Configuring MDaemon for Centralized Spam Blocking and Filtering

Alt-N Technologies, Ltd
2201 East Lamar Blvd, Suite 270
Arlington, TX 76006
(817) 525-2005
http://www.altn.com

July 26, 2004

Contents

A Centralized Approach to Blocking and Filtering Spam

MDaemon PRO contains antispam tools capable of blocking 95% of spam, while allowing all legitimate messages to reach their destinations.

This document describes one way to configure MDaemon PRO to fight spam using a centralized method.

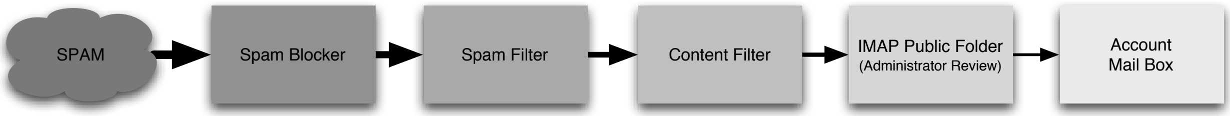
This configuration centralizes the collection and processing of spam. It routes all messages flagged as spam to an IMAP public folder. By reviewing the contents of this folder, an administrator can make sure messages are really spam before deleting them.

In addition, this configuration distributes to authorized email users the ability to identify spam and legitimate messages for the Bayesian filter. Users do this by copying spam messages and legitimate messages to IMAP public folders. The Bayesian filter processes these messages to “learn” the differences between junk mail and real mail, as defined by the users of each email server. Both IMAP and POP account holders can add messages to these public folders.

MDaemon AntiSpam Tools Overview

These configuration instructions use these MDaemon tools:

- Spam Blocker
- Spam Filter
- Content Filter
- IMAP server public folders



The instructions assume the Spam Blocker is enabled and using one or more realtime black lists.

The Spam Filter and IMAP server are features of MDaemon PRO. They are not available with MDaemon Standard.

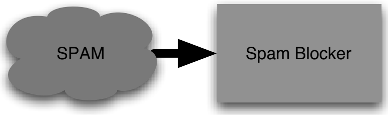
While the IMAP server must be running, this configuration works for both POP and IMAP email accounts.

MDaemon must be in *Advanced* mode to configure the antispam tools. When MDaemon is in its *Easy* mode the antispam tools use MDaemon’s intelligent defaults.

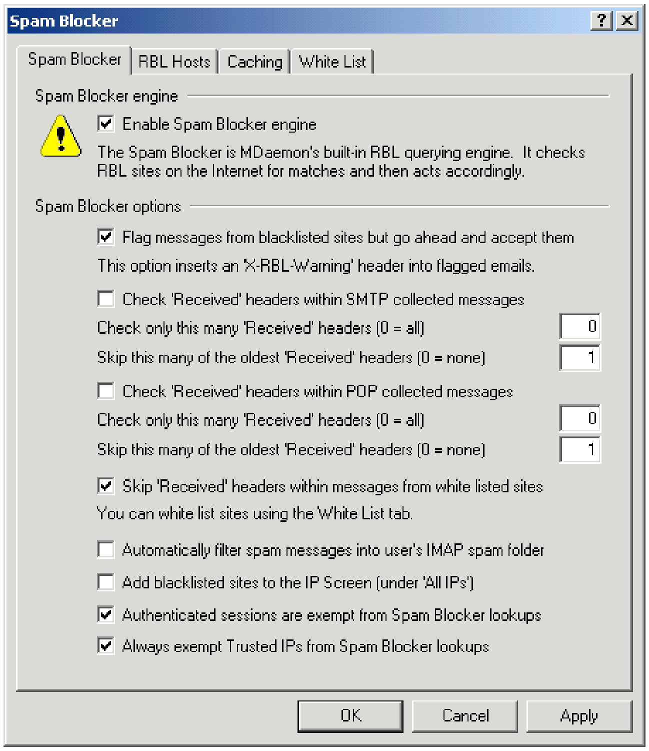
You can change between the *Easy* and *Advanced* modes by using the **File > Switch to. . . mode** command. If the command reads **Switch to easy mode** you are already using *Advanced* mode.

Spam Blocking

The *Spam Blocker* uses publicly available “black lists” to control incoming email sent from likely sources of spam. Several Internet organizations create and maintain these black lists in hopes of blocking email from both known and potential spammers. The goal is to pressure these email sources into being better neighbors on the Internet.



When enabled, the Spam Blocker looks up the IP addresses of incoming email in the black lists. The the IP addresses match, the messages can be flagged for the content filter, isolated or deleted. The inbound SMTP session can also be immediately terminated, refusing the email.



Spam Blocker engine

☑ Enable Spam Blocker engine

The Spam Blocker is MDaemon's built-in RBL querying engine. It checks RBL sites on the Internet for matches and then acts accordingly.

Spam Blocker options

☑ Flag messages from blacklisted sites but go ahead and accept them

This option inserts an 'X-RBL-Warning' header into flagged emails.

☐ Check 'Received' headers within SMTP collected messages

Check only this many 'Received' headers (0 = all) 0

Skip this many of the oldest 'Received' headers (0 = none) 1

☐ Check 'Received' headers within POP collected messages

Check only this many 'Received' headers (0 = all) 0

Skip this many of the oldest 'Received' headers (0 = none) 1

☑ Skip 'Received' headers within messages from white listed sites

You can white list sites using the White List tab.

☐ Automatically filter spam messages into user's IMAP spam folder

☐ Add blacklisted sites to the IP Screen (under 'All IPs')

☑ Authenticated sessions are exempt from Spam Blocker lookups

☑ Always exempt Trusted IPs from Spam Blocker lookups

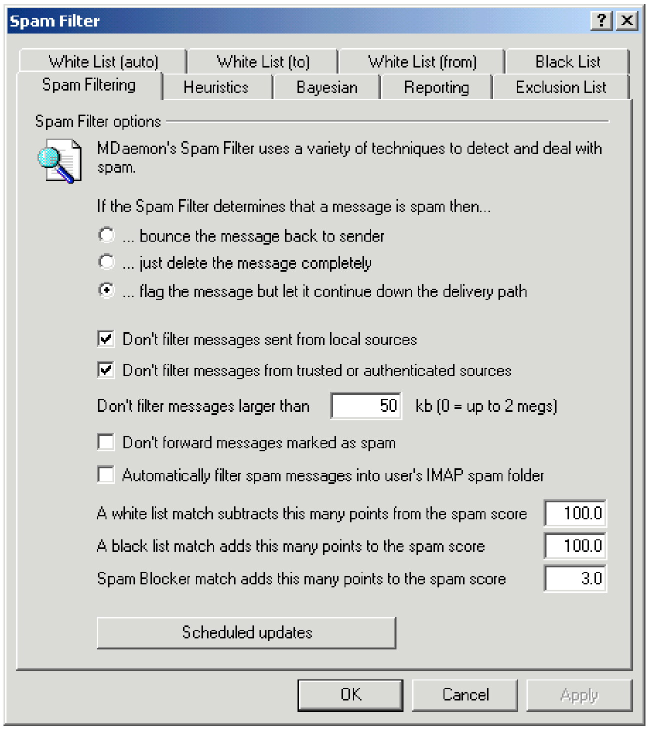
Spam Filtering

Spam Filtering uses heuristic matching and Bayesian classification to intelligently detect and tag email spam.

SPAM
Spam Blocker
Spam Filter

Heuristics employ pattern-matching technology to identify spam.

Bayesian Filtering separates junk mail from legitimate mail by statistically comparing the words of incoming messages to the contents of previous emails known to be either spam or non-spam. The Spam Filter includes white listed email addresses, black listed addresses and addresses excluded from any processing. Recent experience shows Bayesian filtering to be particularly effective at blocking spam while allowing legitimate mail through.



Spam Filter options

MDaemon's Spam Filter uses a variety of techniques to detect and deal with spam.

If the Spam Filter determines that a message is spam then...

○ ... bounce the message back to sender

○ ... just delete the message completely

● ... flag the message but let it continue down the delivery path

☑ Don't filter messages sent from local sources

☑ Don't filter messages from trusted or authenticated sources

Don't filter messages larger than 50 kb (0 = up to 2 megs)

☐ Don't forward messages marked as spam

☐ Automatically filter spam messages into user's IMAP spam folder

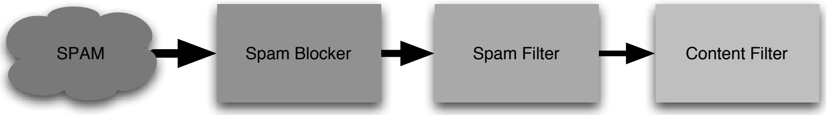
A white list match subtracts this many points from the spam score 100.0

A black list match adds this many points to the spam score 100.0

Spam Blocker match adds this many points to the spam score 3.0

Content Filtering

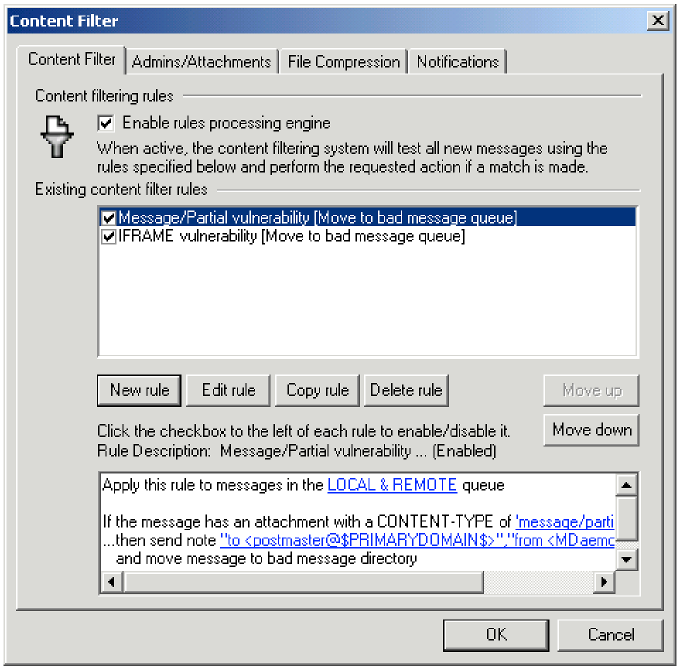
Content filtering operates as a sieve and re-distribution system for MDaemon. It is one way to regulate the flow of messages in, through, and out of your email server.



Content filtering analyzes email content by looking at headers, senders, recipients, subjects and the words in a message.

Depending on the analysis, Content filtering can, for example:

- Delete a message.
- Redistribute a single email to multiple addresses.
- Run a program.
- Copy a message to a public folder.



Content filtering rules

☑ Enable rules processing engine

When active, the content filtering system will test all new messages using the rules specified below and perform the requested action if a match is made.

Existing content filter rules

☑ Message/Partial vulnerability [Move to bad message queue]
☑ IFRAME vulnerability [Move to bad message queue]

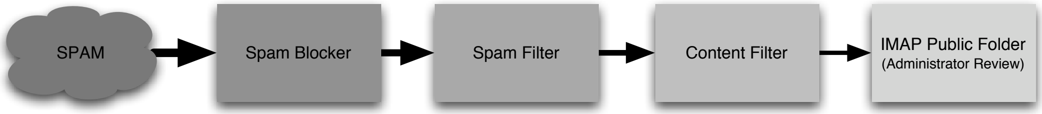
Click the checkbox to the left of each rule to enable/disable it.
Rule Description: Message/Partial vulnerability ... (Enabled)

Apply this rule to messages in the LOCAL & REMOTE queue

If the message has an attachment with a CONTENT-TYPE of 'message/parti
...then send note "to <postmaster@$PRIMARYDOMAIN$>","from <MDaemo
and move message to bad message directory

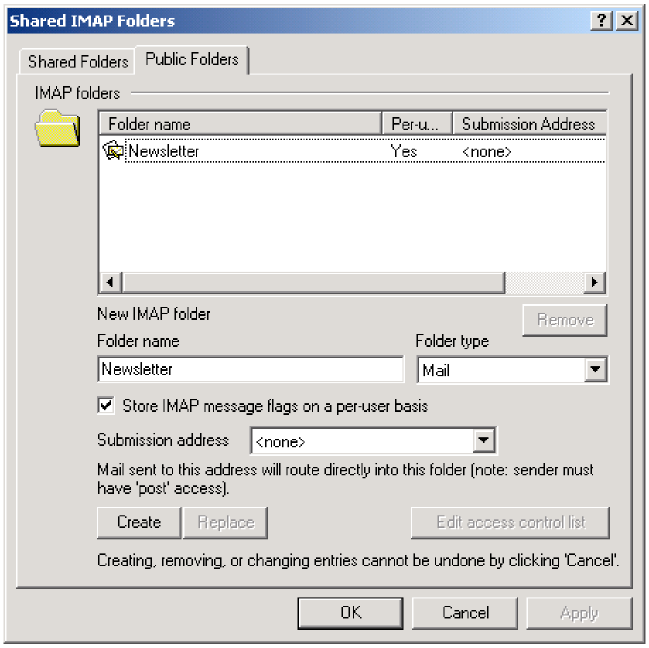
IMAP Public Folders

IMAP public folders enable the sharing of email and attachments. They are part of the *Internet Message Access Protocol*, also known as IMAP.



IMAP is an industry standard protocol for processing email. An IMAP email server stores and keeps email messages for recurring user access. The IMAP account holder can read messages, move them into other folders on the server or copy them to shared folders for access by others, as examples. The account holder can access the same email from any computer with an IMAP client. Because of this, the same email is available at work, at home, from a wireless notebook computer on the road or from a web email client at a computer cafe.

For the purposes of antispam, public folders are useful for collecting spam messages. They are also useful for enabling users to identify spam and legitimate messages for the Bayesian filter.



