



Admin Guide


Boundary Defense for Email Email Content Control Service


MailStreet Live Support: **866-461-0851**

Table of Contents

OVERVIEW	4#
1 ABOUT THE GUIDE	4#
1.1. AUDIENCE AND SCOPE	4#
1.2. INTERNATIONAL CONSIDERATIONS.....	4#
1.3. SECURITY AND LEGAL CONSIDERATIONS	4#
1.3.1 DNS	4#
1.3.2 Legal considerations	4#
1.3.3 Login details	4#
1.3.4 Passwords.....	4#
2 INTRODUCTION TO CONTENT CONTROL	5#
2.1. DESCRIPTION OF EMAIL CONTENT CONTROL	5#
2.2. OVERVIEW OF THE CONFIGURATION PROCESS.....	5#
2.3. EXAMPLE RULES WITHIN EMAIL CONTENT CONTROL.....	7#
3 GETTING STARTED	8#
3.1. LOGGING IN AND LOGGING OUT.....	8#
3.2. LOCATING THE EMAIL CONTENT CONTROL PAGES IN CLIENTNET	8#
3.3. BEST PRACTICE SETTINGS FOR EMAIL CONTENT CONTROL	10#
3.4. GLOBAL AND DOMAIN SETTINGS FOR CONTENT CONTROL.....	10#
3.4.1 Applying custom settings for a domain.....	11#
3.4.2 Applying global settings.....	12#
4 DEFINING GENERAL SETTINGS	13#
4.1. DEFINING A GENERAL ADMINISTRATOR EMAIL ADDRESS	13#
4.2. DEFINING A NOTIFICATION 'SENT FROM' ADDRESS	13#
4.3. DEFINING A DEFAULT TIME ZONE	14#
4.4. DEFINING DEFAULT NOTIFICATIONS.....	14#
4.5. DEFINING DEFAULT SUBJECT LINE TAG TEXT.....	16#
5 USER GROUPS IN EMAIL CONTENT CONTROL	17#
5.1. INTRODUCTION TO USER GROUPS IN EMAIL CONTENT CONTROL.....	17#
5.1.1 User groups at global and domain level	17#
5.1.2 Exception addresses	17#
5.2. VIEWING YOUR USER GROUPS IN EMAIL CONTENT CONTROL.....	18#
5.3. CREATING A CUSTOM USER GROUP FOR EMAIL CONTENT CONTROL	18#
5.4. EDITING A CUSTOM USER GROUP IN EMAIL CONTENT CONTROL	20#
5.4.1 Editing a user group manually in ClientNet.....	20#
5.4.2 Editing a user group using a CSV file.....	21#
6 WORKING WITH LISTS	22#
6.1. PRE-DEFINED LISTS	22#
6.2. DEFINING LISTS AT VARIOUS LEVELS	23#
6.3. VALID AND INVALID CHARACTERS AND CHARACTERISTICS OF LISTS	24#
6.4. VIEWING YOUR LISTS.....	25#
6.5. SEEING THE RULES THAT USE A SPECIFIC LIST	25#
6.6. CREATING A LIST	26#
6.7. CREATING A SUPERLIST	27#
6.8. EDITING A LIST.....	28#
6.9. DELETING A LIST.....	28

7 RULES IN EMAIL CONTENT CONTROL	29#
7.1. INTRODUCTION TO RULES IN EMAIL CONTENT CONTROL	29#
7.2. VIEWING AND MANAGING EMAIL CONTENT CONTROL RULES	31#
7.2.1 <i>Viewing your rules</i>	31#
7.2.2 <i>Managing your rules</i>	31#
7.2.3 <i>Activating and deactivating a rule</i>	33#
7.2.4 <i>Changing the position of a rule</i>	33#
7.3. DEFINING AN EMAIL CONTENT CONTROL RULE	34#
7.3.1 <i>Defining 'all' or 'any' conditions</i>	34#
7.3.2 <i>Defining sender and recipient conditions</i>	35#
7.3.3 <i>Defining email content conditions</i>	38#
7.3.4 <i>Defining attachment conditions</i>	43#
7.3.5 <i>Defining time interval conditions</i>	45#
7.3.6 <i>Defining actions and notifications</i>	46#
8. FREQUENTLY ASKED QUESTIONS (FAQS) ABOUT EMAIL CONTENT CONTROL SERVICE.....	49#
9. GLOSSARY	52#

 **FEEDBACK:** If you note mistakes in this guide, or identify procedures that are incorrect, we encourage you to email your feedback to userguidefeedback@hostaccount.com. We continually strive to improve our customer support resources and your feedback is invaluable in assisting us with our goal to provide exceptional customer service.

 **PLEASE NOTE:** This MailStreet Hosting Control Panel **Support Resources** section is updated periodically as new customer resources are added to assist customers with the use of their hosted services. You should occasionally check for updates to these support resources by logging into the Admin Control Panel and selecting the **Help & Support** menu option under the **Hosting** menu.

Overview

This guide is for Email Content Control service administrators. It provides procedures for configuring the Email Content Control service to your requirements, including defining the rules according to your Email Content Control policy

1 About the Guide

1.1. Audience and Scope

Welcome to the Administrator Guide for the MailStreet Boundary Defense for Email Content Control service. This guide provides you with procedures to set up and manage the Email Content Control service.

1.2. International Considerations

Due to local legislation, some features described in this document are not available in some countries.

1.3. Security and Legal Considerations

1.3.1 DNS

Clients are advised to ensure that their DNS is secure. This is in order to prevent alteration of the MX records, which could allow malicious redirection and interception of email. In addition to technically securing the DNS, it is also important to ensure that contact details and security procedures are in place and up to date with the domain registrar, to prevent domain hi-jacking.

1.3.2 Legal considerations

Clients are advised to seek specialist advice to ensure that they use the MailStreet Boundary Defense for Email Content Control service in accordance with relevant legislation and regulations. Depending on jurisdiction, this may include data protection law, privacy law, telecommunications regulations, employment law and other regulations. In most jurisdictions it is a requirement that users of the service are informed about or give consent to the fact that their email is being monitored and intercepted for the purpose of providing the protection offered by the Boundary Defense for Email service.

1.3.3 Login details

Login details to ClientNet should be kept secure and only used on a secure trusted computer. As ClientNet can be accessed via the Internet, it is of particular importance to ensure that procedures exist for revoking access when a member of staff leaves or no longer needs access. Service desk authorized contacts should also be kept current.

1.3.4 Passwords

Passwords should be chosen and used in accordance with good password usage practice. This includes:

- Not sharing passwords;
- Using long, non-obvious and complex passwords; and
- Changing passwords on a regular basis.

2 Introduction to Content Control

2.1. Description of Email Content Control

Email Content Control can be used by your organization to enforce policy rules that:

- Protect corporate reputation
- Preserve confidentiality and security
- Reduce legal liability
- Defend against careless and malicious actions
- Ensure regulatory compliance
- Reduce lost productivity
- Retain network bandwidth

Email Content Control is a managed email service that allows you to identify and control confidential, malicious, or inappropriate content sent or received by your employees. The service enables you to monitor and enforce your acceptable usage policy, helping to protect your employees and your brand, and safeguarding against the increasing risk of litigation. You define a set of rules that reflect your organization's email security policy. You can manage the size of inbound emails, set restrictions for specific groups in your organization; control the number of attachments received; manage file formats; and monitor the usage of key words. Rules can also be set to apply within or outside certain periods, for example, you can allow large files to be delivered outside normal working hours only.

As well as the email itself, the Email Content Control service scans the contents of MS Office documents that are attached to an email. You can detect specific words or phrases, or alphanumeric templates within the email or its MS Office attachments. The service can also provide protection against specific file types. The scanning engine unpacks and looks inside archive files, such as zipped files, to detect the file extensions or content defined in your rules. This provides a comprehensive content scanning service that incorporates both the content of the email and of its attachments going into and out of your organization.

Some examples of common email content control policies are described in *Section 2.3. , Example rules within Email Content Control.*

2.2. Overview of the Configuration Process

The Email Content Control Service is configured via ClientNet. The service lets you build a set of discrete rules to enforce your organization's email security policy. Each rule identifies emails containing content or attachments that contravene the policy.

An action is associated with each rule. For example, if an email contains a profanity, the action might be to redirect the message to an administrator. You can establish rules as global settings that apply to all of your domains, or as custom settings that are unique to an individual domain.

Here is an overview of the process for creating a set of rules:

STEPS		FOR FULL DETAILS
Plan which rules, user groups, and lists you need to create for all domains and for specific domains: NOTE: It might be useful to create your rules for a single domain and test that they work to your requirements before copying them to all of your domains		Section 3.4 , Global and domain settings for Content Control
Define general settings: <ul style="list-style-type: none"> ○ An administrator's email address. ○ An email address that notifications appear to be sent from ○ The time zone ○ Default notifications: Those set at global level are used unless domain- or rule-level settings are defined. Those set for a domain are used for that domain's rules unless rule-level settings are defined. 		Section 4 , Defining general settings
Create custom user groups and view groups to specify as senders or recipients to use in the rule		Section 5 , User Groups in Email Content Control
Create lists of filenames, text content, MIME types, domain names, and URLs to form the criteria for your rules.		Section 6 , Working with lists
Create rules by defining their conditions and actions: NOTE: The order of rules affects the order in which rules are scanned (see Section 7.3, Defining an Email Content Control rule).	Sender and recipient conditions (as specified in user groups and domain lists)	Section 7.3.2 , Defining sender and recipient conditions
	Email content conditions, including: <ul style="list-style-type: none"> ○ The parts of the email to be scanned. ○ Email size, encrypted files, importance levels, password-protected files. ○ The content to scan for—as specified in your lists 	Section 7.3.3 , Defining email content conditions
	Attachment conditions—number and size of attachments, filenames, MIME types, and spoofed attachments.	Section 7.3.4 , Defining attachment conditions
	Conditions relating to the time an email is received or sent	Section 7.3.5 , Defining time interval conditions
	Actions and notifications for detected mail.	Section 7.3.6 , Defining actions and notifications
Once your rules are defined, you can view a summary of each of them		Section 7.2 , Viewing and managing Email Content Control rules

2.3. Example Rules Within Email Content Control

Some examples of rules that we see within Email Content Control are presented here.



Every organization is different and MailStreet Boundary Defense for Email recommends that you do not simply set up the following rules without understanding your businesses needs and aligning an email security policy with them.

- **Block emails over 25MB** – reduces the size of emails coming into the organization to save bandwidth. All emails over 25MB can be blocked and deleted, and notifications sent to all parties
- **Redirect emails to/from suspicious domains** – monitors emails coming from or going out to competitors' domains, restricting the passing on of intellectual property and poaching of employees
- **Monitoring profanity outbound** – protects the organization's brand and reputation, for example, by blocking an employee from sending out an email containing slander to a friend
- **Redirect encrypted or password-protected mail** – enables administrators to monitor and control who is sending and receiving encrypted or password-protected messages
- **Compress emails between 10MB and 25MB** – reduces the bandwidth taken up by large messages coming into the organization
- **Block video file attachments** – restricts video files to be received only by the marketing department.

3 Getting Started

3.1. Logging In and Logging Out

To log in to the ClientNet portal which is used to manage your Content Control configurations, you will access the Boundary Defense for Email Service through the MailStreet Control Panel:

<https://cp.mailstreet.hostaccount.com>

To log in to ClientNet:

1. Log into the MailStreet Control Panel using your administrator username and login.
2. Click on **Hosting | Boundary Defense for Email** to access the Boundary Defense for Email service window
3. In the section titled Access to Boundary Defense for Email control panel, click on the link next to the **Log in to control panel** option.
4. The ClientNet portal for your account should be displayed in a new window. Use your BDE admin credentials to log in.
5. **NOTE:** Use the BDE Admin login and password that are listed in the Apptix Control Panel just above the **Log in to the control panel** option. Click on the [View Password](#) link to display the admin password.

To log out ClientNet:

1. From any screen in ClientNet, click the **Log Out** link at the top left of the screen.

3.2. Locating the Email Content Control Pages in ClientNet

Depending on your organization's configuration, you may only have access to certain domains. This will affect the rules that you can create, edit, and copy.

To locate the Email Content Control pages in ClientNet:

1. In the top navigation bar, click **Configuration** and then click **Email Services**.
2. In the left navigation bar, click **Content Control**.
 - Four tabs are displayed: **Rules**, **User Groups**, **Lists**, and **Settings**. These tabs are used to manage your rules, user groups, lists, and general settings.

Home | Configuration | Reports | Support | Administration

You are here: Home > Configuration > Email Services > Content Control

Email Services

- Anti-Virus
- Anti-Spam
- Content Control**
- Image Control
- Platform
- Inbound Routes
- Outbound Routes

Content Control

Global Settings

Rules | **User Groups** | Lists | Settings

Create new rule | Delete selected | Copy selected | Move selected

Showing 1 - 10 of 20 << First | < Previous | Next > | Last >>

<input type="checkbox"/>	Rule name	Action and notifications	Last updated	Direction	
<input type="checkbox"/>	Block emails over 25mb	Block and delete	02 April 2009 13:56 GMT , demo4	Inbound	De-activate
<input type="checkbox"/>	Monitor outbound profanity	Log only	02 April 2009 13:55 GMT , demo4	Outbound	De-activate
<input type="checkbox"/>	Redirect encrypted or password protected email	Redirect mail to the administrator	04 March 2009 09:48 GMT , demo4	Inbound or Outbound	De-activate
<input type="checkbox"/>	Compress emails between 10 and 25 MB	Compress attachments	02 April 2009 13:57 GMT , demo4	Inbound	De-activate
<input type="checkbox"/>	Redirect emails to and from suspicious domains	Log only	02 April 2009 14:14 GMT , demo4	Inbound or Outbound	De-activate
<input type="checkbox"/>	Block audio and video file attachments	Block and delete	02 April 2009 14:09 GMT , demo4	Inbound	Activate

<< First | < Previous | Next > | Last >>

When you select a specific rule or create a new rule, seven tabs are displayed: **Sender**, **Recipient**, **Email content**, **Attachments**, **Time intervals**, **Actions & notifications**, and **Summary**. These tabs are used to define the conditions for a rule.

