



Admin Guide

Boundary Defense for Email Email Anti-Virus & Anti-Spam

MailStreet Live Support: [866-461-0851](tel:866-461-0851)

Table of Contents

| | |
|---|------------|
| 1 INTRODUCTION..... | 4# |
| 1.1. AUDIENCE AND SCOPE..... | 4# |
| 1.2. INTERNATIONAL CONSIDERATIONS..... | 4# |
| 1.3. CONVENTIONS..... | 4# |
| 1.4. SECURITY AND LEGAL CONSIDERATIONS | 5# |
| 1.4.1 DNS | 5# |
| 1.4.2 Legal considerations | 5# |
| 1.4.3 Login details | 5# |
| 1.4.4 Passwords..... | 5# |
| 1.5. LOGGING IN AND LOGGING OUT..... | 5# |
| 2 INTRODUCTION TO EMAIL ANTI-VIRUS | 6# |
| 2.1. VIRAL URL LINKS | 6# |
| 3 CONFIGURING EMAIL ANTI-VIRUS | 7# |
| 3.1. LOCATING THE EMAIL ANTI-VIRUS PAGES | 7# |
| 3.2. DEFINING WHETHER SETTINGS APPLY GLOBALLY OR FOR A DOMAIN | 8# |
| 3.3. DEFINING ADMINISTRATOR ALERTS | 8# |
| 3.4. DEFINING USER ALERTS | 8# |
| 3.5. DEFINING AN ADDRESS THAT USER ALERTS APPEAR TO BE SENT FROM..... | 9# |
| 3.6. RELEASING A VIRUS..... | 9# |
| 3.7. LIMITING THE SIZE OF AN EMAIL | 10# |
| 3.8. DEFINING BANNERS..... | 10# |
| 4 GETTING STARTED WITH EMAIL ANTI-SPAM..... | 11# |
| 4.1. INTRODUCTION TO EMAIL ANTI-SPAM | 11# |
| 4.2. ANTI-SPAM BEST PRACTICE SETTINGS..... | 12# |
| 4.3. LOGGING IN AND LOGGING OUT..... | 12# |
| 4.4. LOCATING THE EMAIL ANTI-SPAM PAGES IN CLIENTNET..... | 13# |
| 4.5. DEFINING WHETHER SETTINGS APPLY GLOBALLY OR FOR A DOMAIN | 14# |
| 4.5.1 Applying global settings..... | 14# |
| 4.5.2 Applying settings for a specific domain..... | 14# |
| 5 DEFINING DETECTION SETTINGS AND ACTIONS..... | 16# |
| 5.1. ENABLING USE OF THE APPROVED SENDERS LISTS..... | 17# |
| 5.2. ENABLING USE OF BLOCKED SENDERS LISTS..... | 17# |
| 5.3. USING PUBLIC BLOCK LISTS | 18# |
| 5.4. USING THE SIGNATURE SYSTEM..... | 18# |
| 5.5. USING SKEPTIC HEURISTICS | 19# |
| 5.6. DEFINING A BULK MAIL ADDRESS | 19# |
| 5.7. DEFINING A SUBJECT LINE TAG | 19 |

| | |
|---|------------|
| 6 DEFINING QUARANTINE SETTINGS | 20# |
| 6.1. SPECIFYING NOTIFICATIONS | 20# |
| 6.2. DEFINING A DEFAULT LANGUAGE FOR SPAM MANAGER NOTIFICATIONS | 21# |
| 6.3. DEFINING USER ACCOUNT CONTROLS..... | 21# |
| 6.3.1 <i>User notification control</i> | 21# |
| 6.3.2 APPROVED SENDER REQUEST FACILITY | 22# |
| 6.4. ENABLING CLIENTNET USERS TO REQUEST ADDITIONS TO THE APPROVED SENDERS LIST | 22# |
| 6.5. ALIASES | 22# |
| 6.6. DEFINING QUARANTINE ADMINISTRATORS | 23# |
| 6.7. PASSWORD CONTROLS..... | 24# |
| 6.7.1 <i>Default password control settings</i> | 24# |
| 6.7.2 CONFIGURING THE PASSWORD POLICY | 25# |
| 6.7.3 <i>Customizing password control settings</i> | 28# |
| 7 USING APPROVED SENDERS AND BLOCKED SENDERS LISTS | 30# |
| 7.1. INTRODUCTION TO APPROVED AND BLOCKED SENDERS LISTS | 30# |
| 7.2. DEFINING GLOBAL LISTS | 31# |
| 7.2.1 <i>Viewing global approved and blocked senders lists</i> | 31# |
| 7.2.2 <i>Adding an entry to a global list manually</i> | 32# |
| 7.2.3 <i>Downloading a global approved or blocked senders list</i> | 32# |
| 7.2.4 <i>Uploading a global list to ClientNet</i> | 32# |

1 Introduction

This guide is for administrators of the MailStreet Boundary Defense for Email service. It describes procedures for configuring both the Anti-Virus and Anti-Spam features of the MailStreet Boundary Defense for Email Service.

The first section of this guide details how to configure the Anti-Virus service to your requirements, including defining alerts and banners and releasing viruses.

The second section of this guide is for Administrators of the Email Anti-Spam Service. It provides procedures for configuring the service to your requirements, including defining detection methods, actions for the spam detected exclusions, approved and blocked senders lists, and Spam Quarantine settings.

1.1. Audience and Scope


Welcome to the MailStreet Boundary Defense for Email service. This guide provides step-by-step instructions for administrators on using ClientNet to set up and manage their MailStreet Boundary Defense for Email service. The guide also provides background information on the Email Anti-Virus features of the MailStreet Boundary Defense for Email service.

1.2. International Considerations

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

1.3. Conventions

In this guide, the following conventions are used:

| Formatting | Denotes |
|---|--|
| Bold | Button, tab or field |
| <i>Bold Italic</i> | Window title or description |
|  Note: | A note containing extra information that may be useful |
| Text to type in | Text to type in, or output from a computer |
| <u>Link</u> | A link to a website |

Screenshots normally display an **Internet Explorer** window. If only part of the window is shown, the side where it is trimmed may be shown with a wavy or dashed line. Areas of the screenshot may be highlighted in red.

1.4. Security and Legal Considerations

1.4.1 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.

1.4.2 Legal considerations

Clients are advised to seek specialist advice to ensure that they use the MailStreet Boundary Defense for Email 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 MailStreet Boundary Defense for Email service.

1.4.3 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.

1.4.4 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.

This guide includes information on your password policy and how you can enforce this in your organization; [See Section 6.7, Password Controls](#) for further details

1.5. Logging In and Logging Out

To log in to the ClientNet portal which is used to manage your Anti-Virus and Anti-Spam configurations, you will access the MailStreet 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 | MailStreet Boundary Defense for Email** to access the MailStreet Boundary Defense for Email service window
3. In the section titled Access to MailStreet 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 Aptix 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 the ClientNet portal, click the **Log Out** link at the top left of the screen.

2 Introduction to Email Anti-Virus

MailStreet Boundary Defense for Email Anti-Virus re-routes your inbound and outbound email through the MailStreet Boundary Defense for Email control towers where it is scanned by multiple scanners including the Skeptic scanner before being passed on to its final destination. Skeptic uses predictive technology to identify and stop new virus and malware outbreaks as they occur and before Anti-Virus signatures are available. (A virus signature is a unique string bits that defines a specific computer virus, which can then be used to detect instances of the virus.) Polling for signature updates is performed automatically every ten minutes. Instant updates are carried out in the event of a new outbreak.

If an email is virus-free, it is delivered to the intended recipient. If a virus is detected, the email is quarantined. Any email that is found to be infected with a virus is quarantined for 30 days. Notifications can be generated automatically to the intended recipient, and administrator. The service has no discernible impact on email delivery times.

Use ClientNet to configure the Anti-Virus service to your requirements. The main configuration tasks for the service are defining alerts settings, releasing a virus, and defining banners.

2.1. Viral URL Links

The MailStreet Boundary Defense for Email Anti-Virus service offers protection against positively-identified viral URL links within emails. Such links differ from conventional email virus threats in that direct action is required by a user to follow the link to an infected website.

To counter such threats the Anti-Virus service works by actively following the suspicious link in an email via the scanner and checking the website for viruses or other types of potentially harmful content or payload. If or when a suspicious link is confirmed as viral, a signature is created, and further emails containing that link are treated as being infected with a virus and quarantined.

To keep latency to a minimum, it is important to note that scanning for viral URL links does not happen in real-time. Emails containing unknown URLs are delivered as normal, and the links are normally analyzed within a few minutes following the delivery. If a URL is found to be malicious, a signature is created and all future email with that link is quarantined.

