

---

# AVAS Anti-Virus & Anti-Spam User Manual

Version 1.2 April 2004

---

Please Note: This user manual goes into a lot of technical detail about exactly what AVAS does, how to teach it, how to move and delete messages automatically and how to set up additional filters for you to get even more out of the service. Don't panic – You don't need to know all of this information for AVAS to be able to help protect your inbox.

Due to continued product development, the information contained within this document is subject to change without notice and we do not warrant or guarantee that this document or the information contained within it is free from error or suitable for any particular purpose.

No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the prior written permission of Net Energy Internet Ltd.

Copyright ©1997-2004 Net Energy Internet Ltd. All Rights Reserved.

# Contents

<b>CHAPTER 1 – OVERVIEW.....</b>	<b>4</b>
Introduction.....	4
About AVAS.....	4
Features.....	5
How AVAS Works.....	5
AVAS at a Glance.....	6
<b>CHAPTER 2 – ANTI-VIRUS MODULE.....</b>	<b>7</b>
Summary.....	7
Features.....	7
How it Works.....	8
Moving or Deleting Virus Notifications.....	8
WebMail Interface.....	9
Microsoft Outlook.....	10
Microsoft Outlook Express.....	11
Frequently Asked Questions.....	12
Important Note.....	14
The Anti-Virus Module at a Glance.....	14
<b>CHAPTER 3 – ANTI-SPAM MODULE.....</b>	<b>15</b>
Summary.....	15
Features.....	16
How it Works.....	16
The Five Anti-Spam Engines.....	17
Bayesian Analysis Engine.....	17
SpamAssassin Filtering Engine.....	17
HTML/Character Set Filtering Engine.....	17
Regular Expression Filtering Engine.....	18
DNS Blacklist Lookup Engine.....	18
How the Message is Altered.....	18
Subject Alteration.....	19
Headers Inserted and Altered.....	20
Teaching the Bayesian Analysis Engine.....	21
Moving or Deleting Spam Messages.....	23
WebMail Interface.....	24
Microsoft Outlook.....	25
Microsoft Outlook Express.....	26
Moving or Deleting Spam Messages - Whitelisting.....	27
WebMail Interface.....	28
Microsoft Outlook.....	29
Microsoft Outlook Express.....	29

Moving or Deleting Spam Messages - Advanced .....	30
Frequently Asked Questions .....	33
The Anti-Spam Module at a Glance .....	35
<b>CHAPTER 4 – CUSTOM FILTERS MODULE.....</b>	<b>36</b>
Summary .....	36
Features.....	37
How it Works .....	37
Filter Properties .....	38
Example Filters.....	40
Blocking Attachment File Types.....	40
Rejecting Messages from a Sender .....	41
Marking Messages as Spam.....	42
Deleting Virus Notifications .....	43
Rejecting Likely Spam Messages .....	43
Creating a Whitelist Filter .....	44
Frequently Asked Questions .....	45
The Custom Filters Module at a Glance.....	47
<b>CHAPTER 5 – PUTTING IT ALL TOGETHER.....</b>	<b>48</b>
Introduction.....	48
A ‘Real World’ Example.....	48

## Table of Figures

Figure 1 - The route a message takes through AVAS .....	6
Figure 2 - A 'clean' e-mail that has been scanned by the anti-virus module.....	8
Figure 3 - The flow of a message through the anti-virus module .....	14
Figure 4 - Example of the subject alteration when a message is detected as likely spam.....	16
Figure 5 - Example of the message headers altered when a message is detected as spam.....	16
Figure 6 - Example of the subject alteration.....	19
Figure 7 - Example of the message headers inserted and altered .....	20
Figure 8 - The completed rules in Microsoft Outlook Express .....	33
Figure 9 - The flow of a message through the anti-spam module.....	35
Figure 10 - The custom filters module in the WebMail interface .....	37
Figure 11 - Blocking attachment file types .....	41
Figure 12 - Rejecting messages from a sender .....	42
Figure 13 - Marking messages as spam .....	43
Figure 14 - Rejecting likely spam messages.....	44
Figure 15 - Creating a whitelist filter.....	45
Figure 16 - The flow of a message through the custom filters module .....	47
Figure 17 - The completed domain level filters in the WebMail interface .....	52
Figure 18 - The completed user level filters in the WebMail interface .....	53
Figure 19 - The completed rules in Outlook Express.....	53

---

## CHAPTER 1

# Overview

### In This Chapter

Introduction.....	4
About AVAS.....	4
Features .....	5
How AVAS Works.....	5
AVAS at a Glance.....	6

---

## Introduction

The last year has brought about a significant increase in the amount of viruses and the threat they pose to computer users worldwide. More recently, with the release of W32/Mydoom, W32/Netsky and W32/Bagle, and the speed at which they infect and interfere with systems worldwide, all computer users need to take action to ensure that wherever possible they avoid infection.

With the growth in e-mail as a communication medium, one of the most likely sources of infection is by e-mail. Either from people you know, or from intelligent viruses mass mailing themselves from one computer to another.

But it isn't just about viruses...

With legislation having little or no effect on the amount of spam that is now being sent on a daily basis, Internet users are finding themselves deluged by the sheer amount of junk mail that arrives in their inbox.

Whether its offers for prescription medications, dubious invitations to enlarge body parts, or opportunities to make millions, (simply by following some instructions from the widow of a deceased African general), users need a quicker way to sort and filter their e-mail so that they can easily read and respond to the genuine messages that are important.

AVAS has been introduced to help with both of these problems.

---

## About AVAS

AVAS is our dual anti-virus and multi-level anti-spam system designed to help protect customers who have purchased an e-mail or Web hosting plan from the multitude of e-mail borne viruses and Unsolicited Commercial E-Mail (UCE), or spam that is being sent by e-mail on a daily basis.

By combining two self-updating anti-virus engines from independent vendors and a five level intelligent anti-spam system, users of AVAS should see a significant reduction in the amount of viruses and spam messages that they receive.

Whilst AVAS will help to protect customers e-mail, it is important to note that no system can guarantee a 100% detection rate due to the speed at which new viruses are released and the ever changing tactics of spammers.

The technology behind AVAS does however have the capability to learn and to improve on its detection rate as time goes on, without the customer having to perform any additional configuration.

Please Note: AVAS does not attach any advertising banners to e-mail messages.

---

## Features

- Messages scanned by two independent anti-virus engines
- Intelligent filtering through five levels of spam analysis
- Additional user and domain level filtering via WebMail
- Per domain protection covers all e-mail accounts
- No extra charge to cover additional e-mail accounts
- Works 'out of the box' – No configuration necessary
- Telephone, e-mail and online support

---

## How AVAS Works

Every time a message is received for a customer subscribed to AVAS it is automatically passed through three different modules before being delivered.

The three modules are:

- Anti-Virus – Scans the message for any possible viruses, trojans or worms and ensures that the message doesn't have any attachments of a type blocked by the system.

If the message is found to contain a virus, the message is deleted and both the sender and recipient are notified. In the event that a blocked attachment is found the message is automatically rejected.

- Anti-Spam – Analyses every part of the message looking for any spam like characteristics, and checks to make sure that the message isn't corrupt. Also inserts additional headers in the message containing both the Bayesian Analysis and SpamAssassin scores.

If the message is identified as possible or likely spam both the subject and message headers are altered. In the event that the message is found to be corrupt, it is automatically rejected.

- Custom Filters – Additional user and domain level filters that can be set-up via the WebMail interface to reject, accept, delete or mark as spam any message meeting set criteria, e.g. from a specific sender.

Each module also has a number of different engines attached to it. For example, the anti-virus module uses two different anti-virus engines to scan the message. Likewise, the anti-spam module passes each message through five separate anti-spam engines looking for any characteristics indicative of spam.

By combining the three modules together, AVAS offers a safer, easier way to manage both personal and business e-mail alike.

---

## AVAS at a Glance

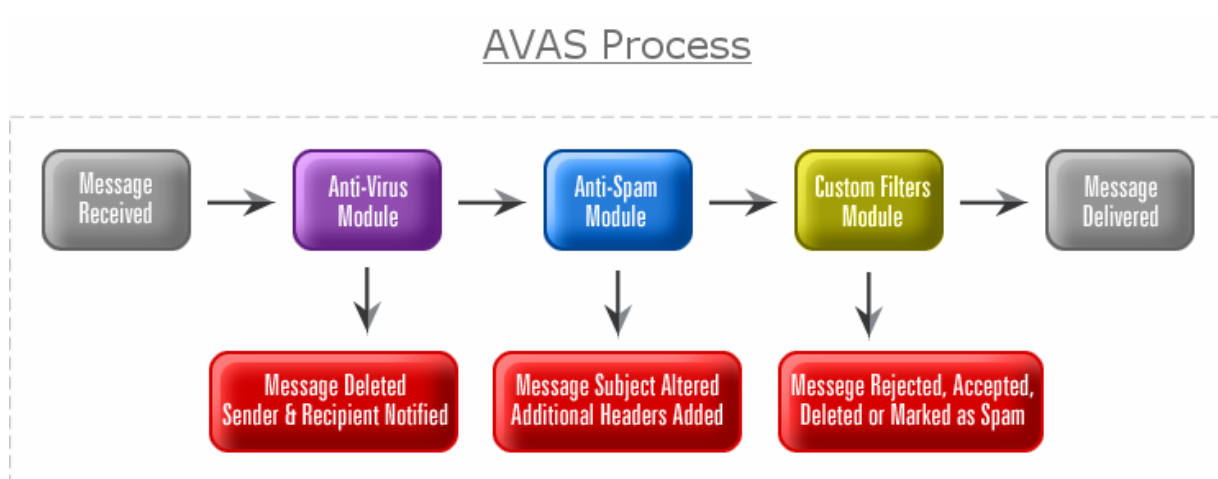


Figure 1 - The route a message takes through AVAS

---

## CHAPTER 2

# Anti-Virus Module

### In This Chapter

Summary .....	7
Features .....	7
How it Works .....	8
Moving or Deleting Virus Notifications.....	8
Frequently Asked Questions .....	12
Important Note.....	14
The Anti-Virus Module at a Glance .....	14

---

## Summary

Using dual anti-virus engines from independent vendors, the anti-virus module of AVAS scans every incoming and outgoing e-mail that passes through the system.

Each e-mail is checked against a database containing thousands of known viruses, trojans and worms. If a virus is detected by either engine, the message is automatically deleted and a notification message is sent to both the sender and recipient of the e-mail informing them that a virus has been found.

As an extra layer of protection, the anti-virus module also ensures that no attachments of a blocked type (e.g. .bat, .cmd, .exe) are delivered to the recipient.

Furthermore, to ensure that it's up to date with the latest virus threats, the anti-virus module automatically checks every hour for updates, which if found, are applied instantly, ensuring that your e-mail is protected around the clock.

---

## Features

- Dangerous attachment file types blocked at the server level
- Incoming and outgoing e-mail scanned by two anti-virus engines
- Checks against thousands of known viruses, trojans and worms
- Attachments decompressed and scanned, e.g. zip files
- Instant, automatic deletion of e-mail containing a virus
- Notification message sent to both sender and recipient
- Message header inserted into each scanned e-mail
- Self updates, every hour, 24hrs a day, 7 days a week

---

## How it Works

As soon as an e-mail enters the anti-virus module of AVAS it is first decoded and any attachments are stripped from the message and if necessary decompressed (e.g. zip files). The message and the attachments are then scanned by two independent, award winning anti-virus engines from different vendors against thousands of known viruses, trojans and worms.

If either engine detects a virus the message is automatically deleted and both the sender and recipient receive a notification message informing them that a virus was found.

