Untitled Page

Help Documentation

Antispam Administration

SmarterMail comes equipped with a number of antispam features and functions that allow you to be as aggressive as you want when combatting spam. Initial antispam settings were configured during installation, but these settings can be modified at any time. Without having to add any third-party measures, SmarterMail's antispam features can rid mail servers of up to 95% of all spam just using the standard configuration when it's installed.

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 settings in the Filtering tab 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 system administrators to keep spam from entering the mail server. SmarterMail helps protect mail users from incoming spam but also includes the added benefit of keeping mail servers from actually sending spam, thereby helping to protect the mail servers from being blacklisted.

To view the antispam settings for your server, click the security icon and then click Antispam Administration in the navigation pane. The antispam settings will load in the content pane and the following tabs will be available:

Spam Checks

Use this tab to select the spam options that you want to enable for filtering (a point-based weighting system for filtering spam) and for blocking at the SMTP level. Weights can also be edited for the various checks from this tab. Note: Only enabled spam checks are used when calculating spam weight. To enable or disable a check, select the appropriate spam check by checking the box next to it and click Save .

The following columns are available for each spam check:

- Spam Check - The name of the spam check available.
- Weight - The weight range available for the spam check.
- Enable for Filtering - When checked, 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 created for a domain.
- Enable for Incoming SMTP blocking - Checking this box enables the spam check for SMTP

blocking of incoming emails. If N/A is listed, then that particular spam check relies on content filtering and does not offer SMTP blocking. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking.
• Enable for Outgoing SMTP blocking - Checking this box enables the spam check for SMTP blocking of outgoing emails. If N/A is listed, then that particular spam check relies on content filtering and does not offer SMTP blocking. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking.

The following types of spam checks are available by default. In most cases, selecting the desired spam check and clicking Edit will allow you to set any properties associated with the check.

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 .

SmarterMail's 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.

• 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.

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:

• 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 - 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 SpamAssasasin score for an email.
• Failures Before Disable - The number of times a remote SpamAssassin server can fail before it is disabled.
• Disable Time - 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

Cyren (formerly Commtouch) 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 .

Custom Rules

Email can be assigned spam weights based on the header, body text or raw content of a message. For example, the system 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 body rules, 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. Note: If you select Header you will need to supply header details separately from the Rule Text .
• Rule Type - The type of rule you use to evaluate the text for a match. Rule types are contains, wildcard or regular expression.
• Weight - The amount to add to the email message's spam weight.
• Rule Text - The text that triggers the custom body rule.

Bayesian Filtering

Bayesian filtering uses statistical analysis to identify whether or not an email appears to be spam. Bayesian filtering "learns" from previous messages that are marked as spam to progressively improve performance. Tying it together with blacklists and SPF allows you to be quite sure that email is or is not spam.

- Weight - The default weight for this spam check. If an email has a high probability of being spam based on its content, this is the value that will be added to the message's total spam weight.
- Max memory to allocate for filtering - Bayesian filtering can be memory intensive. As a result, SmarterMail allows you to configure the maximum resources that will be dedicated to Bayesian filtering. In general, the more memory you reserve for Bayesian filtering, the more accurate the results will be.
- Messages required for filter update - Once this number of messages have been processed as known-good or known-spam email, SmarterMail will reanalyze the filters to help your system protect against new spam threats. In this way, Bayesian filtering can become more tailored to handle the mail of the domains on the server.

DomainKeys and DKIM

DomainKeys is an email authentication system designed to verify the DNS domain of an email sender and the message integrity. The DomainKeys specification has adopted aspects of Identified Internet Mail to create an enhanced protocol called DomainKeys Identified Mail (DKIM). While a possible source for determining whether an email is spam or not, neither is widely adopted so any weights assigned for failing these checks should be minimal.

- 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 probablility that the email was spoofed is very high.
- None Weight - Indicates that there ws not valide DomainKey signature found to validate the sender and message integrity. Except in very special circumstances, leave this set to 0.
- Max message size to sign - The maximum outgoing message size you want the mail server to sign. By default this is set to 0, meaning all outgoing messages are signed.
- Max message size to verify - The maximum incoming message size you want the mail server to verify.
- Max key size allowed - Select the level of security you want used to sign each message.