Shared IMAP Folders

Shared Folders | Public Folders

IMAP folders

Folder name	Per-u...	Submission Address
Newsletter	Yes	<none>

New IMAP folder

Folder name: Newsletter

Folder type: Mail

☑ Store IMAP message flags on a per-user basis

Submission address: <none>

Mail sent to this address will route directly into this folder (note: sender must have 'post' access).

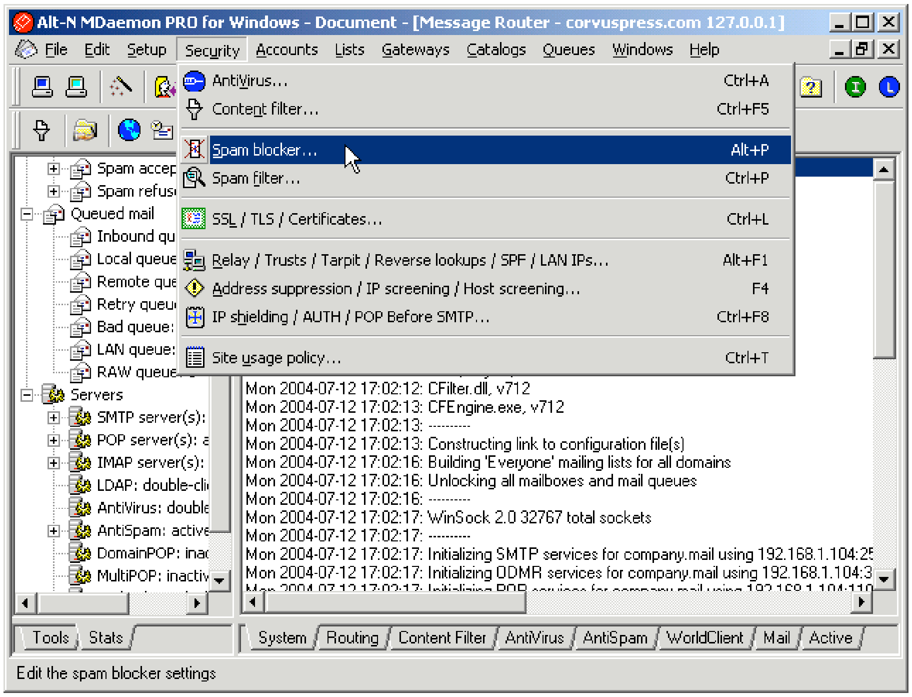
Creating, removing, or changing entries cannot be undone by clicking 'Cancel'.

Step-by-Step Instructions for Configuring MDaemon AntiSpam

Check Spam Blocker

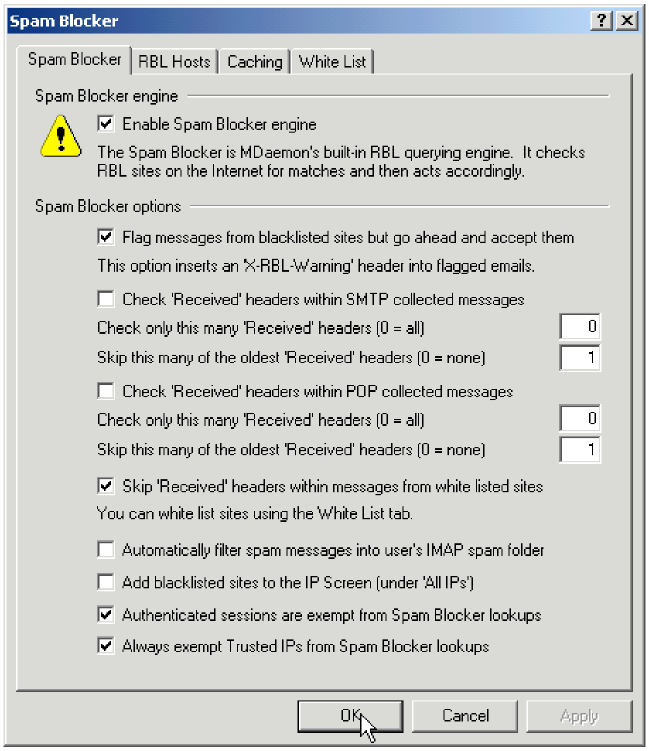
The defaults for the Spam Blocker are very effective. The Spam Blocker is enabled in MDaemon by default. You should check to make sure the Spam Blocker is enabled.

The instructions start on the main screen of the MDaemon administration user interface.


Alt-N MDaemon PRO for Windows - Document - [Message Router - corvuspress.com 127.0.0.1]
File Edit Setup Security Accounts Lists Gateways Catalogs Queues Windows Help
AntiVirus... Ctrl+A
Content filter... Ctrl+F5
Spam blocker... Alt+P
Spam filter... Ctrl+P
SSL / TLS / Certificates... Ctrl+L
Relay / Trusts / Tarpit / Reverse lookups / SPF / LAN IPs... Alt+F1
Address suppression / IP screening / Host screening... F4
IP shielding / AUTH / POP Before SMTP... Ctrl+F8
Site usage policy... Ctrl+T
Spam accep
Spam refus
Queued mail
Inbound qu
Local queue
Remote que
Retry queu
Bad queue:
LAN queue:
RAW queue
Servers
SMTP server(s):
POP server(s): a
IMAP server(s):
LDAP: double-cli
AntiVirus: double
AntiSpam: active
DomainPOP: inac
MultiPOP: inactiv
Tools Stats
System Routing Content Filter AntiVirus AntiSpam WorldClient Mail Active
Edit the spam blocker settings

```
Mon 2004-07-12 17:02:12: CFilter.dll, v712
Mon 2004-07-12 17:02:13: CFEngine.exe, v712
Mon 2004-07-12 17:02:13: ---------
Mon 2004-07-12 17:02:13: Constructing link to configuration file(s)
Mon 2004-07-12 17:02:16: Building 'Everyone' mailing lists for all domains
Mon 2004-07-12 17:02:16: Unlocking all mailboxes and mail queues
Mon 2004-07-12 17:02:16: ---------
Mon 2004-07-12 17:02:17: WinSock 2.0 32767 total sockets
Mon 2004-07-12 17:02:17: ---------
Mon 2004-07-12 17:02:17: Initializing SMTP services for company.mail using 192.168.1.104:25
Mon 2004-07-12 17:02:17: Initializing ODMR services for company.mail using 192.168.1.104:3
Mon 2004-07-12 17:02:17: Initializing POP services for company.mail using 192.168.1.104:110
```

1. Use the *Security > Spam blocker...* command. This displays the Spam Blocker dialog.



Spam Blocker engine

☑ Enable Spam Blocker engine

The Spam Blocker is MDaemon's built-in RBL querying engine. It checks RBL sites on the Internet for matches and then acts accordingly.

Spam Blocker options

☑ Flag messages from blacklisted sites but go ahead and accept them

This option inserts an 'X-RBL-Warning' header into flagged emails.

☐ Check 'Received' headers within SMTP collected messages

Check only this many 'Received' headers (0 = all) 0

Skip this many of the oldest 'Received' headers (0 = none) 1

☐ Check 'Received' headers within POP collected messages

Check only this many 'Received' headers (0 = all) 0

Skip this many of the oldest 'Received' headers (0 = none) 1

☑ Skip 'Received' headers within messages from white listed sites

You can white list sites using the White List tab.

☐ Automatically filter spam messages into user's IMAP spam folder

☐ Add blacklisted sites to the IP Screen (under 'All IPs')

☑ Authenticated sessions are exempt from Spam Blocker lookups

☑ Always exempt Trusted IPs from Spam Blocker lookups

2. Select the **Spam Blocker** tab.
3. Check the settings on this tab. The spam blocker engine should be enabled. The other settings should be those that fit the needs of your organization—in most applications these are the defaults. The other tabs on this dialog are:
   - *RBL Hosts* where you enter the Internet addresses of the black lists you want to use.
   - *Caching* for use if you have a dialup email server and want to store black list look up results "off-line" for a specified period of time.
   - *White List* where you can enter the email addresses you want to always exclude from black list processing.
4. Use the **OK** button to exit from the **Spam Blocker** dialog.

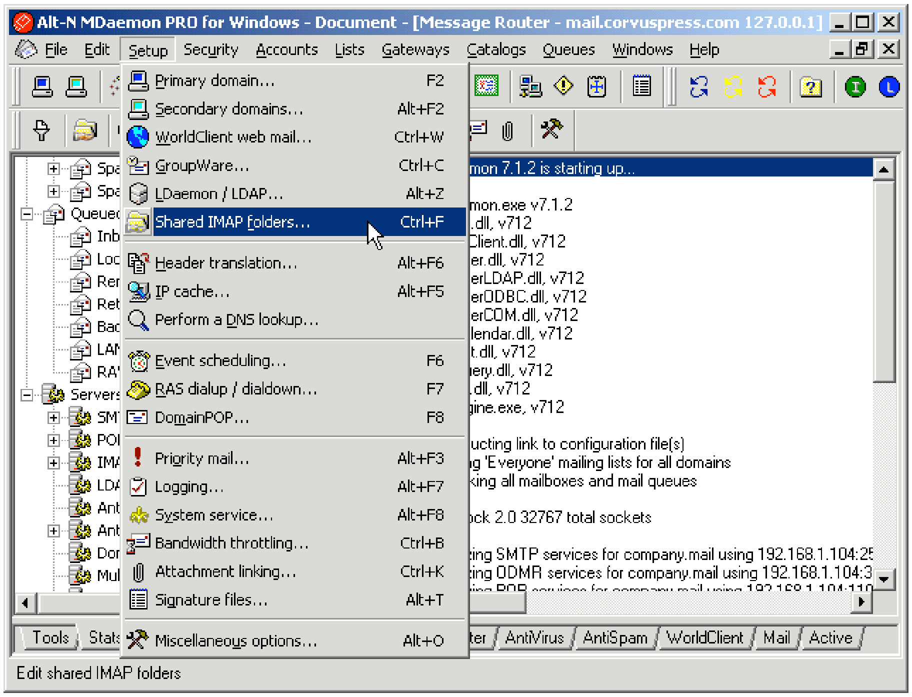
Create Public Folders

These instructions show how to create public folders for:

- centralizing the collection of spam for administrative review.
- collecting “learning” samples of spam and legitimate messages submitted by users to the Bayesian filter.

The instructions show how to create the folders and apply access permissions to the folders. You first create a root folder, then add sub folders for collecting spam and managing messages for the Bayesian filter learning samples.

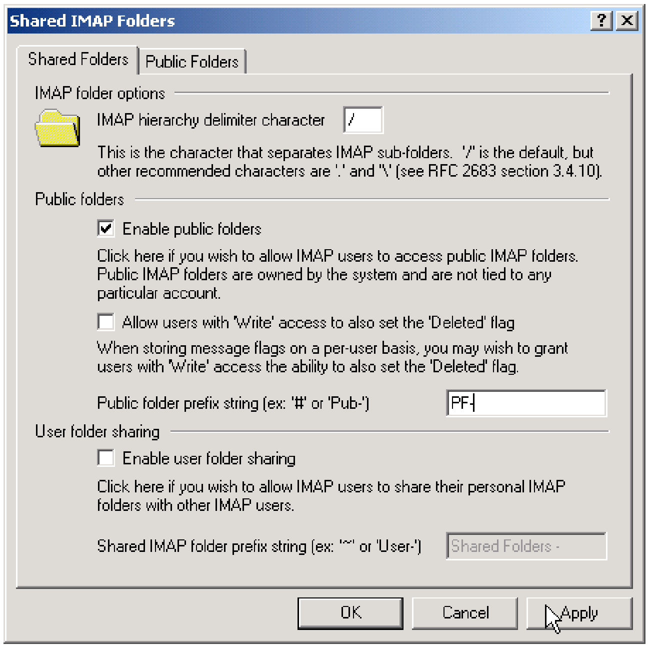
The instructions start on the main screen of the MDaemon administration user interface.



```
mon 7.1.2 is starting up...

mon.exe v7.1.2
.dll, v712
Client.dll, v712
er.dll, v712
erLDAP.dll, v712
erODBC.dll, v712
erCOM.dll, v712
lendar.dll, v712
t.dll, v712
iery.dll, v712
.dll, v712
gine.exe, v712

ucting link to configuration file(s)
g 'Everyone' mailing lists for all domains
king all mailboxes and mail queues

ock 2.0 32767 total sockets

ting SMTP services for company.mail using 192.168.1.104:25
ting ODMR services for company.mail using 192.168.1.104:3
```

Edit shared IMAP folders

1. Use the **Setup > Shared IMAP folders** command. This displays the **Shared IMAP Folders** dialog.



Shared IMAP Folders

Shared Folders | Public Folders

IMAP folder options

IMAP hierarchy delimiter character: /

This is the character that separates IMAP sub-folders. '/' is the default, but other recommended characters are '.' and '\' (see RFC 2683 section 3.4.10).

Public folders

☑ Enable public folders

Click here if you wish to allow IMAP users to access public IMAP folders. Public IMAP folders are owned by the system and are not tied to any particular account.

☐ Allow users with 'Write' access to also set the 'Deleted' flag

When storing message flags on a per-user basis, you may wish to grant users with 'Write' access the ability to also set the 'Deleted' flag.

Public folder prefix string (ex: '#' or 'Pub-'): PF-

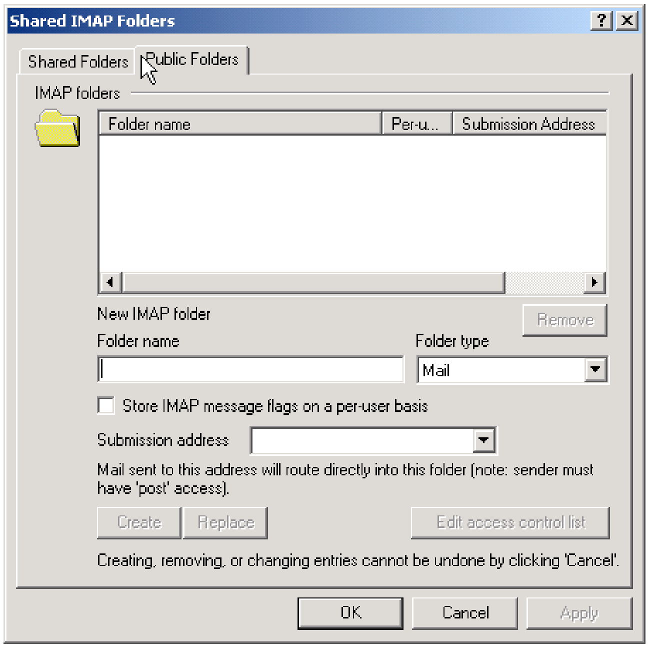
User folder sharing

☐ Enable user folder sharing

Click here if you wish to allow IMAP users to share their personal IMAP folders with other IMAP users.

