



Contents

1.	AVS Principles	3
1.1	What is SPAM?	3
1.2	Why does SPAM get sent?	3
1.3	How to deduce the SPAM?	3
1.3.1	Content Filtering.	3
1.3.2	DNS Based Blacklisting	4
1.3.3	Sender Authentication.	4
1.3.4	Enforced Standards.	4
1.3.5	Regional Blocking (GeoIP).	4
1.3.6	Vigilant Dialogue.	4
1.4	How to reduce the SPAM?	4
1.4.1	Diligent use of your email addresses.	4
1.4.2	NEVER reply to SPAM email.	4
1.4.3	Employ the Netnorth AVS.	4
1.5	What is a SPAM SCORE?	5
1.5.1	Typical score thresholds:	5
1.5.2	How is SPAM Treated?	5
1.6	What is a Scanning Reference?	6
1.7	Anatomy of an email?	7
1.7.1	Email process.	7
1.7.2	Email Content.	8
1.8	What AVS measures are taken?	8
1.8.1	Greeting Delay	8
1.8.2	Greylist	8
1.8.3	Allowed Userlist	8
1.8.4	Content scans	9
1.8.5	Blacklist / Whitelist	9

2.	Customer Portal	10
2.1	How do I access the Customer Portal?.....	10
2.2	How do I leave the Customer Portal?	10
3.	AVS Settings Management.....	11
3.1	How do I manage AVS settings?.....	11
3.2	How do I use Tagging Text?.....	11
3.3	How do I use the Spam Score?.....	11
3.4	How do I use the Discard Score?	12
3.5	How do I use Email Notifications?	12
4.	AVS Whitelist / Blacklist Management.	13
4.1	How do I manage Sender Whitelists and Blacklists?	13
4.1.1	How do I Blacklist a sender's address.	13
4.1.2	How do I Blacklist all senders in a given domain.	14
4.1.3	How do I Whitelist a sender's address.	14
4.1.4	How do I Whitelist all senders in a given domain.....	14
4.1.5	How do I Remove a list entry.	15
4.1.6	Bare domain restrictions.	15
4.2	How do I identify the actual sender of a spam email?.....	15
4.3	Which address should I list?.....	16
5.	AVS Allowed User List management	18
5.1	How do I manage a domain Allowed User list?	18
5.1.1	How do I add an Allowed User?.....	18
5.1.2	How do I Remove a list entry.	19
6.	AVS Statistics	20
6.1	How do I know how effective AVS is?	20
6.2	How do I Use AVS Statistics Graphs?	20
6.3	How do I Use AVS Reports?	20
6.4	How Do I Extract AVS Reports?	23
6.4.1	6.4.1. Summary Text Report.	23
6.4.2	6.4.2. Summary CSV Report.	23
6.5	How do I use Email Notifications?	24
7.	AVS Batch Processing	25
7.1	AVS Batch Remain.....	25
7.2	AVS Batch Whitelist	26

1. AVS Principles

The Internet has become a very efficient way of communicating large amounts of information, between many parties, in a short period of time, at little cost to the users. Unsurprisingly, it has become a medium of choice for speculative advertising and abuse.

The Netnorth anti-virus and anti-spam services (AVS) involve various mechanisms that analyse your inbound email, and attempt to reduce the amount of undesirable email that you finally receive. This document will explain some of the principles involved, and describe how you can configure some of the behaviour to suit your needs.

1.1 What is SPAM?

The relevance and importance of any given email will vary depending on who you ask. Usually if an email addresses a single individual it is likely to carry useful information. However if that same message is simply 'broadcast' speculatively to many people, then with one or two exceptions most recipients are likely to be uninterested, and it can be classified as 'spam'. Aspects of spam email often include: 'being sent in bulk'; 'being unsolicited'; and definitely 'being inappropriately addressed' in the opinion of the recipient.

The term 'spam' originated by way of a Monty Python sketch in which Spam luncheon meat is depicted as 'ubiquitous and unavoidable'.

In all regards, one person's spam will be another person's ham, and since care must be taken not to withhold desired emails (HAM), inevitably some spam emails will end up being delivered.

1.2 Why does SPAM get sent?

The authors of spam have various motives, but broadly they will fall into one of the following types:

Spam-vertising. In which the sender is simply broadcasting a speculative commercial email, often with a URL link back to a vendor's website. Pharmaceutical product makes up the majority of this type of spam.

Investment-Scamming. In which people are cajoled into funding personal or business ventures. Both Nigeria and Russia have been infamously associated with spam of this type.

Phishing. Messages which attempt to collect personal details, often via a URL link to a faked website. These are commonly forged to appear as though they are from your bank or similar important organisation. Some messages may even incorporate known personal details of the recipient to gain provenance, this is known as Spear-phishing.

Malware. Apparently innocuous email may contain attachments which are themselves malicious or detrimental. Some are simply viruses attempting to propagate. Some will attempt to acquire information over a period of time and then silently report it back to the sender. Always be very careful about handling email attachments.

Backscatter. This isn't directed to the recipient as such, but is an unintended result of a spam message failing to be delivered to a non-existent address. Often the authors of spam (or self-propagating viruses) will forge the sending address of the spam before sending it speculatively to a multitude of invented addresses. Any of the recipient addresses that don't exist are likely to refuse delivery with a courtesy message to the apparent sender.

1.3 How to deduce the SPAM?

There are a multitude of approaches that could be adopted to identify undesirable emails:

1.3.1 Content Filtering.

Early mechanisms would simply block emails with particular words or links in their subject line or message body.

1.3.2 DNS Based Blacklisting

(DNSBL). A sending organisation's domain or IP address can be discarded based on a communal blacklist composed by other reported public experiences.

1.3.3 Sender Authentication.

A sending organisation can engender trust by publishing their sending particulars via a 3rd party. eg DKIM / SPF / DMARC

1.3.4 Enforced Standards.

Early spam generation didn't comply fully with SMTP standards, messages can be rejected depending on how compliant they are. HELO/EHLO checking; Validated Pipelining; Non-listed MX;

1.3.5 Regional Blocking (GeoIP).

Some organisations can reasonably expect never to receive email from certain countries. This technique rejects emails based on country of origin, identified by the sender's IP rather than any cosmetic aspect of the email content.

1.3.6 Vigilant Dialogue.

A receiving mail server can be 'cautious' during the conversation with the sending server, often involving 'Greylisting' or a 'Greeting Delay', which many automated spam senders won't bother to handle.

Any of the above techniques will be effective against its ideal form of spam, then again they all have weaknesses and will be ineffective if used in isolation.

The Netnorth AVS service combines the above techniques with some proprietary methods, paying due consideration to the results of each, and deriving an overall 'Spam Score' indicating the 'reputation' of each email processed.

1.4 How to reduce the SPAM?

1.4.1 Diligent use of your email addresses.

This will go a long way to keeping you free from attempted spam emails. By all means pass on your personal email address to individuals as contact details ('yourname@yourdomain.com'), but if possible don't publish it on websites or use it in form fields. If you own the domain, publish 'role accounts' where possible (eg 'temp@yourdomain.com'). This allows the address to be more easily abandoned and replaced with an alternative 'role account' in future should it attract too much spam.

1.4.2 NEVER reply to SPAM email.

Similarly never click on the 'Please remove my address' type links. Any response could either simply signal to the spammer that the address in question (yours) is a valid address, and could easily attract further spam, or in cases where the spammer has forged the sending address, your reply would simply become 'backscatter'.

1.4.3 Employ the Netnorth AVS.

In its native form our service will significantly reduce the amount of spam that you would otherwise receive. In our role as Business ISP, over 60% of the business email that passes through our AVS server heads is classified as 'spam' and handled accordingly.

