

How to Configure Microsoft Exchange to use the Arrowmail Smarthosts

Arrowmail has 3 separate Smarthost mail-servers and, luckily, both Exchange 2003 and 2007 know how to make use of multiple Smarthosts for redundancy and load-balancing. This means that if one of our Smarthosts is very busy, has failed or is undergoing maintenance, your Exchange server can continue to send out emails, uninterrupted.

In Exchange 2003 it's possible to configure a Smarthost on the **Default SMTP Virtual Server** but, if you do it this way, you can only set a *single* Smarthost. You must, therefore, use an **SMTP Connector** for your outgoing emails which *does* allow multiple Smarthosts to be specified.

For Exchange 2007 there's only one way to configure a Smarthost which is on the **Send Connector**.

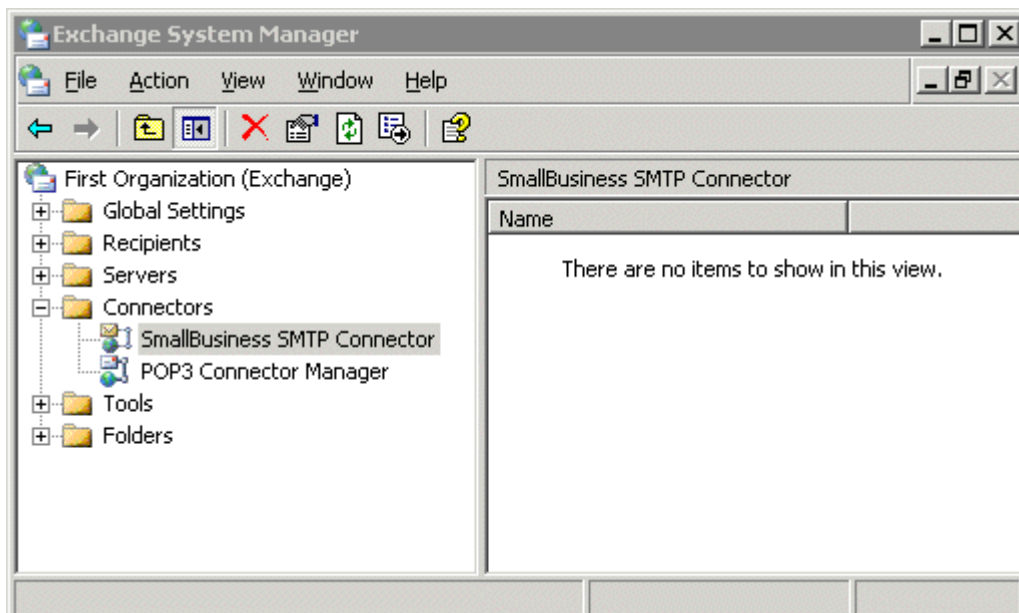
For simplicity, the instructions in this document assume that you only have one Exchange server in your organisation.

If you have multiple Exchange servers, there are a few minor differences which we'll be happy to advise you about.

How To Configure a Smarthost on Exchange 2003

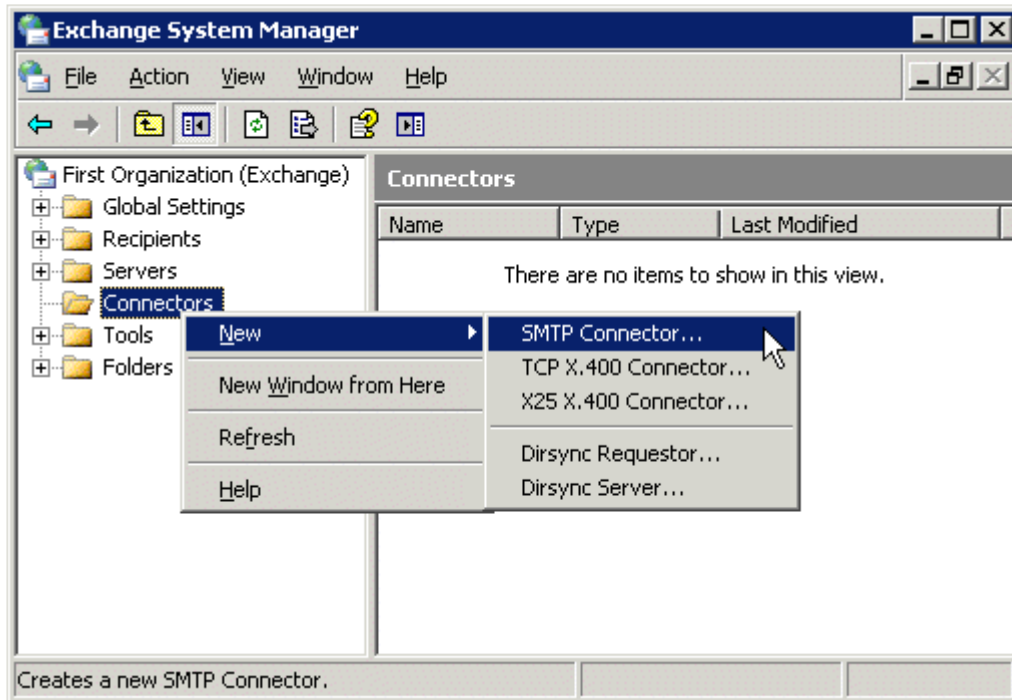
Open **Exchange System Manager** and click on the + next to **Connectors** to see if you are already using an SMTP Connector.

SBS2003 comes with a pre-configured SMTP Connector as shown below:-



If you need to create a new connector:-
Right-click on **Connectors** and select **New - SMTP Connector...**

If a SMTP Connector already exists, right-click on it and choose **Properties**:-



If you only have one Exchange server, it's unlikely you'll need more than one SMTP Connector. Multiple SMTP Connectors are used to send certain emails via different routes.

The **SMTP Connector - Properties** page opens which has 8 tabs.
(There could be a 9th tab called **Security** if you've previously enabled this tab by a registry change, but, in any case, there's nothing to configure on this tab.)

We'll start on the **General** tab where there are 3 things to configure:-

1 - Name

Call it what you want, but "All Outgoing Email" is a good name.

2 - Smarthosts

Select "**Forward all mail through this connector to the following smart hosts**" and enter Arrowmail's 3 Smarthosts, separated by semicolons.