Shared IMAP folder prefix string (ex: '~' or 'User-'): Shared Folders -

2. Activate the **Enable public folders** check box.
3. Enter a short prefix, such as # or PF- for **Public folder prefix string**
4. Use the **Apply** button.



Shared IMAP Folders

Shared Folders | Public Folders

IMAP folders

Folder name	Per-u...	Submission Address

New IMAP folder

Folder name:

Folder type: Mail

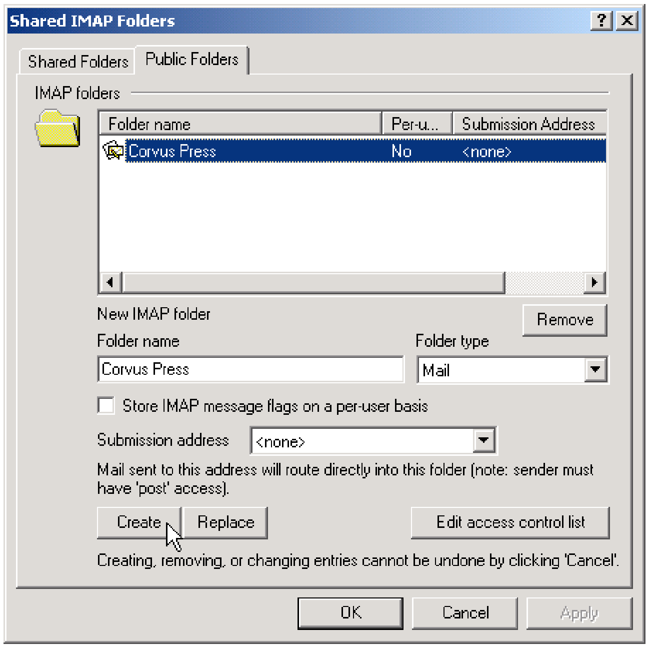
☐ Store IMAP message flags on a per-user basis

Submission address:

Mail sent to this address will route directly into this folder (note: sender must have 'post' access).

Creating, removing, or changing entries cannot be undone by clicking 'Cancel'.

5. Select the **Public Folders** tab. This tab is for adding, changing and deleting IMAP Public Folders. You manage access permissions to the public folders by using the **Edit access control list** button. (The Alt-N web site has a white paper—*Public Folders Concepts and Applications*—explaining IMAP Public Folders.)



Folder name	Per-u...	Submission Address
Corvus Press	No	<none>

New IMAP folder

Folder name: Corvus Press

Folder type: Mail

☐ Store IMAP message flags on a per-user basis

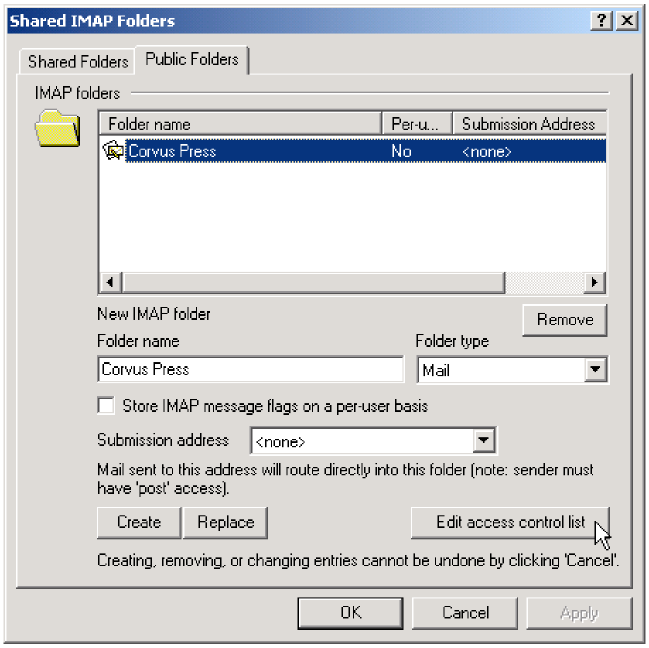
Submission address: <none>

Mail sent to this address will route directly into this folder (note: sender must have 'post' access).

Creating, removing, or changing entries cannot be undone by clicking 'Cancel'.

One way to organize public folders is under a “root” folder named for a department or domain, for example. Sub folders of the root folder inherit the access permissions of the root. The access permissions can be edited for each sub folder.

6. Type the `name of the root folder` for **Folder name** (in this example **Corvus Press**) and use the **Create** button.



Folder name	Per-u...	Submission Address
Corvus Press	No	<none>

New IMAP folder

Folder name: Corvus Press

Folder type: Mail

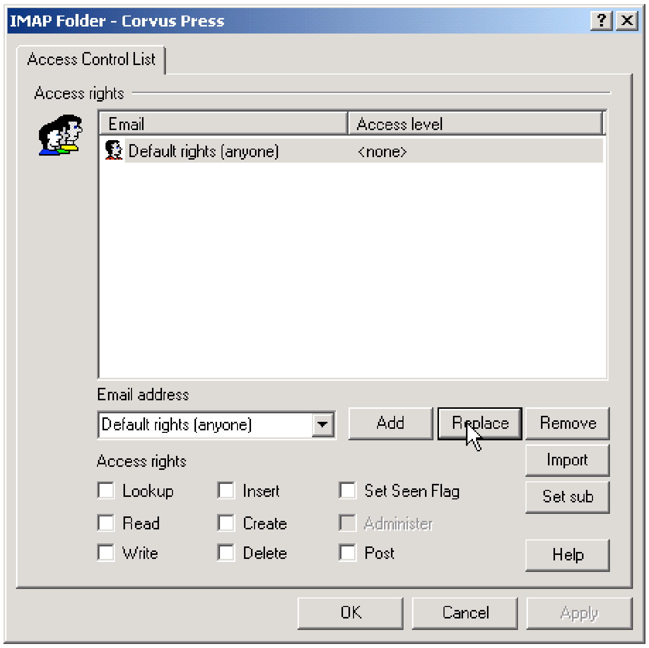
☐ Store IMAP message flags on a per-user basis

Submission address: <none>

Mail sent to this address will route directly into this folder (note: sender must have 'post' access).

Creating, removing, or changing entries cannot be undone by clicking 'Cancel'.

7. Select from the **IMAP folders** list the folder you just created and use the **Edit access control list** button.



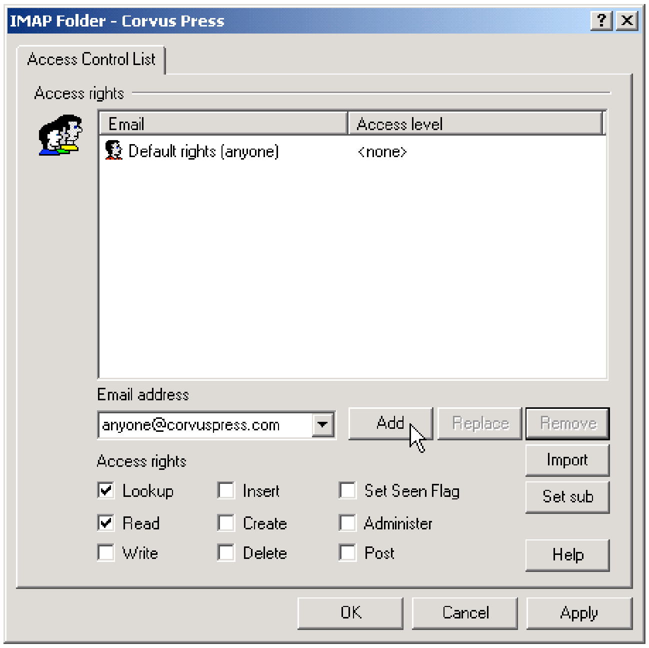
Email	Access level
Default rights (anyone)	<none>

Email address: Default rights (anyone)

Access rights

□ Lookup □ Insert □ Set Seen Flag
□ Read □ Create □ Administer
□ Write □ Delete □ Post

8. Select **Default rights (anyone)** from the list, uncheck all *Access Rights* and use the **Replace** button. This prevents global access to your folders.



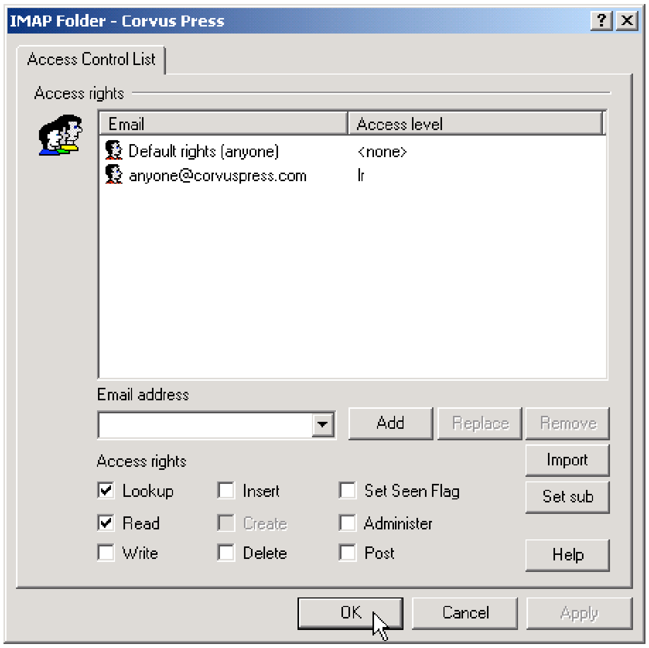
Email	Access level
Default rights (anyone)	<none>

Email address: anyone@corvuspress.com

Access rights

☑ Lookup □ Insert □ Set Seen Flag
☑ Read □ Create □ Administer
□ Write □ Delete □ Post

9. Type `anyone@yourdomain` (where *yourdomain* is your domain), activate the **Lookup** and **Read** *Access Rights* check boxes and use the **Add** button. This provides read access to the public folder for all MDaemon users in your domain.



Email	Access level
Default rights (anyone)	<none>
anyone@corvuspress.com	lr

Email address:

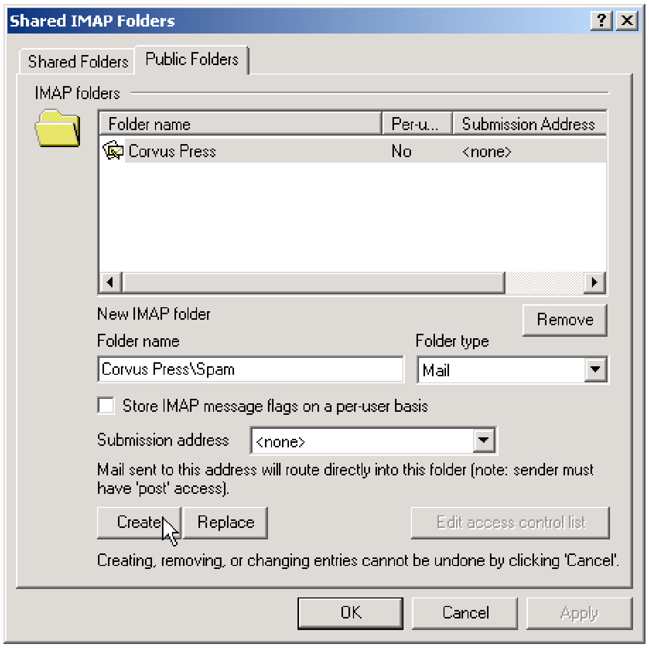
Access rights

☑ Lookup □ Insert □ Set Seen Flag

☑ Read □ Create □ Administer

□ Write □ Delete □ Post

10. Use the **OK** button. This redisplays the **Public Folders** tab of the **Shared IMAP Folders** dialog.



Folder name	Per-u...	Submission Address
Corvus Press	No	<none>

Folder name: Corvus Press\Spam

Folder type: Mail

□ Store IMAP message flags on a per-user basis

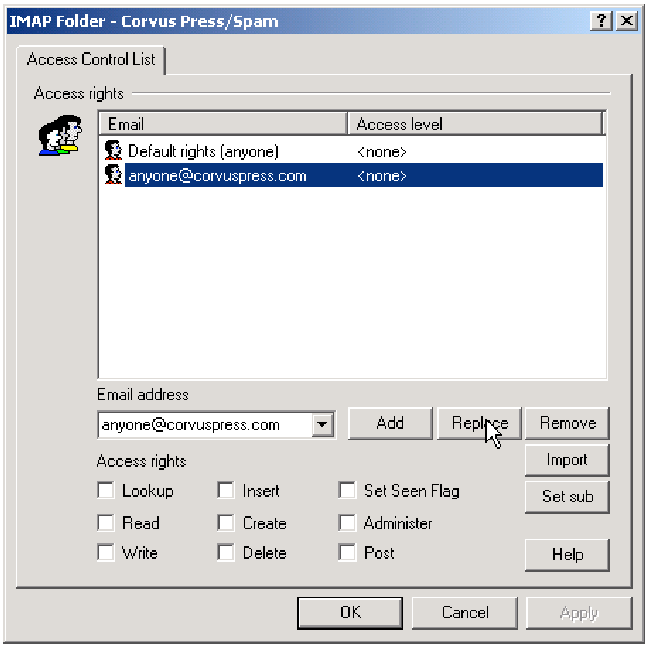
Submission address: <none>

Mail sent to this address will route directly into this folder (note: sender must have 'post' access).