Edit Rule

Rule title: Apply to: Inbound mail Outbound mail Both

Sender | **Recipient** | Email Content | Attachments | Time Intervals | Actions & notifications | Summary



For details of best practice settings for Content Control, see [Section 3.3](#), *Best practice settings for Email Content Control*.

3.3. Best Practice Settings for Email Content Control

When you are provisioned with the Email Content Control service, the service has no rules set up. The rules you define for Email Content Control assist in monitoring and controlling your company's acceptable use policy. MailStreet Boundary Defense for Email recommends that initially you set up five rules to just log various aspects of content within emails, as follows:

- Log inbound emails over 2Mb
- Log outbound profanities
- Log all encrypted email inbound and outbound
- Log inbound emails over 10Mb
- Log audio and video files inbound and outbound

Then once you are familiar with kinds of emails that are being detected, you can feel more confident in blocking some, and redirecting others. The following are some common rules, but note that every organization is different. We recommend that you do not simply set up these example rules without understanding your business' needs and aligning an email security policy with them:

- **Block emails over 25MB** – reduces the amount of email coming into the organization to save bandwidth. All emails over 25MB can be blocked and deleted, and notifications sent to all parties
- **Monitor outbound profanities** – protects the organization's brand and reputation. You may wish to block employees from sending out emails containing profanities, even to friends.
- **Redirect encrypted or password-protected mail** – enables administrators to monitor and control who is sending and receiving encrypted or password-protected messages.
- **Compress emails between 10MB and 25MB** – reduces the bandwidth taken up by large messages coming into the organization.
- **Redirect emails to/from suspicious domains** – monitors emails coming from or going out to competitors' domains, restricting the passing on of intellectual property and poaching of employees.
- **Block audio and video file attachments** – or you may wish to restrict audio and video files to be received only by the Marketing department.

For full details on configuring the Content Control service, see [Section 2 , Introduction to Content Control](#).

3.4. Global and Domain Settings for Content Control

You can apply Email Content Control settings for all domains (global settings), and you can apply custom settings to your individual domains to suit your organization's requirements. At the global and domain level, you can specify the following information:

- **Rules** – a rule specified at global level, can use lists and user groups that are also specified at the global level. A rule specified at domain level can use lists and groups that are specified both at global level or within the same domain (see [Section 7 , Rules in Email Content Control](#))
- **User groups** – at global level, a user group can contain users from all of your domains; at domain level, a user group can contain users from the selected domain. A user group defined for a specific domain can only be used in a rule specified for that same domain (see [Section 5 , User Groups in Email Content Control](#))
- **Lists** – you can specify lists at global level to be used in rules across all domains, or you can specify a list that will only be used in a rule for a selected domain, at domain level. You can also customize a list at rule level. It may be useful to create a default list (at global or domain level) and then make additions or remove items at the rule level. (See [Section 6 , Working with lists](#).)
- **General settings** – the general settings are listed below. You can define these settings to apply at global level, or if you require a specific setting for a specific domain, at domain level (see [Section 4 , Defining general settings](#)):

An administrator email address to which redirected or copied emails and notifications are sent (see [Section 4.1 , Defining a general administrator email address](#)) A "sent from" address for all notifications (see [Section 4.2 , Defining a notification 'sent from' address](#)) The text for administrator, sender, and recipient notifications (see [Section 4.4 , Defining default notifications](#)) The time zone (see [Section 4.3 , Defining a default time zone](#))

3.4.1 Applying custom settings for a domain

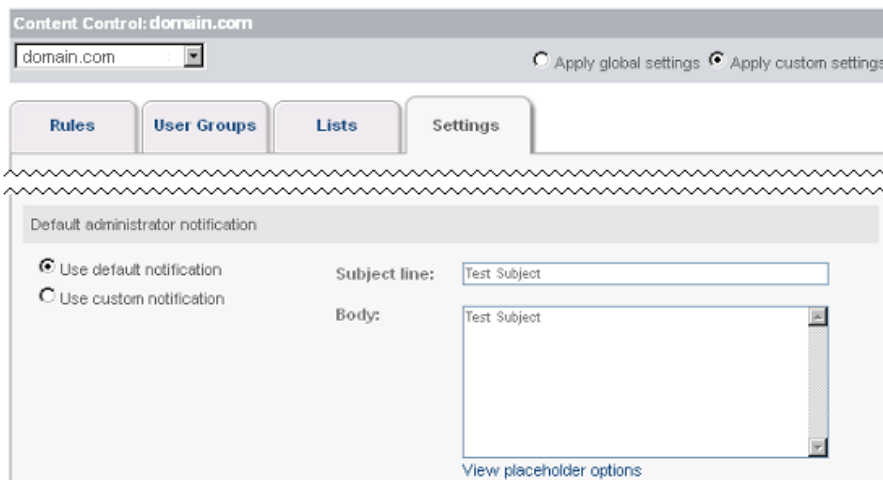
At domain level, you can customize a configuration specifically for the selected domain. On initial set up, each domain is set to use the global settings. If you select a domain from the **Global settings** drop-down list and then apply custom settings using the option button, you can modify the settings for the individual domain without affecting the global settings. To apply settings for a specific domain, ensure the **Apply custom settings** option button is selected. Until this is selected, all fields in these pages are inactive and cannot be edited.



If you have defined any custom settings and you switch from using custom settings back to using global settings (by selecting the **Use global settings** option button at top right of the screen), the settings in the page display the global settings (but are inactive). But your custom settings for that domain are remembered and when you switch back to **Use custom settings**, your custom settings are again displayed and applied when you click **Save and exit**.

To apply settings for a specific domain:

1. Select **Configuration > Email Services > Content Control**.
2. Select the domain from the **Global Settings** drop-down list.
 - Four tabs are displayed – **Rules**, **User Groups**, **Lists**, and **Settings**. If no domain-level settings have been defined yet, all fields in these pages are inactive and cannot be edited.
3. Select **Apply custom settings**.
 - The rules, groups, lists, and settings that you can apply at domain level are now editable. The changes you make are applied only to the selected domain (provided the changes are saved).



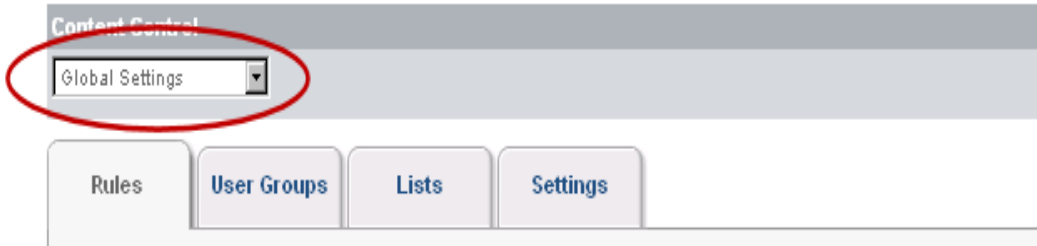
When you select a specific domain to work with, the name of the domain is displayed as a heading:



3.4.2 Applying global settings

To apply global settings:

1. Select **Configuration > Email Services > Content Control**.
2. Ensure **Global Settings** is selected from the drop-down list:



- Four tabs are displayed – **Rules**, **User Groups**, **Lists**, and **Settings**.

4 Defining General Settings

You can define the following general settings:

- An administrator email address to which redirected or copied emails and notifications are sent (see [Section 4.1. , Defining a general administrator email address](#))
- A “sent from” address, which allows you to customize the email address the notifications are sent from and to which recipients can reply to notifications (see [Section 4.2. , Defining a notification ‘sent from’ address](#))
- The text for administrator, sender, and recipient notifications (see [Section 4.4. , Defining default notifications](#))
- The time zone (see [Section 4.3. , Defining a default time zone](#))
- The subject line text to be used when the action to Tag the subject line is selected (see [Section 4.5. , Defining default subject line tag text](#))

The general settings can be applied at global or domain level. If you configure settings at global level, these are inherited at domain and then rule-level, unless any custom settings are defined at those levels. In other words:

- Domain-level settings inherit from global settings
- Rule-level settings inherit from domain settings

4.1. Defining a General Administrator Email Address

Before you can build any rules, you must define an administrator email address. The **Administrator Email Address** specifies the default email account to which notifications and copied and redirected emails are sent.



Administrator email addresses bypass the Email Content Control scans. Therefore, if you are using this email address to test your rules, your results will not be accurate. Emails sent from or to this address will not activate any of your Email Content Control rules.



You can also specify an administrator email address for a specific rule. Doing so enables you to either copy or redirect an email that has triggered a specific rule to a specifically targeted email address. See [Section 7.3.6.2 , Defining a rule-specific administrator email address](#).

To define a general administrator email address:

1. Select **Configuration > Email Services > Content Control**.
2. Click the **Settings** tab.
3. In the **Administrator Email Address** section, enter the required email address.
4. Click **Save**.

4.2. Defining a Notification ‘Sent From’ Address

The **Notification ‘sent from’ address** specifies the email address that notifications appear to come from. Users can reply to a notification to this email address. This ensures that the reply is sent to an appropriate person rather than to a generic email address, from which a user’s reply may be bounced.

To define a notification ‘sent from’ address:

1. Select **Configuration > Email Services > Content Control**.
2. Click the **Settings** tab.
3. In the **Notification ‘sent from’ address** section, enter the required email address.
4. Click **Save**.



A default email address has been inserted for you. This email address is for sending notifications only. If you want to receive replies on this address, you will need to:

- Create a mailbox with this address, OR
- Create a contact and enable forwarding for this address, OR
- Change this address to that of a valid email address for your domain.

4.3. Defining a default time zone

The **Default Time Zone** defines the time zone that is applied by default when generating conditions based on time intervals. If no time zone is specified, the system assumes UTC (Co-ordinated Universal Time). This is the same as GMT (Greenwich Mean Time). Where applicable, daylight saving is accounted for, for example, Europe/London (BST).

To define the default time zone:

1. Select **Configuration > Email Services > Content Control**.
2. Click the **Settings** tab.
3. In the **Default Time Zone** section, select the required time zone from the drop-down list.
4. Click **Save**.

4.4. Defining Default Notifications

When a suspect email is detected, you can define a notification to be sent to an email administrator, the sender, and/or the recipient. The text for each notification can be different. ClientNet provides the flexibility to define each of these notifications at three levels:

- **Global level** – generic notifications for all domains. Use the text defined by MailStreet Boundary Defense for Email, or customize the text in the **Settings** tab with **Global settings** selected. The text of the MailStreet Boundary Defense for Email notifications is as follows:
 - **Default administrator notification:**
 - The MailStreet Boundary Defense for Email Content Control service has identified that an email sent to/from one of your users may contain inappropriate content according to the policy rules established by your Domain Administrator.
 - **Default sender notification:**
 - The MailStreet Boundary Defense for Email Content Control service has identified that an email sent by you may contain inappropriate content according to the policy rules established by either your organization or the intended recipient's organization. The recipient address of the email was: %r
 - The email was sent on %d
 - If your organization subscribes to the MailStreet Boundary Defense for Email Content Control service please contact your IT Helpdesk for further assistance. Otherwise, please contact the IT administrator of the intended recipient's domain.
 - **Default recipient notification:**
 - The MailStreet Boundary Defense for Email Content Control service has identified that an email sent to you may contain inappropriate content according to the policy rules established by your organization. The sender address of the email was: %eThe email was sent on %d
 - Please contact your organization's IT Helpdesk if you require further assistance.
- **Domain level** – notifications for a specific domain. Until you define these, the notifications are inherited from those defined at global level. See [Section 3.4. , Global and domain settings for Content Control](#).
- **Rule level** – notifications for each rule. Unless you define these, the notifications for all rules are inherited from those defined at the global or domain level depending on your current settings. When creating a new or editing an existing rule, you can define your custom notifications in the **Actions and notifications** tab (see [Section 7.3.6.3 , Defining notifications for a rule](#)).

This flexibility enables you to provide your users with explicit information surrounding a suspect email and why it has been triggered by a rule. It also enables you to warn or advise users, rather than to just take action on an email. For example, you can define a notification to be sent to the sender of an email containing a video attachment, informing them that they can only send such emails after 18:00. For full details of defining rule-level notifications, [see Section 7.3.6.3 , Defining notifications for a rule](#).

To define default notifications:

1. Select **Configuration > Email Services > Content Control**.
2. Click the **Settings** tab.
3. Select either **Global settings** or an individual domain from the Global settings drop-down list, as required.
4. In the **Default administrator/sender/recipient notification** section (as required), select **Use custom notification**.



If you are defining the notification at global level, the **Use default notification** option means that text defined by Boundary Defense for Email is used for the notification.

If you are defining the notification at domain level, the **Use default notification** option means that the text defined at global level is used. This could be either the MailStreet Boundary Defense for Email text or custom text if any has been defined at global level.

5. Enter the text you require for the subject line and body of the email.

The placeholder options enable you to enter variables, such as the date, name of an attached file, name of the rule, etc. To see the variables, click **View placeholder options**. The variables can be typed or copied and pasted into the content of the rule.

Placeholder	Description
%d	Date the email was sent For example, "The email was sent on %d"
%t	Subject line of the email For example, "An email sent to you with the following subject line was blocked: %t"
%p	Plain text section of the email body – not allowed in messages to administrators For example, "An email containing the following text has been blocked: %p"
%y	Suspect attachment filenames For example, "An email containing the following attachments has been blocked: %y"
%e	Envelope senders – the actual sender of the email For example, "The sender address of the email was: %e"
%s	Message body senders – the reply to address given in the email For example, "The reply to address of the mail was: %s"
%S	The sending server's IP address For example, "The sender's IP address was: %S"
%r	Envelope recipients – all recipients including bcc's For example, "The recipient address of the email was: %r"
%g	Message body recipients – this does not include bcc's. Not allowed in messages to recipient or administrator. For example, "The recipient address of the email was: %g"
%R	Name of the rule that detected the message For example, "The email contravenes the following policy: %R"
%E	Reason text from the rule that detected the message For example, "The email was blocked for the following reason: %E"
%%	% – use two percentage symbols to insert a %

6. Click **Save**.

4.5. Defining Default Subject Line Tag Text

Selecting **Tag subject line** as an action for detected email enables an email to continue in its intended path but provides the recipient with a warning that it may contain inappropriate content. If you select an action to tag the subject line of a detected email, you must define the text for the tag.

