Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

EFFECTIVE SPAM FILTERING WITH MDAEMON

Introduction

The following guide provides a recommended method for increasing the overall effectiveness of MDaemon's spam filter to reduce the level of spam received to a minimal level.

Note: The spam filter is **only available in MDaemon Pro**. It is recommended that this document is used on conjunction with MDaemon 8 or above.

MDaemon's default configuration

Following a fresh installation, MDaemon is configured to automatically calculate a 'spam score' for each email message it receives using a number of sophisticated built-in spam fighting tools.

MDaemon is configured with a default threshold score of '5.0' - at this score and beyond messages will be tagged as spam. By default, no automated action, such as bouncing, filtering or deleting spam will be taken by MDaemon without further configuration by an administrator.

Inbound messages being received by SMTP which obtain a score equal to or greater than 12.0 are automatically refused – at this level messages are almost certainly spam and so refusing them is a valid thing to do. Note that refusing to accept a message is a different thing to accepting and then later bouncing the message. **Bouncing spam messages is absolutely not recommended** as spammers generally do not use their own email address when sending spam.

Expected results using MDaemon's default configuration

Although results will inevitably vary from site to site, in general the expected accuracy using MDaemon's default configuration would be for it to automatically tag approximately 70% of all spam received whilst causing a negligible quantity of false positives ie. genuine messages incorrectly tagged as spam.

Achieving better results

The key to achieving better spam filtering results lies in improving MDaemon's spam filtering accuracy in conjunction with gradually increasing its aggressiveness.

Accuracy can be improved by training users to feed back spam messages that were missed by the spam filter while aggressiveness can be increased by gradually reducing the threshold spam score ie. the score at which messages will be tagged as spam, until a comfortable level is reached.

It needs to be understood that increasing MDaemon's aggressiveness may also result in a larger quantity of incorrectly tagged false positives. As part of the feedback process it is important that a monitoring process exists that can detect these false positives and then feed them back so improving its accuracy.

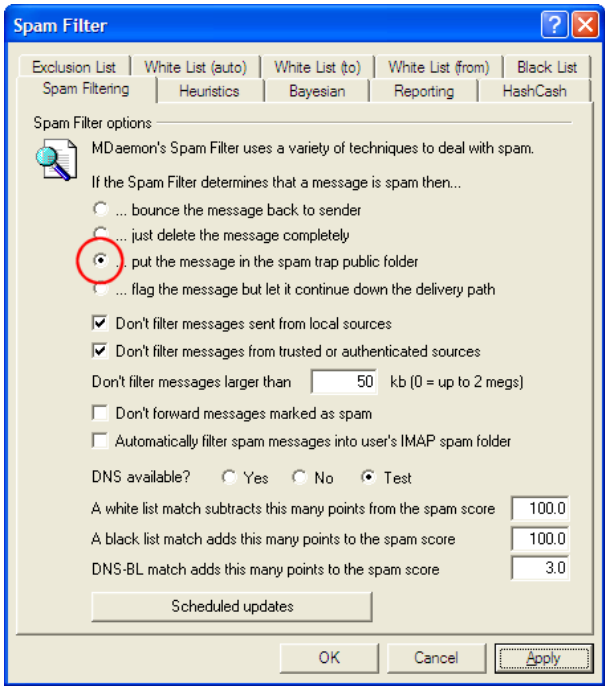
Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

Using MDaemon's 'Spam Trap' folder

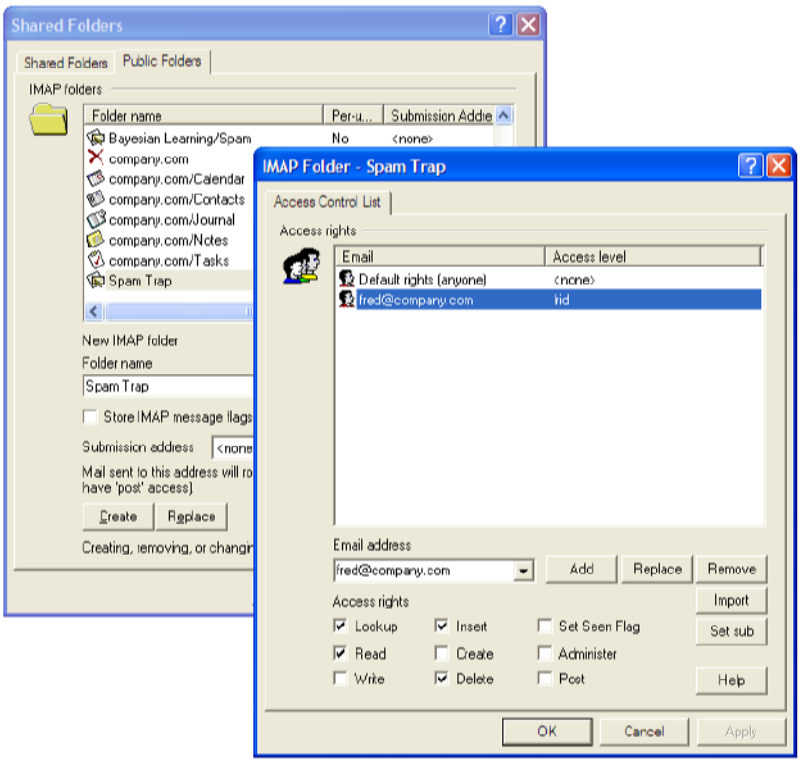
MDaemon's default configuration is to allow tagged spam to continue down to end users' mailboxes allowing users to do what they like with local email filters. In most companies however, it is usually preferable to configure MDaemon to filter off spam centrally at the server so that it can be monitored by an administrator each day for any false positives.

