Options

Help Documentation

Antispam | Options

SmarterMail comes equipped with a number of antispam features and functions that allow you to be as aggressive as you want when combatting spam. Default antispam settings were configured during installation, but these settings can be modified at any time.

Due to the flexible nature of SmarterMail's antispam setup, spam checks can influence the spam decision as much or little as you want. When spam protection runs on a particular email, all enabled spam checks are performed on the email. The total weight of all failed tests is what comprises the spam weight for the email. A spam probability level is then assigned to the email using the Filtering settings and an action is taken on that message based on its total spam weight.

An added benefit to SmarterMail's antispam administration is the ability to combat both incoming and outgoing spam messages. Most mail servers only allow Administrators to keep spam from entering the mail server. SmarterMail helps protect mail users from incoming spam but also keeps mail servers from actually sending spam, thereby helping to protect the mail servers from being blacklisted.

To view the antispam options for your server, log in to SmarterMail as an Administrator and click on the Settings icon . Then click on Antispam in the navigation pane. On the Options tab, the following settings will be available:

Jump To:

- Import/Export Settings - Import or export a JSON file containing a server's antispam configuration
- Reset Antispam Settings - Reset the antispam options and spam checks to the default configuration
- Filtering - Define the weight thresholds and default actions for each spam level.
- Trusted Senders - Exempt specific email addresses or domains from spam filtering.
- SMTP Blocking - Configure the thresholds for blocking incoming and outgoing spam messages
- Options - Adjust basic options relating to the processing of spam and the ability for individual domains to override system-level settings.
- Greylisting Options - Temporarily reject email from unrecognized senders.
- SpamAssassin Servers - Configure a SpamAssassin server for identifying and reporting spam.

Import or Export Spam Settings

SmarterMail exports all global spam settings in a single JSON file and allows that JSON file to be imported as needed. This means Administrators can configure a solid set of antispam rules on one

server, then easily move those settings over to any additional SmarterMail servers by copying over the antispam JSON. Email administrators can even work together to create and share their antispam JSON files files, combining their experience and understanding to create the most reliable settings available.

To import or export SmarterMail's spamConfig.json file, click on the Actions (...) button. This click on Import Spam Settings or Export Spam Settings accordingly. When importing spam configurations, custom rules in the JSON will be merged with existing rules in SmarterMail; the imported JSON will not replace all existing rules. For example, if you import an JSON from another system, it will simply add any custom spam checks, RBLs and URIBLs that do not exist in SmarterMail. If you prefer that all existing rules are overwritten, you must delete those rules prior to importing.

Reset Antispam Settings

SmarterMail's antispam configuration can easily be reset to the default configuration by clicking on the Actions (...) button and selecting Reset Antispam Settings . Note that this reset will impact ALL sections of the Antispam area, with the exception of IP Bypasses. Resetting the antispam options will revert all settings on the Options tab, Spam Checks tab, RBLs tab, URIBLs tab, and Greylist Filters tab to the default configuration. This means all trusted senders and domains, SpamAssassin servers, custom spam checks/RBLs/URIBLs and greylist filters will be deleted. To confirm that you would like to erase all customized antispam options, click Reset on the confirmation modal.

Filtering

Emails are filtered into one of three categories based on their total weight: Low Probability of Being Spam, Medium Probability of Being Spam and High Probability of Being Spam. For example, if an email's spam weight is equal to or higher than a certain category, then it is assigned that probability of being spam. Use this section to define the weight thresholds and the default actions at each level.

- Domains can override filter actions - Many Domain Administrators have their own preference of how potential spam email should be handled for their domain. Enable this to allow them to override the spam filtering actions, if they wish. NOTE: Enabling this will NOT allow Domain Administrators to manage the spam Weights -- they can only manage how they want messages flagged as spam, based on the weights set by the System Administrator, to be handled.
- Weight - The email is sorted into probability levels based on the weight threshold values. Adjust the weight threshold according to the probability status selected.
- Action - The action to take when a message ends up with this level of spam probability: No Action, Delete Message, Move to Junk Email Folder or Add Text to Subject. Note: The Delete Message action will permanently delete messages that match the corresponding weight, preventing them from reaching the user's mailbox. Exercise caution when selecting this action, as messages deleted via spam filtering cannot be recovered.

• Text to Add - If the Action is set to Add Text to Subject, enter the text that will be appended to the beginning of a subject when a message reaches a particular level of spam.

Trusted Senders

Use this section to globally exempt specific email addresses (such as jsmith@example.com) or domains (such as example.com) from SmarterMail's spam filtering. This lets the system know that these messages come from a trusted source and can prevent mail from friends, business associates and mailing lists from being blocked or sent to the Junk Email folder. By default, every contact in a user's My Contacts list is considered a trusted sender and bypasses spam filtering.

