Zen Software Ltd
Web: http://www.zensoftware.co.uk
Email: sales@zensoftware.co.uk
Tel: 0161 660 5738

# MDaemon configuration recommendations for dealing with spam related issues

## Introduction

Without a doubt, our most common support queries these days fall into one of the following groups:-

1. Why did this email get flagged as spam?
2. Why didn't this email get flagged as spam?
3. Is there anything we can do to reduce the amount of spam we receive?

MDaemon has an amazing, probably unsurpassed, arsenal of anti-spam tools that have evolved over the years, however it's fair to say that some of these tools are fairly 'technical' and if mis-managed can often result in more problems than they solve.

While a large proportion of issues to do with spam filtering are as a result of MDaemon's settings being mis-configured, the way email arrives at MDaemon is also a major contributing factor as is the SecurityPlus plug-in for MDaemon not being installed.

This document is designed to provide some very specific guidelines on how your MDaemon server should be configured to reduce spam and false positives to an absolute minimum.

**If you've followed the recommendations in this document, your organisation should not be suffering from any significant issues relating to spam. If you are still, then please contact us!**


Registered office: Parkway 5 (1st Floor), Parkway Business Centre, Princess Road, Manchester, M14 7LU
Registered in England: 4097823
VAT registration number: 748 8527 79

## Some important initial 'requirements'

### Use the latest version of MDaemon Pro

The Free and Standard versions of MDaemon do not incorporate any significant spam filtering features so you should be using the Pro version of MDaemon otherwise this document isn't relevant to you. You should also be running the latest version to ensure you've got all the latest updates and features.

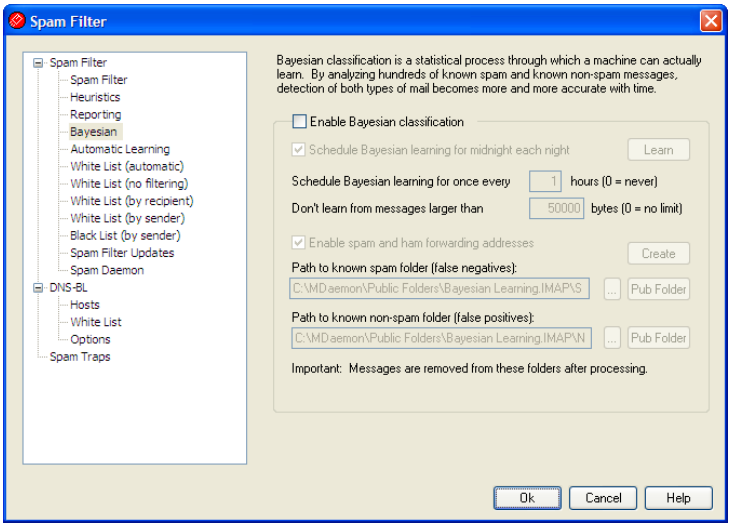
### Install the latest SecurityPlus plug-in

MDaemon's SecurityPlus plug-in adds two significant features to MDaemon's arsenal of security tools. The first is a signature based antivirus scanning engine (which includes automated updates) and the second, only enabled with MDaemon Pro, is Outbreak Protection. Rather than looking at the content of a message to detect spam and viruses, Outbreak Protection filters emails based on the way in which they've been seen to be spreading across the Internet in real-time. Adding SecurityPlus makes a huge difference to the filtering of unwanted emails.

### Disable MDaemon's Bayesian filtering

The Bayesian filtering component of MDaemon's spam filter engine is designed to fine-tune the spam filter scoring based on what is good email and what is spam. It relies on careful management of what is fed back to the Bayesian engine by users so that it can 'learn' (in a statistical sense) about its mistakes as times goes by. In our experience on most MDaemon servers, this feature is either ignored or is 'fed' incorrectly and as a result can begin to act counter-intuitively. Our recommendation is to disable this component of the spam filter unless you are 100% sure that it's working with you rather than against.