To define default subject line tag text:

1. Select **Configuration > Email Services > Content Control**.
2. Click the **Settings** tab.
3. In the **Subject line text** section, enter the text for the tag in the **Enter text** box.
 - a. The default text for the subject line tag is “unacceptable content”. The maximum number of characters that the tag can depend on the language you are entering. The tag text can contain non-Western characters.
4. Select an option button depending on whether to put the text before or after the existing subject line text.

5 User Groups in Email Content Control

You can define Email Content Control rules to detect email according to who sent it and/or who it was sent to. You use **Senders** and/or **Recipients** conditions in your rules to do this. Senders and recipients are set up as groups of users for use in rules (even if a group only consists of a single user).



You can also detect email according to the domains it is sent to and/or from. For this, use domain lists in your sender and recipient conditions. See [Section 7.3.2 , Defining sender and recipient conditions](#) .

5.1. Introduction to User Groups in Email Content Control

A user group is a set of users for use in sender and recipient conditions in your rules.



To use domains as senders or recipients that trigger a rule, define these as lists. (See [Section 6 , Working with lists](#).)

Users and groups can derive from two sources:

- Custom users and groups
- Harvested email addresses—can be used like custom users

Custom users and groups—create and edit custom users and user groups in ClientNet. Custom user groups can be viewed in ClientNet. You can also upload a CSV file listing custom users in a group. This is useful if you require users that are not stored in your directory data, for example, external email addresses.

Harvested email addresses—the Email Content Control service harvests the email addresses of all users who send outbound emails within your organization. As email is sent from your domains, the system checks the email address of each sender. If the sending domain is enabled for the service and the email address does not already exist, the email address is harvested . So, a harvested email address is one that has been recognized and stored by the system. Harvested email addresses can be viewed in ClientNet as custom users and can also be added to your custom groups.



For more information about address harvesting, see [Automatic outbound address harvesting](#).

The following characteristics apply to user groups:

- A user can belong to multiple groups
- If a group is defined at global level, it can contain users from different domains
- A group must have at least one user assigned to it
- A group can contain up to 1,000,000 users

5.1.1 User groups at global and domain level

You can view users and groups, and manage custom groups and users, at global and domain level:

- At global level—enables groups to be managed across all domains
- At domain level—enables you to manage user groups specific to that domain



You can use a group defined at the global level in a rule that is specific to an individual domain; the rule will only apply to those members of the user group who belong to the domain in question. (For more on working at global and domain level, see [Section 3.4 , Global and domain settings for Content Control](#).)

5.1.2 Exception addresses

There is an exception list built into the Email Content Control scanner that enables high priority emails from MailStreet Boundary Defense for Email to get through to you without being stopped; for example, to ensure that you

receive virus alerts and can send spam samples and similar messages without the messages being stopped or copied. This list is not displayed in ClientNet.

5.2. Viewing Your User Groups in Email Content Control

You can view your groups in ClientNet.

To view your user groups

1. Select **Configuration > Email Services > Content Control**.
2. Click the **User Groups** tab.
 - The groups available at the level you have selected (global or domain) are listed with the following details:
 - o **Group Name**—for custom groups, click on the group name to view full details of the group and its members in the **Edit User Group** page.
 - o **Group type**—displays the type of group.
 - o **Members**—displays the number of users in the group
 - o **In use?**—displays whether the group is used in any rules.
 - o **Last Updated**—displays the date and time the group was last edited.



Only 500 groups are displayed at a time. To avoid too long a list, search using the **Group name** box and the **Group type** filter. The **Group name** search box accepts wildcards for partial matching. The wildcard * is interpreted as zero or more unknown characters, for example, W*d finds words including **Wild** and **WithId**.

To view the members of a custom user group

1. Select **Configuration > Email Services > Content Control**.
2. In the **User Groups** tab, click on the name of the group to view in the **Group name** column.
 - The **Edit User Group** page is displayed.
3. You can use the **Email address** search box to display the group members in the **Group members** box.

5.3. Creating a Custom User Group for Email Content Control

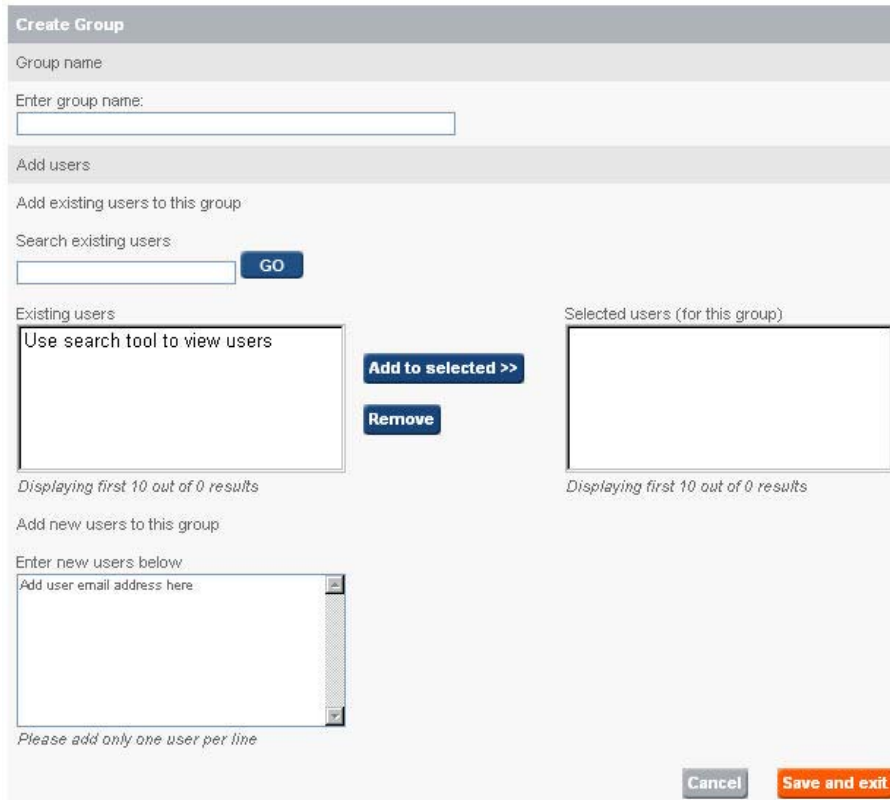
You can create a user group manually in ClientNet and add existing or new email addresses (users) to it. You can also create a new user to add to a group. This is useful to add users who do not send emails, i.e. whose addresses are not harvested, and for external email addresses.



You can also create and edit the users in a group in a CSV file and upload this to ClientNet. See **Section 5.4**, **Editing a custom user group in Email Content Control**.

To create a custom user group

1. Select **Configuration > Email Services > Content Control**.
2. In the **User Groups** tab, click the **Create New Group** button.
 - The **Create Group** page is displayed



The screenshot shows the 'Create Group' interface. It includes a 'Group name' field with a 'GO' button. Below is an 'Add users' section with a search box and another 'GO' button. There are two columns: 'Existing users' and 'Selected users (for this group)'. The 'Existing users' column contains a message 'Use search tool to view users' and a 'GO' button. The 'Selected users' column is empty. Between the columns are 'Add to selected >>' and 'Remove' buttons. At the bottom of the 'Existing users' column is the text 'Displaying first 10 out of 0 results'. At the bottom of the 'Selected users' column is the text 'Displaying first 10 out of 0 results'. Below the columns is an 'Add new users to this group' section with a text area for 'Enter new users below' and a 'GO' button. The text area contains the text 'Add user email address here'. Below the text area is the text 'Please add only one user per line'. At the bottom right are 'Cancel' and 'Save and exit' buttons.

3. Enter a name for the user group.
 - The user group name must be unique, contain alphanumeric characters and spaces (but no other character types), and begin with an alphabetic character.
4. Search for an existing user by using the **Email Address** search box, and highlight the required user in the **Available users** box.
 - The search affects both the **Available users** and **Group Members** boxes. Up to 500 users are displayed. To display fewer users, refine your search criteria:



The available users are those harvested from the emails sent from your organization (see above), and those previously added manually or uploaded to a group.

5. Click the **Add** button.
6. The email address is shown in the **Group Members** box.
7. Click **Save**.

To create a new user for a custom group

1. Select **Configuration > Email Services > Content Control**.
2. In the **User Groups** tab, locate and select the group to create the new user for.
 - The **Edit User Group** page is displayed.
3. Add a new email address in the **New users** box.
4. Click **Save**.

5.4. Editing a Custom User Group in Email Content Control

You can maintain a custom user group either manually in ClientNet or using a CSV file:

- Manually—edit the group name, and/or add and remove users from the group
- Using a CSV (comma-separated values) file—create, or download, a CSV file of the users belonging to a user group. Add new email addresses, or edit existing ones, offline. Upload the list to ClientNet.

5.4.1 Editing a user group manually in ClientNet

To edit a custom user group manually

1. Select **Configuration > Email Services > Content Control**.
2. In the **User Groups** tab, click on the name of the group to edit from the **Group name** column.
 - The **Edit User Group** page is displayed. Locate an existing member of the group by using the **Search existing users** box. Only 500 users are displayed at a time. To avoid too long a list, narrow your search criteria.
3. Edit the group details as required, as required.
4. Click **Save**.

To delete a custom user group

You cannot delete a user group if it is in use in a rule.



After you click the **Delete selected group(s)** button, you are not asked to confirm the delete operation.

1. Select **Configuration > Email Services > Content Control**.
2. In the **User Groups** tab, select the checkbox next to the name of the group to delete.
3. Click the **Delete selected group(s)** button.
4. Click **Save**.

To delete a user from a custom user group

Deleting a user from a group does not permanently delete the user, but merely removes it from the user group or groups that it is associated with.

1. Select **Configuration > Email Services > Content Control**.
2. In the **User Groups** tab, select the checkbox next to the group name that contains the user to delete.
3. Click the **Delete users** button.
 - The **Delete Users** window is displayed.
4. Locate an existing user, using the **Search existing users** box.
 - If you enter a period '.' into the search string, an alphabetical list of all available users is displayed in the Existing users box. To avoid the list becoming too long, only the first 500 users are shown. If more than 500 users are available, use the search facility to reduce the list size.
5. Highlight the required user and click the **Delete** button.
 - The address of the user to delete is displayed in the **Deleted Users** box.
6. Click **Delete users**.

5.4.2 Editing a user group using a CSV file

To download a list of users in a custom user group

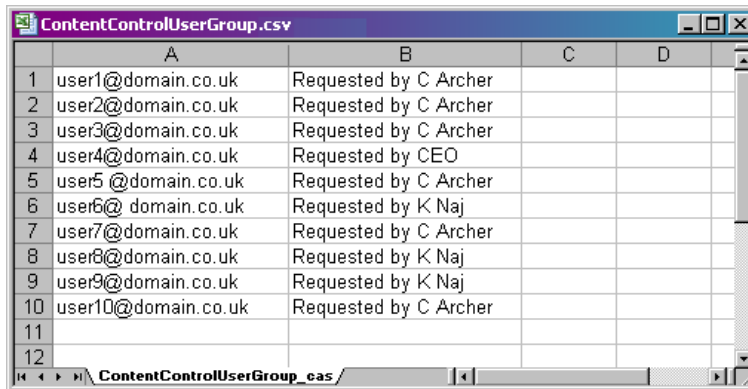
1. Select **Configuration > Email Services > Content Control**.
2. In the **User Groups** tab, locate the name of the group to download and click the **Download** button.
 - A dialog box asks you whether to open or save the CSV file. The file is called **ContentControlUserGroup.csv**, but you can rename it if you wish.



The download operation may take some time to complete depending on the size of the list. You can now edit the file to your requirements, and upload it back to ClientNet.

To edit a CSV list of users in a group

1. Open a new or a previously downloaded CSV file.
2. Edit the file to your requirements.
 - The following screenshot shows the content of a list of users in Microsoft Excel



	A	B	C	D
1	user1@domain.co.uk	Requested by C Archer		
2	user2@domain.co.uk	Requested by C Archer		
3	user3@domain.co.uk	Requested by C Archer		
4	user4@domain.co.uk	Requested by CEO		
5	user5@domain.co.uk	Requested by C Archer		
6	user6@domain.co.uk	Requested by K Naj		
7	user7@domain.co.uk	Requested by C Archer		
8	user8@domain.co.uk	Requested by K Naj		
9	user9@domain.co.uk	Requested by K Naj		
10	user10@domain.co.uk	Requested by C Archer		
11				
12				

- The first column contains the email address.
- The second column contains associated descriptions (optional).



To simplify the list, use wildcards to detect email addresses with slight differences in spelling, for example, *fre*@-domain.com* represents *fred@domain.com* or *freda@domain.com*.

3. Save the file as a CSV file.

To upload a list of users for a custom user group



The file to upload must be a CSV file.

1. Select **Configuration > Email Services > Content Control**.
2. In the **User Groups** tab, select the **Upload** button next to the name of the group to upload. The **Upload users** window is displayed.
3. In the **Select file to upload** field, enter the file path and filename to upload or click **Browse** to locate the file.
4. Select either:
 - *Delete existing addresses and replace with uploaded addresses* – by selecting this option, the uploaded list replaces the existing list. Any entries in the existing list that are not in the uploaded list are lost.
 - *Merge existing addresses with uploaded addresses* – by selecting this option, the uploaded list merges into the existing list. This is a useful way to add new entries to an existing list.
5. Click **Upload**.
 - If the file contains invalid entries, an error message displays the first 100 invalid addresses but continues to upload all the valid addresses. If this is displayed, click **OK**.
 - A confirmation message is displayed.
6. Click **OK**

6 Working With Lists

The Email Content Control service works by matching terms or expressions, and other items of information, contained within various parts of an email. For example, to stop outbound emails that contain potentially sensitive information, define a list of unacceptable terms, and create a rule to specify the list as the email content to trigger the rule. The following types of content can be defined as lists.

