Clearswift SECURE Email Gateway
Version 3.2
Evaluation Guide
Revision 1.0
Introduction

Thank you for taking the time to evaluate Clearswift SECURE Email Gateway.

Modern business simply couldn’t function without email. However, both incoming and outgoing messages can pose significant risks to the security of company networks and confidentiality. It is therefore vital that an organisation’s email gateway is able to mitigate spam, neutralise viruses and prevent data leaks without hindering the free flow of messages.

The Clearswift SECURE Email Gateway is a trusted email gateway security solution that gets the balance right.

This evaluation guide explores and explains some of the many benefits of the SECURE Email Gateway. Rather than overwhelm you with an in-depth analysis of every feature our intention is to present the essential information that will allow you to continue to explore and evaluate SECURE Web Gateway at your own pace.

Note that this guide assumes that you have already followed the Clearswift SECURE Email Gateway Getting Started Guide. As such, you should have completed the Initial Setup Wizard and be able to log in to SECURE Email Gateway. If this is not the case then the Getting Started Guide can be found on the Technical Guides area of the Clearswift website - please read it before proceeding.

We’ll start with a brief overview of what you can expect to see - the user interface. As that’s a bit of a mouthful, we’ll call it the ‘UI’ from hereon. Here’s an overview of what we’ll cover:

- Defining an anti-spam policy for your organisation
- Tailoring anti-spam policy for specific groups or departments
- Blocking unauthorised attachments while allowing the free flow of information
- Performing keyword searches across messages and their attachments
- Safely encrypting email sent to external organisations
The UI

When you first log in you will be presented with this Home page:

The Home page is the starting point for managing SECURE Email Gateway’s features and for implementing and maintaining an effective spam policy for your organisation. It is supported by a further six pages, or Management Centers, displayed as tabs across the top of the GUI - Policy, Message, Report, System, Health and Users. Let’s take a closer look at these...

• The Home page presents an overview of SECURE Email Gateway. It is the first page displayed each time you log in.

• The Policy Center lets you define and maintain an Acceptable Usage Policy (AUP) for your organisation. This involves creating rules to manage information flowing in to and out of your organisation. Use the Policy Center to create rules and ‘routes’ that determine which email addresses and domains are allowed or blocked and who is allowed to send and receive messages.

• The Message Center manages held, or quarantined, email messages. It also offers the ability to run the message-tracking tools, allowing you to trace the paths of any email passing through the SECURE Email Gateway.

• The Report Center provides access to the monitoring capabilities of SECURE Email Gateway. It collates and presents information on the activities of users, including the most popular email domains, the busiest users and the types of attachments sent and received. It can also generate detailed reports on incoming spam and detected viruses.
• The System Center is used to manage some of the more technical aspects of SECURE Email Gateway. The most important settings will have been configured during the Initial Setup Wizard, so there’s not too much to worry about with this Center. However, they can be edited from here at any time.

• The Health Center is the place to view real-time usage information for SECURE Email Gateway. Key metrics available here include such as the spam and virus profiles, SMTP connections, processor usage, system update information and the volume of encrypted/decrypted messages that have been processed.

• The Users Center control access to the aforementioned management Centers. Use it to create new administrative users, allowing access to all or selected Management Centers.

This evaluation guide will focus on the most important Management Centers, offering simple guidelines on making the most of them.

Policy Center

We’ll start by exploring the Policy Center. It is likely that the majority of your of time will be spent here, creating and managing the rules that define the email policy. The good news is that the SECURE Email Gateway comes with a default email policy that can be fine-tuned quickly and easily to meet your organisation’s specific needs.

The policy is defined in SECURE Email Gateway using a combination of content rules, policy ‘routes’ and Clearswift’s TRUSTmanager and SpamLogic technologies to identify and filter 99.5% of spam and prevent malware infections.

In simple terms, content rules examine every message passing through the SECURE Email Gateway, performing a variety of security checks. These rules can be created and reused multiple times to enable the email administrator to manage even complex policies with ease. A plain-English example of a content rule could be written like this: “Detect confidential material in outbound messages and inform IT security personnel”. To view current content rules simply click the Content Tools link.

These content rules become part of policy ‘routes’. So, again in plain English, a route might be thought of along these lines: “Outbound messages from the sales department”. As such, messages can be subjected to different sets of rules dependent on the route through which they’re flowing. Click Mail Policy Routes to see the default settings.

