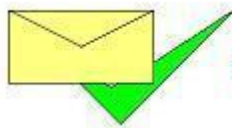




Spam Safe Mail
for Microsoft Exchange Server

Technical Manual

For Clients For



Spam Safe Mail
for Microsoft Exchange Server



Contents

Overview.....	3
Features.....	3
Prerequisite Client Requirements.....	3
Our Goal.....	4
Our Experience.....	4
Email flow diagram.....	5
Diagram 1 – Email Flow Diagram.....	5
Incoming Email Setup – Technical Description.....	5
Changes to the email mappings.....	7
SpamFilterOut Outgoing Queue – Technical Description.....	7
Clients with Failover Internet Connections.....	7
Outgoing Email Setup – Technical Description.....	8
How it works – Technical Description.....	11
Rejection Description.....	12
Still Receiving Spam.....	13
Whitelisting Contacts.....	13
Guarantee.....	14
Two Methods of Contracting.....	14
Frequently Asked Questions.....	15
Notes.....	15
Document Version Control.....	15



Overview

SpamSafeMail for Microsoft Exchange Server is a network email scanning and filtering service provided by Mark Andrew Smith Limited and is aimed at companies who have their own Microsoft Exchange Server in which to send and receive their emails and who need total piece of mind with their email and network security.

This manual is to be used to obtain a better technical understanding of how SpamSafeMail works and so is not aimed at the end user but a technical person needing to know how to best obtain results from our service.

Features

- Spam and Virus email filtering at the network level before reaching your server by professionals.
- Easy set up by Exchange experts via remote control.
- Up to 3 distinctly different email domains per account. More as a cost optional extra.
- Unlimited number of email addresses.
- Optional multiple Exchange server routing ability.
- Ease of use - Managed service by anti-spam professionals.
- Service 'learns' about your Business and email language used in real time.
- Is more than 99.98% accurate in decision making.
- No emails are lost – rejected email notifications to sender.
- Incoming emails are delivered in real time to your Exchange server.
- Incoming emails are stored and delivered later in case of broadband failures.
- Users can report spam by forwarding spam email to 'spam@spamsafemail.net'.
- Users can report not spam by forwarding email to 'notspam@spamsafemail.net'.
- Email examples sent by one user teaching the service helps all users.
- Optional auto forward incoming email to external email addresses or mobiles phones.
- Blackberry friendly.
- Optional incoming fax to email attachment service.
- Easy to sign up, it just works!

Prerequisite Client Requirements

- Microsoft Exchange Server or Microsoft Small Business Server using Exchange.
- Broadband with a static IP address.



Our Goal

At Mark Andrew Smith Limited our goal is to clean the Internet of spam and viral emails by providing the best service on the Internet. In any security system, changes need to be made on a frequent basis to remain current and up to date when new exploits are tried and found. Due to this, the only way in which to keep all servers up to date is by having a centralised network service operated by professionals – hence the birth of SpamSafeMail in 2006.

Our Experience

Mark Andrew Smith Limited are professionals who know all about network security and have experience and a proven track record of network email scanning. Our end user client base who like our invaluable SpamSafeMail service include:-

- Farsight Solutions Ltd
- Ainsbury Insurance Brokers Ltd
- Directives Ltd (as part of MyServer)
- Blackshaw Sykes and Morris Ltd
- Catele Ltd
- Elite Edge Marketing Consultants Ltd