To configure spam to be filtered off into a central '**Spam Trap**' folder, go into MDaemon's interface and select **Security -> Spam filter**… and configure as shown here:-



Once this option has been selected, MDaemon will filter any messages that reach or surpass the threshold score into a root public folder called '**Spam Trap**' – by default, only the postmaster user has access to this folder.

Note: MDaemon's public folders and their permissions can be viewed and modified under **Setup -> Shared Folders -> Public Folders tab** as shown here:-



Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

Accessing and monitoring the 'Spam Trap' folder

There are a number of ways that the postmaster user can access and manage spam that has been filtered into MDaemon's Spam Trap folder:-

Using an IMAP client such as WorldClient, Outlook or Outlook Express or an Outlook Connector enabled Outlook client
Through the MDaemon interface itself via the Queues tab
Through WebAdmin - our recommended method.

Using WebAdmin to manage the Spam Trap folder
WebAdmin is a free plug-in for MDaemon that allows almost total administration of MDaemon through a sophisticated and easy to use web interface. WebAdmin is included as part of MDaemon from version 9 onwards but for version 8 can be downloaded from our website here:-

http://www.headtex.co.uk/shop/download.asp

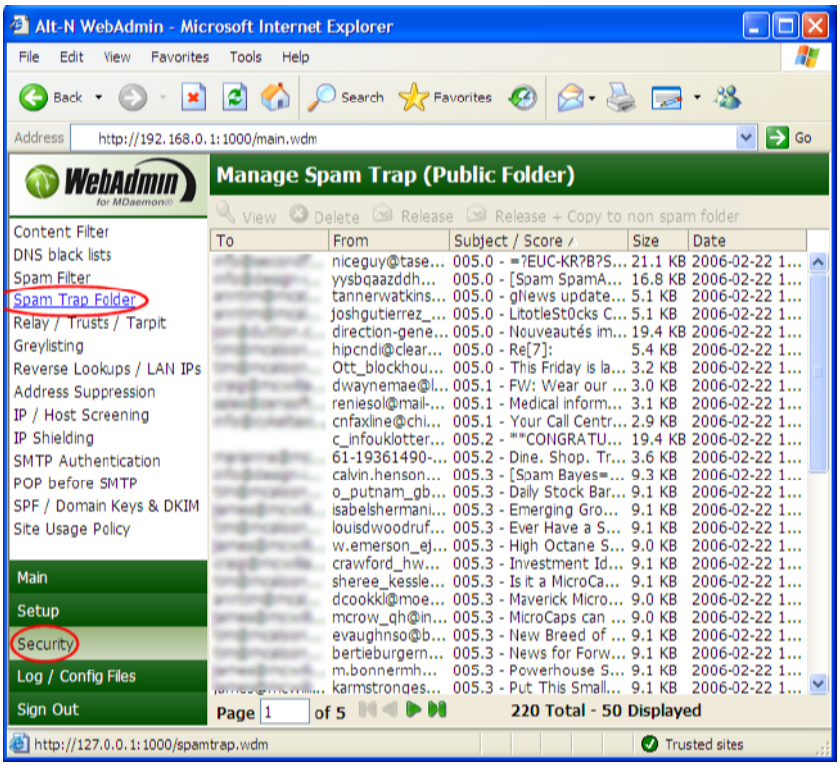
An easy installation guide for WebAdmin is also available on our website.

Once installed, WebAdmin is accessed using a web browser by typing the following URL:-

http://192.168.0.1:1000

…replacing 192.168.0.1 with your server's own network IP address. You will then need to log in using your email address and MDaemon account password.