Netnorth AVS combines the micro-scores of over 30,000 rules to establish an overall reputation 'Spam Score'. Each result can be +ve or -ve, reducing or promoting an individual email reputation. This fine tuning of the test results is far more effective in constructing an overall classification of each email.

Our service offers you further control via a user portal, allowing you to compile your own additional 'sender WHITELIST', and 'sender BLACKLIST', which in turn influence the reputation score. You can also specify how different 'reputation' score thresholds should be handled for your domain: deliver; tag and deliver; discard.

The portal also offers you the facility to compile a recipient 'ALLOWED USERLIST', which will catch and discard any emails that are sent to a speculative non-existent address in your domain.

1.5 What is a SPAM SCORE?

When an email message is processed by AVS it is attributed a 'reputation' by accumulating scores from many individual tests. The bigger the score, the more 'spammy' the message content is considered to be. Individual tests typically score only a fraction of a point, which can be either a positive or a negative number that respectively worsens or improves the overall reputation 'Spam Score'.

1.5.1 Typical score thresholds:

HAM: A reputation score lower than the 'spam threshold' (default 5.1) will be treated as perfectly normal email that will be delivered unchanged.

SPAM: If the reputation score is between the 'spam threshold' and the 'discard threshold' (default 30.0) then it will be considered to be 'managed spam' and will be treated as required by the receiving domain, eg SPAMTRAP / BESPOKE MAILBOX / TAG & FORWARD, see below.

DISCARD: If the score is over the 'discard threshold' then the message is considered to be so bad that it will be discarded altogether, unless you've optionally disabled discard.

Note: These default thresholds can be tweaked in the AVS Portal for any given domain.

1.5.2 How is SPAM Treated?

Messages accruing a score in the 'managed spam' range can be treated in a variety of ways, each with its own benefits and drawbacks.

	Advantages	Drawbacks
SPAM TRAP	<ul style="list-style-type: none">. End users never see spam.. Casual management.. Auto-deletion.	<ul style="list-style-type: none">. Limited management.. Messages only recoverable during retention period.. Accessing users see ALL spam within the domain.
BESPOKE MAILBOX	<ul style="list-style-type: none">. End users never see spam.. No retention period imposed.	<ul style="list-style-type: none">. Requires proactive management.. Accessing users see ALL spam within the domain.
TAG & FORWARD	<ul style="list-style-type: none">. Individuals manage their own messages.. Very versatile.	<ul style="list-style-type: none">. Requires rudimentary knowledge of inbox rules.

SPAM TRAP: Spam messages are intercepted and stored for a retention period in a single webmail mailbox for all addresses at the recipient domain. This webmail can be perused proactively when an expected email isn't received, and trapped emails can be forwarded on to the intended recipient if needed. The main advantage is that recipients are never presented directly with SPAM, and can effectively ignore spam until they choose to investigate it. The spam trap doesn't need to be routinely monitored since after the retention period messages are auto-deleted. The disadvantage is that users given access to the spam trap have access to all SPAM messages for that domain, some of which may contain sensitive information.

BESPOKE MAILBOX: A single mailbox or forwarding address can be designated to receive all spam messages for the recipient domain. Again the main advantage is that recipients are never presented directly with SPAM. Messages delivered into the bespoke mailbox would need to be collected by an email client and managed remotely. There isn't a retention / auto-delete period imposed on the messages, but consequently the mailbox would need to be routinely collected to avoid it reaching storage limits. Again a disadvantage is that users given access to the mailbox have access to all SPAM messages for that domain, some of which may contain sensitive information.

TAG & FORWARD: This is the preferred method, in which spam messages are tagged as such before being delivered to the intended recipient. A tagged message typically prepends the

Subject line with an identifiable phrase that can be used by inbox rules in email clients to marshal 'Suspect Spam' into relevant local mail folders. The main advantage here is that emails are only ever visible to the intended recipient, aren't subject to an auto-delete retention period, and can be searched for and managed more intimately by a user's own email client. The disadvantage is mainly one of perception by the end recipient, they still receive the spam messages and need a rudimentary knowledge to implement inbox rules within their email client.

1.6 What is a Scanning Reference?

Every email passing through our AVS is assigned an AVS Scanning Reference, which can be used when querying our support services, or more usefully for you to identify relevant information in your administration of the AVS portal.

The reference looks like this... **123-avs1-1234567890** ...and is appended to the bottom of a received email body, in the following format...

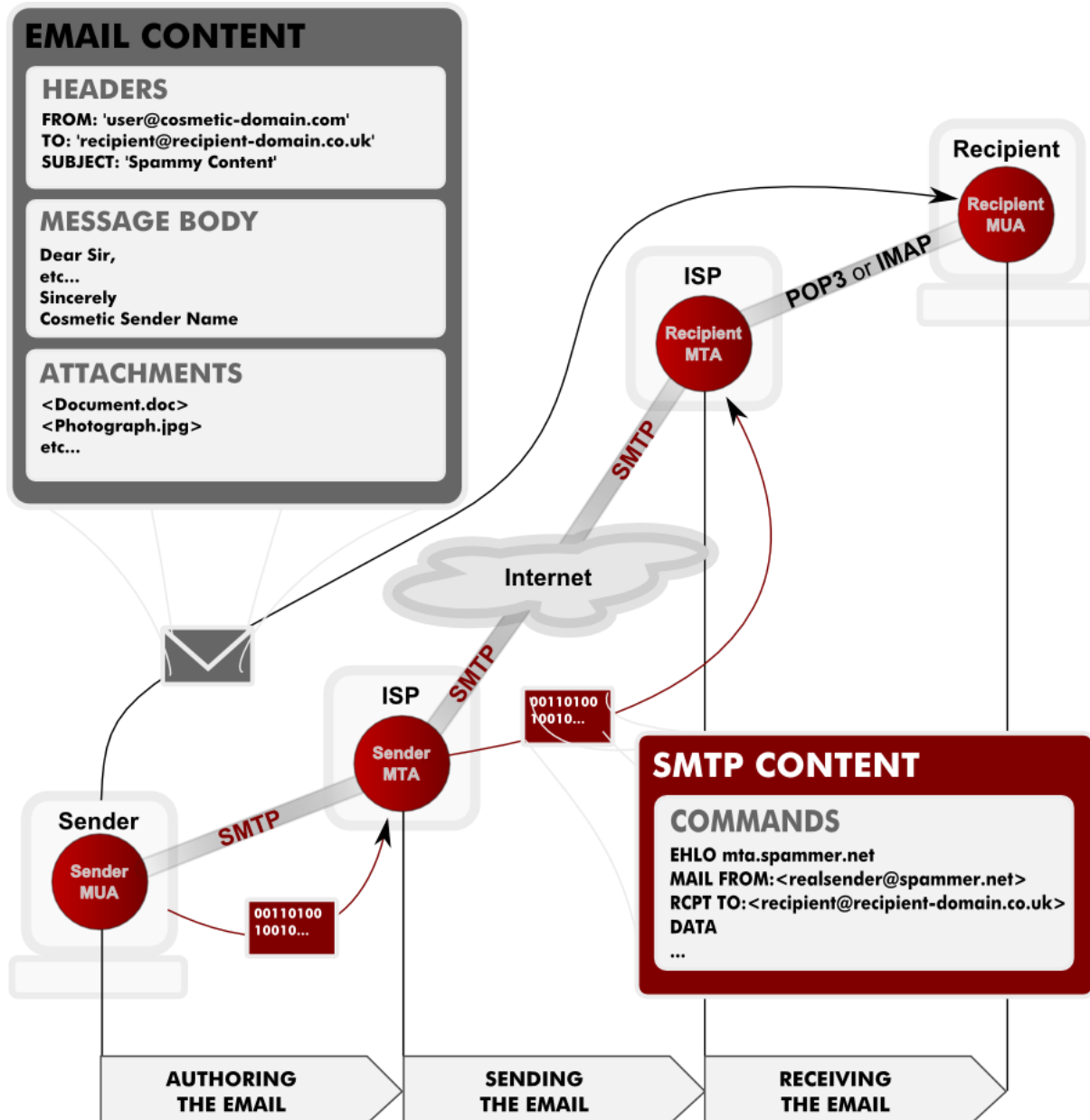
```
++++ Message Scanning REF:123-avs1-1234567890 +++++
```

...or in the email headers, in the following format...

```
X-Spam-Status: No, score= -733.941 required=5.1 tests= ...  
X-Virus-Status: ** CLEAN ** Scanned by Netnorth  
X-AVS-ScanningRef: 123-avs1-1234567890
```

Obviously the actual digits in each email message will vary.