As well, Clearswift’s SpamLogic technology allows for a global spam policy for each SECURE Email Gateway. You might, for example, configure SpamLogic to “reject all messages that come from known spam sources”. For flexibility it is also possible to create a special Spam Content Rule for a particular group of recipients. To explore these options, just click SpamLogic Settings.
Click Mail Zero Hour Malware, meanwhile, to determine how the SECURE Email Gateway will react to attachment-laden messages containing confirmed or suspected malware. It's worth noting at this point that these checks are run early in the sequence of message examination. As such, messages may be rejected or quarantined before the SECURE Email Gateway anti-virus engine is run.

### Content Rules

As noted, Clearswift SECURE Email Gateway uses content rules in conjunction with routes to manage the free flow of information via email. This table describes the available content rule types:

<table>
<thead>
<tr>
<th>CONTENT RULE</th>
<th>DESCRIPTION</th>
<th>USES</th>
<th>CAN CAUSE MESSAGE QUARANTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Disclaimer</td>
<td>Places annotation at the top or bottom of the message body (e.g. ‘Company Disclaimer’)</td>
<td>Message Annotations</td>
<td>No</td>
</tr>
<tr>
<td>Add Disclaimer Conditionally</td>
<td>Places annotation at the top or bottom of the message body (e.g. ‘Company Disclaimer’) based on specified conditions, such as a particular word or phrase being present in or absent from the message</td>
<td>Message Annotations Lexical Expressions</td>
<td>No</td>
</tr>
<tr>
<td>Detect filenames</td>
<td>Checks the message for attached files and then checks if they match the names from a defined list</td>
<td>Filenames</td>
<td>Yes</td>
</tr>
<tr>
<td>Detect Lexical expression</td>
<td>Checks the message for specific words, phrases or patterns against a defined dictionary</td>
<td>Lexical Expressions</td>
<td>Yes</td>
</tr>
<tr>
<td>Detect Spam</td>
<td>Overrides the global spam policy for this particular direction of email traffic</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Detect Virus</td>
<td>Defines the behaviour when a message with a virus is detected. For example, a message subject to this rule may be held or deleted</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Digital Signature Validation</td>
<td>If the message has been digitally signed, this rule checks to see if all or some of the signatures are valid</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Encryption or Decryption Fails</td>
<td>Defines how to process the email if there is a failure when trying to either encrypt or decrypt a message</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Message Modification Fails</td>
<td>Defines how to process the email if there is a failure when trying to modify the message (when adding a disclaimer, for example)</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Message Processing Fails</td>
<td>Defines how to process the email if there is a failure when trying to process the message (when parts of the message are corrupt, for example)</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Message Size Restriction</td>
<td>Defined the behaviour when messages which is over a certain size is processed</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>All traffic</td>
<td>Special rule to force the disposal of a message based purely on who is sending or receiving the message</td>
<td>Disposal actions</td>
<td>Yes</td>
</tr>
<tr>
<td>Detect unacceptable images</td>
<td>Checks message to see if they contain images that have either been dynamically classified as unacceptable or whether the System Administrator has preclassified them as acceptable or unacceptable</td>
<td>Pre-classified images defined in Policy &gt; ImageLogic</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Content rules are constructed using items from the content reference sections in order to define the detailed part of the security check that is being performed on that message.

These base rules can be re-used throughout the policy. It is advisable when creating the rules to use sensible names as it will make the Acceptable Use Policy self-documenting.

Policy Routes
When a message is received by the SECURE Email Gateway it is processed against the security policy in the following order:

1. [optional] Global spam policy
2. [optional] Global anti-malware checks
3. Identify most appropriate policy route based on sender and recipient of that message. Then...
   a. Process message using each content rule in that policy route
   b. Determine the outcome for the message dependent on the triggered rules

Policy routes are listed in a table format, which the SECURE Email Gateway processes from top to bottom. The first route that provides a match for the sender and recipient email addresses will be evaluated. If no route is matched, a final 'catch-all' route is used to define the default actions for the message.