The full string to enter is:-

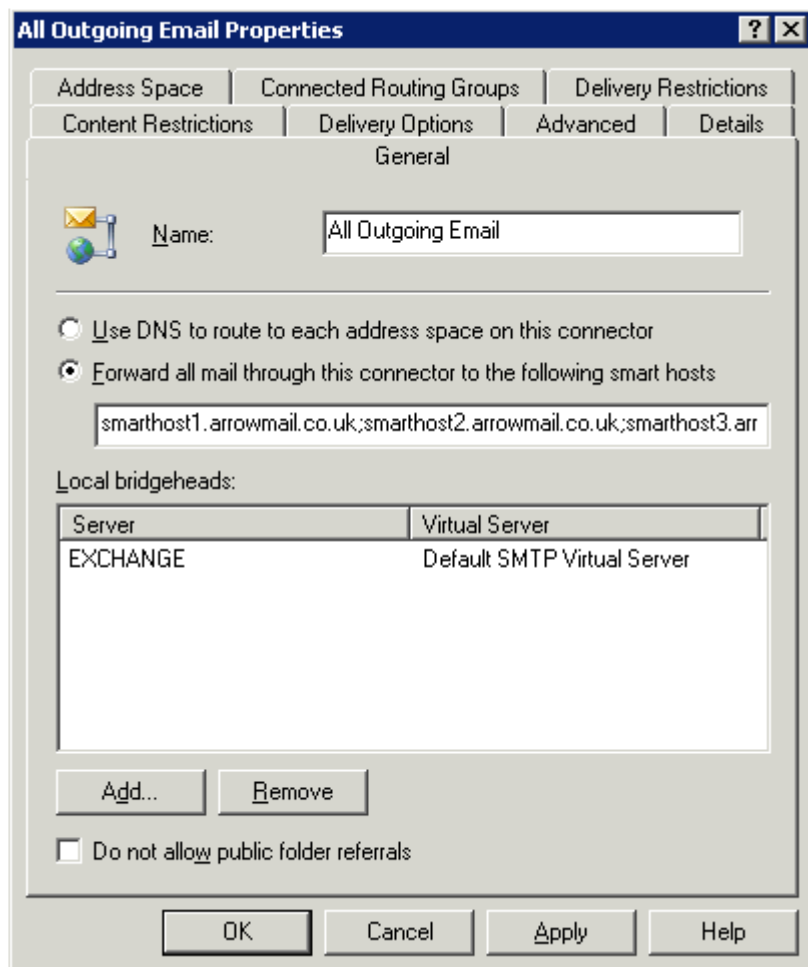
smarthost1.arrowmail.co.uk;smarthost2.arrowmail.co.uk;smarthost3.arrowmail.co.uk

"Copy and Paste" the above line into your SMTP Connector if you like.

3 - Bridgehead Server

This is your Exchange server.

Click **Add...** and there will only be one option.



If you're editing an existing SMTP Connector, it will already have a name which can't be changed here. If you want to rename the connector, close this page, right-click on the **SMTP Connector** and choose **Rename**.

Go to the **Address Space** tab.