Alternatively, if the message is found to be clean, an additional message header is inserted to let you know it has been scanned by the anti-virus module.

```
X-Spam-Flag: Yes  
X-Spam-Bayesian-Score: 100.00%  
X-Spam-SpamAssassin-Score: 0.33  
X-Spam-SpamAssassin-Level:  
X-Spam-SpamAssassin-Tests: INVALID_DATE,HTML_MESSAGE  
X-Spam-Reason: Bayesian=100.00%  
X-Virus-Scanned: Yes
```

Figure 2 - A 'clean' e-mail that has been scanned by the anti-virus module

Please Note: If you accidentally send a virus, the anti-virus module of AVAS will not tell the recipient, thereby ensuring you suffer no embarrassment. Also, no additional message header is inserted in outgoing e-mail.

The anti-virus module of AVAS also has a list of dangerous attachment file types that it will not accept (e.g. .bat, .cmd, .exe). If a message is sent with one of these file types attached to it, it will be rejected and not accepted for delivery.

If you would like the anti-virus module to reject messages containing additional attachment file types, please see 'Blocking Attachment File Types' in Chapter 4 for more information.

---

## Moving or Deleting Virus Notifications

Whenever a virus is detected in an e-mail that is being sent to you or by you, the anti-virus module of AVAS will send you a notification message. This notification message contains various information, such as who sent the



message, who it was being sent to, and what attachments (if any) the message had.

Instead of the notifications arriving in your inbox with your other e-mail, you may prefer to have them moved to a different folder or just deleted. Both of these can be accomplished fairly easily depending on how you receive your e-mail and which program you use.

Below, we have listed information on how to create rules in the WebMail interface, Microsoft Outlook and Microsoft Outlook Express.

Please Note: If you are using IMAP to receive your e-mail you will be unable to set-up these rules on your computer. Please contact technical support for more information.

### WebMail Interface

If you predominately use the WebMail interface and don't collect your e-mail using either POP3 or IMAP and would like to configure a rule to either move or delete the virus notifications, please follow the steps below:

#### Moving Virus Notifications to a Folder

1. Log into the WebMail interface as usual.
2. Create a new folder to hold the virus notifications by entering the name, e.g. 'Viruses' into the text box on the left hand side of the screen above your current folder list and then click on the 'Add' button.
3. Click on the 'Settings' link in the top menu followed by the 'Processing Rules' link on the left hand side and then click on the 'Add' button.
4. In the text box next to 'Filter name:' enter a name for this rule, e.g. 'Move virus notifications' and make sure there is a tick next to 'Active'.
5. Select 'contains' from the drop down list next to 'Subject:' and on the right hand side in the text box enter 'Warning: Virus found by AVAS Anti-Virus module'.
6. Select the new folder you created in step 2 above in the drop down list next to 'Move message to:' and then click on the 'Add Filter' button.
7. You will now be returned to the processing rules window.
8. Make sure that there is a tick next to 'Enable processing rules'.

That's it. Every time you log into the WebMail interface, any virus notifications will be moved automatically to the folder you created.

### Deleting Virus Notifications

1. Log into the WebMail interface as usual.
2. Click on the 'Settings' link in the top menu followed by the 'Processing Rules' link on the left hand side and then click on the 'Add' button.
3. In the text box next to 'Filter name:' enter a name for this rule, e.g. 'Delete virus notifications' and make sure there is a tick next to 'Active'.
4. Select 'contains' from the drop down list next to 'Subject:' and on the right hand side in the text box enter 'Warning: Virus found by AVAS Anti-Virus module'.
5. Select '!! Delete message !!' in the drop down list next to 'Move message to:' and then click on the 'Add Filter' button.
6. You will now be returned to the processing rules window.
7. Make sure that there is a tick next to 'Enable processing rules'.

That's it. Every time you log into the WebMail interface, any virus notifications will be automatically deleted.

### Microsoft Outlook

If you use Microsoft Outlook to collect your e-mail using POP3 and would like to configure a rule to either move or delete the virus notifications, please follow the steps below:

### Moving Virus Notifications to a Folder

1. Open Microsoft Outlook as normal.
2. Select 'Rules Wizard' from the 'Tools' menu.
3. Click on the 'New' button and make sure that 'Start from a blank rule' is selected.
4. Select 'Check messages when they arrive' and then click on the 'Next' button.
5. Tick 'with specific words in the subject' and in the bottom half of the screen click on the 'specific words' link.
6. In the window that opens enter 'Warning: Virus found by AVAS Anti-Virus module' in the text box and then click on the 'Add' button.
7. Click on the 'OK' button followed by the 'Next' button.
8. Tick 'move it to the specified folder' and in the bottom half of the screen click on the 'specified' link and then click on the 'New' button.
9. Enter a name for the new folder to where the virus notifications should be moved, e.g. 'Viruses' and click on the 'OK' button.
10. Highlight the folder you just created and click on the 'OK' button.

11. In the top panel scroll down and tick 'stop processing more rules'.
12. Click on the 'Next' button twice and enter a name for the rule, e.g. 'Move virus notifications' and make sure that there is a tick next to 'Turn on this rule'.
13. Click on the 'Finish' button and then click on the 'OK' button.

That's it. Every time you collect your e-mail, any virus notifications will be moved automatically to the folder you created.

### Deleting Virus Notifications

1. Open Microsoft Outlook as normal.
2. Select 'Rules Wizard' from the 'Tools' menu.
3. Click on the 'New' button and make sure 'Start from a blank rule' is selected.
4. Select 'Check messages when they arrive' and then click on the 'Next' button.
5. Tick 'with specific words in the subject' and in the bottom half of the screen click on the 'specific words' link.
6. In the window that opens enter 'Warning: Virus found by AVAS Anti-Virus module' in the text box and then click on the 'Add' button.
7. Click on the 'OK' button followed by the 'Next' button.
8. In the top panel tick both 'delete it' and 'stop processing more rules'.
9. Click on the 'Next' button twice and enter a name for the rule, e.g. 'Delete virus notifications' and make sure that there is a tick next to 'Turn on this rule'.
10. Click on the 'Finish' button and then click on the 'OK' button.

That's it. Every time you collect your e-mail, any virus notifications will be automatically deleted.

### Microsoft Outlook Express

If you use Microsoft Outlook Express to collect your e-mail using POP3 and would like to configure a rule to either move or delete the virus notifications, please follow the steps below:

### Moving Virus Notifications to a Folder

1. Open Microsoft Outlook Express as normal.
2. From the 'Tools' menu select 'Message Rules' and then select 'Mail'.
3. In section 1, tick 'Where the Subject line contains specific words' and in section 3, click on the 'specific words' link.
4. In the window that opens enter 'Warning: Virus found by AVAS Anti-Virus module'

in the text box and click on the 'Add' button and then click on the 'OK' button.

5. In section 2, tick 'Move it to the specified folder' and in section 3, click on the 'specified' link and then click on the 'New' button.
6. Enter a name for the new folder to where the virus notifications should be moved, e.g. 'Viruses' and then click on the 'OK' button.
7. Highlight the folder you just created and click on the 'OK' button.
8. In section 2, scroll down and tick 'Stop processing more rules'.
9. In section 4, enter a name for the rule, e.g. 'Move virus notifications' and click on the 'OK' button twice.

That's it. Every time you collect your e-mail, any virus notifications will be moved automatically to the folder you created.

### Deleting Virus Notifications

1. Open Microsoft Outlook Express as normal.
2. From the 'Tools' menu select 'Message Rules' and then select 'Mail'.
3. In section 1, tick 'Where the Subject line contains specific words' and in section 3, click on the 'specific words' link.
4. In the window that opens enter 'Warning: Virus found by AVAS Anti-Virus module' in the text box and click on the 'Add' button and then click on the 'OK' button.
5. In section 2, tick both 'Delete it' and 'Stop processing more rules'.
6. In section 4, enter a name for the rule, e.g. 'Delete virus notifications' and click on the 'OK' button twice.

That's it. Every time you collect your e-mail, any virus notifications will be automatically deleted.

---

## Frequently Asked Questions

### Why do you use two anti-virus engines and not just one?

The simple answer is reliability.

As with any anti-virus software, to be able to detect a specific virus the software has to know what to look for. The virus definition files that are supplied and updated by the anti-virus software vendors contain this information.

Until the virus definitions are updated after a new virus has been released, it is unlikely that the software will detect the new virus (heuristic scanning aside).

---

As there is a time delay between the release of a new virus and the virus definitions being updated by each vendor, if we only used one engine, we would be solely reliant on that vendor updating their definitions quickly to be able to protect your e-mail. By using two engines, the time before our anti-virus module protects against the new virus is significantly decreased.

Furthermore, each anti-virus engine works differently. Whilst one engine may not detect a new variant of a virus until the virus definitions have been updated, the other one may, thereby protecting your e-mail even quicker.

#### Why don't you use the same anti-virus software that I do?

Both of the anti-virus engines that the anti-virus module uses are unlikely to be the same as that installed on your computer. This in itself offers a further layer of protection.

If the anti-virus module used the same anti-virus engines as what you have installed on your computer then it becomes semi-redundant, simply because if our engines don't catch the virus, and we're both using the same technology, it's unlikely yours will either.

By using engines that aren't installed on your computer, if a virus passes through our system, it is still possible that your desktop software will detect it.

#### Why do you notify both the sender and recipient?

Firstly, we notify the recipient so that they that know someone tried to send them a message. This enables them to contact the sender if they believe that the message is important.

Secondly, we notify the sender so that they are aware that their computer may be infected and should therefore run a virus scan as soon as possible.

Please Note: If you accidentally send a virus, the anti-virus module of AVAS will not tell the recipient, thereby ensuring you suffer no embarrassment.

#### Why do you block certain attachment file types?

Many current viruses transmit themselves as a .pif file (Program Information File) or a .scr file (Screensaver) attached to a message, and it is quite likely that viruses released in the future will do so as well.

By blocking these file types (amongst others), if a new virus is released which transmits itself as a .pif file and the anti-virus vendors have not yet updated their definitions, you will still be protected as the message with the attachment will be rejected and not delivered.

Furthermore, most e-mail programs such as Outlook prevent access to certain attachments to help protect your e-mail. As you are unable to view these attachments, it makes sense to not accept them.

Please Note: The file types that we block are fairly specific and are unlikely to cause you any inconvenience. If you would like the anti-virus module to reject messages containing additional attachment file types, please see 'Blocking Attachment File Types' in Chapter 4 for more information

---

## Important Note

No anti-virus system can guarantee a 100% detection rate and therefore the anti-virus module of AVAS should be thought of as an add-on and not a replacement for desktop anti-virus software. There are many sources of possible virus infection and whilst the anti-virus module will help with viruses transmitted by e-mail, it will not offer any protection against viruses transmitted by floppy disk, CD, DVD or across a network.