Spam and Malware Policy

<table>
<thead>
<tr>
<th>Action</th>
<th>From</th>
<th>To</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Non-deliver message</td>
<td>Anyone</td>
<td>Competitors</td>
<td></td>
</tr>
<tr>
<td>2. Deliver the message</td>
<td>Anyone</td>
<td>Sales</td>
<td>5</td>
</tr>
<tr>
<td>3. Deliver the message</td>
<td>Marketing</td>
<td>Suppliers</td>
<td></td>
</tr>
<tr>
<td>4. Deliver the message</td>
<td>Anyone</td>
<td>Web Based Email</td>
<td>3</td>
</tr>
<tr>
<td>5. Deliver the message</td>
<td>My Company</td>
<td>Anyone</td>
<td>11</td>
</tr>
<tr>
<td>6. Deliver the message</td>
<td>Anyone</td>
<td>My Company</td>
<td>11</td>
</tr>
<tr>
<td>7. Hold in Misrouted Messages</td>
<td>For all email that does not match another route</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Default action for all messages
Address Lists based on manual and LDAP entries defined in the 'Email Addresses' in the Policy Center

Catch-all route. If messages are processed here, then it is likely that you have incorrectly configured the policy routes
Ordering of policy routes is important. Explicit rules should be placed at the top of the list, with less-specific rules below them. Why? Well, consider this following example routing table:

<table>
<thead>
<tr>
<th>ROUTE NUMBER</th>
<th>FROM</th>
<th>TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*@clearswift.com</td>
<td>*@hotmail.com</td>
</tr>
<tr>
<td>2</td>
<td>*@clearswift.com</td>
<td><a href="mailto:bert@hotmail.com">bert@hotmail.com</a></td>
</tr>
<tr>
<td>3</td>
<td><a href="mailto:fred@clearswift.com">fred@clearswift.com</a></td>
<td><a href="mailto:bert@hotmail.com">bert@hotmail.com</a></td>
</tr>
</tbody>
</table>

Remember, routes are process from top to bottom. So, if the SECURE Email Gateway was evaluating messages using this routing table then emails sent from fred@clearswift.com to bert@hotmail.com would match Route 1 right away, and be processed accordingly. In other words, even though Route 3 provides an explicit match it would never be reached because the message would’ve already been picked up by Route 1. But reverse the order of the table (from 1-2-3 to 3-2-1) and the explicit route would be able to do whatever job is required.

Remember, too, that each route has a specific series of rules to be performed against the messages. The order of these rules is similarly important, as they are evaluated from left to right. Consider this example:

At a casual glance, this may seem like an effective route. However, the order of these rules isn’t terribly sensible. The ‘Detect Confidential Material’ rule performs a keyword search on the message body, looking for sensitive words and phrases. But, there is little point performing such a search if the message contains a virus. Messages carrying viruses are likely to be deleted, so performing the keyword search first is a waste of time and resources. By the same token, it is more sensible to add legal disclaimers after all the other rules have been processed. Here, then, is a more efficient order for this particular set of rules:

1. Drop messages containing a virus
2. Detect Confidential Material
3. Detect Credit Card Lexical Expression
4. Add Legal Disclaimer
Message Center

The Message Center is the place to manage held, or quarantined, email messages. As detailed earlier when discussing the SECURE Email Gateway GUI, the Message Center also offers the ability to run the message-tracking tools and identify messages that are pending delivery.

Batch operations allow for mass operations (delete, release etc.) on messages that match a specific search query

Query the tracking history to identify when and how a message was processed

It is possible to create administrator accounts that have privileges sufficient only to manage a subset of the quarantine areas. Similarly, it is access to the SECURE Email Gateway’s message-tracking feature can be restricted. Note that the security for these sections is managed in conjunction with the User Center.

The maximum size of the message areas is dictated only by the amount of free disk space available to the system. The actual number of quarantine areas is also unrestricted. However, it’s worth noting that SECURE Email Gateway is not designed as a message archive. As such, we wouldn’t recommend long-term archival of messages.

Drilling down into a particular area exposes all the messages in that area. To do this, just click the plus ('+') symbol alongside an area. Here, we’ve drilled down into the Confidential area:

Available message handling

Page length

Page controls

It’s possible to drill down still further, to view information about a particular message. To do this, simply double-click the message:
Clearswift SECURE Email Gateway offers a very powerful message-tracking feature, allowing authorised administrators to be able to search the message-processing logs. This is useful for tracking what has happened to a particular message.

When you start Message Tracking you can define your search criteria based on numerous fields such as sender, recipient, subject, sending host, received date and on which gateways the search is to run. Flexible search criteria allow for generic or precise reporting on messages that have been accepted or rejected on this SECURE Email Gateway or one of its peers. Here’s an example search results:

As before, it is possible to drill down to a particular message - just double-click:
Clearswift SECURE Email Gateway includes versatile management and reporting facilities, all controlled from a simple web-based interface. Dozens of ready-made report templates are included and new ones can be created quickly and simply. Better still, SECURE Email Gateway’s reports are interactive: drill down on the fly to get to the data you need quickly and avoid producing useless reports. Here’s what it looks like:
Obvious, most relevant report groups will depend on your organisation. However, here are a few pointers for useful reports that will provide a good place to start your exploration of SECURE Email Gateway’s Report Center:

Top Addresses. Use this group of reports to find the biggest senders of message in your organisation. Note that it’s possible to view reports both on volumes of messages flowing in and out.

