

AVS4YOU Programs Help



AVS Antispam

www.avs4you.com

© Online Media Technologies, Ltd., UK. 2004 - 2010 All rights reserved

Contact Us

If you have any comments, suggestions or questions regarding **AVS4YOU** programs or if you have a new feature that you feel can be added to improve our product, please feel free to contact us.

When you register your product, you may be entitled to technical support.

General information:	info@avs4you.com
Technical support:	support@avs4you.com
Sales:	sales@avs4you.com
Help and other documentation:	help@avs4you.com

Technical Support

AVS4YOU programs do not require any professional knowledge. If you experience any problem or have a question, please refer to the **AVS4YOU Programs Help**. If you cannot find the solution, please contact our support staff.

 **Note:** only registered users receive technical support.

AVS4YOU staff provides several forms of automated customer support:

- **AVS4YOU Support System**
You can use the **Support Form** on our site to ask your questions.
- **E-mail Support**
You can also submit your technical questions and problems via e-mail to support@avs4you.com.

 **Note:** for more effective and quick resolving of the difficulties we will need the following information:

- Name and e-mail address used for registration
- System parameters (CPU, hard drive space available, etc.)
- Operating System
- The information about the capture, video or audio devices, disc drives connected to your computer (manufacturer and model)
- Detailed step by step describing of your action

Please do **NOT** attach any other files to your e-mail message unless specifically requested by AVS4YOU.com support staff.

Resources

Documentation for your AVS4YOU software is available in a variety of formats:

In-product (.chm-file) and Online Help

To reduce the size of the downloaded software installation files the in-product help was excluded from the installation although you can always download it from our web-site for your convenience. Please, visit AVS4YOU web-site at <http://www.avs4you.com/OnlineHelp/index.aspx> to download the latest available version of the help executable, run it and install into the AVS4YOU programs folder. After that you will be able to use it through the **Help** menu of the installed AVS4YOU software.

Online Help include all the content from the In-product help file and updates and links to additional instructional content available on the web. You can find the **Online Help** at our web-site - <http://www.avs4you.com/OnlineHelp/index.aspx>. Please note, that the most complete and up-to-date version of AVS4YOU programs help is always on the web.

PDF Documentation

The offline help is also available as a pdf-file that is optimized for printing. All PDF help files are available for download at the programs pages at AVS4YOU web-site (both <http://www.avs4you.com/index.aspx> and <http://www.avs4you.com/OnlineHelp/index.aspx>). To be able to read and print AVS4YOU PDF help files you will need to have a PDF reading program installed.

User Guides

You have access to a wide variety of resources that help you make the most of your AVS4YOU software. The step-by-step user guides will be of help not only to the novice users but also to the users that face a certain task to be performed and look for a way to do it. Please, visit our **User Guides** section of AVS4YOU web-site at <http://www.avs4you.com/Guides/index.aspx> to read the detailed instructions for various software and tasks

Technical Support

Visit the **AVS4YOU Support** web-site at <http://support.avs4you.com> to ask your questions concerning AVS4YOU software installation, registration and use. Feel free to also use our e-mail address support@avs4you.com.

Downloads

Visit the **Downloads** section - <http://www.avs4you.com/downloads.aspx> - of our web-site to find free updates, tryouts, and other useful software. We constantly update the software, new versions of the most popular programs and new software are also frequently released.

Overview

AVS Antispam is an intuitive to use application working with POP3 protocol and aimed at preventing you from junk emails on the computer, no matter what e-mail program you use. Define black and white lists of e-mail addresses, use the advantage of realtime black lists which contain the latest data on spammer addresses and URLs, get the comprehensive protection from spam due to five level filtering **AVS Antispam** performs, view the history of actions taken towards each new incoming message including all the details.

AVS Antispam starts automatically after reboot that follows installation (that is so only in case you checked the corresponding option during the installation process). If you happen to exit the program choose **AVS4YOU -> System Utilities -> AVS Antispam** from the **Programs** section of the **Start** menu or click twice on its desktop shortcut to load it again.

Introduction to Spam Problem: Overview

To use **AVS Antispam** efficiently and knowingly we recommend to learn some basics on spam subject, methods spammers use to cover more and more users, harm it brings and the way **AVS Antispam** provides protection.

What is Spam?