- *Text content* – sets of words and phrases, for example, profanities
- *MIME types* – emails and attachments are compared against a selected list of MIME types, for example, applications, audio, video, and email types
- *File names* – sets of file names or extensions
- *URLs* – addresses for websites, for example, to detect emails that direct users to competitor, job alert, or pornographic websites, etc.
- *Domain names* – a list of domain names can be used in a similar way to user groups, for example, to detect emails sent by competitors or your sister organizations

You can also create a superlist. This is a list that contains other lists of the same type. The functionality to concatenate lists into a superlist enables, for example, lists of profanities in English, German, and French, to be gathered into a European profanity superlist.

6.1. Pre-defined Lists

The Email Content Control service includes a number of pre-defined text content lists, containing words and phrases in English, French, and German that assist in identifying unacceptable language such as profanities, and racial and sexual terms. A text content list contains discrete words and phrases. A word is only matched against a complete lexical element. For example, the word 'prove' is not matched with 'approve' or 'improvement'.

Several pre-defined lists are available for you to use. We recommend that you select a list and cut and paste relevant words to create your own list that reflects your organizational policy. The pre-defined lists are not complete and the words and lists provided are simply examples to reflect some possible policies that an organization may have in place. For guidance:

- The standard **Profanity**, **Racial**, and **Sexual** lists contain strong language. If your policy does not condemn this language being transmitted externally, we recommend you use either the 'copy to administrator' or 'redirect' actions to enable you to see trends in the organization.
- The **Ambiguous** lists contain words with two meanings. When constructing a list, a word may be acceptable in one context and not in another. We do not recommend blocking or redirecting mail containing words on these lists.
- The **Mild** lists contain words that may be considered unprofessional in external email. You may wish to copy these mails to the administrator so that you can spot trends.

The Email Content Control service also includes a comprehensive pre-defined list of MIME types containing types and subtypes. These can be used in email content conditions, for matching against the MIME types of emails themselves, and in attachment conditions, for matching against the MIME types of attachments.

The pre-defined lists are visible when you are creating or editing a rule, in the **Email content** tab; they are not visible when creating lists in the **Lists** tab. When creating a rule, select a pre-defined list and then you can amend it to suit the individual condition by selecting **Customize**. This does not modify the existing list but creates expressions specific to the condition.

6.2. Defining Lists at Various Levels

Global and domain level lists can be used by any condition within a rule that requires a list; that is, for sender, recipient, email content, and attachment conditions. For example, a domain list can be used as a sender or recipient condition, a URL list can be used as an email content condition, and a filename list can be used as an attachment condition. To manage lists across all domains, have **Global settings** selected. Manage lists specific to an individual domain, by selecting the required domain from the **Global settings** drop-down list.

You can also customize a list at the rule level. A customized list is specific to a condition and cannot be used by other conditions within the same or different rules. It is sometimes useful to create a default list (at global or domain level) and then make additions or remove items at the rule level. If you do this, the changes do not affect the original list.



Lists defined at global level can be applied to an individual domain but cannot be modified at that level. However, they can be customized within a specific rule.

For more on working at global and domain levels, see [Section 3.4 , Global and domain settings for Content Control.](#)

6.3. Valid and Invalid Characters and Characteristics of Lists

All lists managed via ClientNet support cut and paste functionality. You can create up to 500 lists, each of which can contain up to 2,000 entries.

In addition to the Latin character set, lists support an extended character set, which enables you to enter specific words or phrases in non-Western characters – specifically Japanese, Chinese, and Korean. The following guidelines apply for the five types of lists that you can create:



You can enter characters in extended character set languages into your email content lists. This means that list items in Japanese, Korean, Chinese, and Russian, for example, will be identified in the scanning process. For full details of character sets supported for use in Content Control lists, see *Section Appendix 1: , Non-Latin-based language support*.

List Type	Description	Valid Characters & Invalid Characters of this List Type
Email Content	Text content lists can be used where 'Email content' conditions are required. The content of an email can be matched against entries in a pre-defined or custom list of words and/or phrases	<ul style="list-style-type: none"> o Digits are supported o Spaces are not supported o The following characters are not supported because they are commonly used in coding or scripts: " & ' < > . - + = { } [] ; : @ ~ # \ / \ , ! £ \$ % A () <p>NOTE: A period (.) may be treated as a blank or as a space, and so should be used carefully if included in text content checking – it is better to consider the character as not supported.</p> <ul style="list-style-type: none"> o The following character is supported: - o Wildcards are supported with the following characters (these are only recognized as wildcards and are not translated literally): <ul style="list-style-type: none"> o * represents zero or more characters. Thus B*d will stop Bold, Bid and Billiard. o ? represents a single character. Thus B?d wil stop Bid, Bad and Bod Digits.
MIME Types	MIME type lists can be used where email content and attachment conditions are required. The MIME types can be matched against entries in a pre-defined or custom list of types. There is a comprehensive predefined MIME type list from which you can copy and paste entries for your own lists, for example, if you are unsure of all of the file extensions that are available	<ul style="list-style-type: none"> o Digits are supported o Spaces are not supported o The following characters are not supported: ! " £ \$ % A & () = { } [] ; : @ ' ~ # \ < > , ? o The following characters are supported: \$ - - + o * is supported as a wildcard only o / is supported as a type/subtype separator only o Wildcards are supported to indicate all subtypes for the specified type, for example: Entries must take one of the following forms: <ul style="list-style-type: none"> o type/subtype specific type and subtype o type/* all subtypes for specified type o Validation of MIME type and subtype text is not performed.
File Names	File name lists can be used where attachment conditions are required. File names of email attachments can be matched against entries in a custom list.	<ul style="list-style-type: none"> o Digits are supported o Spaces are supported o The following characters are not supported: " & ; ' \ < > ? o The following characters are supported: ! £ \$ % A () - - + = { } [] ; : @ ~ # o The use of * as a wildcard is allowed, for example: topsecr* *.exe file*.com
URLs	URL lists can be used to detected content in the form of a URL within an email body, header, or subject. This	<ul style="list-style-type: none"> o URL entries must be of the following formats: <ul style="list-style-type: none"> o http://www.xxxxxx.com o https://www.xxxxxx.com o Wildcards are supported with the following characters (these are only

	<p>enables you to restrict the communication of specified URLs around the business and to remove any encouragement for employees to access specific websites. This can be used in combination with the MailStreet Boundary Defense for Email Web Security and Management service to provide complete protection against a user accessing inappropriate or malicious websites</p>	<p>recognized as wildcards and are not translated literally):</p> <ul style="list-style-type: none"> o * represents zero or more characters o ? represents a single characters <p>THUS</p> <ul style="list-style-type: none"> o http://www.*.com will stop all URLs that take the .com format o www.ford*.com will stop http://www.fordcar.com and http://www.-fordescort.com o http://www.ford.* will stop http://www.ford.com, http://www.ford.co.uk, etc.
<p>Domain Lists</p>	<p>Domain lists can be used where sender or recipient conditions are required. The sender and/or recipient of an email can be matched against entries in a custom list</p>	<ul style="list-style-type: none"> o The use of digits are supported o The use of spaces is not supported o The following characters are not supported because they are not permitted in domain names by RFC standards: ! " £ \$ % & ' () * + = { } [] ; : @ ' ~ # / \ < > , ? o The following character is supported: - o The following character is as a sub-domain separator only: . o It is possible to use the * as a wildcard within the domain section, for example: <ul style="list-style-type: none"> o *.example.com stops a subdomain of example.com <p style="text-align: center;">OR</p> <ul style="list-style-type: none"> o example.* stops example.com, example.net, example.co.uk, etc.



You cannot define your own email template list. A pre-defined email template list – which detects specific alphanumeric characters in a set format, e.g. Social Security numbers, or credit card numbers – is available to use when you create a rule. If you have additional requirements for templates, please contact your MailStreet Boundary Defense for Email Client Services representative.

6.4. Viewing Your Lists

To view your lists:

1. Select Configuration > Email Services > Content Control.
2. Click the *Lists* tab.
3. The lists that you can modify at the level you have selected (global or domain) are displayed.

6.5. Seeing the Rules That Use a Specific List

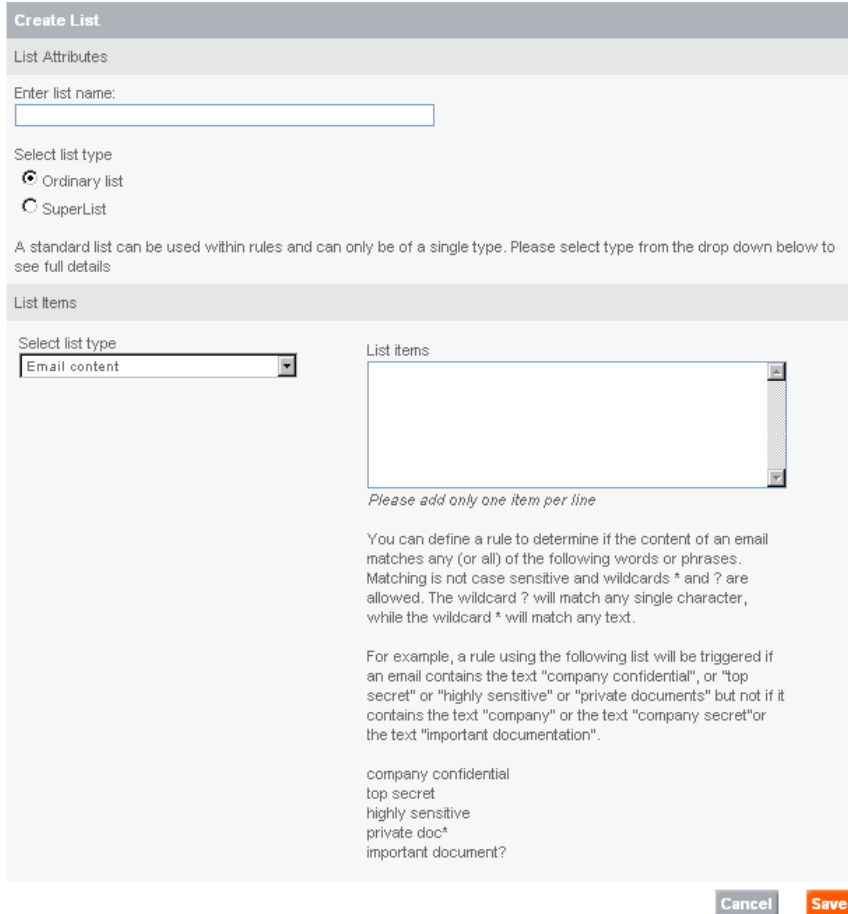
To see the rules that use a specific list:

1. Select **Configuration > Email Services > Content Control**.
2. Click the *Lists* tab.
3. Locate the required list and select the link in the **In Use** column.

6.6. Creating a List

To create a list:

1. Select **Configuration > Email Services > Content Control**.
2. In the **Lists** tab, click the **Create new list** button.
 - The **Create List** page is displayed



The screenshot shows the 'Create List' form. It has a title bar 'Create List' and a section 'List Attributes'. Under 'List Attributes', there is a text input field for 'Enter list name:'. Below that, there are two radio buttons for 'Select list type': 'Ordinary list' (selected) and 'SuperList'. A note states: 'A standard list can be used within rules and can only be of a single type. Please select type from the drop down below to see full details'. The 'List Items' section contains a 'Select list type' dropdown menu with 'Email content' selected. To the right is a large text area for 'List items' with a vertical scrollbar. Below the text area is the instruction 'Please add only one item per line'. Further down, there is explanatory text: 'You can define a rule to determine if the content of an email matches any (or all) of the following words or phrases. Matching is not case sensitive and wildcards * and ? are allowed. The wildcard ? will match any single character, while the wildcard * will match any text. For example, a rule using the following list will be triggered if an email contains the text "company confidential", or "top secret" or "highly sensitive" or "private documents" but not if it contains the text "company" or the text "company secret" or the text "important documentation".' Below this text is a list of example items: 'company confidential', 'top secret', 'highly sensitive', 'private doc*', and 'important document?'. At the bottom right of the form are 'Cancel' and 'Save' buttons.

3. Enter a name for the list.
 - The list name must be unique, only contain alphanumeric characters and spaces (but no other character types), begin with an alphabetic character, and not exceed 50 characters.
4. Select the **Ordinary list** option button.
5. Select the type of list to create from the **Select list type** drop-down list.
6. In the **List items** box, enter the items for the list. See Valid and invalid characters and characteristics of lists. Cut and paste functionality is available in this box.
7. Click **Save**.



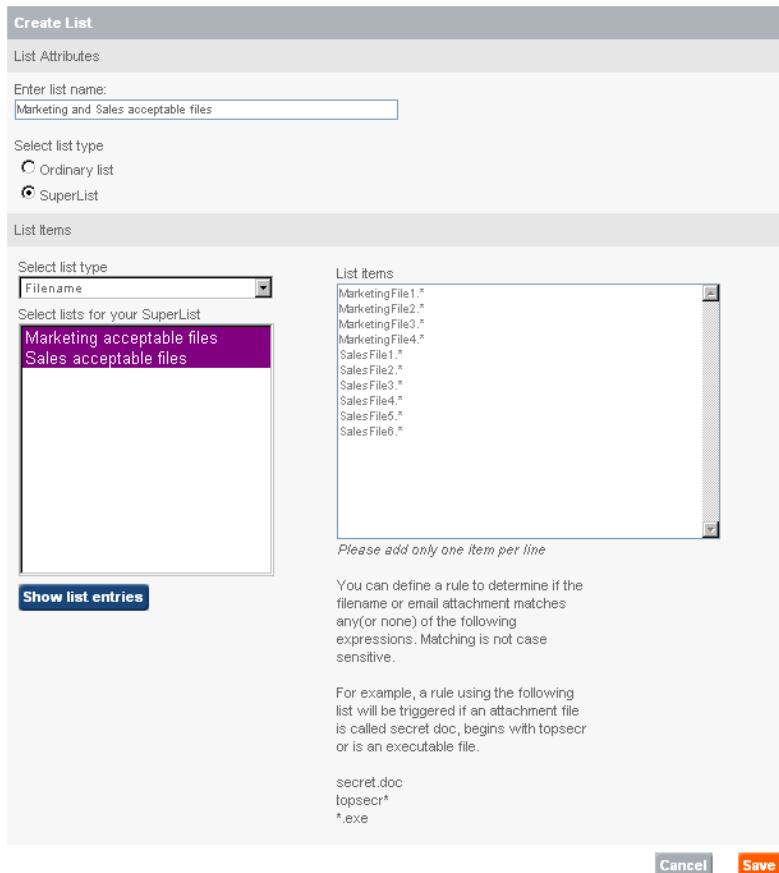
When you select a **List type**, explanation text provides you with hints specific to that list type.

