSR using OpenSSL .....	6
4.2	Using Your CSR to Purchase a Signed Certificate .....	8
5	What to do when you Receive Your Signed Certificate.....	10
5.1	Importing the Signed Certificate and Private Key Pair.....	10
6	Configuring a TLS Endpoint for the Encryption Portal .....	13
7	Defining the Encryption Portal as a Relay Server .....	16
8	Adding the Encryption Portal as an Internal Email Server .....	17
9	Creating an Encryption Portal Notifications Content Rule .....	18
10	Configuring a Mail Policy Route for Notifications from the Encryption Portal..	21
11	Configuring the Appropriate Mail Policy Routes and/or Content Rules.....	23
11.1	Relaying Email to the Encryption Portal Using Mail Policy Routes .....	23
11.2	Relaying Email to the Encryption Portal Using Content Rules .....	25
12	Finished .....	27
	Appendix A - Glossary .....	28
	Appendix B – Using WinSCP.....	29

## Implementing the Clearswift SECURE Encryption Portal

### 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.

Your email can be encrypted using the following methods:

- Transport Layer Security (TLS)
- Password encryption
- PGP
- S/MIME
- Portal based encryption

This document focuses on configuring portal based encryption. If you wish to learn how to configure the other encryption options on the Clearswift SECURE Email Gateway, please refer to the following documents available from:

<http://www.clearswift.com/resources/setup-and-configuration>

- Implementing TLS on the Clearswift SECURE Email Gateway
- Implementing Encryption on the Clearswift SECURE Email Gateway

You can use the Clearswift SECURE Encryption Portal in conjunction with the Email Gateway to offer encryption based on:

- Mail policy routes – Who the message is going to
- Content rules – The detection of certain content within a message (e.g. confidential material, a particular file type, etc.)

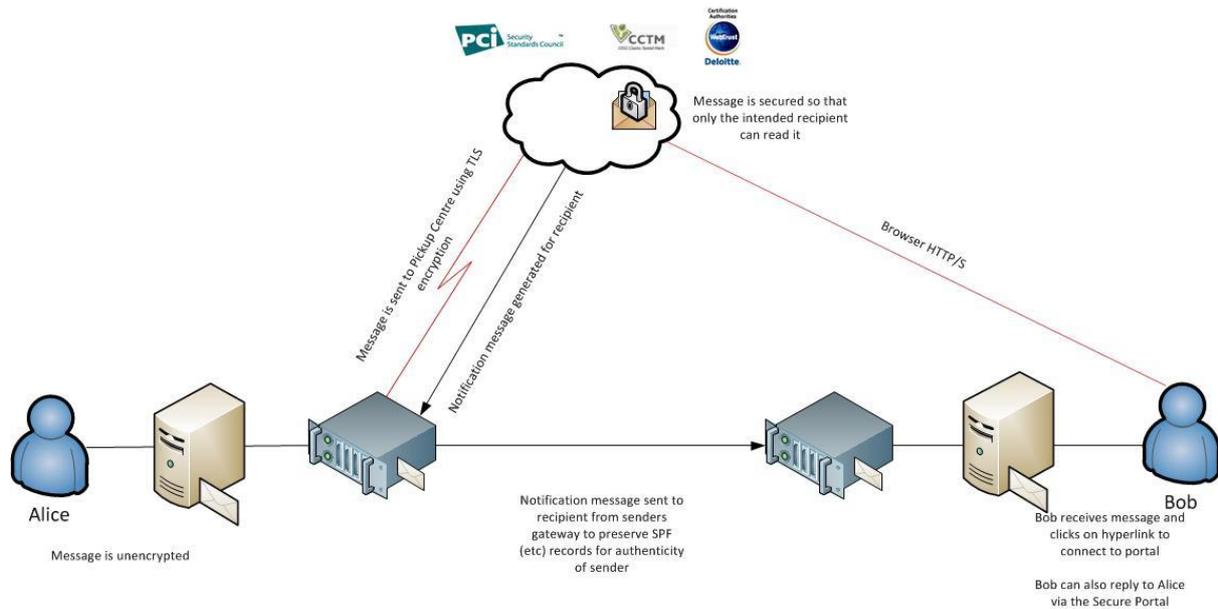
Please note that you will need to contact your Clearswift representative in order to activate the Clearswift SECURE Encryption Portal and obtain the appropriate configuration information.

## Implementing the Clearswift SECURE Encryption Portal

## 2 How it Works

The following diagram explains how the Clearswift SECURE Encryption Portal can be used in conjunction with the Clearswift SECURE Email Gateway to send encrypted messages to recipients outside your organization.

### Secure Encryption Portal



1. Email Gateway routes email to the Encryption Portal via a TLS connection
2. Encryption Portal generates a notification message to the recipient and sends it to the Email Gateway
3. Email Gateway routes notification message to the recipient (to preserve SPF records, etc.)
4. Recipient receives message informing them they have been sent an encrypted message and clicks on hyperlink to access it
5. Recipient connects to Encryption Portal using HTTPS and views email
6. Encryption Portal generates a read notification message to the sender and sends it to the Email Gateway
7. Email Gateway routes read notification message to the sender
8. Recipient can reply to sender from within the Encryption Portal

### 3 Configuration Overview

There are a number of steps that you need to perform to configure your Clearswift SECURE Email Gateway to use the Clearswift SECURE Encryption Portal.

