# Security

Help Documentation

# Security

## Antivirus Administration

SmarterMail's default installation includes, at no additional cost, effective and self-updating antivirus protection with ClamAV. In addition, SmarterMail can support additional third-party solutions that include a quarantine directory as well as support for command-line antivirus solutions. SmarterMail has the ability to check the quarantine directory and respond to users that attempted to send an email containing a virus.

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

### Options

- Virus Quarantine - Allows you to specify the amount of time you want to quarantine any detected viruses.
- Enable ClamAV - Select this checkbox to enable ClamAV.
- Enable real-time AV - Select this checkbox to enable virus checking in real-time.
- Enable command-line AV - Select this checkbox to enable a command-line virus scanner.
- Enable Cyren zero-hour antivirus - Select this checkbox to enable the Cyren Zero-hour Antivirus add-on.

### ClamAV

Clam AntiVirus is a third-party open source antivirus toolkit, designed especially for scanning email on mail gateways. ClamAV is included at no additional cost in the default installation of SmarterMail. For more information on ClamAV, visit: www.clamav.com

- IP Address - The IP address of the ClamAV server to use.
- Port - The port that the ClamAV server is listening on.
- Remote Server - Select this checkbox if the server is a remote server.
- Timeout - The maximum number of seconds SmarterMail should wait for ClamAV to respond before moving on to the next message. By default, the timeout is 10 seconds.
- Failures Before Disable - The maximum number of ClamAV timeouts allowed before it is disabled. By default, ClamAv is limited to 5 failures.
- Virus Definitions - The date and time the virus definitions were last updated. The definitions are updated whenever the service starts and every 6 hours thereafter.

### Real-Time AV

- Quarantine Directory - The full path to the quarantine directory for the server. This is where emails that are allegedly infected with a virus are temporarily held.
- Virus Action - The action taken when an email contains a virus. The available actions are:

- Delete - Deletes any files attached to the message from the spool directory. This does not take any action on the quarantine directory.
- Inform Sender - Informs the "From" address that a message was received by the server, and because a virus was found in the message, it did not reach the intended recipient. Note: With some of the more recent viruses, this action becomes less useful, as many viruses now spoof the "From" email address.

### Command-line AV

- Command Line - The command that you want to execute. %FILEPATH will be replaced with the path to the file to be scanned.

### Cyren (formerly Commtouch) Zero-hour Antivirus

The Cyren Zero-hour Antivirus add-on uses Recurrent Pattern Detection technology to identify viruses based on their unique distribution patterns and provides a complementary shield to conventional AV technology, protecting in the earliest moments of malware outbreaks and continuing protection as each new variant emerges.

Cyren evaluates each message and determines the probability that the message contains a virus. System administrators can choose the default action taken on a message when Cyren determines the it has a medium, high, or definite probability of containing a virus. For more information, or to purchase this add-on, visit the SmarterTools website .

## 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.
- Avg. Time - The average time, in milliseconds, that the spam check takes to process.
- 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.

## 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.

## 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.

## 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 .

## 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 .

## 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 probability that the email was spoofed is very high.
- None Weight - Indicates that there was not a valid 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.

## RBL Lists (Real-Time Blacklists)

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 click either Add RBL or Add URIBL in the content pane toolbar. 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 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□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 .

## 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 SpamAssasassin 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

## Reverse DNS (Domain Name Server)

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.

## 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.

## 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 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.

## 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 SpamAssassin, Cyren Premium Antispam, custom rules and Bayesian filtering. Note: Increasing this number will also increase the mail server's memory usage.
• Allow 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 whitelisted 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.

# Greylisting

## What is Greylisting and how does it work?

Greylisting is a popular tool in the fight against spam. It will temporarily block incoming mail from a sender and then returns the mail to the sender's mail server with a message saying effectively, "try again later." The sending server must then retry sending the mail after the Block Period but before the Pass Period (see below for definitions of these values).

Greylisting is effective because spammers will not usually bother to attempt a second delivery, but legitimate e-mail servers will.

## 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.

## How do I set up Greylisting?

Note: You must be a system administrator to change greylisting settings.