---

## The Anti-Virus Module at a Glance

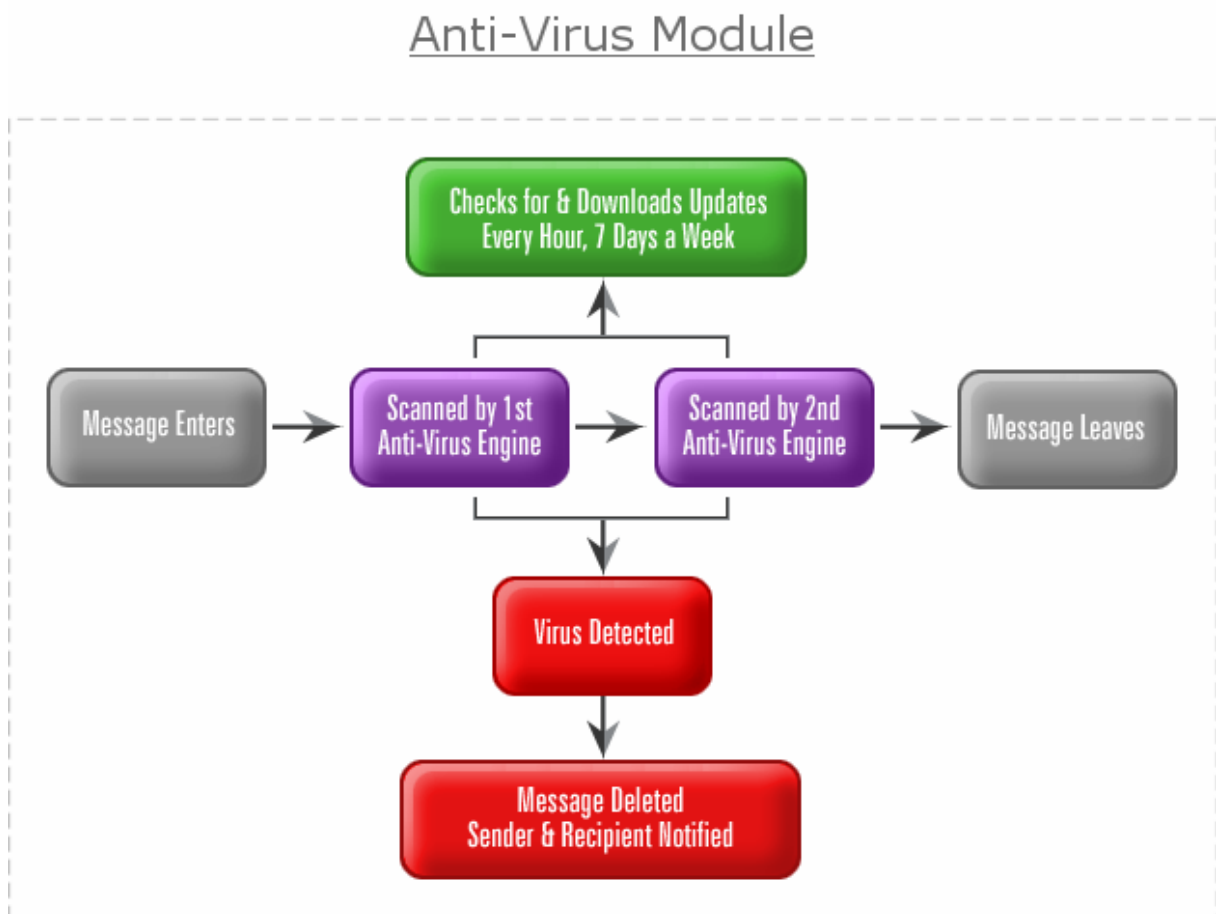


Figure 3 - The flow of a message through the anti-virus module

---

## CHAPTER 3

# Anti-Spam Module

### In This Chapter

Summary .....	15
Features .....	16
How it Works .....	16
The Five Anti-Spam Engines.....	17
How the Message is Altered.....	18
Teaching the Bayesian Analysis Engine .....	21
Moving or Deleting Spam Messages.....	23
Moving or Deleting Spam Messages - Whitelisting ..	27
Moving or Deleting Spam Messages - Advanced ....	30
Frequently Asked Questions .....	33
The Anti-Spam Module at a Glance .....	35

---

## Summary

The multi-level anti-spam module of AVAS passes every incoming message through five separate anti-spam engines to identify any spam like characteristics. If any engine considers the message to be possible or likely spam, both the subject and message headers are altered to let you know which engine failed the message as well as the relevant Bayesian Analysis and SpamAssassin scores.

As the anti-spam module will never reject a message unless it is corrupt, you can use the features available to you in your e-mail program to set up advanced rules defining exactly what you would like to do with any spam messages.

For example, you could specify that messages marked as likely spam are automatically moved to a separate folder, except for messages failed by the DNS Blacklist Lookup engine, these you choose to automatically delete - The choice is endless, and you're in control!

To ensure that messages are delivered, spammers constantly change tactics to avoid anti-spam systems. The anti-spam engines within the anti-spam module of AVAS are updated by both the software vendors and ourselves to increase their accuracy and to ensure that they remain up to date. Using a feature available to you in the WebMail interface, you can also teach the Bayesian Analysis engine so that it learns from the messages that you receive, further helping to reduce the amount of spam reaching your inbox.

---

## Features

- Non-fixable, corrupt messages automatically rejected
  - Incoming e-mail passed through five separate anti-spam engines
  - Message subject automatically altered if the message fails any engine
  - Message headers inserted providing more detailed information
  - Periodically updated by both the software vendors and ourselves
  - The ability to teach the Bayesian Analysis engine from e-mail you receive
  - Additional custom filters and spam marking capability (see Chapter 4)
- 

## How it Works

When an incoming e-mail enters the anti-spam module of AVAS it first has additional message headers inserted to hold the Bayesian Analysis and SpamAssassin scores. It is then automatically passed through five separate anti-spam engines before leaving.

Whilst passing through the module, if any of the engines detect the message as possible or likely spam both the subject of the message and the message headers are altered to provide more detailed information.

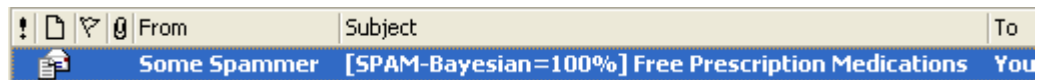


Figure 4 - Example of the subject alteration when a message is detected as likely spam

```

X-Spam-Flag: Yes
X-Spam-Bayesian-Score: 100.00%
X-Spam-SpamAssassin-Score: 0.33
X-Spam-SpamAssassin-Level:
X-Spam-SpamAssassin-Tests: INVALID_DATE,HTML_MESSAGE
X-Spam-Reason: Bayesian=100.00%
  
```

Figure 5 - Example of the message headers altered when a message is detected as spam

Please see 'The Five Anti-Spam Engines' section below for more detailed information on what each engine does. To find out how the message is altered, please see the 'How the Message is Altered' section, also below.

Please Note: Messages you send to remote users do not pass through the anti-spam module and therefore are not altered. Also, messages between local users, whilst analysed, will never be marked as spam.



Finally, the anti-spam module of AVAS also checks each e-mail to ensure that it conforms to certain rules and isn't 'corrupted', i.e. it has a complete message-id, the addressing information is present and that it doesn't violate RFC822.

In certain circumstances the anti-spam module will automatically attempt to fix a corrupt message and only reject it if it's unfixable, in others, e.g. in the case of a missing message-id it is rejected immediately.

If you would like the anti-spam module to reject or perform other actions on incoming e-mail, please see Chapter 4 for more information.

---

## The Five Anti-Spam Engines

The five anti-spam engines used by the anti-spam module of AVAS are:

### Bayesian Analysis Engine

**Method:** The Bayesian Analysis engine calculates the probability of a message being spam by comparing the occurrence of words with a database containing both genuine and spam messages.

**Determination:** If the probability is higher than a pre-set percentage, the engine determines that the message is likely spam. If it's slightly lower, it's determined that it's possible spam. If it's lower still, it's determined that the message is probably not spam.

**Updated by:** Software vendor, ourselves and users.

### SpamAssassin Filtering Engine

**Method:** The SpamAssassin Filtering engine, which is based on the open source project at <http://www.spamassassin.org/>, performs a wide range of heuristic tests on both the headers and content of a message by using its own extensive rule base. Each rule a message fails has a set score.

**Determination:** If the total score is higher than the pre-set limit, the engine determines that the message is likely spam. If it's slightly lower, it's determined that it's possible spam. If it's lower still, it's determined that the message is probably not spam.

**Updated by:** Software vendor and ourselves.

### HTML/Character Set Filtering Engine

**Method:** The first part of the HTML/Character Set Filtering engine performs a range of tests on an HTML message looking for common techniques used by spammers. The second part detects messages which have information about the character set missing from the message header or are either using a forbidden character set or have characters outside of the usual range.

**Determination:** If a message fails any individual test, the engine determines that the message is likely spam. This engine may label some HTML newsletters as spam, simply because of their formatting.

**Updated by:** Software vendor and ourselves.

### Regular Expression Filtering Engine

**Method:** The Regular Expression Filtering engine analyses the entire message, from the headers through to the body looking for strings that match a particular regular expression. Each matched expression is allocated a set score. With several thousand specific expressions defined, this engine is designed to catch spam messages that may have been already passed by the other engines.

**Determination:** If the total score is high enough, the engine determines that the message is likely spam.

**Updated by:** Software vendor and ourselves.

### DNS Blacklist Lookup Engine

**Method:** The DNS Blacklist Lookup engine makes use of three public databases that contain a list of IP addresses of verified open relays, spam sources (including spammers, spam gangs and spam support services) and 3<sup>rd</sup> party exploits (including open proxies, worms and viruses with built-in spam engines and other types of trojan-horse type exploits). The server that the e-mail has originated from is then 'looked up' in these databases.

**Determination:** If the IP address of the server is listed in one of the databases the engine determines that the message is likely spam.

**Updated by:** Not applicable. IP addresses in the databases are added and removed through a process of automatic testing and re-testing.

---

## How the Message is Altered

Every message that is passed through the anti-spam module of AVAS has additional headers inserted to hold both the Bayesian Analysis and SpamAssassin scores.

Whilst passing through the module, if any of the anti-spam engines detect the message as possible or likely spam both the subject of the message and the message headers are altered to provide more detailed information.

Listed below are the alterations that are made to the subject by each engine, as well as information on the headers that are inserted and altered.

## Subject Alteration

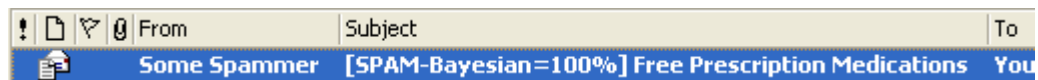


Figure 6 - Example of the subject alteration

### Bayesian Analysis Engine

**Possible Spam:** [SPAM?-Bayesian=xx%] <Original Subject>  
**Example:** [SPAM?-Bayesian=83.5%] Free Prescription Medications

**Likely Spam:** [SPAM-Bayesian=xx%] <Original Subject>  
**Example:** [SPAM-Bayesian=98.8%] Free Prescription Medications

### SpamAssassin Filtering Engine

**Possible Spam:** [SPAM?-SpamAssassin=x.xx] <Original Subject>  
**Example:** [SPAM?-SpamAssassin=7.16] Free Prescription Medications

**Likely Spam:** [SPAM-SpamAssassin=x.xx] <Original Subject>  
**Example:** [SPAM-SpamAssassin=9.45] Free Prescription Medications

### HTML/Character Set Filtering Engine

**Likely Spam:** [SPAM-HTML/CharSet] <Original Subject>  
**Example:** [SPAM-HTML/CharSet] Free Prescription Medications

### Regular Expression Filtering Engine

**Likely Spam:** [SPAM-RegEx] <Original Subject>  
**Example:** [SPAM-RegEx] Free Prescription Medications

### DNS Blacklist Lookup Engine

**Likely Spam:** [SPAM-DNSBL] <Original Message>  
**Example:** [SPAM-DNSBL] Free Prescription Medications

## Headers Inserted and Altered

```
X-Spam-Flag: Yes  
X-Spam-Bayesian-Score: 100.00%  
X-Spam-SpamAssassin-Score: 0.33  
X-Spam-SpamAssassin-Level:  
X-Spam-SpamAssassin-Tests: INVALID_DATE,HTML_MESSAGE  
X-Spam-Reason: Bayesian=100.00%
```

Figure 7 - Example of the message headers inserted and altered

### X-Spam-Flag:

The X-Spam-Flag will be set to one of three values; 'Yes' 'No' or 'Possible' depending on whether or not the anti-spam module determined the message to be spam, not spam or possible spam.

