

LEGEND FOR MENU NAVIGATION

Menu | Structure [Buttons] **Tab or Sub-Tab** Hyperlink **Column Name, Drop-Down Menu, Checkbox etc.** *Instruction*

ANTI-VIRUS

FEATURE	MENU NAVIGATION QUICK REFERENCE	COMMENT
Log In to ClientNet	Hosting Boundary Defense for Email <u>Log-in to control panel</u> <i>Enter your Admin login credentials</i>	Access ClientNet through the MailStreet Control Panel: https://cp.mailstreet.hostaccount.com . The admin credentials can be found above the Log-in to control panel link of the MailStreet CP
Log Out of ClientNet	[Log Out]	You can Log Out of ClientNet from any screen. The [Log Out] button is at the top left of the screen.
Access the Anti-Virus configuration settings	Configuration Email Services Configuration Anti-Virus	Two (2) Tabs are displayed: Virus Settings; Banners . All Anti-Virus configuration settings listed below are accessed from this section of ClientNet.
Defining settings as Global (Applying to ALL domains)	Global Settings: "Global Settings" <i>Enter your settings on the Virus Settings and Banners tabs</i>	If no specific domain is selected from the Global Settings drop-down menu, all settings are applied Globally to all domains.
Defining settings for a specific domain	Global Settings: Select a domain <i>Enter your settings on the Virus Settings and Banners tabs</i>	The name of the domain for which the settings are being applied is displayed as a heading.
Defining Administrator Alerts	Virus Settings Administrator Alerts: <i>Enter the email address of the administrator</i> [Save and Exit]	By default this is blank (disabled). Leave this field blank if the admin does NOT wish to receive virus alerts.
Defining User Alerts	Virus Settings User Alerts: <i>Select the desired option</i> [Save and Exit]	By default the Virus alert email for Users is ENABLED. Change this setting as desired.
Defining an Address that User Alerts Appear to be Sent From	Virus Settings Use custom virus settings: <i>Enter an email address to be used</i> [Save and Exit]	This feature can only be setup for individual domains, AND the email address entered must be a valid email address within the domain.
Releasing a Virus from Quarantine	Virus Settings Virus Release (Upper right corner) <i>Enter the PIN number of the virus sent from the Virus Alert email</i> [Go] <i>Locate the entry required</i> [Release] [Confirm]	If implemented, the email containing the virus is released to the intended recipient. Only Admins can release a virus-quarantined email.
Limiting the Size of an Email	Virus Settings Set maximum email size to: <i>Enter the maximum size for emails in KBs</i> [Save and Exit]	Use this setting to set a maximum size above which inbound email will not be received.
Defining Banners	Banners Inbound Mail and Outbound Mail sections: <i>Select the option button and enter the text for customer banners if desired</i> [Save and Exit]	The banner must not exceed the maximum of 4,000 characters.

LEGEND FOR MENU NAVIGATION

Menu | Structure [Buttons] *Tab or Sub-Tab* Hyperlink **Column Name, Drop-Down Menu, Checkbox etc.** *Instruction*

