# Configuring MDaemon for Centralized Spam Blocking and Filtering

## Contents

**A Centralized Approach to Blocking and Filtering Spam** 2

**MDaemon AntiSpam Tools Overview** 2

- Spam Blocking .......................................................... 2
- Spam Filtering .......................................................... 3
- Content Filtering ......................................................... 4
- IMAP Public Folders ..................................................... 5

**Step-by-Step Instructions for Configuring MDaemon AntiSpam** 7

- Check Spam Blocker ..................................................... 7
- Create Public Folders .................................................. 9
- Configure Spam Filter ............................................... 17
- Create Content Filter for Collecting Spam ......................... 21

**Using the AntiSpam Configuration** 26

- Using the Public Folders for Spam Processing ..................... 26
- Administrator Instructions .......................................... 27
- User Instructions ....................................................... 29
  - IMAP Email Client Method .......................................... 29
  - WorldClient Method ............................................... 29
  - POP Email Attachment Method ................................. 30
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 Filtering

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

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.

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.
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.
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.

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

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

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.)
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.

7. Select from the **IMAP folders** list the folder you just created and use the **Edit access control list** button.
8. Select Default rights (anyone) from the list, uncheck all Access Rights and use the Replace button. This prevents global access to your folders.

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

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.
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.

14. Select from the **Email address** list the address of the person to review the messages (penderagon@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 redisplay 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

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
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 redisplayes 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.

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

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.
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.

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.
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.

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

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.

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.
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.

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.
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.

![Specify Search text dialog](image)

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.

![Options dialog](image)
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.

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

18. Use the **OK** button on the **Create Rule** dialog.

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.

The administrator can also do these functions using WorldClient as shown on the next page.
Configuring MDaemon for Centralized Spam Control

Alt-N Technologies (www.altn.com)
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.

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.

### 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 '@'.