Antispam

Help Documentation

Antispam

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 message, all enabled spam checks are performed on the message. The total weight of all failed tests is what comprises the ultimate spam weight for the message. 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 inbound and outbound spam messages. Most mail servers only allow Administrators to keep spam from entering the mail server. SmarterMail helps protect mail users from inbound 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 inbount and outbound 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 can export all global spam settings as a single JSON file then allows that JSON file to be imported to other SmarterMail servers as needed. This means System Administrators can configure a solid set of antispam rules on one server, then easily move those settings over to any additional SmarterMail servers by importing 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.

It's important to note that the spamConfig.json file is not actually part of the SmarterMail system files -- it's generated during export by pulling individual spam settings from the Settings.json file. These settings are then merged with existing Settings.json files when the spamConfig.json file is imported. Therefore, spamConfig.json files can only be shared between servers running the same version of SmarterMail.

To import or export SmarterMail's spamConfig.json file, click on the Actions (...) button. Then 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 their 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.

- Allow domains to override spam settings - 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.

• 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.
• Weight - The email is sorted into probability levels based on the weight threshold values. Adjust the weight threshold according to the probability status selected.

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 Contacts list is considered a trusted sender and bypasses spam filtering.

Important Note : If SPF and DKIM spam checks are enabled, SmarterMail will run those checks on ALL emails, including those from trusted senders, whitelisted IP addresses and IP bypasses. 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 an SPF or DKIM check fails on an incoming message, the trusted sender status will be bypassed, and the weights of all enabled spam checks will be applied. The specific spam check results that will bypass the trusted sender status are SPF_Fail, SPF_Softfail, SPF_PermError, or DKIM_Fail.

If the trusted sender status of an email was bypassed due to a failed SPF or DKIM check, the TotalSpamWeight line in the email header would appear in the following format:

```
X-SmarterMail-TotalSpamWeight: {Total Spam Weight} ({Where the trusted sender status originates}, {Reason the trusted sender status was bypassed})
```

For example:

```
X-SmarterMail-TotalSpamWeight: 9 (Trusted Sender - Domain, failed SPF)
```

This example indicates that the sender is in the domain-level Trusted Senders list, but the email received a total spam weight of 9 because the message failed the SPF check.

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

SMTP Blocking

The idea behind SMTP blocking of inbound and outbound email is to filter out spam messages before they can be delivered. With SMTP Blocking enabled, messages that are rejected don't even hit the spool. That means that they can't be delivered, but it also means they bypass any other function, like content filtering and even message archiving: messages rejected due to SMTP blocks simply don't exist to SmarterMail, so they aren't processed in any way by the server. Therefore, it's important to exercise caution when enabling SMTP Blocking as rejected messages can not be recovered.

Regarding the weight calculation, when setting up your Spam Checks, RBLs and URIBLs you have the ability to enable each of those for Inbound and/or Outbound SMTP. When enabled for either inbound or outbound, SmarterMail uses the weights associated with those various checks when determining whether a message should be blocked at the SMTP level or not.

For example, imagine you have four spam checks enabled for Inbound SMTP blocking and each of those spam checks have a weight of 10. If the Inbound Weight Threshold is set to 30, that means incoming messages will be rejected if they fail at least three of the four spam checks.

- Inbound Weight Threshold - By enabling this field, an inbound 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 inbound 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.)
- Outbound Weight Threshold - By enabling this field, an outbound 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.)
- Outbound Block Action - This setting is used in conjunction with the Outbound Weight Threshold and allows administrators to quarantine outgoing messages that have met the specified spam weight threshold or block them entirely. When Quarantine Message is selected, messages are quarantined for 30 days. (The quarantine period cannot be changed.) The quarantine can be found by clicking on the Manage icon, clicking on Spool in the navigation pane, then selecting the Spam Quarantine tab.
- Bounce messages when blocked by Outbound SMTP Blocking - Enable this to send a user a

bounce email notification when their outbound message has not been sent due to its spam probability.