- Obtain the IP address of the Encryption Portal from your Clearswift representative
- Obtain a digital certificate for your Email Gateway
- Configure a TLS endpoint for the Encryption Portal
- Define the Encryption Portal as a relay server
- Add the Encryption Portal as an internal email server
- Create a content rule to detect and deliver notifications from the Encryption Portal
- Configure a Mail Policy Route for password reset notifications from the Encryption Portal
- Configure the appropriate mail policy routes and/or content rules to route suitable emails through the Encryption Portal

## 4 Obtaining a Digital Certificate for Your Email Gateway

The Email Gateway must use TLS to communicate with the Encryption Portal. Therefore, you need to obtain a digital certificate (suitable for SMTP TLS communication) from a Certificate Authority (CA) such as VeriSign, Entrust, Thawte, etc.

This section briefly explains how to obtain a digital certificate. For an in depth discussion on how to configure TLS on your Email Gateway, please refer to the "Implementing TLS on the Clearswift SECURE Email Gateway" guide available from: <http://www.clearswift.com/resources/setup-and-configuration>

### 4.1 Creating a Private Key and CSR using OpenSSL

You need to begin by creating a private key and Certificate Signing Request (CSR) pair.

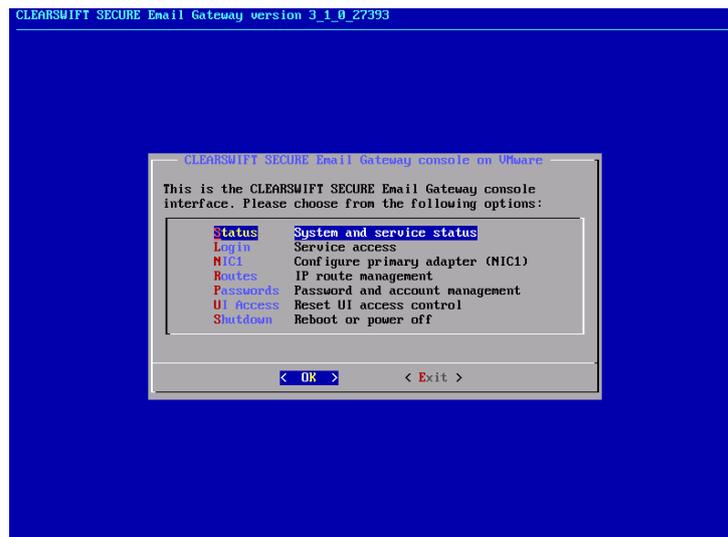
To do this from the Email Gateway's command line:

1. Log in to your Email Gateway via SSH or a KVM (Keyboard - Video - Mouse) connection.
2. When prompted, enter **console** for the username followed by the password you created during the initial Email Gateway set-up.

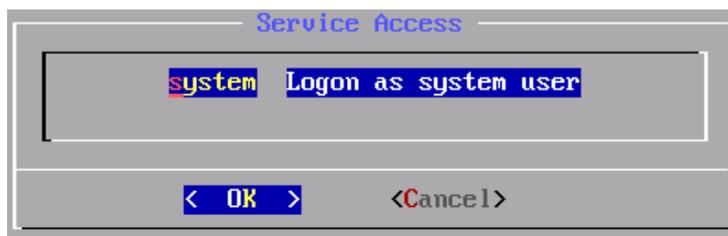
```
emailgateway01.examplecompany.org login: console  
Password:
```

3. Choose **Login** from the Clearswift SECURE Email Gateway console menu and then select **OK**.

## Implementing the Clearswift SECURE Encryption Portal



4. Choose **system** from the Service Access menu and then select **OK**.



5. Enter the password for the system account and then press **Enter**.
6. Enter **sudo su -** and then press **Enter**.

```
# sudo su -
Password:
#
```

7. Enter the password for the system account and then press **Enter**.
8. Enter **openssl genrsa -out emailgateway.key 2048** and then press **Enter**.
  - a. This command generates a 2048 bit RSA private key and stores it in the file `emailgateway.key`. The key must be kept safe as it is used in conjunction with the signed certificate as detailed later in this document.
9. Enter **openssl req -new -key emailgateway.key -out emailgateway.csr** and then press **Enter**.

## Implementing the Clearswift SECURE Encryption Portal

## 10. Complete the CSR with the relevant details.

```
# openssl req -new -key emailgateway.key -out emailgateway.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:Berks
Locality Name (eg, city) []:Theale
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Clearswift
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:emailgateway01.clearswift.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
# _
```

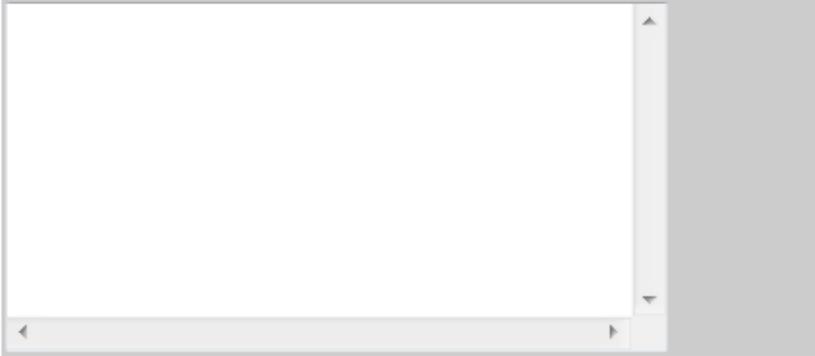
11. A public/private key pair has now been created.
  - a. emailgateway.key – Is the private key used for decryption and should be stored locally on the Email Gateway.
  - b. emailgateway.csr – Is the CSR used for certificate enrolment.
12. You can use a utility such as WinSCP to copy the private key and CSR off the Email Gateway. Please refer to “Appendix B – Using WinSCP” for information on how to do this.