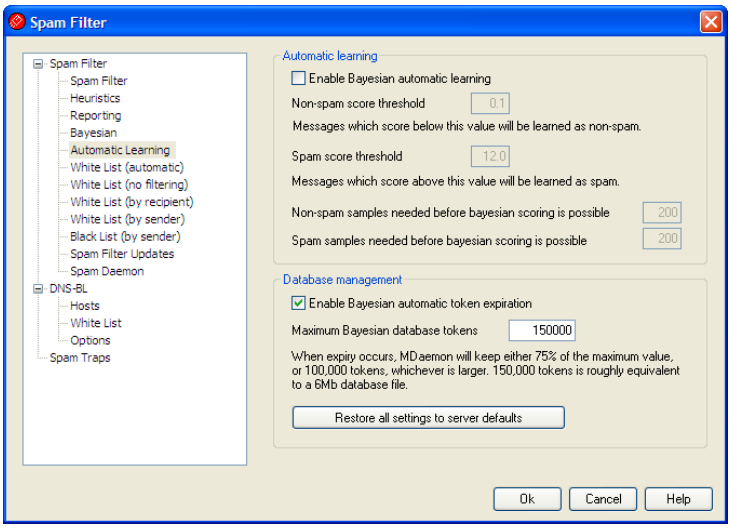
To disable the Bayesian filtering, press CTRL+P, and configure the 'Bayesian' section as shown below:-



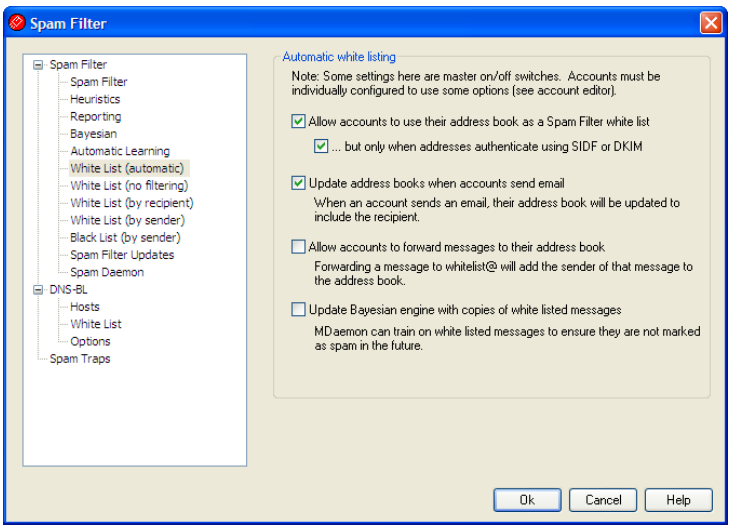


Registered office: Parkway 5 (1st Floor), Parkway Business Centre, Princess Road, Manchester, M14 7LU
Registered in England: 4097823
VAT registration number: 748 8527 79

Also ensure that the 'Automatic Learning' section is disabled as shown below:-



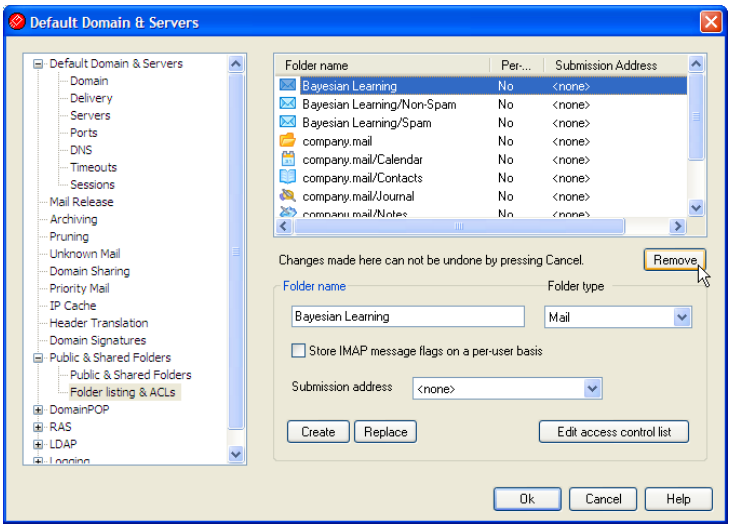

Finally, disable the 'Update the Bayesian engine with white listed messages' option in the 'White List (automatic)' section here:-





Registered office: Parkway 5 (1st Floor), Parkway Business Centre, Princess Road, Manchester, M14 7LU
Registered in England: 4097823
VAT registration number: 748 8527 79

Once you've disabled all the Bayesian features, you may also want to delete the public folders relating to this feature to avoid any confusion your users may have. To do this, press F2, then select 'Folder listing & ACLs' from the 'Public & Shared Folders' section. Highlight the 'Bayesian Learning' parent folder on the right and click the 'Remove' button as shown below:-




This should remove the two Bayesian Learning sub-folders at the same time.