### X-Spam-Bayesian-Score:

Contains a percentage between 0 and 100 with the probability that the message is spam as determined by the Bayesian Analysis engine.

### X-Spam-SpamAssassin-Score:

Contains a score between 0.00 and 1000.00 with the total score of the rules that the message failed as determined by the SpamAssassin Filtering engine.

### X-SpamAssassin-Level:

A visual indicator of the total SpamAssassin score, using \*'s, e.g. if the score is 5.0, the X-Spam-SpamAssassin-Level would show five stars, (\*\*\*\*\*).

### X-SpamAssassin-Tests:

Contains a comma separated list of the SpamAssassin rules that the message failed.

### X-Spam-Reason:

Primarily reflects the information in the subject of a message marked as spam, however does contain additional information if the Regular Expression Filtering or DNS Blacklist Lookup engines determine the message as spam.

In the case of the Regular Expression Filtering engine, the X-Spam-Reason header will contain the name of the filter file that was triggered, e.g. RegEx=nigerian\_scam.

If the DNS Blacklist Lookup engine is triggered, the X-Spam-Reason header will contain the name of the blacklist on which the IP address is listed, e.g. DNSBL=sbl.spamhaus.org.

If no engine is triggered the X-Spam-Reason will be set to 'N/A'.

Please Note: Messages between local users are never marked as spam so the subject will remain unaltered, the X-Spam-Flag will be set to 'No' and the X-Spam-Reason will be set to 'N/A'. The other message headers may contain data as the message is still analysed.

---

## Teaching the Bayesian Analysis Engine & the 'Spam Folder'

Out of the five anti-spam engines, the Bayesian Analysis engine is the only one that can be taught by users of AVAS. By teaching the Bayesian Analysis engine you can help it to improve on its detection rate and reduce the number of false positives (genuine e-mails) that it marks as spam.

There are currently two ways to teach the engine. You can either forward e-mail to a specific e-mail address or use your inbox and the 'Spam Folder'.

Below is information on each method and which method may best suit you.

Please Note: You don't have to teach the Bayesian Analysis engine.

### **Forwarding E-Mail – You use POP3 and not the WebMail interface**

If you are using POP3 to collect your e-mail you won't actually have a 'Spam Folder', so the only way you can teach the engine is to forward any e-mail you would like indexed to one of the e-mail addresses below.

Depending on the e-mail address to which you forward an e-mail, the e-mail will be indexed as either genuine or spam and stored in a database. The database is then used by the Bayesian Analysis engine when determining the probability of an incoming message being spam.

[genuine@mail.netenergy.net](mailto:genuine@mail.netenergy.net)

E-Mail forwarded to this address is indexed as genuine and therefore messages containing similar content should have a low probability of being spam.

spam@mail.netenergy.net

E-Mail forwarded to this address is indexed as spam and therefore messages containing similar content should have a high probability of being spam.

Please Note: Any e-mail you forward to the e-mail addresses shown above may be reviewed before being indexed and may be rejected.

### Using your Inbox and the 'Spam Folder' – You use IMAP and/or WebMail

If you are using IMAP and/or the WebMail interface to manage your e-mail then to index messages as spam or genuine and to have them stored in the database that is used by the Bayesian Analysis engine when determining the probability of incoming messages being spam couldn't be easier.

Simply move the messages you would like indexed as spam into your 'Spam Folder' and the messages you would like indexed as genuine into your inbox. Then log into the WebMail interface and select 'Spam Index Now' from the drop down list and click on the 'OK' button.

Please Note: Any messages stored in the 'Spam Folder' are automatically deleted after they are 14 days old.

After indexing you can either delete the messages in your 'Spam Folder' or alternatively leave them in the folder and the system will automatically delete them when they are 14 days old.

Please Note: You should have an equal number of genuine messages in your inbox before clicking 'Spam Index Now'.

### Correcting Mistakes

If you accidentally forward an e-mail to the wrong address, or move an e-mail to the spam folder which you meant to move to your inbox before indexing (or vice-versa), you can simply forward the same e-mail to one of the following addresses to fix the problem.

genuine-spam@mail.netenergy.net

**When to Use:** You accidentally forwarded the spam e-mail to the genuine e-mail address, or you had the spam e-mail in your inbox when you clicked 'Spam Index Now' in the WebMail interface.

**Action Taken:** The message will be de-indexed from the genuine category.

spam-genuine@mail.netenergy.net

**When to Use:** You accidentally forwarded the genuine e-mail to the spam e-mail address, or you had the genuine e-mail in your 'Spam Folder' when you clicked 'Spam Index Now' in the WebMail interface.

**Action Taken:** The message will be de-indexed from the spam category.

Please Note: Any e-mail you forward to the e-mail addresses shown above may be reviewed before being de-indexed and may be rejected.

---

## Moving or Deleting Spam Messages

Whenever an e-mail is detected as possible or likely spam by any of the five engines within the anti-spam module of AVAS, both the subject and message headers are altered to enable you to visibly see that the anti-spam module believes the message to be spam.

Instead of the messages arriving in your inbox with your other e-mail, you may prefer to have them moved to a different folder (including the special 'Spam Folder') or just deleted. Both of these can be accomplished fairly easily depending on how you receive your e-mail and which program you use.

Below we have listed information on how to create rules in the WebMail interface, Microsoft Outlook and Microsoft Outlook Express to either move or delete likely spam messages.

Please Note: If you are using IMAP to receive your e-mail you will be unable to set-up these rules on your computer. Please contact technical support for more information.

To ensure that messages from specific senders which may be marked as spam are not moved or deleted, you can set-up a whitelist rule in addition to the rules below. For more information on whitelisting, please see the 'Moving or Deleting Spam Messages – Whitelisting' section below.

If you would like to move or delete possible spam messages or build rules to perform different actions based on the engine that failed the message then you can follow the same procedures outlined below, however you need to use the information contained within 'How the Message is Altered' section above to ensure that you use the correct subject text.

A few examples of moving and deleting both possible spam messages as well as likely spam messages that failed a specific engine can be found in the section below, 'Moving or Deleting Spam Messages – Advanced'. These examples also use whitelisting to ensure e-mails from specific senders are not moved or deleted.

Please Note: We do not recommend you delete any possible or likely spam messages unless you are 100% happy with the accuracy of the anti-spam module. If you find that certain engines perform better than others you can create rules that are based only on messages that fail those specific engines by altering the subject text the rule is based on.

Please see the 'How the Message is Altered' section above for a complete breakdown of the different subject text used by each engine as well as the 'Moving or Deleting Spam Messages – Advanced' section below for a few examples.

## WebMail Interface

If you predominately use the WebMail interface and don't collect your e-mail using either POP3 or IMAP and would like to configure a rule to either move or delete messages identified as likely spam, please follow the steps below:

### Moving Likely Spam Messages to a Folder

1. Log into the WebMail interface as usual.
2. Create a new folder to hold the likely spam messages by entering the name, e.g. 'Spam-Likely' into the text box on the left hand side of the screen above your current folder list and then click on the 'Add' button.
3. Click on the 'Settings' link in the top menu followed by the 'Processing Rules' link on the left hand side then click on the 'Add' button.
4. In the text box next to 'Filter name:' enter a name for this rule, e.g. 'Move likely spam messages' and make sure there is a tick next to 'Active'.
5. Select 'contains' from the drop down list next to 'Subject:' and on the right hand side in the text box enter '[SPAM-']
6. Select the new folder you created in step 2 above in the drop down list next to 'Move message to:' and then click on the 'Add Filter' button.
7. You will now be returned to the processing rules window.
8. Make sure that there is a tick next to 'Enable processing rules'.

That's it. Every time you log into the WebMail interface, any likely spam messages will be moved automatically to the folder you created.

Please Note: If you wish you can use the special 'Spam Folder' as the folder to which you move the likely spam messages. Simply select it from the drop down list in step 6. By doing so you can then periodically select 'Spam Index Now' from the drop down list in the WebMail interface to teach the Bayesian Analysis engine. For more information, please see the 'Teaching the Bayesian Analysis Engine & the Spam Folder' section above.

If you do decide to use the 'Spam Folder' please remember that any messages stored within it are automatically deleted after they are 14 days old.



### Deleting Likely Spam Messages

1. Log into the WebMail interface as usual.
2. Click on the 'Settings' link in the top menu followed by the 'Processing Rules' link on the left hand side and then click on the 'Add' button.
3. In the text box next to 'Filter name:' enter a name for this rule, e.g. 'Delete spam messages' and make sure there is a tick next to 'Active'.
4. Select 'contains' from the drop down list next to 'Subject:' and on the right hand side in the text box enter '[SPAM-']
5. Select '!! Delete message !!' in the drop down list next to 'Move message to:' and then click on the 'Add Filter' button.
6. You will now be returned to the processing rules window.
7. Make sure that there is a tick next to 'Enable processing rules'.

That's it. Every time you log into the WebMail interface, any likely spam messages will be automatically deleted.

### Microsoft Outlook

If you use Microsoft Outlook to collect your e-mail using POP3 and would like to configure a rule to either move or delete messages identified as likely spam, please follow the steps below:

### Moving Likely Spam Messages to a Folder

1. Open Microsoft Outlook as normal.
2. Select 'Rules Wizard' from the 'Tools' menu.
3. Click on the 'New' button and make sure that 'Start from a blank rule' is selected.
4. Select 'Check messages when they arrive' and click the 'Next' button.
5. Tick 'with specific words in the subject' and in the bottom half of the screen click on the 'specific words' link.
6. In the window that opens enter '[SPAM-' in the text box and then click on the 'Add' button.
7. Click on the 'OK' button followed by the 'Next' button.
8. Tick 'move it to the specified folder' and in the bottom half of the screen click on the 'specified' link and then click on the 'New' button.
9. Enter a name for the new folder to where the likely spam messages should be moved, e.g. 'Spam-Likely' and click on the 'OK' button.
10. Highlight the folder you just created and click on the 'OK' button.

11. In the top panel scroll down and tick 'stop processing more rules'.
12. Click on the 'Next' button twice and enter a name for the rule, e.g. 'Move likely spam messages' and make sure that there is a tick next to 'Turn on this rule'.
13. Click on the 'Finish' button and then click on the 'OK' button.

That's it. Every time you collect your e-mail, any likely spam messages will be moved automatically to the folder you created.

### Deleting Likely Spam Messages

1. Open Microsoft Outlook as normal.
2. Select 'Rules Wizard' from the 'Tools' menu.
3. Click on the 'New' button and make sure that 'Start from a blank rule' is selected.
4. Select 'Check messages when they arrive and click on the 'Next' button.
5. Tick 'with specific words in the subject' and in the bottom half of the screen click on the 'specific words' link.
6. In the window that opens enter '[SPAM-' in the text box and then click on the 'Add' button.
7. Click on the 'OK' button followed by the 'Next' button.
8. In the top panel, tick both 'delete it' and 'stop processing more rules'.
9. Click on the 'Next' button twice and enter a name for the rule, e.g. 'Delete likely spam messages' and make sure that there is a tick next to 'Turn on this rule'.
10. Click on the 'Finish' button and then click on the 'OK' button.

That's it. Every time you collect your e-mail, any likely spam messages will be automatically deleted.

### Microsoft Outlook Express

If you use Microsoft Outlook Express to collect your e-mail using POP3 and would like to configure a rule to either move or delete messages identified as likely spam, please follow the steps below:

### Moving Likely Spam Messages to a Folder

1. Open Microsoft Outlook Express as normal.
2. From the 'Tools' menu select 'Message Rules' and then select 'Mail'.
3. In section 1, tick 'Where the Subject line contains specific words' and in section 3, click on the 'specific words' link.
4. In the window that opens enter '[SPAM-' in the text box and click on the 'Add'

button and then click on the 'OK' button.