In order to set up Greylisting, click the security icon and click Greylisting in the navigation pane. The greylisting settings will load in the content pane and the following tabs will be available:

### Options

Use this tab to specify the following settings:

- 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).
- Apply To - Select who greylisting applies to.
- Enable greylisting - Select this option to enable greylisting.
- Enable users to override greylisting - Select this option to allow users to selectively turn off greylisting (useful if you have an account that receives time sensitive mail).

• Greylist if the country for the IP address is unknown - Select this option to greylist messages when the country cannot be identified for the IP address. System administrators should note that the following cases are exempt from greylisting:

• Whitelisted IPs for SMTP or Greylisting
• Anyone who authenticates (includes SMTP Auth Bypass list)
• Trusted senders
• Anyone who has already sent you an email. Note: This list generates only after greylisting has been enabled.
• Any IP in the greylistBypass.xml file

**Filters**

If you set the grelisting "Apply To" setting to "Everyone except specified coutries / IP addresses" then you are able to add filters based on the countries or IP addresses you want to exclude from being greylisted.

## Disadvantages of Greylisting

The biggest disadvantage of Greylisting is the delay of legitimate e-mail 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 e-mail servers will not attempt to re-deliver email or the re-delivery window is too short. Whitelisting can help resolve this.

# Blacklist / Whitelist

System administrators can control which IP addresses are blacklisted (not allowed) from mail services on this machine, or whitelisted (trusted) to access the mail services on this machine.

To manage the blacklist, click the security icon and click Blacklist in the navigation pane.

To manage the whitelist, click the security icon and click Whitelist in the navigation pane.

Note: Whitelisted IP addresses are not subject to relay restrictions which you may have imposed. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your server.

## Adding/Editing an Entry

To edit a blacklist or whitelist, click Edit in the content pane toolbar. To create a new entry in the blacklist or whitelist, click New in the content pane toolbar. The blacklist or whitelist settings will load in a popup window and the following options will be available:

• IP Address - Enter a single IP address in dotted quad notation (X.X.X.X) in this box if you want to add only a single IP (ex: 192.168.1.26).
• IP Range - Enter a range of IP addresses in the two boxes, and all IP addresses that are contained in the range will be added (ex: 192.168.1.1 - 192.168.1.255).
• Blacklist or Whitelist SMTP / POP / IMAP / XMPP / Disable greylisting - Check the boxes for the protocols you wish to include in the blacklist or whitelist entry. The Disable greylisting checkbox is only available for whitelisting IPs, and if checked, the whitelisted IP will not be greylisted.

NOTE: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authenication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the administrator may want to review the settings prior to adding the IP range.

# Blacklist / Whitelist

System administrators can control which IP addresses are blacklisted (not allowed) from mail services on this machine, or whitelisted (trusted) to access the mail services on this machine.

To manage the blacklist, click the security icon and click Blacklist in the navigation pane.

To manage the whitelist, click the security icon and click Whitelist in the navigation pane.

Note: Whitelisted IP addresses are not subject to relay restrictions which you may have imposed. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your server.

## Adding/Editing an Entry

To edit a blacklist or whitelist, click Edit in the content pane toolbar. To create a new entry in the blacklist or whitelist, click New in the content pane toolbar. The blacklist or whitelist settings will load in a popup window and the following options will be available:

• IP Address - Enter a single IP address in dotted quad notation (X.X.X.X) in this box if you want to add only a single IP (ex: 192.168.1.26).
• IP Range - Enter a range of IP addresses in the two boxes, and all IP addresses that are contained in the range will be added (ex: 192.168.1.1 - 192.168.1.255).
• Blacklist or Whitelist SMTP / POP / IMAP / XMPP / Disable greylisting - Check the boxes for the protocols you wish to include in the blacklist or whitelist entry. The Disable greylisting

checkbox is only available for whitelisting IPs, and if checked, the whitelisted IP will not be greylisted.

NOTE: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authenication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the administrator may want to review the settings prior to adding the IP range.

## SMTP Authentication Bypass

SMTP Authentication is a security measure that can be very beneficial in the fight against spam and unauthorized email as it forces the sender to authenticate their username and password before an email is sent through the mail server.