Creating, removing, or changing entries cannot be undone by clicking 'Cancel'.

11. Type `name of the root folder/` Spam for **Folder name** (in this example **Corvus Press/ Spam**) and use the **Create** button.

12. Select from the **IMAP folders** list the folder you just created and use the **Edit access control list** button.



IMAP Folder - Corvus Press/Spam

Access Control List

Access rights

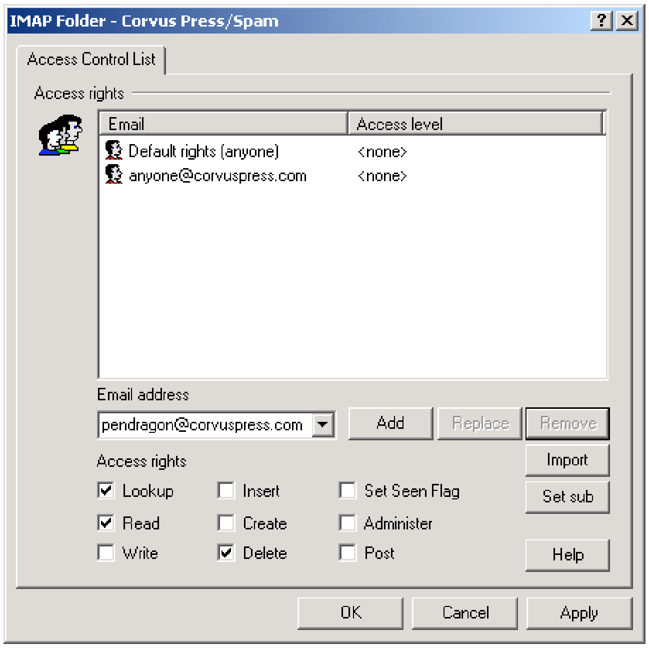
Email	Access level
Default rights (anyone)	<none>
anyone@corvuspress.com	<none>

Email address: anyone@corvuspress.com

Access rights

□ Lookup □ Insert □ Set Seen Flag
□ Read □ Create □ Administer
□ Write □ Delete □ Post

13. Select from the *Access rights* list **anyone@*yourdomain***, deactivate all *Access Rights* and use the **Replace** button. This removes access for everyone in the domain.



IMAP Folder - Corvus Press/Spam

Access Control List

Access rights

Email	Access level
Default rights (anyone)	<none>
anyone@corvuspress.com	<none>

Email address: pendragon@corvuspress.com

Access rights

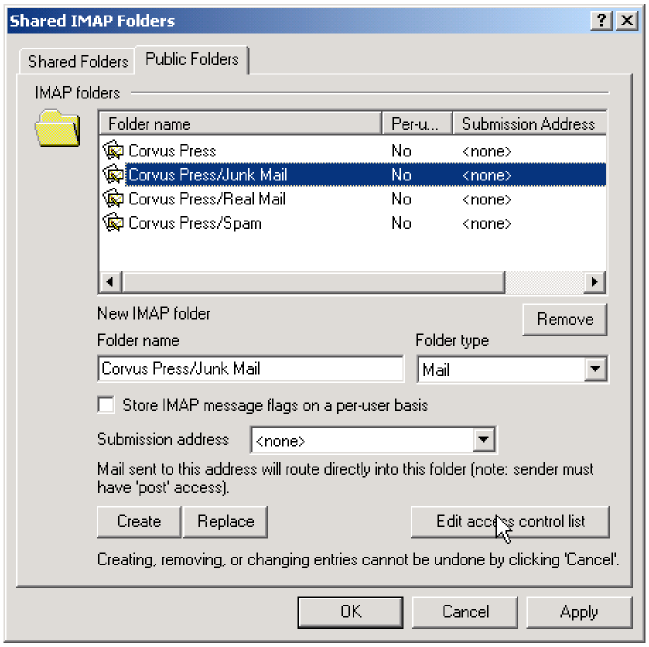
☑ Lookup □ Insert □ Set Seen Flag
☑ Read □ Create □ Administer
□ Write ☑ Delete □ Post

14. Select from the *Email address* list the address of the person to review the messages (pendragon@corvuspress.com in this example) labeled as spam, activate the **Lookup**, **Read** and **Delete** access rights check boxes and use the **Add** button. This enables access for the person who reviews the messages. More than one person can be given this access.

15. Add any other users to the access list.

16. Use the **OK** button. This redisplays the **Public Folders** tab of the **Shared IMAP Folders** dialog.

17. Add these two public folders to your domain:
    - *name of the root folder/**Real Mail***
    - *name of the root folder/**Junk Mail***

Folder name	Per-u...	Submission Address
Corvus Press	No	<none>
Corvus Press/Junk Mail	No	<none>
Corvus Press/Real Mail	No	<none>
Corvus Press/Spam	No	<none>

    Folder name: Corvus Press/Junk Mail
    Folder type: Mail

    ☐ Store IMAP message flags on a per-user basis

    Submission address: <none>

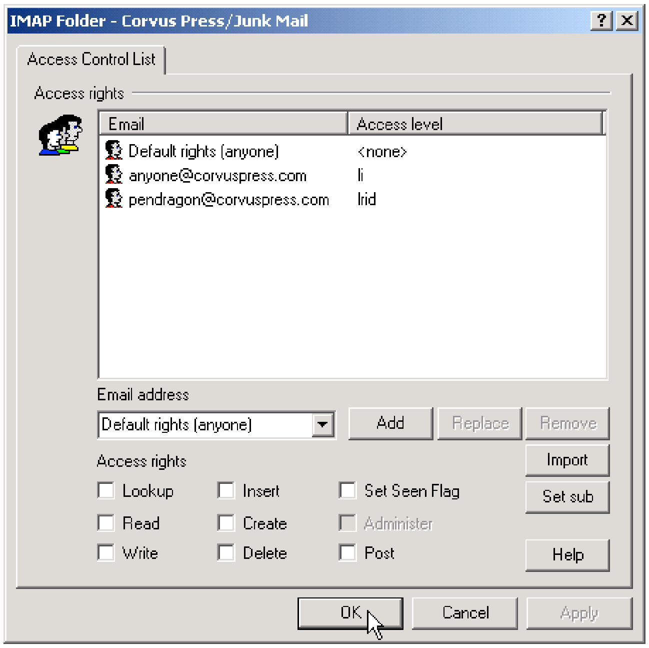
    Mail sent to this address will route directly into this folder (note: sender must have 'post' access).

    Creating, removing, or changing entries cannot be undone by clicking 'Cancel'.

    These two folders are for users to identify spam and legitimate messages for the Bayesian filter. Users do this by copying spam messages and legitimate messages to the IMAP public folders. The Bayesian filter processes these messages to "learn" the differences between junk mail and real mail, as defined by the users of your email server. Both IMAP and POP account holders can add messages to these public folders.

    POP account users can copy messages to these folders by mailing the messages as attachments to **SpamLearn@*yourdomain*** and **HamLearn@*yourdomain***. For example, these email addresses could be **SpamLearn@corvuspress.com** and **HamLearn@corvuspress.com**.

18. Select the **Real Mail** and **Junk Mail** folders in turn, then use the **Edit access control list** button



Email	Access level
Default rights (anyone)	<none>
anyone@corvuspress.com	li
pendragon@corvuspress.com	lrid

Email address: Default rights (anyone)

Access rights

□ Lookup □ Insert □ Set Seen Flag
□ Read □ Create □ Administer
□ Write □ Delete □ Post

19. Set these access permissions for both the **Real Mail** and **Junk Mail** folders:

    Default rights (anyone) <none>

    anyone@*yourdomain* Lookup, Insert

    With these settings, general users (anyone) can add messages to the public folders cannot see the contents of the folders.

    your email administrator Lookup, Read, Insert, Delete

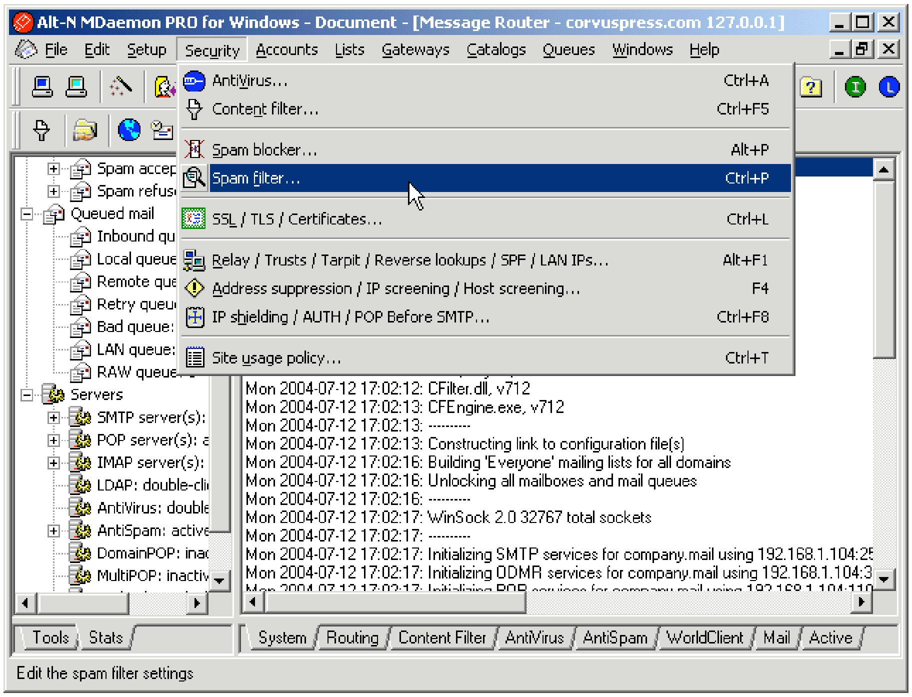
20. Use the **OK** button. This redisplays the **Public Folders** tab of the **Shared IMAP Folders** dialog.

21. Use the **OK** button to exit from the **Shared IMAP Folders** dialog.

Configure Spam Filter

These instructions show how to configure the Spam Filter, including general settings, Heuristic Filtering and Bayesian learning.

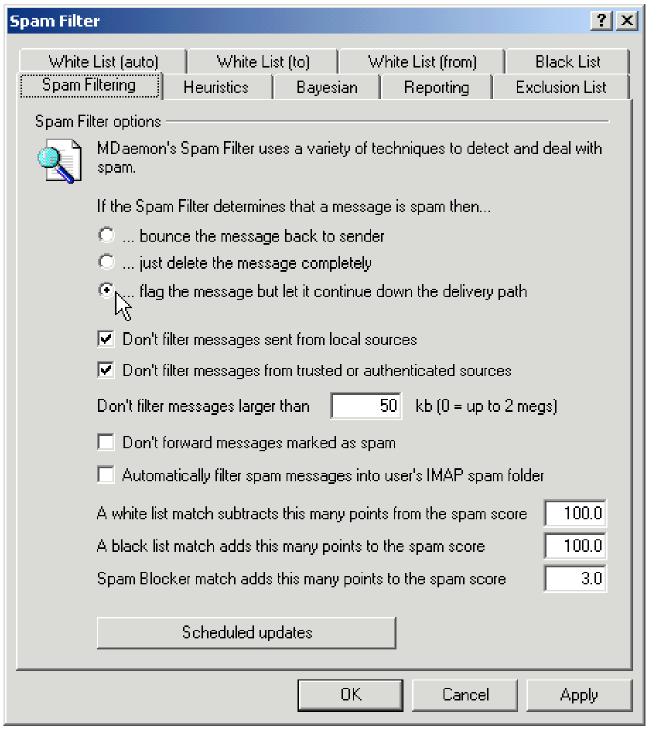
The instructions start on the main screen of the MDaemon administration user interface.


Alt-N MDaemon PRO for Windows - Document - [Message Router - corvuspress.com 127.0.0.1]
File Edit Setup Security Accounts Lists Gateways Catalogs Queues Windows Help
AntiVirus... Ctrl+A
Content filter... Ctrl+F5
Spam blocker... Alt+P
Spam filter... Ctrl+P
SSL / TLS / Certificates... Ctrl+L
Relay / Trusts / Tarpit / Reverse lookups / SPF / LAN IPs... Alt+F1
Address suppression / IP screening / Host screening... F4
IP shielding / AUTH / POP Before SMTP... Ctrl+F8
Site usage policy... Ctrl+T
Spam accep
Spam refus
Queued mail
Inbound qu
Local queue
Remote que
Retry queu
Bad queue:
LAN queue:
RAW queue
Servers
SMTP server(s):
POP server(s): a
IMAP server(s):
LDAP: double-cli
AntiVirus: double
AntiSpam: active
DomainPOP: inac
MultiPOP: inactiv
Tools Stats
System Routing Content Filter AntiVirus AntiSpam WorldClient Mail Active

```
Mon 2004-07-12 17:02:12: CFilter.dll, v712
Mon 2004-07-12 17:02:13: CFEngine.exe, v712
Mon 2004-07-12 17:02:13: ---------
Mon 2004-07-12 17:02:13: Constructing link to configuration file(s)
Mon 2004-07-12 17:02:16: Building 'Everyone' mailing lists for all domains
Mon 2004-07-12 17:02:16: Unlocking all mailboxes and mail queues
Mon 2004-07-12 17:02:16: ---------
Mon 2004-07-12 17:02:17: WinSock 2.0 32767 total sockets
Mon 2004-07-12 17:02:17: ---------
Mon 2004-07-12 17:02:17: Initializing SMTP services for company.mail using 192.168.1.104:25
Mon 2004-07-12 17:02:17: Initializing ODMR services for company.mail using 192.168.1.104:3
Mon 2004-07-12 17:02:17: Initializing POP services for company.mail using 192.168.1.104:110
```

Edit the spam filter settings

1. Use the *Security > Spam Filter...* command. This displays the Spam Filter dialog.


Spam Filter
White List (auto) White List (to) White List (from) Black List
Spam Filtering Heuristics Bayesian Reporting Exclusion List
Scheduled updates
OK Cancel Apply

Spam Filter options

MDaemon's Spam Filter uses a variety of techniques to detect and deal with spam.