Click **Add...** and select the default options which are:-

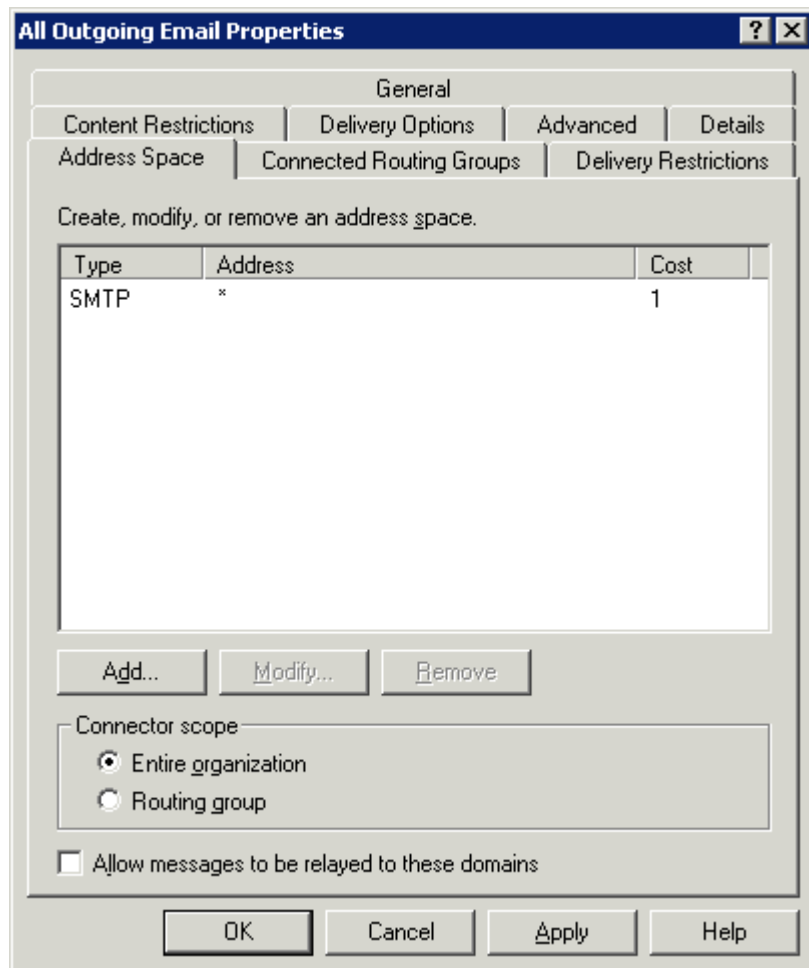
Type = SMTP

Email Domain = *

Cost = 1

Connector scope = Entire Organisation

"**Allow messages to be relayed to these domains**" is not selected



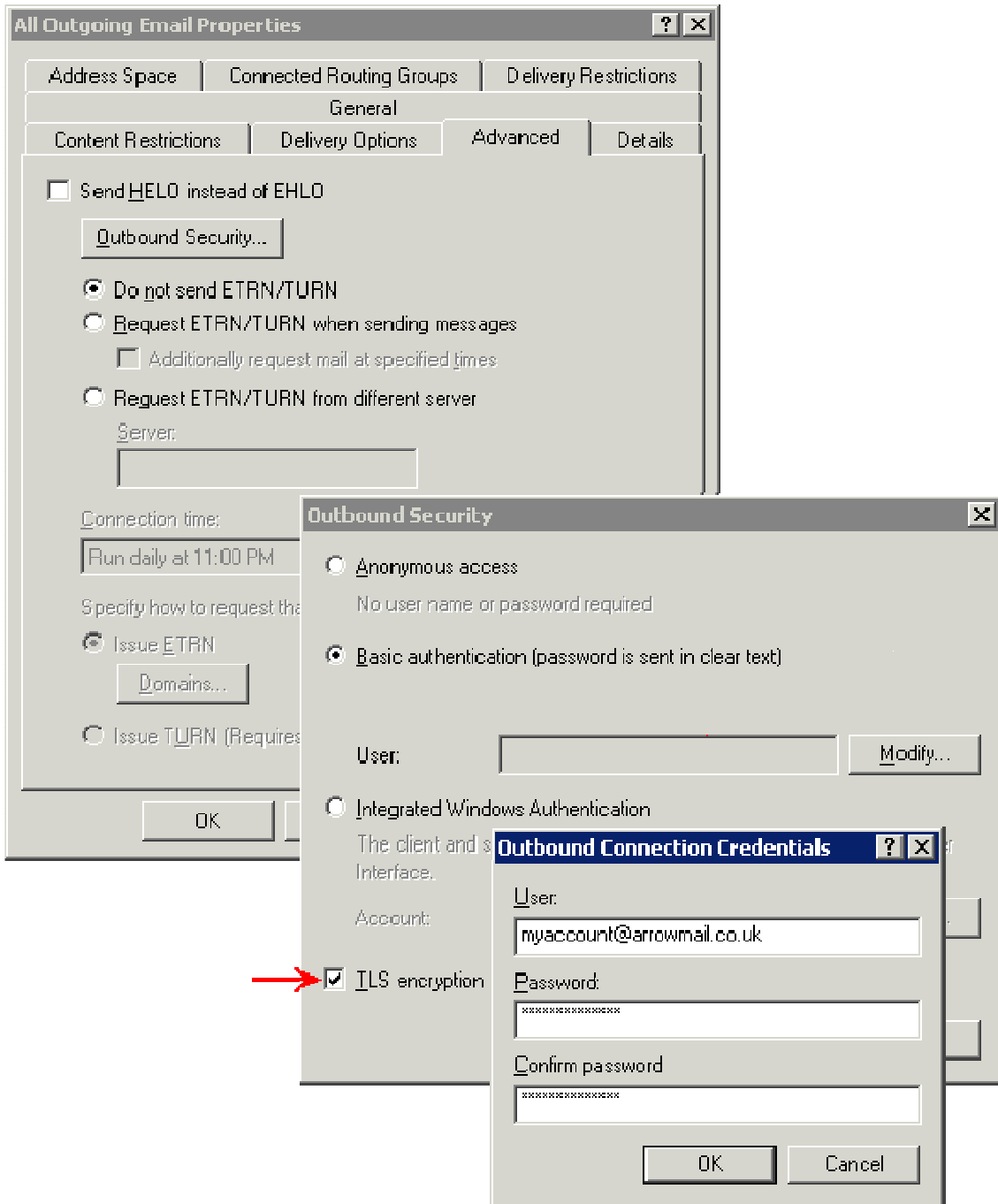
Go to the **Advanced** tab.

Click on **Outbound Security...**

Select **Basic authentication (password is sent in clear text)** and then **Modify...**

Enter your username and password for the Arrowmail Smarthosts.

If you would like all messages, sent from your server to our Smarthosts, to be encrypted then select **TLS encryption**:-

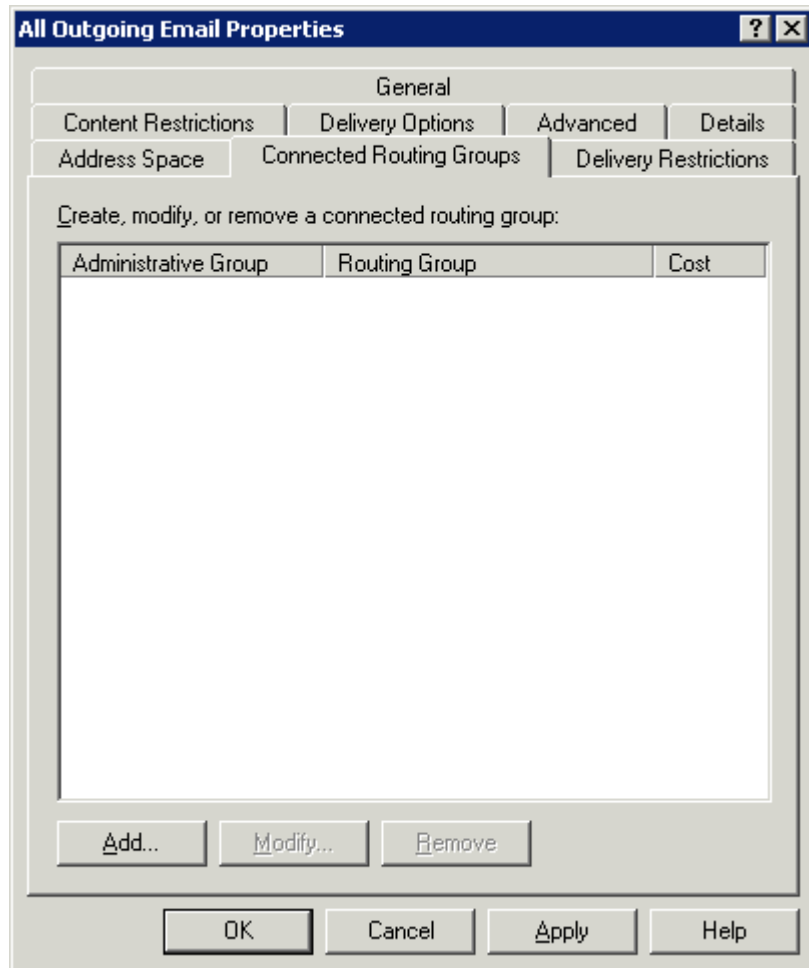


The Arrowmail Smarthosts **require** authentication and support TLS encryption.

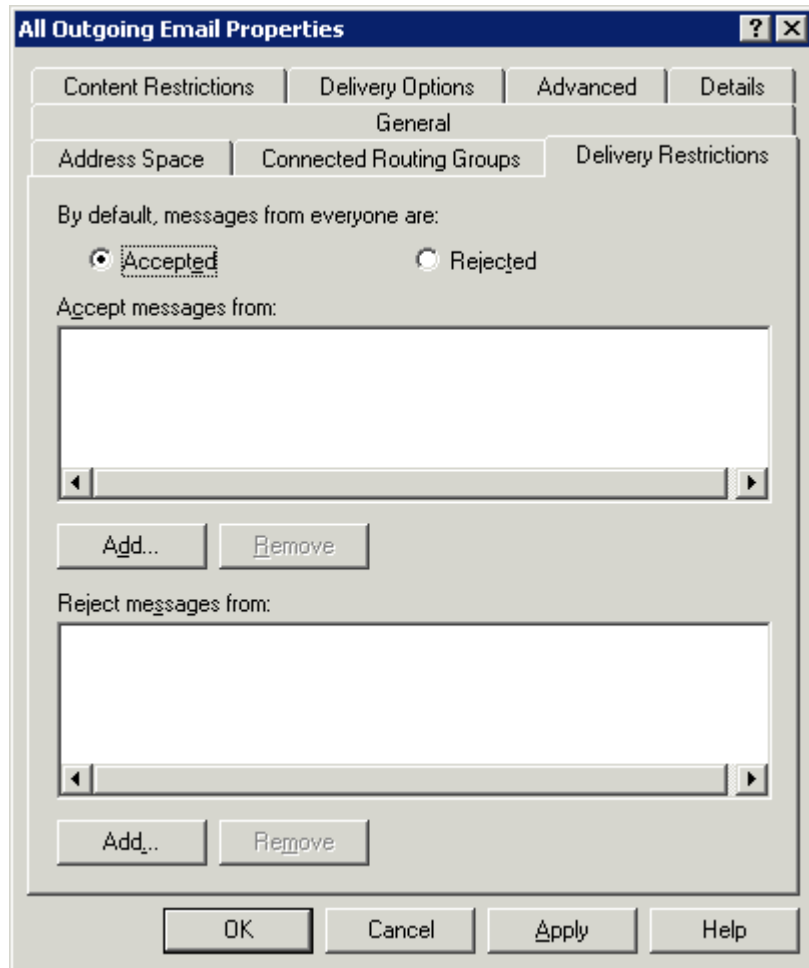
We will issue you with your own username and password which will be the same for **all** 3 of our Smarthosts.