This procedure means that on rare occasions you may receive an email that contains a potentially harmful link (before the link is confirmed as viral). When the URL is confirmed as viral, MailStreet Boundary Defense for Email emails you a 'missed' report informing you that you received an email containing a viral link prior to it being found malicious.

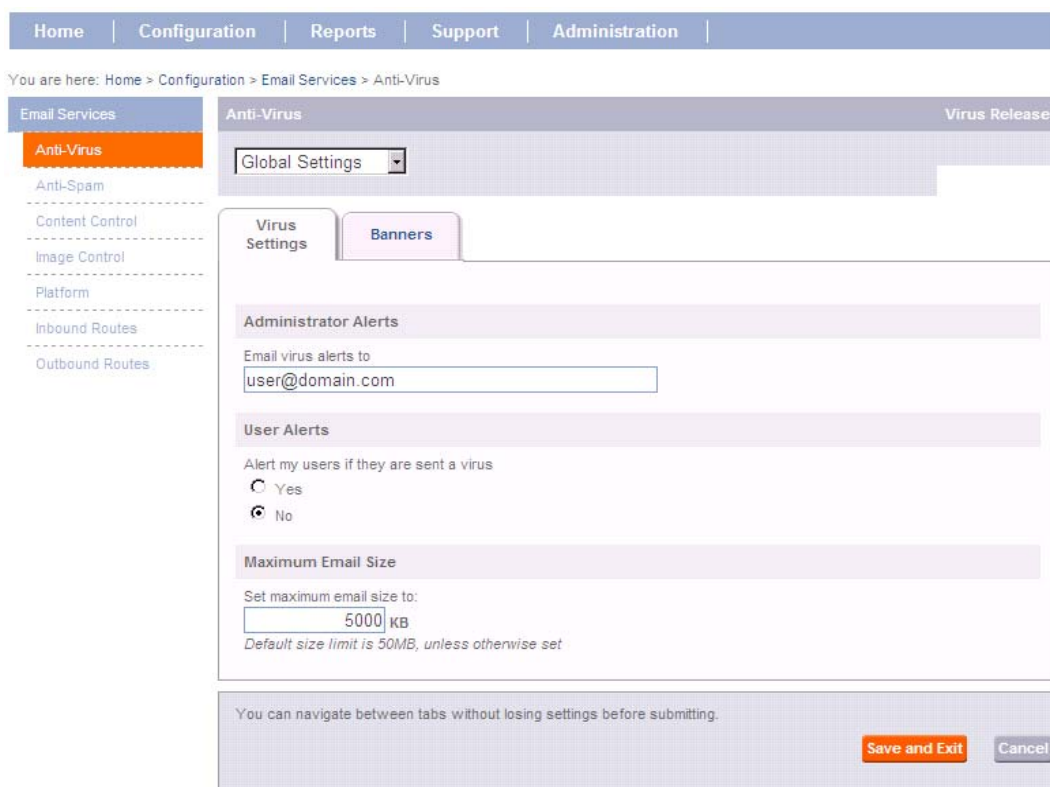
3 Configuring Email Anti-Virus

3.1. Locating the Email Anti-Virus pages

To locate the Email Anti-Virus pages:

1. In the top navigation bar, click **Configuration** and then **Email Services Configuration**.
2. In the left navigation bar, click **Anti-Virus**.

Two tabs are displayed; **Virus Settings** and **Banners**.



The screenshot shows the MailStreet web interface for configuring Anti-Virus settings. At the top, there is a navigation bar with links for Home, Configuration, Reports, Support, and Administration. Below this, a breadcrumb trail reads: You are here: Home > Configuration > Email Services > Anti-Virus. On the left, a sidebar menu lists various services, with 'Anti-Virus' highlighted. The main content area is titled 'Anti-Virus' and includes a 'Global Settings' dropdown menu. Below this, there are two tabs: 'Virus Settings' (selected) and 'Banners'. The 'Virus Settings' tab contains three sections: 'Administrator Alerts' with a text input field for 'Email virus alerts to' (containing 'user@domain.com'); 'User Alerts' with a radio button selection for 'Alert my users if they are sent a virus' (selected 'No'); and 'Maximum Email Size' with a text input field for 'Set maximum email size to:' (containing '5000 KB') and a note: 'Default size limit is 50MB, unless otherwise set'. At the bottom of the page, there is a message: 'You can navigate between tabs without losing settings before submitting.' and two buttons: 'Save and Exit' and 'Cancel'.

All of the Anti-Virus configuration settings are defined within these two tabbed pages. The procedures in the sections that follow assume that you have navigated to the Email **Anti-Virus** pages.

3.2. Defining Whether Settings Apply Globally or for a Domain

You can configure and apply default Anti-Virus settings to all domains, or you can apply custom settings to an individual domain, using the **Global Settings** drop-down list. Most often you will be configuring the Anti-Virus service using your global settings and making fewer changes on a domain-level basis.



You can only specify an email alerts address (the address to which alert notifications appear to be sent from) at domain level. See [Section 3.3. , Defining administrator alerts.](#)

To apply settings for a specific domain:

1. Select the domain from the **Global Settings** drop-down list.
The **Virus Settings** and **Banners** pages present a further option to **Use custom virus settings**. Until this is selected, all fields in these pages are inactive and cannot be edited.
2. Select **Use custom virus settings**.
The fields in the **Virus Settings** and **Banners** pages are editable and inherit the global settings until you make any changes. 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.

3.3. Defining Administrator Alerts

An administrator alert is an email that is sent to the Anti-Virus administrator when a user has sent or has been sent a potential virus. By default, this field is left blank, and will need to be filled in by the administrator. Alerts to administrators contain the Pen number for the quarantined email. This is a unique reference number that is used to locate and release the email from within ClientNet (see [Section 3.6., Releasing a virus](#)). Currently, the content of virus alerts is not configurable.

To specify an address for administrator alerts to be sent to:

1. Navigate to the **Anti-Virus** area.
2. Click the **Virus Settings** tab.
3. In the **Administrator Alerts** section, enter the Anti-Virus administrator's email address.
4. Click **Save and Exit**.

3.4. Defining User Alerts

A user alert is an email that can be sent to the intended recipient of a potential virus, if the recipient's email address is inside the client's network. By default, these alerts are enabled.

Alerts to users contain the Pen number for the quarantined email. This is a unique reference number that is used to locate and release the email from within ClientNet (see [Section 3.6., Releasing a virus](#)). Currently, the content of virus alerts is not configurable.

To specify whether the recipients of an infected email receive alerts:

1. Navigate to the **Anti-Virus** area.
2. Click the **Virus Settings** tab.
3. In the **User Alerts** section, select the required option button.
4. Click **Save and Exit**.

3.5. Defining an Address that User Alerts Appear to be Sent From

For individual domains, you can define the email address from which virus alerts appear to be sent. For example, you may wish email alerts to internal and external users to be sent from an internal administrator email account. This means that alert recipients can respond to an email account within the client's organization. This can be done only for individual domains, i.e. the email address specified must be in the same domain that the alerts apply to.

To define an email alerts address:

1. Navigate to the **Anti-Virus** area.
2. Click the **Virus Settings** tab.
3. Select the domain for the setting from the **Global Settings** drop-down list.
4. Select the **Use custom virus settings** option button.
5. Enter the email alerts address for the domain and select the option button to the left.
6. Click **Save and Exit**.

3.6. Releasing a Virus

When MailStreet Boundary Defense for Email Anti-Virus intercepts a virus in an email, it places the infected email into a holding pen, where it is stored for up to 30 days, before being deleted. This quarantine period ensures that the virus is isolated and cannot infect the intended recipient's computer.

Each quarantined email has a unique identifier known as a Pen number. This number is stated in the administrator and user alerts that are issued when an email containing a suspect virus is received.

An administrator can allow a virus-infected email to be released from the quarantine pen and delivered to the intended recipient. The functionality for releasing a virus is provided by the **Virus Release** link at the top right of the **Anti-Virus** pages.



To release an email from quarantine:

1. Navigate to the **Anti-Virus** area.
2. Click the **Virus Settings** tab.
3. Select **Virus Release**.
4. Enter the Pen number of the virus.
This is found in the administrator alert.
5. Click **Go**.
Details of the quarantined email are displayed in a pop-up window.
6. Locate the entry required and click the **Release** button in the right hand column.
A disclaimer is displayed.
7. To release the quarantined email, click the **Confirm** button.
A confirmation message is displayed. The email containing the virus is released to the intended recipient.

3.7. Limiting the Size of an Email

You can set a maximum size above which inbound emails will not be received. You cannot specify the maximum size to be more than 1,000,000 KB.

To set an email size limit:

1. Navigate to the **Anti-Virus** area.
2. Click the **Virus Settings** tab.
3. Enter the maximum size for emails (in KB) in the **Set maximum email size to** field.
4. Click **Save and Exit**.