5. In section 2, tick 'Move it to the specified folder' and in section 3, click on the 'specified' link and then click on the 'New' button.
6. Enter a name for the new folder to where the likely spam messages should be moved, e.g. 'Spam-Likely' and then click on the 'OK' button.
7. Highlight the folder you just created and click on the 'OK' button.
8. In section 2, scroll down and tick 'Stop processing more rules'.
9. In section 4, enter a name for the rule, e.g. 'Move likely spam messages' and click on the 'OK' button twice.

That's it. Every time you collect your e-mail, any likely spam messages will be moved automatically to the folder you created.

### Deleting Likely Spam Messages

1. Open Microsoft Outlook Express as normal.
2. From the 'Tools' menu select 'Message Rules' and then select 'Mail'.
3. In section 1, tick 'Where the Subject line contains specific words' and in section 3, click on the 'specific words' link.
4. In the window that opens enter '[SPAM-' in the text box and click on the 'Add' button and then click on the 'OK' button.
5. In section 2, tick both 'Delete it' and 'Stop processing more rules'.
6. In section 4, enter a name for the rule, e.g. 'Delete likely spam messages' and click on the 'OK' button twice.

That's it. Every time you collect your e-mail, any likely spam messages will be automatically deleted.

---

## Moving or Deleting Spam Messages - Whitelisting

If you haven't as yet read the section above, 'Moving or Deleting Spam Messages' please do so before reading this section.

On occasions you may find that one or more of the anti-spam modules label a genuine message as spam and if you are using rules similar to the ones in the previous section, the message may have been automatically moved to a separate folder. To prevent this for a particular sender, you are able to create a 'whitelist' rule containing the senders address.

Below we have listed information on how to create a 'whitelist' rule in the WebMail interface, Microsoft Outlook and Microsoft Outlook Express.

Please Note: If you are using IMAP to receive your e-mail you will be unable to set-up these rules on your computer. Please contact technical support for more information.

Messages sent by a whitelisted sender will still be marked as spam if any of the anti-spam engines believe the message is spam. By whitelisting a sender you are simply stopping any other rules from moving the message.

## WebMail Interface

If you predominately use the WebMail interface and don't collect your e-mail using either POP3 or IMAP and would like to configure a rule to whitelist a particular sender, please follow the steps below:

### Creating a Whitelist Rule

1. Log into the WebMail interface as usual.
2. Click on the 'Settings' link in the top menu followed by the 'Processing Rules' link on the left hand side and then click on the 'Add' button.
3. In the text box next to 'Filter name:' enter a name for this rule, e.g. 'Whitelist messages from someone@domain.co.uk' and make sure there is a tick next to 'Active'.
4. Select 'contains' from the drop down list next to 'From:' and on the right hand side in the text box enter either the e-mail address or domain name of the sender you would like to whitelist, e.g. 'someone@domain.co.uk'.
5. Select 'Inbox' in the drop down list next to 'Move message to:' and then click on the 'Add Filter' button.
6. You will now be returned to the processing rules window.
7. Using the arrows in the middle of the screen, move the rule you just created above any other rules that move possible or likely spam messages.
8. Finally, make sure that there is a tick next to 'Enable processing rules'.

That's it. Every time you log into the WebMail interface, any messages from someone@domain.co.uk will be left in your inbox.

## Microsoft Outlook

If you use Microsoft Outlook to collect your e-mail using POP3 and would like to configure a rule to whitelist a particular sender, please follow the steps below:

### Creating a Whitelist Rule

1. Open Microsoft Outlook as normal.
2. Select 'Rules Wizard' from the 'Tools' menu.
3. Click on the 'New' button and make sure that 'Start from a blank rule' is selected.
4. Select 'Check messages when they arrive' and then click the 'Next' button.
5. Tick 'with specific words in the sender's address' and in the bottom half of the screen click on the 'specific words' link.
6. In the window that opens enter either the e-mail address or domain name of the sender you would like to whitelist in the text box, e.g. 'someone@domain.co.uk' and then click on the 'Add' button.
7. Click on the 'OK' button followed by the 'Next' button.
8. In the top panel scroll down and tick 'stop processing more rules'.
9. Click on the 'Next' button twice and enter a name for the rule, e.g. 'Whitelist messages from someone@domain.co.uk' and make sure that there is a tick next to 'Turn on this rule'.
10. Click on the 'Finish' button.
11. Using the 'Move Up' and 'Move Down' buttons, move the rule you just created above any other rules that move possible or likely spam messages.

That's it. Every time you collect your e-mail, any messages from someone@domain.co.uk will be left in your inbox.

## Microsoft Outlook Express

If you use Microsoft Outlook Express to collect your e-mail using POP3 and would like to configure a rule to whitelist a particular sender, please follow the steps below:

### Creating a Whitelist Rule

1. Open Microsoft Outlook Express as normal.
2. From the 'Tools' menu select 'Message Rules' and then select 'Mail'.
3. In section 1, tick 'Where the From line contains people' and in section 3, click on the 'contains people' link.
4. In the window that opens enter either the e-mail address or domain name of the sender you would like to whitelist in the text box, e.g. 'someone@domain.co.uk'

and click on the 'Add' button and then click on the 'OK' button.

5. In section 2, scroll down and tick 'Stop processing more rules'.
6. In section 4, enter a name for the rule, e.g. 'Whitelist messages from someone@domain.co.uk' and click on the 'OK' button.
7. Using the 'Move Up' and 'Move Down' buttons, move the rule you just created above any other rules that move possible or likely spam messages.
8. Click on the 'OK' button.

That's it. Every time you collect your e-mail, any messages from someone@domain.co.uk will be left in your inbox.

---

## Moving or Deleting Spam Messages - Advanced

If you haven't as yet read the two sections above, 'Moving or Deleting Spam Messages' and 'Moving or Deleting Spam Messages – Whitelisting' please do so before reading this section.

For the purpose of this section we are going to assume you are using Microsoft Outlook Express to collect your e-mail via POP3 and want to perform the following actions:

1. Messages from someone@domain.co.uk should be whitelisted and never be moved or deleted whether or not they are marked as possible or likely spam.
2. Messages determined as possible spam by either the Bayesian Analysis or SpamAssassin Filtering engines should be moved to a folder called 'Spam-Possible'.
3. Messages determined as likely spam by either the Bayesian Analysis, or SpamAssassin Filtering engines should be moved to a folder called 'Spam-Likely'.
4. Messages determined as likely spam by the HTML/Character Set or RegEx Filtering engines should be moved to a folder called 'Spam-Review'.
5. Messages determined as likely spam by the DNS Blacklist Lookup engine should be deleted.

We are also assuming you do not currently have any rules set-up in Outlook Express and have also already opened the program.

Please Note: To avoid downloading spam messages and to perform other actions, please see Chapter 4 for more information.

### 1. Whitelisting Messages from someone@domain.co.uk

1. From the 'Tools' menu select 'Message Rules' and then select 'Mail'.
2. In section 1, tick 'Where the From line contains people' and in section 3, click on the 'contains people' link.
3. In the window that opens enter 'someone@domain.co.uk' in the text box and click on the 'Add' button and then click on the 'OK' button.
4. In section 2, scroll down and tick 'Stop processing more rules'.
5. In section 4, enter 'Whitelist messages from someone@domain.co.uk' as the name for the rule and click on the 'OK' button.

### 2. Moving Possible Spam Messages (Bayesian/SpamAssassin)

1. Click the 'New' button.
2. In section 1, tick 'Where the Subject line contains specified words' and in section 3, click on the 'contains specific words' link.
3. In the window that opens enter '[SPAM?-Bayesian' in the text box and then click on the 'Add' button.
4. Enter '[SPAM?-SpamAssassin' in the text box and click on the 'Add' button and then click on the 'OK' button.
5. In section 2, tick 'Move it to the specified folder' and in section 3, click on the 'specified' link and then click on the 'New' button.
6. Enter 'Spam-Possible' as the name for the new folder and click on the 'OK' button.
7. Highlight the folder you just created and click on the 'OK' button.
8. In section 2, scroll down and tick 'Stop processing more rules'.
9. In section 4, enter 'Move possible spam messages to Spam-Possible (Bayesian/SpamAssassin)' as the name for the rule and click on the 'OK' button.

### 3. Moving Likely Spam Messages (Bayesian/SpamAssassin)

1. Click the 'New' button.
2. In section 1, tick 'Where the Subject line contains specified words' and in section 3, click on the 'contains specific words' link.
3. In the window that opens enter '[SPAM-Bayesian' in the text box and then click on the 'Add' button.
4. Enter '[SPAM-SpamAssassin' in the text box and click on the 'Add' button and then click on the 'OK' button.

5. In section 2, tick 'Move it to the specified folder' and in section 3, click on the 'specified' link and then click on the 'New' button.
6. Enter 'Spam-Likely' as the name for the new folder and click on the 'OK' button.
7. Highlight the folder you just created and click on the 'OK' button.
8. In section 2, scroll down and tick 'Stop processing more rules'.
9. In section 4, enter 'Move likely spam messages to Spam-Likely (Bayesian/SpamAssassin)' as the name for the rule and click on the 'OK' button.

#### 4. Moving Likely Spam Messages (HTML/Character Set/RegEx)

1. Click the 'New' button.
2. In section 1, tick 'Where the Subject line contains specified words' and in section 3, click on the 'contains specific words' link
3. In the window that opens enter '[SPAM-HTML/CharSet]' in the text box and then click on the 'Add' button.
4. Enter '[SPAM-RegEx]' in the text box and click on the 'Add' button and then click on the 'OK' button.
5. In section 2, tick 'Move it to the specified folder' and in section 3, click on the 'specified' link and then click on the 'New' button.
6. Enter 'Spam-Review' as the name for the new folder and click on the 'OK' button.
7. Highlight the folder you just created and click on the 'OK' button.
8. In section 2, scroll down and tick 'Stop processing more rules'.
9. In section 4, enter 'Move likely spam messages to Spam-Review (HTML/Character Set/RegEx)' as the name for the rule and click on the 'OK' button.

#### 5. Deleting Likely Spam Messages (DNSBL)

1. Click the 'New' button.
2. In section 1, tick 'Where the Subject line contains specific words' and in section 3, click on the 'specific words' link.
3. In the window that opens enter '[SPAM-DNSBL]' in the text box and click on the 'Add' button and then click on the 'OK' button.
4. In section 2, tick both 'Delete it' and 'Stop processing more rules'.
5. In section 4, enter 'Delete likely spam messages (DNSBL)' as the name for the rule and then click on the 'OK' button twice.



That's it. Below is a screenshot of how the rules window should now look.



Figure 8 - The completed rules in Microsoft Outlook Express

---

## Frequently Asked Questions

### Why do you use five anti-spam engines?

If you look at a handful of spam messages you will see that whilst there are (on occasion) similar characteristics, there are also a lot of differences in the messages, whether it's in the content or in the way that they are constructed.

No single anti-spam technology can claim to catch every single spam message, simply because of the differences between spam messages and because spammers constantly change tactics to ensure that wherever possible their messages are delivered.

By using five separate technologies that look at every part of a message, from the header through to the content and even the IP address that sent the message, there is a far higher probability of catching more spam than relying on a single technology.

---

### Why don't you just reject likely spam messages?

As with any anti-spam system, a genuine message can always be incorrectly labelled as spam. Because of this, when building the anti-spam module of AVAS the decision was taken not to reject likely spam messages automatically, but to let the user decide what they would like to do.

In fact, by us not automatically rejecting all likely spam messages, you are able to build a complex set of rules and filters to handle incoming messages. For example, if preferred messages detected as likely spam by some engines can be rejected, whilst others can simply be moved to a folder for review.

### Why isn't this message being marked as spam – it obviously is spam?

As spammers constantly change tactics and because no system is perfect, sometimes a message will get through that should have been marked as spam.