If the Spam Filter determines that a message is spam then...

○ ... bounce the message back to sender
○ ... just delete the message completely
● ... flag the message but let it continue down the delivery path

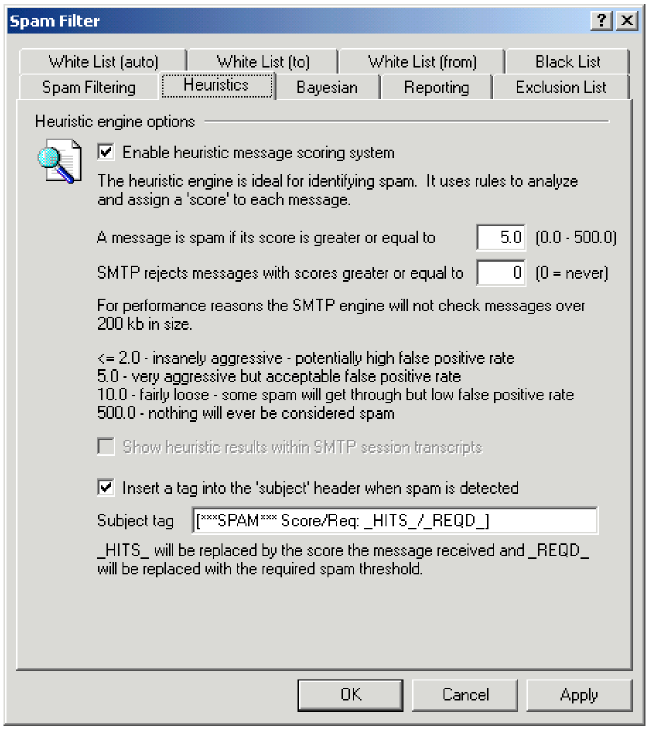
☑ Don't filter messages sent from local sources
☑ Don't filter messages from trusted or authenticated sources

Don't filter messages larger than 50 kb (0 = up to 2 megs)

□ Don't forward messages marked as spam
□ Automatically filter spam messages into user's IMAP spam folder

A white list match subtracts this many points from the spam score 100.0
A black list match adds this many points to the spam score 100.0
Spam Blocker match adds this many points to the spam score 3.0

2. Select the **Spam Filtering** tab.
3. Choose the **. . . flag the message but let it continue down the delivery path** option. The other settings should be those that fit the needs of your organization—in most applications these are the defaults.



Heuristic engine options

☑ Enable heuristic message scoring system

The heuristic engine is ideal for identifying spam. It uses rules to analyze and assign a 'score' to each message.

A message is spam if its score is greater or equal to 5.0 (0.0 - 500.0)

SMTP rejects messages with scores greater or equal to 0 (0 = never)

For performance reasons the SMTP engine will not check messages over 200 kb in size.

<= 2.0 - insanely aggressive - potentially high false positive rate
5.0 - very aggressive but acceptable false positive rate
10.0 - fairly loose - some spam will get through but low false positive rate
500.0 - nothing will ever be considered spam

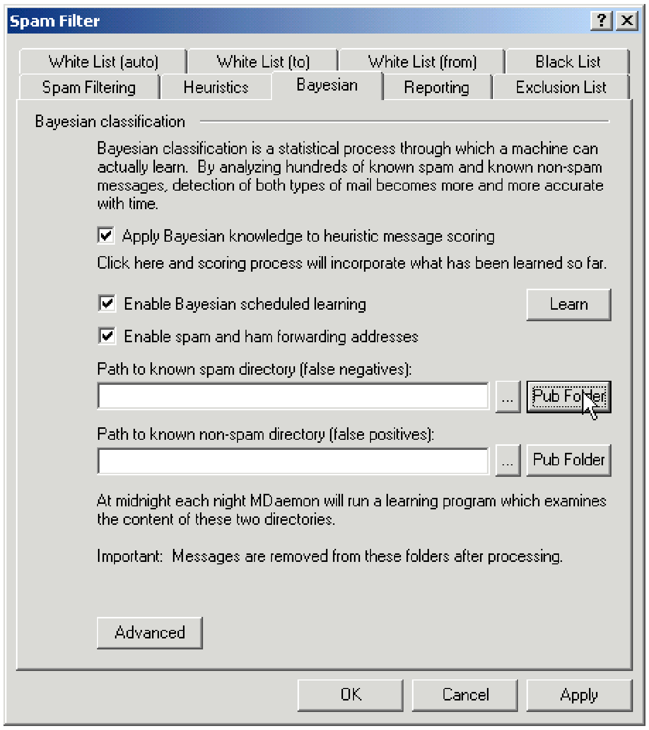
☐ Show heuristic results within SMTP session transcripts

☑ Insert a tag into the 'subject' header when spam is detected

Subject tag [***SPAM*** Score/Req: _HITS_/_REQD_]

HITS will be replaced by the score the message received and _REQD_ will be replaced with the required spam threshold.

4. Select the **Heuristics** tab. Heuristic filtering is enabled in MDaemon by default.
5. Check the settings on this tab. **Enable heuristic message scoring system** should be enabled. The other settings should be those that fit the needs of your organization—in most applications these are the defaults.



Bayesian classification

Bayesian classification is a statistical process through which a machine can actually learn. By analyzing hundreds of known spam and known non-spam messages, detection of both types of mail becomes more and more accurate with time.

☑ Apply Bayesian knowledge to heuristic message scoring

Click here and scoring process will incorporate what has been learned so far.

☑ Enable Bayesian scheduled learning

☑ Enable spam and ham forwarding addresses

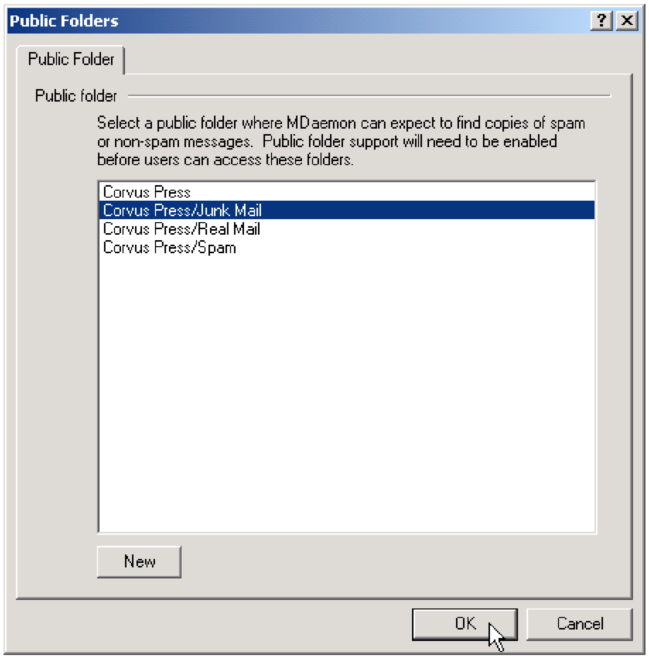
Path to known spam directory (false negatives):

Path to known non-spam directory (false positives):

At midnight each night MDaemon will run a learning program which examines the content of these two directories.

Important: Messages are removed from these folders after processing.

6. Select the **Bayesian** tab.
7. Activate all check boxes on this tab.
8. Use the **Pub Folder** button to select the *spam* Public Folder you created earlier. Using a **Pub Folder** button displays a **Public Folders** dialog.

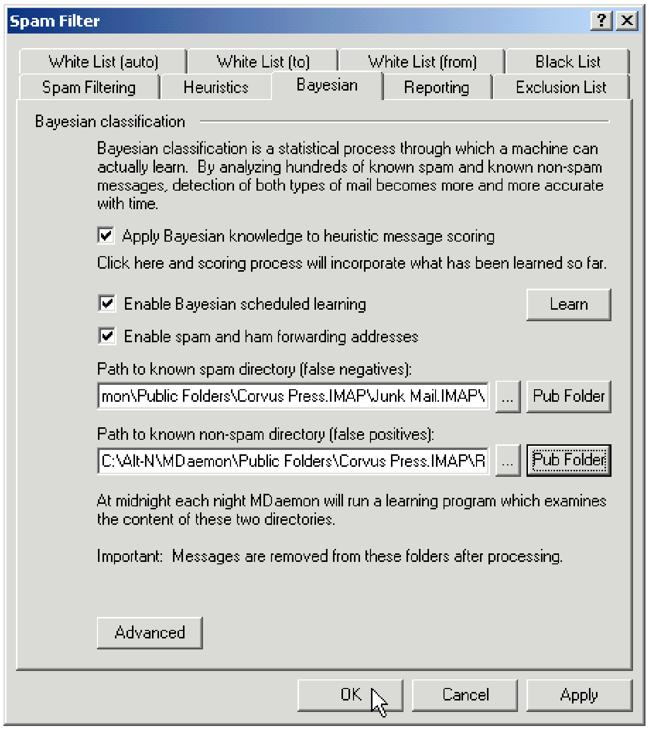


Public folder

Select a public folder where MDaemon can expect to find copies of spam or non-spam messages. Public folder support will need to be enabled before users can access these folders.

Corvus Press
Corvus Press/Junk Mail
Corvus Press/Real Mail
Corvus Press/Spam

9. Select the appropriate public folder for *spam* and use the **OK** button.
10. Repeat steps 8 and 9 for the *non-spam* **Pub Folder** button.



Bayesian classification

Bayesian classification is a statistical process through which a machine can actually learn. By analyzing hundreds of known spam and known non-spam messages, detection of both types of mail becomes more and more accurate with time.

☑ Apply Bayesian knowledge to heuristic message scoring

Click here and scoring process will incorporate what has been learned so far.

☑ Enable Bayesian scheduled learning

☑ Enable spam and ham forwarding addresses

Path to known spam directory (false negatives):
mon\Public Folders\Corvus Press.IMAP\Junk Mail.IMAP\

Path to known non-spam directory (false positives):
C:\Alt-N\MDaemon\Public Folders\Corvus Press.IMAP\R

At midnight each night MDaemon will run a learning program which examines the content of these two directories.

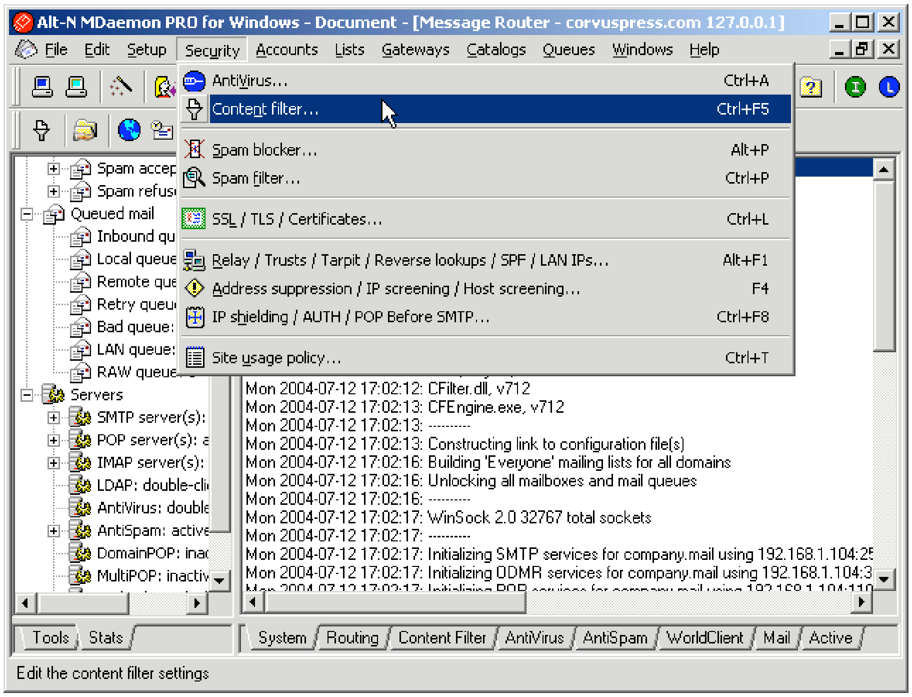
Important: Messages are removed from these folders after processing.

11. Use the **OK** button to exit from the **Spam Filter** dialog.

Create Content Filter for Collecting Spam

These instructions create a content filter for routing all messages flagged as spam into the public folder you created in step 11 on page 13.

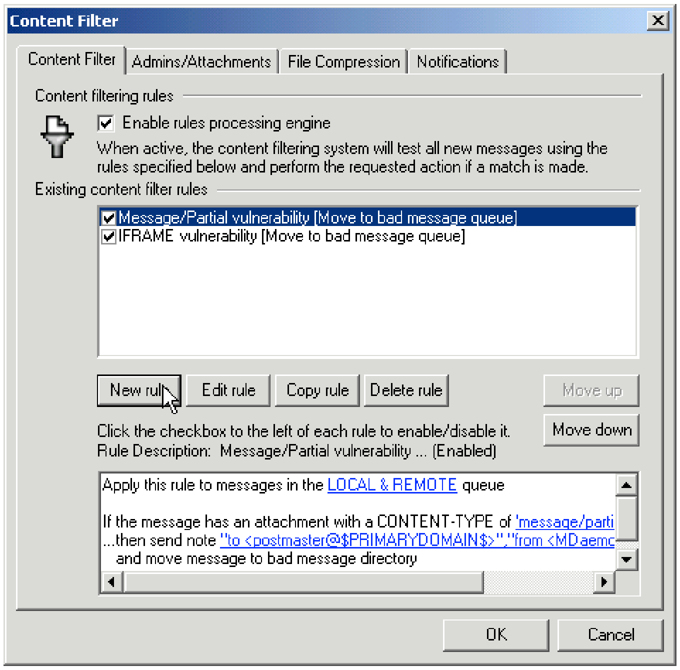
The instructions start on the main screen of the MDaemon administration user interface.


