Domain Spam Filtering

Help Documentation

Domain Spam Filtering

SmarterMail includes many advanced Anti-Spam measures that will help protect your users from unwanted email. The system administrator has probably already set up some default spam options which you may accept or override as you feel is best.

To get started, click the Settings button on the main toolbar, and then select Spam Filtering under the Filtering folder in the Domain Settings tree view.

Options

- Use default spam settings - Choose this option to accept the default spam options provided by your system administrator. The settings will be displayed for your reference.
- Override spam settings for this domain - Select this option to customize the way spam is handled. Spam check weights and actions will become overridable by end users. More information about the types of actions allowed can be found below.

Spam check weights

Each type of spam check has an associated weight that factors into the spam probability of a message. When an email comes in, all of the checks listed are run, and for each check that the message fails, the weight is added to the overall score of the email. The thresholds for each spam probability are examined, and the email is placed into the appropriate category.

SPF (Sender Policy Framework) Filtering Options

- Pass - 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 - 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 - 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 - 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 - Indicates that the email sender does not publish an SPF record or there is a syntax error in the 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 popular on the internet.

SpamAssassin

The SpamAssassin weights can only be changed at the system administrator level. If you would like to change these weights, we recommend getting together with your system administrator and working out an agreeable anti-spam strategy.

What is SpamAssassin and how does it work? SpamAssassin is a powerful, free mail filter used to identify spam. It utilizes a wide array of tools to identify and report spam. These include:

- Header and text analysis
- Bayesian filtering
- DNS block lists
- Collaborative filtering databases

When should you use SpamAssassin? SpamAssassin in conjunction with Greylisting is as good as any available product on the market when you care about limiting spam from getting to your mailbox.

For more information on SpamAssassin, see SmarterTools deployment guides.

Actions

When you choose to override the spam options set by your system administrator, you get to choose the actions that are taken when email comes in that has a low, medium, or high priority of being spam. For each spam level, choose the action you wish to have taken. If you chose to add text to the subject line of messages, enter in the text in the box below the action drop down.

Trusted Senders - Email addresses (ex: joe@example.com) or domain names (ex: example.com) can be added to the domain list of trusted senders. When email comes in from a trusted sender, all spam filtering for that email is bypassed. Enter one email address or domain name per line.

When all settings are entered, click on the Save icon from the actions toolbar.