There's nothing to change on the other 5 tabs, but we've shown what they should look like, anyway, so you can check that nothing's been changed.

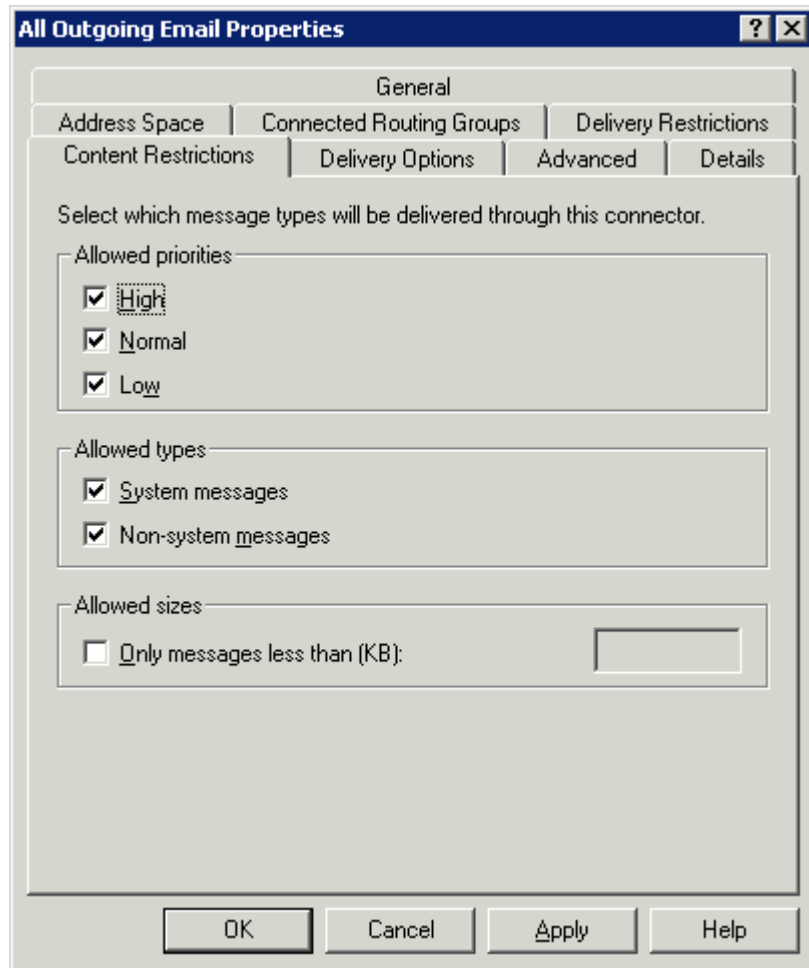
The **Connected Routing Groups** tab:-



The **Delivery Restrictions** tab:-



The **Content Restrictions** tab:-



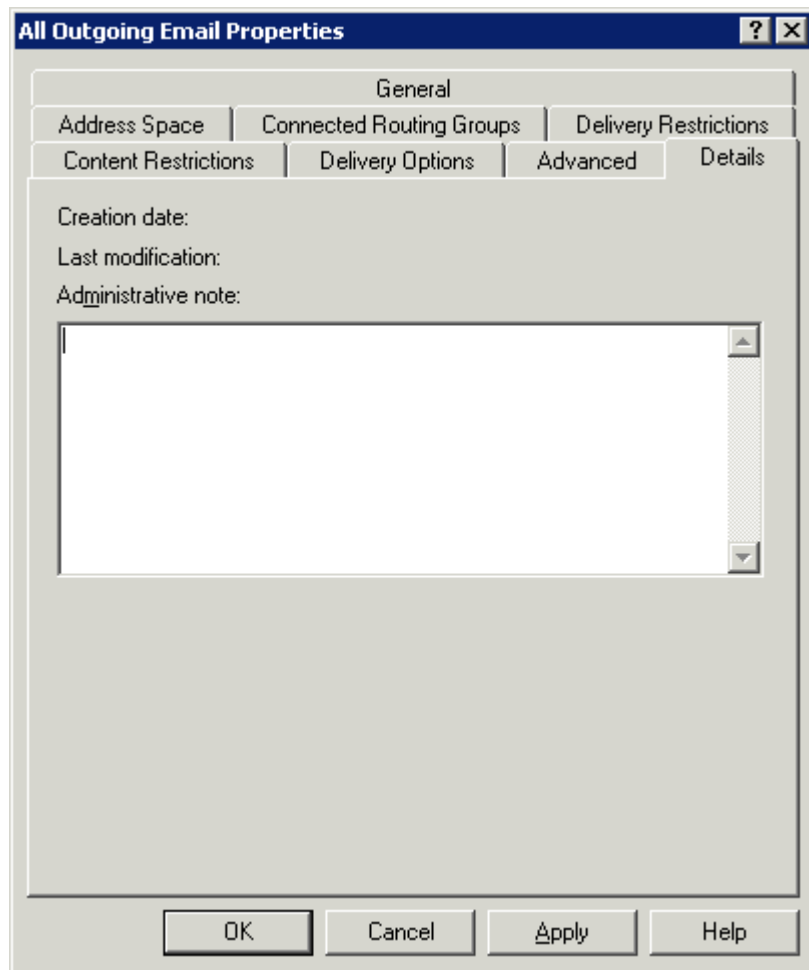
The **Delivery Options** tab:-

The screenshot shows the 'All Outgoing Email Properties' dialog box with the 'Delivery Options' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are several tabs: 'General', 'Address Space', 'Connected Routing Groups', 'Delivery Restrictions', 'Content Restrictions', 'Delivery Options' (selected), 'Advanced', and 'Details'. The 'Delivery Options' tab contains the following settings:

- Specify when messages are sent through this connector:**
 - Connection time: Always run (dropdown menu) [Customize...]
 - Use different delivery times for oversize messages**
 - Oversize messages are greater than (KB): 2000
 - Connection time: Use custom schedule (dropdown menu) [Customize...]
- Queue mail for remote triggered delivery**
 - Accounts authorized to use TURN/ATRN:
 - [Add...]
 - [Remove]

At the bottom of the dialog are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

...and finally, the **Details** tab:-



Click **OK** and close **Exchange System Manager**.

In order for the new settings to take effect, you need to restart the following services:-
Microsoft Exchange Routing Engine and
Simple Mail Transport Protocol (SMTP).