1.7 Anatomy of an email?



1.7.1 Email process.

Authoring the Email.

The message is authored in the sender's email client, a Mail User Agent (MUA), which composes the Message Body, and any associated Headers and Attachments into a single Email object. These Headers include a cosmetic 'from address', which can be easily forged by a Spammer to misrepresent who sent the message.

The Email is sent, either via a Local Area Network (LAN) or the Internet, to the sender's Mail Transfer Agent (MTA), often at the sender's Service Provider (ISP). This conversation uses the Simple Mail Transfer Protocol (SMTP), which in turn defines the actual sender's and recipient's 'envelope' addresses in **MAIL FROM** and **RCPT TO** commands.

Sending the Email.

The intended recipient mail server IP is determined from the MX record of the recipient's domain via Domain Name Services (DNS).

The sender's MTA communicates with the recipient's MTA, transacting the Email via SMTP using the **MAIL FROM** and **RCPT TO** 'envelope' addresses declared outside of the Email. These are the addresses which can be most usefully Whitelisted or Blacklisted by a recipient.

Receiving the Email

The Recipient's mail server might apply any applicable AVS measures to the inbound Email, before conditionally accepting the Email for delivery, and holding it in a pertinent mailbox for collection. Alternatively the AVS measures may determine that the Email should be routed to a spamtrap, or discarded completely.

Email delivered to the recipient mailbox is checked for and collected periodically by the recipient's email client (MUA), typically via POP3 or IMAP.

The Email content is unravelled by the recipient's mail client, which proceeds to display Headers, Message Body and Attachments that were originally authored, this includes the cosmetic 'from address' which may be forged.

1.7.2 Email Content

Headers.

Message headers contain various pieces of information, some originating from the sender, others added by MTAs en route, or by AVS systems and receiving servers.

Headers can usually be viewed from within your MUA, and will often give clues to times and routes taken, along with spam reputation scores, etc. This is where the apparent sender address is derived and displayed in your email client.

Message Body.

The message body essentially contains the narrative authored by the sender. This may be repeated in different guises, (Plaintext / RTF / HTML), the most suitable of which will be interpreted and displayed by the receiving MUA.

Attachments.

Each attachment is usually a discrete file, providing a simple way to share documents and images. Many MTAs will impose size and content-type limits on email, and attachments will often be the cause of rejected email.

1.8 What AVS measures are taken?

1.8.1 Greeting Delay

When the receiving server is challenged by a sending server, the receiving server 'pauses' briefly during the initial dialogue. A genuine sending server will wait patiently for the expected response, whereas a programmatic spambot will often misidentify the delay as a failure and quickly move on to its next intended target. This sounds simple, but is surprisingly effective.

1.8.2 Greylist

The receiving server will deliberately dismiss the mail service temporarily for an unknown or suspect sending server, typically for a matter of minutes. A competent sending server is expected to 'retry' sending any messages in these circumstances, whereas a spambot is unlikely to queue outgoing email, and will simply move on to its next intended target. When a genuine sending server proves itself to be capable of retrying delivery, it is recorded in a 'greylist' along with the associated 'envelope' addresses as a trusted server for a matter of months, during which no further delays would be applied. This is an extremely powerful counter-measure to spam sources, and the one off minimal delay imposed on a genuine sender is well worth the benefits gained.

Note: Sending servers with legitimate SPF records will be accepted immediately by the 'greylist'.

1.8.3 Allowed Userlist

This is a list of allowed recipients at a given domain. It allows a receiving server to immediately reject speculative emails targeted to a domain using presupposed usernames. This list can be managed via the Customer Portal.

1.8.4 Content scans

After successfully negotiating a connection with the receiving server, the email content (headers / message body / attachments) are investigated for characteristics matching: virus; malware; phishing; GeoIP; DNSBL etc. This is the conventional Anti-Virus / Anti-Spam methodology that the world has come to expect. The many thousands of rules / checks / measures taken during this process are being constantly administered and improved to keep up with the ever changing tapestry of inappropriate content that should be avoided. The resulting reputation of an email is represented as a 'spam score', which can be actioned according to score thresholds that are managed via the Customer Portal.

1.8.5 Blacklist / Whitelist

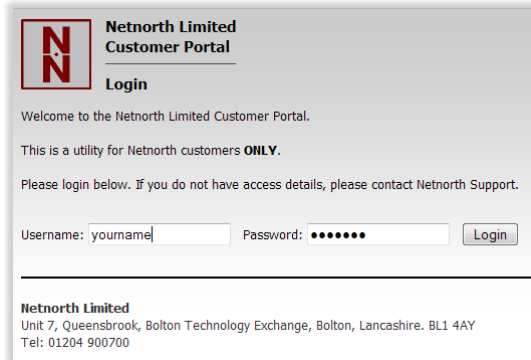
These are lists of denied / allowed senders, defined for a given recipient domain. These lists can be managed via the Customer Portal.

2. Customer Portal

The Customer Portal allows you an element of control over the AVS behaviour and thresholds used when processing SPAM / HAM email.

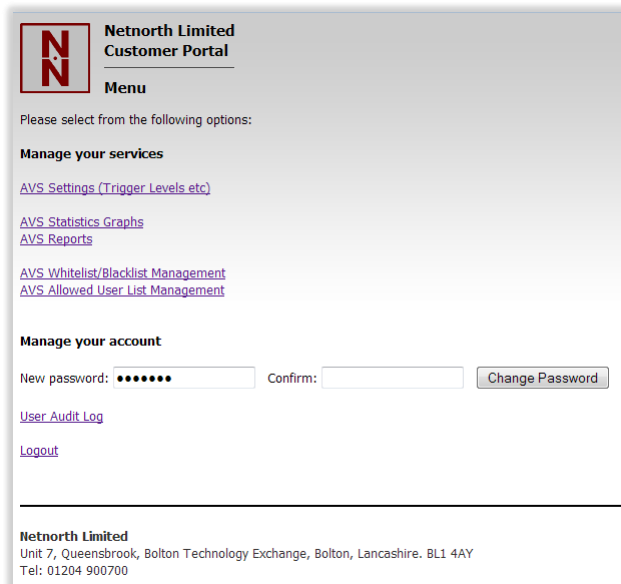
2.1 How do I access the Customer Portal?

The portal is accessed via your web browser at <https://portal.netnorth.co.uk> , and entering your Customer Portal username and password...