Email flow diagram

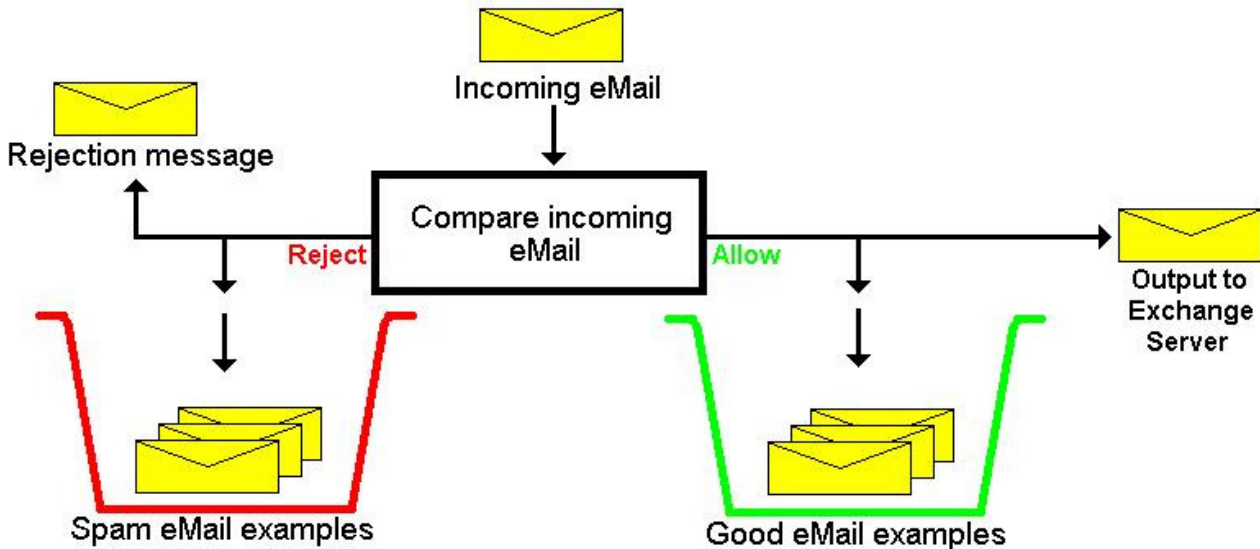


Diagram 1 – Email Flow Diagram

Incoming Email Setup – Technical Description

Clients who sign up to the service need to point their domains MX records at our SpamSafeMail service. We do not need to host their website nor handle their DNS nor domain renewals, all we need to make the service work for them is to exclusively handle their domains email.

We usually ask them to setup their domains MX records to point to us, for example, if their company is Acme Ltd and have a domain acme.co.uk, then they setup the records as follows:-

acme.co.uk.	MX	10	mx1.spamsafemail.net.
acme.co.uk.	MX	20	mx2.spamsafemail.net.

Clients **must not** add their own MX records as backups in addition to our own as it potentially will allow security to be bypassed undoing our work not to mention that emails will be routed wrongly and lost.

Many clients have not the technical expertise to alter their MX records themselves. This can be delegated to the person or company who looks after their IT or domain, or we can assist if they supply us their credentials to sign on and make the technical changes to the MX records for them. **We will not offer any other additional IT nor DNS services** as it is outside the remit of the SpamSafeMail service.

Clients will need to ensure the SMTP port, port 25 is open on their broadband firewall and be port forwarding to the local static IP address of their Microsoft Exchange Server on their local LAN (or DMZ if they are using one). Again, we can assist with this if they have not an ISP managed broadband router but of course we will need the username and password sign on details to the router to do this.



Clients also will need to pass to us their public static IP address of their broadband router. We can then setup the out bound queue on the SpamSafeMail service to redirect scanned emails to their Microsoft Exchange Server at their premises. This is done by setting up an internal DNS service on our mail servers so that for example a company called ACME Ltd who will have set their servers domain up as “acme.local”, we will setup a DNS as follows:-

```
acme.local.          MX    10    spamfilterout.acme.local.  
spamfilterout.acme.local.    A      <client public static IP address>
```

Now all we need to do is map valid email addresses as follows:-

sales@acme.co.uk: sales@acme.local

peter.smith@acme.co.uk: peter.smith@acme.local

This stops spammers trying default “catch all” addresses which are not needed on our system. They would get their spam email through by using an address like:-

dhlkrhjc@acme.co.uk

This **would not** get through as it is not mapped on our systems.

At this point we will need a list of valid email addresses from the end user to setup on the valid address list.

Note: End user clients who have erroneously setup their local security domain as “acme.co.uk” instead of “acme.local” as Microsoft recommend, then they will have to setup the server to additionally accept email for “acme.local” since you cannot change the domains name. Not only was erroneously setup it is now however set in stone.