Note: If SPF and DKIM spam checks are enabled, SmarterMail will run those checks on ALL emails, including those from trusted senders. Because anyone can write any return path that they want when sending a message, this extra check helps prevent spammers from flooding users with hundreds of messages that aren't truly from a trusted sender. If the SPF and DKIM weights on a message from a trusted sender meet the Low, Medium or High spam filtering threshold, the corresponding spam filtering action (Move to Junk Email Folder, Delete Message, Add Text to Subject) will be performed on that email, despite the email coming from a trusted sender.

When entering trusted senders or domains, enter only one item per line.

SMTP Blocking

The idea behind SMTP blocking of incoming and outgoing email is to filter out spam messages before they are delivered. For example, imagine you have four spam checks enabled for Incoming SMTP Blocking and each of those spam checks have a weight of 10. If the Incoming Weight Threshold is set to 30, that means incoming messages will be rejected if they fail three or all four of the spam checks. This card allows you to configure the thresholds and actions taken for SMTP Blocking. Note: Messages rejected due to SMTP blocking do not hit the spool and, therefore, will not be included in the message archive, if enabled. Exercise caution when enabling SMTP Blocking, as rejected messages cannot be recovered.

• Incoming Weight Threshold - By enabling this field, an incoming email must have a total spam weight score of this value or higher in order to be blocked. The score is established by the settings on the Spam Checks, RBLs and URIBLs tabs. (By default, this threshold is set to 50 and is enabled.)
• Greylist Weight Threshold - By enabling this field, an incoming email must have a total spam weight score of this value or higher in order to be greylisted. The score is established by the settings on the Spam Checks, RBLs and URIBLs tabs. (By default, this threshold is set to 30 and is disabled.)
• Outgoing Weight Threshold - By enabling this field, an outgoing email must have a total spam

weight score of this value or higher in order to be blocked. The score is established by the settings on the Spam Checks, RBLs and URIBLs tabs. (By default, this threshold is set to 30 and is disabled.)

• Outgoing Quarantine - This setting is used in conjunction with the Outgoing Weight Threshold and allows administrators to quarantine outgoing messages that have been blocked due to meeting the specified spam weight threshold. Outgoing messages can be quarantined for 15 or 30 days. (By default, this setting is set to None.) When enabled, the quarantine can be found by clicking on the Manage icon, clicking on Spool in the navigation pane, then selecting the Spam Quarantine tab.

Options

• Autoresponders - This setting allows you to add restrictions to a user's ability to create or send autoresponders. Certain antispam organizations will block servers that autorespond to spam traps. To reduce the possibility of this occurring, set the autoresponder option to be as restrictive as your clients will permit:

• Enabled - Users' autoresponder messages will be sent without any restrictions.

• Disabled - Users will not have the ability to configure an autoresponder.

• Require message pass SPF - A user's autoresponder will not be sent if the original sender's message failed the SPF spam check or if the sender's SPF record is not configured. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the user's autoresponder from being sent if the original sender's SPF record is not configured or if the SPF check has failed. Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, autoresponder messages will not be sent. (By default, this option is selected.)

• Require message pass SPF if SPF record exists - A user's autoresponder will not be sent if the original sender's message failed the SPF spam check. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the user's autoresponder from being sent if the original sender's SPF check fails. (This option is distinguishable from the option above as it will only impact messages where the SPF record IS configured and fails the check. If the original sender doesn't have SPF configured, the autoresponder message will be sent.) Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, autoresponder messages will not be sent.

• Content Filter Bouncing - This setting allows you to add restrictions to the content filter action 'Bounce message'. Certain antispam organizations will block servers that send bounce messages back to spam traps. To reduce the possibility of this occurring, set the autoresponder option to be as restrictive as your clients will permit:

• Enabled - An incoming message that triggers the content filter will send the bounce message without any restrictions.
• Disabled - Users will not have the ability to configure a content filter with a 'Bounce message' action.
• Require message pass SPF - An incoming message that triggers the content filter will not have the bounce message sent if the original sender's message failed the SPF spam check or if the sender's SPF record is not configured. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the bounce message from being sent if the original sender's SPF record is not configured or if the SPF check has failed. Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, bounce messages via content filtering will not be sent. (By default, this option is selected.)
• Require message pass SPF if SPF record exists - An incoming message that triggers the content filter will not have the bounce message sent if the original sender's message failed the SPF spam check. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the bounce message from being sent if the original sender's SPF check fails. (This option is distinguishable from the option above as it will only impact messages where the SPF record IS configured and fails the check. If the original sender doesn't have SPF configured, the bounce message will be sent.) Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, bounce messages via content filtering will not be sent.
• Max message size to content scan (KB) - The maximum message size for which content-based spam checks will run. Content-based spam checks include SpamAssassin-based Pattern Matching, Remote SpamAssassin, Cyren Premium Antispam and any custom rules. Note: Increasing this number will also increase the mail server's memory usage. (By default, this limit is set to 4096.)
• Bounce messages when blocked by Outgoing SMTP Blocking - Enable this to send a user a bounce email notification when their outgoing message has not been sent due to its spam probability.
• Enable spool proc folder - Enable this to have SmarterMail place messages into a Spool\Proc folder to be analyzed in the background, usually by third-party products such as Declude or custom-built applications. (By default, the location of the Proc folder is C:\SmarterMail\Spool\Proc.) While the messages are in the Proc folder, .hdr can manipulate elements of the message, such as edit, write, and add headers. Once the scan has been completed, the third-party app is responsible for moving the message back into the spool to be handled by SmarterMail from that point on. This option is most often necessary when using the third-party program, Declude. However, this setting can be used to prevent the disruption of