In this situation you have a few options. You could send it to the Bayesian Analysis engine for indexing which should help in detecting a message with similar content being sent to you in the future (please see the 'Teaching the Bayesian Analysis Engine & the Spam Folder' section above for more information). Alternatively, you could create a custom filter to mark the message as spam based on a range of criteria (please see Chapter 4 for more information).

### Why is this message being marked as spam – it obviously isn't spam?

There are numerous reasons a message may be marked as spam even though it isn't. By looking between the square brackets in the subject, or in the X-Spam-Reason message header you will see which engine thought the message was spam.

If it was labelled as likely spam by the Bayesian Analysis engine then you should send it to the engine so it can de-index the message to help prevent similar messages from being labelled as spam in the future (please see the 'Teaching the Bayesian Analysis Engine & the Spam Folder' section above for more information).

You could also add the sender to a whitelist rule to prevent it from being moved or deleted by any other rules you have already set up to deal with spam messages (please see the 'Moving and Deleting Spam – Whitelisting' section above as well as Chapter 4 for more information).

If it was labelled as spam by the HTML/Character Set or RegEx filtering engines and is a message that you believe other users will frequently receive, e.g. a newsletter from a large Internet company such as Amazon, please send a copy of the message to technical support. We will then look to whitelist the sender globally so that messages originating from that address are never marked as spam.

Please Note: If the message was labelled as spam by the DNS Blacklist Lookup engine then until the IP address is removed from the database it will always be marked as spam as it is known to be either deliberately or inadvertently involved in spamming.

## The Anti-Spam Module at a Glance

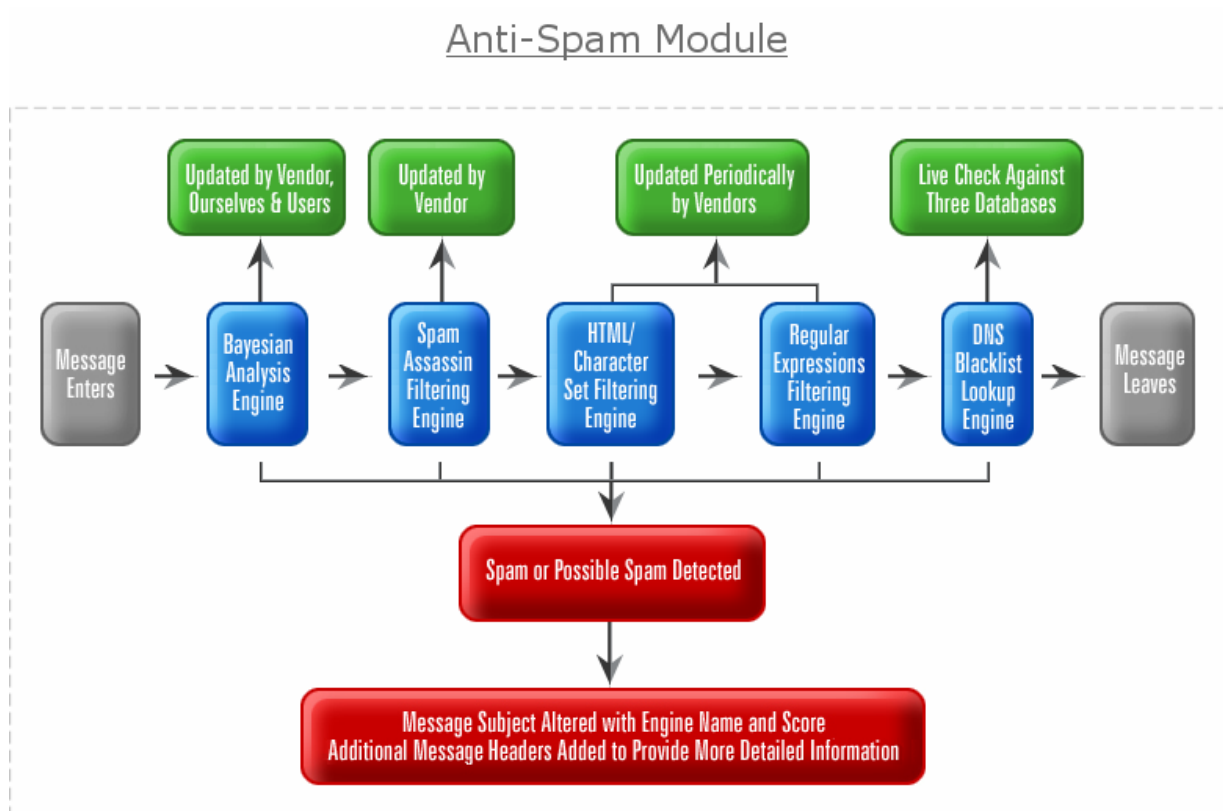


Figure 9 - The flow of a message through the anti-spam module

---

## CHAPTER 4

# Custom Filters Module

### In This Chapter

Summary .....	36
Features .....	37
How it Works .....	37
Filter Properties .....	38
Example Filters .....	40
Frequently Asked Questions .....	45
The Custom Filters Module at a Glance.....	47

---

## Summary

The custom filters module of AVAS, which is available via the WebMail interface, allows you to filter incoming messages to either a specific user or the domain name as a whole, based on a wide range of criteria and to then perform an action on any matching messages.

By making use of the custom filters module in conjunction with the anti-virus and anti-spam module provides you with even more flexibility when handling incoming e-mail.

For example, by filtering based on 'Message body' and using 'Where it contains a string' and entering 'Prescription Medications', you are able to either reject, accept, delete or mark as spam, any message with the words 'Prescription Medications' in the message body.

These filters can also be used in conjunction with the WebMail facility or your e-mail program to provide additional message processing rules.

For example, if you set up a rule to move spam messages to a folder labelled 'Spam' and create a user filter to mark messages from a particular sender as spam. When messages are received from that sender, they will first be marked as spam and then moved to the folder you created.

## Features

- Individual user and domain level filtering capability
- Filter on header, sender, recipient, IP address, attachment, body and more
- Where it contains, starts, ends or matches a string, or regular expression
- Choose between case sensitive or non-case sensitive matching
- Either reject, accept, delete, or mark a message as spam

## How it Works

Once an incoming message has passed through the anti-virus and anti-spam modules of AVAS, it is then passed through the custom filters module. If any filters are set-up, and if the message matches the pre-set criteria, the filter is activated and an action is then performed, e.g. reject all messages with the word 'Medications' in the subject.

Within the custom filters module there are two separate levels of filters that can be created; User filters and Domain filters. User filters only apply to the specific user and any aliases that user has, where as domain filters apply to all users at the domain name including any 'catch-all' account that is set up.

By combining the two different levels, you are able to specify filters that should apply for every user and filters that should only apply to a specific user.

All management of the custom filters, both user and domain level are carried out through the WebMail interface using the two links available under the 'Settings' menu.

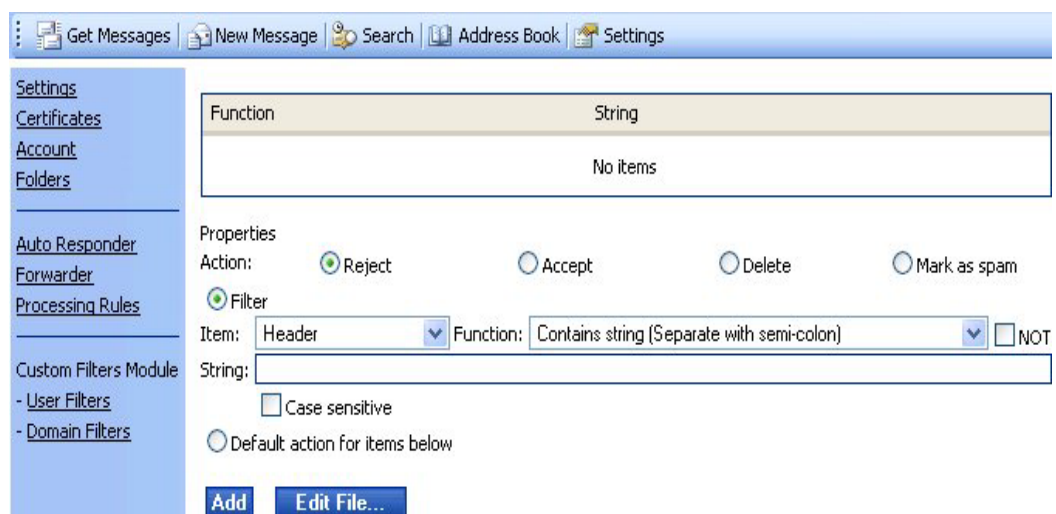


Figure 10 - The custom filters module in the WebMail interface

## Filter Properties

Each filter that is set-up, whether as a user filter or a domain level filter has a number of properties that control exactly when the filter should be activated and what it should do if activated.

Below is a list of each of the properties, what they do and how to use them.

### Action – The action that should be performed if the item matches the string

Reject	Rejects the message. The SMTP server that is sending the message receives an error containing the text 'spam filter rejection'. This error is then returned to the person who originally sent the message. You will not receive the message.
Accept	Accepts the message. You will receive the message unless you have other rules set-up that are activated.
Delete	Deletes the message. The SMTP server that is sending the message is unaware that the message has been deleted. Likewise the person who originally sent the message does not know it has been deleted. You will not receive the message.
Mark as Spam	Marks the message as spam. The subject is prefixed by [SPAM-UserMarked]. You will receive the message unless you have other rules set-up that are activated.

### Item – The part of the message to check

Header	Checks the string against a specific message header.  <b>Example:</b> Messages containing 'Medications' in the subject. <b>String Box Value:</b> Subject: Medications
Sender	Checks the string against the sender of the message.  <b>Example:</b> Messages from spam@domain.co.uk. <b>String Box Value:</b> spam@domain.co.uk
Recipient	Checks the string against the recipient of the message.  <b>Example:</b> Messages sent to me@domain.co.uk. <b>String Box Value:</b> me@domain.co.uk
IP Address	Checks the string against the sending servers IP address.  <b>Example:</b> Messages sent by 1.1.1.1 <b>String Box Value:</b> 1.1.1.1
Any Header	Checks the string against any message header.  <b>Example:</b> Messages containing 'Medications' in any header. <b>String Box Value:</b> Medications

Attachment	<p>Checks the string against any attachment name.</p> <p><b>Example:</b> Messages with a Microsoft Excel (.xls) file attachment.  <b>String Box Value:</b> .xls</p>
Body	<p>Checks the string against the message body.</p> <p><b>Example:</b> Messages containing 'Medications' in the body.  <b>String Box Value:</b> Medications</p>
rDNS (PTR)	<p>Checks the string against the reverse DNS pointer record of the sending SMTP server.</p> <p><b>Example:</b> Messages sent by mail.spam.co.uk  <b>String Box Value:</b> mail.spam.co.uk</p>
Standard	<p>Checks the string against the whole message.</p> <p><b>Example:</b> Messages containing 'Medications' in any part.  <b>String Box Value:</b> Medications</p>

#### Function – How the string should be matched against the item

**Contains String:** If the item contains any strings appearing in the 'String' text box then the filter is activated. To include multiple strings separate each one by a semi-colon, e.g. 'String one;String two'.

**RegEx:** If the item matches the regular expression appearing in the 'String' text box then the filter is activated. For examples of regular expressions, please visit <http://www.regular-expressions.info/>.

**Starts with String:** If the item starts with the string appearing in the 'String' text box then the filter is activated. If any characters appear before the string then the filter will not be activated.

**Ends with String:** If the item ends with the string appearing in the 'String' text box then the filter is activated. If any characters appear after the string then the filter will not be activated.