One of the big advantages of having the “.local” local security domain is that we can map multiple domains through without additional work at the clients own premises. For example, the client now additionally want to handle email for wigets.com, we can now do something in the mapping like:-

sales@acme.co.uk: sales@acme.local

peter.smith@acme.co.uk: peter.smith@acme.local

sales@wigets.com: sales@acme.local

In another scenario, the end user client now expands and decides that their company will now be handled by two email servers, one called “london.acme.local” and one called “newyork.acme.local”. No problem for us, we can create two internal DNS entries on our systems as follows:-

```
london.acme.local.    MX    10    spamfilterout.london.acme.local.  
spamfilterout.london.acme.local.    A      <london public static IP address>
```

and:-

```
newyork.acme.local.  MX    10    spamfilterout.newyork.acme.local.  
spamfilterout.newyork.acme.local.    A      <newyork public static IP address>
```

mapping now becomes:-

sales@londonwigets.com: sales@london.acme.local.



sales@newyorkwigets.com: sales@newyork.acme.local.

allsales@acme.co.uk: sales@london.acme.local,sales@newyork.acme.local

As you can see, the routing is extremely flexible and allows for multiple users, multiple domains, multiple servers and for all manner of expansion that a Business may need.

Changes to the email mappings

The above email mappings can be add to, changed or deleted easily by emailing request changes to 'Support@SpamSafeMail.com' in the above format. Note: Resellers must handle the email request from clients and forward on to us. Changes will be completed within one working day and a confirmation reply by email sent.

SpamFilterOut Outgoing Queue – Technical Description

If the broadband that the Microsoft Exchange server is behind happens to be down due to a technical fault, we can hold the email in a post filtering outgoing queue that we call 'SpamFilterOut' for 72 hours. We will try to deliver to the broadband every hour until 72 hours has passed when we will time out the delivery and return a error '451 Mail Server Unavailable' error to the sender.

If the public static IP address needs changing for the clients broadband, then so long as the new broadband SMTP port is correctly port forwarding we can do this and the queue will be delivered within the next hour retry. This method works well if a client changes ISP.

Clients with Failover Internet Connections

If a client has two paths into their premises and Microsoft Exchange Server, we can cater for this fail over ability on our internal DNS servers by adding in multiple spamfilterout routing records as follows:-

acme.local.	MX	10	spamfilterout.acme.local.
spamfilterout.acme.local.		A	<client public static IP address 1>
spamfilterout.acme.local.		A	<client public static IP address 2>



Outgoing Email Setup – Technical Description

Our system needs to learn about the words and the type of language used in the clients Business. This means that the clients Microsoft Exchange server needs to send all outgoing email via SpamSafeMail. We will keep a copy of all outgoing email for a period of 28 days as examples in a good bin. This has significant advantages over other systems as the SpamSafeMail system learns about the language used in Business emails in real time and this is how it can make such a high accuracy rate of more than 98%.

All versions of Microsoft Exchange Server have a function to forward all outgoing emails to a “smart host” in which to send email on behalf of a company. The SpamSafeMail service allows you to log on using authentication to send email via ourselves using this “smart host” function. All emails sent via this method are added to the good bin so that the decision making part of the system immediately starts learning about the clients Business, words and language used.

Sending emails from Microsoft Exchange Server using the “smart host” function is **mandatory** as otherwise SpamSafeMail will not be able to learn about the emails sent from the Business and we would not be able to whitelist contacts, nor make accurate decisions about incoming emails. **We cannot stress how important this is.**

An additional benefit of sending outgoing emails via SpamSafeMail is that network scanning systems like ours that compare the IP address with PTR records and do reverse DNS lookups would reject email from the local Microsoft Exchange Server as it is only behind a broadband connection. We overcome this problem once and for all for the client.