Rebooting the server will also enable the new settings, if this is easier.

How To Configure a Smarthost on Exchange 2007

If your Exchange Server 2007 is currently able to send emails externally, a **Send Connector** must already have been created and configured correctly on the Hub Transport server.

Configuring Exchange 2007 to use the Arrowmail Smarthosts, therefore, just requires you to modify the settings on this Send Connector.

For Exchange 2007, Microsoft has split up into separate roles, the various jobs that Exchange has to perform, with the implication that each role will be handled by a different server.

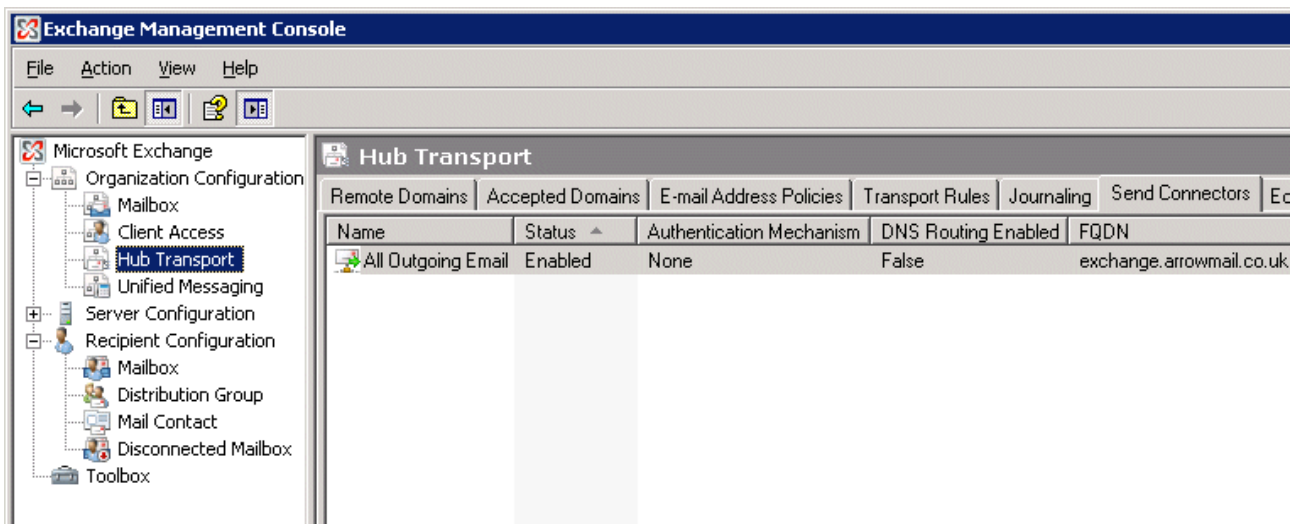
The Hub Transport role is the one responsible for sending and receiving external emails.

In the real world of small to medium sized companies, a *single* Exchange server is likely to be performing *all* the various roles.