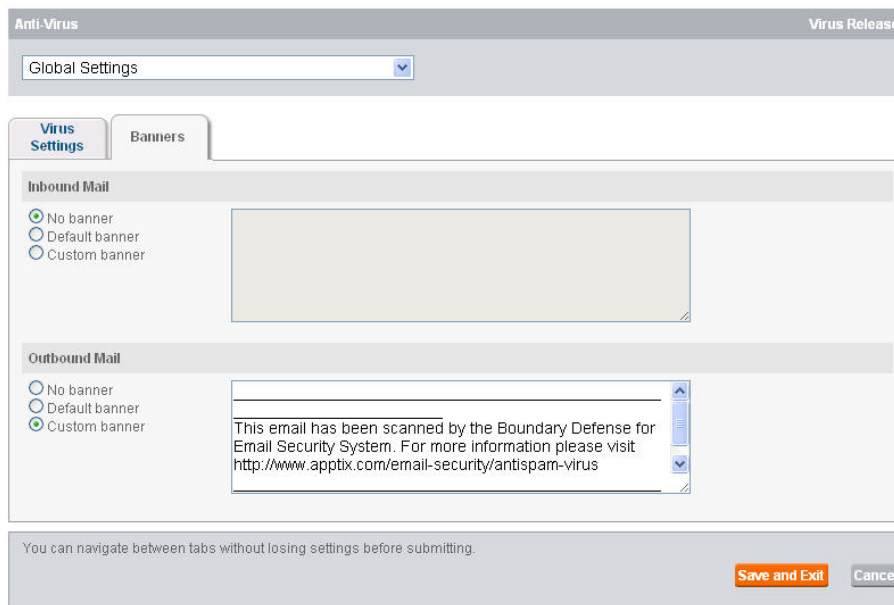
3.8. Defining Banners

You can define a default or custom banner to be appended to inbound and/or outbound emails to let your users and recipients of their emails know that their mail is protected. By default there is no banner being sent to the users.

You can define default or custom banners for inbound and outbound emails either globally or for individual domains.

To define a banner:

1. Navigate to the **Anti-Virus** area.
2. Click the **Banners** tab.



The screenshot shows the 'Anti-Virus' configuration page with the 'Banners' tab selected. At the top, there is a 'Global Settings' dropdown menu. Below it, there are two tabs: 'Virus Settings' and 'Banners'. The 'Banners' tab is active and contains two sections: 'Inbound Mail' and 'Outbound Mail'. In the 'Inbound Mail' section, there are three radio buttons: 'No banner' (selected), 'Default banner', and 'Custom banner'. To the right of these buttons is a large empty text box. In the 'Outbound Mail' section, there are three radio buttons: 'No banner', 'Default banner', and 'Custom banner' (selected). To the right of these buttons is a text box containing the text: 'This email has been scanned by the Boundary Defense for Email Security System. For more information please visit http://www.apptix.com/email-security/antispam-virus'. At the bottom of the page, there is a note: 'You can navigate between tabs without losing settings before submitting.' and two buttons: 'Save and Exit' and 'Cancel'.

3. For each section – **Inbound mail** and **Outbound mail** – select the option button as required. If you define a custom banner, enter the banner text in the text box. The banner must not exceed the maximum of 4000 characters.
4. Click **Save and Exit**.

***** *End of MailStreet Boundary Defense for Email: Email Anti-Virus Section -- Email Anti-Spam Section to Follow* *****

4 Getting Started with Email Anti-Spam

4.1. Introduction to Email Anti-Spam

The MailStreet Boundary Defense for Email service stops unsolicited email from entering your email system. The following Anti-Spam detection methods can all be used to check your incoming email for spam:

- **Skeptic heuristic engine:** artificial intelligence that creates an ever-expanding knowledge base for identifying spam.
- **Signaturing system:** proprietary and commercially available signature-building engines that create a vast knowledge base of signatures of spam messages currently in email circulation.
- **Public block lists:** recognized public block lists of IP addresses of globally known sources of spam.
- **Exclusions:** a list of email addresses to be excluded from the protection of the Anti-Spam service.
- **Blocked senders list:** a blocked senders list that you can specify in a global list (depending on your organization's configuration). The list can contain email addresses, domains, or IP addresses that you recognize as sources of spam or other unwanted email.
- **Approved senders list:** an approved senders list that you can specify in a global list (depending on your organization's configuration). The list can contain email addresses, domains, or IP addresses. The list enables email from a sender on list to pass through the spam service without interruption.

You can specify which of these detection methods you require incoming email to be checked against and set different actions for the suspected mail found by each method. You may also be able to define exclusions (email addresses that are not subject to the scanning process).

As an Administrator, you can use ClientNet to configure the Anti-Spam service to suit your organization's requirements. The MailStreet Anti-Spam service has layers of settings to give you complete flexibility with regard to your users. You can define global settings for all your domains.

The main administration tasks for the service:

- Define the detection settings, which entails:
 - o Defining the spam detection methods to use
 - o Defining the actions to be taken on detection of spam
 - o If spam email redirection is selected as an action, setting the email address to which spam email is routed
 - o If tagging the subject line is selected as an action, defining the tag text for emails tagged as spam
- Define Spam Quarantine settings



Depending on your organization's configuration, you may not see Spam Quarantine settings.

- Define approved senders and blocked senders lists

4.2. Anti-Spam Best Practice Settings

When you are provisioned with the Anti-Spam service, the service is enabled with default, best practice settings. MailStreet Boundary Defense for Email recommends that you evaluate the tagged spam that you receive using these settings, and how these settings work for your organization's mail flow. After you have used the service for a while you can change to the best practice settings if decided:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Select **Global Settings** or a specific domain from the domains drop-down list
3. In the **Detection Settings** tab, the following settings are enabled:
 - o Blocked senders list (IP addresses only)—set to **Block and delete the mail**
 - o Blocked senders list (domains and email addresses only)—set to **Block and delete the mail**
 - o RBL public block list—set to **Block and delete**
 - o RSS public block list— set to **Block and delete**
 - o DUL public block list—set to **Block and delete the mail**
 - o Signaturing system—set to **Block and delete the mail**
 - o Skeptic heuristics—set to **Quarantine the mail**. *See Section 5.5. , Using Skeptic Heuristics*



For full details on configuring detection settings, see [Section 5, Defining detection settings and actions](#).

4.3. Logging In and Logging Out

To log in to the ClientNet portal which is used to manage your Anti-Virus and Anti-Spam configurations, you will access the MailStreet 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 | MailStreet Boundary Defense for Email** to access the MailStreet Boundary Defense for Email service window
3. In the section titled Access to MailStreet 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

To log out ClientNet:

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

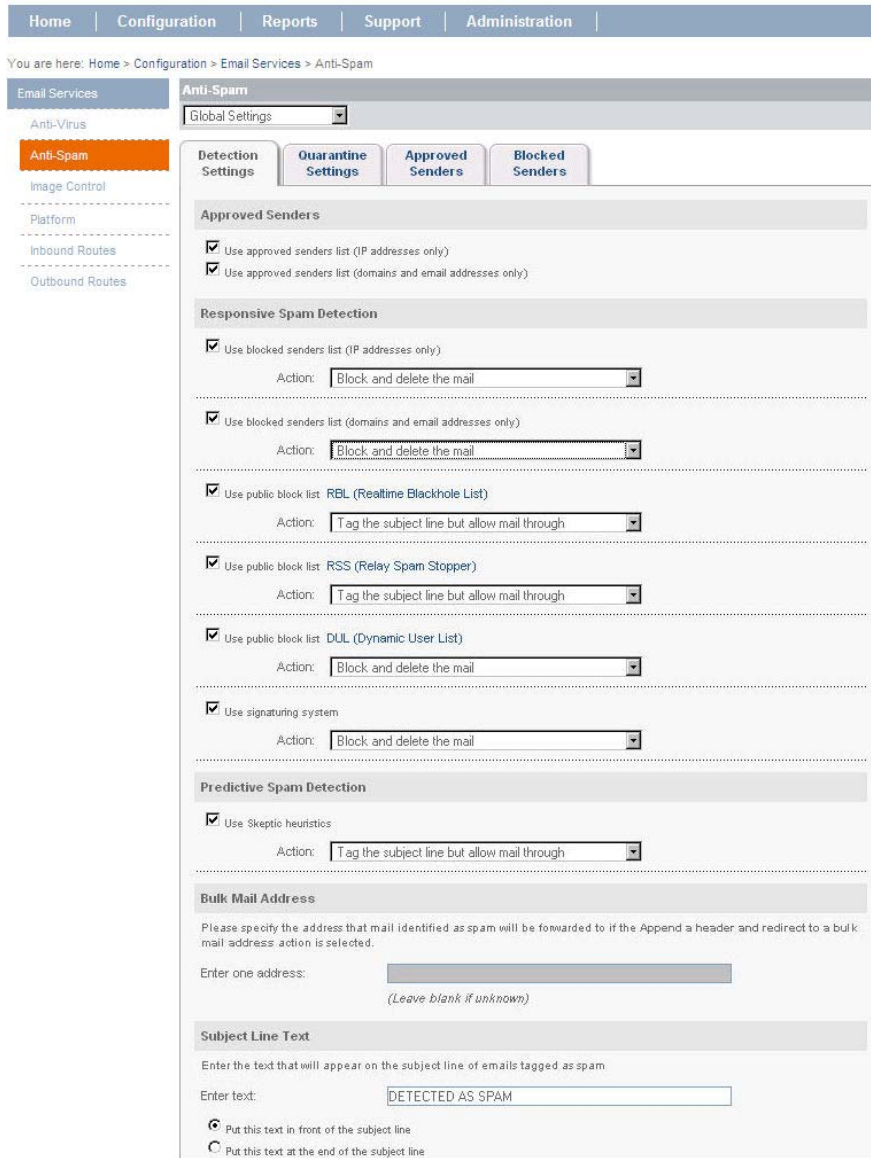
4.4. Locating the Email Anti-Spam Pages in ClientNet