Options

• Autoresponders - This setting allows you to add restrictions to a user's ability to create or send autoresponders outside of the domain. (Autoresponders sent locally, to others on your domain, are not affected by these settings.) 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 bounce option to be as restrictive as your clients will permit:

• 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.)

• 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.

• 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, "Tryagain 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 willautomatically 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 (Minutes) - The period of time that mail will not be accepted. The default 15 minutes.
- Pass Period (Minutes) - The period of time in which the sender's mail server has to retry sending the message. The default 360 minutes.

- Record Expiration (Days) - The period of time that the sender will remain immune from greylisting once it has passed. The default 36 days.
- Enable Greylisting - Select this option to enable greylisting.
- Allow users to 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: SMTP Whitelisted IPs, IP Bypasses that are specified to skip 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 or country code specified as being exempt in the Greylist Filters tab.

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.

Spam Checks, RBL and URIBL Lists

SmarterMail comes equipped with a number of antispam features and functions that allow you to be as aggressive as you want when combating 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. Each spam check has one or more associated weights. When spam protection runs on an email, all enabled spam checks are performed. The total weight of all spam checks is what comprises the final spam weight for the email. A spam probability level (Low, Medium or High) is then assigned to the email using the weights configured by the System Administrator on the Filtering card of the Options tab. Based on the email's total spam weight / probability of being spam, the corresponding spam filtering action is taken.

An added benefit to SmarterMail's antispam administration is the ability to combat both inbound and outbound spam messages. Most mail servers only allow administrators to keep spam from entering the mail server. SmarterMail helps protect mail users from inbound spam and also includes the added

benefit of keeping mail servers from actually sending spam, thereby helping to protect the mail server from being blacklisted.

To view and modify the spam checks for your server, log in to SmarterMail as an Administrator and click on the Settings icon. Then click on Antispam in the navigation pane. The Spam Checks , RBLs and URIBLs tabs can be used to create or modify existing spam checks and RBLs for the system.

Note: Only enabled spam checks, RBLs and URIBLs are used when calculating spam weight. To enable or disable a check, enable the appropriate spam check in its configuration options.

Spam Checks

The Spam Checks tab shows all non-RBL/non-URIBL checks that are performed on a message. These checks can include licensed add-ons such as Cyren and Message Sniffer, as well as standard checks such as DKIM, SPF and more. Any of these checks can be enabled or disabled for Inbound and/or Outbound SMTP, and each can be edited or removed. To edit a check, simply click it to open its settings. To add a new Spam Check, such as adding in an antispam appliance, click the New button.

SmarterMail includes several spam checks by default. Each check is described in detail, below.

In general, one or more of the following options may be available when creating a custom spam check or modifying an existing one:

- Enable Spool Filtering - When enabled, the weight assigned for the spam check is added to the message and used as part of its overall spam score. SmarterMail then handles the message based on the spam settings configured for a domain.
- Enable Inbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this spam check is counted toward to weight threshold for the blocking of inbound emails. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking. If this option is not available, then that particular spam check does not offer SMTP blocking and must rely on content filtering instead.
- Enable Outbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this spam check is counted toward to weight threshold for the blocking of outbound emails. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking. If this option is not available, then that particular spam check does not offer SMTP blocking and must rely on content filtering instead.
- Weight - The weight range available for the spam check. Each spam check may utilize unique spam weight options.

Creating Custom Rules

Email can be assigned spam weights based on the header, body text or raw content of a message. For example, the administrator can create a rule that assigns a specific spam weight to all messages containing the word "viagra" in the body text. To configure weights for custom rules, click New , then complete the following fields:

- Rule Name - The name of the rule.
- Rule Source - What you want the rule to be based on: a message's header, body text or raw content. When selecting "body text" or "raw content", you'll need to supply additional information that is applied to the Rule Text: whether the Source "contains" the information, whether the a wildcard is used for a range of information or whether you want to supply a regular expression. If you select Header you will need to supply header details separately from the Rule Text.
- Rule Text - The text that will be used in conjunction with the Rule Source. For example, if you use create a Rule Source based on Body, then an additional Rule Source for "Contains", Rule Text can include words such as "Cialis", "Viagra", etc.
- Weight - The amount to add to the email message's spam weight.
- Enable Spool Filtering - When enabled, the weight assigned for the spam check is added to the message and used as part of its overall spam score. SmarterMail then handles the message based on the spam settings configured for a domain.
- Enable Outbound SMTP Blocking - See above for details.