6.7. Creating a Superlist

A superlist is a list that contains multiple lists of the same type, that is, email content, domain name, URL, MIME type, or file name. The functionality to link lists into a superlist, enables, for example, lists of profanities in English, German, and French, to be gathered into a European profanity list. If a change is made to an ordinary list contained within a superlist, the change affects the superlist too. However, if you make a change to a superlist, the component lists are not affected. A superlist can only contain lists of the same type.

To create a superlist:

1. Select **Configuration > Email Services > Content Control**.
2. In the *Lists* tab, click the Create new list button.
 - The **Create List** page is displayed
3. Enter a name for the superlist.
 - The superlist name must be unique, only contain alphanumeric characters and spaces (but no other character types), begin with an alphabetic character, and not exceed 50 characters.
4. Select the **SuperList** option button.
5. Select the type of superlist to create from the **Select list type** drop-down list.
6. The **Select lists** for your superlist box displays the available lists of the selected type.



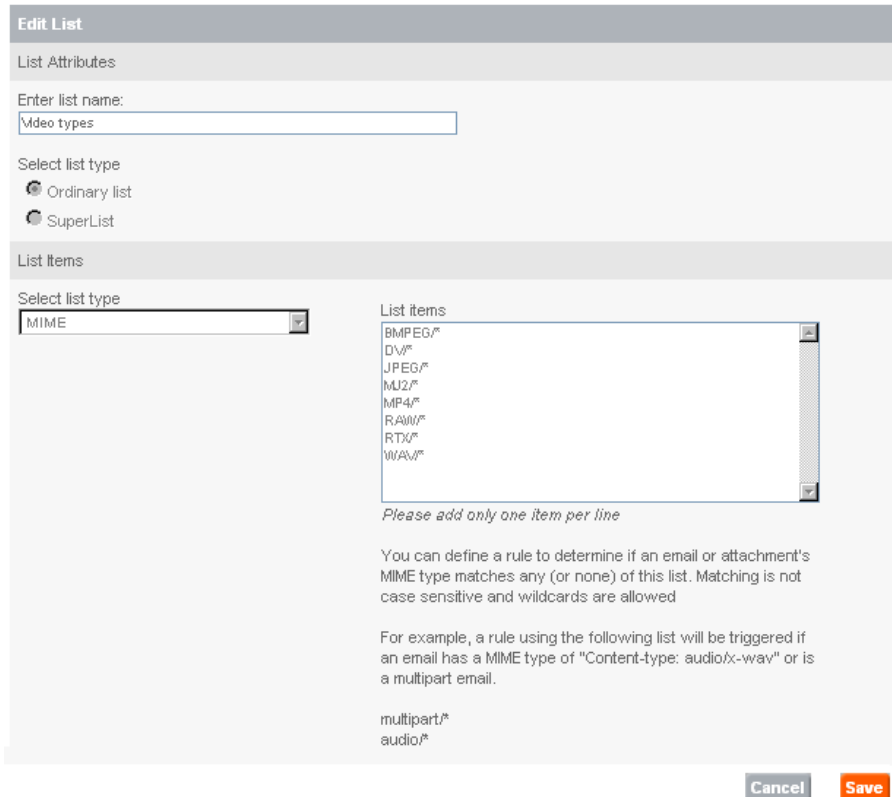
7. Select the lists to add to the superlist by clicking on the list name.
 - The expressions from the selected lists are displayed in the **List items** box.
8. In the **List items** box, you can amend, add to, or remove any expressions in the new superlist.
 - Any changes you make do not affect the ordinary list from which the expressions come. Cut and paste functionality is available in this box. For the valid and invalid characters and the characteristics of each list type, see Valid and invalid characters and characteristics of lists.
9. Click **Save**.

6.8. Editing a List

You can edit the name of a list and the items within it. However, you cannot change the list type, due to the variation in expected content between different list types.

To edit a list:

1. Select **Configuration > Email Services > Content Control**.
2. In the **Lists** tab, locate the list to edit and click on its name in the **List name** column.
 - The **Edit List** page is displayed.



3. In the **List items** box, edit the items in the list as required.
 - Cut and paste functionality is available in this box. For the valid and invalid characters and the characteristics of each list type, see Valid and invalid characters and characteristics of lists.
4. Click **Save**.

6.9. Deleting a List

You can only delete a list if it is not used in any rule. Also, you cannot delete any of the pre-defined MailStreet Boundary Defense for Email lists.



After you click the **Delete selected item(s)** button, you are not asked to confirm the delete operation.

To delete a list:

1. Select **Configuration > Email Services > Content Control**.
2. In the **Lists** tab, select the checkbox next to the list to delete.
3. Click the **Delete selected list(s)** button.

7 Rules in Email Content Control

The Email Content Control service enables you to control your inbound and outbound email. You can define rules to filter email according to who sent it, who it was sent to, what it contained, and so on.

7.1. Introduction to Rules in Email Content Control

A rule is made up of the following components:

- A *descriptive name* – MailStreet Boundary Defense for Email recommends using meaningful names for your rules so that they will be appropriate in the various contexts in which they are displayed. For example, when a rule is triggered the rule name may be included in the notification email sent to an administrator. Avoid using unacceptable language in a rule name because this will appear in statistics, reports, X-Headers, etc.
- A *set of conditions* that must be met in order to trigger the rule – you can define whether all or any of the specified conditions must be met to trigger the rule. Being able to define AND or OR relationships between components of a rule provides you with the flexibility to configure your rules to your needs very specifically.
- An *action* that is performed when an email satisfies the conditions of the rule

Each rule is created by combining a set of individual conditions that characterize a particular circumstance. The more conditions that are defined, the more specific the rule becomes.

Conditions can be used in your rules

	Condition	Description
Who	Sender	A user group, a list of domains, a single email address, a single domain, or domains containing wildcards
	Recipient	A user group, a list of domains, a single email address, a single domain, or domains containing wildcards
Where	Email body, subject line, attachment (including in MS Office documents and archive files), and header	Specify which parts of an email to scan for content (can include wildcards)
What	Email content	Lists of words and phrases
	Email MIME type	Lists of email MIME types
	File attachment names and types	Lists of file names, file types and MIME types
	URLs	Lists of URLs
	Templates	Pre-defined formats, such as US Social Security numbers or credit card numbers
	Spoofed file attachments	Files masquerading as other types
	Encrypted messages	S/MIME encrypted content
	Password-protected files	MS Office files that have been password-protected
	Overall size of the email	The size of the email including any attachments
	Priority/urgency of the email	The priority applied to an email by the sender; either low, normal, or high
	Number of attachments	The number of attachments
Size of attachments	The combined size of all attached files	
When	Email receipt or send time	Select from a set of time periods

Example

To identify messages that are sent from either the Sales team or anyone in the abc.com domain, and that contain profanities or are over 25MB, you would create the rule as follows:

Define the rule, for example, at global level using the following conditions:

- Sender condition 1 – sender is in the Sales team (set up as a user group) OR

- Sender condition 2 – sender is in the abc.com domain (set up as a domain)
 - Email content condition 1 – email contains words on the profanity lists
- OR
- Email content condition 2 – email is over 25MB Define one of the following actions for this rule.
One of:
 - o Log only
 - o Compress attachments
 - o Block and delete
 - o Tag with header
 - o Copy to administrator
 - o Redirect to administrator
 - o Tag subject line



For further details of actions, see [Section 7.3.6.1 , Defining an action for a rule.](#)

You can apply each rule to:

- Inbound email only
- Outbound email only
- Both inbound and outbound email

Rules are executed in the sequence in which they are listed. Each rule is executed in turn until an action that stops the scan for that email is reached – an exit action. The exit actions are *Block and delete*, and *Redirect to administrator*. A single email might trigger more than one rule. Therefore building the correct sequence of rules ensures that priority rules appear earlier in the sequence. New rules are appended to the end of the rule listing, to avoid overwriting any existing rule sequence.

When the scanner is evaluating an email, if a 'block and delete' or 'redirect' action is encountered in the rule sequence, that action is taken and no subsequent rules are applied to that email for the recipient to whom that rule applies.

An email may trigger more than one rule and therefore may result in more than one action. However, an email is never copied or redirected to an administrator on multiple occasions. In this case, a single email that contains a summary of all of the triggered actions is sent to the administrator.

An email with multiple recipients can be regarded as multiple single-recipient emails. Different rules may apply depending on which recipient the particular email is directed to.

To add further flexibility, you can invert most conditions – that is, you can define actions that are triggered if the message does *not* meet a particular condition.

7.2. Viewing and Managing Email Content Control Rules

When you have created your Email Content Control rules, you can view the pertinent details of them in a list, view a summary of a rule's conditions, edit them, delete them, move their position in the list, copy them to other domains, and activate and deactivate them.



For full details of creating rules, see [Section 7, Rules in Email Content Control](#).

7.2.1 Viewing your rules

To view your rules

1. Select **Configuration > Email Services > Content Control**.
2. Click the **Rules** tab.
 - The rules that are available for modification at the level you have selected (global or domain) are displayed. The action that is applied to a rule and its direction are also displayed. You can use this page to copy a rule to another domain, move a rule up or down the scan order, or deactivate a rule temporarily, instead of having to delete and recreate it.

To view rules that apply to a specific user group

1. Select **Configuration > Email Services > Content Control**.
2. Click the **User Groups** tab.
3. Locate the rule of interest and select the corresponding link in the **In Use** column.

To view the summary of a rule's conditions



To specify whether all or at least one of the tabs must be satisfied to trigger the rule, see [Section 7.3.1, Defining 'all' or 'any' condition](#).

1. Select **Configuration > Email Services > Content Control**.
2. In the **Rules** tab, click the name of the rule.
3. Click the **Summary** tab.
4. The conditions of the rule are set out so that you can see all of the conditions of the rule in an easy-to-read format.

7.2.2 Managing your rules

To delete a rule



When you delete a rule, you are not asked to confirm the deletion.



Instead of deleting a rule, if you think you may need to use the rule in future, you can deactivate it (see above.)

1. Select **Configuration > Email Services > Content Control**.
2. In the **Rules** tab, select the checkbox to the left of the rule to delete.
3. Click the **Delete selected** button.

To copy a rule

You can copy a rule to the same domain, to another domain, or to global level so that it applies to all domains. It may be useful to copy a rule that contains common conditions to the same domain, make minor amendments, and rename it. You can also use this functionality to set up and test a rule set within a test domain, and transfer the rules to another domain without having to re-enter them.

Only one rule can be copied at a time. The name of the copied rule is appended with (n), where n is the next incremented number required to ensure a unique rule name. The copied rule is appended to the end of the rule list to avoid overwriting your existing rule sequence. When a rule is copied, it retains the state of the original rule; that is, whether the rule is active or deactivated.

1. Select **Configuration > Email Services > Content Control**.
2. In the **Rules** tab, select the checkbox to the left of the rule to copy.
3. Click the **Copy selected** button.
The **Copy rule** window is displayed.

Copy rule

Rule name

You have selected to copy the following rule

Copy of Email to and from competitors

Copy rule to the following domain:

Select which domain you would like this rule to be copied to:

Copy rule to another domain

Select domain:

Copy rules to global level

4. Use the option buttons to define whether to copy the rule to another domain or to global level. If you are copying the rule to another domain, select the domain to copy it to from the drop-down list.
5. Click **Save**.

To edit a rule

You can edit a rule's name and any of the conditions and other settings for a rule.

1. Select **Configuration > Email Services > Content Control**.
2. In the **Rules** tab, click on the name of the rule to edit

Rules | **User Groups** | Lists | Settings

Showing 1 - 8 of 8 << First | < Previous | Next > | Last >>

<input type="checkbox"/>	Rule name	Action and notifications	Last updated	Direction	
<input checked="" type="checkbox"/>	Block email over 25MB	Block and delete	03 October 2006 01:49 GMT, Steve	Inbound or Outbound	<input type="button" value="De-activate"/>

<< First | < Previous | Next > | Last >>

The **Edit Rule** pages are displayed. The tabs contain the settings for the rule to edit. Navigate to the relevant tabs to make the changes you require. For full details of the settings for rules, see [Section 7, Rules in Email Content Control](#).

3. Click **Save and exit**.

7.2.3 Activating and deactivating a rule

If you have created a rule and do not wish to use it, but may in the future, instead of deleting it you can deactivate it. Then you can reactivate it as required.

To activate and deactivate a rule

1. Select **Configuration > Email Services > Content Control**.
2. In the **Rules** tab, locate the required rule, and in the right hand column click the **Activate** or **De-activate** button to change the status.
 - You do not need to save this change; it is effective immediately.

7.2.4 Changing the position of a rule

A single email might trigger more than one rule. Therefore building the correct sequence of rules ensures that priority rules appear earlier in the sequence. Rules are executed in the sequence in which they are listed. Each rule is executed in turn until an action that stops the scan for that email is reached – an exit action. The exit actions are Block and delete, and Redirect to administrator. When the scanner is evaluating an email, if a block and delete or redirect action is encountered in the rule sequence, that action is taken and no subsequent rules are applied to that email for the recipient to whom that rule applies.