Depending on your organization's configuration, you may not see all of the ClientNet pages described in this guide.

To locate the Anti-Spam pages in ClientNet:

1. In the top navigation bar, click **Configuration** and then **Email Services Configuration**.
2. In the left navigation bar, click **Anti-Spam**.
 - If **Global Settings** is selected in the drop-down list, up to four tabs are displayed: **Detection Settings**, **Quarantine Settings**, **Approved Senders**, and **Blocked Senders**.



The screenshot shows the ClientNet interface for Anti-Spam configuration. The top navigation bar includes Home, Configuration, Reports, Support, and Administration. The breadcrumb trail reads: Home > Configuration > Email Services > Anti-Spam. The left sidebar shows 'Anti-Spam' selected under 'Email Services'. The main content area has four tabs: 'Detection Settings', 'Quarantine Settings', 'Approved Senders', and 'Blocked Senders'. The 'Approved Senders' tab is active and contains the following settings:

- Approved Senders:**
 - Use approved senders list (IP addresses only)
 - Use approved senders list (domains and email addresses only)
- Responsive Spam Detection:**
 - Use blocked senders list (IP addresses only)
 - Action:
 - Use blocked senders list (domains and email addresses only)
 - Action:
 - Use public block list: RBL (Realtime Blackhole List)
 - Action:
 - Use public block list: RSS (Relay Spam Stopper)
 - Action:
 - Use public block list: DUL (Dynamic User List)
 - Action:
 - Use signaturing system
 - Action:
- Predictive Spam Detection:**
 - Use Skeptic heuristics
 - Action:
- Bulk Mail Address:**

Please specify the address that mail identified as spam will be forwarded to if the Append a header and redirect to a bulk mail address: action is selected.

Enter one address:

(Leave blank if unknown)
- Subject Line Text:**

Enter the text that will appear on the subject line of emails tagged as spam

Enter text:

 - Put this text in front of the subject line
 - Put this text at the end of the subject line

If a specific domain is selected from the domains drop-down list, you will see the same four (4) tabs as the Global Settings list: **Detection Settings**, **Quarantine Settings**, **Approved Senders**, and **Blocked Senders**.

All of the **Anti-Spam** settings are defined in these tabs.

4.5. Defining Whether Settings Apply Globally or for a Domain

You can configure and apply default Anti-Spam settings to all domains, or you can apply custom settings to an individual domain, using the domains drop-down list. Most often you will be configuring the Anti-Spam service using your global settings and making fewer changes on a domain-level basis.

You use the domains drop-down lists on the Anti-Spam pages to select the domain to work with.

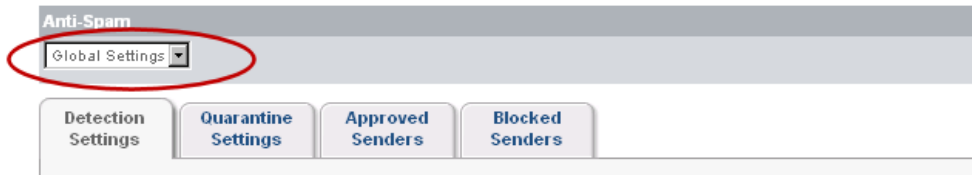


Then you specify the required settings and these will be applied at the selected level. When you select a domain to work with, the settings from the next highest level are inherited. You can then make your required amendments to apply for the domain. Different tabs are available at the various levels, reflecting the settings that are available at each level.

4.5.1 Applying global settings

To apply global settings:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Ensure that **Global Settings** is selected in the domains drop-down list:



Up to four tabs are displayed (**Detection Settings**, **Quarantine Settings**, **Approved Senders**, and **Blocked Senders**) depending on your organization's configuration. Any settings at this level apply globally across all of your domains.

4.5.2 Applying settings for a specific domain

To apply settings for a specific domain:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Select the domain from the domains drop-down list.



To reduce the number of domains in the list, you can enter the first three or more characters of the domain name. Only those that contain those starting characters are listed.

3. In the **Detection Settings** and **Quarantine Settings** pages, ensure the **Use custom settings** option button is selected; unless this is selected, all fields in these pages are inactive and cannot be edited.
 - The fields in these pages inherit the global settings until you make any changes.

- When you select **Save & Exit** on this screen, the changes you make are applied only to the selected domain.



Changes to approved senders and blocked senders lists can only be made at the global level. When you select a specific domain to work with, the name of the domain is displayed as a heading:



Anti-Spam: dom.co.uk

dom.co.uk

Use global settings Use custom settings

5 Defining Detection Settings and Actions

Within the **Detection Settings** tab you can define which of the various detection methods your Email Anti-Spam service makes use of, and define the actions required for mail detected by each method. You can define these settings to apply globally or for a specific domain. In this way, a particular domain can use specific detection methods and have specific actions for mail detected by these methods.

These spam detection methods are available:

- **Public block lists:** the Anti-Spam service can detect email from globally known sources of spam. These are companies and individuals who have demonstrated patterns of junk emailing. These sources are identified within recognized public block lists of IP addresses. Administrators can use these public block lists through ClientNet.
- **Signaturing system:** the signaturing system leverages both proprietary and commercially available signature-building engines to create a vast knowledgebase of samples of spam messages currently in email circulation. This enables exact matching of spam, significantly reducing chances of real business mail being stopped by the scanner, as well as speeding identification and message-handling. (A signature is a unique string that defines a specific spam email, which can then be used to detect further instances of the email.)
- **Skeptic heuristic engine:** Skeptic™ uses artificial intelligence to create an ever-expanding knowledgebase for identifying spam. The heuristics method works by scoring each email against a set of rules. If the email in question achieves more than a specified score, it is immediately identified as spam.
- **Approved senders list:** you can define a list of IP addresses, domains, or email addresses that are approved senders. Email from these senders will not be identified as spam. The approved senders list can also be used to ensure that email news- letters, which may occasionally be detected as spam, pass through the anti-spam service without interruption. For full details, [see Section 7, Using approved senders and blocked senders lists](#).
- **Custom blocked senders list:** you can define a list of IP addresses, domains, or email addresses that you recognize as sources of spam or other unwanted email. For full details, see [Section 7, Using approved senders and blocked senders lists](#).

You can specify one of these actions for the suspected mail found by each method:

- Append a header but allow the mail through
- Append a header and redirect the mail to a bulk mail address
- Block and delete the mail
- Tag the subject line but allow the mail through
- Quarantine the mail

If an action to **Append a header...** is selected, a string is added to the Internet email header. The format for the string is: X-Spam-Flag: YES

This string identifies the email as spam, enabling further action when it enters the client's mail system or an end user's email client, for example, diverting the email into a 'spam' folder. If an action to **Tag the subject line...** is selected, you can enter the text to add as a tag in the **Detection Settings** tab.

If an action to redirect suspect mail is selected, you must specify a bulk email address to redirect it to. When you are first configuring your Anti-Spam service, a bulk email address may be useful to ensure that spam is being trapped as expected.

Because there is minimal risk of a real business mail being stopped by the scanner (a ‘false-positive’) when using the signaturing and public block elements of the Anti-Spam service, MailStreet Boundary Defense for Email recommends that, once you have confirmed that the service is working as expected, you select the **Block and delete** action for these detection methods. Otherwise a large amount of spam will collect in your bulk mail address mailbox in a short space of time. Using the **Block and delete** action immediately reduces the spam burden with little or no risk. If you use the Spam Quarantine service, this also cuts the time taken by employees to review their Spam Manager accounts.