**Is String:** If the item exactly matches the string appearing in the 'String' text box then the filter is activated. If any characters appear before, after or in the middle of the string then the filter will not be activated.

#### Other

**NOT:** Matches the opposite of the filter specified. For example, if you create a filter to activate when 'Medications' appears in the subject and tick the 'NOT' checkbox, then it will activate when a message doesn't contain 'Medications' in the subject.

**Case Sensitive:** When ticked the string specified will only be matched if it is in the same case as the one appearing in the item. For example, if you create a filter to activate when 'MEDICATIONS' appears in the subject and tick the 'Case sensitive' checkbox, then it will not activate when a message contains 'medications', 'Medications' or any other derivative.

**Edit File...:** Allows you to manually edit the filter file and copy and paste filters between users or domains.

---

## Example Filters

In the following six sections we have listed example filters which can be used either at the user or domain level which you may find helpful to accomplish a variety of tasks.

All of these filters can be used in conjunction with the anti-virus and anti-spam modules as well as any rules you have set-up in the WebMail interface, Microsoft Outlook or Outlook Express to help you to manage your e-mail.

In all of the examples we presume you are already logged into the WebMail interface and have clicked on the 'Settings' link in the top menu.

---

## Blocking Attachment File Types

To block messages that have certain file attachments which are not currently blocked by the anti-virus module of AVAS, please follow the steps below.


In this example we are blocking all Microsoft Excel spreadsheets (.xls files).

### Blocking Attachment File Types

1. First decide whether you would like this to apply to the user you are currently logged in as, or to all accounts at the domain name. Then click on the relevant link underneath the 'Custom Filters Module' section in the left hand menu.
2. Click on the 'Add' button.
3. Select 'Reject'.
4. From the 'Item' drop down list, select 'Attachment'.
5. From the 'Function' drop down list, select 'Contains string'.
6. In the 'String' text box, enter '.xls'.
7. Click on the 'Add' button.

That's it. Every time you are sent a message with a Microsoft Excel spreadsheet attachment it will be automatically rejected and not delivered to you.



Function	String
 <b>Attachment Contains String</b>	.xls

Properties

Action:  Reject  Accept  Delete  Mark as spam

Filter

Item: Attachment  NOT  
Function: Contains string (Separate with semi-colon)  NOT  
String: .xls

Case sensitive

Default action for items below

**Add** **Modify** **Delete** **Up** **Down** **Edit File...**

Figure 11 - Blocking attachment file types

---

## Rejecting Messages from a Sender

To reject messages from a specific sender, please follow the steps below.

In this example we are rejecting messages from 'Annoying Spammer <spam@domain.co.uk>'

### Rejecting Messages from a Sender

1. First decide whether you would like this to apply to the user you are currently logged in as, or to all accounts at the domain name. Then click on the relevant link underneath the 'Custom Filters Module' section in the left hand menu.
2. Click on the 'Add' button.
3. Select 'Reject'.
4. From the 'Item' drop down list, select 'Sender'.
5. From the 'Function' drop down list, select 'Contains string'.
6. In the 'String' text box, enter 'Annoying Spammer;spam@domain.co.uk'.
7. Click on the 'Add' button.

That's it. Every time you are sent a message from 'Annoying Spammer' it will be automatically rejected and not delivered to you.

Function	String
 <b>Sender Contains String</b>	Annoying Spammer;spam@domain.co.uk

Properties

Action:  Reject  Accept  Delete  Mark as spam

Filter

Item:  Function:   NOT

String:

Case sensitive

Default action for items below

**Add** **Modify** **Delete** **Up** **Down** **Edit File...**

Figure 12 - Rejecting messages from a sender

## Marking Messages as Spam

To mark certain messages as spam which are not currently being marked as possible or likely spam by the anti-spam module of AVAS, please follow the steps below.

In this example we are marking messages containing 'Medications' in the subject as spam.

### Marking Messages as Spam

1. First decide whether you would like this to apply to the user you are currently logged in as, or to all accounts at the domain name. Then click on the relevant link underneath the 'Custom Filters Module' section in the left hand menu.
2. Click on the 'Add' button.
3. Select 'Mark as spam'.
4. From the 'Item' drop down list, select 'Header'.
5. From the 'Function' drop down list, select 'Contains string'.
6. In the 'String' text box, enter 'Subject: Medications'.
7. Click on the 'Add' button.

That's it. Every time you are sent a message with a subject that contains 'Medications' it will be automatically marked as spam.

Function	String
 <b>Header Contains String</b>	Subject: Medications

Properties

Action:  Reject  Accept  Delete  Mark as spam

Filter

Item:  Function:   NOT

String:

Case sensitive

Default action for items below

Figure 13 - Marking messages as spam

---

## Deleting Virus Notifications

If you do not want to download the virus notifications that the anti-virus module of AVAS sends you when it detects a virus in a message sent to you or by you, then whilst you can create a filter that should delete them, it won't.

Virus notifications are designated as a system level message and therefore cannot be deleted by setting up a user or domain level filter.

We can however, turn off the notifications for either a specific user or an entire domain name on your behalf. Please contact technical support for more information.

---

## Rejecting Likely Spam Messages

To reject any message identified as likely spam by the anti-spam module to avoid you having to download them, please follow the steps below.

Please Note: We do not recommend you reject any possible or likely spam messages unless you are 100% happy with the accuracy of the anti-spam module. If you find that certain engines perform better than others you can create filters that are based only on messages that fail those specific engines by altering the subject text the filter is based on.


Please see the 'How the Message is Altered' section in Chapter 3 for a complete breakdown of the different subject text used by each engine.

Also, you should never set a filter to delete spam messages, simply because if it was a genuine message the original sender would never know you didn't receive it.

## Rejecting Spam Messages

1. First decide whether you would like this to apply to the user you are currently logged in as, or to all accounts at the domain name. Then click on the relevant link underneath the 'Custom Filters Module' section in the left hand menu.
2. Click on the 'Add' button.
3. Select 'Reject'.
4. From the 'Item' drop down list, select 'Header'.
5. From the 'Function' drop down list, select 'Starts with string'.
6. In the 'String' text box, enter 'Subject: [SPAM-]'.
7. Click on the 'Add' button.

That's it. Every time a message is marked as likely spam by the anti-spam module of AVAS it will be automatically rejected and it won't be available to download.

Function	String
 <b>Header Is String</b>	Subject: [SPAM-

Properties

Action:  Reject  Accept  Delete  Mark as spam

Filter

Item:  Function:   NOT

String:

Case sensitive

Default action for items below

Figure 14 - Rejecting likely spam messages

## Creating a Whitelist Filter

If you decide to use the example above to reject likely spam messages then you may wish to create a whitelist filter to prevent messages marked as spam from a specific sender from being rejected. To do this, please follow the steps below.

In this example we are whitelisting messages from 'A Friend <friend@domain.co.uk>'.

Please Note: Domain level filters override user level filters. If you have set-up a domain level filter to reject messages marked as likely spam and want to whitelist a specific sender you must whitelist them at the domain level to ensure that even if their message is marked as spam it will still be delivered.

### Creating a Whitelist Filter

1. First decide whether you would like this to apply to the user you are currently logged in as, or to all accounts at the domain name. Then click on the relevant link underneath the 'Custom Filters Module' section in the left hand menu.
2. Click on the 'Add' button.
3. Select 'Accept'.
4. From the 'Item' drop down list, select 'Sender'.
5. From the 'Function' drop down list, select 'Contains string'.
6. In the 'String' text box, enter 'A Friend;friend@domain.co.uk'.
7. Click on the 'Add' button.
8. Using the 'Up' and 'Down' buttons move the filter you just created above any other filters that reject, delete or mark as spam any messages.

That's it. Every time you are sent a message from 'A Friend' it will not be automatically rejected even if it is marked as spam by the anti-spam module.

Function	String
 <b>Sender Contains String</b>	A Friend;friend@domain.co.uk

Properties

Action:  Reject  Accept  Delete  Mark as spam

Filter

Item:  Function:   NOT

String:

Case sensitive

Default action for items below

**Add** **Modify** **Delete** **Up** **Down** **Edit File...**

Figure 15 - Creating a whitelist filter

## Frequently Asked Questions

### When should I use a user level or a domain level filter?

If you want to create a generic filter which should be applied to all users, for example blocking messages with a JavaScript file attachment, you should create the filter as a domain level filter.

If on the other hand, for example, a particular user doesn't want to receive a newsletter from a specific company, but other users do, then the filter should be created at the user level.

### How can I reject possible spam?

Firstly, we strongly recommend that you do not do this, simply because if the message is only identified as possible spam after passing through the five anti-spam engines within the anti-spam module of AVAS, there is a high probability that it isn't spam.

However, if you do want to reject possible spam, simply follow the instructions contained within the 'Rejecting Spam Messages' example above and at step 6 replace '[SPAM-' with '[SPAM?-

### How can I move user level filters to the domain level (or vice-versa)?

If you would like to move existing user level filters to the domain level so that they apply to all users, simply click on the 'Edit File...' button at the user level.

Then highlight and cut all of the text to the clipboard, click on the 'Edit File...' button at the domain level and paste the text in. When you close the window, the filters will appear automatically.

To move existing filters from the domain level to the user level, simply reverse the steps above.

### Can I restrict access to the domain level filters?

At the moment this isn't possible, however it is likely to be possible in the future.

## The Custom Filters Module at a Glance

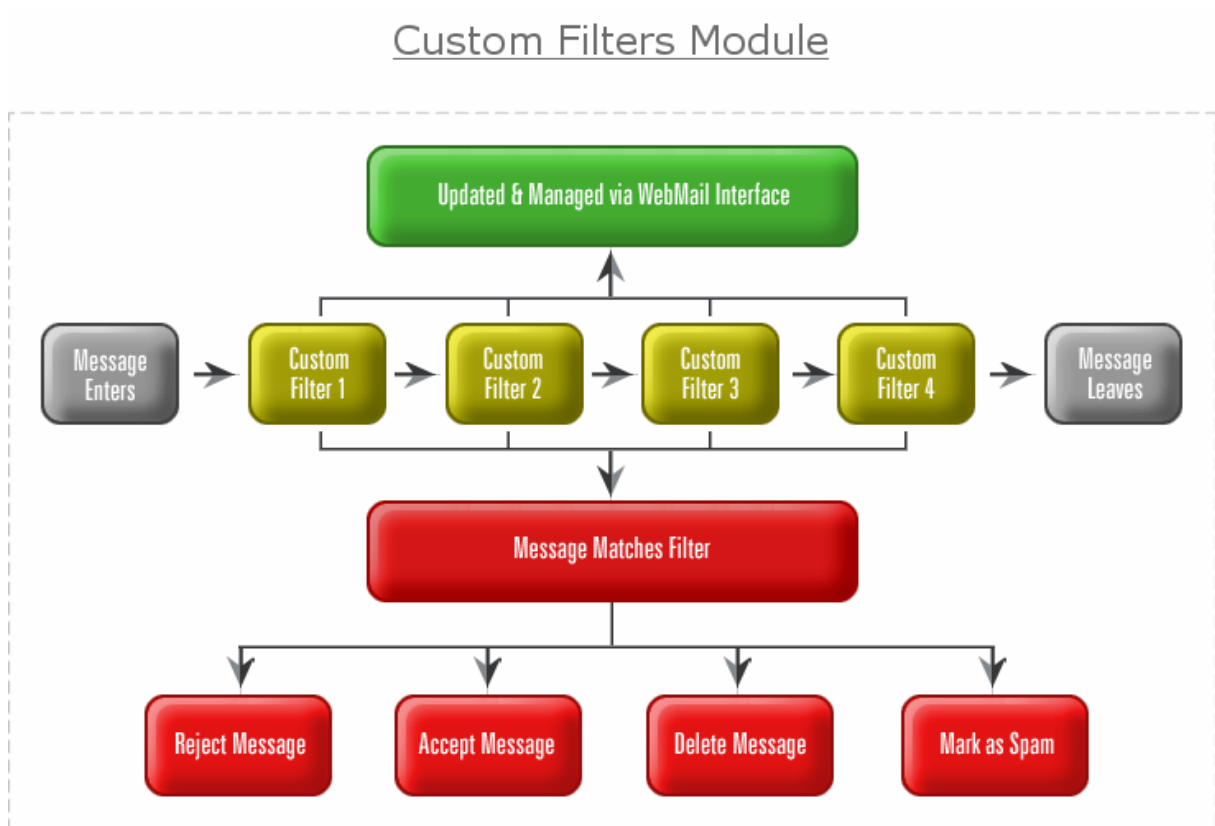


Figure 16 - The flow of a message through the custom filters module

---

## CHAPTER 5

# Putting it all Together

### In This Chapter

Introduction.....	48
A 'Real World' Example.....	48

---

## Introduction

By now you will have read some, or all of this manual (if you haven't we strongly recommend you do) and you will hopefully have an understanding of how AVAS works and how it can help with both protecting and making your e-mail easier to manage.