**Switch to direct SMTP delivery with a single MX record**

Many MDaemon customers still use DomainPOP or MultiPOP collection to receive email into their MDaemon server or have their email forwarded on via SMTP from a third party mail service. Unfortunately, doing this massively reduces MDaemon's ability to detect unwanted spam and virus infected messages.

***Until you switch to direct SMTP delivery, you will continue to have problems with spam!***

If email doesn't arrive directly at your MDaemon server and instead is accepted on your server's behalf by another mail server, then it's unreasonable to expect MDaemon to be able to do its job properly. This is because a number of MDaemon's security features rely on it being able to see the connecting IP, the rate of connections, to verify the sender's address, to validate the recipient's address and to check the email content and distribution pattern before accepting or rejecting the message during the SMTP session itself.

Switching to SMTP delivery is actually a straightforward process and requires three initial things to be in place:-

1. A permanent reliable Internet connection;
2. A static IP address;
3. A route through your firewall/gateway so that inbound connections from the Internet on TCP port 25 can be routed to your internal MDaemon server.

Once these three requirements are in place, you would then need to ensure that your domain name's DNS is set-up so that:-

1. You have an 'A record' eg. mail.yourdomain.com pointing to your static IP address;
2. You have a SINGLE MX record pointing to the new 'A record', ie. make sure that you don't have any additional 'back-up' MX records.

***Why only a single MX record?***

Back-up MX servers tend not to provide the same number of validation checks on inbound emails and as a result can become the target for spammers because they represent a 'back door' into your MDaemon server. MDaemon is much better able to filter unwanted emails if it receives them directly rather than via an interim relaying email server.

***But won't we lose email if our connection or server goes down?***

No, you shouldn't because sending email servers on the Internet ought to be configured to attempt redelivery at regular intervals for up to 5 days. So if your server is unavailable, once it comes back up, the emails should arrive as normal without any further intervention. At worst, if you don't get your server back up and running quickly enough, the sending server should simply give-up trying and will send a non-delivery notification message back to the original sender.

If timely receipt of your email is ultra-critical, it is recommended that you apply resources to a second Internet connection and spare redundant server hardware. If you have a second Internet connection, then setting up a secondary MX record pointing to a second A record which routes via the alternative connection to your main MDaemon server is a good idea.

If having a backup MX record pointing to a third party email relay is an absolute requirement, then we would recommend configuring it as a secondary MX, but then adding another tertiary MX record which duplicates your primary MX record. Because spammers will tend to target the lowest priority MX record they will still hit your MDaemon server and be subject the usual security checks.

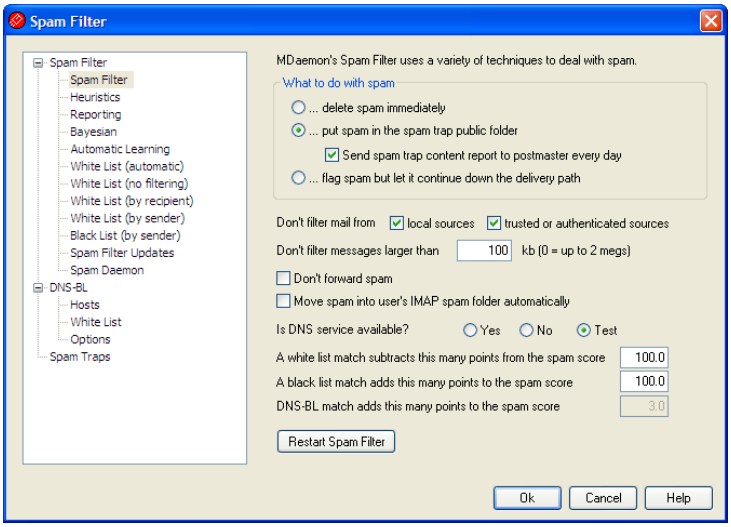

Registered office: Parkway 5 (1st Floor), Parkway Business Centre, Princess Road, Manchester, M14 7LU
Registered in England: 4097823
VAT registration number: 748 8527 79

## Spam filter settings

Press CTRL+P to access MDaemon's Spam Filter settings.