The screenshot shows the login page of the Netnorth Limited Customer Portal. It features the Netnorth logo (a stylized 'N' in a square) and the text "Netnorth Limited Customer Portal". Below the logo is a "Login" heading. The page includes a welcome message: "Welcome to the Netnorth Limited Customer Portal. This is a utility for Netnorth customers ONLY. Please login below. If you do not have access details, please contact Netnorth Support." There are two input fields: "Username: yourname|" and "Password: ●●●●●●", followed by a "Login" button. At the bottom, there is contact information for Netnorth Limited: "Unit 7, Queensbrook, Bolton Technology Exchange, Bolton, Lancashire. BL1 4AY Tel: 01204 900700".

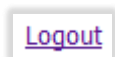
...which will display the Customer Portal menu. From this point you can either change your password, manage the various AVS services, or logout...



The screenshot shows the menu page of the Netnorth Limited Customer Portal. It features the Netnorth logo and the text "Netnorth Limited Customer Portal". Below the logo is a "Menu" heading. The page includes a message: "Please select from the following options:". There are two main sections: "Manage your services" and "Manage your account". Under "Manage your services", there are links for "AVS Settings (Trigger Levels etc)", "AVS Statistics Graphs", "AVS Reports", "AVS Whitelist/Blacklist Management", and "AVS Allowed User List Management". Under "Manage your account", there is a "New password: ●●●●●●" field, a "Confirm:" field, and a "Change Password" button. There are also links for "User Audit Log" and "Logout". At the bottom, there is contact information for Netnorth Limited: "Unit 7, Queensbrook, Bolton Technology Exchange, Bolton, Lancashire. BL1 4AY Tel: 01204 900700".

2.2 How do I leave the Customer Portal?

After logging-in to the Customer Portal as described above, and effecting any required management of your domain as described below, click on the link ...



This will return you to the Customer Portal login screen, and safely disconnect your session. You should never leave your Customer Portal session unattended where other people may have access to your terminal.

3. AVS Settings Management.

The Customer Portal allows you to tweak the thresholds that govern how spam emails are handled for your domain.

3.1 How do I manage AVS settings?

Login to the Customer Portal, as described above, and click on the link ...

[AVS Settings \(Trigger Levels etc\)](#)

Select your domain from the drop-down, and click 'Manage', which will display a table of tag and thresholds that are currently associated with your receiving domain.

Netnorth Limited
Customer Portal

AVS Settings Management

[Main Menu](#)

Please select the email domain you wish to manage from the list below:

yourdomain.com

Management for the domain: yourdomain.com

Tagging Text:	*** SPAM - Tagged by Netnorth ***		
	Threshold	Allowed Range	Recommended
Spam Score:	5.1	5.1 and above	5.1
Discard Score:	0.0 Disabled	0.0 or 20.0 - 50.0	30.0
Last Updated:	never		<input type="button" value="Update Settings"/>

Any of these values can be edited directly, and committed by clicking 'Update Settings'.

3.2 How do I use Tagging Text?

The 'Tagging Text' is used as the prepended 'spam tag' in an email's subject line when the email reputation score is greater than the 'spam score' threshold. It can be edited to suit your needs. Typically you could create an inbox rule in your email client, which after matching the start of the received subject line with your known 'tagging text' would handle suspected spam in whichever manner you choose.

You could configure your client to automatically move tagged messages into a 'suspected spam' folder as soon as they were delivered, this would stop your inbox from being cluttered, but still allow you to casually check any accumulated spam at your leisure.

If you are more adventurous, and familiar with the features of your email software, you could further attempt to check the email headers for the actual spam score, and choose to automatically delete the very spammy emails from your 'suspected spam' folder altogether.

At the very least, you can leave everything in your Inbox and just use the subject line to flag the fact that our AVS considered the message to be spam.

3.3 How do I use the Spam Score?

The 'Spam Score' is a lower threshold used to identify HAM from SPAM.

Allowable values are in the range (**5.1** to **20.0**), the recommended value is **5.1**

Any email with a reputation score lower than the 'Spam Score' will be delivered naturally as HAM without modification by the 'Tagging Text', though of course you can still check the email headers to see what reputation score was actually achieved.

Any email with a reputation score greater than (or equal to) the 'Spam Score' will be tagged with the 'Tagging Text' prepended to the subject line, and processed as spam for your domain. Usually delivered to the intended recipient.

3.4 How do I use the Discard Score?

The 'Discard Score' determines if and when a spam email will simply be discarded rather than delivered to the intended recipient as suspect spam.

Allowable values are in the range (**20.0 to 50.0**, or **0.0**), the recommended value is **30.0**

Any email with a reputation score greater than the 'Discard Score' will be silently deleted, UNLESS the discard score is set to 0.0, in which case emails will never be discarded, and ALL spam emails will be tagged and delivered, no matter what the reputation score is.

Note: Even when an email's reputation score is higher than the Discard Score, emails may still be delivered by any Whitelisted sender details that you have configured.

Note: Even when discard is disabled with a Discard Score threshold of **0.0**, emails may still be blocked by any Blacklisted sender details that you have configured.

3.5 How do I use Email Notifications?

AVS notifications tabulate stats of the different message categories processed for a domain, and when relevant include a link to 'Review and Remail' messages via the Portal Reporter...

Daily stats for

	Min	Max	Avg	Total
Period	22-11-2015 00:00	23-11-2015 00:00		
Email Date	22-11-2015 00:05	22-11-2015 20:21		
Size	5 KB	142 KB	51 KB	355 KB

Status	Count	%age	URL Link
HAM	4	57.14	
LARGE	0		
SPAM	2	28.57	Review and Remail SPAM here:
DISCARD	1	14.29	
MALWARE	0		
Total	7		

[Unsubscribe from AVS notifications for:](#)

You can configure up to 3 different notifications per domain. Each notification is defined by entering the intended recipient email address, and then tweaking the notification parameters. A notification can be configured to run Daily, Weekly, Monthly or Yearly, and to run at a particular hour of the day covering the preceding period up to that hour. By default a notification will be Daily at midnight.

Management for the domain: yourdomain.com

Tagging Text:	*** SPAM - Tagged by Netnorth ***		
	Threshold	Allowed Range	Recommended
Spam Score:	5.1	5.1 and above	5.1
Discard Score:	0.0 Disabled	0.0 or 20.0 - 50.0	30.0
Enable Notification:	Email Address...	Scheduled...	
Enabled <input checked="" type="checkbox"/>	yourname@anywhere.com	Daily	@ 00:00
Last Updated:	never		Update Settings

Management for the domain: yourdomain.com

Tagging Text:	*** SPAM - Tagged by Netnorth ***		
	Threshold	Allowed Range	Recommended
Spam Score:	5.1	5.1 and above	5.1
Discard Score:	0.0 Disabled	0.0 or 20.0 - 50.0	30.0
Enable Notification:	Email Address...	Scheduled...	
Enabled <input checked="" type="checkbox"/>	yourname@anywhere.com	Daily	@ 00:00
Enabled <input checked="" type="checkbox"/>	stats@yourdomain.com	Weekly	Sunday @ 23:00
Last Updated:	never		Update Settings

Note: Multiple notifications with different periods can be configured to the same address. If they are run at the same hour of the day, they will be concatenated into one message.

Note: Notifications can be removed by simply deleting the address from the notification settings within the Portal, or they can be disabled by the recipient using the 'Unsubscribe' links included within any received notification.

4. AVS Whitelist / Blacklist Management.

Now that you're familiar with the 'natural behaviour' of the AVS system described above, you may want to influence it further by maintaining your own lists of senders to be 'allowed delivery' (whitelisted) or 'refused delivery' (blacklisted), no matter what the derived Spam Score turns out to be.