Default is set to 1024 bits. Setting this value higher may increase the CPU load on your mail server.

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. As more and more companies add SPF information to their domain DNS records, this check will prevent spoofing at an increasing rate.

- 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 probablility 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.

Reverse DNS (Domain Name Sever)

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

- 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.

RBL Lists (Real-Time Blacklists)

RBL lists (also known as IP4R Lists) are publicly accessible lists of known spammer IP addresses. These lists can be a very important part of spam protection. To attach to a list, click Add List in the actions toolbar.

- 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.
• Hostname - The hostname of the RBL.
• Required Lookup Value(s) - 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.
• Enable bitmap checking - Select this checkbox if the RBL supports bitmapping. Bitmap checking can be used for RBL□sand URIBL□sthat 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 .

Filtering

Emails are filtered into one of three categories based on their total weight: 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. Use the Default Action option to define the weight thresholds and the default actions at each level. Note: Users can override these settings if you permit them to.

• Weight Threshold - The email is sorted into probability levels based on the weight threshold values.
• Default Action - The action to take when a message ends up with this probability.
• Text to Add - This is the text that will be displayed when a message reaches a particular level of spam.

SMTP Blocking

This tab allows you to set up extra spam checks that block emails at delivery if a certain amount of spam checks fail. Use the Enabled checkbox to enable a particular SMTP block.

• Incoming Weight Threshold - Enable this and an incoming email must score this value or higher in order to be blocked. The score is established by the settings on the Spam Checks tab. (Default is 30)
• Greylist Weight Threshold - Enable this and an incoming email must score this value or higher to be greylisted. (Default is 30)
• Outgoing Weight Threshold - Enable this and an outgoing email must score this value or higher in order to be blocked. The score is established by the settings on the Spam Checks tab. (Default is 30)
• Outgoing Quarantine - The amount of time to quarantine blocked SMTP messages.

Options

This tab contains options relating to the processing of spam and the ability for individual domains to override system-level settings.

• Auto Responders - Allows you to restrict what types of automated responses are permitted for the system. Certain anti-spam organizations are starting to block those servers that auto-respond to spam traps. To reduce the possibility of this occurring, set the auto-respond option to be as restrictive as your clients will permit.
• Content Filter Bouncing - As with auto-responses, certain anti-spam organizations also blacklist those servers that send bounce messages back to spam trap accounts. SmarterTools recommends setting this option to be as restrictive as your clients will allow.
• Max message size to content scan - The maximum message size for which content-based spam checks will run. Content-based spam checks include the SpamAssassin-based Pattern Matching Engine, remote Spam Assassin, Cyren Premium Antispam, custom rules and Bayesian filtering. Note: Increasing this number will also increase the mail server's memory usage.
• Enable domains to override filter weights and actions - Many domain administrators have their own opinions on what spam checks work best for their domain. Enable this to allow them to override the spam options if they wish.
• Enable bounces for outgoing SMTP blocking - Enable this to give a user a notification when a mail message has not been sent due to spam.
• Enable spool proc folder - Enable this to have SmarterMail place messages into this folder to be analyzed in the background. While the messages are in the Spool Proc folder, .hdr can manipulate elements of the message, such as edit, write, and add headers. Once the scan has been completed, the message will be placed back into the spool and handled by SmarterMail from that point on.
• Disable spam filtering on SMTP whitelisted IP addresses - Disables antispam processing and zeroes the spam weight on whitlisted IPs.
• Enable catch-all accounts to send auto-responders 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
.

Bypass Gateways

This tab gives administrators the ability to enter an IP Address or an IP Range of an incoming gateway. SmarterMail will analyze the .EML file and pull the most recent IP Address from the header which will usually be an organizations incoming gateway. By 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 organizations incoming gateway will not be listed on any RBL lists, but the originating server may be.

To add an IP Address or IP Range, click the Add IP icon from the Actions toolbar.