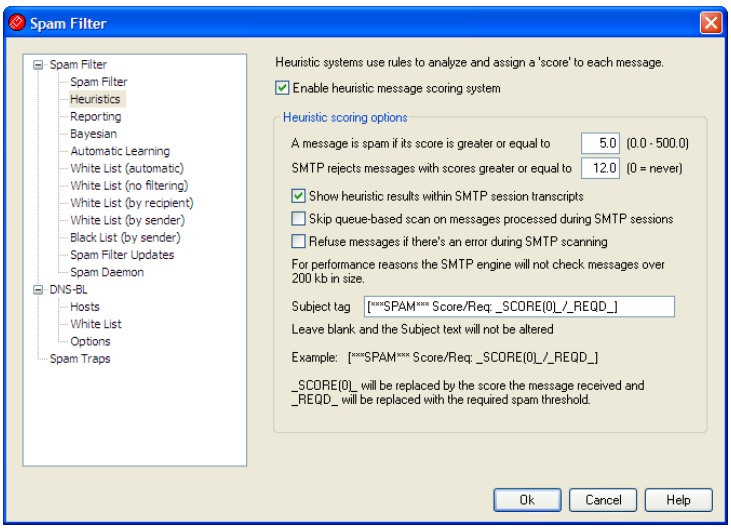
### Spam Filter general settings

By default, when MDaemon detects a spam email, it flags its headers and pre-pends a ***SPAM*** tagline and score to the message subject before allowing them to continue down the delivery path to the end user. In most cases, it is actually preferable to filter messages flagged as spam into a 'spam trap' public folder which can be monitored for false positives by an administrator (how to do this using WebAdmin is described later on in this document). To enable this to happen, select the middle option in the 'What to do with spam' section on the window shown below.




### Heuristic scoring options

In the 'Heuristics' section, configure the scores as shown below:-



The default values of 5.0 and 12.0 are fine for most sites although the score of 5.0 can be lowered a bit (eg. to 4.0) if you want to make the spam filter more aggressive at the risk of seeing a few more false positives.

We also recommend disabling the option to 'Skip queue-based scan on messages processed during SMTP sessions'. This does put more load on MDaemon's spam filter, but should provide more accurate filtering in certain circumstances.

**White List (no filtering)**

This section allows you to define email addresses or domain names to be excluded from MDaemon's spam filtering. If you find that emails from genuine senders are continually being flagged as spam by your server, then add the sender's email address here. We would recommend using this sparingly and only when necessary.

**White List (by recipient)**

This whitelists (ie. subtracts 100 from the message's overall spam score) email TO any address or domains listed here. We often see customers add their own addresses in here before complaining that they're getting lots of spam. Our recommendation is to not have any addresses or domains listed in here unless you're completely happy for them to receive spam.

**White List (by sender)**

This whitelists (ie. subtracts 100 from the message's overall spam score) email FROM any address or domains listed here. It's hard to see why you would use this list instead of the 'White List (no filtering)' list and our recommendation is to not add any of your own entries in here.

**Black List (by sender)**

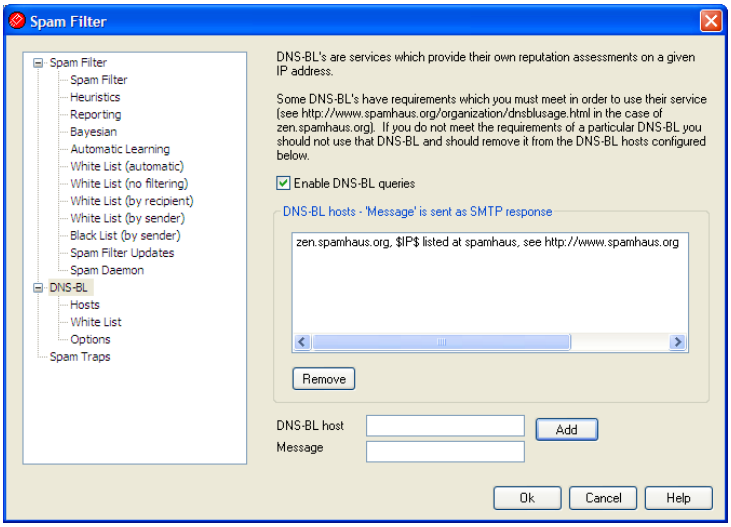
This blacklists (ie. adds 100 to the message's overall spam score) email FROM any address or domains listed here. Because spammers generally don't use their own email addresses when sending spam, blacklisting the addresses they've spoofed is largely ineffective. Our recommendation is to not add any of your own entries in here and instead use MDaemon's 'Address Blacklist' feature (see later) to block emails from unwanted senders.