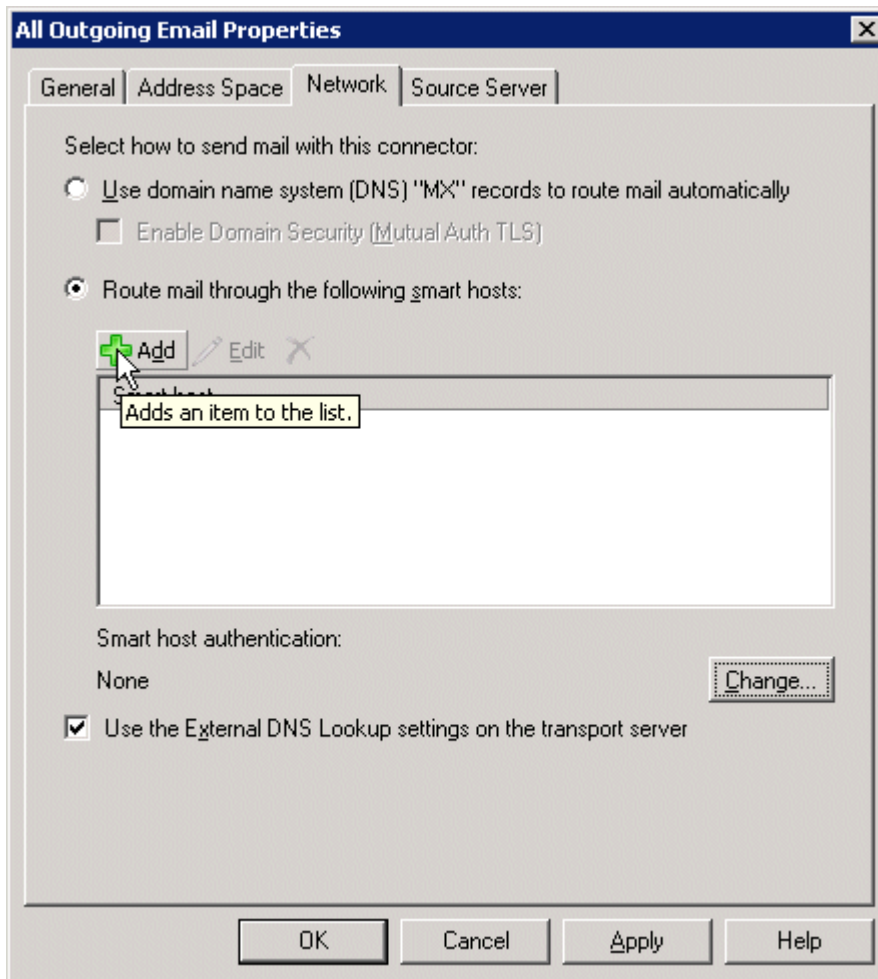
Open Exchange Management Console

Click on the + next to **Organization Configuration**

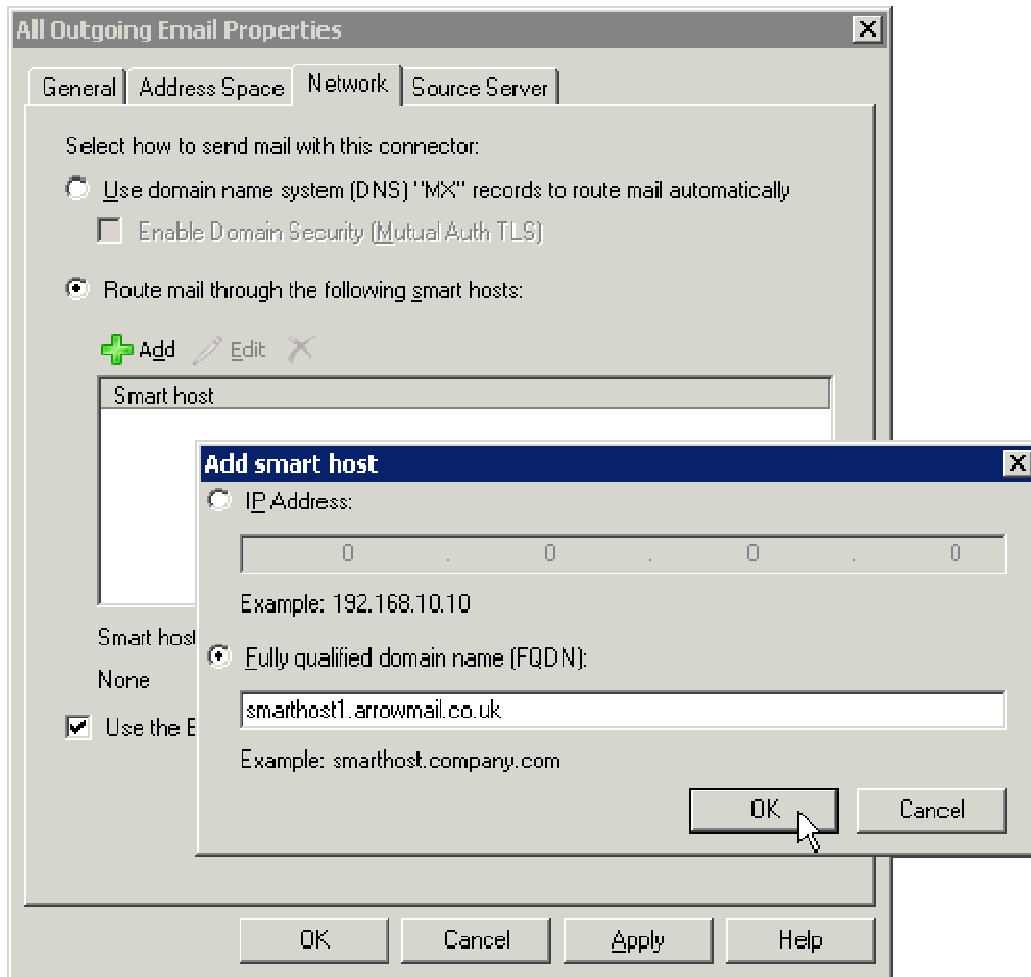
Select **Hub Transport** and select the **Send Connectors** tab:-



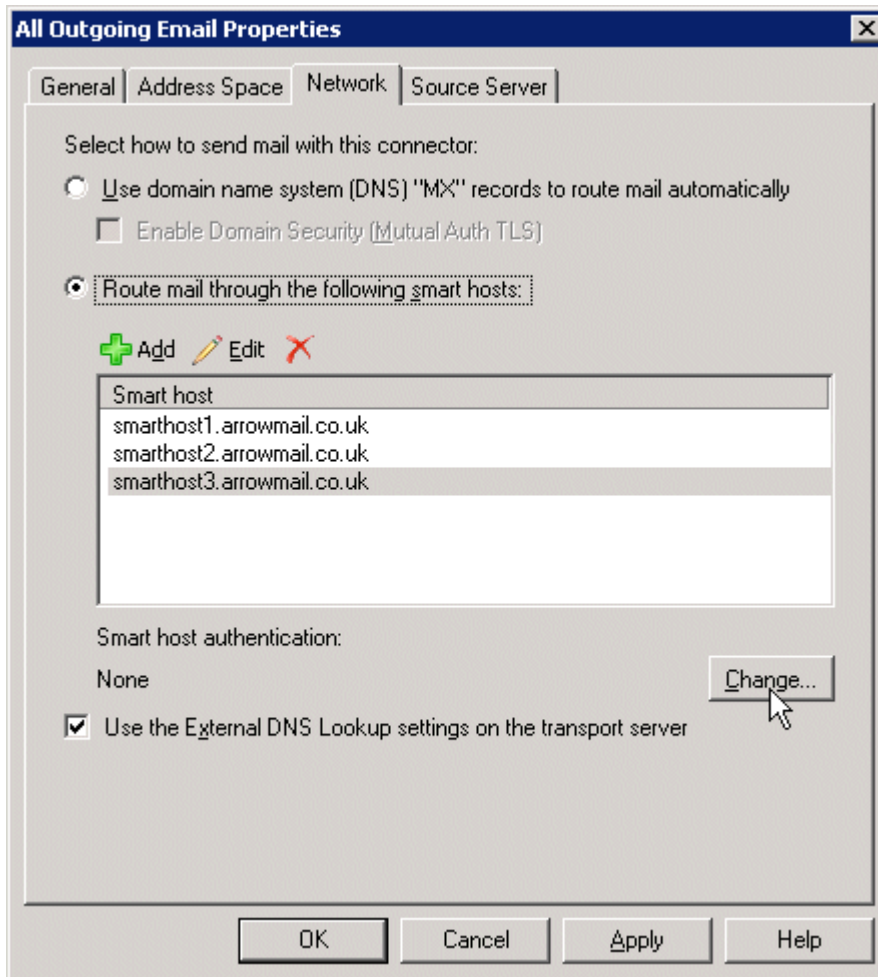
Right-click on the existing **Send Connector**, select **Properties** and go to the **Network** tab. Select "**Route mail through the following smart hosts:**" and click **Add**:-



Specify the first Smarthost as shown below:-



Add all 3 of Arrowmail's Smarthosts:-



Click **Change...** to set the authentication options.

Type the username and password we've issued to you below:-

Configure Smart Host Authentication Settings

None

Basic Authentication

Basic Authentication over TLS

User name:
www@arrowmail.co.uk

Password:
●●●●●●●●●●

Note: all smart hosts must accept the same user name and password.