Definition. The origin of the term spam comes from a sketch by the British comedy troupe Monty Python. They did a bit on a restaurant where all the dishes cooked with SPAM (an acronym for **S**houlder of **P**ork and **H**am), which is a canned ham product from Hormel Foods Corporation. When the waitress describes items on the menu to a couple of customers landed from above, a group of Vikings sing a song that goes something like "SPAM, SPAM, SPAM, SPAM. Lovely SPAM, lovely SPAM..." So spam was thus named because, like the song, it is an endless repetition of worthless text.

Nowadays the lowercase word **spam** relates either to **unsolicited bulk** or **commercial email** and has nothing to do with the compressed ham in a can called and written as **SPAM**. There is fairly widespread agreement what spam general characteristics are:

- Spam is an electronic message.
- Spam is unsolicited. To understand that, refer to the electronic subscription thing. Many reputable companies use emails for lawful marketing purposes. If you agree to receive emails from a company by means of a voluntary subscription, the emails the company sends you is not spam. More than that if you do not want to be on the mailing list of the company any longer you can unsubscribe without a problem.
- Spam is sent in bulk. This means that the spam is distributed by a large number of essentially identical messages and that recipients are chosen indiscriminately.

These three traits define **unsolicited bulk email (UBE)**

If to add the fourth characteristic:

- Spam is of a commercial nature.

That defines **unsolicited commercial email (UCE)**.

Spam categories:

- **Commercial advertising.** That is spam that follows any commercial intention or UCE. UCE is a kind of marketing too, rather cheap and easy way to cover a large group of customers. Usually UCEs are not sent by the advertising companies themselves, but by spammers, who receive commissions from these companies.
- **Non-commercial advertising.** That can be political or religious propaganda without a commercial context at all.
- **Fraud and phishing.** Often spammers send fraudulent emails, for instance, think out a pathetic and tragic story where a person suffering from a disease or who is a victim of a disaster appeals to you for financial help; inform you about a lotto winning demanding to pay a service charge first. A particular type of fraud is phishing - emails that appear to be from a well-known company, but they are not. The aim of such emails is to obtain user financial information or passwords.
- **Hoaxes and chain e-mails.** Such spam emails are sent to trick people into believing false information with a recommendation or an appeal to forward them to as many people as possible. That can be warning against viruses, misinformation about social events or even a dodge that makes you visit a web page and after that malicious software will be installed on your computer.
- **Joe jobs.** These are unsolicited emails with irritating, immoral or abusive content sent by a spammer who forges the From: field address and provokes angry recipients into flooding an innocent sender with complaints.
- **Bounce messages.** These are messages that are returned to senders by a receiving e-mail server in case it gets undeliverable addresses. Spammers distribute such undeliverable messages forging the From: field address and servers return bounce messages to innocent people in response to emails they have never actually sent. Bounce messages are not themselves spam but due to spammer tricks they become a significant part of email traffic.

Terminology. Two terms are commonly used to classify emails with a view to the spam problem:

- **junk email** - a message that comes under the spam definitions stated above;
- **legitimate email** - a message that is received from a trusted and known sender or the one you gave agreement to be sent to.

How do Spammers Obtain E-mail Addresses?

It is rather obvious that there are some ways through which spammers get e-mail addresses and cover the huge quantity of users all over the world:

- **Website harvesting programs.** Using special program tools spammers extract e-mail addresses from web site page HTML code and gather a single e-mail address warehouse.
- **Dictionary based programs.** Spammers often use these programs to generate e-mail addresses. Such programs combine separate letters, words, numbers and symbols together so that to generate admissible e-mail names which are joined to a chosen e-mail service provider domain name so forming the whole e-mail addresses.
- **Opt-in lists.** Such lists store e-mail addresses of users who indirectly but voluntarily gave their agreement to that. That means the users accepted the offer to be subscribers and agreed to add their e-mail addresses to mailing list. Commonly opt-in lists are organized as records within a database. So dishonest employees who somehow have an access to such a database may sell it to spammers via Internet or on CD-ROM.
- **Forums and interactive web sites.** When you post your email address to the Web to sign up for a discussion forum and forget to hide it from public eyes, you expose yourself to spammers who are among the forum registered users as well.
- **Email forwarding.** If you forward an email to many people, make sure you send it to yourself in the To: field and put everyone else in the Bcc: field. Bcc means blind carbon copy. It's used to send a copy of the email to someone without revealing his or her e-mail address to others who are going to receive the copy too. If you use the Cc: field instead you expose everyone's e-mail address to a lot of other people. If you are not that careful, you may accidentally include a spammer e-mail address into the Cc: field becoming this way an indirect accessory of the spam distribution.
- **Public WHOIS database.** When a company or an individual registers a domain name, the Internet Corporation for Assigned Names and Numbers requires the domain name registrar to submit the company/individual personal