Cyren Premium Antispam

The Cyren Premium Antispam add-on uses Recurrent Pattern Detection technology to protect against spam outbreaks in real time as messages are mass-distributed over the Internet. Rather than evaluating the content of messages, the Cyren Detection Center analyzes large volumes of Internet traffic in real time, recognizing and protecting against new spam outbreaks the moment they emerge. For more information, or to purchase this add-on, visit the SmarterTools website .

- Enable Spool Filtering - See above for details.
- Enable Outbound SMTP Blocking - See Creating Custom Rules for details.
- Confirmed Weight - The weight that will be assigned if the Cyren Detection Center determines the message as coming from known spam sources.
- Bulk Weight - The weight that will be assigned if the Cyren Detection Center determines the message as sent in bulk. Note: Newsletters or mailing list messages may be included in this classification.
- Suspect Weight - The weight that will be assigned if the Cyren Detection Center suspects the message may be spam because it was sent to a slightly larger than average distribution.

• Unknown Weight - The weight that will be assigned if the Cyren Detection Center is unable to determine the spam probability of a message. This should be treated similarly to a None Weight.

• None Weight - The weight that will be assigned if the Cyren Detection Center deems the message as not spam.

Declude

Declude integration allows you to use Declude products in conjunction with the SmarterMail weighting system. Declude addresses the major threats facing networks, and are handled by a multi-layered defense. Configuration of Declude is done through the Declude product, so all you need to do in SmarterMail is enable the spam check and the Declude score will be included when calculating the total spam weight of a message. For more information, visit www.declude.com .

• Low Spam Weight - The weight that will be assigned if Declude determines a low probability of spam.
• Medium Spam Weight - The weight that will be assigned if Declude determines a medium probability of spam.
• High Spam Weight - The weight that will be assigned if Declude determines a high probability of spam.

DKIM and DomainKeys

DomainKeys and DKIM are an email authentication system designed to verify the DNS domain of an email sender and the authenticity of a message. While a possible source for determining whether an email is spam or not, neither is universally adopted so any weights assigned for failing these checks should be minimal. In addition, because the DomainKey method has become obsolete; we recommend utilizing DKIM instead.

• Enable Spool Filtering - See above for details.
• Pass Weight - Indicates that the email sender and message integrity were successfully verified (less likely spam). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.
• Fail Weight - Indicates that the email sender and message integrity verifications failed (most likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is very high.
• None Weight - Indicates that there was not a valid DomainKey/DKIM signature found to validate the sender and message integrity. Except in very special circumstances, leave this set to 0.
• Max message size to verify - The maximum inbound message size you want the mail server to verify.

Honey Pot

A "honey pot" spam check derives its name because implementing it can attract spammers -- or, more likely, spam bots -- like "bees to honey." Basically, a system administrator populates the honey pot spam check with email addresses that are designed to be seen by, or otherwise used by, spammers. These addresses can be commonly used addresses that spammers will automatically target such as admin@your-domain.com, info@your-domain.com, hr@your-domain.com, etc. These types of addresses are commonly targeted, but SHOULD NOT be addresses that are actually used by any user of a given domain. You don't want to add admin@your-domain.com IF that is an actual address used BY a user on that domain. In fact, any addresses added as honey pot addresses DO NOT need to be an actual account. So if you DO use admin@yourdomain.com as a honey pot address, you do NOT need to add that as an actual account TO the domain. In addition, there's no limit to the number of addresses you can add. It's totally up to the system admin.