Once logged in, the Spam Trap management page can be accessed by selecting **Security -> Spam Trap Folder** as shown here:-

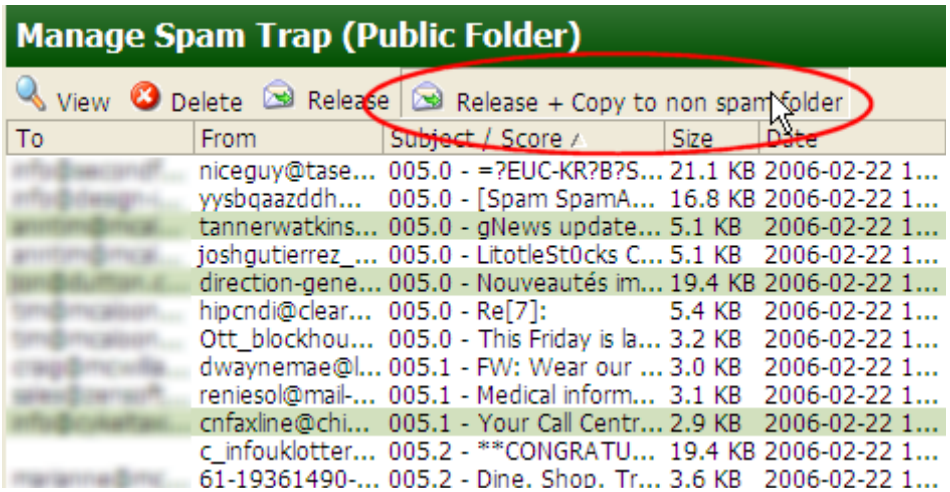


The Spam Trap folder contents can be sorted by their '**Subject / Score**' so that the lowest scored messages are shown at the top of the list. A quick scan through the first couple of pages should highlight any potential false positives.

Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

These can be selected, using CTRL+left click to highlight multiple items, and then released and fedback by simply clicking the '**Release + Copy to non spam folder**' button as shown here:-



The remaining messages which should now be definite spam can then be deleted to empty the spam trap folder.

The task of using WebAdmin to check the contents of the spam trap folder and releasing and feeding back any false positives, is an important one that should be done each day by an MDaemon '**Global Administrator**'.

Note: The level of access any MDaemon user has through WebAdmin is controlled on a per account basis in the MDaemon account options. This can be accessed by selecting **Accounts -> Account Manager -> Admin tab** in MDaemon as shown here:-

The user assigned as the postmaster during the MDaemon installation should already be configured as a '**Global Administrator**'.

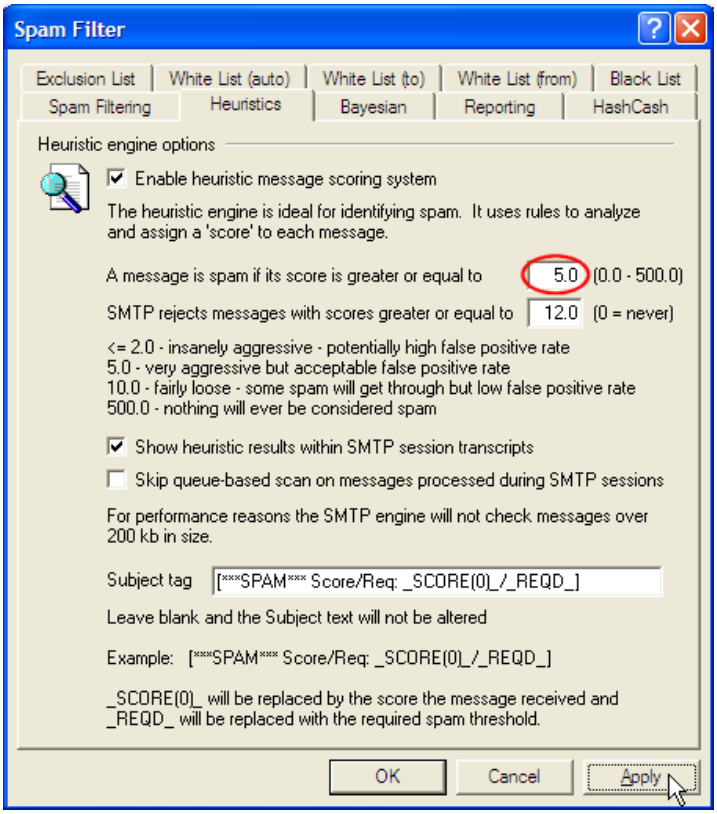
Using WebAdmin in this way provides the basis for being able to gradually lower the spam threshold score so making MDaemon's spam filtering more aggressive while feeding back the false positives also helps to improve the spam filtering accuracy.

Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

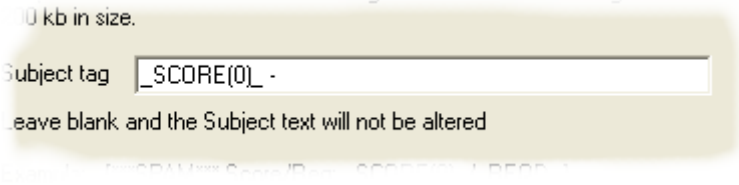
Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

Increasing MDaemon's spam filtering aggressiveness

The main setting that governs the aggressiveness of MDaemon's spam filtering is the spam threshold value – by default this value is 5.0 which is a good compromise value for new installations but in practice quite a few spam messages will score slightly lower than this value. This value can be found in the main MDaemon interface, or WebAdmin, under **Security -> Spam Filter -> Heuristics tab**.