mail flow with any other third-party app that manipulates messages.

• Disable spam filtering on SMTP whitelisted IP addresses - Disables antispam processing and zeroes the spam weight on whitelisted IPs.

• Enable catch-all accounts to send autoresponders and bounce messages - Enable this if you rely on auto-responders being sent when a message comes in through a catch-all. In general, this is a bad idea, so it should be left unchecked unless your situation specifically requires it.

• Enable SRS when forwarding messages - Enable this to allow the mail server to re-email (as opposed to "forward") an email message so that it passes any SPF checks on the recipient's end.

• Enable DMARC policy compliance check - Enable this to allow the mail server to check messages against the DMARC policy standard. For more information, see the DMARC website .

Greylisting Options

What is greylisting and how does it work?

Greylisting has proven itself to be an effective method of spam prevention. When enabled, the system will keep track of the sending IP address, sending email address and recipient's email address for every message received. If an incoming message has a combination of a sending IP, sending address and recipient address that has not previously been seen, it will return a temporary failure to the sending server, effectively saying, "Try again later." Valid servers will retry the email a short time later, which would be permitted. Spammers, on the other hand, typically create scripts that bombard your server with emails, and they rarely retry on temporary failures. When these messages are bounced back because of greylisting, they are typically not retried, therefore reducing the amount of spam that your customers receive. (Emails sent from whitelisted and authenticated senders will automatically bypass greylisting and are delivered directly to the spool.)

For those messages that are sent from valid email servers, the sending server should retry at least four times. If the first retry is beyond the block period (default 15 minutes) and within the pass period (default 6 hours), the message is passed to the spool and it goes through its normal processing without a delay. A record is also created that says this is a valid email address from that server to the given recipient and keeps it for 36 days (default). If another email from the same email address is received from the same server to the same recipient within the 36 days, the clock is reset for an additional 36 days and delivered directly to the spool.

Why use greylisting?

Greylisting is a very effective method of spam blocking that comes at a minimal price in terms of performance. Most of the actual processing that needs to be done for greylisting takes place on the sender's server. It has been shown to block upwards of 95% of incoming spam simply because so

many spammers don't use a standard mail server. As such, spam servers generally only attempt a single delivery of a spam message and don't reply to the "try again later" request.

Disadvantages of greylisting

The biggest disadvantage of greylisting is the delay of legitimate email from servers not yet verified. This is especially apparent when a server attempts to verify a new user's identity by sending them a confirmation email. Some email servers will not attempt to re-deliver email or the re-delivery window is too short. Whitelisting can help resolve this.

Greylisting configuration options

- Block Period - The period of time (in minutes) that mail will not be accepted (default 15 minutes).
- Pass Period - The period of time (in minutes) in which the sender's mail server has to retry sending the message (default 360 minutes).
- Record Expiration - The period of time(in days) that the sender will remain immune from greylisting once it has passed (default 36 days).
- Applies To - Select who greylisting applies to: 'Everyone', 'Only specified countries/IP address', or 'Everyone except specified countries/IP addresses'. If you choose 'Only specified countries/IP address' or 'Everyone except specified countries/IP addresses', use the Greylist Filters tab to add the specific countries or IP addresses.
- Enable Greylisting - Select this option to enable greylisting.
- Users can override greylisting - Select this option to allow users to selectively turn off greylisting. (This is useful if you have an account that receives time sensitive mail.)

Note: The following cases are exempt from greylisting: Whitelisted IPs for SMTP or greylisting, anyone who authenticates (includes SMTP Auth Bypass list), trusted senders (includes users' contacts), anyone who has already sent you an email (this list generates only after greylisting has been enabled), any IP address specified as being exempt by a greylist filter.

SpamAssassin Servers

SpamAssassin is a powerful, free mail filter used to identify spam. It utilizes a wide array of tools to identify and report spam, including header and text analysis, Bayesian filtering, DNS blocklists and collaborative filtering databases. To setup a SpamAssassin server, click New Server . The following options will be available:

- Name - The name of the SpamAssassin server.
- IP Address - The IP address of the server running SpamAssassin.
- Port - The port on which the SpamAssassin server should listen. By default, the port is 783.