Threats Summary. This report, which you’ll find in the Threats group, gives an overall view of the number of messages that have been detected with viruses, spam or other content check.

Message Processing Rates. These reports, found in the General Processing group, can provide an at-a-glance view of peak email sending/receiving times.

Reports can be run by selecting the report and pressing View, or by simply double-clicking the report name.

The provided reports display user activity for all users. It is likely, though, that you’ll want reports to focus on specific user groups or individuals over a specific time periods. Moreover, it is useful to schedule reports for automatic delivery, rather than executing them on a manual basis. As such, we’d advise tweaking some of the report-filtering parameters to create reports tailored for your organisation’s needs. Here, for example, are the parameters for the provided Average Message Processing Lag Per Day report:

Changing a report’s filters is easy. First click to highlight the report that is the closest match for your reporting requirements. Now click Copy to create a copy of the report that can be edited as necessary. To change any of the filter parameters, just click the appropriate tab:

The filter parameters and their meaning should be self-explanatory. Note that in order to generate reports based on domains or address routes; these will obviously need to be created prior to customising a report.

When creating a report notice that its icon changes to include a blue person. Create a report with a schedule and a little clock icon is added, too.
Processing Lag

- Average Message Processing Lag Per Day (count)
- Average Message Processing Lag Per Week by Month (count)

SECURE Email Gateway’s reports are interactive. As such, it is possible to drill down on data to receive a more detailed report. For example, after running the ‘Top Virus Names’ report, clicking on the virus name will run another report to show the list of senders of that particular virus.
The System Center provides access to settings that define how the SECURE Email Gateway operates and how it interacts with components in your existing environment. Here’s what it looks like:

The System Center is split into three sections - Monitoring & Control, Configuration and Appliance Version & License. Let’s explore these in more depth.

**Monitoring and Control**

The Logs & Alarms section allows the administrator to be able to view the logs that been generated by the SECURE Email Gateway. Each log is automatically rolled over at the end of the day and held for 30 days. If you require a longer retention periods, then use the Backup & Restore feature in the System Center or create scripts to move the files off the SECURE Email Gateway installation as and when required.
As well, you can use this section to modify how SECURE Email Gateway handles triggered alerts. By default alerts will be displayed in the GUI. If desired, use the relevant option to send an alarm by email or SNMP.

The Service Control section offers administrators with sufficient privileges the ability to gracefully shut down individual services or the entire SECURE Email Gateway.

**Service Control**

![Service Control GUI](image)

**Current Status**

<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health and System Collector</td>
<td>Started</td>
</tr>
<tr>
<td>Kaspersky Virus Blocking</td>
<td>Started</td>
</tr>
<tr>
<td>LDAP Address Synchronization</td>
<td>Started</td>
</tr>
<tr>
<td>Message Area Manager</td>
<td>Started</td>
</tr>
<tr>
<td>Message Auditor</td>
<td>Started</td>
</tr>
<tr>
<td>Personal Message Management</td>
<td>Started</td>
</tr>
<tr>
<td>Policy Enforcement</td>
<td>Started</td>
</tr>
<tr>
<td>Service watchdog</td>
<td>Started</td>
</tr>
<tr>
<td>SMTP Alert Transport</td>
<td>Started</td>
</tr>
<tr>
<td>SMTP HyperTransport</td>
<td>Started</td>
</tr>
<tr>
<td>SMTP Outbound Transport</td>
<td>Started</td>
</tr>
<tr>
<td>SQL Databases</td>
<td>Started</td>
</tr>
<tr>
<td>user interface</td>
<td>Started</td>
</tr>
</tbody>
</table>

**Shutdown option. Available to administrators with shutdown access rights**

**Configuration**

The majority of the options found in the System Settings section will have already been defined in the Initial Setup Wizard. Should adjustments need to be made when moving the SECURE Email Gateway from a test to a live deployment, though, they will most likely be enacted here:

**IP Address, Subnet, Default Gateway and hostname defined here**

**This section needs to be completed for HTTP access via a proxy**

**SSH is off by default, but can be enabled for a subset of IP addresses**

**Access control to the management interface is defined here**

**Time settings such as NTP server are defined here**

Perhaps obviously, SECURE Email Gateway SMTP configuration is managed in the SMTP Settings section of the product lets you define the SMTP configuration of the product.
The PMM Settings section is the place to configure SECURE Email Gateway’s Personal Message Management (PMM) feature. It’s possible, for instance, to specify the format of the message such as text and company logo and how frequently the users will receive messages showing messages held for them.