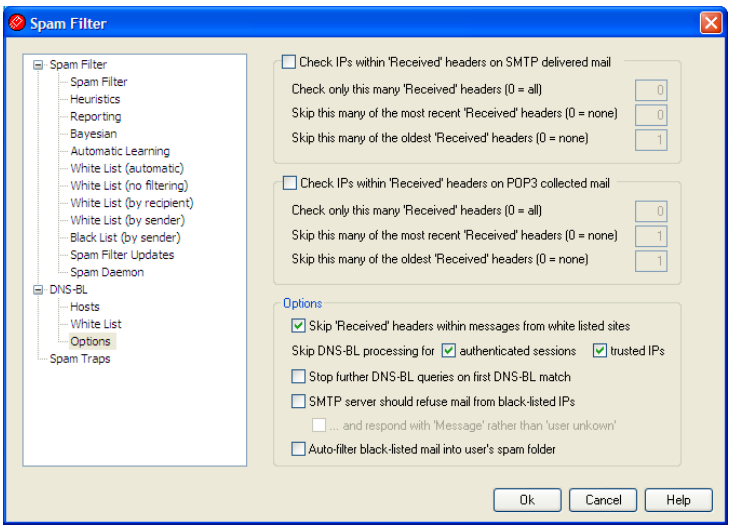
## DNS-BL

This feature checks the IP address of incoming SMTP connections against publicly hosted IP based blacklists. Different lists have varying sets of criteria relating to why any particular IP address is blacklisted but over the years, one list which has proven to be very reliable is the Spamhaus one. By default, MDaemon incorporates this list but the feature is disabled because there are some commercial requirements that Spamhaus stipulate must be satisfied before an organisation can utilise their list. These criteria are listed on the Spamhaus website here:-

http://www.spamhaus.org/organization/dnsblusage.html

If your site meets the criteria for free usage (most MDaemon sites will), then we'd recommend enabling this feature and configuring it with the default settings as shown below:-



## Spam Traps

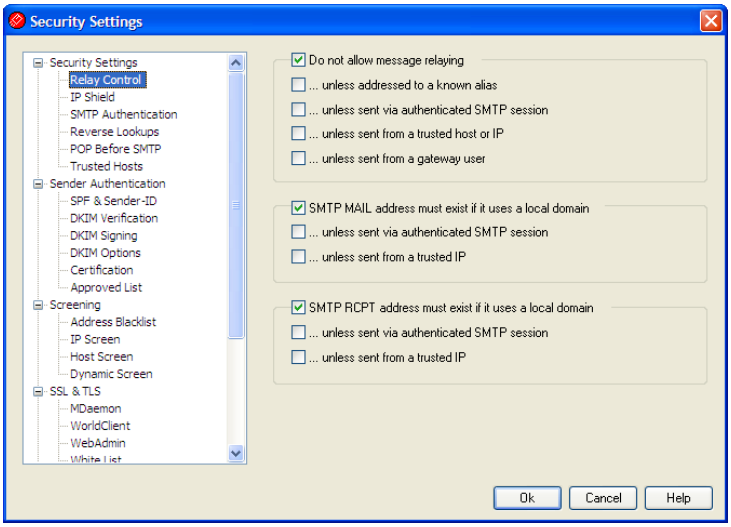
Confusingly named, this feature differs from the 'Spam trap' folder where messages flagged as spam are sent to. This feature is designed to provide email addresses which act as 'honey traps' for spammers so that their spam can then be fed to MDaemon's Bayesian filtering engine. Because our recommendation is to disable MDaemon's Bayesian features, we'd also recommend not using this feature at all.


Registered office: Parkway 5 (1st Floor), Parkway Business Centre, Princess Road, Manchester, M14 7LU
Registered in England: 4097823
VAT registration number: 748 8527 79