You can move a rule within the list. For example, any emails to be deleted should be positioned before other rules so that they are deleted first and do not continue to be scanned for other rules. The following two rules should be ordered as shown:

- Block and delete all email that is over 5MB
- Copy emails containing profanity to the administrator

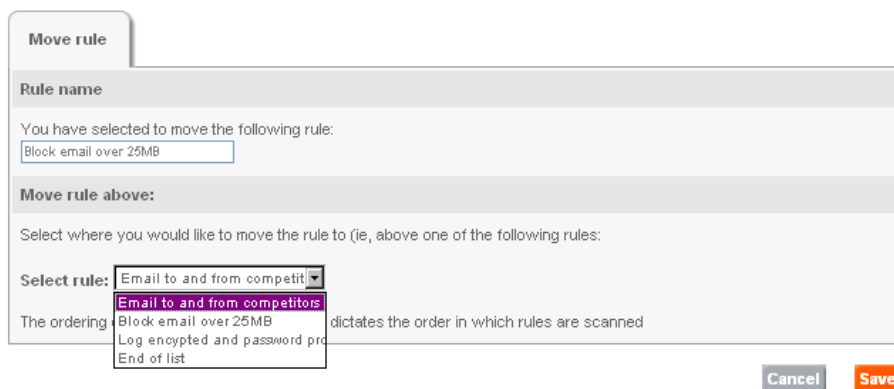


Once the move has been validated, all subsequent rules affected by the move are automatically re-sequenced.

To move a rule

1. Select **Configuration > Email Services > Content Control**.
2. In the **Rules** tab, select the checkbox to the left of the rule to move.
3. Click the **Move selected** button.

The **Move rule** window is displayed.



4. The drop-down list displays the existing rules in order. Select the position to move the rule to, that is, above an existing rule.
5. Click **Save**.
 - The list of rules is displayed with the rule in its new position.

7.3. Defining an Email Content Control Rule

Most rules require that user groups (for sender and recipient conditions) and lists (for email content and attachment conditions) are defined. For full details of working with user groups and lists, see [Section 5 , User Groups in Email Content Control](#). and [Section 6 , Working with lists](#).

You can create up to 500 rules. Typically, between five and ten are enough to define a comprehensive rule set. You can define rules at global and domain level. Rules defined at the global level can be applied for an individual domain by copying the rule to the domain (see [Section 7.2. , Viewing and managing Email Content Control rules](#)).

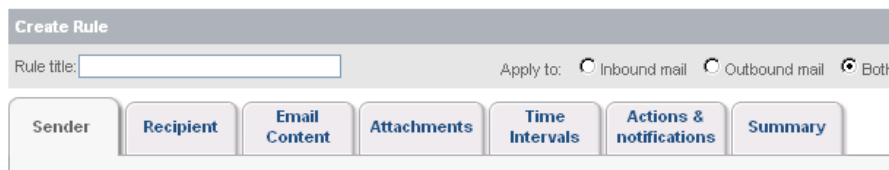
Likewise, a rule defined for a domain can be copied to global level. (For more on working at global and domain levels, see [Section 3.4. , Global and domain settings for Content Control](#).)



If you have defined any custom settings (for example, for a domain) and you switch from using custom settings back to using global settings, the settings in the page display the global settings. However, your custom settings for that domain are remembered and when you switch back to **Use custom settings**, your custom settings are again displayed.

To define a rule

1. Select **Configuration > Email Services > Content Control**.
2. In the **Rules** tab, click the **Create new rule** button.
The **Create Rule** page is displayed.



3. Enter the rule title.
The rule title can contain up to 255 alphanumeric characters including spaces, but no other character types. The rule title is displayed at the top of all of the pages within these rule configuration tabs.
4. Using the **Apply to** option buttons at the top of the page, select whether the rule is to apply to inbound mail, outbound mail, or both.
5. Use the settings in each tab to define the conditions, actions, and notifications for the rule.



You can navigate between the tabs without saving the changes you make in an individual tab. The **Save and exit** button affects all of the rule's tabs collectively.

7.3.1 Defining 'all' or 'any' conditions

You can define whether all or any of the conditions defined within a tab must be met to trigger the rule – that is, within the **Sender**, **Recipient**, **Email content**, or **Attachment** tabs.

As well as having this flexibility within a tab, you can also define whether any or all of the tabs themselves need to be met to trigger the rule, using the **Summary** tab. For example, you can specify that both the sender and recipient conditions must be met or that the conditions in just one of those tabs can be met.

To define any or all conditions within a tab:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule.
3. In the **Rule conditions** section of the **Sender**, **Recipient**, **Email content**, or **Attachment** tabs (as required), select the appropriate option button depending on whether at least one or all of the conditions defined within the tab should be met to trigger the rule.



Sender Recipient **Email Content** Attachments Time Intervals Actions & notifications Summary

Rule conditions

At least one of the conditions below needs to be satisfied for this rule to be triggered

All of the conditions below need to be satisfied for this rule to be triggered

To define any or all conditions between tabs:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule.
3. Click the **Summary** tab.



Sender Recipient Email Content Attachments Time Intervals Actions & notifications **Summary**

Rule summary

All tabs must be satisfied to trigger this rule

At least one of the tabs must be satisfied to trigger this rule

4. In the **Rule summary** section, select the appropriate option button depending on whether at least one or all of the conditions defined within each tab should be met to trigger the rule.

7.3.2 Defining sender and recipient conditions

For an Email Content Control rule to apply to specific senders and recipients (rather than all senders and recipients), use the **Sender** and **Recipient** tabs when creating a rule.

You can build sender and recipient conditions based on:

- User groups (see [Section 5, User Groups in Email Content Control](#))
- Domain lists (see [Section 6, Working with lists](#))

Edit Rule

Rule title: Apply to: Inbound mail Outbound mail Both

Sender
Recipient
Email Content
Attachments
Time Intervals
Actions & notifications
Summary

Rule conditions

At least one of the conditions below needs to be satisfied for this rule to be triggered
 All of the conditions below need to be satisfied for this rule to be triggered

User groups

Use user groups in this rule

Senders in ANY of the selected groups
 Sender in ALL selected groups
 All senders EXCEPT those in selected groups

Use the options below to search for groups already selected for this rule. To find groups currently not used in this rule, use the Add Group option to find and select the group you want to use.

Group name: Group type:

The table below includes only the groups that have been selected for this rule.

Showing 1 to 3 of 3 Entries Per Page: << First < Prev Next > Last >>

<input type="checkbox"/>	Selected Groups	Type	Members	In Use?	Last Modified
<input type="checkbox"/>	Administrators	LDAP	0	11	05 Oct 2009 9:19 AM
<input type="checkbox"/>	Legal	Custom	3	5	05 Oct 2009 11:10 AM
<input type="checkbox"/>	Marketing	Custom	3	7	05 Oct 2009 11:11 AM

Domain lists

Use domain lists in this rule

Senders in ANY of the selected domains All senders EXCEPT those in selected domains

Select a list of domains:

Selected domain list

- company1.com
- company2.com
- company3.com

Customize this list

To define sender conditions using user groups

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.
3. Click the **Sender** tab.
4. In the **User groups** section, select the **Use user groups in this rule** checkbox. The groups that are available to use in the rule at this level are displayed.



To locate specific user groups in the **Selected groups** list, use the search controls.

5. Select the appropriate option button depending on whether the rule should apply to senders/recipients in all, any, or none of the groups that you will select next:

- **Senders in ANY of the selected groups**—the rule will be triggered if an email that meets the rule's conditions is sent to *any* of the users in the selected groups

- **Senders in ALL selected groups**—the rule will be triggered if an email that meets the rule's conditions is sent to *all* of the users in the selected groups
 - **All senders EXCEPT those in selected groups**—the rule will be triggered if an email that meets the rule's conditions is sent to *none* of the users in the selected groups
6. To add a group to use in the rule, click the **Add Group** button.
The available groups are listed.
 7. Locate and select the group(s) to use in the rule.
 8. Click the **Add Selected** button.
 9. Newly added groups are displayed in the **Selected groups** list.
 10. To save the rule, click **Save and exit**.

To define recipient conditions using user groups

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.
3. Click the **Recipient** tab.
4. In the **User groups** section, select the **Use user groups in this rule** checkbox.
The groups that are available to use in the rule at this level are displayed.



To locate specific user groups in the **Selected groups** list, use the search controls.

5. Select the appropriate option button depending on whether the rule should apply to recipients in all, any, or none of the groups that you will select next:
 - o **Recipients in ANY of the selected groups**—the rule will be triggered if an email that meets the rule's conditions is received from *any* of the users in the selected groups
 - o **Recipients in ALL selected groups**—the rule will be triggered if an email that meets the rule's conditions is received from *all* of the users in the selected groups
 - o **All recipients EXCEPT those in selected groups**—the rule will be triggered if an email that meets the rule's conditions is received from *none* of the users in the selected groups
6. To add a group to use in the rule, click the **Add Group** button. The available groups are listed.
7. Locate and select the group(s) to use in the rule.
8. Click the **Add Selected** button.
9. Newly added groups are displayed in the **Selected groups** list.
10. To save the rule, click **Save and exit**.

To define sender conditions using domain lists

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.
3. Click the **Sender** tab.
4. In the **Domain lists** section, select the **Use domain lists in this rule** checkbox.
The domain lists that are available to use in the rule at this level are presented in the drop-down list.
5. Select the appropriate option button depending on whether the rule should apply to senders in any or none of the domains you will define next.
 - o **Senders in ANY of the selected domains**—the rule will be triggered if an email that meets the rule's conditions is sent to *any* of the users in the selected domains
 - o **All senders EXCEPT those in selected domains**—the rule will be triggered if an email that meets the rule's conditions is sent to *none* of the users in the selected domains

6. From the **Select a list of domains** drop-down list, either:
 - a. Select an existing list. The entries in the list are added to the **Selected domain list** box. To add further entries to the **Selected domain list** box, click the **Customize this list** checkbox. The box becomes editable for you to add domains.



Any additional entries you add here are not saved to the original domain lists.

- b. Select **<Custom list>**. The **Selected domain list** box is editable, for you to enter your domain entries for this rule.



For details of wildcards and other valid characters, see [Valid and invalid characters and characteristics of lists](#).

7. To save the rule, click **Save and exit**.

To define recipient conditions using domain lists

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.
3. Click the **Recipient** tab.
4. In the **Domain lists** section, select the **Use domain lists in this rule** checkbox.
The domain lists that are available to use in the rule at this level are presented in the drop-down list.
5. Select the appropriate option button depending on whether the rule should apply to recipients in any or none of the domains you will define next.
 - o **Recipients in ANY of the selected domains**—the rule will be triggered if an email that meets the rule's conditions is received from *any* of the users in the selected domains
 - o **All recipients EXCEPT those in selected domains**—the rule will be triggered if an email that meets the rule's conditions is sent to *none* of the users in the selected domains
6. From the **Select a list of domains** drop-down list, either:
 - a. Select an existing list. The entries in the list are added to the **Selected domain list** box. To add further entries to the **Selected domain list** box, click the **Customize this list** checkbox. The box becomes editable for you to add domains.



Any additional entries you add here are not saved to the original domain lists.

- b. Select **<Custom list>**. The **Selected domain list** box is editable, for you to enter your domain entries for this rule.



For details of wildcards and other valid characters, see [Valid and invalid characters and characteristics of lists](#).

7. To save the rule, click **Save and exit**.

7.3.3 Defining email content conditions

You can build email content conditions based on:

- The parts of the email in which to check for content – email body, subject line, attachments, and/or header
- Whether the email has any specific attributes – a maximum email size, is encrypted, a specified importance level, contains any password-protected files
- Comparing the content of the email against pre-defined email content lists
- Comparing the content of the email against pre-defined URL lists
- Comparing the MIME type of the email against pre-defined MIME type lists.



Conditions based on the MIME types of attachments are defined as attachment conditions. See [Section 7.3.4 , Defining attachment conditions](#).

Comparing the email template against pre-defined email template lists, for example, to detect social security numbers or credit card numbers.



Be aware of potential confusion when using email templates while at the same time using the rule condition "Scan Email header" – internal mail header information can sometimes appear in the same format as credit card or social security numbers. This could result in some emails being blocked unexpectedly.

 Notes:

- If a condition within a rule is set to *Ignore*, that condition is not used in that rule's search parameters. In a new rule, every condition is initially set to *Ignore*.
- For full details of working with lists, see *Section 6 , Working with lists*.

Create Rule

Rule title: Apply to: Inbound mail Outbound mail Both

Sender
Recipient
Email Content
Attachments
Time Intervals
Actions & notifications
Summary

Rule conditions

At least one of the conditions below needs to be satisfied for this rule to be triggered
 All of the conditions below need to be satisfied for this rule to be triggered

Scan email body Scan email subject line Scan Microsoft® Office™ & PDF documents Scan email header

Email attributes

Ignore email size Email is larger than MB(including attachments)
 Ignore encrypted emails Email is encrypted
 Ignore importance levels Email has importance level of
 Ignore password protected files Email contains these password protected file types

Email content

Ignore content Email contains ALL selected content Email contains at least of these items

Select a list of content: Selected content:
 Customize this list

URL lists

Ignore URL lists Email contains ANY of the selected URL lists of these items

Select a list of URLs: Selected URLs:

www.facebook.com
www.googlemail.com

 Customize this list

Email MIME types

Ignore mime types Email is of selected MIME type Email is of any MIME type except those selected

Select a list of MIME types: Selected MIME types:
 Customize this list

Email templates

Ignore templates Email contains text matching any of the selected templates

Select a list of templates: Selected templates:

To define the parts of the email to scan:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.

3. Click the **Email content** tab.
4. In the **Rule conditions** section, select the checkboxes, as required.
 - a. **Scan email body** – to scan for content in the body of emails
 - b. **Scan email subject line** – to scan for content that appears in the subject line of emails
 - c. **Scan attachments** – to scan for content within attached MS Office documents. This option provides protection against specific file types that are hidden within other files
 - d. **Scan email header** – to scan for content in the header of emails



The subject line is also a header, so when this option is selected, the rule also scans the subject for the specified content.

