NewsletterBanner.pdf

## In this issue



---

**Osirusoft RBL Gone!**

Osirusoft, a popular antispam black list site, is offline following extended denial of service attacks. The Osirusoft listing should be removed from MDaemon's Spam Blocker:

1. Choose the *Security > Spam Blocker* command.
2. Select the *Spam Blocker Hosts* tab.
3. Click on the item containing *osirusoft* and click on *Remove*.
4. Click on *OK* to exit.

**Positive Reviews!**

MDaemon continues to receive positive reviews of its speed, security, low cost, easy installation and usability. It is praised for professional strength and beginner ease of use. See the review summaries, plus links to the complete reviews.

MDaemonLogo.pdf

**RelayFax Upgrade/Rewrite**

RelayFax is being rewritten with new technology. Also, Upgrade Protection is available. See the Upgrade Protection questions in the RelayFax FAQ. Also see the RelayFaX white paper.

# MDaemon 6.8 Stops Spam

Two new features — Bayesian filtering and heuristic detection — have made MDaemon 6.8 very effective at stopping spam before it reaches users.

*New AntiSpam tools come included, at no additional cost, with MDaemon 6.8 PRO!*

With *Bayesian filtering*, each email site decides what is spam and legitimate email by dragging and dropping examples of both into the filtering engine. The filter then compares the content of the examples to the content of new messages to separate spam from real mail. Given several hundred examples of each type, Bayesian filtering is more than 95 percent accurate on spam, with virtually zero mistakes for important email.

*Heuristic spam detection* uses feature-matching rules — red HTML text, for example — to identify spam. Through years of "learning" what spam (and legitimate) messages typically look like, the heuristic rules have become very reliable in separating spam from normal email.

MDaemon supports multiple means of fighting spam, including assured access through white lists.

For more information on stopping spam with MDaemon, see the *Security Tools for Spam Control* white paper, the MDaemon AntiSpam HowTos and the AntiSpam tutorial, by Ross McWilliam.

# SSL How To's

The Secure Socket Layer (SSL) can protect your MDaemon email communications on the Internet by using:

- server authentication certificates
- data encryption
- personal authentication certificates

An authentication certificate resides on your server and makes sure your users are communicating with your server only.

Data encryption converts ordinary data into codes only the sender and receiver software can understand.

A personal authentication certificate resides on a client computer and verifies the identify and ownership of the client computer.

MDaemon can use SSL for its IMAP, POP, SMTP and WorldClient webmail functions.

Setting up SSL for email and webmail are individual and independent processes. See the MDaemon SSL HowTos.

## White Lists & Exclusions

In their most basic form, *white lists* and *exclusion lists* contain the IP addresses of email senders who should always have access to your email server.

This typically means your server accepts email from these addresses without subjecting it to normal security scans, although that is not totally true for spam processing. White lists and exclusion lists help make sure security scanning does not accidentally block or hinder the delivery of critical legitimate email.

MDaemon uses *white lists* for it's *Spam Blocker* and *Spam Filter*. For the *Spam Blocker* you can enter the email addresses you always want to exclude from black list processing.

*Spam Filtering* uses numeric "scoring" for deciding if a message is spam — a higher "score" means a message is more likely spam. While white lists for the *Spam Filter* contain IP addresses not likely to be spam sources, the filter still processes messages from the white listed sites. However, the white listed sites start out weighted heavily against being spam sources. A message from a white listed site has to be very obviously spam before it is filtered out.

MDaemon uses *exclusion lists* for various types of server security. Sites on exclusion lists are trusted and receive no security scanning at all. The *Spam Filter* has an exclusion list. Other security measures with exclusion lists include:

*Relay Settings.* Trusted Hosts are exempted from the relay restrictions. See the *Security > Relay / Trust...* command, the *Trusted Hosts* tab.

*IP Screening.* Sites can be specifically prohibited or permitted to connect. For example the range `192.168.*.*` can be prohibited, but the single address `192.168.1.108` can be permitted. See the *Security > Address suppression...* command, the *IP Screening* tab.

You can set up white lists and exclusion lists for single addresses and for ranges of addresses. Examples include: `192.168.1.108` for a single address and `192.168.*.*` for a range of addresses.

Back to Contents

## Server Security Basics

A few MDaemon settings can protect your server from unauthorized access. They can also keep you from being blacklisted as an open relay or postmaster-accessible server. To find and configure these settings:

1. Use the *Security > IP shield...* command.
2. Select the *SMTP Authorization* tab.
3. Enable all of the check boxes.
4. Use the *OK* command button to save and exit.
5. Use the *Security > Relay / Trust...* command.
6. Select the *Relay Settings* tab
7. Enable all of the check boxes.
8. Use the *OK* command button to save and exit.

Back to Contents

## Customer Quotes

> *"May I just say congratulations on excellent service on the anti-virus service? While most of Denmark was severly attacked by the Sobig.F worm, not ONE virus came through our mailserver! Thank You Very Much!!!!"* — Christian Koerner

## GW Folder Sharing

In Outlook:

1. Right-click in the folder list on the folder you want to share.
2. Select *Properties* and then the *MDaemon GroupWare Folder* tab. The *Permissions* box lists all users with access to the folder.
3. Click the *Add* button, then choose a user from the list or type an email address. You can share with any GroupWare user on the same mail server. Use *"anyone"* to give access to all GroupWare users, or enter *anyone@example.com* to give access to all users in the *example.com* domain.
4. Assign permissions to the user. Your options are:

   *Folder visible* to make it visible to the user.

   *Read items* to make items visible in the folder.

   *Add items* to allow the creation of folder entries.

   *Edit Items* to enable making changes to the items.

   *Delete items* to allow the removal of things from the folder.

   *Create Subfolders* to permit the creation of folders within the current folder. Subfolders inherit the permissions of their parent folders.

Back to Contents

Alt-N Technologies, Ltd.
2201 East Lamar Blvd, Suite 270
Arlington, Texas 76006 USA
http://www.mdaemon.com
http://www.relayfax.com
http://www.altn.com