Advanced Settings

Help Documentation

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□soutgoing 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 differnt 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 .