5.1. Enabling Use of the Approved Senders Lists

If you are using global lists you must enable the use of approved senders lists as a detection method. For full details of using approved senders lists, see [Section 7, Using approved senders and blocked senders lists](#).

To enable the use of approved senders lists:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Detection Settings** tab.
3. In the **Approved Senders** area, select the appropriate checkbox to enable the approved senders list—this depends on which type of listed senders are allowed to bypass the scan: just IP addresses, just domain names and email addresses, or all types of sender (select both boxes).
4. Click **Save and Exit**.
 - A confirmation of the setting is displayed.

5.2. Enabling Use of Blocked Senders Lists

Whether you are using a global list you must enable the use of blocked senders lists. When you enable use of your blocked senders lists you must define an action for any email that is identified as being sent by a blocked sender. (For full details of using blocked senders lists, [see Section 7, Using approved senders and blocked senders lists](#).)

To enable the use of blocked senders lists:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Detection Settings** tab.
3. In the **Responsive Spam Detection** area, select the appropriate checkbox to enable the blocked senders list depending on which type of senders in your lists are allowed to bypass the scan: just IP addresses, just domain names and email addresses, or all types of sender (select both boxes).
4. For each **Use blocked senders list** checkbox that you have selected, select an action for the detected spam from the **Action** drop-down list.
5. Click **Save and Exit**.
 - A confirmation message is displayed.

5.3. Using Public Block Lists

Public block lists are existing lists of information about known spammers. The Anti-Spam service uses several public block lists as part of its protection. You can choose to have your emails scanned for senders on any of these lists. They are:

- Public block list RBL (Real Time Blackhole List)
- Public block list RSS (Relay Spam Stopper)
- Public block list DUL (Dynamic User List)

To enable the use of a public block list:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Detection Settings** tab.
 - In the **Responsive Spam Detection** area, there are four checkboxes to enable the public block lists.
3. Select the public block lists to use.
 - Links are provided to the web sites of the public block list providers (click the name).
4. For each public block list that you have selected, specify an **Action** from the drop-down list, to be used for any emails sent by senders on the list.
5. Click **Save and Exit**.
 - A confirmation of the settings is displayed.

5.4. Using the Signaturing System

The signaturing system uses proprietary and commercially available signature-building engines to create a vast knowledgebase of known spam messages currently in email circulation. A signature is a unique string of bits that define a specific spam email, which can then be used to detect further instances of the email. This enables exact matching of spam, significantly reducing chances of false-positives as well as speeding identification and message-handling.

To enable the use of the signaturing system:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Detection Settings** tab.
3. In the **Responsive Spam Detection** area, select the **Use signaturing system** checkbox.
4. Select an **Action** from the drop-down list, to be used for any emails found by the signaturing system.
5. Click **Save and Exit**.
 - A confirmation of the setting is displayed.

5.5. Using Skeptic Heuristics

The Skeptic™ heuristics engine is a predictive spam detection technology patented by MailStreet Boundary Defense for Email, which works by scoring email against a set of rules. If an email achieves more than a specified score, it is identified as spam. The Skeptic heuristics detection method is distinctly different from the signaturing system because it is predictive rather than reactive technology. The proactive nature of this element of the Anti-Spam service targets unknown spam threats, thus attempting to prevent new spam from reaching your network. It is often this detection method that is responsible for identifying those spam emails that change most frequently, such as pornographic or fraudulent mailings. Due to the predictive nature of this method you may wish to quarantine this mail, although many organizations opt to block and delete suspect mail found by Skeptic.

To enable the use of Skeptic:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Detection Settings** tab.
3. In the **Predictive Spam Detection** area, select the **Use Skeptic heuristics** checkbox.
4. Select an **Action** from the drop-down list, to be used for any emails found by Skeptic.
5. Click **Save and Exit**.
 - Confirmation of the setting is displayed.

5.6. Defining a Bulk Mail Address

If an action to **Append a header and redirect to a bulk mail address** is selected for a detection method, you must define an address to which the spam mail is redirected.

To define a bulk email address:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Detection Settings** tab.
3. In the **Bulk Mail Address** area, enter the email address to redirect the spam mail to.
 - This field is inactive unless one of the spam detection actions is **Append a header and redirect to a bulk mail address**.
4. Click **Save and Exit**.
 - Confirmation of the setting is displayed.

5.7. Defining a Subject Line Tag

You can define the text that is used in the subject line of a suspected spam email when the action **Tag the subject line but allow mail through** is selected. The default tag is 'SPAM:' as a prefix to the subject line. You can define whether to put the tag before or after the subject line text.

To define a subject line tag:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Detection Settings** tab.
3. In the **Subject Line Text** area, enter the text to appear on the subject line of emails tagged as spam.
 - This field is inactive unless one of the spam detection actions is **Tag the subject line but allow mail through**.
4. Click **Save and Exit**.
 - A confirmation of the setting is displayed.

6 Defining Quarantine Settings

The spam mail detected by Anti-Spam is held in Spam Manager and from there can be viewed, released to the original recipient's inbox, or deleted. The messages in Spam Manager can be handled by individual users or other nominated individuals, depending on the deployment policy chosen. Similarly, the contents of Spam Manager may be reviewed regularly or checked only occasionally for specific messages.



For full details of deploying and managing Spam Manager accounts, see the *Anti-Spam Service- Spam Manager Deployment Guide* and the *Anti-Spam Service - Spam Manager Quarantine Administrator Guide*.

The following general quarantine settings are defined within ClientNet:

- **Specifying notifications:** specify whether, when an account is created, a welcome message is generated and summary notifications are enabled. Notifications provide information to your users and ask them to register with and log on to Spam Manager.
- **Defining a default language for Spam Manager notifications:** specify the default language for the content of welcome messages and notifications.
- **Defining Quarantine Administrators:** Quarantine Administrators are users of Spam Manager who have extended privileges to perform administrative functions in Spam Manager.
- **Enabling ClientNet users to request additions to the global approved senders list:** specify whether your users can request that senders of suspect emails can be added to the organization's global approved senders list.
- **Aliases:** specify whether your Spam Manager users are informed when aliases are created by the Quarantine Administrator in Spam Manager. An example of using this is that if a user has multiple email addresses, each with their own Spam Manager account, they can be aliased to a single account—this would mean that the spam sent to any of their email addresses is managed using a single Spam Manager account.

Quarantine settings can be defined to apply at global and domain level.

6.1. Specifying Notifications

You can specify whether, when an account is created, a welcome message is generated and summary notifications are enabled. Welcome messages provide information to your users and ask them to register with and log on to Spam Manager. Summary notifications contain a list of received spam emails and provide a link for the user to log on to Spam Manager to view them.

If welcome messages and notifications are not sent, deployment is 'silent'—that is, a designated Quarantine Administrator accesses the user's Spam Manager account on the user's behalf.

To configure Spam Manager notifications:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Quarantine Settings** tab.
3. In the **Notifications** area, check the **Users receive welcome messages and summary notifications** checkbox to enable this feature. Typically, the setting to send welcome messages and summary notifications is applied to all new accounts created in Spam Manager. This notification setting can be overridden when a Quarantine Administrator creates an account. Also, where notifications are enabled for a Spam Manager user's account, that user may also be able to switch notifications off themselves (see *Step 4*).
4. If you have selected to send notifications, specify the frequency with which summary notifications are sent, by selecting an option from the drop-down list. By default, these notifications are sent every Monday.
5. This setting only affects the default configuration for new accounts. If this setting is changed after the activation of Spam Manager, it does not affect existing accounts.
6. Click **Save and Exit**.
 - A confirmation message is displayed.



You can set the default to permit new users to override these notification settings, if required. See [Section 6.3, Defining user account controls](#).

6.2. Defining a Default Language for Spam Manager Notifications

You can specify the default language used for the content of welcome messages and notifications triggered by Spam Manager. Users may select a different language from within the Spam Manager interface, which overrides this default setting.

To define a default language for Spam Manager notifications:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Quarantine Settings** tab.
3. In the **Default Language for Spam Manager Notifications** area, select the required language from the drop-down list.
4. Click **Save**.



The Spam Manager login screen is not associated with a specific domain or client.—Spam Manager detects the appropriate language for the login screen using the web browser's localization settings.

6.3. Defining User Account Controls

6.3.1 User notification control

This setting determines whether users can override the default notification setting defined in [Section 6.1, Specifying notifications](#)—if enabled, users are given notification options in their Spam Manager accounts. By default this is enabled for the users.

1. Select **Configuration > Email Services > Anti-Spam**.
2. Select **Quarantine Settings**.
3. Check the **Users can override notification defaults** checkbox to permit users to amend their notification settings, if required.