## Additional security features to check/configure

### Block relaying attempts with 'Relay Control'

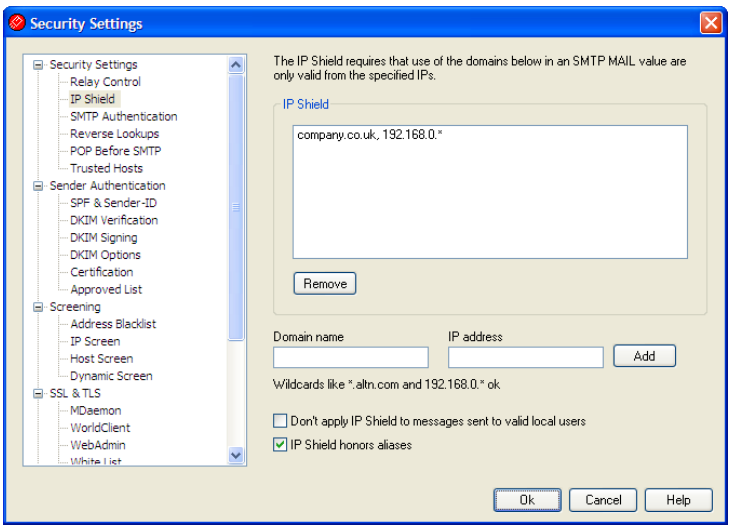
Mail Relaying is where email is neither to or from a local address. In almost all cases, you should not be allowing relaying through your MDaemon server. To check that this is the case, you should press CTRL+S, select the 'Relay Control' section and configure as shown here:-




### Block spoofing with the 'IP Shield'

A method commonly used by spammers is to send emails to or through a server claiming to be users at the local domain (ie. spoofing). To ensure that this doesn't happen to your server, you should configure MDaemon's 'IP Shield' to protect your local domains.

Press CTRL+S , select the 'IP Shield' section and configure as shown (but using your own domain name and internal IP range):-



This tells your server to check that anyone sending email to or through your MDaemon server claiming to be from the listed domain is actually connecting from the expected IP address range. It is highly recommended that you configure an IP Shield entry for each domain name on your MDaemon server.

Note that once configured if you do have local users connecting from outside of your local network to send email through your server, that they will need to enable the 'Use SMTP Authentication' option in their own email clients (by default, SMTP authenticated sessions bypass the IP Shield checks).

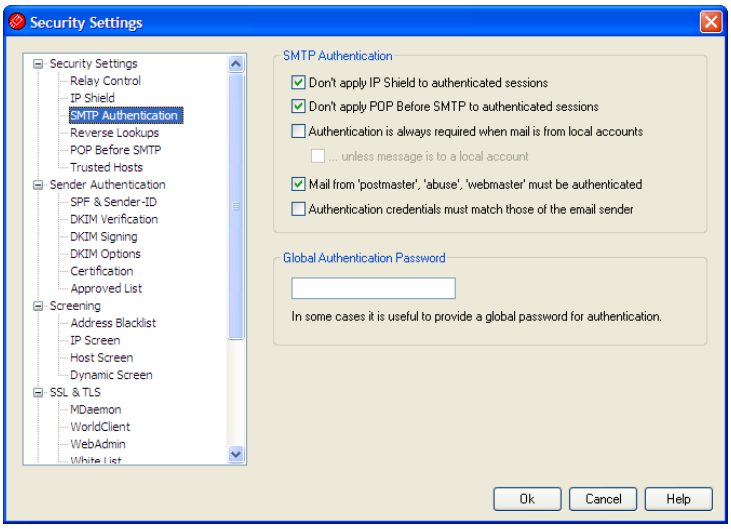
**Check that your account passwords are strong enough!**

You should ensure that all your MDaemon accounts are configured with passwords which are not easy to guess. Otherwise, a spammer may be able to authenticate as a local user and bypass most of MDaemon's security settings – obviously not a good thing.

Passwords such as '1234', 'password', 'letmein' or ones that are the same as the user's mailbox name (very common!) should be avoided at all costs.

**SMTP Authentication**

Press CTRL+S and select the 'SMTP Authentication' section. You should check that the settings are configured with at least the three tickboxes shown below being enabled. Enabling the other two settings will tighten up your security considerably but you will need to enable SMTP Authentication on all your users' email clients first so enable these with care!