## 4.2 Using Your CSR to Purchase a Signed Certificate

To obtain your signed certificate for use within the Email Gateway, the CSR created in the previous section must be submitted to your chosen Certificate Authority (e.g. VeriSign, Entrust, Thawte, etc.).

An example of a typical Certificate Authority SSL submission form is displayed below.

## Implementing the Clearswift SECURE Encryption Portal

1. Copy and paste your CSR into this box:	
2. Select the server software used to generate the CSR:	Apache-ModSSL
3. Select the validity period for your Certificate:	<input checked="" type="radio"/> 90 days

**Please note that you should consult your CA before purchasing the certificate to ensure that it is suitable for SMTP TLS communication.**

Paste the contents of the CSR in the first window. If the CSR was created on the Gateway using OpenSSL, Apache-ModSSL can generally be used (consult your CA first) as the server software option.

Once submitted, the CA will usually send instructions via email explaining how to download the signed and root certificates.

It is important to ensure that you download both the signed certificate and the CA's root certificate, as you'll need both of them later in this process.

## 5 What to do when you Receive Your Signed Certificate

For the Clearswift SECURE Email Gateway to be able to use TLS it must be enabled within the web interface and the following items imported:

- The private key and signed certificate to use when acting as a TLS client.
- The private key and signed certificate to use when acting as a TLS server.
- The CA's root certificate.

### 5.1 Importing the Signed Certificate and Private Key Pair

1. Copy the **root certificate**, **emailgateway.crt** and **emailgateway.key** to a machine that is connected to the Email Gateway web user interface.
2. From within the web user interface, click on the **System** tab.
3. Click on **Encryption**.

Local administrator (admin) | Logout

Home Policy Messages Reports System Health Users

Home | System Center | Encryption

### Encryption

This page brings together all of the message encryption settings for your Gateway.

#### Configuration

- Certificate Store**  
Manage certificates and keys.
- Key Server Queries**  
Manage key server queries.
- Mail Encryption Endpoints**  
Define the encryption endpoints for messages that should be delivered securely.
- Encryption/Decryption Defaults**  
Define the default encryption and decryption options.

#### TLS Management

- TLS Certificates & Private Keys**  
Manage the certificates and keys used for TLS.
- TLS Endpoints**  
Manage the settings for each TLS end point.

4. Click on **TLS Certificates & Private Keys** in the TLS Management section.
5. Ensure that **Use TLS Communications** is enabled by highlighting the section, clicking on **Click here to change these settings** and selecting the **Use TLS where possible** checkbox.

#### Use TLS Communications



Use TLS where possible. The precise use of TLS will depend on the TLS endpoints configured.

[Click here to change these settings](#)

## Implementing the Clearswift SECURE Encryption Portal

6. Edit the Signing Certificate section and add the CA certificate by browsing to the folder where the **root certificate** was placed.

### Signing Certificate

Select the PEM file to upload. For more information about PEM files and how to get create or acquire them, please see the online documentation.

Certificate :

7. Edit the Server Certificate and Private Key section and add both the certificate and key to the appropriate sections by browsing to the folder where you placed **emailgateway.crt** and **emailgateway.key**.

### Server Certificate and Private Key

[Click here to change these settings](#)

Select the PEM files to upload. For more information about PEM files and how to get create or acquire them, please see the online documentation.

Certificate :

Private Key :

8. Edit the Client Certificate and Private Key section and add both the certificate and key to the appropriate sections by browsing to the folder where you placed **emailgateway.crt** and **emailgateway.key**.

### Client Certificate and Private Key

Select the PEM files to upload. For more information about PEM files and how to get create or acquire them, please see the online documentation.