The administrator can afford end users control over the delivery of certain emails. Messages identified as spam, for example, could be released if the user determines that the email is in fact legitimate. Alternatively, certain staff may be given the right to release outbound messages that would otherwise be blocked by the SECURE Email Gateway. These PMM features can be enabled on an individual, group or company-wide level. To do this click the Policy tab followed by Manage Disposal Actions.

Enable for PMM

Control what users will be able to self release messages
The pink cells indicate a ‘Full Distribution’. At these times, SECURE Email Gateway will send notifications to all users showing all held messages. The green cells indicate a ‘Partial Distribution’: this generates notifications only for users for whom new messages have been held since the last full distribution.

SECURE Email Gateway also offers the ability for users to add email addresses (including full domains) to a ‘whitelist’, to prevent these messages being held. These options are also managed from this part of the UI.

Clearswift knows that many organisations will deploy more than one SECURE Email Gateway. This affords common policy, common message management and common reporting but the Gateways must first be ‘peered’ together. This is a straightforward process. Simply enter the IP address and user credentials of an additional peer in the Peer Appliances section. Clearswift SECURE Web Gateway devices can also be added to the peer group, allowing policy to be shared and simple administration from a unified interface. Here is what the Peer Appliances section looks like – you’d just click New to add a peer:

The SECURE Email Gateway product is of course very reliable. However, the Backup & Restore section provides a simple way to schedule an automatic backup of policy, system settings and the auditing database to an FTP server. Here’s a typical view:
The_SECURE_Email_Gateway_stores_the_last_20_configurations_online,_each_is_tagged_with_the_reason_why_the_configuration_was_made,_by_whom_and_from_where._Previous_copies_of_policy_cab_easily_be_made_into_the_live_version,_if_a_change_made_needed_to_be_reverted.
Appliance Version & License

SECURE Email Gateway is able to automatically update its anti-virus and anti-spam defences, without administrator intervention. Similarly, updates to the SECURE Email Gateway itself are also downloaded automatically. However, it is important to understand that these product updates are NOT applied without action from the administrator. This is where the Appliance Version & Upgrades section comes in. The administrator is notified of new releases, via GUI alerts and optional SNMP or SMTP alerts, and then must decide what action to take. This screenshot shows the Appliance Version & Upgrades section on a SECURE Email Gateway that has had some upgrades applied:

Self-testing the SECURE Email Gateway

One of the SECURE Email Gateway’s strengths is its comprehensive collection of self-test features. These save time wasted on needless support calls, allowing you to detect and resolve issues quickly and easily. Click the System tab to return to the System Center’s home page and you’ll see these options displayed in the left-hand control panel:

It is impossible to consider all possible permutations of situations that may lead to problems but a good first step would be the Connectivity Test - just click the link. This provides confirmation that the SECURE Email Gateway is connected and able to communicate before deciding which areas should be the focus of subsequent troubleshooting steps. And be reassured that when expert help is needed, Clearswift can be contacted 24 hours a day, 7 days a week.
SpamLogic Settings

Clearswift’s long experience in managing spam has shown us that customers demand both high-performance spam detection and simple controls over the behaviour of the anti-spam measures.

As well, some customers choose to reject as many identified messages as possible, while others want spam quarantined for later review - just in case.

The Clearswift SECURE Email Gateway’s granular controls can be configured to deal with spam in just the way you want. We call this SpamLogic.

These filters are coupled with the Clearswift TRUSTmanager. This is a cloud-based IP-reputation service that contains the standing of over 50 million IP addresses. These are gathered from a number of trusted sources, including other SECURE Email Gateways around the world. So, as Clearswift continues to grow, so too does our virtual map of good and bad senders of email.

This first-class information means that Clearswift SECURE Email Gateways are able to reject connections from known bad senders at the SMTP connection, saving valuable network bandwidth. In most environments the SECURE Email Gateway is able to block around 90% of spam using this technique and it uses other filtering technology to bring the total spam detection rate up to a genuine 99%+.