Another common way to instantiate a honey pot spam check is to add a hidden email address to a form used on a website. Spam bots can scrape email addresses from these forms, then populate spam lists that are used by, or potentially sold to, spammers. By adding in a hidden (using CSS) honey pot email address to a form, you can essentially trick these bots into scraping that email address, then block any sender who uses the address.

Regardless of HOW you set your trap, honey pots can be a simple, yet effective, way of finding, scoring and then disposing of email spam for your users as well as blocking sending IP addresses.

- Enable Spool Filtering - See above for details.
- Reject found entries at SMTP level - Enabling this will automatically reject the message prior to it being delivered if the IP of the sending mail server has already been listed. NOTE: This will occur as long as the IP is not whitelisted, is not a gateway and is not IP Bypassed.
- Pass Weight - The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating. (Setting negative numbers is not recommended.)
- Listed Weight - This is the weight that is assigned to a message sent from an IP address that was already part of the honey pot.
- Triggered Weight - This is the weight that is assigned to a message that is sent to one of your Honey Pot Addresses. The email address must match one in the list of Honey Pot Addresses for this weight to be added to the message.
- Honey Pot Addresses - These are the actual, full email addresses you're targeting for use by spammers. For example, generic email addresses can be used such as info@example.com or contact@example.com. These should NOT be actual email addresses that are used by anyone on any domain. Ideally, they're addresses that are general enough that spammers would target them

with blanket spam attacks, but not addresses that are posted anywhere or used to actually send email. They are explictly to be used ONLY for trapping potential spammers.

Message Sniffer

The Message Sniffer add-on is an intelligent antispam scanner that uses advanced pattern recognition and collaborative learning technologies to accurately identify spam, scams, viruses, and other email borne malware before it gets to a user's mailbox. For more information, or to purchase this add-on, visit the SmarterTools website .

- Enable Spool Filtering - See above for details.
- Enable Outbound SMTP Blocking - See above for details.
- Confirmed Weight - The weight that will be assigned if Message Sniffer determines the message as coming from known spam sources.
- None Weight - The weight that will be assigned if Message Sniffer deems the message is not spam.

Null Sender

A common spam technique is to send messages with missing, or "Null" sender values. That means that the message appears to come from no one as the sender details are blank. This check allows you to assign a spam weight to messages that meet this criteria.

- Enable Spool Filtering - See above for details.
- Enable Outbound SMTP Blocking - See above for details.
- Weight - The weight assigned to messages that fail this check.

Remote SpamAssassin

SpamAssassin itself is a powerful, third party open source mail filter used to identify spam that can be easily used alongside SmarterMail. It utilizes a wide array of tools to identify and report spam. By default, SpamAssassin will run on 127.0.0.1:783. For more information, or to download SpamAssassin, visit spamassassin.apache.org .

SmarterMail can use SpamAssassin with its weighting system:

- Enable Spool Filtering - See above for details.
- Enable Outbound SMTP Blocking - See above for details.
- Low Spam Weight - The weight that will be assigned if SpamAssassin determines a low probability of spam.
- Medium Spam Weight - The weight that will be assigned if SpamAssassin determines a medium probability of spam.
- High Spam Weight - The weight that will be assigned if SpamAssassin determines a high

probability of spam.

• Client Timeout (seconds) - The timeout that SmarterMail will impose on a server if it cannot connect.

• Max Attempts per Message - The number of times SmarterMail will attempt to acquire a SpamAssasassin score for an email.

• Failures Before Disable - The number of times a remote SpamAssassin server can fail before it is disabled.

• Disable Time (minutes) - The length of time before the SpamAssassin server is re-enabled.

• Header Log Level - The amount of information SpamAssassin inserts into the header of the message

Reverse DNS

Reverse DNS checks to make sure that the IP address used to send the email has a friendly name associated with it.

• Enable Spool Filtering - See above for details.

• Enable Inbound SMTP Blocking - See above for details.

• Weight - The default weight for this spam check. If an email sender does not have a reverse DNS entry, this is the value that will be added to the message's total spam weight.