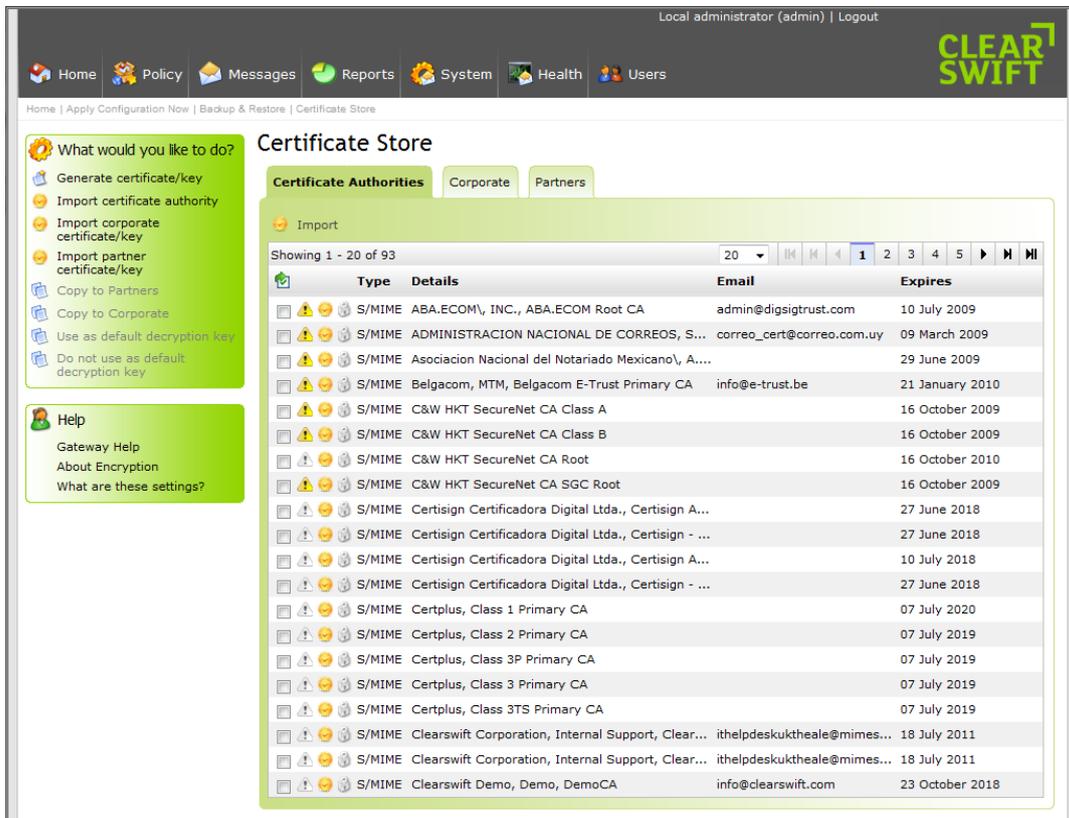
Certificate :

Private Key :

9. Click on the **System** tab.
10. Click on **Encryption**.

Implementing the Clearswift SECURE Encryption Portal

11. Click on **Certificate Store**.



12. Click on **Import**.

13. Browse to **CA.crt** and then click on the **Import** button.



## 6 Configuring a TLS Endpoint for the Encryption Portal

You now need to define a TLS Endpoint for the Encryption Portal. While the Email Gateway supports Opportunistic TLS, Clearswift recommends that you explicitly define the Encryption Portal as a TLS Endpoint. This ensures that all communication with the Encryption Portal is conducted using TLS.

To define the Encryption Portal as a TLS Endpoint:

1. Click on the **System** tab.
2. Click on **Encryption**.
3. Click on **TLS Endpoints**.
4. Click on **New**.
5. In the Overview area, click on **Click here to change these settings**.
6. Enter the following in the Name field: **Encryption Portal**
7. Click on the **Save** button.

### Overview

Encryption Portal

[Click here to change these settings](#)

8. In the When Acting as a Client area, click on **Click here to change these settings**.
9. In the General area:
  - a. Tick the **Encryption should meet or exceed** check box and enter: **256**
  - b. Tick the **If a certificate is received it must validate** check box.
10. In the Certificate Subject Validation area:
  - a. Tick the **CN of the certificate must match** check box and enter: **securemail.clearswift.com**
  - b. Tick the **DN of the certificate must match** check box and enter: **/OU=Go to https://www.thawte.com/repository/index.html/OU=Thawte SSL123 certificate/OU=Domain Validated/CN=securemail.clearswift.com**
11. In the Certificate Issuer Validation area:
  - a. Tick the **DN of the certificate issuer must match** check box and enter: **/C=US/O=Thawte, Inc./OU=Domain Validated SSL/CN=Thawte DV SSL CA**
12. Click on the **Save** button.

## Implementing the Clearswift SECURE Encryption Portal

[Click here to change these settings](#)

### When Acting as a Client

**General**

- Encryption should meet or exceed 256 bits.
- If a certificate is received it must validate.

**Certificate Subject Validation**

- CN of the certificate subject must match 'securemail.clearswift.com'
- DN of the certificate subject must match '/OU=Go to https://www.thawte.com/repository/index.html/OU=Thawte SSL123 certificate/OU=Domain Validated/CN=securemail.clearswift.com'

**Certificate Issuer Validation**

- DN of the certificate issuer must match '/C=US/O=Thawte, Inc./OU=Domain Validated SSL/CN=Thawte DV SSL CA'

13. In the When Acting as a Server area, click on **Click here to change these settings**.

14. In the General area:

- a. Tick the **Encryption should meet or exceed** check box and enter: **128**
- b. Do not tick the **Request a certificate from the client** check box.
- c. Do not tick the **If a certificate is received it must validate** check box.

15. In the Certificate Subject Validation area:

- a. Do not tick the **CN of the certificate must match** check box.
- b. Do not tick the **DN of the certificate must match** check box.

16. In the Certificate Issuer Validation area:

- a. Do not tick the **DN of the certificate issuer must match** check box.

17. Click on the **Save** button.

[Click here to change these settings](#)

### When Acting as a Server

**General**

- Encryption should meet or exceed 128 bits.
- Do not request a certificate from the client.
- If a certificate is received ignore the validity.