In order to get the best out of TRUSTmanager it is important that your organisation’s firewalls are correctly configured. This table lists the relevant information:

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>DNS</td>
<td>CURBL - used for checking URLs within Messages</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>Spam signatures checked against a highly scalable cloud-based service</td>
</tr>
<tr>
<td>8007</td>
<td>UDP</td>
<td>TRUSTmanager look-ups</td>
</tr>
</tbody>
</table>
The effectiveness of SECURE Email Gateway's anti-spam measures can be checked by using the various reports or the real-time graphs in the Health Center.

If the SECURE Email Gateway is deployed behind other message-transfer agents (MTAs) in your environment you can still use TRUSTmanager - just enter the IP address or hostname of these hosts:

Occasionally, the SECURE Email Gateway may need to process email differently for a specific sender. For example, it’s possible that - for whatever reason - the sender’s MTA has wrongly ended up on a real-time block list whitelist.

Another common example is where a specific staff members or groups cannot risk an inaccurate identification of messages as spam - a false-positive - but still want any spam marked on the subject line. Here’s how to deal with this:

1. Create an address list for the special group of recipients
2. Create a new Detect Spam content rule

3. Create a new Detect Spam content rule

4. Add any other content rules to that route
Blocking Files

Most organisations will want to stop certain file types from being sent or received. When it comes to inbound messages, the obvious candidates include any file type that could potentially carry a virus, oversized messages and frivolous attachments, such as MP3s, MPEGs and AVIs. For messages leaving your organisation concerns include leakage of sensitive data, any comments or materials that could damage the company brand or reputation, profanity and embarrassing content.

Fortunately, managing these issues while still allowing staff to communicate freely is easy with the SECURE Email Gateway.

We’ll consider the Detect Media Type content rule can help weed out those time-wasting attachments. The advantage of the Detect Media Type content rule is that it uses binary recognition of the data to determine the file type. So, even if a file is renamed it will still be detected. Here’s what it looks like:

By selecting this grouping, all executable filetypes can be blocked, or click on the ‘+’ and select the individual formats that can be blocked.
Determine what to look for and then define what to do in the event that the file type was detected in a message. The options available in particular content rule are:

- Drop the message
- Non-deliver the whole message
- Hold in a <particular> message area
- Relay to a specific mail server
- Deliver the message
- Strip the attachment
- Add a message header
- Annotate the message
- Generate an alert
- Trigger the message to be encrypted

Obviously, some of these can only be used once - like 'Drop the message'. However, in most cases it is possible to have the SECURE Email Gateway perform multiple actions based on the detection criteria. You could, for example, strip the attachment but still deliver the message.

This new rule would be added to the appropriate route of email to achieve the desired goal.

**Controlling content by keyword**

One of the most powerful and popular features of SECURE Email Gateway is the ability to block or reroute messages based upon words or phrases found either in any of the following locations:

- SMTP headers
- Subject lines
- Message bodies
- Attachments

In terms of attachments, the SECURE Email Gateway is able to extract and analyse documents and files from many common business applications. These include all versions Microsoft Office, OpenOffice and Adobe PDF files, as well as HTML. What’s more, SECURE Email Gateway can even separate where in the document the content was detected, be it the body, the headers and footers or even the metadata.

When it comes to search strings and patterns, SECURE Email Gateway gives customers the freedom to create their own lists of words, phrases and regular expressions. However, the product includes various ready-made lists. As well, the SECURE Email Gateway can access a special set of ‘Managed Lists’: these are built and managed remotely by Clearswift, and are regularly updated with new words and phrases.

These lists of lexical expressions are defined within the References section of the SECURE Email Gateway. They can be used in multiple instances of the Text Analysis content rule.
Defining the list

The lexical expression lists are essentially collections of words, phrases, common expressions, operators and special tokens. Each entry in the list carries an expression ‘value’, from 1 to 10; there is also a special ‘instant’ trigger value. By associating different values to each phrase we can ensure that a degree of sensitivity is achieved.

Credit card numbers provide a good example of the usefulness of special tokens. Obviously, every credit card number is different, so SECURE Email Gateway can employ a credit card token as a pattern-matching tool. In other words, the credit card token looks for a sequence of numbers that match the known credit card. The token looks for strings of digits between 13 and 18 characters in length and prefixes commonly used by the major credit card providers. A checksum formula is also applied to ensure that the match is accurate.