Unfortunately, some applications do not have support for SMTP authentication when sending mail. Most often, these are web sites that have automated mail sending mechanisms. The solution is to add the IP addresses of these servers/sites to SmarterMail's SMTP Authentication Bypass. Any IP address entered into this page will not be asked to provide an SMTP Authentication login. In this list you can see all IP addresses that are bypassing SMTP Authentication.

To get started, click the security icon and click SMTP Authentication Bypass in the navigation pane. A list of bypasses IP addresses will load in the content pane and the following options will be available in the content pane toolbar:

• New - Adds a new IP address or IP Address Range to bypass.
• Edit - Edits the selected IP address.
• Delete - Permanently removes the IP address from the SMTP authentication bypass list.

## Trusted Senders

This section allows system administrators to exempt specific email addresses (such as jsmith@example.com) or domains (such as example.com) from SmarterMail's spam filtering. This can prevent mail from friends, business associates and mailing lists from being blocked and lets the system know that these messages come from a trusted source.

To view the trusted senders list for the server, click the security icon and click Trusted Senders in the navigation pane. A list of trusted senders will load in the content pane and the following options will be available in the content pane toolbar:

• New - Creates a new trusted sender.

- Edit - Edits an existing trusted sender.
- Delete - Permanently deletes the selected trusted sender(s).

## Server Blacklist Checker

Knowing when a mail server is listed by one of the realtime black lists (RBL) SmarterMail incorporates into its various spam checks used to mean system administrators would have to log in to various websites and perform manual checks of their domains and/or IP addresses. However, with the Server Blacklist Check, these checks are performed automatically for all IP addresses added to a SmarterMail server so system administrators know if a server is actively blacklisted. Once a day, SmarterMail checks all of the RBLs available by default for any server IP addresses (besides localhost), regardless of whether the RBL is actively being used as a spam check. If the RBLs come back showing an IP as blacklisted, it changes that IPs blacklist status from False to True on the Server Blacklist page. System administrators are advised to set up Blacklist Status Changed system events that will immediately notify them if a server becomes listed by a RBL.

To access the Server Blacklist Check, click the Security icon and then click Server Blacklist Check . A list of IP addresses on the server will load in the content pane and the following columns will appear in the content pane:

- IP Address - The IP address used for a domain, or for several domains, on that mail server.
- Spam Check - THe name of the RBL or URIBL that is being used.
- Blocked - If the IP is blocked by the specific spam check, this column will say True . If the IP address is NOT blocked, this will say Fales .
- Change - THe last date and time the IP was checked against the specific list.

# Advanced Settings

## Abuse Detection

SmarterMail has several methods of preventing abuse and denial of service (DoS) attacks. The ones that can be configured are explained below. Any number of detection methods can be added.

To view the configurable abuse detection settings, click the security icon . Then expand the Advanced Settings folder and click Abuse Detection in the navigation pane. A list of abuse detection rules will load in the content pane and the following options will be available in the content pane toolbar:

- New - Creates a new abuse detection rule.
- Edit - Edits the selected abuse detection rule.
- Delete - Permanently deletes the selected abuse detection rule(s).

• Wizard - Displays the Abuse Detection section of the SmarterMail setup wizard, which offers the following preset security options:

• Do not change abuse detection settings
• Relaxed abuse detection (Includes: DoS, SMTP Brute Force)
• Strict abuse detection (Includes: DoS, SMTP Brute Force, Email Harvesting, Internal Spammer Notifications, Bounces Indicate Spammer)

To create a new abuse detection rule, click New in the content pane toolbar. The abuse detection settings will load in the content pane and the following options will be available:

Denial of Service (DoS) - Too many connections from a single IP address can indicate a Denial of Service (DoS) attack. Enable this option to block IPs that are connecting too often to the server. It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists or make many connections if you enable this option.

• Service - Select the service that will be monitored for this type of attack (SMTP/IMAP/POP/XMPP/LDAP).
• Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many connections in this period of time, and a block will be initiated.
• Connections Before Block - The number of connections before a block is placed. It is common for several connections to be open at once from an IP address. Set this to a relatively high value so that you can catch DoS attacks while not impacting legitimate customers.
• Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
• Description - A friendly name or brief description of the rule.