ANTI-SPAM

FEATURE	MENU NAVIGATION QUICK REFERENCE	COMMENT
Log In to ClientNet	Hosting Boundary Defense for Email <u>Log-in to control panel</u> <i>Enter your Admin login credentials</i>	Access ClientNet through the MailStreet Control Panel: https://cp.mailstreet.hostaccount.com . The admin credentials can be found above the Log-in to control panel link of the MailStreet CP.
Log Out of ClientNet	[Log Out]	You can Log Out of ClientNet from any screen. The [Log Out] button is at the top left of the screen.
Access the Anti-Spam configuration settings	Configuration Email Services Configuration Anti-Spam	Four (4) Tabs are displayed: Detection Settings; Quarantine Settings; Approved Senders; Blocked Senders . All Anti-Spam configuration settings listed below are accessed from this section of ClientNet.
Defining settings as Global (Applying to ALL domains)	Global Settings: “Global Settings” <i>Enter your settings on the four (4) Tabs: Detection Settings; Quarantine Settings; Approved Senders; Blocked Senders.</i>	If no specific domain is selected from the Global Settings drop-down menu, all settings are applied Globally to all domains.
Defining settings for a specific domain	Global Settings: <i>Select a domain Enter your settings on the four (4) Tabs: Detection Settings; Quarantine Settings; Approved Senders; Blocked Senders.</i>	The name of the domain for which the settings are being applied is displayed as a heading.
Enabling Use of the Approved Senders List	Detection Settings Approved Senders: <i>Select the appropriate checkbox [Save and Exit]</i>	For those using global lists, you must enable the use of approved senders as a detection method.
Enabling Use of the Blocked Senders List	Detection Settings Responsive Spam Detection: <i>Select the appropriate checkbox(es) For each Use blocked senders list selected, select an action from the Action drop-down list [Save and Exit]</i>	Enable this by selecting the desired Block Senders List option(s).
Using Public Block Lists	Detection Settings Responsive Spam Detection: <i>Select the Public Block Lists to use For each Public Block List selected, select an action from the Action drop-down list [Save and Exit]</i>	Enable this by selecting the desired Public Block List option(s).
Using the Signaturing System	Detection Settings Responsive Spam Detection: <i>Select the signaturing system checkbox Select an action from the Action drop-down list [Save and Exit]</i>	Enable this spam prevention method which uses known databases of spammers, etc.
Using Skeptic Heuristics	Detection Settings Responsive Spam Detection: <i>Select the Use Skeptic heuristics checkbox Select an action from the Action drop-down list [Save and Exit]</i>	Enable this spam prevention method which utilizes heuristics and algorithms to determine spam to be quarantined.
Defining a Bulk Mail Address	Detection Settings Bulk Mail Address: <i>Enter the email address to redirect the spam email to [Save and Exit]</i>	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.
Defining a Subject Line Tag	Detection Settings Subject Line Tag: <i>Enter the text to appear on the subject line of emails tagged as spam [Save and Exit]</i>	This field is inactive unless one of the spam detection actions is Tag the subject line but allow the mail through .
Configure Spam Manager Notifications	Quarantine Settings Notifications: <i>Check the Users receive welcome messages and summary notifications checkbox Specify the frequency [Save and Exit]</i>	This setting only affects the default configuration for new accounts. Users may change the frequency via activation of their Spam Manager account.

LEGEND FOR MENU NAVIGATION

Menu | Structure [Buttons] *Tab or Sub-Tab* Hyperlink **Column Name, Drop-Down Menu, Checkbox etc.** *Instruction*

ANTI-SPAM (Continued)

FEATURE	MENU NAVIGATION QUICK REFERENCE	COMMENT
Defining the default language for Spam Manager Notifications	Quarantine Settings Default Language for Spam Manager Notifications: <i>Select the language from the drop-down list</i> [Save]	Users may select a different language from within the Spam Manager interface, which overrides this default setting.
Define User notification control	Quarantine Settings Notifications: <i>Check the Users can override notification defaults checkbox</i> [Save and Exit]	This setting determines if Users can override the default settings. By default this is enabled for Users. Users are notified via the Spam Manager email.
Define Quarantine Administrators	Quarantine Settings <i>Enter the email addresses of the desired Quarantine Administrators</i>	Multiple addresses must be separated by a semi-colon (;).
Configuring Password Policy	Quarantine Settings Configure password policy <i>Select radio button for template to be used (Basic, Standard or Enhanced)</i> <i>Modify the template as needed for your desired Password Policy</i> [Save and Exit]	Communicate the Password Policy established to your Users.
Force Users to change passwords	Quarantine Settings Password Controls > Password Policy: <i>Check the Initial password change checkbox</i> <i>Select All accounts password change</i> [Save and Exit]	This can be set for individual Users to force a password change for a specific User.
Viewing global approved and blocked senders lists	Approved Senders OR Blocked Senders <i>Review as needed:</i> <ul style="list-style-type: none"> • <i>To Search > Use the Search box and enter a few characters</i> • <i>To Show ALL results again after a search > Leave Search blank and click Search</i> • <i>To Sort the Entries > Click on the column heading to sort on</i> 	For global lists make sure that the Global Settings is selected in the top-level drop-down menu.
Adding an entry to a global list manually	Approved Senders OR Blocked Senders Add Entry > <i>the Domain/Email/IP and Description fields become editable</i> <i>Enter the new item</i> [Update]	Use this procedure for approved OR blocked senders.
Download a global approved or blocked senders list	Approved Senders OR Blocked Senders [Download] <i>A dialog box asks you whether to open or save the file.</i>	Use this to download a CSV file of approved/blocked senders so that you can edit existing entries, add new entries and then re-upload the edited list to ClientNet.
Uploading a global list to ClientNet	Approved Senders OR Blocked Senders [Upload] <i>Browse to the file to upload</i> On Upload: <i>Select the appropriate Merge or Replace option</i> [Upload] [Finish]	Also use this method for uploading a “batch” of multiple entries and use the Merge option during the upload process.