Whilst in this section, we'd also recommend changing the '**Subject tag**' as shown below – this simply makes the subject lines of messages filtered into the spam trap folder easier to view in WebAdmin.



Reducing the spam threshold will reduce the quantity of missed spam but may also increase the probability of false positives.

Based on this knowledge, our recommendation is to **reduce the spam threshold score by 0.1 every 3 or 4 days until a level is reached at which your system provides accurate spam filtering with a low level of false positives**. Resist the temptation to make large changes in one go – after 2 or 3 weeks you should find that you reach a value between 3.5 and 4.5 that suits your particular installation.

Remember that the system is a dynamic one and will adjust as you and your users feed false positives and missed spam back to it – in effect the system 'learns' the difference between genuine emails and spam emails for your own site. So while a value of say 4.3 may initially seem too aggressive, as the feedback takes effect, the same value may actually seem conservative over time.

Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

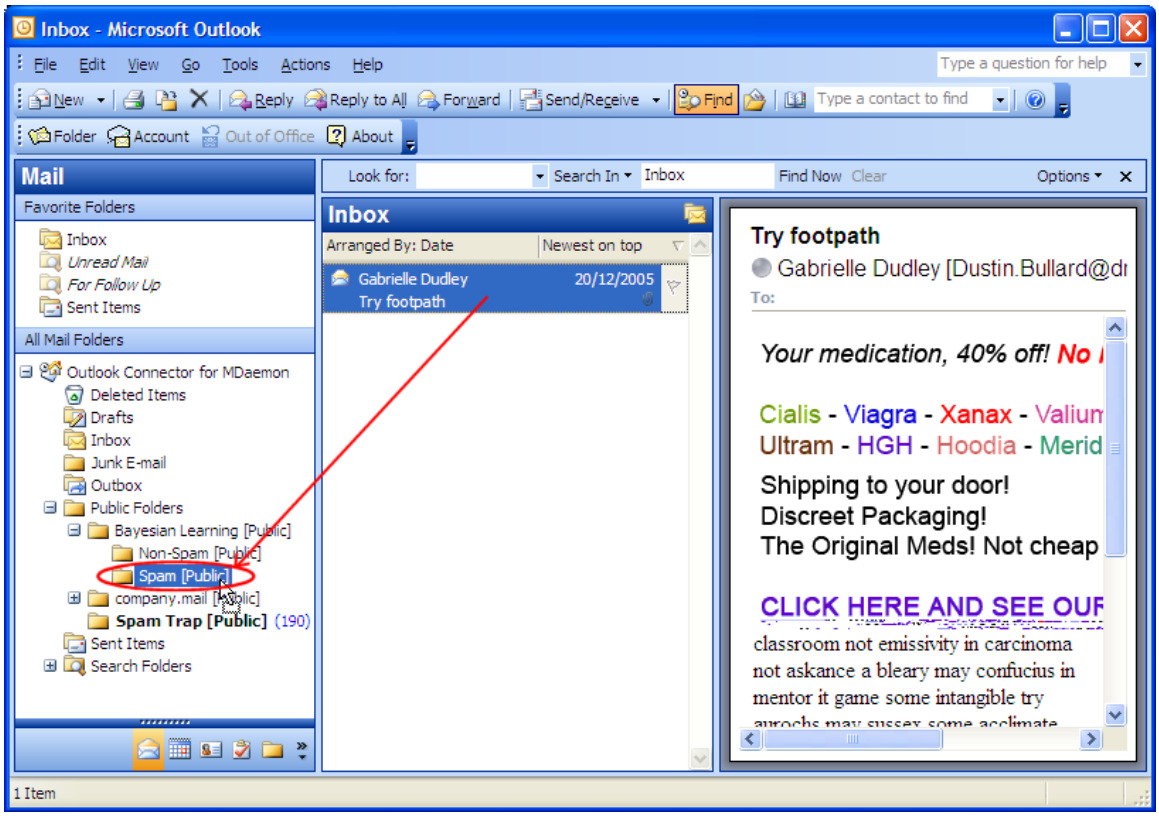
Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

Allowing users to feed missed spam back into the system

A significant part of MDaemon's spam filtering accuracy also depends on it having spam that it missed, fed back to it directly from end users.

There are two ways that this can be done – for IMAP users both methods are possible but for POP3 users, only the second method is possible.