Alt-N MDaemon PRO for Windows - Document - [Message Router - corvuspress.com 127.0.0.1]
File Edit Setup Security Accounts Lists Gateways Catalogs Queues Windows Help
AntiVirus... Ctrl+A
Content filter... Ctrl+F5
Spam blocker... Alt+P
Spam filter... Ctrl+P
SSL / TLS / Certificates... Ctrl+L
Relay / Trusts / Tarpit / Reverse lookups / SPF / LAN IPs... Alt+F1
Address suppression / IP screening / Host screening... F4
IP shielding / AUTH / POP Before SMTP... Ctrl+F8
Site usage policy... Ctrl+T
Spam accep
Spam refus
Queued mail
Inbound qu
Local queue
Remote que
Retry queu
Bad queue:
LAN queue:
RAW queue
Servers
SMTP server(s):
POP server(s): a
IMAP server(s):
LDAP: double-cli
AntiVirus: double
AntiSpam: active
DomainPOP: inac
MultiPOP: inactiv
Tools Stats
System Routing Content Filter AntiVirus AntiSpam WorldClient Mail Active

```
Mon 2004-07-12 17:02:12: CFilter.dll, v712
Mon 2004-07-12 17:02:13: CFEngine.exe, v712
Mon 2004-07-12 17:02:13: ----------
Mon 2004-07-12 17:02:13: Constructing link to configuration file(s)
Mon 2004-07-12 17:02:16: Building 'Everyone' mailing lists for all domains
Mon 2004-07-12 17:02:16: Unlocking all mailboxes and mail queues
Mon 2004-07-12 17:02:16: ----------
Mon 2004-07-12 17:02:17: WinSock 2.0 32767 total sockets
Mon 2004-07-12 17:02:17: ----------
Mon 2004-07-12 17:02:17: Initializing SMTP services for company.mail using 192.168.1.104:25
Mon 2004-07-12 17:02:17: Initializing ODMR services for company.mail using 192.168.1.104:3
Mon 2004-07-12 17:02:17: Initializing POP services for company.mail using 192.168.1.104:110
```

Edit the content filter settings

1. Use the **Security > Content filter...** command. This displays the Content Filter dialog.



☑ Enable rules processing engine

When active, the content filtering system will test all new messages using the rules specified below and perform the requested action if a match is made.

☑ Message/Partial vulnerability [Move to bad message queue]
☑ IFRAME vulnerability [Move to bad message queue]

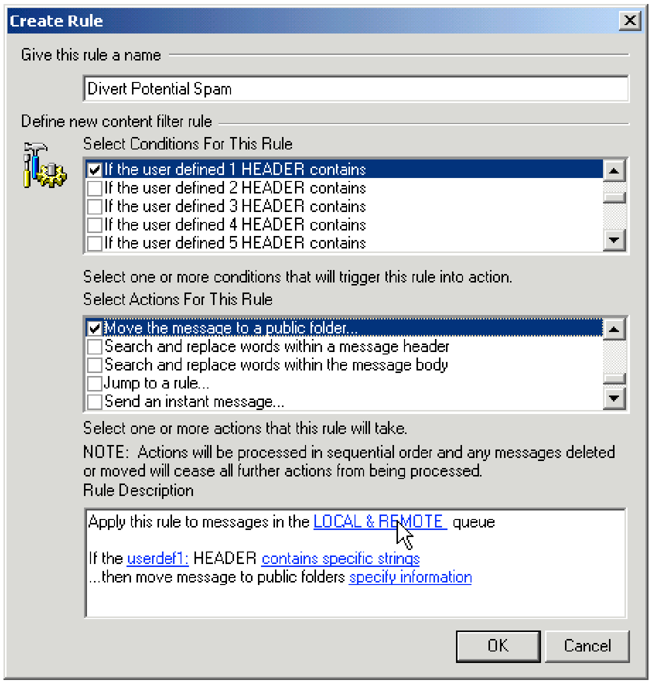
Click the checkbox to the left of each rule to enable/disable it.
Rule Description: Message/Partial vulnerability ... (Enabled)

Apply this rule to messages in the LOCAL & REMOTE queue

If the message has an attachment with a CONTENT-TYPE of 'message/parti
...then send note "to <postmaster@$PRIMARYDOMAIN$>","from <MDaemo
and move message to bad message directory

2. Use the **New rule** button. This displays the **Create Rule** dialog.

The new rule processes local queue messages containing the `X-Spam-Flag` header. A message contains this header if MDaemon antispam has labeled it as spam.



Create Rule

Give this rule a name

Divert Potential Spam

Define new content filter rule

Select Conditions For This Rule

☑ If the user defined 1 HEADER contains
☐ If the user defined 2 HEADER contains
☐ If the user defined 3 HEADER contains
☐ If the user defined 4 HEADER contains
☐ If the user defined 5 HEADER contains

Select one or more conditions that will trigger this rule into action.

Select Actions For This Rule

☑ Move the message to a public folder...
☐ Search and replace words within a message header
☐ Search and replace words within the message body
☐ Jump to a rule...
☐ Send an instant message...

Select one or more actions that this rule will take.

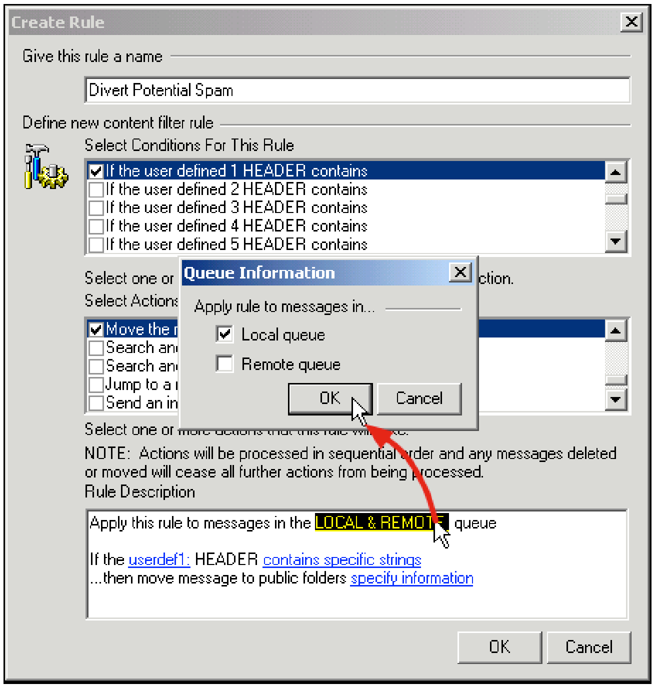
NOTE: Actions will be processed in sequential order and any messages deleted or moved will cease all further actions from being processed.

Rule Description

Apply this rule to messages in the LOCAL & REMOTE queue

If the userdef1: HEADER contains specific strings
...then move message to public folders specify information

3. Type `Divert Potential Spam` into the **Give this rule a name** box.
4. Scroll to and activate **If the user defined 1 HEADER contains** in the **Select Conditions For This Rule** box.
5. Scroll to and activate **Move the message to a public folder. . .** in the **Select Actions For This Rule** box.



Create Rule

Give this rule a name

Divert Potential Spam

Define new content filter rule

Select Conditions For This Rule

☑ If the user defined 1 HEADER contains
☐ If the user defined 2 HEADER contains
☐ If the user defined 3 HEADER contains
☐ If the user defined 4 HEADER contains
☐ If the user defined 5 HEADER contains

Queue Information

Apply rule to messages in...

☑ Local queue
☐ Remote queue

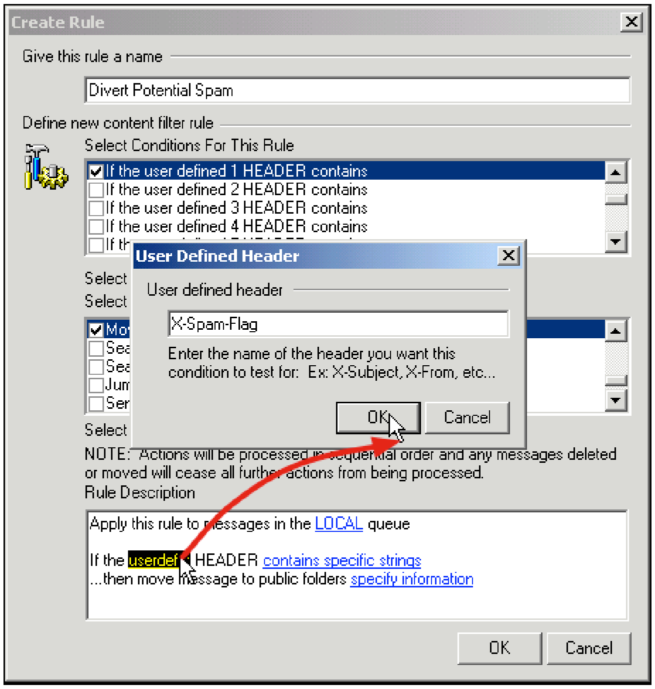
NOTE: Actions will be processed in sequential order and any messages deleted or moved will cease all further actions from being processed.

Rule Description

Apply this rule to messages in the LOCAL & REMOTE queue

If the userdef1: HEADER contains specific strings
...then move message to public folders specify information

6. Click on **Local & Remote** in the **Rule Description** box of the **Create Rule** dialog. This displays a dialog for selecting local and remote queues.
7. Deactivate the **Remote queue** box. Keep the **Local queue** box active. Use the **OK** button.



Create Rule

Give this rule a name

Divert Potential Spam

Define new content filter rule

Select Conditions For This Rule

☑ If the user defined 1 HEADER contains
□ If the user defined 2 HEADER contains
□ If the user defined 3 HEADER contains
□ If the user defined 4 HEADER contains
□ If th

User Defined Header

User defined header

X-Spam-Flag

Enter the name of the header you want this condition to test for: Ex: X-Subject, X-From, etc...

Select
Select
☑ Mo
□ Sea
□ Sea
□ Jun
□ Ser
Select

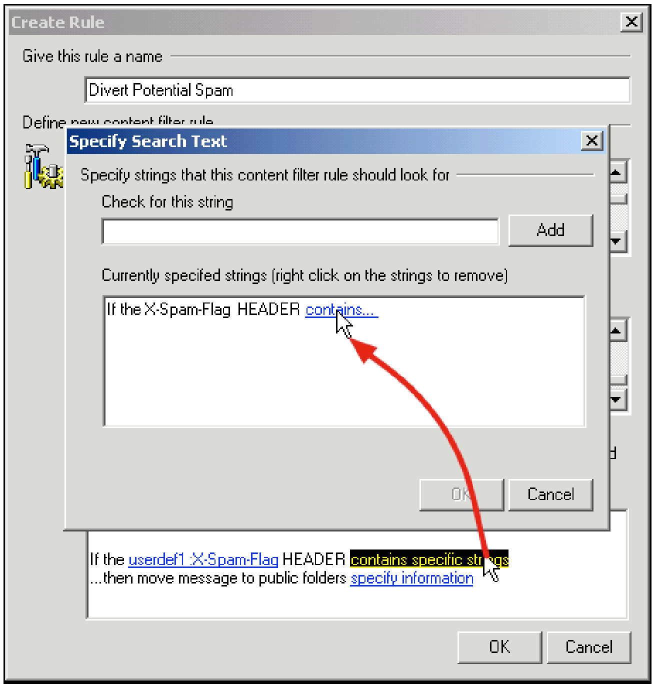
NOTE: Actions will be processed in sequential order and any messages deleted or moved will cease all further actions from being processed.

Rule Description

Apply this rule to messages in the LOCAL queue

If the userdef1 HEADER contains specific strings
...then move message to public folders specify information

8. Click on **userdef1** in the **Rule Description** box of the **Create Rule** dialog. This displays a dialog for entering a user-defined header.
9. Type `X-Spam-Flag` into the **User defined header** box. Use the **OK** button.



Create Rule

Give this rule a name

Divert Potential Spam

Define new content filter rule

Specify Search Text

Specify strings that this content filter rule should look for

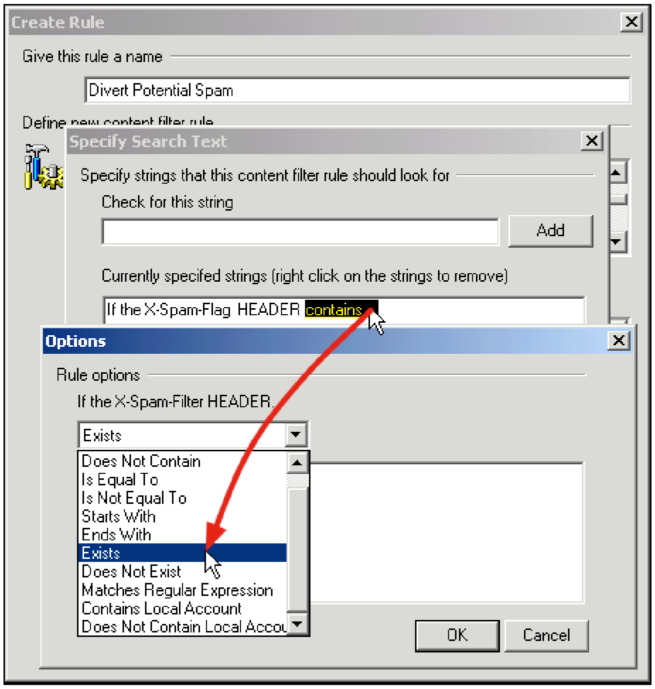
Check for this string

Currently specifed strings (right click on the strings to remove)

If the X-Spam-Flag HEADER contains...

If the userdef1 X-Spam-Flag HEADER contains specific strings
...then move message to public folders specify information

10. Click on **contains specific strings** in the **Rule Description** box of the **Create Rule** dialog. This displays a **Specify Search text** dialog for specifying the string.