**Certificate Subject Validation**

- Do not check the CN of the certificate subject
- Do not check the DN of the certificate subject

**Certificate Issuer Validation**

- Do not check the DN of the certificate issuer

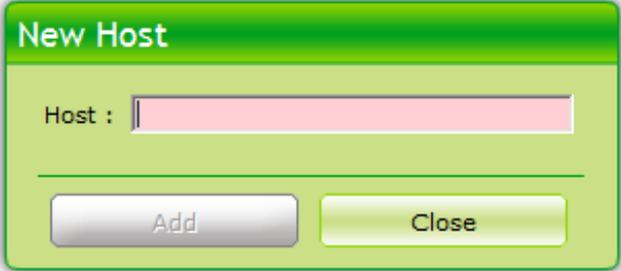
18. Click on the **Hosts** tab.

19. Click on **New**.

20. Enter the following in the Host field: ***IP address of the Encryption Portal – provided by your account manager***

## Implementing the Clearswift SECURE Encryption Portal

21. Click on the **Add** button.



The image shows a 'New Host' dialog box with a green header. Below the header is a text input field labeled 'Host :'. At the bottom of the dialog are two buttons: 'Add' and 'Close'.

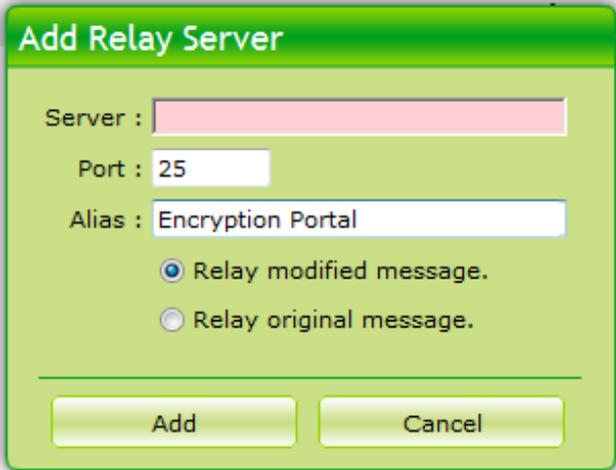
22. Click on the **Close** button to dismiss the New Host dialog.

## 7 Defining the Encryption Portal as a Relay Server

In order to route traffic to the Encryption Portal, you first need to define it as a relay server. You can then reference this relay server in the appropriate mail policy routes and content rules.

To define the Encryption Portal as a relay server:

1. Click on the **Policy** tab.
2. Click on **Disposal Actions**.
3. Click on the **Relay Servers** tab.
4. Click on **New**.
5. In the Add Relay Server dialog box:
  - a. Enter the following in the Server field: ***IP address of the Encryption Portal – provided by your account manager***
  - b. Enter the following in the Port field: **25**
  - c. Enter the following in the Alias field: **Encryption Portal**
  - d. Select the **Relay modified message** radio button.
  - e. Click on the **Add** button.



The screenshot shows a dialog box titled "Add Relay Server". It has a green header bar. Below the header, there are three input fields: "Server" (with a pink highlight), "Port" (containing "25"), and "Alias" (containing "Encryption Portal"). Below the input fields, there are two radio buttons: "Relay modified message." (selected) and "Relay original message.". At the bottom of the dialog, there are two buttons: "Add" and "Cancel".

At the time of writing, the default server names for the encryption portals are

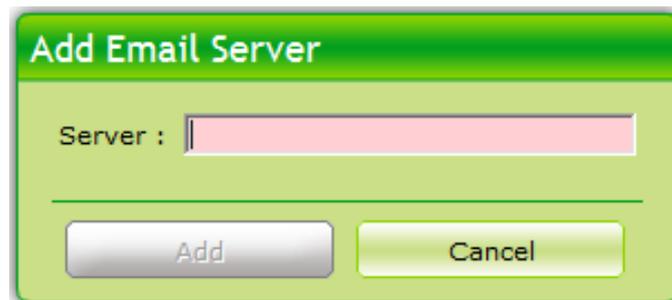
1. Securemail.Clearswift.Com - Rest of the world customers
2. Securemail2.Clearswift.Com - North American customers

## 8 Adding the Encryption Portal as an Internal Email Server

The Encryption Portal sends notification messages to your Email Gateway for onward routing to the external recipients. To ensure that these messages are delivered, you need to define the Encryption Portal as an internal email server.

To define the Encryption Portal as an internal email server:

1. Click on the **System** tab.
2. Click on **SMTP Settings**.
3. Click on **Internal Email Servers**.
4. Click on **New**.
5. In the Add Email Server dialog box:
  - a. Enter the following in the Server field: ***IP address of the Encryption Portal – provided by your account manager***
  - b. Click on the **Add** button.



At the time of writing, the IPs for the encryption portals are

UK Site (Securemail.clearswift.com)

1. 94.236.18.49
2. 94.236.18.51
3. 94.236.21.41

US Site (Securemail2.clearswift.com)

1. 184.106.34.97
2. 184.106.34.99
3. 184.106.34.101
4. 184.106.34.156

## 9 Creating an Encryption Portal Notifications Content Rule

In order to protect your SPF records, etc. the Encryption Portal sends all notification messages back to your Email Gateway to be forwarded onto the recipients.