If the credit card token is assigned the aforementioned ‘instant’ value, then as soon as the SECURE Email Gateway detects a message containing credit card number a trigger event will take place: the message could be quarantined, for instance.

However, to allow for the free flow of information the expression value can be altered. Change the credit card token’s expression value to 3, say - and set a threshold of 10 in the content rule - and users would be able to send messages containing up to three credit card numbers. Attempting to send four credit card numbers, though, would trigger an event.
Creating the content rule
A new Detect Lexical Expression content rule can be created and configured for use.

Overview
Detect Credit Card Lexical Expression

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 ‘Credit Card Details’ expression list scores at least 10 in one of
- The message body.
- The attachments matching the conditions in the other clauses.

And Which Media Types
- if any of the detectable media types are detected.

And Size Restriction Of
No size restriction will be applied to this content rule.

What To Do?
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
- and also
- Hold in Confidential area

Generate An Inform
If the ‘What to Look For’ conditions are met generate an Inform SMTP message:
Using the template : ‘Inform for “Detect Credit Card Lexical Expression”’
To : security@mscompany.com

Whilst creating this particular policy rule you can define where in the message you want to check, what the necessary threshold will be to trigger a violation, what the scoring algorithm will be and also what to do when a violation does occur.

Once this has been created it should be added to the appropriate Policy Routes and the configuration needs to be committed.

For Mail Sent
From : Sales, Marketing
To : Suppliers

Do NOT Decrypt or Apply Encryption Endpoints
- Do NOT decrypt PGP and S/MIME messages.
- By default do NOT apply encryption endpoint delivery policy.

By Default Perform This Disposal Action
Deliver the message

Unless One Of These Content Rules Triggers

6 rules on route (applied in the order shown)

1. [ ] Once Messages Containing a Virus
   Hold in Viruses area

2. [ ] Detect Credit Card Lexical Expression
   Hold in Confidential area

3. [ ] Detect media type
   Hold in Multimedia area

4. [ ] Fail to Modify a Message
   Hold in Message Processing Failure area

5. [ ] Fail to Process a Message
   Hold in Message Processing Failure area

6. [ ] Add Legal Disclaimer
   Perform no action
Managing Encryption

Clearswift SECURE Email Gateway supports multiple methods to encrypt data from one organisation to another, including TLS, S/MIME and PGP. There’s also an ‘ad-hoc’ method of encryption, for password-protecting messages sent to external organisations and people. This wide choice of different techniques allows an organisation to engage in secure communications to a wide range of receiving systems.

This table of typical uses provides a guide to the various types of encryption offered by the SECURE Email Gateway:

<table>
<thead>
<tr>
<th>USE CASE</th>
<th>METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>All messages to particular domain must be encrypted</td>
<td>TLS</td>
</tr>
<tr>
<td>Messages sent to a domain must be secured over the internet but do not need to be secured to the desktop</td>
<td>TLS, S/MIME, PGP</td>
</tr>
<tr>
<td>Messages sent to a domain must be secured over the internet but only to a group of named individuals</td>
<td>S/MIME, PGP</td>
</tr>
<tr>
<td>Messages sent to recipients who are familiar with encryption software on their system and must receive the message in a secure fashion</td>
<td>S/MIME, PGP</td>
</tr>
<tr>
<td>Messages encrypted at the desktop, content checked at the corporate gateway and delivered to the recipient’s desktop in an encrypted format</td>
<td>S/MIME, PGP</td>
</tr>
<tr>
<td>Messages sent to recipients who have no desire for any encryption software on their system and must receive the message in a secured fashion</td>
<td>Ad-hoc</td>
</tr>
<tr>
<td>Messages sent to recipients that should only be encrypted based on the presence of certain content, such as credit card numbers</td>
<td>S/MIME, PGP, Ad-hoc</td>
</tr>
</tbody>
</table>

Encrypting a message

Encrypting an email requires appropriate keys or pass phrases that can be used to convert the unsecured data into a secure format.

Both S/MIME and PGP employ a public/private keys format (S/MIME keys are also known as certificates), while the ad-hoc method relies on a single pass phrase. The special keys required for S/MIME or PGP can be generated automatically by the SECURE Email Gateway, a key generator tool (such as GnuPG) or by using a third-party service such as Verisign, Thawte or GlobalSign. These keys can be separated out into a private part, which must not be disclosed to anyone else, and a public part that can be distributed to anyone.