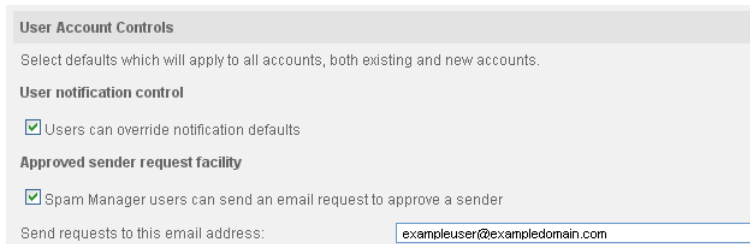


This setting only affects the default configuration for new accounts and does not affect existing accounts.

6.3.2 Approved sender request facility

To specify an email address to which approved sender requests will be sent:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Select **Quarantine Settings**.



User Account Controls

Select defaults which will apply to all accounts, both existing and new accounts.

User notification control

Users can override notification defaults

Approved sender request facility

Spam Manager users can send an email request to approve a sender

Send requests to this email address:



When **Save & Exit** is clicked, or when another tab is selected, the email address is validated—that it is a valid email address format and has a domain belonging to the client.

6.4. Enabling ClientNet Users to Request Additions to the Approved Senders List

The **Approved Senders Request Facility** setting (see also [Section 6.3.2, Approved sender request facility](#)) determines whether Spam Manager users can request that the senders of email that has been identified as spam are added to the organization's global approved senders list. For more information on approved senders lists, see [Section 7, Using approved senders and blocked senders lists](#). By default, this is disabled for the users.

If this facility is enabled, when a user releases a message from Spam Manager (that is, the message is not considered by the user to be spam) the option to request that the sender is added to the approved senders list is provided in the user's message release page.

If you enable this facility, enter the address to which approved senders list requests are sent. This should be the address of the person who is responsible for managing the approved senders lists in ClientNet.



This functionality does not need to be enabled for users who have control of their own user approved and blocked senders lists in Spam Manager (see [Section 9, Using approved senders and blocked senders lists](#)).

6.5. Aliases

Aliases are established to:

- Direct the spam for a user with multiple email addresses to a single Spam Manager account.
- Manage spam sent to a distribution list email address, using a single Spam Manager account.

By their nature, aliases operate in the background and users simply check any spam using Spam Manager as required. If Administrators make any changes to aliases, it may be useful for the users who are affected to be made aware of those changes. This can be done by selecting the checkbox as shown below.

Aliases

Users are always informed when administrators change settings which affect their aliases.

6.6. Defining Quarantine Administrators

Quarantine Administrators are users of Spam Manager who have extended privileges. These privileges allow them to perform some administrative functions in Spam Manager, including:

- viewing details of Spam Manager accounts
- creating accounts
- deleting accounts
- creating aliases to direct the spam of a distribution list or group of users to a single account
- logging on to another user's Spam Manager account and managing their spam.



For full details of managing Spam Manager accounts, see the [Email Anti-Spam Service - Spam Manager Quarantine Administrator Guide](#).

To define your Quarantine Administrators:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Select **Quarantine Settings**.
3. Enter the email addresses of the Quarantine Administrators. Multiple addresses must be separated with a semi-colon.



You can enter up to 65 Quarantine Administrator email addresses.

6.7. Password Controls

6.7.1 Default password control settings

Password Controls are used to enable and enforce your password policy. The system includes default templates at three levels which may be selected as a basis for a password policy. These are described briefly below, and detailed in the table.

- **Basic.** These settings are for minimal security, and would (for example) permit weak passwords to be used which could potentially be more easily guessed or cracked. This is the default setting for the system when it is first provisioned—clients are recommended to adjust these individual settings to whatever is more appropriate for their requirements, or to select the Standard or Enhanced security settings level.
- **Standard.** These settings offer increased security which many organizations may consider to be sufficient for their requirements, such as mandatory numeric characters in passwords, and set some of the security levels of other settings to increased values.
- **Enhanced.** These settings are for enhanced security, by turning on all the features and setting the security levels of appropriate items to an advanced security level, whilst maintaining the system at a level of usability which should still be manageable and not excessive



These settings are intended as a starting guideline only—most organizations will want to customize some or all of these settings to their own requirements and to fit in with their Acceptable Use and Security policies. See [Section 6.7.2, Configuring the password policy](#) for details of how to apply these templates, and how to customize the password control settings.

| Default Password Settings | | Basic | Standard | Enhanced |
|---|------------------|-------|----------|----------|
| Character Requirements | | | | |
| Minimum characters required in a password | | 8 | 8 | 12 |
| Character requirements | | | | |
| | Alphabetic | ✓ | ✓ | ✓ |
| | Numeric | ✗ | ✓ | ✓ |
| | Non-alphanumeric | ✗ | ✗ | ✓ |

| Default Password Settings | Basic | Standard | Enhanced |
|--|-------------|-------------|-------------|
| Character repetition and sequences within passwords | | | |
| Max length of sequences of repeated characters | 4 | 4 | 2 |
| Max number of characters in alphabetic, numeric or keyboard order | Not Set | Not Set | 3 |
| Other password content | | | |
| Use of words in a dictionary (including common substitutions) | Allowed | Not Allowed | Not Allowed |
| Use of part of the user email address (including common substitutions) | Not Allowed | Not Allowed | Not Allowed |
| Re-use and changes | | | |
| Number of password resets before a user can re-use the same password | 3 | 5 | 20 |
| Maximum number of password changes in 24 hours | 10 | 10 | 5 |
| Password expiry | | | |
| Password expiry time | 90 days | 30 days | 30 days |
| Time prior to expiry to alert users | 7 days | 7 days | 7 days |
| Spam Manager lock-outs (Standard Accounts) | | | |
| Number of incorrect password entries prior to lock-out | 100 | 20 | 9 |
| Lock-out period | 30 minutes | 4 hours | 1 day |
| Spam Manager lock-outs (Administrator Accounts) | | | |
| Number of incorrect password entries prior to lock-out | 20 | 10 | 3 |
| Lock-out period | 1 hour | 8 hours | Permanent |

6.7.2 Configuring the Password Policy

In the **Password Controls** section of the *Anti-Spam Quarantine Settings* page, under **Password policy**, the current policy in use is displayed—this will be **Basic**, **Standard**, **Enhanced** or **Custom**.

Custom is displayed if any changes have been made to the default settings inserted by any of the templates

To configure the password policy:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Select **Quarantine Settings**.
3. Click on the **Configure password policy** button.
 - See sample **Password Policy** screen next page

Password Policy

Global Settings

Basic Standard Enhanced

Customize selected policy

Character requirements

Minimum characters required in a password:

Character types required in a password: alphabetic numeric non-alphanumeric (for example ! \$ # %)

Character repetition and sequences within passwords

Maximum length of sequences of repeated characters:

Maximum number of characters in alphabetic, numeric or keyboard order:

Other password content

Use of words in a dictionary (including common substitutions):

Use of part of the user email address (including common substitutions):

Re-use and changes

Number of password changes before a user can re-use the same password:

Maximum number of password changes in 24 hours:

Password expiry

Password expiry time:

Time prior to expiry to alert users:

Spam Manager lock-outs (Standard Accounts)

Number of incorrect password entries prior to lock-out:

Lock-out period:

Spam Manager lock-outs (Administrator Accounts)

Number of incorrect password entries prior to lock-out:

Lock-out period:



When you leave the current page by selecting this **Configure password policy** button, the settings on the current page are remembered, but they are not saved until you select **Save & Exit**.

4. Select the radio button for the template to be used as a starting point for your password policy: **Basic**, **Standard** or **Enhanced**—the page will be populated with the default settings for that policy. If this is the first time of viewing this configuration screen since the service was provisioned, the **Basic** setting is probably already selected—simply select **Standard** or **Enhanced** to change this. To be able to change the policy settings displayed to meet your requirements, ensure that the **Customize selected policy** checkbox is checked.
5. Specify the minimum length for your users' passwords, using the drop-down list in the **Character requirements** section. The character types required in passwords can be selected by checking the boxes—**alphabetic**, **numeric** and **non-alphanumeric** characters. If a box is not checked, that type of character can still be used in passwords, but its use is not enforced.
6. **Character repetition** controls the number of times a particular character is repeated (for example, dddd). Specify the maximum number of repeated characters allowed in passwords, using the drop-down list. **Character sequences** controls the number of alphabetic (for example defg), numeric (for example 4567), and keyboard (for example qwerty) characters which are allowed in sequence. Select the maximum number of characters in sequence which can be used, using the drop-down list.



These character sequences take into account several languages, including English, where they affect the alphabet or keyboard layout.