These lists are comprised of either a sender's full email address, or just the sender's bare domain name which will cover any and all users sending from that domain. They actually work by simply adding their own fairly large reputation score to the derived Spam Score.

Domains alone score less than a full email address, allowing you to blacklist a domain generally, but whitelist individual addresses from within that domain. Or vice versa.

Note: Although the WHITELIST / BLACKLIST greatly influence the reputation score of a spam email, it is still possible under extreme circumstances to derive a contradicting delivery status of SPAM / HAM if other rules significantly reduce / improve the reputation score respectively.

4.1 How do I manage Sender Whitelists and Blacklists?

Login to the Customer Portal, as described above, and click on the link ...

[AVS Whitelist/Blacklist Management](#)

Select your domain from the drop-down, and click 'Manage', which will display a combined list of blacklisted / whitelisted senders that are currently associated with your receiving domain.

The screenshot shows the Netnorth Limited Customer Portal interface for AVS Whitelist / Blacklist Management. It includes a 'Main Menu' link, a domain selection dropdown (currently showing 'yourdomain.com') with a 'Manage' button, and a section for 'Management for the domain: yourdomain.com'. Below this, there is a 'Search based on scanning reference' section with a 'Scanning Reference' input field and a 'Search' button. A red banner indicates 'No filterlist entries'.

You can then freely do any of the following to manage your lists.

4.1.1 How do I Blacklist a sender's address.

Select 'blacklist' from the drop-down, enter the unwanted sender address, and click 'ADD!', which will modify the senders list. Repeat this for all unwanted senders...

The screenshot shows the 'ADD' section of the AVS Whitelist / Blacklist Management interface. The 'ADD' dropdown is set to 'blacklist', and the 'FOR' field contains 'alfie@adomain.co.uk'. The 'Add!' button is visible. Below this, a table displays the current list of blacklisted senders:

Total of 3 entries		
<input type="checkbox"/>	BLACK	alfie@adomain.co.uk
<input type="checkbox"/>	BLACK	bertie@bdomain.com
<input type="checkbox"/>	BLACK	charlie@cdomain.co.uk
Total of 3 entries		

Note: Rather than go through the repeated process of adding many individual addresses, you can enter a comma separated list of multiple addresses in one click. For example, the following could be typed or pasted into the ADD field:

alfie@adomain.com,bertie@bdomain.com,charlie@cdomain.com

4.1.2 How do I Blacklist all senders in a given domain.

Select 'blacklist' from the drop-down, enter the unwanted sender domain, (ie the part of the address after 'username@', and click 'ADD!'...

ADD	blacklist	FOR	ddomain.com	Add!
Total of 4 entries				
<input type="checkbox"/>	BLACK		alfie@adomain.co.uk	
<input type="checkbox"/>	BLACK		bertie@bdomain.com	
<input type="checkbox"/>	BLACK		charlie@cdomain.co.uk	
<input type="checkbox"/>	BLACK		ddomain.com	
Total of 4 entries				

...which will modify the senders list and blacklist all users sending from 'ddomain.com'.

Note: Exceptions can be made by adding the full addresses of individual users at this domain to the WHITELIST.

4.1.3 How do I Whitelist a sender's address.

Select 'whitelist' from the drop-down, enter the desired sender address, and click 'ADD!'...

ADD	whitelist	FOR	friend@ddomain.com	Add!
Total of 5 entries				
<input type="checkbox"/>	BLACK		alfie@adomain.co.uk	
<input type="checkbox"/>	BLACK		bertie@bdomain.com	
<input type="checkbox"/>	BLACK		charlie@cdomain.co.uk	
<input type="checkbox"/>	BLACK		ddomain.com	
<input type="checkbox"/>	WHITE		friend@ddomain.com	
Total of 5 entries				

Note: In this example the whitelisted 'friend@ddomain.com' emails will still be delivered even though the 'ddomain.com' bare domain has been blacklisted separately, because a full email address is more influential than a domain name.

Note: Rather than go through the repeated process of adding many individual addresses, you can enter a comma separated list of multiple addresses in one click. For example, the following could be typed or pasted into the ADD field:

alfie@adomain.com,bertie@bdomain.com,charlie@cdomain.com

Note: Ad-hoc WHITELIST addresses can also be added from the **B/W** column in the 'AVS Reports' area of the Customer Portal.

4.1.4 How do I Whitelist all senders in a given domain.

Select 'whitelist' from the drop-down, enter the desired sender domain, (ie the part of the address after 'username@', and click 'ADD!'...

ADD	whitelist	FOR	edomain.net	Add!
Total of 6 entries				
	BLACK	alfie@adomain.co.uk		
	BLACK	bertie@bdomain.com		
	BLACK	charlie@cdomain.co.uk		
	BLACK	ddomain.com		
	WHITE	edomain.net		
	WHITE	friend@ddomain.com		
Total of 6 entries				

...which will modify the senders list and whitelist all users sending from 'edomain.net'.

Note: Exceptions can be made by adding the full addresses of individual users at this domain to the BLACKLIST.

4.1.5 How do I Remove a list entry.

To delete any list entry, simply click the cross at the start of the line.

4.1.6 Bare domain restrictions.

The AVS platform will not allow bare domains to be whitelisted for the popular community mail services, eg gmail.com, hotmail.co.uk, aol.com, etc. However, full addresses which start 'username@' at these domains can be added to the lists as usual.

4.2 How do I identify the actual sender of a spam email?

The sender information that you see in your email client is largely cosmetic, it only exists in the 'header' content of the email and isn't necessarily the sender's 'envelope' address used to transact the email delivery. Of course for normal email the cosmetic 'header' and actual 'envelope' sender addresses are likely to be similar if not exactly the same, but spammers will often take advantage of the fact that they can easily forge the displayed 'header' sender address to try and gain your trust.

So, when attempting to blacklist a sender it's important to recognise that the displayed sender address is possibly false, because blacklisting a forged header address won't necessarily stop the actual sender from sending you further spam.

At the bottom of the AVS Whitelist / Blacklist management screen, shown above, there is a tool to help you identify the actual 'envelope' sender used to transact the email delivery. Enter a 'Scanning Reference' from any email that has already been processed by AVS, and click 'Search'...

Search based on scanning reference

Scanning Reference:

...this will display the following information...

Search based on scanning reference

Scanning Reference:

Search Results:

Scanning Reference: 123-avs1-1234567890
Sender: realsender@spam.com
Recipient: yourname@yourdomain.com
Subject: This is an important message from your bank!
Mail Status: SPAM (9.83)

...In this example you would choose to blacklist the address 'realsender@spam.com' or the more encompassing domain 'spam.com'.

4.3 Which address should I list?

The apparent sender's address displayed in your email client is purely cosmetic. It is derived from the 'header' section within the email that was composed by the sender's email client. Whereas the actual sender's 'envelope' address is used by SMTP to transact the email delivery. It is announced to the sending and receiving mail servers when the email is sent.

Considering a typical spam email, either of these addresses can be forged. The 'header' address is easily forged and could be set to anything, usually something with authority that would gain your trust. The 'envelope' address can also be forged, but since it is partially policed by the sending server and you rarely actually see this address, it is usually less covert, and possibly a real domain that has been compromised elsewhere.

Considering a genuine email, the cosmetic 'header' and the actual 'envelope' sender addresses are likely to be similar if not exactly the same, (See **1.7** above).

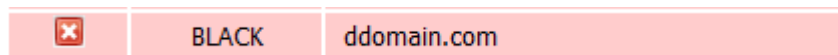
Netnorth's AVS services will attempt to compare both of these sender addresses to your Whitelist / Blacklist entries, but it is always better to list the actual 'envelope' sender address when possible.