To define email attribute conditions:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.
3. Click the **Email content** tab.
4. In the **Email attributes** section, select the option buttons, as required.
 - a. **Email is larger than** – enter an email size in MB above which emails will be detected. Email size is based on the size of the whole email, including encoded attachments
 - b. **Email is encrypted** – to detect encrypted emails. The detection of encryption is based on whether the email itself is encrypted and is limited to the detection of encryption using S/MIME
 - c. **Email has importance level of** – to detect emails with a specific importance level. Enter an importance level from the drop-down list. The available options are low, normal, and high
 - d. **Email contains password-protected files** – to detect emails that contain password-protected files. This setting can help you identify if users are sending unauthorized confidential material out of the company

To define text content conditions:

1. Click the **Email content** tab.
2. In the **Email content** section, select the required option button depending on whether the scan should detect all or a specific number of phrases in the list that you will select next.

The ability to specify a minimum number of items to match with enables you to define a threshold that avoids an email being stopped if it contains, for example, a name that happens to appear on a list. (If real profanities occur in emails, the tendency is for more than one profanity to be used.)
3. Either:
 - a. **Select a list of content** (or superlist) from the drop-down list.

The expressions in the selected list are displayed in the **Selected content** box. You can customize the content for this rule, by selecting the **Customize this list** checkbox. The box becomes editable.



If you customize the list, the changes are not saved to the original list.

Or

- b. To define text content for this rule only, select **Custom list** from the drop-down list. The **Selected content** box becomes editable. Enter the custom expression for this rule. For details of wildcards and other valid characters, see Valid and invalid characters and characteristics of lists.



For full details of working with lists, see [Section 6](#), *Working with lists*.

To define URL content conditions:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**
3. Click the **Email content** tab.
4. In the **URL lists** section, select the required option button depending on whether the scan should detect all or any of the URLs in the list that you will select next.
5. Either:
 - a. **Select a list of URLs** from the drop-down list.
The URLs in the selected list are displayed in the **Selected URLs** box. You can customize the content for this rule, by selecting the **Customize this list** checkbox.



If you customize the list the changes are not saved to the original list

Or

- b. To define URLs for this rule only, from the drop-down list, select **Custom list**. The **Selected URLs** box becomes editable. Enter the custom URLs for this rule. For details of wildcards and other valid characters, see Valid and invalid characters and characteristics of lists.



For full details of working with lists, see [Section 6 , Working with lists](#).

To define email MIME type conditions:



An email MIME type condition relates to the MIME type of the actual email. To define conditions related to the MIME types of attachments, see [Section 7.3.4 , Defining attachment conditions](#).

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click the **Create new rule**.
3. Click the **Email content** tab.
4. In the **Email MIME types** section, select the required option button depending on whether the scan should detect one or none of the MIME types in the list.
5. Either:
 - a. **Select a list of MIME types** (or superlist) from the drop-down list. The items in the selected list are displayed in the **Selected MIME types** box. You can customize the content for this rule, by selecting the **Customize this list** checkbox.



If you customize the list, the changes are not saved to the original list.

Or

- b. To define MIME types for this rule only, from the drop-down list, select **Custom list**. The **Selected MIME types** box becomes editable. Enter the custom MIME types for this rule. For details of wildcards and other valid characters, see Valid and invalid characters and characteristics of lists.



For full details of working with lists, see [Section 6 , Working with lists](#).

To define email template conditions:

MailStreet Boundary Defense for Email provides a pre-defined list of templates that enable you to monitor and control specific alphanumeric characters in a set format, e.g. social security numbers, or credit card numbers. The templates include all standard ways of formatting the type of data represented (for example, US Social Security Numbers as ###-##-####, ### ## ####, ###|##|####, etc). You can monitor information matching the templates going into or out of the organization.

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rules, or click **Create new rule**.
3. Click the **Email content** tab.
4. In the **Email templates** section, select the option button if the scan should detect any (rather than all) of the templates that you will select next.
5. **Select a list of templates** from the drop-down list.

The items in the selected list are displayed in the **Selected templates** box.



Be aware of potential confusion when using email templates while at the same time using the rule condition “Scan Email header” – internal mail header information can sometimes appear in the same format as credit card or social security numbers. This could result in some emails being blocked unexpectedly



For full details of working with lists, see *Section 6, Working with lists*.

7.3.4 Defining attachment conditions

You can build attachment conditions based on:

- Maximum size of attachments
- Maximum number of attachments
- Whether the file extension matches the implied contents (file spoofing) – file-spoofing detection identifies attached files that are sent under the guise of a different file extension
- Comparing an attachment file name against pre-defined file name lists
- Comparing an attachment’s MIME type against pre-defined MIME type lists



Zipped archive and MS Office attachments are also scanned. The scanner opens a zipped archive file and scans the file types within it.



If a condition within a rule is set to *Ignore*, that condition is not used in that rule’s search parameters. In a new rule, every condition is initially set to *Ignore*.

Edit Rule

Rule title:
Apply to: Inbound mail Outbound mail Both

Sender
Recipient
Email Content
Attachments
Time Intervals
Actions & notifications
Summary

Rule conditions

At least one of the conditions below needs to be satisfied for this rule to be triggered

All of the conditions below need to be satisfied for this rule to be triggered

Attachment attributes

Ignore attachment size

Email contains an attachment larger than MB

Ignore number of attachments

Email contains more than attachments

Ignore spoofing

Attachment filename is spoofed

Attachment filenames

Ignore filenames

Email contains ANY of the selected filenames

Email contains any filenames EXCEPT those selected

Select a list of filenames:

Selected filenames:

Customize this list

Attachment types

Ignore MIME types

Attachment filename is of selected MIME type

Attachment filename is of any MIME type except those selected

Select a list of MIME types:

Selected MIME types:

video/mpeg
 video/quicktime
 video/x-la-asf
 video/x-ms-asf
 video/x-msvideo
 video/x-sgi-movie

Customize this list

To define attachment attribute conditions:

1. Select Configuration > Email Services > Content Control.
2. Click the name of the required rule, or click Create new rule
3. Click the *Attachment* tab.
4. In the Attachments attributes section, select the option buttons, as required.
 - o **Email contains an attachment larger than** – to detect attachments above a certain size. Enter an attachment size in MB. Attachment size is based on the size of the encoded attachment
 - o **Email contains more than x attachments** – to detect emails with more than a specified number of attachments. Enter the number of attachments.
 - o **Attachment filename is spoofed** – to detect any files that have been sent under the guise of another file type. File spoofing detection involves checking an attached file to ensure that the file is of the type that it says it is. The Anti-Virus service contains functionality that looks at malicious files that may be spoofed. The Email Content Control service takes this a step further and investigates all recognized file types and determines whether they are spoofed or not. This ensures that a user cannot get around an organization's email security policy by spoofing files.

To define attachment filename conditions:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.
3. Click the *Attachment* tab.
4. In the **Attachment filenames** section, select the required option button depending on whether the scan should detect any or none of the filenames that you will select next.
5. Either:
 - a. **Select a list of filenames** (or superlist) from the drop-down list. The filenames in the selected list are displayed in the **Selected filenames** box. You can customize the filenames for this rule, by selecting the **Customize this list** checkbox.



If you customize the list, the changes are not saved to the original list.

Or

- b. To define filenames for this rule only, from the drop-down list, select **Custom list**. The **Selected filenames** box becomes editable. Enter the custom filenames for this rule. For details of wildcards and other valid characters, see Valid and invalid characters and characteristics of lists.



For full details of working with lists, see [Section 6, Working with lists](#).

To define attachment file type conditions:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.
3. Click the *Attachment* tab.
4. In the **Attachments types** section, select the required option button depending on whether the scan should detect one or none of the MIME types in the **Selected MIME types** list.
5. Either:
 - Select a pre-defined MIME type list (or superlist) from the drop-down list. The MIME types in the selected list are displayed in the **Selected MIME types** box. You can customize the MIME types for this rule, by selecting the **Customize this list** checkbox.



If you customize the list, the changes are not saved to the original list.

Or

- To define MIME types for this rule only, from the drop-down list, select **Custom list**. The **Selected MIME types** box becomes editable. Enter the custom MIME types for this rule. For details of wildcards and other valid characters, see Valid and invalid characters and characteristics of lists.



For full details of working with lists, see [Section 6, Working with lists](#).

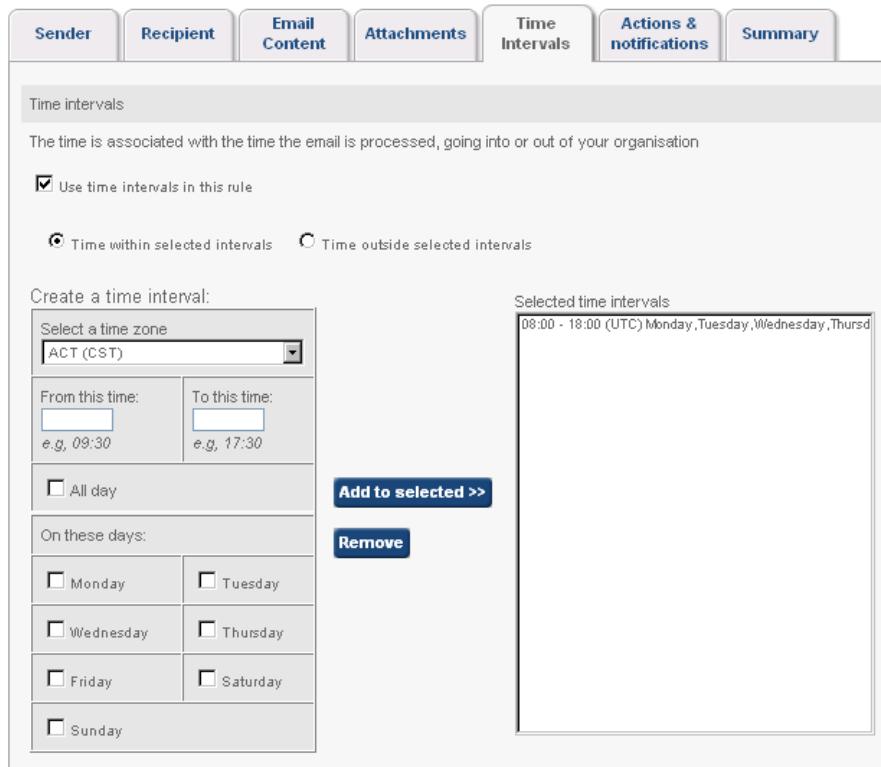
7.3.5 Defining time interval conditions

You can define conditions based on the time that an email is sent or received. This is useful, for example, to limit email size in order to retain network bandwidth during the working day



Times are based on when the email arrives on a mail server within an MailStreet Boundary Defense for Email tower. They are then converted to the time zone specified.

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create** new rule.
3. Click the **Time intervals** tab.



4. Select the **Use time intervals** in this rule checkbox.
5. Select the appropriate option button depending on whether the rule should apply to email scanned within or outside of the specified time intervals.
6. To specify a time zone other than that specified as a default setting (see *Section 4.3. , Defining a default time zone*), select the required time zone from the drop-down list.
 - o Daylight savings are determined by the time zone selected.
7. Enter the required times for the **From this time** and **To this time** values.
 - o Use the 24-hour clock format, e.g. 09.30. You must enter the intervals spanning midnight as two separate time intervals: one for the time interval leading up to midnight and one for the time interval following midnight the next day.
8. Select the required checkboxes to apply the time interval on the required days of the week.
9. Click the Add to selected button.
 - o The time interval is displayed in the **Selected time intervals** box.

7.3.6 Defining actions and notifications

For each rule, you must define an action for the email detected by the rule. For each action you can also define an appropriate notification to be sent to an email administrator, the sender, and/or the recipient of the suspect email (or you can use the default global or domain notifications). You can also define the text of these notifications to suit the situation, or you can use the default notification text defined at the global or domain level. (For full details of general notifications, see [Section 4.4 , Defining default notifications.](#))

- One of several actions may be taken for an email triggered by several rules. Thus, the sequence in which the rules are applied is important. If an email triggers a rule that applies a 'block and delete' or a 'redirect' action, the email does not continue through any further rules

If an email triggers more than one rule, none of which have a block action, depending on the actions for the rule, this could result in multiple copies of an email being sent to the administrator – one for each rule triggered. To overcome this, each occurrence sent to the administrator is combined into a single email.

If a rule is triggered and the resulting action indicates that a multi-recipient email is stopped for a particular recipient, the action is only applied to that recipient. Scanning continues for all other intended recipients.

For all action types, the ClientNet Email Content Control statistics record that a rule has been triggered. All email detected by the Email

Content Control service has the following information added into its header:

- *X-ContentInfo* – displays the name of the rule matched
- *X-Content-Flag* – set to 'yes' if content is detected
- *X-ContentReason* – displays the reason that the email has been detected, that is, the suspect content and its location within the email

7.3.6.1 Defining an action for a rule



When you initially set up a new rule, MailStreet Boundary Defense for Email recommends that you set one of the less severe actions, such as Log only, Tag with header, Tag subject line, or Copy to administrator, while you check that the rule is working, before instigating a more severe action such as Redirect to administrator or Block and Delete.

To define an action:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule.
3. Click the **Actions and notifications** tab.
4. Select the required action from the drop-down list. The possible actions are:
 - **Block and delete** – the email is prevented from reaching the intended recipients. It is permanently deleted. The scanning process is terminated for this email.
 - **Redirect to administrator** – the email is redirected so that it does not continue on to the intended recipients, but is sent to a nominated administrator of the Email Content Control service. The scanning process is terminated for this email.
 - **Copy to administrator** – the email is flagged to be copied to a nominated Email Content Control administrator once scanning is completed. The scanning process continues. The email is sent to the intended recipient.
 - **Tag with header** – a comment is added into the email X-Header to indicate that an Email Content Control rule has been triggered by this email. The scanning process continues.
 - **Tag subject line** – a tag is added to the subject line. You define the text for the tag (see [Section 7.3.6.4 , Defining a subject line tag](#)). Tagging the subject line provides the benefit of warning an end user before they open it that the email may contain unacceptable content.
 - **Compress attachments** – all email attachments of an email are individually converted to .zip files. By individually zipping each attachment, the attachment count and basic file naming is preserved, while the overall email size is reduced. If the email does not have any attachments, the

- action has no effect. The scanning process continues.
- **Log only** – the ClientNet Email Content Control statistics record that a rule has been triggered. No other action is taken. The scanning process continues.