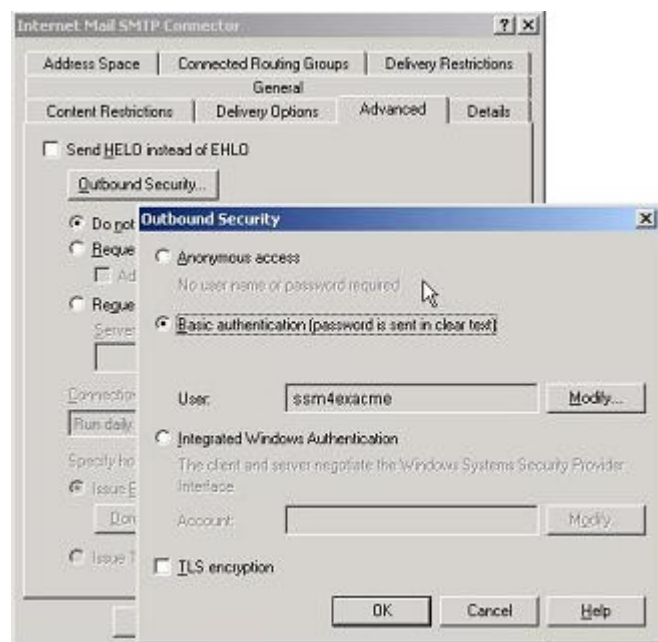
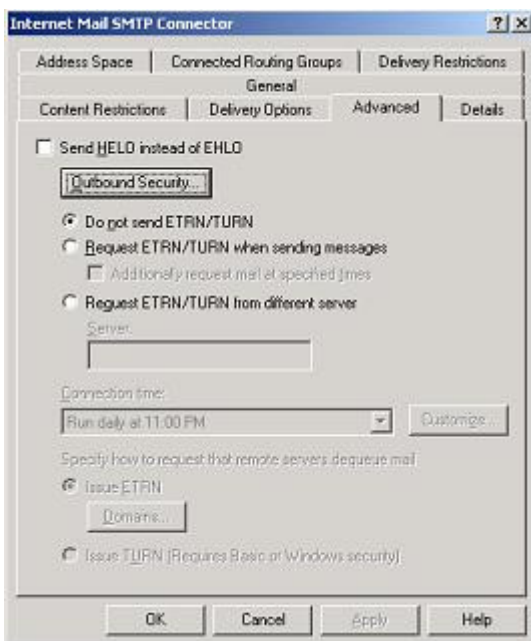
To set up the “smart host” function within Microsoft Exchange Server, on the server console go into the Exchange System Manager. Locate and expand the “Connectors” section and right click and select the properties of the “Internet Mail SMTP Connector”.



You will see a screen like this:-

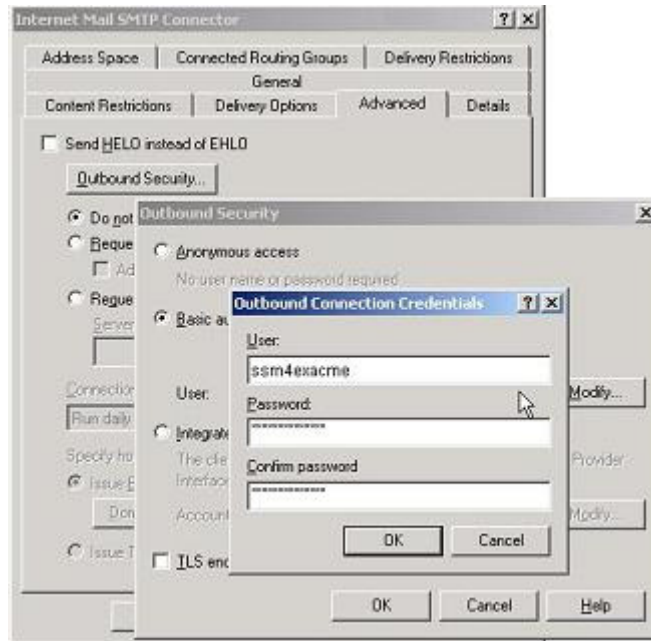


Click on “Forward all mail through this connector to the following smart hosts” and in the box immediately below type “mail.spamsafemail.net”. Now click on the “Advanced” tab. You are now navigating to enter your username and password to be able to authenticate to our SpamSafeMail system to be able to send email via ourselves and to automatically whitelist your contacts. Now click on the “Outbound Security...” button and choose “Basic Authentication”.