It should be noted that when a spammer uses a forged cosmetic 'header' address, the actual 'envelope' sender address is typically a short-lived randomised user, and it may be more useful to carefully list the whole spammer's domain. For example, a spammer may send you a message with a forged 'header' address of accounts@your.trusted.bank.com, which you would see displayed by your email client once the message is delivered, but from an actual 'envelope' sender address of wss-john-844j@big.spammer.org.

Any of the following actions could have stopped the message from being delivered...

Action	Example	Comment
Blacklist the 'header' address, as displayed in your email client.	accounts@your.trusted.bank.com.	If this forged address matches the real address of other legitimate email, then that too would be blocked.
Blacklist the 'envelope' address, as derived from the Scanning Reference described above, or as listed in the AVS Reports described below.	wss-john-844j@big.spammer.org	Since the username appears to be generated randomly, this address is unlikely to be used repeatedly by the spammer, and would be ineffective in future.
Blacklist only the spammer's actual 'envelope' domain.	big.spammer.org	This is the most awkward action to implement, but is the most effective measure to take. (See How do I Blacklist all senders in a given domain above)

In summary, it's best to identify the spammer's actual 'envelope' address, reduce it to a plain domain (the part after the '@' symbol), and Blacklist the whole domain.



5. AVS Allowed User List management

Spam emails typically target real email addresses that have been harvested via: compromised address books, purchased mailing lists, malware, etc.

Additionally, automated spam will often send to known domains without actually knowing any of the real email addresses that are used by the domain. These speculative addresses will use:

common 'role accounts' (eg sales@yourdomain.com);
common usernames (eg david@yourdomain.com);
or completely random addresses (eg zjd7wwp@yourdomain.com).

'Allowed User' lists let you restrict delivery of email to only the predefined addresses that you want to be addressable at your domain. When an 'Allowed User' list is defined for your domain, then any attempt to send mail to non-listed recipients will be blocked regardless of the Spam Score for a message.

In practice this technique can increase the proportion of identified spam from the native 70% average to over 90% for heavily targeted domains.

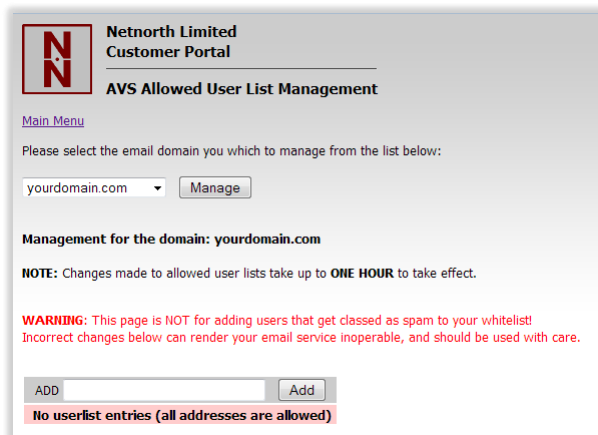
5.1 How do I manage a domain Allowed User list?

Login to the Customer Portal, as described above, and click on the link ...

[AVS Allowed User List Management](#)

Select your domain from the drop-down, and click 'Manage', which will display a list of recipients that are currently associated with your receiving domain.

Note: An empty list indicates that there isn't any restriction based on recipient addresses at your domain, and all email will be processed based on the Spam Score and associated Whitelist / Blacklist directly.



Netnorth Limited
Customer Portal

AVS Allowed User List Management

[Main Menu](#)

Please select the email domain you which to manage from the list below:

Management for the domain: **yourdomain.com**

NOTE: Changes made to allowed user lists take up to **ONE HOUR** to take effect.




WARNING: This page is NOT for adding users that get classed as spam to your whitelist!
Incorrect changes below can render your email service inoperable, and should be used with care.

No userlist entries (all addresses are allowed)

You can then freely do any of the following to manage your list.

5.1.1 How do I add an Allowed User?

Enter the allowed recipient address, and click 'ADD!', which will modify the allowed user list. Repeat this for all allowed recipients...

ADD	<input type="text" value="charlie@yourdomain.com"/>	Add!
Total of 3 entries		
	alfie@yourdomain.com	
	bertie@yourdomain.com	
	charlie@yourdomain.com	
Total of 3 entries		

Rather than go through the repeated process of adding many individual addresses to the same domain, you can enter a comma separated list of multiple addresses in one click. Additionally you can omit the '@yourdomain.com' from each address and it will be auto-appended as addresses are added. For example, either of the following could be typed or pasted into the ADD field:

alfie@yourdomain.com, bertie@yourdomain.com, charlie@yourdomain.com

OR


alfie, bertie, charlie

Note: Changes made to the Allowed User lists can take up to 1 hour to take effect.

Note: If your users have email aliases at the same domain (eg alfie@yourdomain.com and alfie.surname@yourdomain.com), then don't forget to add them into this list too.

Note: If your organisation uses more than one variant of a domain name (eg yourdomain.com and yourdomain.co.uk), then don't forget to create a separate Allowed User list for each domain.

5.1.2 How do I Remove a list entry.

To delete any list entry, simply click the cross at the start of the line. 

6. AVS Statistics

6.1 How do I know how effective AVS is?

- Use AVS Statistics Graphs.
- Use AVS Reports
- Extract AVS Reports

6.2 How do I Use AVS Statistics Graphs?

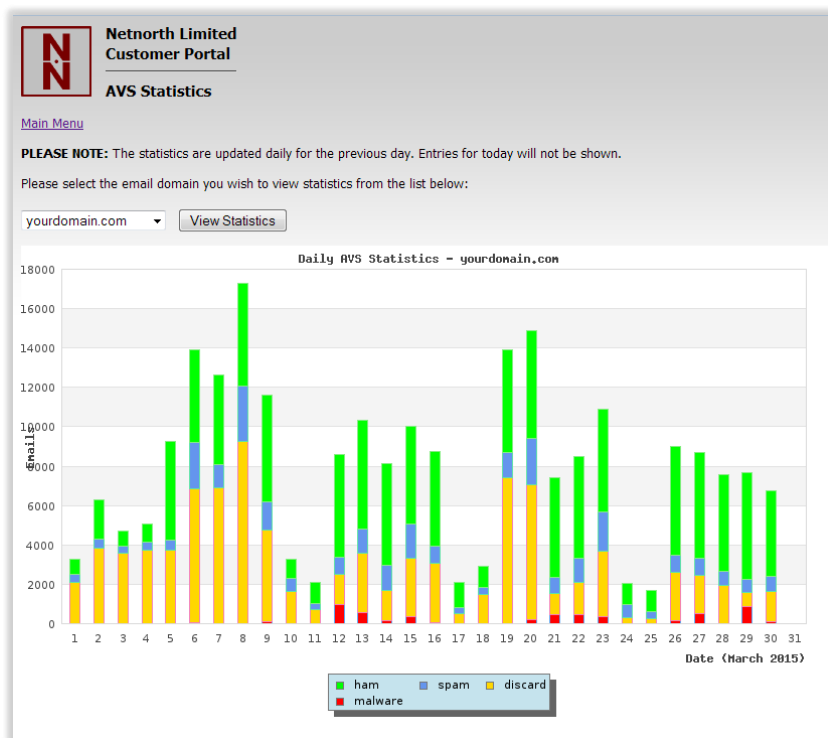
Login to the Customer Portal, as described above, and click on the link ...

[AVS Statistics Graphs](#)

Select your domain from the drop-down, and click 'View Statistics', which will display graphs of email quantities processed for:

Monthly quantities in the preceding 12 month period.

Daily quantities in the current calendar month (shown here).