contact information, including the e-mail addresses of people that are in charge of technical issues, to the WHOIS database. Once such information appears in this online database, it is publicly available to spammers who take e-mail addresses out of it using the WHOIS utility. To prevent spammers from that it is preferable to keep domain name information in private WHOIS database, commonly this service requires a small monthly fee to be paid.

What Harm Can Spam Do?

Spam is a disaster these days, the real damage and harm it can do are not always so clear. Relying on the spam categories unsolicited emails bring the following issues:

- **Money costs.** Due to the large volume of sent spam, Internet Service Providers have to buy and install anti-spam products and increase network bandwidth by purchasing new equipment. That influences the amount of money you pay in the long run.
- **Wasted time and productivity.** Spam wastes workers' time and productivity. It takes time for an employee to sort out which emails he or she needs among all the sent ones where spam may make up at least 50 %. That distracts from performing work and decreases the general productivity therefore profits.
- **Viruses and spyware.** Some spam emails have attachments that if downloaded can infect your computer with a virus or spyware that gathers information on you and distributes it to someone else through Internet.
- **Offensive and lecherous content.** Spam exposes children to topics and images that include obscene language and adult content.

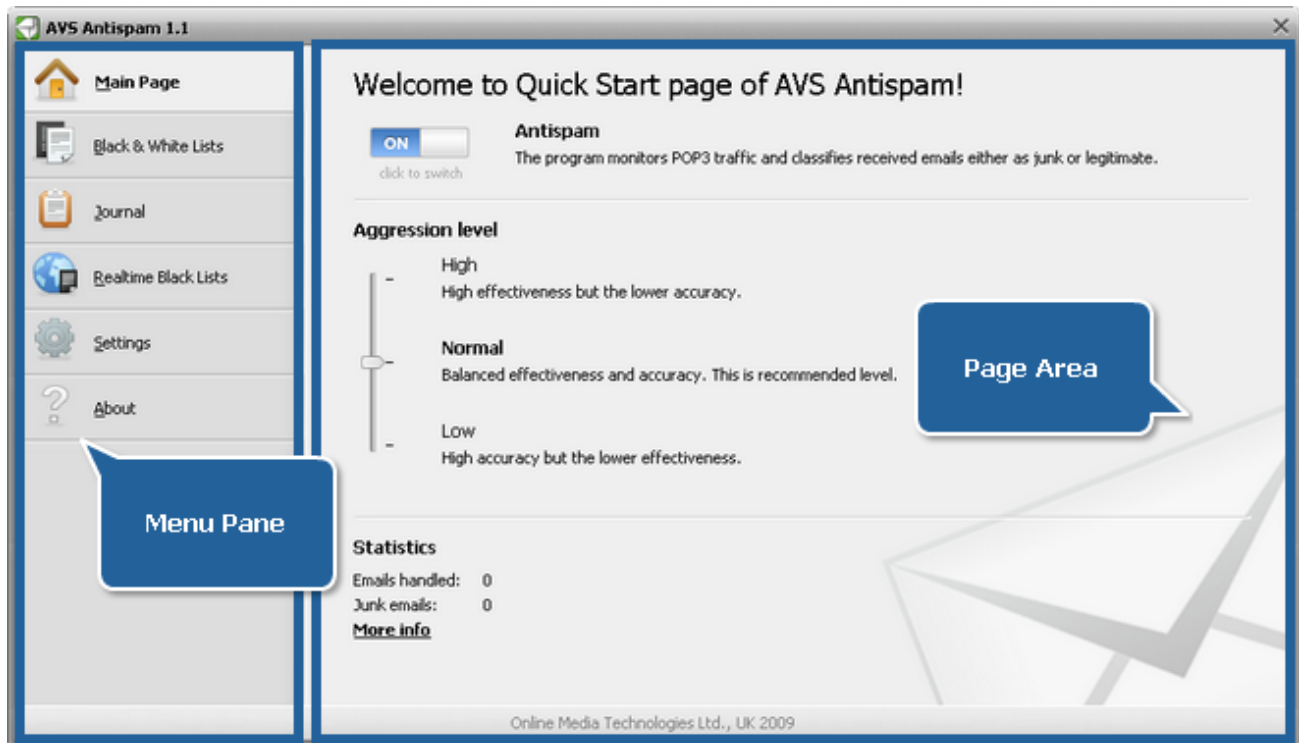
How does AVS Antispam Prevent from Spam?