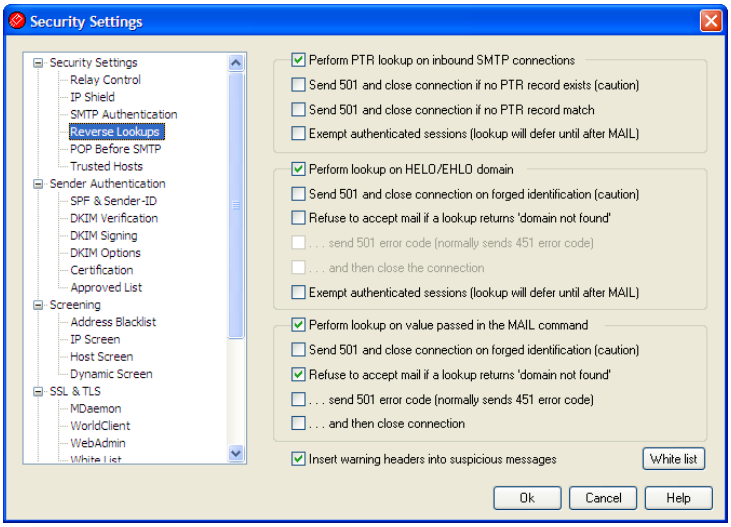




Registered office: Parkway 5 (1st Floor), Parkway Business Centre, Princess Road, Manchester, M14 7LU
Registered in England: 4097823
VAT registration number: 748 8527 79

### Reverse Lookups

Press CTRL+S and select the 'Reverse Lookups' section. The defaults settings (shown below) are the recommended ones.




### Trusted Hosts

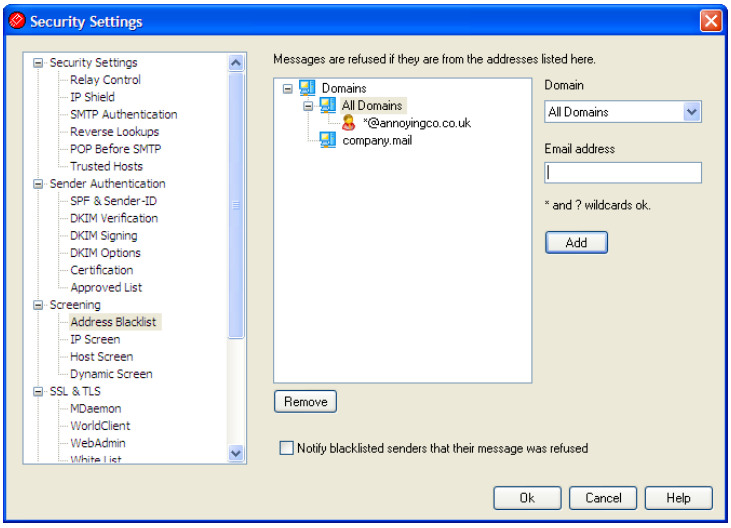
Press CTRL+S and select the 'Trusted Hosts' section. By default there are no entries listed here and this is recommended. Trusted hosts are exempt from a lot of MDaemon's security checks and are only validated by their IP address or host name. If you do have any IP addresses listed in this section, you should be 100% sure that you know why they're there. We highly recommend that you do not have any trusted hosts configured.

**Handling annoyance emails with 'Address Blacklist'**

Spam can generally be classed into two types. The first type are the typical Viagra, bank fraud and porn touting emails which typically originate from hijacked/spoofed addresses. The second type are the annoyance type marketing emails which are sent out by genuine companies touting for business, but which are hard or impossible to unsubscribe from.

The former type are really best left to MDaemon's spam filtering because attempting to blacklist a hijacked/spoofed email address is usually a futile exercise.

The latter type can simply be blocked during the initial SMTP transaction using MDaemon's 'Address Blacklist' feature. To access this, select 'Security Settings' from the 'Security' menu (CTRL+S) and then go to the 'Address Blacklist' section. In general, when adding an address we would recommend adding the sender's entire domain name by using a wildcard entry eg. *@annoyingco.co.uk as shown below:-

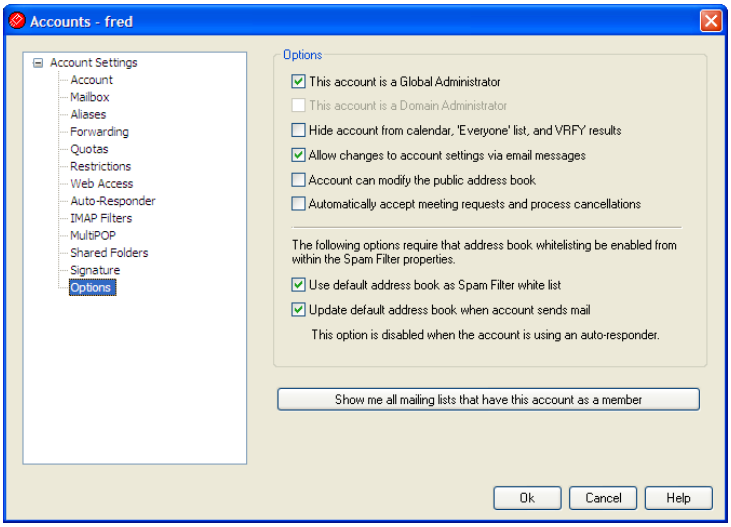




Registered office: Parkway 5 (1st Floor), Parkway Business Centre, Princess Road, Manchester, M14 7LU
Registered in England: 4097823
VAT registration number: 748 8527 79

