Help Documentation

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.