AVS Antispam provides the superb protection from spam due to five filters:

- **Heuristic filter.** This is the rule based filter. The rules (nearly several hundred altogether) are pre-defined and serve a certain area in the email structure. The rules check if, for instance:
 - weird symbols repeat in the email body;
 - 80-90% of lines in the email body are blank;
 - the email header has an invalid date (e.g. non-existing time zone);
 - the email subject talks about money reward;
 - the email message text is disguised using an additional encoding, etc.
- **Statistical filter.** This filter is pre-trained initially and as the emails are marked as "Spam" or "Not spam" manually the statistical filter enriches its spam sign knowledge. The filter knowledge is presented as a database that contains words and associated with them numeric coefficients specifying the probability that a word is attributable to junk email. When an email is handled with the statistical filter each word of the email is checked on presence in the database. If a word is found, its numeric coefficient is used to calculate the word contribution in treating the email as junk by means of the Bayes' formula. Then, such word contributions are summarized to get the email total spam value which is compared with a certain threshold value to make a final decision.
- **Realtime black list of IPs.** This filter checks presence of the message sender IP address in remote black lists that are published on hosted nameservers. Such black lists are expanded in several ways, for instance, by a nameserver owner manually, by an anti-spam server software that detects the spam sender IP address and add it to the remote black list, by users who mark suspicious messages as spam when use the web based interface from a mail service provider rather than an e-mail program.
- **Realtime black list of URIs.** This filter is similar to the previous one excepting it checks the email for spammer URLs using the corresponding remote black lists.
- **Black and White lists.** This filter is customizable because you define the untrusted and trusted sender e-mail addresses by yourselves. The filter enabled (**Use black list** or **Use white list** is checked) with addresses added overlaps a decision made by any other filter, in other words it has the priority over others in such a case.

Program Interface

The interface of **AVS Antispam** is designed to provide the proper spam protection with incredible ease and clarity - you just switch between the functional page tabs within the same window and manage customizable filters, get information on actions taken towards the incoming emails, adjust the program behaviour the way you like:



Menu Pane is the set of page tabs:

Page tab	Description
Main Page	Press the tab to set the AVS Antispam aggression level, enable or disable the spam protection and view the statistics on handled emails.
Black and White Lists	Press the tab to define the trusted and untrusted e-mail addresses.
Journal	Press the tab to track the history of handled emails including all the details.
Realtime Black Lists	Press the tab to manage and define remote hosts that contain the lists of the spammer IP addresses.
Settings	Press the tab to adjust the plugins of e-mail programs that AVS Antispam supports and the way you want AVS Antispam to work.
About	Press the tab to get information about the AVS Antispam version you are working with and read the end-user license agreement.

Page Area is the area where all the information and controls relating to a certain feature are placed. The view of this area differs depending upon the **Menu Pane** tab pressed.

If **AVS Antispam** is loaded the icon is shown in system tray (which is green in case the program is enabled and red if not):



Working with AVS Antispam: Overview

AVS Antispam marks an email as spam depending upon the aggression level you set, which defines how rigorous the set of all the spam signs should be taken into consideration. So the aggression level is what you should start with to get the **AVS Antispam** corresponding efficiency.