The purpose of this final chapter is to bring together all of the examples of rules and filters in a 'real world' example that illustrates the flexibility of AVAS and which you can customise and use on a daily basis.

Whilst the following example is fairly specific, you should be able to easily adapt it to your specific configuration, both in the sense of e-mail software you use and the type of e-mail that you receive.

---

## A 'Real World' Example

For the purpose of this section we are going to assume you are using Microsoft Outlook Express to collect your e-mail via POP3 and want to perform the following actions:

1. Virus notifications that originate from the anti-virus module of AVAS and are being sent to any user at the domain name should be deleted and therefore not be available to download. (Contact technical support)
2. Messages containing the word 'Medications' in the subject line that are being sent to a specific user should be rejected and therefore not be available to download. (User level filter)
3. Messages from 'Annoying Spammer <spam@domain.co.uk>' should be rejected if they are being sent to any user at the domain name and therefore not be available to download. (Domain level filter)
4. Messages from 'A Friend <friend@domain.co.uk>' should be whitelisted if they are being sent to a specific user and therefore downloaded and not moved. (Domain level filter + Outlook Express rule)



5. Messages determined as possible spam by either the Bayesian Analysis or SpamAssassin Filtering engines should be downloaded and moved to a folder called 'Spam-Possible'. (Domain level filter + Outlook Express rule)
6. Messages determined as likely spam by either the Bayesian Analysis, SpamAssassin Filtering, or DNS Blacklist Lookup engines should be rejected and therefore not be available to download. (Domain level filter)
7. Messages determined as likely spam by the HTML/Character Set or RegEx Filtering engines should be downloaded and moved to a folder called 'Spam-Review'. (Domain level filter + Outlook Express rule)

Please Note: Domain level filters override user level filters. If you have set-up a domain level filter to reject messages marked as likely spam and want to whitelist a specific sender you must whitelist them at the domain level to ensure that even if their message is marked as spam it will still be delivered.

We are assuming you do not currently have any filters set-up in the WebMail interface or any rules set-up in Outlook Express and that you have both the WebMail interface and Outlook Express already open.

### 1. Deleting Virus Notifications (Contact Technical Support)

Whilst you are able to create an Outlook Express rule to delete virus notifications originating from the anti-virus module of AVAS, you would still have to download them.

To avoid having to download the notifications, please contact technical support who will turn them off for your entire domain name.

### 2. Reject Messages with a Subject Containing 'Medications' (User Level Filter)

1. In the WebMail interface, click on the 'User Filters' link on the left hand side and then click on the 'Add' button.
2. Select 'Reject'.
3. From the 'Item' drop down list, select 'Header'.
4. From the 'Function' drop down list, select 'Contains string'.
5. In the 'String' text box, enter 'Subject: Medications'.
6. Click on the 'Add' button.

### 3. Reject Messages from 'Annoying Spammer' (Domain Level Filter)

1. In the WebMail interface, click on the 'Domain Filters' link on the left hand side and then click on the 'Add' button.

2. Select 'Reject'.
3. From the 'Item' drop down list, select 'Sender'.
4. From the 'Function' drop down list, select 'Contains string'.
5. In the 'String' text box, enter 'Annoying Spammer;spam@domain.co.uk'.
6. Click on the 'Add' button.

#### 4. Whitelisting Messages from 'A Friend' (Domain Level Filter + OE Rule)

1. In the WebMail interface, click on the 'Domain Filters' link on the left hand side and then click on the 'Add' button.
2. Select 'Accept'.
3. From the 'Item' drop down list, select 'Sender'.
4. From the 'Function' drop down list, select 'Contains string'.
5. In the 'String' text box, enter 'A Friend;friend@domain.co.uk'.
6. Click on the 'Add' button.
7. In Outlook Express, from the 'Tools' menu select 'Message Rules' and then select 'Mail'.
8. In section 1, tick 'Where the From line contains people' and in section 3, click on the 'contains people' link.
9. In the window that opens enter 'friend@domain.co.uk' in the text box and click on the 'Add' button and then click on the 'OK' button.
10. In section 2, scroll down and tick 'Stop processing more rules'.
11. In section 4, enter 'Whitelist messages from someone@domain.co.uk' as the name for the rule and click on the 'OK' button.

#### 5. Move Messages Marked as Possible Spam (Domain Level Filter + OE Rule)

1. In the WebMail interface, click on the 'Domain Filters' link on the left hand side and then click on the 'Add' button.
2. Select 'Accept'.
3. From the 'Item' drop down list, select 'Header'.
4. From the 'Function' drop down list, select 'Starts with string'.
5. In the 'String' text box, enter 'Subject: [SPAM?]-'.
6. Click on the 'Add' button.

7. In Outlook Express, from the 'Tools' menu select 'Message Rules' and then select 'Mail'.
8. In section 1, tick 'Where the Subject line contains specified words' and in section 3, click on the 'contains specific words' link.
9. In the window that opens enter '[SPAM?-Bayesian' in the text box and click on the 'Add' button.
10. Enter '[SPAM?-SpamAssassin' in the text box and click on the 'Add' button and then click on the 'OK' button.
11. In section 2, tick 'Move it to the specified folder' and in section 3, click on the 'specified' link and then click on the 'New' button.
12. Enter 'Spam-Possible' as the name for the new folder and click on the 'OK' button.
13. Highlight the folder you just created and click on the 'OK' button.
14. In section 2, scroll down and tick 'Stop processing more rules'.
15. In section 4, enter 'Move possible spam messages to Spam-Possible (Bayesian/SpamAssassin)' as the name for the rule and click on the 'OK' button.

#### 6. Reject Likely Spam Messages – Bayesian/SA/DNSBL (Domain Level Filter)

1. In the WebMail interface, click on the 'Domain Filters' link on the left hand side and then click on the 'Add' button.
2. Select 'Reject'.
3. From the 'Item' drop down list, select 'Header'.
4. From the 'Function' drop down list, select 'Starts with string'.
5. In the 'String' text box, enter 'Subject: [SPAM-'.
6. Click on the 'Add' button.

#### 7. Move Likely Spam Messages (HTML/CharSet/RegEx) (DL Filter + OE Rule)

1. In the WebMail interface, click on the 'Domain Filters' link on the left hand side and then click on the 'Add' button.
2. Select 'Accept'.
3. From the 'Item' drop down list, select 'Header'.
4. From the 'Function' drop down list, select 'Starts with string'.
5. In the 'String' text box, enter 'Subject: [SPAM-HTML/CharSet]'.
6. Click on the 'Add' button.

7. Click on the 'Up' button once to move the new filter above the filter which rejects a message with a subject starting with '[SPAM-'.
8. In the 'String' text box, enter 'Subject: [SPAM-Regex]'.
9. Click on the 'Add' button.
10. Click on the 'Up' button once to move the new filter above the filter which rejects a message with a subject starting with '[SPAM-'.
11. In Outlook Express, from the 'Tools' menu select 'Message Rules' and then select 'Mail'.
12. In section 1, tick 'Where the Subject line contains specified words' and in section 3, click on the 'contains specific words' link.
13. In the window that opens enter '[SPAM-HTML/CharSet]' in the text box and click on the 'Add' button.
14. Enter '[SPAM-Regex]' in the text box and click on the 'Add' button and then click on the 'OK' button.
15. In section 2, tick 'Move it to the specified folder' and in section 3, click on the 'specified' link and then click on the 'New' button.
16. Enter 'Spam-Review' as the name for the new folder and click on the 'OK' button.
17. Highlight the folder you just created and click on the 'OK' button.
18. In section 2, scroll down and tick 'Stop processing more rules'.
19. In section 4, enter 'Move likely spam messages to Spam-Review (HTML/Character Set/Regex)' as the name for the rule and click on the 'OK' button twice.

That's it. The screenshots below show what you should now have set-up.

Function	String
 Sender Contains String	Annoying Spammer;spam@domain.co.uk
 Sender Contains String	A Friend;friend@domain.co.uk
 Header Starts with String	Subject: [SPAM?-
 Header Starts with String	Subject: [SPAM-HTML/CharSet]
 Header Starts with String	Subject: [SPAM-Regex]
 <b>Header Starts with String</b>	Subject: [SPAM-

Properties

Action:  Reject  Accept  Delete  Mark as spam

Filter


Item:  Function:   NOT

String:

Case sensitive

Default action for items below

Figure 17 - The completed domain level filters in the WebMail interface

Function	String
 <b>Header Contains String</b>	Subject: Medications

Properties

Action:  Reject  Accept  Delete  Mark as spam

Filter

Item:  Function:   NOT

String:

Case sensitive

Default action for items below

**Add** **Modify** **Delete** **Up** **Down** **Edit File...**

Figure 18 - The completed user level filters in the WebMail interface

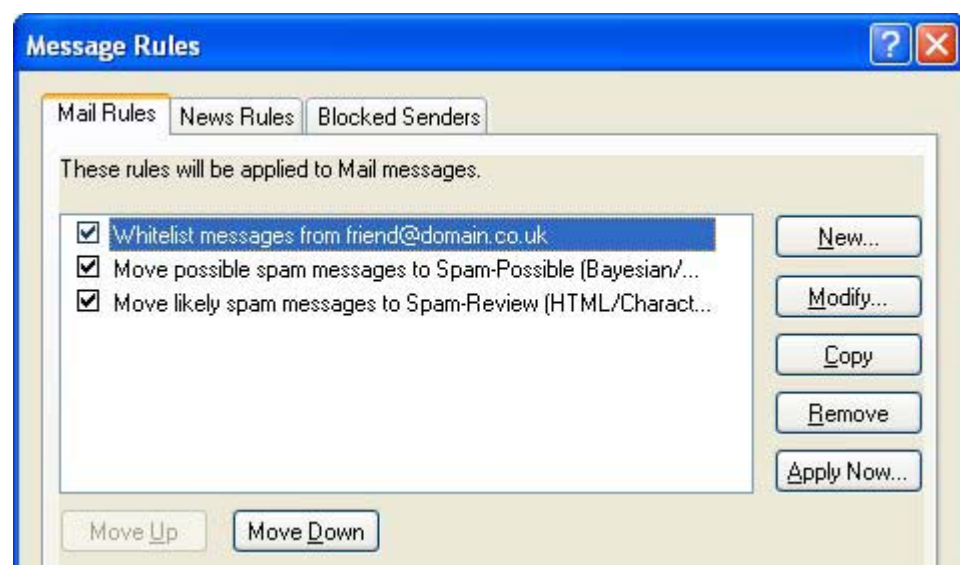


Figure 19 - The completed rules in Outlook Express