• Forward Confirm Fail Weight - Forward Confirm Reverse DNS means that an hostname has both forward and reverse DNS entries that utilize the same IP address. Using this check, SmarterMail checks the rDNS and fDNS and if there is no A record, the check fails.

• Forward Confirm Mismatch Weight - Using this check, SmarterMail checks the rDNS and fDNS and if the IPs exist, but don't match, the check fails.

SpamAssassin-Based Pattern Matching

SmarterMail includes a proprietary pattern matching engine built upon the SpamAssassin technology as part of the default installation of the product. It includes a number of spam detection techniques, including DNS-based and fuzzy-checksum-based spam detection, Bayesian filtering and more.

• Enable Spool Filtering - See above for details.

• Enable Outbound SMTP Blocking - See above for details.

• Low Spam Weight - The weight that will be assigned if the pattern matching engine determines a low probability of spam.

• Medium Spam Weight - The weight that will be assigned if the pattern matching engine determines a medium probability of spam.

• High Spam Weight - The weight that will be assigned if the pattern matching engine determines a high probability of spam.

• Header Log Level - The amount of information the pattern matching engine inserts into the header of the message.

SPF (Sender Policy Framework)

SPF is a method of verifying that the sender of an email message went through the appropriate email server when sending. Therefore, as it's verifying the sending server, SPF is set up by the sending server's System Administrator or the domain owner as a DNS record. (More information can be found at DMARC Analyzer .) As more and more companies add SPF information to their domain DNS records, this check will prevent spoofing at an increasing rate.

• Enable Spool Filtering - See above for details.
• Enable Inbound SMTP Blocking - See above for details.
• Scan From header instead of Return Path - Enabling this means the check will use the From address for the SPF check as opposed to the message's RETURN-PATH, which is where NDRs (bounce messages) are sent. Many times spammers will spoof messages by changing the From address to make it appear like a message is coming from a legitimate person/organization even though the RETURN-PATH may be for the actual source of the message. While it is possible to spoof a message's RETURN-PATH, spoofing the From address is a much more common method used by spammers.
• Pass Weight - Indicates that the email was sent from the server specified by the SPF record (more likely good mail). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.
• Fail Weight - Indicates that the email was sent from a server prohibited by the SPF record (highly likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is very high.
• SoftFail Weight - Indicates that the email was sent by a server that is questionable in the SPF record. This should either be set to 0 or a low spam weight.
• Neutral Weight - Indicates that the SPF record makes no statement for or against the server that sent the email. Except in very special circumstances, leave this set to 0.
• PermError Weight - Indicates that there is a syntax error in the SPF record. Since SPF is relatively new, some domains have published improperly formatted SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.
• None Weight - Indicates that the domain has no published SPF record. Since SPF is relatively new, many legitimate domains do not have SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.

RBLs and URIBLs

RBL lists (also known as IP4R Lists) and URIBL lists are publicly accessible lists of known spammer IP addresses. These lists can be a very important part of spam protection. To attach a list, navigate to the appropriate tab and then click New . Dependent on the list you're adding, the following settings are available:

- Name - A friendly name for the list that will help you and your customers identify it.
- Description - This field allows you to store additional information about the list.
- Weight - The default weight for this spam check. If an email sender is listed with the spam list, this is the value that will be added to the message's total spam weight.
- Max Weight - The maximum weight that a single URIBL check can add to the message.
- Hostname - The hostname of the blacklist being added. For example, uribl.spameatingmonkey.net.
- Lookup Prefix - Many subscription-based RBLs and URIBLs require some type of authorization or login token to be added to the front of the RBL/URIBL. When using such a service, that token is entered here.
- Required Lookup Values - The expected value(s) returned from an RBL if the sender's IP is listed with the RBL provider. Note: Multiple lookup values may be entered, separated by a comma. These values are generally available from the RBL/URIBL provider in their set up documentation.
- Enable Spool Filtering - See above for details.
- Enable Inbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this RBL/URIBL is counted toward the weight threshold for the blocking of inbound emails.
- Enable for Outbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this RBL/URIBL is counted toward the weight threshold for the blocking of outbound emails.
- Enable bitmap checking - Enable this option if the RBL supports bitmapping. Bitmap checking can be used for RBL's and URIBL's that support this kind of spam check. For example, SURBL utilizes a multi-blacklist check. For more information and documentation on the appropriate usage, please visit www.surbl.org/lists .