Choosing the Aggression Level

Aggression level, if to go into details a bit, defines a decision making on whether an email should be treated as junk or not. Changing the aggression level influences two characteristics of filtering:

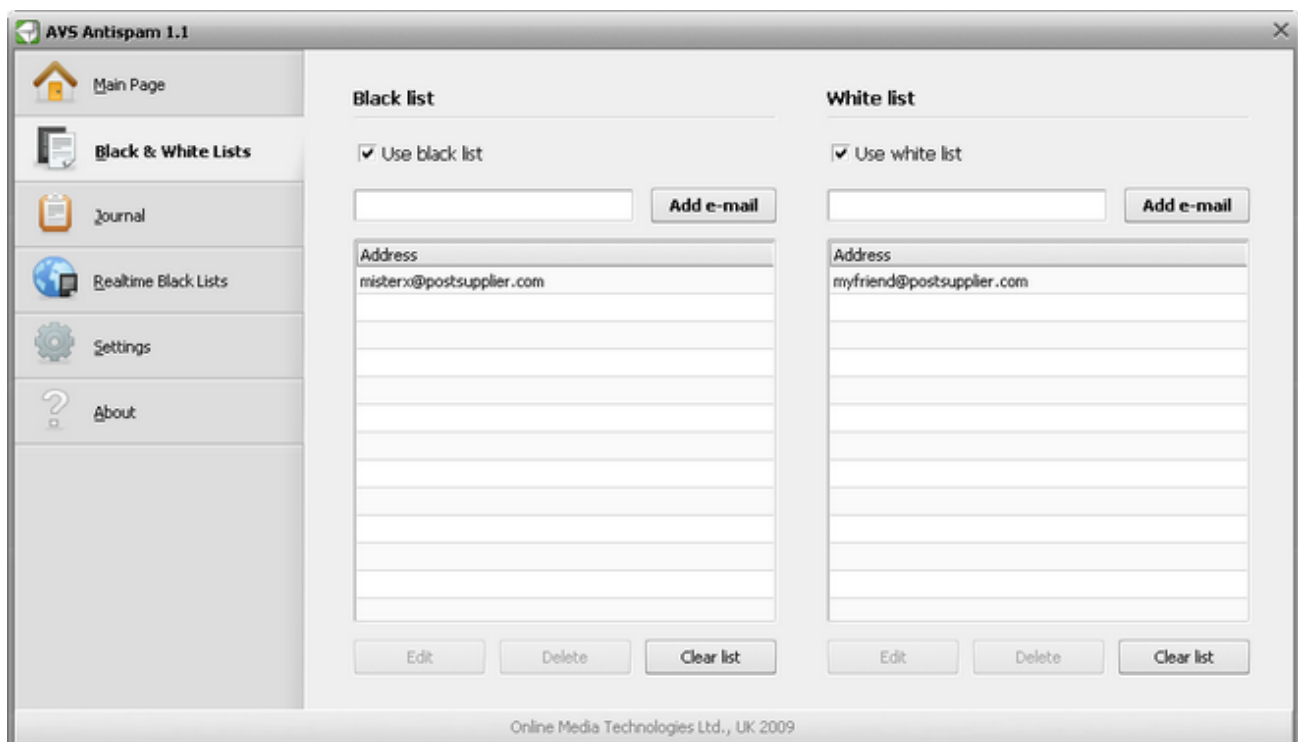
- **Effectiveness.** That indicates the percentage of emails detected as junk.
- **Accuracy.** That indicates the ability to distinguish legitimate emails from junk. The accuracy is determined as the false positive rate. The less accuracy is, the higher false positive rate is and the more legitimate emails will be treated as junk.

To change the aggression, click the **Main Page** tab and set the **Aggression level** slider to the desired position:

- **High.** Set this level, if you see more junk emails income undetected. The downside is that the probability of the legitimate emails treated as junk is increased that's why you should use the black and white lists of e-mail addresses with this level.
- **Normal.** The effectiveness-accuracy ratio is optimal. Setting this level, you rely on the most comfortable values of effectiveness and accuracy **AVS Antispam** suggests.
- **Low.** Set this level, if you see more legitimate emails are treated as junk. The downside is that the probability of junk email incoming undetected is increased.

Using the Black and White Lists

To define the untrusted or trusted sender e-mail addresses, click the **Black and White Lists** tab:



To disable/enable the black list, uncheck/check the **Use black list** option.

To disable/enable the white list, uncheck/check the **Use white list** option.

To add a sender e-mail address into the black list, make sure the **Use black list** option is checked, enter the untrusted address into the **Black list** editbox then press the **Add e-mail** button.

To add a sender e-mail address into the white list, make sure the **Use white list** option is checked, enter the trusted address into the **White list** editbox then press the **Add e-mail** button.