7.3.6.2 Defining a rule-specific administrator email address

If a rule has an action to redirect or copy suspect email, you can define the email address to send the email to. This can be set for the individual rule or the general setting can be used (see **Section 4.1. , Defining a general administrator email address**). Specifying the administrator email address for the rule enables the appropriate personnel to review the triggered email. For example, a breach of confidentiality might go to the Legal department, and a case of harassment might go to the Human Resources department.

The default administrator email address (see **Section 4.1., Defining a general administrator email address**) is an address to which both notifications and the suspect email are sent.



Administrator email addresses bypass the Email Content Control scans. Therefore, if you are using this email address to test your rules, your results will not be accurate. Emails sent from or to this address will not activate any of your Email Content Control rules.

To define a rule-specific administrator email address:

1. Select Configuration > Email Services > Content Control.
2. Click the name of the required rule
3. Click the *Actions and notifications* tab.
4. Either:
 - a. To use a specific administrator email address for this rule, select the **Use Custom Email address** checkbox, and enter the required email address in the **Administrators email address** box.
 - b. To use the default administrator email address (see *Section 4.1. , Defining a general administrator email address*), ensure the **Use Custom Email address** checkbox is unchecked.

7.3.6.3 Defining notifications for a rule

You can define notifications (for the administrator, sender, and/or recipient) that are appropriate for a rule's particular conditions and actions. In the **Actions and notifications** tab, the text for the notifications is displayed according to the current global or domain setting (see **Section 4, Defining general settings**). The text boxes are not editable unless you select the **Send custom notification to...** option button.

If an action to redirect or copy mail to the administrator is selected as an action to the rule, an administrator email address, for the emails and notifications to be sent to, must be specified either at global or domain level or specifically for a rule.

To define notifications for a rule:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.
3. Click the **Actions and notifications** tab.
4. In each section, use the option buttons to define whether:
 - a. No notification is to be sent.
 - b. The default notification is to be sent. This is either the global or domain setting (see *Section 4 , Defining general settings*). The default text for the notification is displayed.
 - c. A custom notification is to be sent. You define the text for the notification here.
5. To define a custom notification, enter the **Subject line** and **Body** text.
The placeholder options enable you to enter variables, such as the date, name of an attached file, name of the rule, etc. To see the variables, click **View placeholder options**. The variables can be pasted and copied into the content of the rule. For a description of the placeholder options (see *Section 4.4. , Defining default notifications*).
6. To define an administrator email address specific to this rule, enter the address in the **Notifications for this rule will be sent to this address** box.



The notification for this rule is sent to this email address.

7.3.6.4 Defining a subject line tag

Specifying *Tag subject line* as an action for detected email enables an email to continue in its intended path but provides the recipient with a warning that it may contain inappropriate content. If you select an action to tag the subject line of a detected email, you must define the text for the tag. You can specify a subject line tag for a specific rule or use the default subject line tag (see [Section 4.5., Defining default subject line tag text](#)).

To define a subject line tag for a rule:

1. Select **Configuration > Email Services > Content Control**.
2. Click the name of the required rule, or click **Create new rule**.
3. Click the **Actions and notifications** tab.
4. In the **Subject line text** section, either:
 - To use specific subject line text for this rule, select the **Use custom subject line text** checkbox, and enter the required text in the **Enter text** box.
 - To use the default subject line text, ensure that the **Use custom subject line text** checkbox is unchecked.
 - The maximum number of characters that the tag can depend on the language you are entering. The tag text can contain non-Western characters.
5. Select an option button depending on whether to put the text before or after the existing subject line text.

8. Frequently Asked Questions (FAQs) About Email Content Control Service

QUESTIONS	ANSWERS
GROUPS FAQs Q & A	
What characters can I use in a user group name?	User group names must be alphanumeric; spaces are allowed. Names can be up to 50 characters in length.
I have deleted users from a user group but they have re-appeared. Why?	The email address in question has sent outbound mail through the towers and the address was harvested again.
How many user groups can I create?	500 per domain.
How many users can exist in a user group?	500,000
Can I add a user group to another group?	No. A user group can only contain email addresses. However, a single email address can exist in multiple user groups.
I can see user groups available for selection when I create a new rule but visiting the <i>User groups</i> page the settings are grayed out. What is happening?	You are at domain level. User groups created at global level can be applied to rules at domain level but cannot be edited. Therefore they are not editable in the <i>User groups</i> page at domain level.
Why are some of my users not displayed in a user group that I added them to?	Only the first 500 users are displayed. You will need to search for users that are not displayed
I want to delete a user group but I am unable to select it; the box is grayed out. What should I do?	The user group is being used in a rule and cannot be deleted until it is removed from all of the rules it is used in.
LISTS FAQs Q & A	
What characters can I use in a list name?	List names must be alphanumeric, spaces are allowed. Names can be up to 50 characters long.
Can I change the type of a list that already exists?	No. You will need to create a new list.
MailStreet Boundary Defense for Email provided a set of default lists. Can I delete these?	No. The default lists cannot be deleted.
I can see lists available for selection when I create a new rule, but visiting the LISTS page the settings are grayed out. What is happening?	You are at domain level, lists created at default level can be applied to rules at domain level but cannot be edited, and therefore they are not editable in the <i>Lists</i> page at domain level.
We work for a global organization that operates in countries that speak foreign languages. Is it possible to add word lists in any language?	Yes it is possible to configure a word list in any language, whether it is Latin-based, Asian, or Eastern-European.
I want to use the default word lists for profanity but I have found that one of the words is triggered by a user's surname. How can I get round all of his emails triggering the rule?	There are two options. You can either: <ul style="list-style-type: none"> - Customize the list to remove the offending word, in the <i>Email content</i> tab for the rule. - Use the threshold functionality. In the <i>Email content</i> tab, set the Email contains at least two of these terms setting

so that at least two words on this list must be present. This ensures that an email will not simply be stopped for having the surname in once. The threshold can be increased up to ten words, if necessary. This should mean that all emails containing profanity are stopped correctly, but emails that detail a sensitive word in an ambiguous context will not

Can I concatenate lists together to create one large list?

Yes. It is possible to create a 'superlist' by selecting multiple lists of a single type. A superlist cannot include multiple list types. A superlist is automatically updated if one of the lists it includes is changed.

Is it possible to stop specific MIME types coming into our organization by selecting them from a pre-defined list?

Yes. You can define a list of MIME types to scan for. However, if a rule that stops specific MIME types is to be used to protect the organization against harmful executables and malware, the MailStreet Boundary Defense for Email Anti-Virus service will detect these; so it may not be necessary to block all of these MIME types.

RULES FAQs Q & A

I want to set up rules within Email Content Control but I am concerned that I may set something up and it blocks business critical email. What should I do?

When configuring rules within the MailStreet Boundary Defense for Email Content Control service we recommend that you set the action to Log only for the first 48 hours to enable you to monitor any irregular activity. If there is a problem and you cannot work out how to resolve it, please contact MailStreet Boundary Defense for Email Client Services

I have just subscribed to Email Content Control and cannot add a new Rule. Why?

Make sure you have defined an administrator email address and time zone in the **Settings** tab.

What characters can I use in a rule name?

Rule names must be alphanumeric; spaces are allowed. Names can be up to 50 characters in length.

How many rules can I have?

Up to 500 per domain.

Can I configure a rule to be from a group of specific users OR a list of domains?

Yes. It is possible to use 'and' and 'or' relationships between different components of the rule to ensure that the rule meets your requirements.

I want to setup a rule to monitor emails coming from joe@example.com and going to the marketing department, which contain password-protected files, or are encrypted. Is this possible?

Yes. You can decide how you wish to link each component of a rule together within each tab and between tabs. Your choice will be either linking 'all the components' or 'any of the components'

What order are my rules processed in?

The order in which they are displayed within ClientNet.

I set an attachment size restriction of 2Mb but emails are being blocked with attachments smaller than this. Why?

Check that you have not set the size restriction on the **Email content** tab rather than the **Attachments** tab.

I have created a rule with multiple conditions and it is not stopping any emails. Why?

Check that you are using the AND and OR elements of your conditions correctly.

Can I get a quick view of which components are in the rule?

Yes. Simply go to the **Summary** tab, where you can see what conditions are in place for this rule.

I have set up all my rules in a test domain and I am happy that they are running correctly. How can I now switch them on for all of my other domains?

Use the **Copy rule** functionality to select each rule and copy it to another domain or to the global level.

I have set up a rule in a test domain, but it

You may be testing the rule using an email sent from or to the email address

does not seem to be working when I test it. Why?	that is specified as the Administrator email address. Administrator email addresses bypass the Email Content Control scans. Emails sent from or to this address will not activate any of your Email Content Control rules.
I do not want our IT administrator to have to sift through all of the emails that have been triggered. Can I share the responsibility depending on which rule an email breaks?	Yes. You can set a separate email address for each rule for redirect or copy actions. This enables, for example, the legal team to look at all emails that have breached confidentiality and the HR team to look at emails that may potentially cause harassment
Is it possible to configure notifications for individual rules?	Yes. In the Actions and notifications tab, you can activate or deactivate each notification, adding new text or selecting the option button that inherits text from default notifications.
If I make a change to a rule, how long does it take to update and take effect?	Rules are updated every time that the MailStreet Boundary Defense for Email infrastructure builds the configurations, collecting information and distributing it across the infrastructure. Currently this process runs approximately every four hours
Are there any restrictions on which types of files can be used for conditions in Email Content Control rules?	Content in Microsoft Office 2007 documents will not be detected by Email Content Control rules. Rules should not be based on document content if you use Microsoft Office 2007.

OTHER QUESTIONS FAQs Q & A

How can I add email addresses to Email Content Control?	When a user sends an outbound email, Email Content Control automatically harvests their email address for future use. Addresses can also be added manually to a user group or added for a specific rule. See <i>Section 5, User Groups in Email Content Control</i> .
Can I differentiate between the parts of the email to look in?	Yes. You can define whether to scan within the header, subject line, body, and the attachment of emails.
Does Email Content Control scan within MS Office documents as well as the email?	Yes. The Boundary Defense for Email Content Control Service scans within MS Office documents for words and phrases or regular expressions. Select the Scan attachments checkbox in the Email content tab.
Does Email Content Control automatically scan within archive files such as ZIP and RAR for file types?	Yes, if you set up a rule to detect specific file types or content, Email Content Control will look inside the archive files to see if the file type or content are hidden in there.
If I am sent a spoofed file, for example an Excel XLS file renamed with a DOC file extension, is the Email Content Control service able to pick this up?	Yes. If the spoofed file is malicious, it will already have been detected by the MailStreet Boundary Defense for Email Anti-Virus service. However if the file is simply spoofed, then the Email Content Control service can be configured to detect this within the Attachment tab.
Are email addresses case-sensitive?	Yes. If you wish to search for an email address, you will need to type it as it is recorded. Most email addresses are stored in lower case.
An email has triggered a rule. How can I find out why it was triggered?	You can look in the headers of the email where the rule name and the word that triggered the rule are displayed.
How do the templates work?	The templates use a formula that stops all data that is in the same format as the template. For example, credit card numbers are always sixteen digits, which are displayed in one of several formats.
How do wildcards work?	Wildcards are used when you do not want to state exactly the numbers or characters to trigger a rule, but when there are specific alphanumeric characters that must be present. An example of this may be something like patient numbers, which, in a certain scenario, may always have the first five characters as HGTYU, but after those characters could be any combination of letters or numbers. So you could use HGTYU* to monitor emails leaving an organization that include this arrangement of characters.

9. Glossary

TERM	DEFINITION
Action	The consequence of a rule being triggered by an email. These are Block and delete, Redirect to administrator, Copy to administrator, Tag with header, Tag subject line, Compress attachments, and Log only
Attachment Number	The number of individual attachments on a single email
Body	The message text of an email.
Default Settings	XXXX at a lower level of granularity. For example, a global notification is used unless custom text is defined for the notification for a specific domain. Likewise, the domain-level notification is used by a domain-level rule for that domain, unless custom text is defined at rule level.
Domain List	The sender and recipient of an email are compared against entries in a custom list. Wildcards are not permitted; domain name references must be specific and complete.
Domain Settings	Domain settings are the configuration settings for Email Content Control that apply to the specific domains of your organization. Settings for a specific domain can be viewed and configured by selecting the domain from the Global Settings drop-down list towards the top of each page.
Email Size Limit	The total size of a single email, including all content and attachments.
General Settings	General settings are those that appear in the Settings tab of the Email Content Control pages. These can be set at global level and at domain level. These settings are used by all rules unless rule-specific settings are defined. Rule-specific settings override the general settings.
Global Settings	Global settings are the configuration settings for Email Content Control that apply to all of your organization's domains. Global settings can be viewed and configured by selecting Global Settings from the drop-down list towards the top of each page.
Header	The part of an email that precedes the body of a message and contains information about the email, its sender, the date and time the message was sent, amongst other items of information
Ignor	If a condition within a rule is set to <i>Ignore</i> , that condition is not used in that rule's search parameters. In a new rule, every condition is initially set to <i>Ignore</i> .
Lists	A list is a collection of search conditions that can be used for content-matching during the email scanning process. There are five types of list available: domain names, email content, URLs, MIME types, and filenames
MIME Types	Attachments and emails are compared against a selected list of MIME types/subtypes, for example: application, audio, image, message, text, video, application, audio/wav, and video/mpeg. Email Content Control does not validate or check the accuracy of types/subtypes entered. No default lists are provided, although they can easily found by using internet search engines.
Rule Name	The name applied to an individual rule. Rule names must begin with a letter of the alphabet.
S/MIME	A protocol for adding cryptographic signature and encryption services to MIME data, to enable secure email.
Spoofing	Sending executable programs under the guise of a different extension than ".exe".