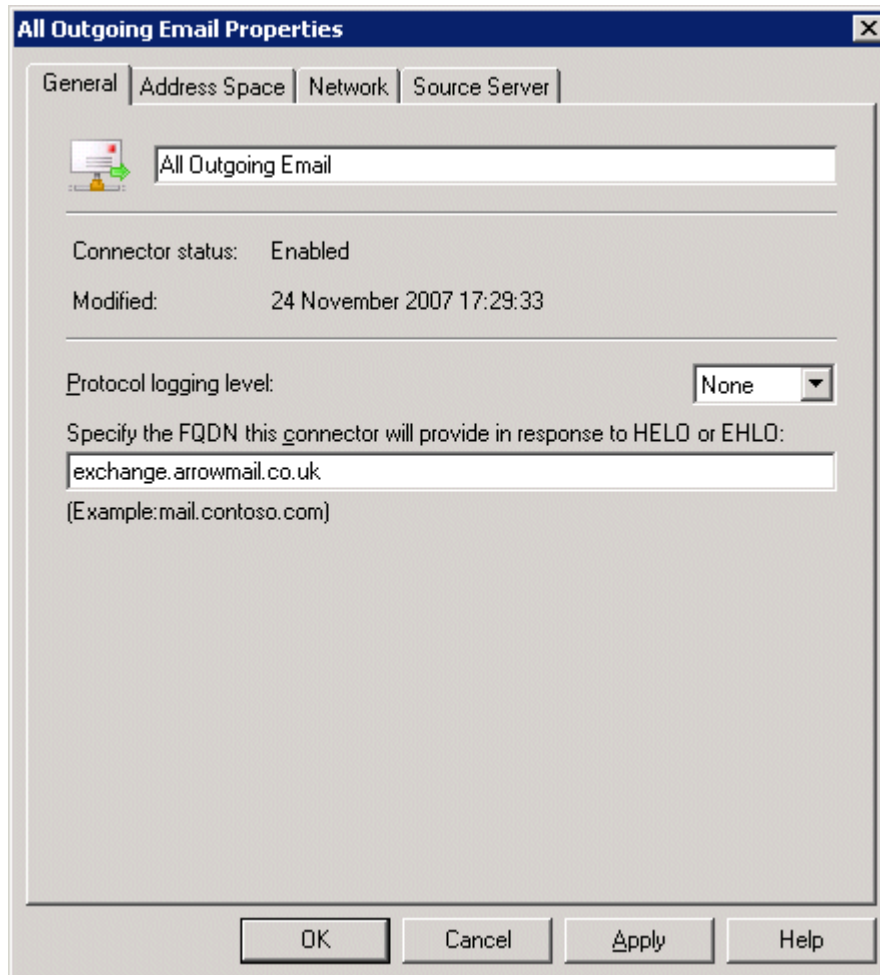
Exchange Server Authentication

Externally Secured (for example, with IPsec).

OK Cancel

There shouldn't be anything that needs changing on the other 3 tabs, but we've shown below, what they should typically look like.

The **General** tab:-

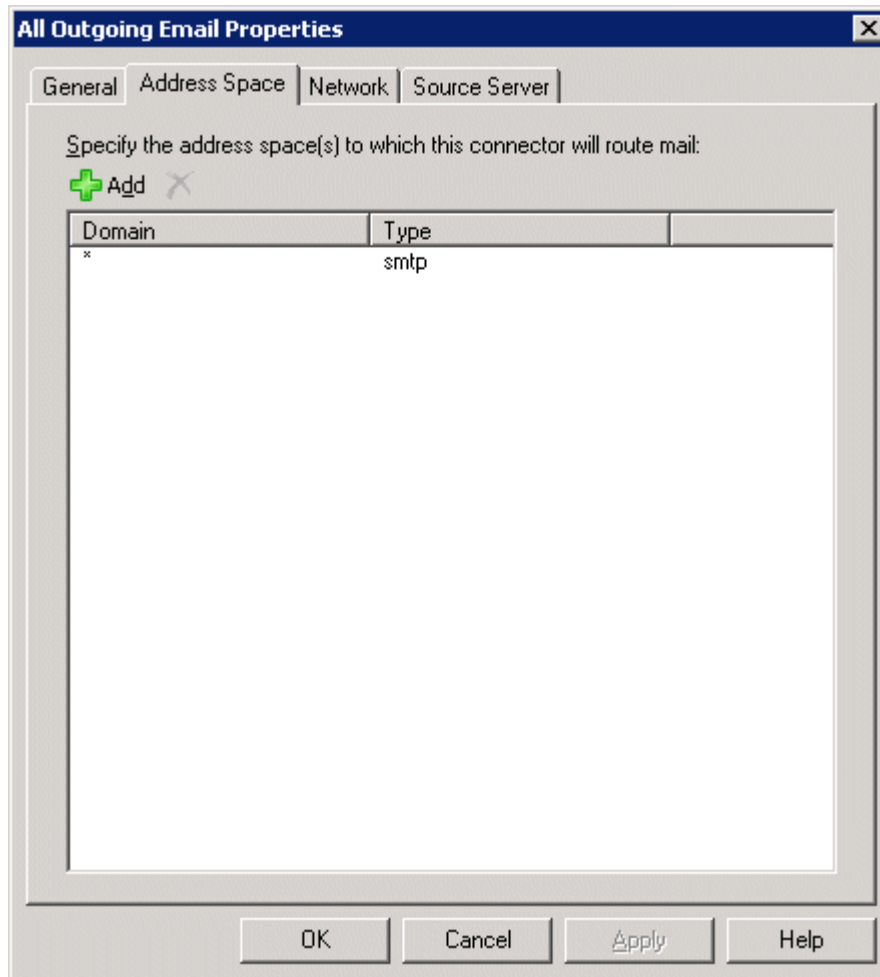


The **Fully Qualified Domain Name (FQDN)** should be the DNS name of the public IP address your server operates behind.

Our Smarthosts don't care what FQDN you enter, but if you're sending email *directly*, without using a Smarthost, it's important to get this entry to match your *actual* FQDN.

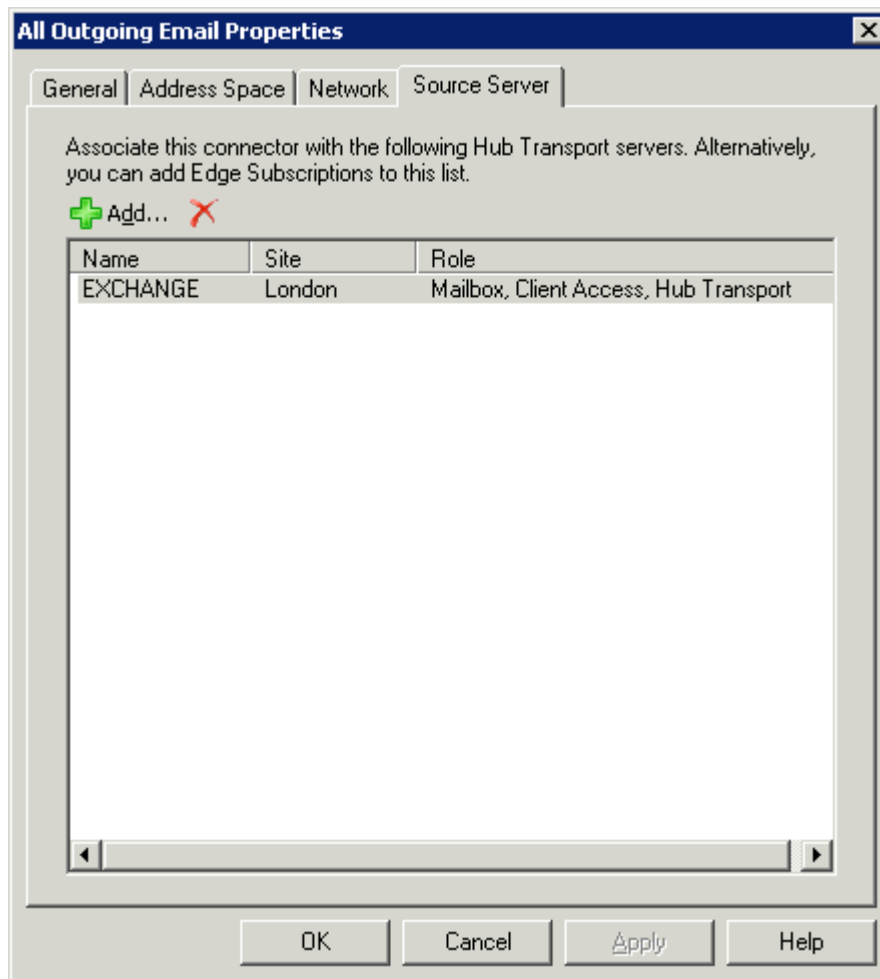
When you need help trouble-shooting Smarthost connection problems, you can change the "**Protocol logging level:**" to **Verbose**.