Note: you can also use the wildcards "?" and "*" to specify an address mask, for instance:

- *@postsupplier.com - any emails from the postsupplier.com mail domain;
- doctorsmith??@postsupplier.com - emails from the postsupplier.com mail domain where the sender name begins with "doctorsmith" and ends on any two admissible symbols;
- doctorsmith???@postsupplier.* - emails from the mail domain that begins with "postsupplier" and where the sender name begins with "doctorsmith" but ends on any three admissible symbols.

To change an e-mail address, select its row then press the **Edit** button or just use a double click.

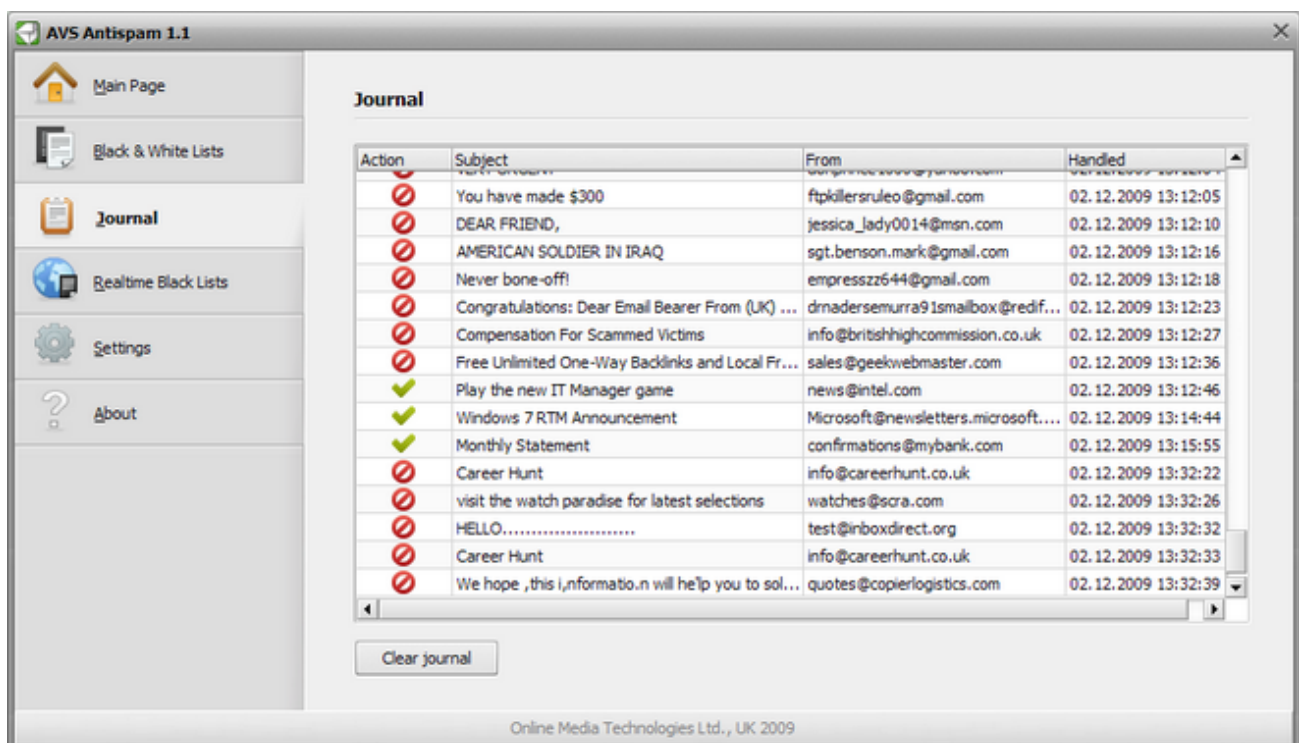
To remove an e-mail address, select its row then press the **Delete** button.

To remove all the e-mail addresses added, press the **Clear list** button.



Viewing the Journal

Journal is useful if you want to track the history of the handled incoming emails and learn whether an email was marked as junk or legitimate including all the necessary details.






To view the journal, click the **Journal** tab:



The page contains the table with the following fields:

Field	Description
Action	Shows a mark given to a message: <ul style="list-style-type: none"> •  - the message is marked as junk; •  - the message is marked as legitimate.
Subject	Shows the subject of a message.
From	Show a sender e-mail address.
Handled	Shows a date and time when a message has been handled.