Now click the “Modify...” button to enter your SpamSafeMail username and Password as follows:-



Click “OK” three times and restart your Microsoft Exchange Server to reset the outgoing email queues.



How it works – Technical Description

The SpamSafeMail system attacks spam emails in the following ways:-

1. Any new email from a contact not known on a whitelist (ie not previously corresponded with) will be delayed for 300 seconds. Most spammer systems give up after 30 seconds and do not return. Real email server systems retry every 5 minutes so on the second automatic redelivery attempt, the email is passed through this stage. If the incoming contact is on a whitelist, then this delay is skipped.
2. The sending email server is checked against the SpamHaus list of known spammers and open email relays and rejected email from that server with the SpamSafeMail rejection message.
3. We will check the sending servers domain name and IP address and compare this against the registered MX and PTR records for the domain and IP address and make a genuine decision on if this is the authorised mail server for this email domain and rejecting the email if necessary with the SpamSafeMail rejection message.
4. If an email gets through to this stage, we will now compare the incoming email with the examples of good and bad emails. This comparison stage compares not only the words in the email but the language used in the email. If the email is deemed to be good, it is passed through to the next stage. If it is bad, it is rejected with the SpamSafeMail rejection message.
5. If an incoming email is received from someone not known on a whitelist (ie not previously corresponded with) and contains an attachment of an “executable type” (ie .exe or .bat or Office attachments etc) then the email is rejected with the SpamSafeMail rejection message. Ensure that the contact is known to the client by whitelisting them to receive these emails with attachments.
6. Finally, we do not allow “catch all” emails on our system which spammers rely on to get email through. Each valid end user email address **must be** mapped to a local address on the Exchange server on the SpamSafeMail service.
7. Before final delivery to the local Exchange server, the email is checked for viruses.



Rejection Description

When a rejection of an incoming email occurs, the incoming transmission is stopped and an error is raised and passed back to the originating server.

The error raised is error 500 a permanent error so that the sending server does not continue to retry. We also pass back a human readable error message that the sending originating server can use to pass back to the sender of the email in case the email was falsely rejected by us.

The rejection message from SpamSafeMail says:-

500 Your email appears to be unsolicited -- Please make contact by telephone and ask the recipient to unlock you and whitelist you by sending a blank email from them to you.

Please note: That some web based email systems like AOL and Hotmail simply report back to the user that there was an error and do not display our rejection message. There is nothing we can do about this as this is a limitation of those web mail systems. Our own web mail product acts correctly in this respect.

When we reject an email, a copy is placed in the rejection examples bin and stays there for 7 days. Please note also that we cannot hold large email messages in the rejection bin otherwise that would be one way in which to bring down our system by passing spam with huge attachments. To counter this, we only keep up to where we broke off transmission as described above. This is usually at 64Kbytes of information so we may only have an incomplete message.

Mark Andrew Smith Limited should not be contacted to recover incomplete messages, users simply email a blank message to the originating sender and then ask them to resend.

In the case of automated systems that send an email out as part of a sign up process, these emails can be lost as the rejection message is not being read by the automated system. These same automated systems are actually the bulk of spam as they collect email addresses and then those companies sell or share them on to other third parties. It is not advisable to use these systems but instead contact the companies by telephone to sign up for their goods and services. Mark Andrew Smith Limited can retrieve the email from the rejection bin upon request. This may take up to 24 hours due to support volume.



Still Receiving Spam

Occasionally our systems will look at a message and decide if it is not sure that the message is not spam and pass it through. If the client thinks differently, then they can forward this email to a special email address which will take it out of the good bin and place the example in the bad bin. The address in which to make this correction and forward the email to do this is:-

spam@SpamSafeMail.net

The SpamSafeMail system will then learn from its mistakes as it has now moved the email from the good to the bad bin. This single action by one user adds benefit for all the users in that company as the rules are constantly being updated as part of a real time learning process by SpamSafeMail.