Create Rule

Give this rule a name: Divert Potential Spam

Define new content filter rule

Specify Search Text

Specify strings that this content filter rule should look for

Check for this string

Currently specifed strings (right click on the strings to remove)

If the X-Spam-Flag HEADER contains

Options

Rule options

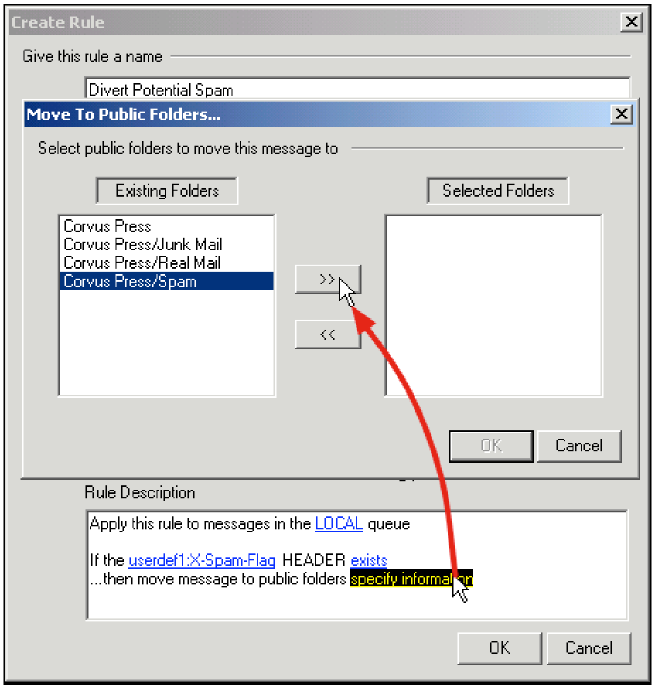
If the X-Spam-Filter HEADER

Exists

11. Click on **contains. . .** in the dialog. This displays an **Options** dialog for selecting content options.

12. Select **Exists** from the drop down list.

13. Use the **OK** button on the **Options** dialog. Use the **OK** button on the **Specify Search text** dialog.



Create Rule

Give this rule a name: Divert Potential Spam

Move To Public Folders...

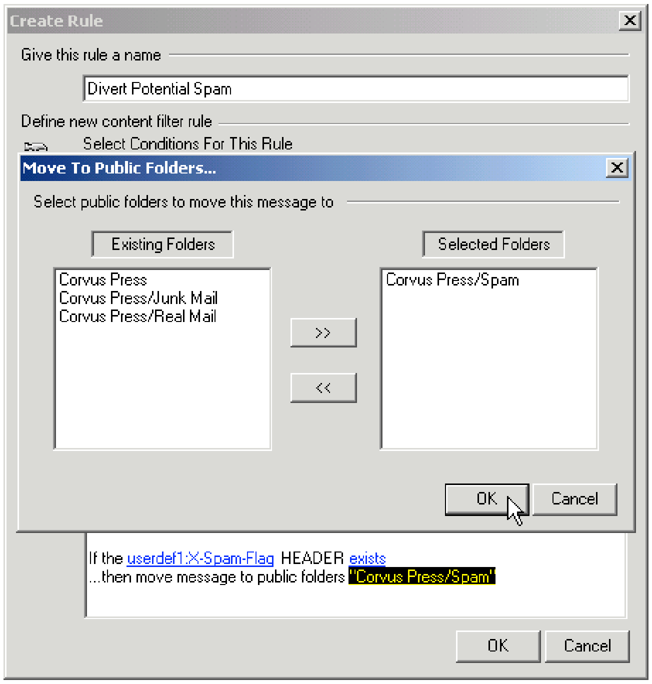
Select public folders to move this message to

Rule Description

Apply this rule to messages in the LOCAL queue

If the userdef1:X-Spam-Flag HEADER exists
...then move message to public folders specify information

14. Click on **specify information** in the **Rule Description** box of the **Create Rule** dialog. This displays a **Move to Public Folders. . .** dialog.
15. Select the public folder you created in step 11 on page 13. This is the public folder for centralizing the collection of spam for administrative review.
16. Use the >> button to choose the selected folder.



Give this rule a name

Divert Potential Spam

Define new content filter rule

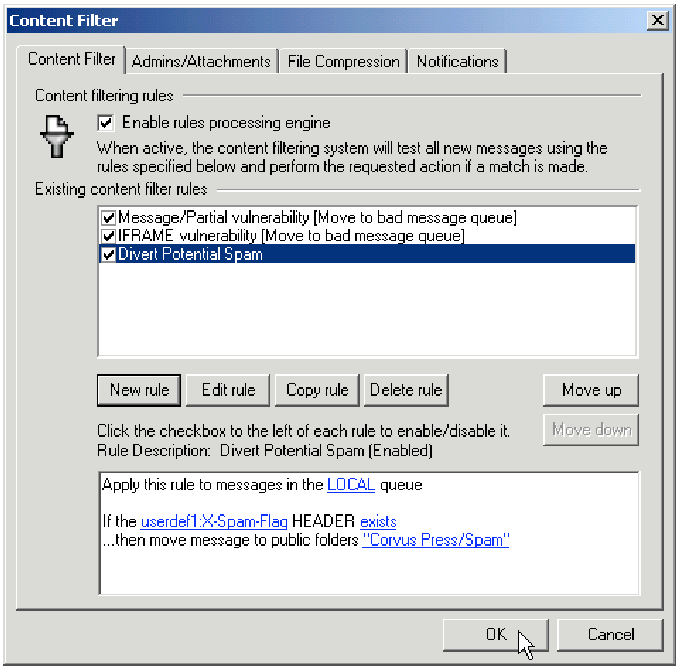
Select public folders to move this message to

Corvus Press
Corvus Press/Junk Mail
Corvus Press/Real Mail

Corvus Press/Spam

If the userdef1:X-Spam-Flag HEADER exists
...then move message to public folders "Corvus Press/Spam"

17. Use the **OK** button on the **Move to Public Folders. . .** dialog.
18. Use the **OK** button on the **Create Rule** dialog.



Content filtering rules

☑ Enable rules processing engine

When active, the content filtering system will test all new messages using the rules specified below and perform the requested action if a match is made.

Existing content filter rules

☑ Message/Partial vulnerability [Move to bad message queue]
☑ IFRAME vulnerability [Move to bad message queue]
☑ Divert Potential Spam

Click the checkbox to the left of each rule to enable/disable it.
Rule Description: Divert Potential Spam (Enabled)

Apply this rule to messages in the LOCAL queue

If the userdef1:X-Spam-Flag HEADER exists
...then move message to public folders "Corvus Press/Spam"

19. Use the **OK** button to exit from the Content Filter.

Using the AntiSpam Configuration

Using the Public Folders for Spam Processing

From the administrator and user points of view, MDaemon has two public folders for processing spam. Both of these were created in step 17 on page 15.

Junk Mail This folder is for spam messages not identified as spam by the antispam tools. When a message is placed in this folder it is processed by Bayesian learning. In this way the next similar message received will be labeled as spam.

Real Mail This folder is for legitimate messages falsely identified as spam by the antispam tools. When a message is placed in this folder it is processed by Bayesian learning. In this way the next similar message received will be passed to its recipient and not labeled as spam.

In addition, the administrator has a third spam-related public folder: Spam. This folder is for messages identified as spam by the antispam tools and routed to the folder by the content filter rule.

Administrator Instructions

Using an IMAP email client, the administrator checks all messages routed to the Spam folder.

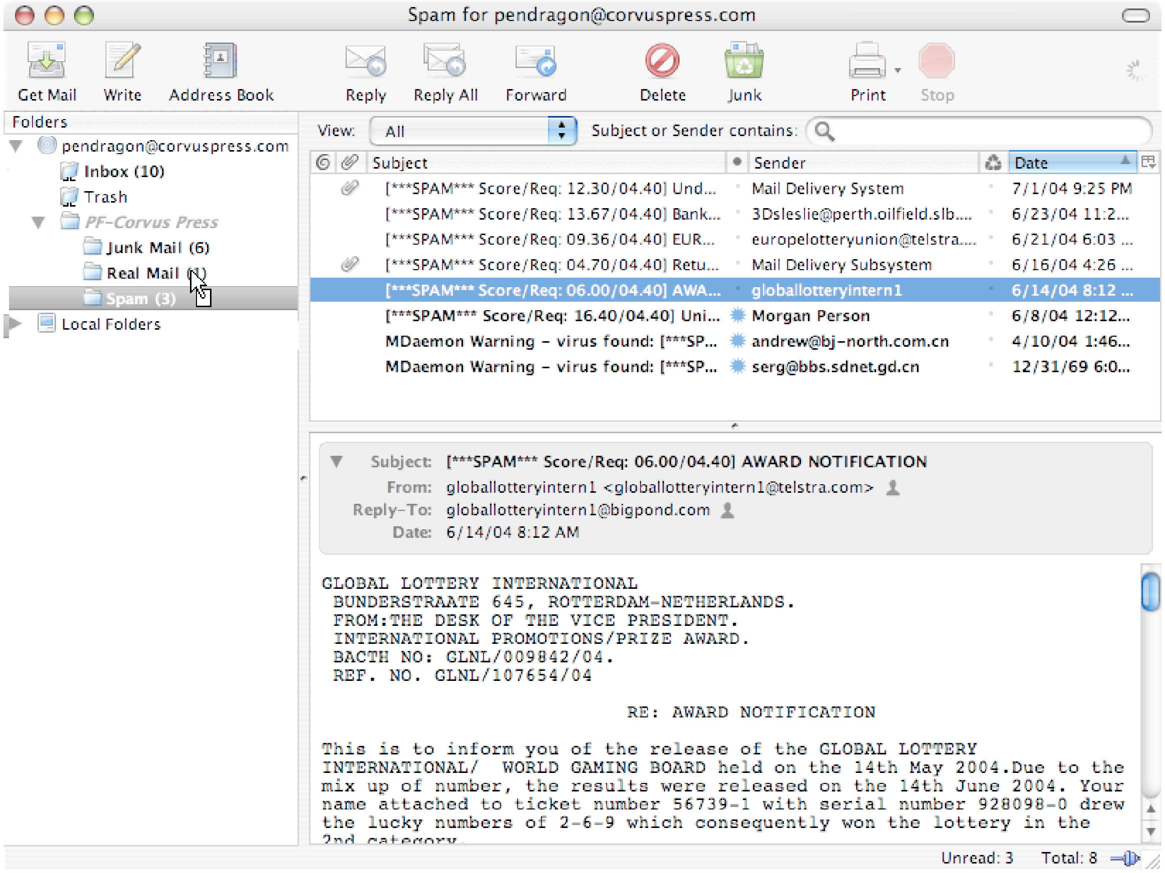
The main purpose is to find messages marked incorrectly as spam.

When such a wrongly-marked message is found, the administrator should:

1. Copy the message to the Real Mail folder.
2. Forward the message to the original recipient.

These functions can be carried out by using an IMAP email client and subscribing to the three public folders used for processing spam.

For example, the administrator can drag and drop mis-labeled messages into the Real Mail folder.

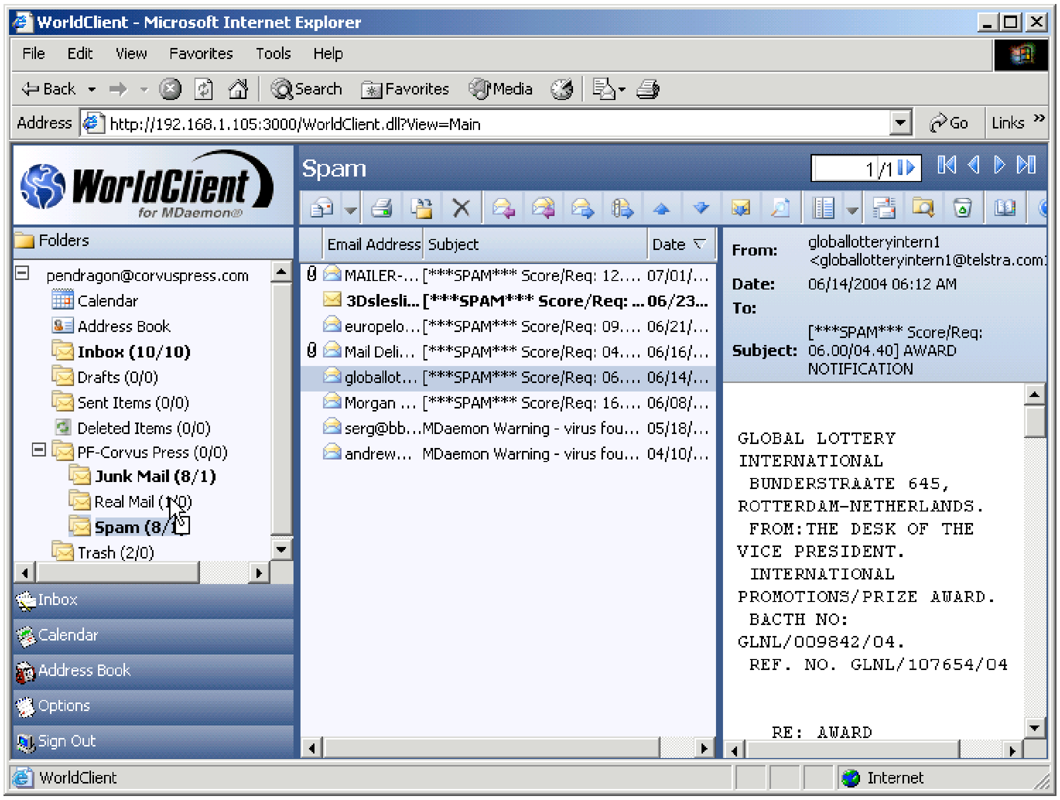


Subject	Sender	Date
[***SPAM*** Score/Req: 12.30/04.40] Und...	Mail Delivery System	7/1/04 9:25 PM
[***SPAM*** Score/Req: 13.67/04.40] Bank...	3Dsleslie@perth.oilfield.slb....	6/23/04 11:2...
[***SPAM*** Score/Req: 09.36/04.40] EUR...	europelotteryunion@telstra....	6/21/04 6:03 ...
[***SPAM*** Score/Req: 04.70/04.40] Retu...	Mail Delivery Subsystem	6/16/04 4:26 ...
[***SPAM*** Score/Req: 06.00/04.40] AWA...	globallotteryintern1	6/14/04 8:12 ...
[***SPAM*** Score/Req: 16.40/04.40] Uni...	Morgan Person	6/8/04 12:12...
MDaemon Warning – virus found: [***SP...	andrew@bj-north.com.cn	4/10/04 1:46...
MDaemon Warning – virus found: [***SP...	serg@bbs.sdnet.gd.cn	12/31/69 6:0...