Method 1 (IMAP clients only) – copying missed spam into the 'learning' folder Here the users would drop any spam emails that were missed, into the public folder titled '**Bayesian Learning -> Spam**' as shown here:-



Note: while all users can see the Bayesian Learning folders, the permissions are configured such that while messages can be dropped into the folders, the contents of the folders cannot be viewed. This is to protect users from inadvertently viewing inappropriate spam content placed there by other users.

Method 2 (POP3 or IMAP clients) – forwarding missed spam to a 'learning' address

Because POP3 clients don't have access to shared public folders, it will be necessary for users to forward the missed spam emails back to the server as attachments to the special reserved address of **spamlearn@yourdomain.com**.

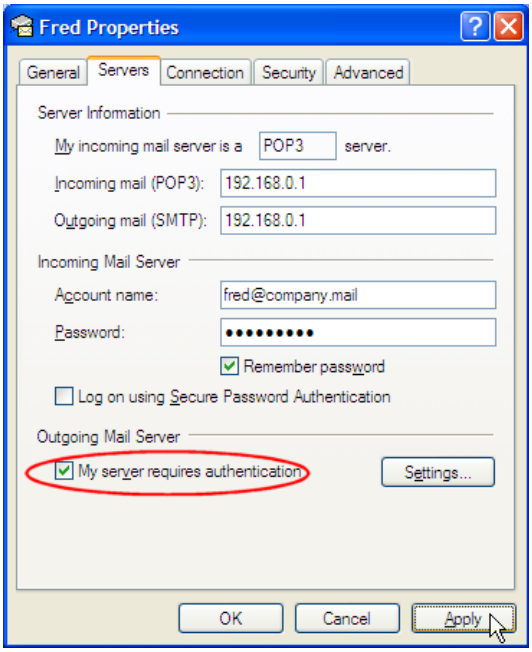
It is important to note that messages sent to the **spamlearn@**... address will only be accepted if they are sent using Authenticated SMTP. In most email clients, turning on Authenticated SMTP is just a case of ticking a box in the client's account properties. In general **the use of SMTP Authentication is highly recommended for all email clients** as authenticating all users who send email through your server will provide the basis for a much more secure operating environment.

Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

Enabling SMTP Authentication in Outlook Express

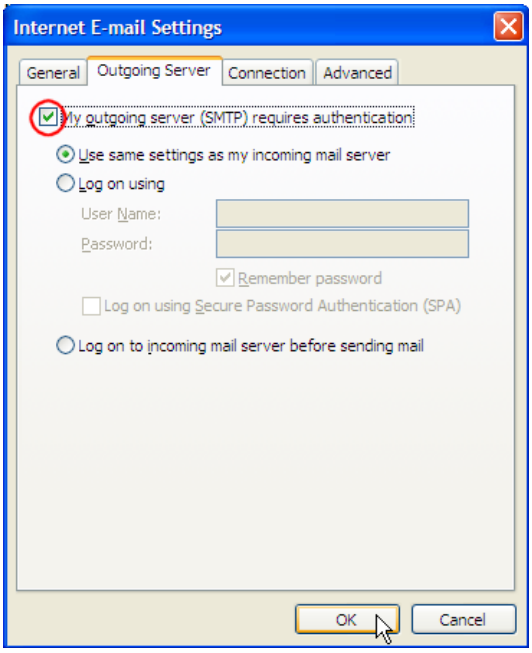
In Outlook Express, the SMTP Authentication option can be found under **Tools -> Accounts… -> Properties button -> Servers tab** as shown here:-



Ensure that the highlighted option is ticked.

Enabling SMTP Authentication in Outlook

In Outlook, the SMTP Authentication option can be found under **Tools -> E-mail Accounts -> View or change existing e-mail accounts -> Change button -> More Settings -> Outgoing Server tab** as shown here:-