IP Bypasses

IP Bypasses allow a System Administrator to prevent spam checks and greylisting on email delivered from specific IP addresses. Typically, this functionality is used to enter the IP address of an inbound gateway. In incoming messages, SmarterMail will analyze the .EML file and pull the most recent IP

Address from the header, which will usually be an organization's inbound gateway. Inputting that IP address on this page will allow SmarterMail to analyze the IP of the originating server rather than focusing on the gateway that SmarterMail received the message from. This is important because the majority of the time an organization's incoming gateway will not be listed on any RBL lists, but the originating server may be.

To access the IP Bypasses section, log in to SmarterMail as an Administrator and click on the Settings icon . Then click on Antispam in the navigation pane and click on the IP Bypasses tab . To add an IP Address or IP Range, click New .

- IP Addresses (single, range or CIDR block) - Enter the IP address or IP range that should be bypassed.
- Description - Enter a note for identifying the bypass.
- Bypass spam checks - Keep this option enabled in order to prevent spam checks on messages sent from the specified IPs. IMPORTANT NOTE: If SPF and DKIM spam checks are enabled, SmarterMail will run those checks on ALL emails, including those from trusted senders, whitelisted IP addresses and IP bypasses. 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.
- Bypass greylisting - Keep this option enabled in order to prevent greylisting on messages sent from the specified IPs.

Greylist Filters

SmarterMail's antispam options include greylisting, which is a very effective method of spam blocking that comes at a minimal price in terms of performance. 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. This temporary failure essentially tells the sending server to “Try again later.” Valid servers will retry the email a short time later, at which point SmarterMail accepts the message. 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.

In addition to the greylisting configuration on the Antispam | Options tab, Administrators can use Greylist Filters to prevent greylisting based on the sender's country or IP address. To access greylist filters, log in to SmarterMail as an Administrator and click on the Settings icon. Then click on Antispam in the navigation pane and click on the Greylist Filters tab. To add an IP address or country

code, click New . To edit an existing filter, simply click on it from the list. The following options will be available:

- Filter Type - Select the type of filter you would like to add: IP Address or Country Code.
- IP Address - If the filter type is set to IP Address, enter the IP address that should bypass greylisting / be greylisted.
- Country - If the filter type is set to Country Code, select a country code from the list. The greylisting exception / limitation will apply to all messages that are identified as coming from an IP address matching that country.
- Description - The friendly name or descriptor you want to give to the IPs. For example, Office365 or Yahoo!

Note: Some greylist filters are included by default and cannot be modified or removed. These default filters are indicated in the grid by having a checkmark in the Internal column.

Recommended Antispam and Antivirus Settings

SmarterMail comes equipped with several industry-standard antispam options that can block up to 97% of all spam from entering or leaving the server and help keep mail systems running smoothly. These built-in protections include SPF, DKIM, reverse DNS, greylisting, pre-configured settings for multiple popular and effective RBLs and URIBLs, and more. However, when considering your spam configuration, it’s important to remember that spam administration is not a "fire and forget" task. Using these built-in options requires constant tweaking to keep that level of effectiveness, and mail administrators will need to monitor incoming and outgoing spam as spammers frequently change their tactics. (Learn more about configuring the built-in antispam options below.)

In addition, SmarterMail comes equipped with industry-standard, and open source, antivirus protection using ClamAV. It also supports quarantining messages, and the ability to manage messages in the quarantine, an Events system for dealing with quarantined items and much more.