The majority of the notification messages will be sent using from your internal domain(s). To prevent these notification messages looping back to the Encryption Portal, you need to:

- Create a content rule that detects certain phrases used within the notification messages
- Apply this content rule to any mail policy routes that route messages to the Encryption Portal

To do this:

1. Click on the **Policy** tab.
2. Click on **Lexical Expressions**.
3. Click on **New**.
4. In the Overview area, click on **Click here to change these settings**.
5. Enter the following in the Name field: **Detect Encryption Portal Notification**
6. Click on the **Save** button.



7. In the Expressions area, click on **New**.
8. In the New Expression dialog box:
  - a. Select **Simple Expression** from the Expression Type drop down list.
  - b. Select **Instant** from the If matched drop down list.
  - c. Enter the following in the Expression field: **y**
  - d. Ensure that the **Case sensitive** check box is not ticked.
  - e. Click on the **Add** button.



## Implementing the Clearswift SECURE Encryption Portal

9. Click on the **Policy** tab.
10. Click on **Content Rules**.
11. Click on **New**.
12. In the Overview area, click on **Click here to change these settings**.
13. Enter the following in the Name field: **Detect Encryption Portal Notification**
14. Click on the **Save** button.

### Overview

Detect Encryption Portal Notification

[Click here to change these settings](#)

15. In the Lexical Expression area, click on **Click here to change these settings**.
  - a. Ensure that only the **Specific message header(s)** check box is ticked.
  - b. Click on the **Add** button.
  - c. In the Add a message header dialog box, enter the following in the Header field: **x-echoworx-emx-notification-type**
  - d. Click on the **Add** button.
  - e. Select **Detect Encryption Portal Notification** from the Expression list drop down list.
  - f. Click on the **Save** button.

### What To Look For?

In order for this content rule to trigger the test conditions detailed on this panel must be met by the message being processed. If the conditions are met, then the collection of actions described within the 'What to do?' panel will be carried out.

#### Lexical Expression

If the '**Detect Encryption Portal Notifications**' expression list scores **at least 10** in one of

- Specific message header '**x-echoworx-emx-notification-type**'

Document options (where applicable) :

- Scan body
- Scan header and footer
- Scan properties

[Click here to change these settings](#)

#### And Which Media Types

- If any of the detectable media types are detected.

[Click here to change these settings](#)

#### And Size Restriction Of

No size restriction will be applied to this content rule.

[Click here to change these settings](#)

16. Ensure that the Disposal Action for the content rule is to **Deliver the message**.

## Implementing the Clearswift SECURE Encryption Portal

### What To Do? New

If the conditions in the **'What to Look For?'** panel are met then the actions defined in this panel will be carried out.

#### Disposal Action

- Deliver the message

[Click here to change these settings](#)

17. This content rule must be added to all mail policy routes that forward emails to the Encryption Portal. If you use a content rule to detect messages that should be forwarded to the Encryption Portal, the **Detect Encryption Portal Notification** content rule must be positioned before this content rule.

## 10 Configuring a Mail Policy Route for Notifications from the Encryption Portal

The Encryption Portal sends password reset notifications from a specific email address. To prevent your Email Gateway from rejecting these notifications, you need to:

- Create an Address List containing the sending email address:
  - UK portal: [clearswiftemx@clearswift-uk.ips.emailprivacy.net](mailto:clearswiftemx@clearswift-uk.ips.emailprivacy.net)
  - US portal: [clearswiftemx@clearswift-us.ips.emailprivacy.net](mailto:clearswiftemx@clearswift-us.ips.emailprivacy.net)
- Create a Mail Policy Route to deliver emails coming from this address

To do this:

1. Click on the **Policy** tab.
2. Click on **Email Addresses**.
3. Click on **New**.
4. In the Overview area, click on **Click here to change these settings**.
  - a. Enter the following in the Name field: **Encryption Portal Notifications**
  - b. Click on the **Save** button.



5. Click on **New**.
  - a. Enter one of the following in the Email Address field:
    - i. UK portal: **clearswiftemx@clearswift-uk.ips.emailprivacy.net**
    - ii. US portal: **clearswiftemx@clearswift-us.ips.emailprivacy.net**
  - b. Click on the **Update** button.
6. Click on the **Policy** tab.
7. Click on **Mail Policy Routes**.
8. Click on **New**.
9. In the For Mail Sent area, click on **Click here to change these settings**.
  - a. In the From area, select:
    - i. **Encryption Portal Notifications**
  - b. In the To area, select:
    - i. **Anyone**
    - ii. **My Company**
  - c. Click on the **Save** button.

## Implementing the Clearswift SECURE Encryption Portal

### For Mail Sent

From : Encryption Portal Notifications  
To : My Company, Anyone

[Click here to change these settings](#)

10. Ensure that the Default Disposal Action for this route is to **Deliver the message**.

### By Default Perform This Disposal Action

Deliver the message

[Click here to change these settings](#)

11. Add the appropriate content rules to the mail policy route.
  - a. Note: You must add the **Detect Encryption Portal Notification** content rule.



12. This policy route should be positioned towards the top of your Manage Policy Routes table to ensure that the password reset notifications are routed appropriately.

## 11 Configuring the Appropriate Mail Policy Routes and/or Content Rules

You can now configure your policy to route the appropriate emails to the encryption portal. To achieve this, you can use:

- Mail policy routes – Who the message is being sent from/going to
- Content rules – The detection of certain content being present in the message (e.g. confidential material, a particular file type, etc.)