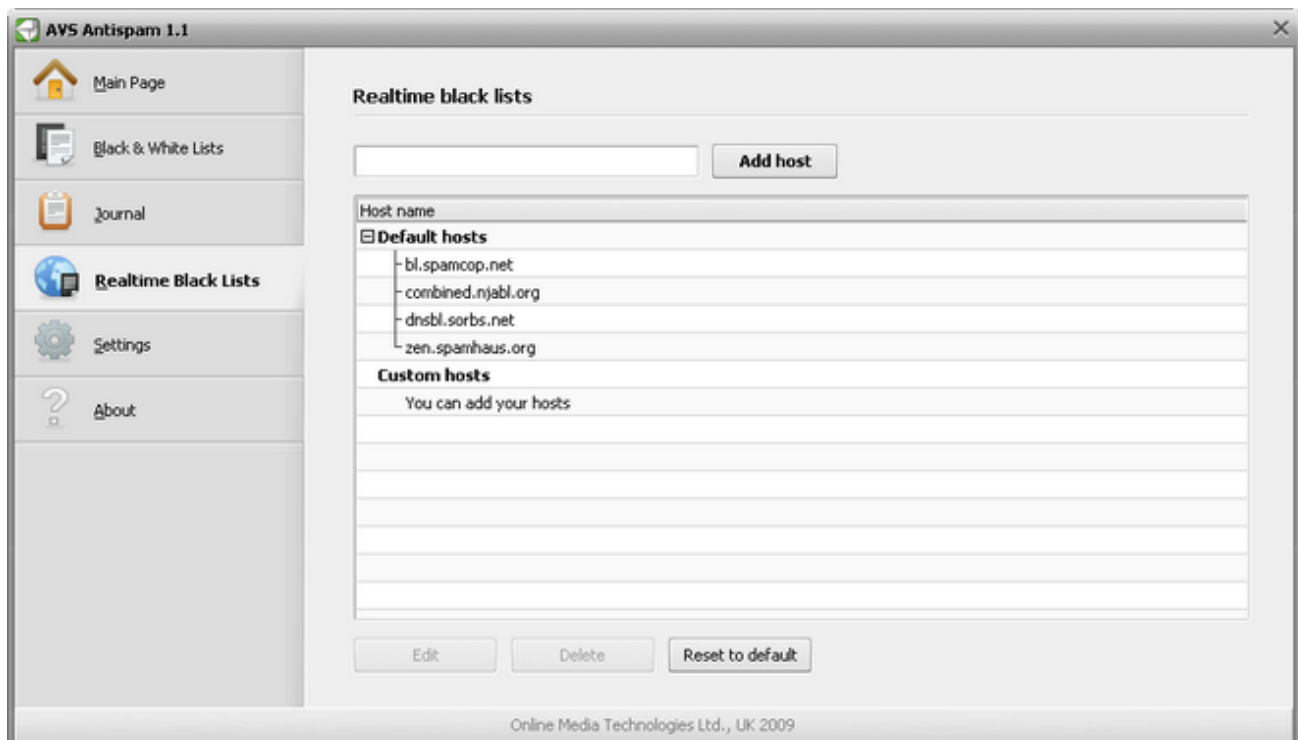
To add a sender address to the black or white list, select its row then press the **Add to black list** or **Add to white list** button:

Action	Subject	From	Handled
	Assalamu'alaikum!	hamizban906@msn.com	10/29/2009 2:37:54 PM
	Sender: boopy324@hotmail.com Subject: All Meds are onsale Today Come see our closeout ,prices		
	Notification of Payment	eerhcxdwbsr@cavallibeachhouse....	10/29/2009 2:38:00 PM
	Target new markets	michellewatson01@confworldwide....	10/29/2009 2:38:03 PM

To remove all the records, press the **Clear journal** button.

Using the Realtime Black List Hosts

To view or manage the list of host names, click the **Realtime Black Lists** tab:



The page contains the table with two categories:

Category	Description
Default hosts	Contains the predefined black list host names.
Custom hosts	Contains the black list host names you added.

To add a host name, input it into the editbox then press the **Add host** button.