Bad SMTP Sessions (Harvesting) - A bad session is any connection that ends without successfully sending a message. Many bad sessions usually indicate spamming or email harvesting. Leaving all of these options set to 0 (zero) will disable this type of abuse detection. Note: It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists if you enable this option.

• Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many bad sessions in this period of time, and a block will be initiated.
• Bad Sessions Before Block - The number of bad sessions before a block is placed. A few bad sessions happen once in a while, for instance when a person sends an email to an email account that does not exist. It is not these people that you are targeting, but rather those that are attempting to compromise or harass your customers.
• Time to Block - The number of minutes that a block will be placed once an IP address hits the

threshold.
• Description - A friendly name or brief description of the rule.

Internal Spammer - Enabling this rule in SmarterMail will block or quarantine an account from sending mail, as well as alert an administrator, whenever multiple emails from a single sender are received on the server during a specified time frame.

• Action - Choose whether to send a notification email only, block messages from the sender or quarantine messages from the sender.
• Time Frame - The period of time in the past that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.
• Messages Before Notify - After this many messages are received within the time period specified, the email notification is sent and the Action chosen is performed.
• Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
• Email to Notify - The email address of the administrator account to which the notification will be sent.
• Description - A friendly name or brief description of the rule.

Password Brute Force by Protocol - A common ploy by spammers and hackers is attempting to guess passwords for users. Many times this entails continual log in attempts to an account using different passwords, each a bit different than the one before it. This thereby brute forcing the password.

• Service - Select the service that will be monitored for this type of attack (SMTP/IMAP/POP/XMPP/LDAP).
• Time Frame - The period of time in the past that is examined to determine if an login attempt is a brute force attempt. Too many connections in this period of time, and a block will be initiated.
• Connections Before Block - The number of failed login attempts before the IP is blocked.
• Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
• Description - A friendly name or brief description of the rule.

Bounces Indicate Spammer - Enabling this rule in SmarterMail will block or quarantine an account from sending out mail, as well as alert an administrator, after receiving a certain number of bounce messages in the specified time frame.

• Action - Choose whether to send a notification email only, block messages from the sender or quarantine messages from the sender.

• Time Frame - The period of time in the past that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.
• Bounce Threshold - After this many bounce messages are received within the time period specified, the email notification is sent and the Action chosen is performed.
• Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
• Email to Notify - The email address of the administrator account to which the notification will be sent.
• Description - A friendly name or brief description of the rule.

## Password Requirements

To ensure the security of the mail server and its mailboxes, system administrators can specify minimum requirements for user passwords. To access the password requirements settings, click the security icon . Then expand the Advanced Settings folder and click Password Requirements in the navigation pane. The password requirement settings will load in the content pane and the following options will be available:

• Minimum Password Length - The minimum number of characters the password must have.
• Password Expiration - The number of months that a password is valid. After the specified time, a user□s outgoing SMTP will be disabled and a password change will be forced upon Web interface login. Check the Enabled box to enable this setting.
• Auto-block Grace Period - The number of days a user can wait to update their account password before outgoing SMTP is disabled due to password policy violation. Note: This setting only applies if the "Disable outgoing SMTP when auto-block grace period ends" setting is checked.
• User Notification Timing - The interval(s) used to notify users of when their password will expire or when their auto-block grace period will end and, subsequently, their outgoing SMTP will be disabled. The default values are 28, 14, 7, 3, 2, 1 days. This means SmarterMail will send out warning messages to the user to change their password 28 days, 14 days, 7 days, 3 days, 2 days and 1 day before their password officially expires or the grace period ends if their password violates the requirements. Note: SmarterMail will send one, single notification for all missed intervals. For example, imagine "Auto-block Grace Period" is set for 30 days and the "User Notification Timing" is set at 60, 45, 25, 10, 2, 1. When a user is in violation, SmarterMail will send a single notification for the 60 and 45 day intervals then continue as normal at the 25 day interval.
• Require a number in the password - Select this option to force users to include a number in the

password.

• Require a capital letter in the password - Select this option to force users to include a capital letter in the password.

• Require a lower case letter in the password - Select this option to force users to include a lowercase letter in the password.

• Require a symbol in the password - Select this option to force users to include a symbol in the password.

• Require password does not match username - Select this option to ensure that the username and password do not match.