### 11.1 Relaying Email to the Encryption Portal Using Mail Policy Routes

To relay emails to the Encryption Portal based upon the sender/recipient email address:

1. Click on the **Policy** tab.
2. Click on **Email Addresses**.
  - a. Create the appropriate address list(s) for one or both of the following:
    - i. Internal senders whose outgoing emails must be sent via the Encryption Portal.
    - ii. External recipients whose emails must be sent via the Encryption Portal.
3. Click on the **Policy** tab.
4. Click on **Mail Policy Routes**.
5. Click on **New**.
6. In the For Mail Sent area, click on **Click here to change these settings**.
7. In the From and To areas, select the appropriate address lists (e.g. My Company to Portal Recipients).

#### For Mail Sent

From : My Company  
To : Portal Recipients

[Click here to change these settings](#)

8. In the By Default Perform This Disposal Action area, click on **Click here to change these settings**.
  - a. Select the **Relay modified message to Encryption Portal [*IP address of the Encryption Portal:25*]** option from the drop down list.
  - b. Click on the **Save** button.

## Implementing the Clearswift SECURE Encryption Portal

### By Default Perform This Disposal Action

Relay modified message to **Encryption Portal [94.236.21.41:25]**

[Click here to change these settings](#)

9. Add the appropriate content rules to the mail policy route.
  - a. Note: You must add the **Detect Encryption Portal Notification** content rule.

### Unless One Of These Content Rules Triggers New

Show rule action

7 Rules on route (applied in the order shown)

<input checked="" type="checkbox"/> Rules	Virus	Spam	Content	Other
1. <input type="checkbox"/> Hold Messages Containing a Virus and Inform the Administrator and Sender Hold in <b>Virus</b> area	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> 
2. <input type="checkbox"/> Hold Messages Containing Encrypted Files and Inform the Administrator and Sender Hold in <b>Encrypted</b> area	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> 
3. <input type="checkbox"/> Hold Messages Containing an Unrecognised Media Type Hold in <b>Unknown Binary</b> area	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> 
4. <input type="checkbox"/> Add Legal Disclaimer Perform no action	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> 
5. <input type="checkbox"/> Detect Encryption Portal Notifications Deliver the message	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 
6. <input type="checkbox"/> Fail to Modify a Message Hold in <b>Message Processing Failure</b> area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> 
7. <input type="checkbox"/> Fail to Process a Message Hold in <b>Message Processing Failure</b> area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> 

## 11.2 Relaying Email to the Encryption Portal Using Content Rules

To relay emails to the Encryption Portal based upon the content of a message, you need to create content rule(s) to scan for the appropriate content. For example, you may wish to use the Encryption Portal for emails containing a specific word or phrase.

1. Click on the **Policy** tab.
2. Click on **Lexical Expressions**.
3. Create a new lexical expression list that contains the words/phrases you wish to search for.

The screenshot displays the Clearswift Policy Center interface. At the top, the user is logged in as 'Local administrator (admin)'. The navigation menu includes Home, Policy, Messages, Reports, System, Health, and Users. The current page is 'Manage Lexical Expression Lists'. A sidebar on the left offers options like 'Changes Made', 'What would you like to do?' (with sub-options: Delete the Expression List, New expression, Import expressions, Manage Content Rules), and 'Help'. The main content area shows an 'Overview' section with a warning 'This item is not being used within the policy.' and an 'Expressions' table. The table has columns for 'Weight' and 'Expression' and contains one entry: 'Instant' with the expression 'Confidential health record'.

Weight	Expression
Instant	Confidential health record

4. Click on the **Policy** tab.
5. Click on **Content Rules**.

## Implementing the Clearswift SECURE Encryption Portal

6. Create a content rule that references the above lexical expression list and contains the primary disposal action **Relay modified message in the clear to Encryption Portal [IP address of the Encryption Portal:25]**.

Local administrator (admin) | Logout

Home Policy Messages Reports System Health Users

Manage Policy Routes | Modify Policy Route | Manage Lexical Expression Lists | Modify Expression List | Manage Content Rules | Edit Content Rule

**Changes Made**  
Click here to apply the changes made to the configuration.

**What would you like to do?**  
Add a 'What to do' action...  
Create a copy of this rule  
Delete the content rule  
Manage Mail Policy Routes

**Help**  
Gateway Help

**This Content Rule has not been applied to a policy route.**  
[Click here to change these settings](#)

**Overview**  
Detect Encryption Portal Terms  
[Click here to change these settings](#)

**What To Look For?**  
In order for this content rule to trigger the test conditions detailed on this panel must be met by the message being processed. If the conditions are met, then the collection of actions described within the 'What to do?' panel will be carried out.

**Lexical Expression**  
[Click here to change these settings](#)

If the '**Detect Encryption Portal Terms**' expression list scores **at least 10** across

- The message body.
- The subject line.
- The attachments matching the conditions in the other clauses.

Additional options :

- Combine the scores from all message parts that the expression list is applied to.

**And Which Media Types**  
[Click here to change these settings](#)

- If any of the detectable media types are detected.

**And Size Restriction Of**  
[Click here to change these settings](#)

No size restriction will be applied to this content rule.

**What To Do?** [New](#)  
If the conditions in the '**What to Look For?**' panel are met then the actions defined in this panel will be carried out.