Each plotted column shows the relative proportion of HAM and tagged SPAM that were delivered compared to discarded SPAM and VIRUS that were blocked.

6.3 How do I Use AVS Reports?

Login to the Customer Portal, as described above, and click on the link ...

[AVS Reports](#)

Select your domain from the drop-down, and click 'Manage', which will display a table of search criteria:

Enter any specific search criteria you may have, blank filter terms will be ignored during the search. Filter email terms can incorporate wildcards where:

- * (an asterisk) will match any number of characters.
- ? (a question mark) will match any single character.

If 'Sender' or 'Recipient' are filtered but don't contain @ (an at symbol) then the filter is applied only to the address's domain. So for example:

- 'nameA@domainA.com' would match only the specified full address;
- 'domainA.com' would match all addresses at the specified domain;
- 'nameA@*' would match the user 'nameA' at any domain;
- 'domainA.*' would match all addresses at all variants of 'domainA';
- '*alf*@*' would match any users with 'alf' anywhere in their name at any domain.

- 'Date From' values are assumed to be from 00:00:00 AM
- 'Date To' values are assumed to be to 23:59:59 PM

By default the search will be limited to the most recent 150 transactions, this can be increased in the form if needed, but large result sets may take some time to be compiled.

AVS Statuses can be un/ticked to confine results to statuses of interest.

Click on 'Search' to collate matching email transaction. This will display 'Searching...' whilst results are compiled, followed by 'Matched **xx** emails...' when the search is complete...

Matched 17 emails...

Check All Status Checked Report Checked Batch Process

Summary Text Report Report Remail Remail & Whitelist Whitelist

Status	Score	AVS Ref	Dated	Size	B/W	Sender	Recipient	Subject
<input type="checkbox"/> HAM	-2497.61	542-avs4-1421536390	17-01-2015 23:13	1354	+	gaynor@nodue.com	someone@yourdomain.com	Helix s2
<input type="checkbox"/> SPAM	14.432	840-avs4-1421528687	17-01-2015 21:04	5174	B	104812@hewsl03.webreus.nl	saab-central@yourdomain.com	Your account PayPal ha
<input type="checkbox"/> DISCARD	78.255	873-avs2-1421497585	17-01-2015 12:26	44497	+	bounce-mc.us3_24314663.512973-1plus...	1plus@yourdomain.com	An invitation to improve
<input type="checkbox"/> HAM	-168.795	216-avs1-1421462138	17-01-2015 02:35	25212	W	bounce-mc.us5_12680195.139177-kicksta...	kickstarter@yourdomain.com	Test Drive the Mustang
<input type="checkbox"/> HAM	-173.191	925-avs1-1421462058	17-01-2015 02:34	25212	W	bounce-mc.us5_12680195.139177-starciti...	starcitizen@yourdomain.com	Test Drive the Mustang
<input type="checkbox"/> HAM	-2496.446	600-avs1-1421452983	17-01-2015 00:03	10975	+	portal@www10.netnorth.co.uk	avs@yourdomain.com	Netnorth AVS Daily Sun
<input type="checkbox"/> HAM	-909.845	299-avs1-1421430634	16-01-2015 17:50	167115	+	bounce-mc.us2_2906690.1713237-elite=...	elite@yourdomain.com	Elite: Dangerous Newsl
<input type="checkbox"/> HAM	1.381	253-avs3-1421421463	16-01-2015 15:17	93068	+	bounces+608722-11a7-howtogeek=yourd...	howtogeek@yourdomain.com	How to Enable HDMI-Ce
<input type="checkbox"/> HAM	-96.967	758-avs4-1421420480	16-01-2015 15:01	8039	+	account-security-noreply@account.micros...	skype@yourdomain.com	Verify your email addre
<input type="checkbox"/> HAM	-2496.446	232-avs1-1421366583	16-01-2015 00:03	11473	+	portal@www10.netnorth.co.uk	avs@yourdomain.com	Netnorth AVS Daily Sun
<input type="checkbox"/> HAM	1.601	956-avs4-1421335078	15-01-2015 15:18	84159	+	bounces+608722-11a7-howtogeek=yourd...	howtogeek@yourdomain.com	Wearables 101: What T
<input type="checkbox"/> HAM	-243.01	467-avs2-1421329169	15-01-2015 13:39	62750	W	bounce+a1e407.2810-instructables=your...	instructables@yourdomain.com	Floating Bed, Perpetual
<input type="checkbox"/> HAM	-255	676-avs2-1421323212	15-01-2015 12:00	2042	W	atlas@ripe.net	ripe@yourdomain.com	Probe 11168 is disconn
<input type="checkbox"/> SPAM	9.643	242-avs1-1421318901	15-01-2015 10:48	9005	+	noreply.newcastleaccommodationnews@sp...	info@yourdomain.com	Superb property opport
<input type="checkbox"/> HAM	-754.69	951-avs4-1421312591	15-01-2015 09:03	2202	W	fred@bloggs.co.uk	someone@yourdomain.com	RE: Ford Performance
<input type="checkbox"/> HAM	-260.02	896-avs1-1421310618	15-01-2015 08:30	2039	W	atlas@ripe.net	ripe@yourdomain.com	Probe 11168 is disconn
<input type="checkbox"/> HAM	-2496.446	716-avs1-1421280182	15-01-2015 00:03	11074	+	portal@www10.netnorth.co.uk	avs@yourdomain.com	Netnorth AVS Daily Sun

These results can be browsed directly on screen, or can be individually selected via checkboxes, and extracted into a separate report. (See 6.4 below.)

A status shown in GREEN is clean and will have been delivered naturally.

A status shown in AMBER has not been ratified as clean, but will usually have been delivered or treated as potential spam, possibly with an additional 'Spam Tag'.

A status shown in RED will have been blocked from delivery, either because of an extreme spam reputation or because it has been identified as dangerous malware.

A 'Sender' listed with a background colour of RED or GREEN will, at the time the message was processed, have been recognised as an entry in your domain's BLACKLIST or WHITELIST respectively. Note that the displayed Sender's status may have been subsequently changed in 'AVS Blacklist / Whitelist management' options, and that the current Sender status will be flagged in the B/W marker column of the results.

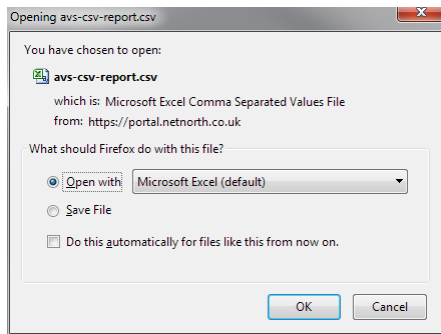
- W - Sender address is in your WHITELIST when the report was run.
- W - Sender domain is in your WHITELIST when the report was run.
- B - Sender address is in your BLACKLIST when the report was run.
- B - Sender domain is in your BLACKLIST when the report was run.

For example in the image above, the second message was identified as SPAM, and the sender is showing in a BLACKLIST at the time the report was run, but not BLACKLISTED at the time the message was originally sent.

After the tabulated results is a short summary...