In this same way, Mark Andrew Smith Limited can also add known spam emails to the central bad spam bin which of course benefits all users across all clients and end users.

This centralised system allows better control over what is determined to be spam and what is genuine email in real time during the working day and is something that cannot be achieved if the software is only installed locally on a clients server.

Whitelisting Contacts

When a new external email contact is made it is common practise using SpamSafeMail to first send a blank email to that contact in the normal manner. Sending a blank "wasted" email in this manner has the effect of white listing this contacts email address so that they are then allowed to send email into the SpamSafeMail end user unhindered. This also has the effect that this white listed email address is now available to all users of the end user client, ie only one user in the company needs to white list the new contact.

Note also, that if the contact themselves are on SpamSafeMail, this "wasted" email may never arrive, so both parties may need to send a "wasted" email to white list each other. Email will now flow unhindered between these two addresses.



Guarantee

Mark Andrew Smith Limited take seriously network security and guarantee that clients who use our SpamSafeMail filtering service that they receive the up most of care when handling their emails and we realise and respect that Business is conducted over the Internet.

We will go out of our way in which to ensure that customers are happy with our system and will ensure that every query raised will be looked into in full and changes to the SpamSafeMail system made on behalf of the client.

Clients can raise queries by emailing 'Support@SpamSafeMail.net' the following information:-

- Client/User Contact Information
- Description of problem
- Email Address From
- Email Address To
- Date and Time of Problem
- Nature of email sent or received

Failure to submit all these would mean a delay into looking into the problem or the problem not being able to be found resulting a further delay and the possibility of lost Business. It is important that the client is able to assist with valuable details so that we can provide in return full technical assistance as part of the service.

Two Methods of Contracting

There are two ways in which we can set up contracts for SpamSafeMail, direct with the end user client or as a service provider to other IT or Telecoms companies. The differences are as set out in the table below:-

<u>Direct to End User Client</u>	<u>Via Reseller as a Service Provider</u>
<ol style="list-style-type: none">1. End User clients will be a direct client of Mark Andrew Smith Limited and so will be invoiced directly.2. As a direct client the End User will be entitled to support and Mark Andrew Smith Limited will provide support direct to the End User Client.3. Mark Andrew Smith Limited may from time to time offer other services to our direct client base.	<ol style="list-style-type: none">1. Mark Andrew Smith Limited will provide the SpamSafeMail service as a white badged service for resale by other third party reseller IT and Telecom companies.2. We will invoice the third party reseller who we have a contract with as a Service Provider for SpamSafeMail on behalf of their clients.3. The reseller must make their own provision for billing the End User and collecting revenue in a timely fashion.4. Only the third party reseller is entitled to support. We will not contact nor allow contact from the End User Client.5. The reseller must make their own provision for dealing with End User queries and if necessary passing them on to ourselves for further investigation.



Frequently Asked Questions

- Question: What happens to rejected emails?
Answer: An error message is returned to the sender to make telephone contact.
- Question: Email attachments are not coming through.
Answer: Ask the user to whitelist the sender by sending them a blank email.
- Question: Some not all inbound emails are not coming through.
Answer: Either the outgoing 'smarthost' is setup incorrectly or there is an error in the MX records setup for the domain for incoming emails. Check both.
- Question: What happens if our broadband is down.
Answer: We will hold the emails for 72 hours in a queue, retrying hourly.
- Question: Can clients or IT companies have access to the rejected bin?
Answer: No, in case the files contain viruses.
- Question: I still get the occasional item of spam through, how can I stop it?
Answer: The system was unsure and so passed it through. Please teach it by forwarding the spam email to a special learning email address spam@SpamSafeMail.net. **DO NOT** forward to Mark Andrew Smith Limited support otherwise the system will learn this email is acceptable as SpamSafeMail learns about everything you send out.
- Question: If I wish to transfer off SpamSafeMail, how much notice period do I need to give?
Answer: One calendar month.

Notes

Document Version Control

	Name	Dated
Author	Mark Andrew Smith	26 th July 2008
Approved by		
Last Revised by	Mark Andrew Smith	7 th August 2008