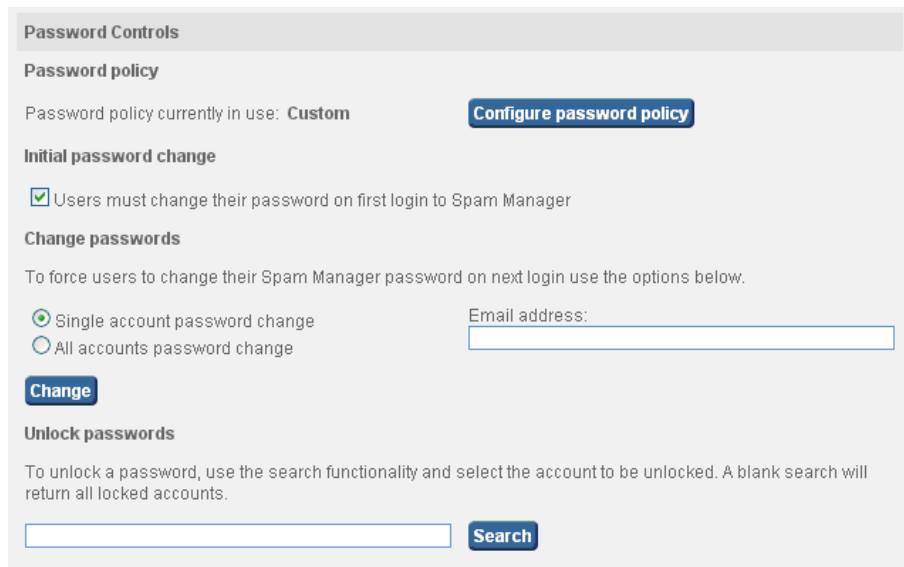
7. From the drop-down list, select whether any words in a standard dictionary can be used in passwords. Also select whether a user can include in their password part of the email address they use when logging in to Spam Manager. Both of these conditions include substituting characters with commonly used alternatives (for example, using the number 3 instead of the letter E, or using the number 1 instead of the letters I or L).
8. Set the options for re-use of the same password, and how frequently users can reset their password—these options can be used to prevent users from resetting their password repeatedly until they are able to use the password they started off with.
9. Password expiry settings are selected using the drop-down lists. The password expiry time is the time which will elapse after a password is set up until it expires—when it expires, the user is allowed to log in using the old password, but is immediately prompted to change it. It can be helpful to prompt users in advance of their password expiring, to give them the opportunity to think of a new password—set this advance warning time as required.
10. When a user or administrator is logging in to Spam Manager, the number of attempts to key in the correct password can be limited—this is to stop password cracking systems from persisting in trying random passwords until they gain access to the system. When the user or administrator is locked out, until the lockout expires, they will be unable to gain access to Spam Manager even if they use the correct login credentials.
 - The most extreme setting for the administrator lockout is Permanent—if the administrator is locked out in this way, they must contact MailStreet Boundary Defense for Email Global Client Support Center to have their account unlocked before they can log in to Spam Manager.
11. Select **Save & Exit** to apply the password control settings.
 - You are returned to the **Password Controls** configuration screen.

6.7.3 Customizing password control settings

To customize password control settings:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Select **Quarantine Settings**.
3. In the **Password Controls** section, under **Password policy**, the current policy in use is displayed—this will be **Basic, Standard, Enhanced** or **Custom**.

Custom is displayed if any changes have been made to the default settings inserted by any of the templates. See [Section 6.7.2, Configuring the password policy](#) for details of how to configure the password policy



The screenshot shows the 'Password Controls' configuration page. It includes a 'Password policy' section with a dropdown menu currently set to 'Custom' and a 'Configure password policy' button. Below this is the 'Initial password change' section, which has a checked checkbox for 'Users must change their password on first login to Spam Manager'. The 'Change passwords' section has two radio buttons: 'Single account password change' (selected) and 'All accounts password change'. There is an 'Email address:' input field next to the 'Single account password change' option. A 'Change' button is located below the radio buttons. The 'Unlock passwords' section has a text box and a 'Search' button.

4. Check the **Initial password change** checkbox to ensure that any new users created after you check this box have to change their password when they first log in to Spam Manager—this new password must comply with the password policy that you have put in place.



When you enable this option, all accounts already in existence, even if they have not yet logged in to Spam Manager, would not have this password change enforced.

5. To force an individual user to change their password, enter their email address in the box, and select the **single account password change** button. You must select **Save & Exit** to force the user to change their password.
 - To force all users to change their passwords when they next log in, select **All accounts password change** then select **Save & Exit**.
6. Your company's Acceptable Use Policy is key in the enforcement of your password policy. If this is available online for your users to read, check the **Acceptable Use Policy** checkbox, and enter its URL in the **AUP** box. This link can be displayed in Spam Manager and Email Notifications—check the checkboxes to display it as required

Acceptable Use Policy

To provide users with details of your company Acceptable Use Policy and password requirements, provide a URL link and select where you wish the URL to be visible.

Users can view your company Acceptable Use Policy (AUP)

Specify URL link to your AUP :

Display in : Spam Manager Email Notifications

7. Select the appropriate **Visibility** checkboxes, so that in Spam Manager users can, if required, view subject lines of emails, pre- view message text content, or delete emails. In email digest notifications, the ability to see the subject line of emails can also be enabled.
 - These options are of particular relevance in those countries where legislation precludes the display of these items without the whole email being read by the user—this legislation may mean that these items must not be viewed without the email being received in the normal way.

Visibility

Control user access to message information.

Spam Manager

Users can view subject lines within the Spam Manager interface.

Users can preview message content within the Spam Manager interface.

Users can delete messages within the Spam Manager interface.

Notifications

Include subject line in digest notifications.

8. When all options have been set up as appropriate, select **Save & Exit** to apply the settings.

7 Using Approved Senders and Blocked Senders Lists

This section introduces the concept of approved senders and blocked senders lists.

7.1. Introduction to Approved and Blocked Senders Lists

You can define a list of approved senders or blocked senders for your organization. An approved sender is identified by their IP address, domain name, or email address that you want to receive email from, even though they may be on a public block list or a custom blocked list. A blocked sender is an IP address, domain name, or email address that you want to block emails from.

You can define approved and blocked senders lists by adding entries to the list manually or by downloading the existing list from Client-Net, editing it offline, and uploading the revised list to ClientNet.

You can define approved and blocked senders lists at a global level. Global approved and blocked senders lists can contain up to 3000 entries each.

- You should not put your domain name in your own approved senders list, for example, if you use an external mailing company to contact your internal users and they spoof your domain name within the sent address. By including your own domain name, you open the organization up to a security exploit, because spammers sometimes spoof the sending email address to match the target email domain (you) in an attempt to bypass Anti-Spam scanning. Instead, include your partners' sending IP addresses.
- You cannot define approved senders and blocked senders lists at domain level.

These **validation rules** apply to all approved senders and blocked senders list entries:

- Email address
 - o Full email addresses with valid domain names, such as **broberts@shopping.com** are valid
 - o Partial email addresses, such as **broberts@shopping** are not valid
- Domain name
 - o Full domain names, such as **example.com** are valid
 - o Top-level domains, such as **.com** or **.uk** or **.org** are valid
 - o Partial domains with the top-level domain present, such as **defender.com** are valid
 - o Subdomains, such as **name.domain.com** are valid
 - o Partial domains without the top-level domain, for example **defender** or **webcam** are not valid
 - o The * wildcard is also not valid within a domain name
- IP address
 - o A series of basic IP address validation rules prevent any invalid IP addresses being entered into the spam lists
 - o The * wildcard is valid to match the number in the last part of a dotted-quad IP address. For example **192.168.0.*** can be used to represent all the host IP addresses on the **192.168.0.0/24** network. Two wildcards cannot be used in an IP address
 - o IPv6 IP addresses are not valid

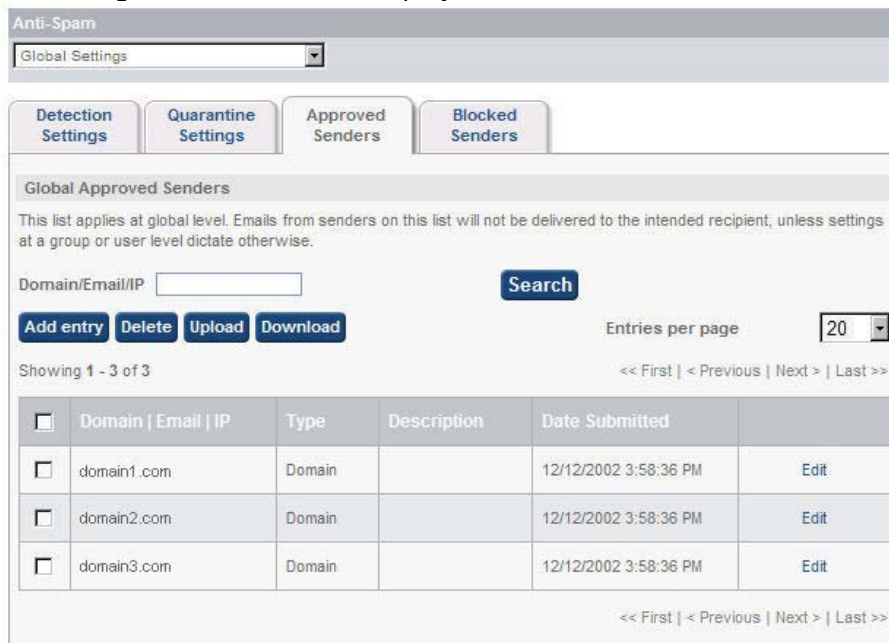
7.2. Defining Global Lists

Global lists are defined in ClientNet—first, select **Global Settings** from the domains drop-down list.