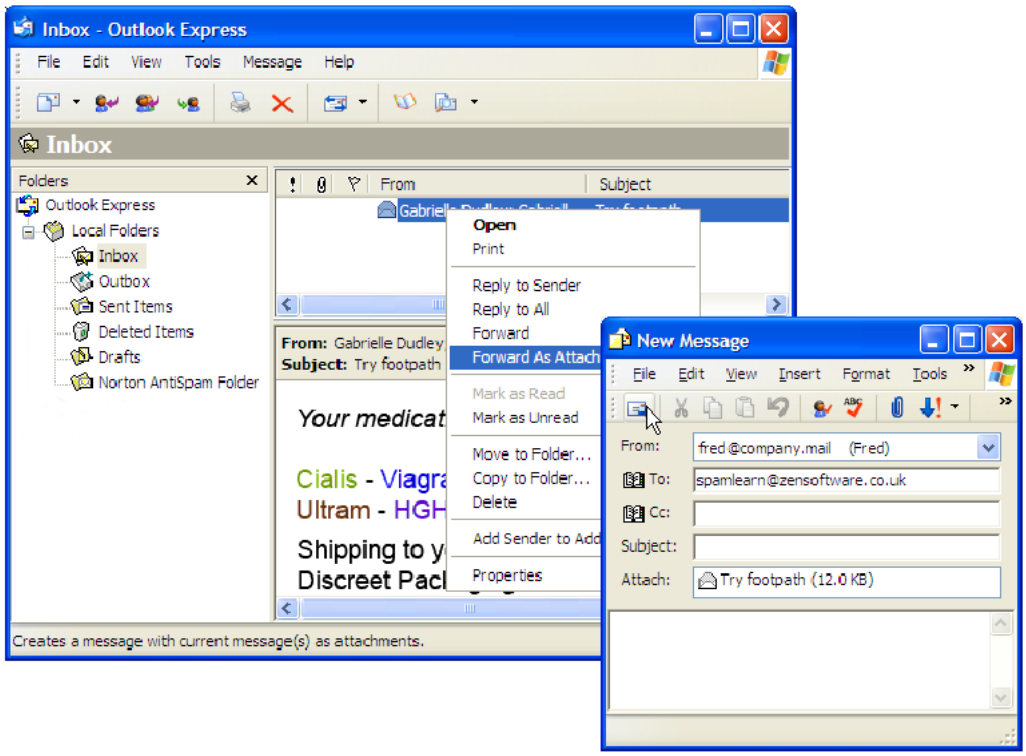
Ensure that the highlighted option is ticked.

Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

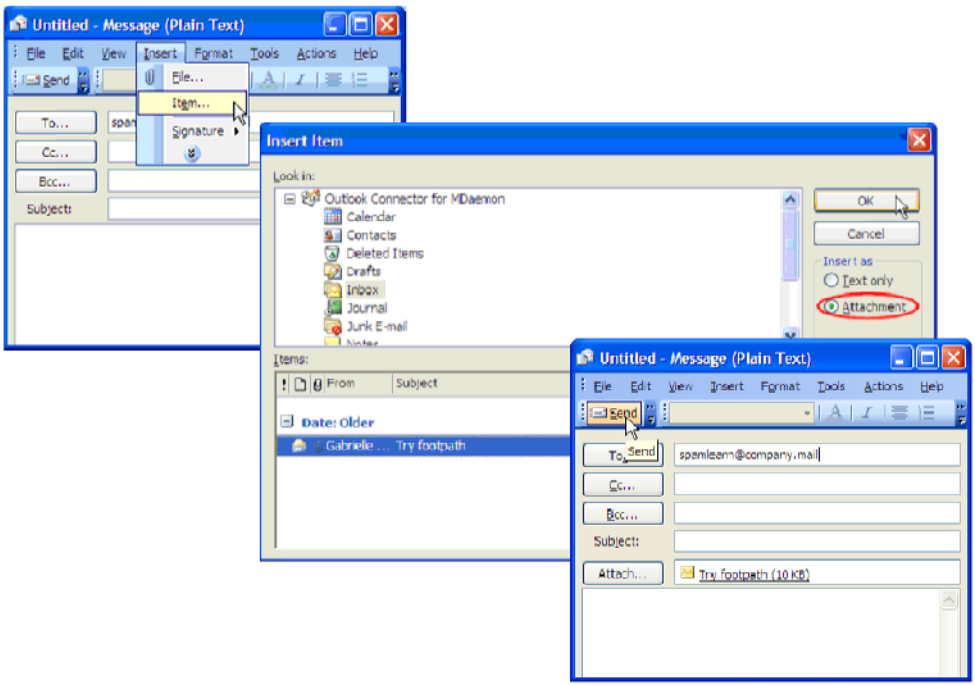
Forwarding a message as an attachment in Outlook Express

In Outlook Express, you can forward a message as an attachment simply by right-clicking on it and selecting '**Forward as Attachment**' as shown here:-



Forwarding a message as an attachment in Outlook

In Outlook you need to create a new message, select **Insert -> Item…** and then select the offending spam message to insert as an attachment to the message as shown below:-



Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

White lists, Black lists and Exclusions

In certain cases it may useful to supplement MDaemon's spam filtering rules by white listing or black listing certain addresses or domain names.

White listing an address or domain name means that the spam score for the message will be decreased by 100 making it very unlikely to be flagged as spam. White listing can be applied in one of two ways:-

Either based on the sender's address or domain name – '**White List (from)**';
or based on the recipient's address or domain name – '**White List (to)**'.