## Monitoring your spam trap folder using WebAdmin

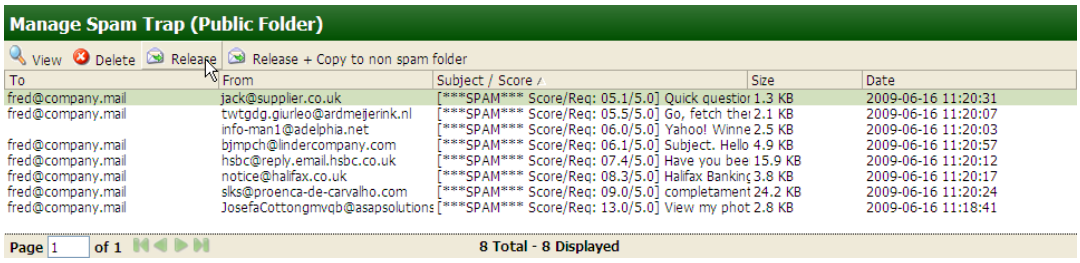
If you've configured MDaemon's spam filter to automatically filter spam into a public 'spam trap' folder, you'll want to have someone monitor that folder each day for any false positives before clearing out any remaining spam. You can do this very easily from any web browser on your network by logging into WebAdmin. First of all, you'll need to check that your account is configured as a 'Global administrator'. To check this, go into your accounts settings (ALT+F3, then double-click your account). In the 'Options' section, check that the account is enabled as a 'Global Administrator' as shown below:-




You should now be able to log into WebAdmin by entering the following URL into any web browser on your local network using your usual MDaemon email address and account password:-

http://192.168.0.1:1000
(replacing 192.168.0.1 with your server's own local network IP address)

Once, logged in, select 'Security' from the bottom left and then 'Spam Trap Folder' from the 'Spam Filter' section. By sorting the messages in the spam trap folder by their score so that the lower scored messages are at the top, you can quickly pick out any false positives that may have been flagged in error. If you do see any false positives, simply highlight them and then click the 'Release' button to have them delivered to the original recipient as shown below.




After releasing any false positives, you can highlight the remaining spam messages and delete them to clear the spam trap folder.


Registered office: Parkway 5 (1st Floor), Parkway Business Centre, Princess Road, Manchester, M14 7LU
Registered in England: 4097823
VAT registration number: 748 8527 79

## Still suffering from too much spam?

If after making the recommendations in this document, your organisation is still suffering from significant volumes of spam you should check to make sure that you've not inadvertently whitelisted or excluded the sender's or recipient's address from MDaemon's spam filter. You should also check that the spammer didn't manage to authenticate their SMTP session by guessing a local user's account password and that their connection didn't originate from a trusted or local IP address.

To check these things, it's best to refer to your MDaemon server's inbound SMTP and anti-spam log files. You will find these in your '\MDaemon\Logs' folder, look for filenames like this:-

MDaemon-20090616-SMTP-(in).log
MDaemon-20090616-AntiSpam.log

## Suffering from too many false positives?

If you find that you're suffering from a lot of false positives, check that you've not inadvertently blacklisted the sender's or recipient's address in MDaemon's spam filter settings.

## Conclusions

The combination of MDaemon Pro, its SecurityPlus plug-in and direct SMTP delivery via a single MX record should mean that your organisation does not suffer from significant volumes of spam or false positives.

Most spam related issues derive from either not using MDaemon Pro, not having SecurityPlus installed, not having direct SMTP delivery via a single MX or mis-configuration of MDaemon's settings.

In addition to checking that the majority of features are reset to their defaults, there are a few additional changes that we would highly recommend making based on our experience over years of supporting MDaemon. These are detailed in this document.

If after following these recommendations, you are still having problems, please double-check the relevant logs on your server to see if something obvious has been missed, but then contact us for further assistance and advice.


Registered office: Parkway 5 (1st Floor), Parkway Business Centre, Princess Road, Manchester, M14 7LU
Registered in England: 4097823
VAT registration number: 748 8527 79