**Disposal Action**  
[Click here to change these settings](#)

- Relay modified message to **Encryption Portal [94.236.21.41:25]**

7. Apply the new content rule to the appropriate mail policy route(s).
8. Add the **Detect Encryption Portal Notification** content rule to the same mail policy route(s). This content rule must be positioned before the content rule that relays messages to the Encryption Portal.



## **12 Finished**

Once you have applied these changes to your Clearswift SECURE Email Gateway, the appropriate email traffic should be routed to the Clearswift SECURE Encryption Portal.

## Appendix A - Glossary

- CA - Certificate Authority (e.g. VeriSign, Entrust, Thawte, etc.) that issues digital certificates
- CN – Common Name
- CSR - Certificate Signing Request
- DN – Distinguished Name
- PGP - Pretty Good Privacy, a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication
- Private Key – Used to decrypt a message that has been encrypted using the corresponding public key
- Public Key - Used to transform a message into an unreadable form
- Root Certificate - Either an unsigned public key certificate, or a self-signed certificate that identifies the CA
- S/MIME - Secure/Multipurpose Internet Mail Extensions, a standard for public key encryption and signing of MIME data
- SSH - Secure Shell, a network protocol for remote administration of Unix computers
- TLS Client – Initiates the TLS connection
- TLS Server – Recipient of a request to initiate a TLS connection
- TLS – Transport Layer Security

## Appendix B – Using WinSCP

To copy files off the Clearswift SECURE Email Gateway:

1. Download and Install WinSCP from: <http://winscp.net/eng/download.php>
2. On the Email Gateway, click on the **System** tab.
3. Click on **System Settings**.
4. Click on **SSH Access**.
5. In the Settings area, click on **Click here to change these settings**.
6. Tick the **Enable network access to the Console via SSH for these IP addresses** check box.
7. Enter the IP address of the machine where you installed WinSCP.

Local administrator (admin) | Logout

Home Policy Messages Reports System Health Users

Home | System Center | System Settings | SSH Access

**Changes Made**  
Click here to apply the changes made to the configuration.

**What would you like to do?**  
Traceroute to a host

**Help**  
Gateway Help  
When should I use these settings?

### SSH Access

Care should be taken when enabling network access to the Console via SSH, in order to reduce the associated potential security risks. We do not advise leaving SSH access enabled for long periods.

**Enabling this feature exposes protocols not typically required for day to day operation.**  
SSH access should only be enabled as directed by your support provider.

### Settings

Enable network access to the Console via SSH for these IP addresses :

IP Address	Notes (optional)
1. 192.168.250.99	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

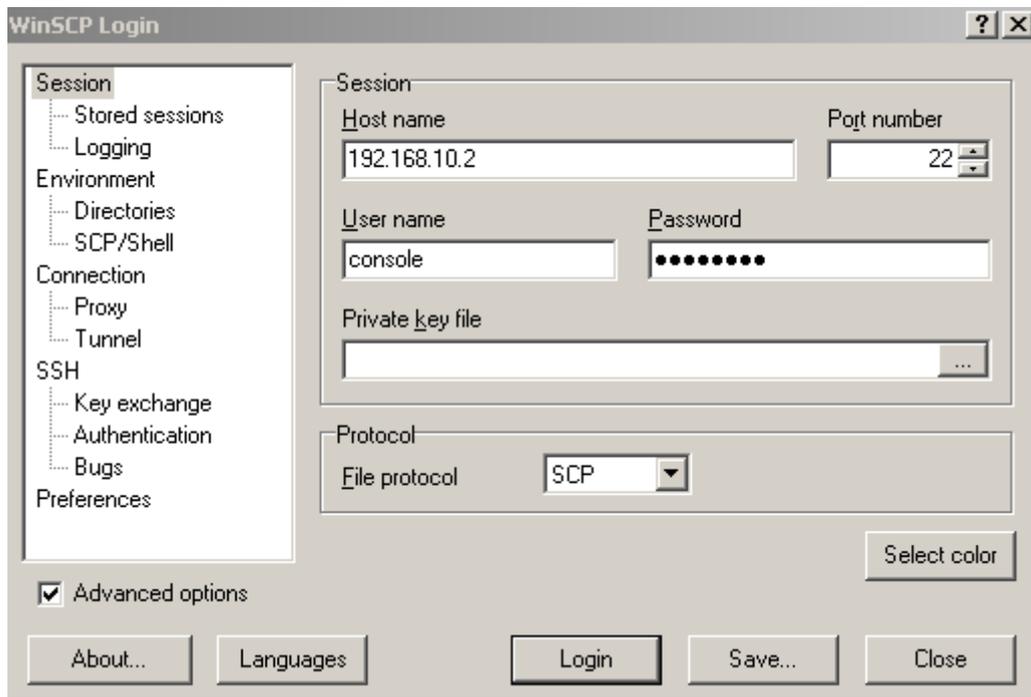
Save Cancel

Copyright ©2005-2011 Clearswift Ltd. (3\_3\_1\_33320)

8. Run WinSCP and click on **New**.
9. Enter the IP address of the Email Gateway in the Host name field,
10. Enter **console** in the User name field.
11. Enter the password for the console account.
12. Select **SCP** from the File protocol drop down list.

Implementing the Clearswift SECURE Encryption Portal

13. Click on the **Login** button.



14. You can now copy the appropriate files from the /home/console directory on the Email Gateway to your local machine.