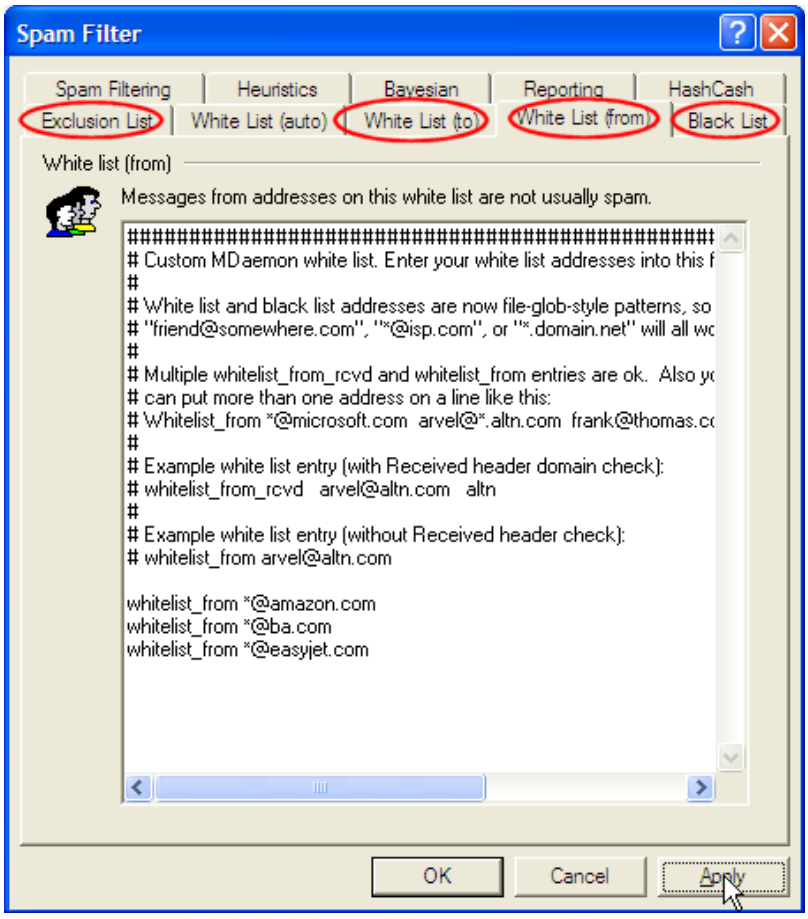
Black listing an address or domain name means that any messages from that address or domain name will have their spam score increased by 100 making it very likely that the message will be flagged as spam.

Although typically it is not necessary to add to these lists yourself, they do offer useful flexibility in situations where:-

email from a certain source is consistently being picked up as spam even though it isn't eg. Airline tickets or car hire confirmations;
'pest' emails from a certain source are not wanted but are not enough like spam to automatically be picked up by the spam filter rules.

Exclusions can also be configured which simply allow for all spam filtering to be completely bypassed if the message is destined for a specific address or domain name. This particular feature is not commonly used.

The white list, black list and exclusion lists can be found in the **Security -> Spam filter** settings as shown here:-



Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

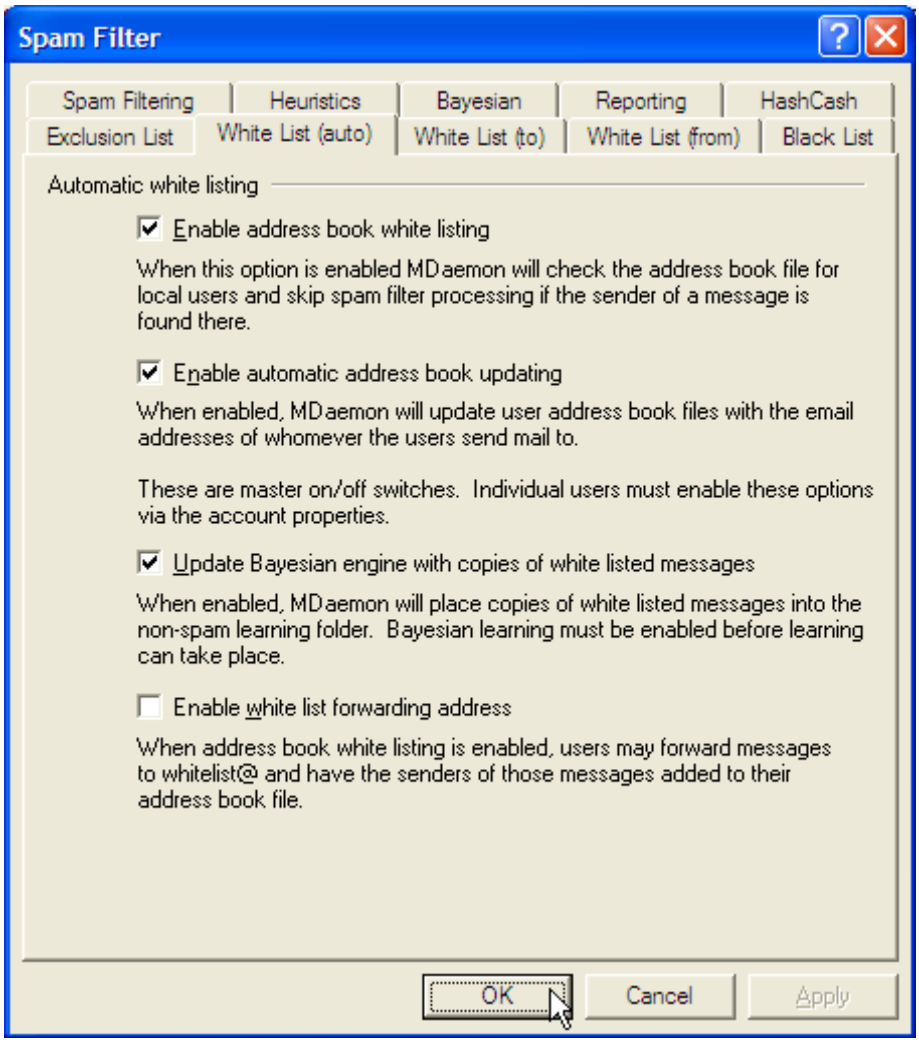
Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

