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 get started, click the Security button on the main toolbar, then select Abuse Detection from the Security folder tree view.

Once you arrive on the Abuse Detection screen, you will see three icons on the actions toolbar— New , Edit , and Delete .

When clicking the New icon on the actions toolbar you will have these options:

Denial of Service (DoS) Prevention - 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 Type - Select the service that will be monitored for this type of attack (POP/SMTP/IMAP/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 hits the threshold.

Bad SMTP Sessions (Email 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. 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 targetting, 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 hits the threshold.

Internal Spammer Detection and Notification - Enabling this feature in SmarterMail will alert an administrator whenever a multiple emails are received on the server of the same size.

• Time Frame - The period of time in the past that is examined to determine if an alert should be sent. Too many duplicate emails in this period of time, and an alert will be sent.
• Messages Before Notify - After this many duplicate messages are received within the time period specified, the email notification is sent.
• Email to Notify - The administrator account to which the notification will be sent.

Edit Icon - Editing and item can be done three ways:

• Select the item and then choose the Edit icon from the actions toolbar, or
• Right-click the item and choose Edit from the drop down list, or
• Double-click the item you would like to edit

Delete Icon - Deleting an item can be done two ways:

• Select the item and click the Delete icon from the actions toolbar, or
• Right-click the time and select Delete from the drop down list

Password Requirements

Minimum Password Length - This will allow System Administrators to designate the minimum numbers of characters a password requires.

Password Strength Requirements - The System Administrator is able to set the requirements for passwords and, as a result, all users must adhere to those standards. The password options available to the System Administrator are: Number, Capital Letter, Lower Case Letter, Symbol, Not User Name.

SMTP Blocked Senders

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 get started, click on the Security button on the main toolbar, then select SMTP Blocked Senders from the Security folder tree view.

Blocked Senders - Enter the email addresses or domain names you want to block, one per line. The asterisk (*) wildcard symbol is permitted in the list.

SSL

This page is available in Enterprise Edition only

SmarterMail allows System Administrators to add Secure Socket Layer (SSL) and Transport Layer Security (TLS) rules.

To get started click the Security button on the main toolbar, then select SSL from the Security folder tree view.

When adding a new rule there are several fields that need to be addressed. These fields are:

IP Address - This is the IP address where SmarterMail will listen.

SMTP, POP, IMAP - Determines on which port SmarterMail will listen for the respective protocol.

Type - Sets the type of rule you would like to add, SSL or TLS. SSL always assumes the connnection will be secure, and therefore, sends the encryption immediately. TSL connects normally, and then looks to see if the connection is secure before sending the encryption.

Certificate Path - The path to the certificate file on the server. Typically, named a *.cer file.

- The certificate you are using must be added to the Certificates Microsoft Management Console within your Windows operating system. In addition, you must associate the Private Key with this same certificate.

Please Note: When removing a SSL rule, the System Administrator will need to perform a service restart.

Edit Icon - Editing and item can be done three ways:

- Select the item and then choose the Edit icon from the actions toolbar, or
- Right-click the item and choose Edit from the drop down list, or
- Double-click the item you would like to edit

Delete Icon - Deleting an item can be done two ways:

- Select the item and click the Delete icon from the actions toolbar, or
- Right-click the time and select Delete from the drop down list

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

Adding a SpamAssassin Server

To add a SpamAssassin server go to the SpamAssassin page in the Security menu. Here you will be presented with a list of servers currently set up to run SpamAssassin checks. To edit one of these servers simply click on it in the list, see below for a complete list of options. To add a new server simply click the Add SpamAssassin Server button, see below for a complete list of options. When you are finished adding the server click on the save button to add it to the list. For more information on downloading and installing SpamAssassin on your server please check out their website .

Add SpamAssassin Server Form

- Name - The name you wish to call this server
- IP Address - The IP address of the server running SpamAssassin
- Port - The SpamAssassin port on the server running SpamAssassin (783 by default)
- Multithreaded - If the server you have installed SpamAssassin on is a Linux machine it is recommended that you check this. If it is running on a Windows machine you cannot have this selected.