Matched filter Stats				Last 7 Days Summary				Last 30 Days Summary						
	Min	Max	Avg		Min	Max	Avg		Min	Max	Avg			
Size		1 KB	163 KB	32 KB	Size		1 KB	162 KB	33 KB	Size		506 B	833 KB	36 KB
Date	15-01-2015 00:03 17-01-2015 23:13			Date	09-03-2015 15:17 16-03-2015 10:03			Date	14-02-2015 15:00 16-03-2015 10:03					
Status	Count	%age	Main Sender	Main Recipient	Status	Count	%age	Main Sender	Main Recipient	Status	Count	%age	Main Sender	Main Recipient
HAM	14	82.35	www10.netnorth.co.uk - 3	avs@yourdomain.com - 3	HAM	41	93.18	www10.netnorth.co.uk - 7	someone@yourdomain...	HAM	167	93.82	www10.netnorth.co.uk - ...	someone@yourdomain...
LARGE	0				LARGE	0				LARGE	0			
SPAM	2	11.76	hewsl03.webreus.nl - 1	saab-central@yourdom...	SPAM	3	6.82	easysender.biz - 1	info@yourdomain.com - 3	SPAM	9	5.06	bar-sending.org - 2	info@yourdomain.com - 7
DISCARD	1	5.88	mail65.atl71.mcdlv.net - 1	1plus@yourdomain.com...	DISCARD	0				DISCARD	0			
MALWARE	0				MALWARE	0				MALWARE	2	1.12	webxc49s06.ad.aruba.it...	saab-central@yourdom...
Total	17				Total	44				Total	178			

...which details statistics for the filtered 'Matched' results that have just been collated, compared to statistics for the 'Last 7 days' and the 'Last 30 days'.



...from which you can manipulate the details as you see fit...

	A1									
	A	B	C	D	E	F	G	H	I	J
1	Date/Time	Status	Score	Size	Sender	Recipient	Subject	Scanning Ref		
2	17/01/201	SPAM	14.432	5174	104812@h	saab-centr	Your accou	840-avs4-1421528687		
3	17/01/201	DISCARD	78.255	44497	bounce-mc	1plus@you	=?utf-8?Q?	873-avs2-1421497585		
4										
5										

6.5 How do I use Email Notifications?

(See 3.5 above)

7. AVS Batch Processing

From within AVS Reports, any 'checked' results can be submitted for 'Whitelisting' and/or re-delivery via 'Remail', using the same selection methods as with Reports (See **section 6.4** above). This facility is subject to your user privileges and to message availability.

7.1 AVS Batch Remail

Matched 17 emails...

Check All Status		Checked Report		Checked Batch Process				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Summary Text Report	Report	Remail	Remail & Whitelist	Whitelist
Status	Score	AVS Ref	Dated	Size	B/W	Sender		
<input type="checkbox"/>	HAM	-2497.61	542-avs4-1421536390	17-01-2015 23:13	1354	+	gaynor@noclue.com	
<input checked="" type="checkbox"/>	SPAM	14.432	840-avs4-1421528687	17-01-2015 21:04	5174	B	104812@hewsl03.webreus.nl	
<input checked="" type="checkbox"/>	DISCARD	78.255	873-avs2-1421497585	17-01-2015 12:26	44497	+	bounce-mc.us3_24314663.512973-1pl	
<input type="checkbox"/>	HAM	-168.795	216-avs1-1421462138	17-01-2015 02:35	25212	W	bounce-mc.us5_12680195.139177-kick	
<input type="checkbox"/>	HAM	-173.191	925-avs1-1421462058	17-01-2015 02:34	25212	W	bounce-mc.us5_12680195.139177-sta	
<input type="checkbox"/>	HAM	-2496.446	600-avs1-1421452983	17-01-2015 00:03	10975	+	portal@www10.netnorth.co.uk	

After making a checkbox selection and clicking on 'Remail', the messages concerned will only be sent to the original recipients as specified by the message author, and cannot be 'redirected' to an alternative address.

Any messages submitted for re-delivery will be reported on in a separate browser tab delivery report...

```
Session User: yourname

Remail: SKIPPED : This email is older than the 30 day retention limit, and cannot be redelivered.
Date/Time: Sat 17th Jan 2015 9:04:50pm
Size: 5174
Sender: 104812@hewsl03.webreus.nl
Recipient: saab-central@yourname.com
Subject: Your account PayPal has been Limited !
Status: !SPAM 14.432
Scanning Ref: 840-avs4-1421528687
Queue ID: tOHL4kaY072937

Remail: SKIPPED : This email was originally DISCARDED and cannot be redelivered.
Date/Time: Sat 17th Jan 2015 12:26:31pm
Size: 44497
Sender: bounce-mc.us3_24314663.512973-1plus=yourname.com@mail65.atl71.modlv.net
Recipient: 1plus@yourname.com
Subject: =?utf-8?Q?An=20invitation=20to=20improve=20the=20OnePlus=20experience=?
Status: !DISCARD 78.255
Scanning Ref: 873-avs2-1421497585
Queue ID: tOHCQN9s046036

SUMMARY:
SKIPPED 2

#####
#
# WARNING...
#
# Some of the messages
# have not been queued.
#
#####
```

Note in the above example neither of the selected messages could be Remailed. One message was originally discarded, the other message is simply too old, both are no longer available.

7.2 AVS Batch Whitelist

Matched 17 emails...

Check All Status		Checked Report			Checked Batch Process			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Summary Text Report ▾	Report	Remail	Remail & Whitelist	Whitelist
Status	Score	AVS Ref	Dated	Size	B/W	Sender		
<input type="checkbox"/>	HAM	-2497.61	542-avs4-1421536390	17-01-2015 23:13	1354	+	gaynor@noclue.com	
<input checked="" type="checkbox"/>	SPAM	14.432	840-avs4-1421528687	17-01-2015 21:04	5174	B	104812@hewsl03.webreus.nl	
<input checked="" type="checkbox"/>	DISCARD	78.255	873-avs2-1421497585	17-01-2015 12:26	44497	+	bounce-mc.us3_24314663.512973-1pl	
<input type="checkbox"/>	HAM	-168.795	216-avs1-1421462138	17-01-2015 02:35	25212	W	bounce-mc.us5_12680195.139177-kick	
<input type="checkbox"/>	HAM	-173.191	925-avs1-1421462058	17-01-2015 02:34	25212	W	bounce-mc.us5_12680195.139177-sta	
<input type="checkbox"/>	HAM	-2496.446	600-avs1-1421452983	17-01-2015 00:03	10975	+	portal@www10.netnorth.co.uk	

After making a checkbox selection and clicking on 'Whitelist', the messages concerned will have their sender addresses whitelisted.

Any senders that are already blacklisted will be skipped, and must be manually edited (See **section 4** above).

```

Session User: yourname

Whitelist: LISTED : This sender address has been added to your WHITELIST for the domain.
(Additionally the sender's bare domain is already BLACKLISTED)
Date/Time: Sat 17th Jan 2015 9:04:50pm
Size: 5174
Sender: 104812@hewsl03.webreus.nl
Recipient: saab-central@yourname.com
Subject: Your account PayPal has been Limited !
Status: SPAM 14.432
Scanning Ref: 840-avs4-1421528687
Queue ID: tOHL4kaY072937

Whitelist: LISTED : This sender address has been added to your WHITELIST for the domain.
Date/Time: Sat 17th Jan 2015 12:26:31pm
Size: 44497
Sender: bounce-mc.us3_24314663.512973-1plus=yourname.com@mail65.at171.mcdlv.net
Recipient: 1plus@yourname.com
Subject: =?utf-8?Q?An=20invitation=20to=20improve=20the=20OnePlus=20experience?=
Status: DISCARD 78.255
Scanning Ref: 873-avs2-1421497585
Queue ID: tOHCQN9s046036

WHITELIST SUMMARY:
-----
LISTED 2
-----

```

Note in the above example both senders were successfully Whitelisted, even though one of the messages is already flagged as having its domain blacklisted. This is because you are able to Whitelist a sender's full address as an exception to existing blacklisted domains, (See **section 4.1.3** above).