MDaemon's automatic white listing features

MDaemon has a number of advanced features which go a long way to automatically white listing email from genuine addresses so reducing the chance of false-positives.

As users send emails out to the Internet, MDaemon will automatically add the recipient's email address to the user's personal Contacts folder. MDaemon then white lists all emails coming from contacts listed for that user. At the same time, it also feeds samples of genuine email from those white listed contacts back to the spam filter to assist its own learning process by showing it what genuine emails look like.

These features are accessible under **Security -> Spam filter -> White List (auto) tab** as shown below:-



The above options are the recommended defaults.

Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

Other recommendations to help reduce spam

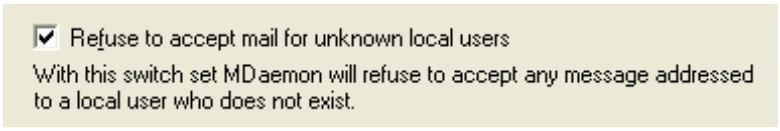
A typical ploy by spammers is to target email servers which blindly accept all emails for a domain name – if they discover one of these they will usually target the domain with spam messages addressed to hundreds of random addresses at the domain name. Because they are accepted, the spammers will often treat these as good targets for further spam.

Avoiding situations where emails to random addresses at your domain name are accepted is an extremely important and effective step in reducing the volume of spam you receive.

Here are some recommendations related to this:-

Wherever possible use direct SMTP delivery to your MDaemon server rather than using DomainPOP with a catch-all address at your ISP. Switching to SMTP delivery is usually a straightforward procedure – for further information about this, please contact our support team.

Ensure that your server is configured to refuse messages addressed to unknown addresses at the local domain name. This option is under **Security -> Relay / Trusts / Tarpit… -> Relay Settings tab**. Always ensure that the following option is ticked:-



Avoid the use of catch-all address aliases
eg. *@yourdomain.com = sales@yourdomain.com

Avoid the use of back-up MX mail servers that are unable to validate incoming emails as being for valid local recipients.

Headtex Limited
Century House 100 Ringer Lane
Clowne
Chesterfield
Derbyshire S43 4BZ

Tel: 01246 812821
Fax: 08700 553568
Web: www.headtex.co.uk

Conclusions

The Spam Filter feature is only included with MDaemon Pro. This document relates primarily to MDaemon v8 onwards.

MDaemon in its default state will tag approximately 70% of received spam with very few false positives. In its default state, no action is taken except to tag the subject line of detected spam.

Most companies will benefit from centrally filtering tagged spam into MDaemon's Spam Trap folder.

Improved spam detection rates come from a combination of:-

Gradually increasing the spam filter's 'aggressiveness';
Daily monitoring of the spam trap folder for false positives;
Feedback of spam filtering errors such as false positives and missed spam.

WebAdmin provides an excellent way for MDaemon administrators to monitor the Spam Trap folder, releasing and feeding back false positives as required.

WebAdmin is included as part of MDaemon 9 onwards and can be downloaded as a free plug-in for earlier versions of MDaemon - using MDaemon v8 onwards is recommended.

End users can assist MDaemon's spam filtering accuracy by feeding back missed spam to the system. If they use IMAP, they can simply drag and drop missed spam into the '**Bayesian Learning/Non-Spam folder**'. POP3 users can forward missed spam as attachments to the **spamlearn@**... system address using authenticated SMTP.

MDaemon provides a level of 'self teaching' using its auto-white listing features which automatically updates users' personal Contacts folders with email recipients, white lists emails from senders listed in the personal Contacts folders and learns from samples of emails from those senders. These features can be enabled or disabled as required.

Avoiding catch-all email addresses, switching to direct SMTP delivery and refusing email addressed to unknown local addresses is a vital step towards reducing the amount of spam you have to deal with.

Following the recommendations made in this document will increase the effectiveness of MDaemon's spam filtering engine within a few weeks to approximately 95% detection rate with a negligible rate of false positives.