7.2.1 Viewing global approved and blocked senders lists

To view an approved or blocked senders list:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Approved Senders** or **Blocked Senders** tab, as required.
 - The global senders list is displayed:



The screenshot shows the 'Anti-Spam' configuration window. At the top, there is a dropdown menu set to 'Global Settings'. Below this are four tabs: 'Detection Settings', 'Quarantine Settings', 'Approved Senders', and 'Blocked Senders'. The 'Approved Senders' tab is selected. The main content area is titled 'Global Approved Senders' and contains a descriptive paragraph: 'This list applies at global level. Emails from senders on this list will not be delivered to the intended recipient, unless settings at a group or user level dictate otherwise.' Below the text is a search box labeled 'Domain/Email/IP' with a 'Search' button. There are also buttons for 'Add entry', 'Delete', 'Upload', and 'Download'. To the right, there is a 'Entries per page' dropdown set to '20'. Below the search area, it says 'Showing 1 - 3 of 3' and navigation links: '<< First | < Previous | Next > | Last >>'. A table with the following data is displayed:

| <input type="checkbox"/> | Domain Email IP | Type | Description | Date Submitted | |
|--------------------------|---------------------|--------|-------------|-----------------------|------|
| <input type="checkbox"/> | domain1.com | Domain | | 12/12/2002 3:58:36 PM | Edit |
| <input type="checkbox"/> | domain2.com | Domain | | 12/12/2002 3:58:36 PM | Edit |
| <input type="checkbox"/> | domain3.com | Domain | | 12/12/2002 3:58:36 PM | Edit |

At the bottom of the table area, there are navigation links: '<< First | < Previous | Next > | Last >>'.

Both approved and blocked senders are listed in the same window. Each sender's domain or email address is listed, along with whether it is an approved or blocked sender.

To search for a specific entry:

- Use the **Search** box to locate a specific entry by entering at least the first few characters of the sender domain, email address, or IP address in the **Domain/Email/IP** box. The * wildcard can be used for partial matching.

To show all results again after a specific search:

- Leave the search box blank and click **Search**.

To sort the entries:

- Click the column heading to sort on.

7.2.2 Adding an entry to a global list manually

To add an entry to the approved or blocked senders list:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
3. Click the **Add Entry** button.
 - The **Domain/Email/IP** and **Description** fields become editable.
4. Enter the email address or domain name (or IP address, if working at global level) and the entry description.
5. To add the entry to the list, click **Update**.
 - The entry is added to the list.

7.2.3 Downloading a global approved or blocked senders list

You can download a CSV file of approved senders or blocked senders so that you can edit existing entries and insert new entries into the list and then upload it back to ClientNet. When saving the list, ensure that it is saved using CSV (comma-separated values, also known as comma delimited) format.

To download a list from ClientNet:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
3. Click the **Download** button.
 - A dialog box asks you whether to open or save the file.

See also:

[Section 7.2.1, Viewing global approved and blocked senders lists](#)

[Section 7.2.4, Uploading a global list to ClientNet](#)

7.2.4 Uploading a global list to ClientNet

You can create or edit a list of approved or blocked senders offline, and upload the list to ClientNet.



The maximum file size for each list is 2 Mb.

There are two options available for uploading lists into ClientNet:

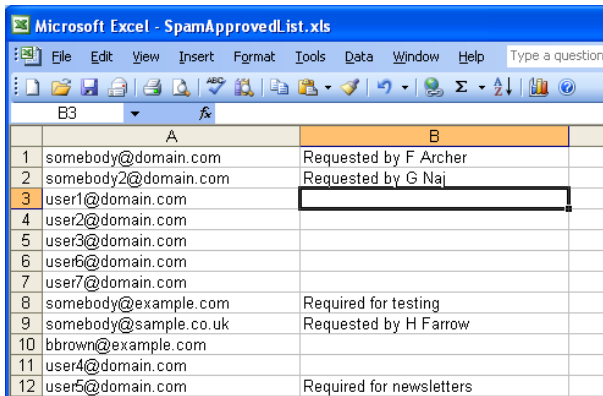
- **Delete existing addresses and replace with uploaded addresses:** by selecting this option the uploaded list replaces the existing list.



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. When merging, if duplicate IP addresses, email addresses, or domain entries exist within both the uploaded and existing list, ClientNet highlights the number of duplicates and gives you the option to overwrite the entries in the existing list (and to change their description, if required), or to cancel the list merge process. This **screenshot** shows the content of an approved senders list in Microsoft Excel:



| | A | B |
|----|-----------------------|--------------------------|
| 1 | somebody@domain.com | Requested by F Archer |
| 2 | somebody2@domain.com | Requested by G Naj |
| 3 | user1@domain.com | |
| 4 | user2@domain.com | |
| 5 | user3@domain.com | |
| 6 | user6@domain.com | |
| 7 | user7@domain.com | |
| 8 | somebody@example.com | Required for testing |
| 9 | somebody@sample.co.uk | Requested by H Farrow |
| 10 | bbrown@example.com | |
| 11 | user4@domain.com | |
| 12 | user5@domain.com | Required for newsletters |

The first column lists the IP address, email address, or domain entry, and the second column lists the associated descriptions.

To upload a list:

1. Select **Configuration > Email Services > Anti-Spam**.
2. Click the **Approved Senders** or **Blocked Senders** tab, as appropriate.
3. Click **Upload**.
 - The **Upload Approved Addresses** or **Upload Blocked Addresses** (as appropriate) is displayed.
4. Enter the file path and name to upload or click **Browse** to locate the file.
5. Select the appropriate option button in the **On upload** area, depending on whether the new addresses should replace or be merged with any existing addresses (duplicate entries are ignored).
6. Click **Upload**.
7. Click **Finish**.
 - The new list entries are added to the list displayed in the **Approved Senders** or **Blocked Senders** tab.

Glossary

| TERM | DEFINITION |
|--|---|
| Activation (Of Spam Manager) | The final stage in the deployment process, after which spam is redirected to Spam Manager. |
| Alias | An email address that is designated to be managed by the account of another email address (the owner address) so that spam sent to each of the aliased addresses is managed by and uses the settings of the owner account. |
| Anti-Spam Service | The service that processes incoming email messages, directs suspected spam to Spam Manager, and lets other 'clean' messages through to users' email inboxes. |
| ClientNet | The tool through which the Anti-Spam Service is configured |
| Configuration (of Spam Manager) | The stage during the deployment of Spam Manager when the service is set up to operate in the chosen way. This is performed within ClientNet |
| Default | An option that is used if no other option is supplied. (Defaults may sometimes be overridden.) |
| Domain | A name used to identify a collection of resources on the Internet, e.g. example.com |
| False Negative | A positive instance that is erroneously reported as being negative—that is, a spam email which is erroneously reported as not being spam |
| False Positive | A negative instance that is erroneously reported as being positive—that is, a non-spam email which is erroneously reported as being spam |
| Notification | An email message, generated automatically, and at preset intervals, listing new spam held in the user's Spam Manager account. |
| Quarantine Administrator | A user of Spam Manager with additional privileges, allowing them to perform some administrative functions |
| Silent Deployment | A method of deploying Spam Manager, in which accounts do not issue welcome messages or periodic notifications of spam. In this way an account can be created, but the presence of Spam Manager is not made visible to the user. The spam is viewed and managed by an Administrator |
| Spam | Unwanted email, often sales literature, sent indiscriminately to many addresses |
| Targeted Deployment | A method of deploying Spam Manager, in which most accounts are 'silent', but some 'targeted users' (key personnel) are given access to their accounts |
| Welcome Message | <p>A message, sent automatically by Spam Manager to the email addresses of users for whom either:</p> <ul style="list-style-type: none"> • New Spam Manager accounts have been created explicitly; or • Spam has been received for the first time (i.e. an account is being created (implicitly)) <p>The message invites the User to visit their Spam Manager account and review their spam</p> |

***** *End of MailStreet Boundary Defense for Email Admin Guide* *****