• Disable password strength for existing passwords - Select this option to allow changes to the password requirements to only affect new users or new passwords.

• Enable password retrieval - Select this option to allow users to reset their password if they forget it. Note: In order for users to utilize password retrieval, they must have a backup email address configured in their account settings.

• Prevent commonly used passwords - Select this option to prevent users from configuring passwords that are included in the list of commonly used, insecure passwords. Note: The default location of the list of commonly used passwords is: C:\Program Files (x86)\SmarterTools\SmarterMail\Service\Common_Passwords.xml.

• Disable outgoing SMTP when auto-block grace period ends - Select this option to disable outgoing SMTP after the auto-block grace period ends when a user□spassword does not meet the password requirements.

# SMTP Blocking

The SMTP Blocked Sender list is an effective method for temporarily canceling a domain or indiviual user's ability to send email on the server. For example, if a particular account is sending an abnormal amount of email, you can add their address to Blocked Senders and they will be unable to send email until you remove them from the Blocked Senders list. Users and/or domains can be left on the list for whatever time you deem appropriate, and can be an effective stop-gap versus actually deleting the user and/or domain from the server.

To view blocked senders, click on the security icon . Then expand the Advanced Settings folder and click SMTP Blocked Senders in the navigation pane. A list of blocked senders will load in the content pane and the following options will be available from the content pane toolbar:

• New - Adds a new SMTP blocked sender.

• Edit - Edits the selected blocked sender.

• Delete - Permanently removes the email or domain from the blocked senders list.

## Adding a New SMTP Blocking Rule

To add a new SMTP blocking rule, simply click the New button. You are presented with the following options:

- Block Type - Options are set as either Email Address or EHLO Domain.

- Email Address - The complete email address to set up for the block.
- EHLO Domain - This is the return value given when SmarterMail sends the EHLO or HELO command. A standard EHLO domain is the fully qualified domain name set up for the mail server you're wanting to block. (E.g., mail.smartertools.com). However, it IS possible that it will be something diffrent based on whether the command is sent by the SmarterMail Web interface or an email client. For example, it may be the local IP address of the sending machine. Therefore, there is no well-established rule for what should be entered until some testing is done by the system administrator.
- Blocked Address - Enter either the full email address or the EHLO Domain, based on the Block Type that was selected.
- Direction - Specify whether to block either incoming SMTP, outgoing SMTP or both.
- Description - Friendly description for the block.

NOTE: SMTP blocking does NOT occur immediately when the EHLO command is given. Instead, a "soft" block is used and SmarterMail will fail any authentication attempts or RCPT TO commands. This is because if the failure occurs right after the EHLO commaned, any person attempting to spam from a mail server could figure out what the problem is and change the domain given with the command on each send. A "soft" failure should, instead, make the spammer believe he is using an incorrect password.

# SpamAssassin

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 blocklists
- Collaborative filtering databases

To view a list of servers currently set up to run SpamAssassin checks, click the security icon / Then expand the Advanced Settings folder and click SpamAssassin Servers . A list of SpamAssassin servers will load in the content pane and the following columns will be available:

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

In general, the following options will be available in the content pane toolbar:

- New - Adds a new SpamAssassin server. Administrators will need to provide the server's IP address and the port on which SpamAssassin should listen.
- Edit - Modifies the SpamAssassin server settings.
- Delete - Permanently deletes the SpamAssassin server.

For more information on SpamAssassin, please visit http://spamassassin.apache.org .

# Reserved Domain Names

System administrators can prevent certain domains names from being added to SmarterMail. For example, domains that are already used for free email services, like gmail.com or yahoo.com, are ideal additions to the reserve list as allowing administrators to add such domains to SmarterMail could affect message delivery. Similarly, domains that are traditionally reserved for testing and documentation, such as test.com or example.com are also ideal candidates for the reserve list.

To view a list of reserved domains, click the security icon and expand the Advanced Settings folder in the navigation pane. Then click Reserved Domain Names . A list of reserved domains will load in the content pane and the following options will be available from the content pane toolbar:

- New - Adds a domain to the reserve list.
- Edit - Edits the selected domain.
- Delete - Deletes the selected domain(s) from the reserve list.