First, though, S/MIME and PGP keys must be imported into the SECURE Email Gateway’s Certificate Store. To do this, click the System tab followed by Certificate Store then Partners - like this:
It is possible to import the S/MIME and PGP certificates in the following key formats: PEM, ASC, B64, CER and P7B.

With the keys loaded into the Certificate Store, it is possible to create encryption ‘endpoints’ – which define the certificates and encryption method to use for particular email recipients. Here, we'll consider an example recipient called Bob Smith, whose PGP key has already been loaded into the Certificate Store:

We're going to create an encryption endpoint for any email messages sent to him via the SECURE Email Gateway. Click New in the Mail Encryption Endpoints and follow the screen options. It would look like this:

Click Save and this new endpoint will be listed in the Encryption Endpoints section of the Systems Center, here:
As such, we are now able to enforce an encryption policy for email sent to bob.smith@abc.com.

To do this, we would create an email policy for messages sent to this address. Then, every email sent from your organisation to bob.smith@abc.com will be encrypted using his key. This is achieved by creating a new policy route, in the Policy Center:

Address List entry for Bob Smith. This could be a generic address list for all recipients of encrypted email

For Mail Sent
From: Anyone
To: Bob Smith

Apply Encryption Endpoints
- Do NOT decrypt PGP and S/MIME messages.
- By default apply encryption endpoint delivery policy.

Enable encryption

So, assuming the message is processed and does not get quarantined, it will be encrypted using Bob’s certificate details and sent to him.

The SECURE Email Gateway can also force encryption based on triggering of a particular content rule. You might, for example, employ the Detect Lexical Expression rule to check for sensitive words or phrases by referencing the Confidential Material expression list and, if found, encrypt the message automatically. Here’s how to do it:

Overview
Detect Confidential Material and Encrypt

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 ‘Confidential Material’ expression list scores at least 10 in one of
  - The message body.
  - The subject line.
  - The attachments matching the conditions in the other clauses.

And Which Media Types
- If any of the detectable media types are detected.

And Size Restriction Of
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
- Deliver the message applying encryption endpoint policy

Where in the message to scan for keywords

To make encryption even simpler, it is possible to create an endpoint that uses password protection. The password can be a phrase defined by and known to both sender and recipient, or it can be generated automatically by the SECURE Email Gateway. When this option is selected, the sender receives an acknowledgement of the password via email, like this:
It’s also possible to configure the SECURE Email Gateway to encrypt based on the type of files sent. For example, the act of sending an Excel spreadsheet could trigger an encryption event, either for all messages or to particular recipients only (like an external accounting firm, say).

**Decrypting Messages**

Finally for this guide - we will cover decrypting messages. This is straightforward in the SECURE Email Gateway. Simply save the message recipient’s private key in the Corporate tab of the Certificate Store and set it as a default key. You should see that the envelope icon will be highlighted for that key. Then, configure a policy route that will apply decryption using the key.

We hope that this brief guide has given you a head start in your evaluation of Clearswift SECURE Email Gateway. Of course, there’s plenty more to explore. For more help or guidance either follow the links below or simply give us a call - we’d love to hear from you.

---

**For further information**


Clearswift knowledge base: [http://kb.clearswift.com/](http://kb.clearswift.com/)

Technical Support: [http://www.clearswift.com/support/support-services](http://www.clearswift.com/support/support-services)

Contact Clearswift

UK - International HQ
Clearswift Limited
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA
UK
Tel: +44 (0) 118 903 8903
Fax: +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift
5th Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA
Tel: +61 2 9424 1200
Fax: +61 2 9424 1201
Email: info@clearswift.com.au

Germany
Clearswift GmbH
Amstickstrasse 67
20997 Hamburg
GERMANY
Tel: +49 40 23 999-0
Fax: +49 40 23 999-100
Email: info@clearswift.de

Japan
Clearswift K.K
7F Hanai Bldg,
1-2-9 Shibakoen,
Minato-ku, Tokyo
105-0011
JAPAN
Tel: +81 (3)5777 2248
Fax: +81 (3)5777 2249
Email: info.jp@clearswift.co.jp

Spain
Clearswift España S.L.
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcón
Madrid
SPAIN
Tel: +34 91 7901219 / +34 91 7901220
Fax: +34 91 7901112
Email: info.es@clearswift.com

United States
Clearswift Corporation
161 Gaither Drive
Centerpointe
Suite 101
Mt. Laurel, NJ 08054
UNITED STATES
Tel: +1 856-359-2360
Fax: +1 856-359-2361
Email: info@us.clearswift.com