On top of the included options, SmarterMail supports third-party protections like:

- Cyren Premium Antispam
- Message Sniffer
- Declude
- Command-line antivirus
- Antispam appliances, such as Barracuda
- Many more

Paid add-ons like Message Sniffer, Cyren Premium Antispam, Cyren Zero Hour Antivirus and more can definitely come in handy. These third-party services act as additional spam and virus checks and

may be worthwhile investments as a multi-tiered solution is the best course of action when it comes to dealing with spam and antivirus. Often times, users are not satisfied with 97% spam protection out-of-the-box -- keeping in mind that, at this level of protection, for every 100 messages a user receives per day, only 3 of these could be spam. Both Message Sniffer and Cyren will catch a higher percentage of spam than the default options, and better yet, neither require consistent updating by a SmarterMail System Administrator - updates are handled by the service provider. Using one of these services, or ideally both together, is easily the most effective option in battling spam.

Regarding antivirus, When proper antivirus solutions are in place within SmarterMail -- using ClamAV plus something like Cyren Zero Hour -- using an antivirus solution at the network level is not necessary. In fact, antivirus solutions at the network level can cause numerous issues for system administrators and/or users. Therefore, it is NOT recommended. That's because antivirus solutions at the network level can't relay information to SmarterMail in a reliable way. If a network antivirus solution removes suspected virus attachments from an incoming email, the email will still be delivered to the recipient. However, while the message list will show that the email contains an attachment, no attachments will be available. Not only does this leave the user with no information regarding the missing attachments, it leaves them vulnerable to receiving, and perhaps responding to, email from malicious sources.

Below are some recommendations for the various spam settings SmarterMail has to offer. Please keep in mind that these are only suggestions. Administrators can, and should, keep an eye on these settings and adjust them as necessary to concoct a viable antispam solution for their end users.

SPAM CHECKS

In the Spam Checks, RBL Lists and URIBL Lists sections, you can enable individual spam checks for email spool filtering and inbound/outbound SMTP blocking. (Checks that are not available for inbound or outbound SMTP blocking are denoted with ‘N/A’.) Each spam check comes with unique spams weights, which can be adjusted as desired.

Determining the weight values of each spam check depends on how accurately you believe that check identifies spam messages. If you’re confident that it accurately identifies spam and has very few false positives, you would give its weight a higher value. If you are less confident in a spam check’s accuracy, assign it a lower value. By configuring your spam checks this way, those that you have less confidence in will not cause a message to be marked as spam on its own. However, if multiple checks that you have lower confidence in all consider a message to be spam, their combined weights would likely cause the messages to be marked as spam. Find our recommended spam weight values below:

Cyren Premium Antispam

(Leave disabled if you do not have the Cyren add-on)

- Confirmed Weight = 30
- Bulk Weight = 10
- Suspect Weight = 10
- Unknown Weight = 0
- None Weight = 0

Message Sniffer

(Leave disabled if you do not have the Message Sniffer add-on)

- Confirmed Weight = 30
- None Weight = 0

Remote SpamAssassin

SpamAssassin itself is a powerful, third party open source mail filter used to identify spam that can be easily used alongside, or in place of, SmarterMail's spam settings. It utilizes a wide array of tools to identify and report spam.

DKIM

(DKIM is the primary mechanism for signing messages which proves to the receiving user that the message was not altered during transit and was sent from the signing domain. Not all valid messages are signed however so no spam weight should be given for no signature.)

- Pass Weight = 0
- Fail Weight = 10
- None Weight = 5
- Max message size to sign (MB) = 100
- Max message size to verify (MB) = 100

SPF

- Pass weight = 0 (Sender's IP is valid for sender's domain)
- Fail weight = 10 (Sender's IP is not valid for sender's domain)
- Soft Fail weight = 5 (Sender's IP is questionable for sender's domain)
- Neutral weight = 0 (No strong statement can be made for or against sender's IP)
- PermError weight = 5 (The SPF record could not be processed.)
- None weight = 5 (No SPF record has been configured.)