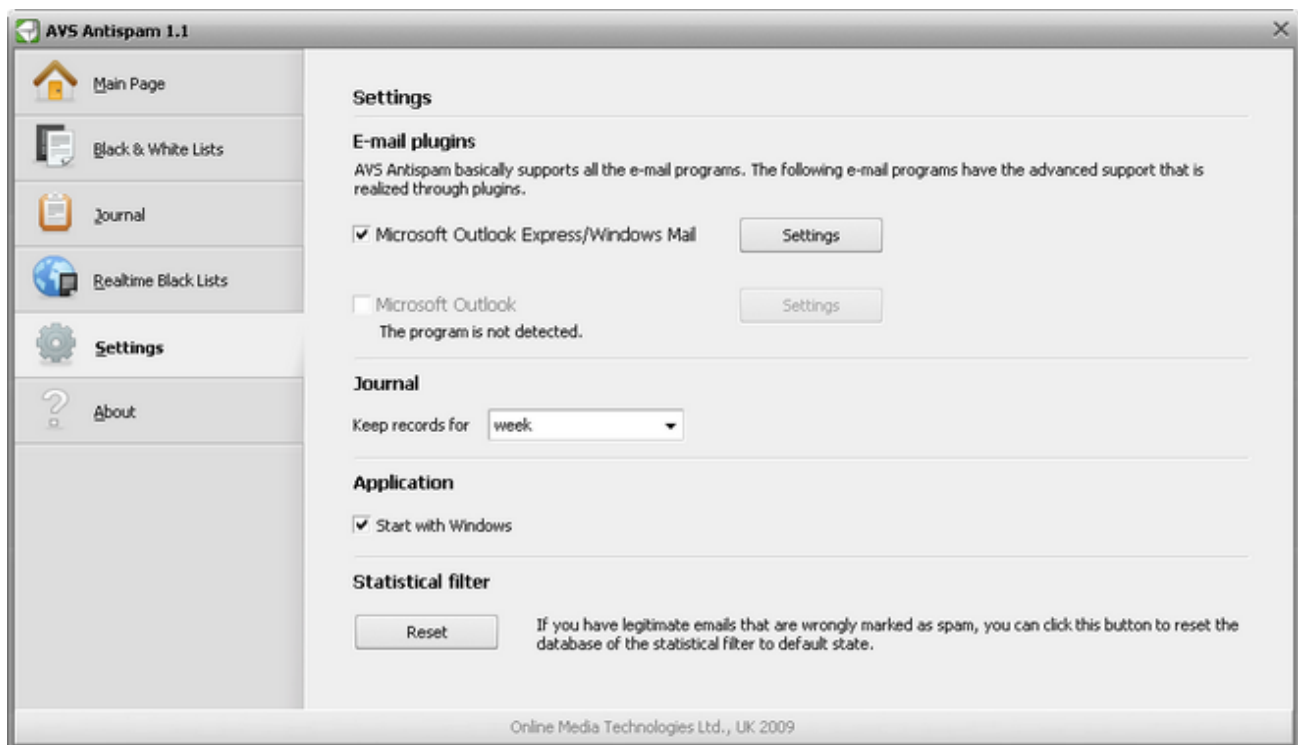
To change a host name from the **Custom hosts** category, select its row then press the **Edit** button.

To remove a host name, select its row then press the **Delete** button.

To return the default set of the predefined host names and clear the **Custom hosts** category, press the **Reset to default** button.

Changing the Program Settings

To change settings, click the **Settings** tab:



The page contains the sections with settings:

E-mail plugins

AVS Antispam works with all the E-mail programs, but the following E-mail programs have the advanced support by means of the plugins **AVS Antispam** is bundled with:

- Microsoft Outlook Express;
- Microsoft Windows Mail;
- Microsoft Outlook.

To disable/enable a plugin, uncheck/check the corresponding option.

To adjust a plugin, enable it first then press the **Settings** button.



Note: the plugin checkbox is available only if the supported E-mail program it serves is installed on your computer.

Journal

Keep records for - specify how long the records should be kept before the journal is cleared: **week**, **2 weeks** or **month**.

Statistical filter

With time, due to your marking messages as "spam" manually, the statistical (Bayesian) filter can accumulate inaccuracy because a message marked as spam may also contain words that are in general use, not only the ones that made you decide the message is junk, thereby the false positive is increased. If you see that more and more legitimate messages are marked as spam, press the **Reset** button to return the default pre-trained database of the filter.

Application

Start with Windows - **AVS Antispam** starts together with Windows (in case you checked the corresponding option during installation) but you can disable that by unchecking this option.