Subject: [***SPAM*** Score/Req: 06.00/04.40] AWARD NOTIFICATION
From: globallotteryintern1 <globallotteryintern1@telstra.com>
Reply-To: globallotteryintern1@bigpond.com
Date: 6/14/04 8:12 AM

```
GLOBAL LOTTERY INTERNATIONAL
 BUNDERSTRAATE 645, ROTTERDAM-NETHERLANDS.
 FROM:THE DESK OF THE VICE PRESIDENT.
 INTERNATIONAL PROMOTIONS/PRIZE AWARD.
 BACTH NO: GLNL/009842/04.
 REF. NO. GLNL/107654/04

                             RE: AWARD NOTIFICATION

This is to inform you of the release of the GLOBAL LOTTERY
INTERNATIONAL/  WORLD GAMING BOARD held on the 14th May 2004.Due to the
mix up of number, the results were released on the 14th June 2004. Your
name attached to ticket number 56739-1 with serial number 928098-0 drew
the lucky numbers of 2-6-9 which consequently won the lottery in the
2nd category.
```

The administrator can also do these functions using WorldClient as shown on the next page.



Email Address	Subject	Date
MAILER-…	[***SPAM*** Score/Req: 12.…	07/01/…
3Dslesli…	**[***SPAM*** Score/Req: …**	**06/23…**
europelo…	[***SPAM*** Score/Req: 09.…	06/21/…
Mail Deli…	[***SPAM*** Score/Req: 04.…	06/16/…
globallot…	[***SPAM*** Score/Req: 06.…	06/14/…
Morgan …	[***SPAM*** Score/Req: 16.…	06/08/…
serg@bb…	MDaemon Warning - virus fou…	05/18/…
andrew…	MDaemon Warning - virus fou…	04/10/…

From: globallotteryintern1 <globallotteryintern1@telstra.com

Date: 06/14/2004 06:12 AM

To:

Subject: [***SPAM*** Score/Req: 06.00/04.40] AWARD NOTIFICATION

```
GLOBAL LOTTERY
INTERNATIONAL
 BUNDERSTRAATE 645,
ROTTERDAM-NETHERLANDS.
 FROM:THE DESK OF THE
VICE PRESIDENT.
 INTERNATIONAL
PROMOTIONS/PRIZE AWARD.
 BACTH NO:
GLNL/009842/04.
 REF. NO. GLNL/107654/04


    RE: AWARD
```

User Instructions

Users can help define spam and legitimate email for a site by copying messages of both types to the *Junk Mail* and *Real Mail* folders, respectively.

Note: Because of the type of permissions assigned to these folders for **anyone@*yourdomain***, users can drag and drop email messages into the spam processing public folders but cannot view the contents of the folders.

By defining both types of messages, the users help the Bayesian filter do a better job of separating junk mail from real mail.

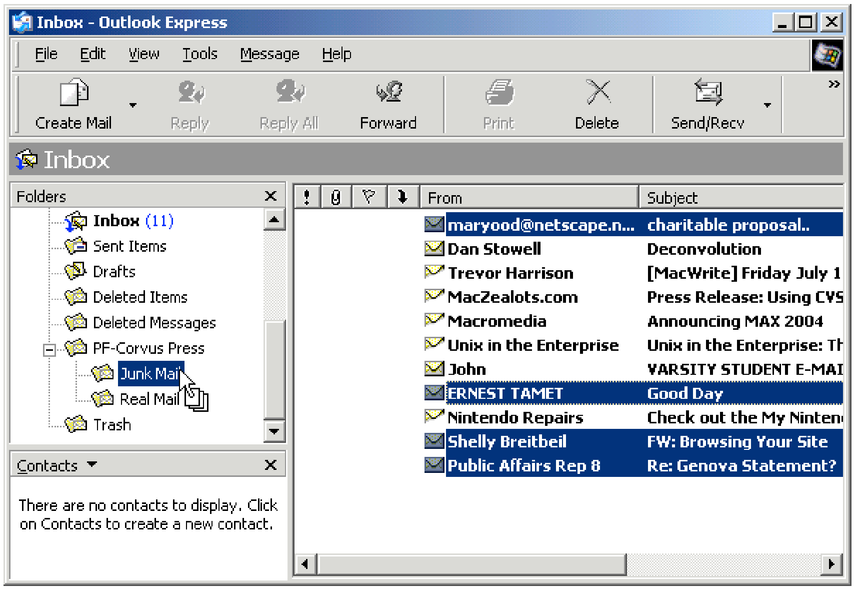
Users can copy messages to the spam processing public folders by using any of three methods:

1. IMAP email client
2. WorldClient webmail
3. Email attachments sent to the public folders from a POP email account

IMAP Email Client Method

With this method, the user has an IMAP email account. Many enterprises are now deploying IMAP because of the obvious convenience factors of having your email always available online and sharing messages online.

Using an IMAP email client, the account holder can just copy spam and real mail to their respective public folders.



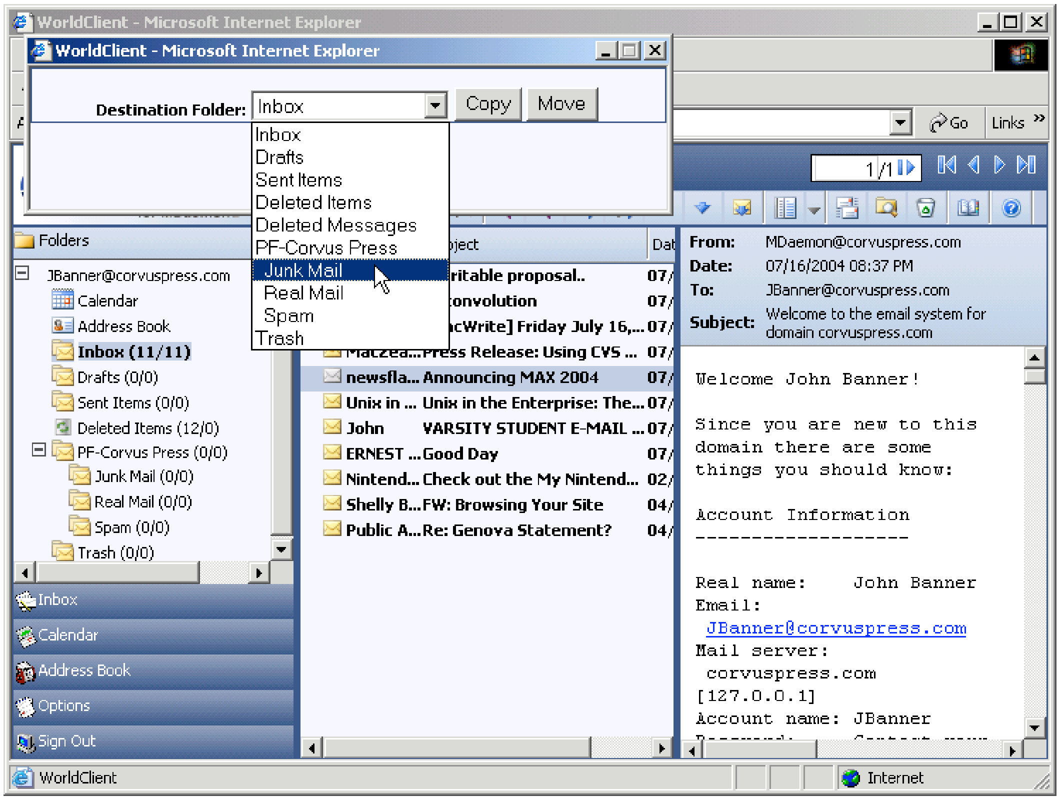
From	Subject
maryood@netscape.n...	charitable proposal..
Dan Stowell	Deconvolution
Trevor Harrison	[MacWrite] Friday July 1
MacZealots.com	Press Release: Using CVS
Macromedia	Announcing MAX 2004
Unix in the Enterprise	Unix in the Enterprise: Th
John	VARSITY STUDENT E-MAI
ERNEST TAMET	Good Day
Nintendo Repairs	Check out the My Ninten
Shelly Breitbeil	FW: Browsing Your Site
Public Affairs Rep 8	Re: Genova Statement?

There are no contacts to display. Click on Contacts to create a new contact.

WorldClient Method

In terms of helping define spam and real mail, WorldClient operates similarly to an IMAP client.

The account holder selects the messages and copies them to the corresponding public folder.



Destination Folder: Inbox

...ritable proposal.. 07/
...onvolution 07/
...cWrite] Friday July 16,... 07/
Maczea...Press Release: Using CVS ... 07/
newsfla... Announcing MAX 2004 07/
Unix in ... Unix in the Enterprise: The... 07/
John VARSITY STUDENT E-MAIL ... 07/
ERNEST ...Good Day 07/
Nintend... Check out the My Nintend... 02/
Shelly B...FW: Browsing Your Site 04/
Public A...Re: Genova Statement? 04/

From: MDaemon@corvuspress.com
Date: 07/16/2004 08:37 PM
To: JBanner@corvuspress.com
Subject: Welcome to the email system for domain corvuspress.com

```
Welcome John Banner!

Since you are new to this
domain there are some
things you should know:

Account Information
-------------------

Real name:    John Banner
Email:
 JBanner@corvuspress.com
Mail server:
 corvuspress.com
[127.0.0.1]
Account name: JBanner
```

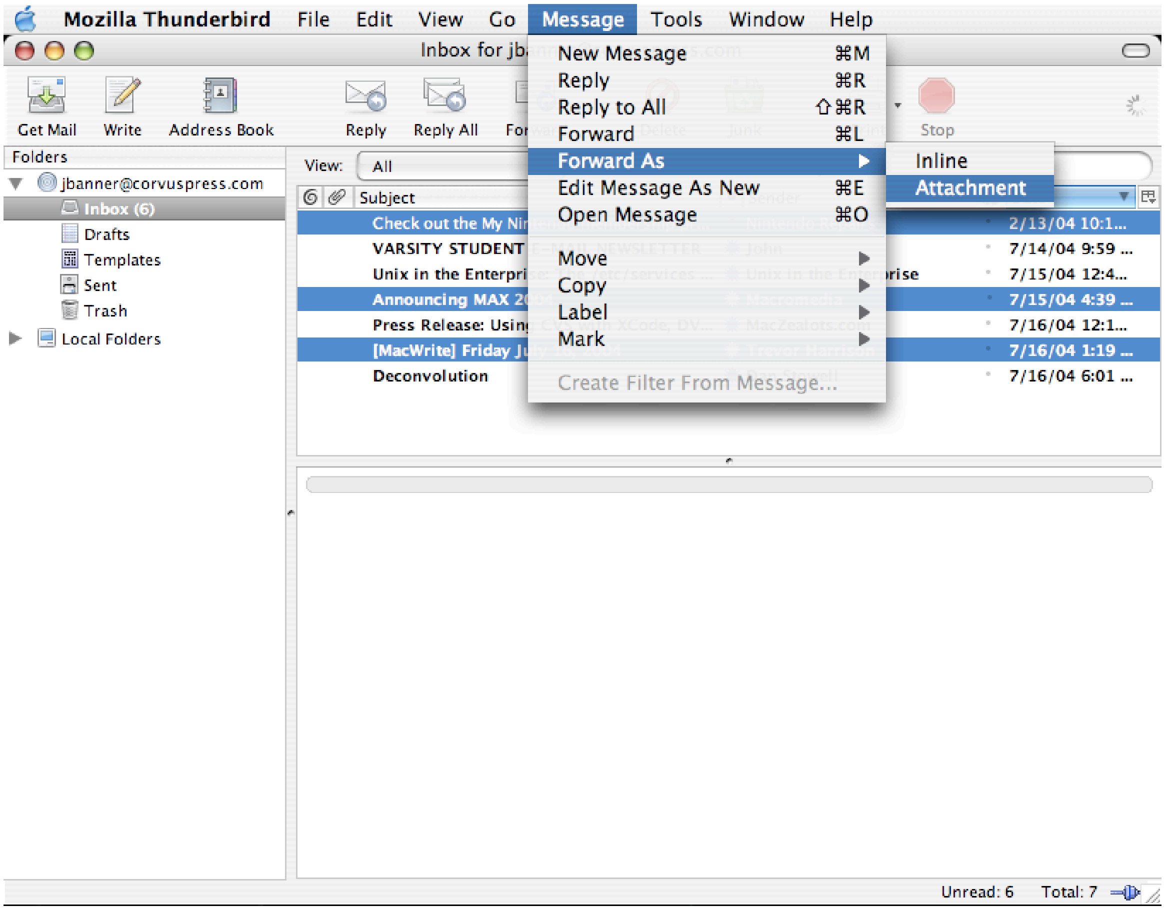
POP Email Attachment Method

Note: SMTP authentication must be enabled for this method to prevent abuse of the `SpamLearn` and `HamLearn` email addresses. You enable SMTP authentication by using the *Security > IP Shielding / AUTH / POP Before SMTP ...* command. The default settings work well.

On email servers with POP accounts only, users can email spam and real mail to:

`SpamLearn@`*`yourdomain`* `for spam`
`HamLearn@`*`yourdomain`* for real mail

The messages must be sent as attachments of the type `message/rfc822`. MDaemon rejects all other types of messages sent to these accounts.



Note: You can change the addresses MDaemon uses by editing these lines the CFILTER.INI file:

```
[SpamFilter]
SpamLearnAddress=SpamLearn@
HamLearnAddress=HamLearn@
```

The last character of these must be '@'.