Reverse DNS

- Reverse DNS Fail Weight = 10

- Forward Confirm Fail Weight = 10
- Forward Confirm Mismatch Weight = 5

RBL: SpamCop

- Weight = 10

RBL: SpamHaus CSS

- Weight = 10

RBL: SpamHaus PBL

- Weight = 10

RBL: SpamHaus SBL

- Weight = 10
- Additional RBLs can be added and weights applied.

FILTERING

On the Filtering card within the Options tab, you can adjust the global actions taken on emails that are considered to be spam, based on one of three probabilities determined by their spam weights: Low Probability, Medium Probability and High Probability. If a weight is equal to or higher than a certain category, then it is assigned that probability of being spam and the corresponding action is taken. The defaults for Filtering are as follows:

Low Probability of Spam weight = 10

- Default Action: None

Medium Probability of Spam weight = 20

- Default Action: Move to Junk Email folder

High Probability of Spam weight = 30

- Default Action: Move to Junk Email folder

Once you are comfortable with your antispam settings and have a better understanding of the spam messages that impact your domain, you may wish to adjust these settings. For example, you may consider changing the default action on the Low Probability to Move to Junk Email folder or the High Probability to Delete Message. (IMPORTANT NOTE: Email that is deleted via spam filtering CANNOT be recovered.)

SMTP BLOCKING

On the SMTP Blocking card within the Options tab, you can access the configuration options for 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 six 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 50, that means messages being received via SMTP will be rejected if they fail five or all six of the spam checks. (Because SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer incoming or outgoing SMTP blocking.)

Choosing which spam checks are used for Incoming/Outgoing SMTP Blocking is done on the Spam Checks, RBLs and URIBLs tabs. In order to actually enable the blocking feature, enable the corresponding weight threshold on the SMTP Blocking card. When an email arrives or is attempted to be sent that exceeds the threshold value, the email will be blocked and never delivered. Note: By default, the Incoming Weight Threshold is enabled and set to 50. This means that messages that have a spam weight of 50 will be blocked and deleted before they reach the spool. You can decrease that weight threshold once you have a better understanding of the spam that impacts your domain.

In addition to SMTP Blocking, this section also contains settings for the Outgoing Quarantine and Greylisting. If Outgoing Quarantine is enabled, SmarterMail will quarantine any outbound blocked messages for the specified time period. (If set to ‘None,’ messages are immediately deleted from the spool.) The Greylisting Threshold allows you to add extra options for what items get greylisted. If you prefer that messages with a high potential of spam are delayed, you can set the greylist weight threshold on the SMTP Blocking card. We recommend starting the threshold at 30 and decreasing to 20 if you’re confident in your spam checks.

GREYLISTING

On the Greylisting Options card within the Options tab, you can enable greylisting. Greylisting is a popular method of fighting spam as it temporarily rejects unrecognized incoming emails that are not sent by whitelisted or authenticated users, effectively saying, “Try again later.” Valid servers will retry the email a short time later, which would be permitted and delivered. Spammers, on the other hand, rarely retry on temporary failures, therefore reducing the amount of spam that customers receive. Find our recommended values below:

- Block Period = 3 minutes
- Pass Period = 360 minutes (6 hours)
- Record Expiration = 36 days

As part of the greylisting configuration, you can choose to greylist messages from everyone, greylist messages from the specified countries / IP addresses, or greylist messages from everyone except the specified countries / IP addresses. If the greylisting 'Applies To' is set to 'Only specified countries / IP addresses' or 'Everyone except specified countries / IP addresses', you use the Greylist Filters tab to add those exceptions / limitations.

Summary

When it comes to antispam and antivirus administration, it’s important to keep in mind that spammers change their tactics often and each installation/setup is unique. What one person may consider the ideal spam configuration, others may find too restrictive. What works for one mail server, may not work for all. Discussing your configuration with other server administrators is a great way to get ideas flowing on what will work best for you. If you’ve still got more questions or want additional ideas on how to configure SmarterMail’s antispam, please consider posting in the Community or reviewing one of the many threads discussing antispam topics.