The **Address Space** tab:-



The asterisk in the **Domain** column indicates that *all* emails will be sent through this Send Connector.

The **Source Server** tab:-



Notice, in the **Role** column, that this server is performing *all* the Exchange 2007 roles.

When you've finished, the Send Connector should look like this:-

Hub Transport						
Remote Domains	Accepted Domains	E-mail Address Policies	Transport Rules	Journaling	Send Connectors	Edge Subscriptions
Name	Status	Authentication Mechanism		DNS Routing Enabled	FQDN	
All Outgoing Email	Enabled	Offer Basic authentication only after starting Transport Layer Security (TLS)		False	exchange.arrowmail.co.uk	

The changes you've made to the **Send Connector** will take effect straight away without you having to reboot the server or restart any services.

What if you don't use Exchange as your in-house Mail-server?

Many mail-server programs, other than Exchange, can take advantage of multiple Smarthosts. However, if the one you're using can only be configured for *one* Smarthost, you should set it to use:-

smarthost.arrowmail.co.uk

We will make sure that this DNS name is always pointing to a functional mail-server.

If your mail-server isn't able to authenticate to our Smarthosts then, as long as you are using a fixed public IP address, we can allow anonymous access from that specific IP address.

Stop your Exchange Server generating emails in response to incoming Spam

Now that you're paying for outgoing emails at something under 0.3p each, it's a good idea to make sure you are not sending out ones you don't need to.

By default, Exchange will accept emails to non-existent users and then generate an outgoing email to each sender, telling them, politely, that their email couldn't be delivered as the user doesn't exist.

Today, spammers often bombard an exchange server with large numbers of emails to addresses that have been guessed - usually wrongly.

Not only is it a waste of your monthly email allowance to reply to these emails but, the sender's address in the original email is likely to have been forged and so your server's reply will go to someone innocent of sending spam, who will now see *you* as spamming *them*.

The technical term for sending an NDR to someone who didn't send you the email is "Backscatter".

It's very simple to enable "Recipient Filtering" so emails to non-existent users are rejected but, for some reason, this configuration step is often missed out by people setting up Exchange.

We had one customer where Backscatter NDRs made up 80% of their total out-going emails.

We don't like them coming through our servers, even though we charge for them, as they mostly can't be delivered and, if they can, it risks annoying the recipient.

If you are about to configure your Exchange server to use our Smarthosts then, do everyone a favour by checking your Recipient Filtering settings.

Step-by-step instructions for configuring Recipient Filtering for Exchange 2003 and 2007 are here:-

<http://www.arrowmail.co.uk/howto/recfilt.aspx>

How to Create a Sender Policy Framework Record to Authorise our Server to send out your Company's Email

It's by no means essential, but if you use our Smarthosts, it can help make email delivery more reliable if you create a special DNS record with whoever is handling the DNS for your domain name, usually your domain registrar.

This DNS record is to comply with the Sender Policy Framework (SPF) anti-spam initiative and it identifies our servers as approved for sending emails from your domain.

It's a TXT record, which not all DNS servers or ISP control panels can handle, but if they can this is the record you need to add:-

mycompany.co.uk. IN TXT "v=spf1 include:arrowmail.co.uk -all"

This is how it should appear in your DNS Zone File, including the inverted commas, but with your domain name substituted for mycompany.co.uk.

If you give us the logon details for your domain registrar's control panel we'll set it up for you. If your current DNS servers can't handle TXT records you could move to DNS servers that can. This doesn't require you to change your domain registrar.

www.nettica.com will host your domain's DNS service, along with TXT records, on their servers forever for a one-off payment of US\$40.

You can check that your SPF record has been successfully setup by sending an email to:-

check-auth@verifier.port25.com

Make sure that the **From** address you use is covered by the SPF record, no need to put anything in the Subject Line or the body of the email.

You should receive a reply containing something like the extract shown on the next page. This system also checks out any other anti-spam initiatives such as DomainKeys, DKIM, and Sender-ID.

The SPF system has not yet been adopted widely enough to be a reliable method for identifying spam but, when sending emails, it can tip the balance your favour, especially with heavy-handed anti-spam systems.

From: auth-results@verifier.port25.com
 To: prvs=18523fa5a3=info@arrowmail.co.uk
 Cc:
 Subject: Authentication Report

Sent: Wed 28/11/2007 16:13

This message is an automatic response from Port25's authentication verifier service at verifier.port25.com. The service allows email senders to perform a simple check of various sender authentication mechanisms. It is provided free of charge, in the hope that it is useful to the email community. While it is not officially supported, we welcome any feedback you may have at <verifier-feedback@port25.com>.

Thank you for using the verifier,

The Port25 Solutions, Inc. team

=====
 Summary of Results
 =====

SPF check: pass
 DomainKeys check: pass
 DKIM check: pass
 Sender-ID check: pass
 SpamAssassin check: ham

=====
 Details:
 =====

HELO hostname: mail1.arrowmail.co.uk
 Source IP: 83.245.15.239
 mail-from: prvs=18523fa5a3=info@arrowmail.co.uk

 SPF check details:

Result: pass
 ID(s) verified: smtp.mail=prvs=18523fa5a3=info@arrowmail.co.uk
 DNS record(s):
 arrowmail.co.uk. 3600 IN TXT "v=spf1 mx -all"
 arrowmail.co.uk. 3600 IN MX 30 mail3.arrowmail.co.uk.
 arrowmail.co.uk. 3600 IN MX 10 mail1.arrowmail.co.uk.
 arrowmail.co.uk. 3600 IN MX 20 mail2.arrowmail.co.uk.
 mail3.arrowmail.co.uk. 3600 IN A 217.45.193.165
 mail1.arrowmail.co.uk. 3600 IN A 83.245.15.239

 DomainKeys check details:

Result: pass
 ID(s) verified: header.From=info@arrowmail.co.uk DNS record(s):
 MDAemon._domainkey.arrowmail.co.uk. 3600 IN TXT "t=y; k=rsa;
 p=MIGfMA0GCQSqS1b3DQEB&QUAA4GNADCB1QKBgQDOzHZAGzUkKv4QIcV6DT09qF+R7O3fW5V/ncTWC
 Oj58TbYdsdneM5yGDKV8mq4VK/xyW18K3RdZOS09wcV+IV95hQkB+mTiBAN55
 +pLi5gt24vjR46s58wizIi9YiOY/jnX551iXuCL9POvr6q8ij05egq7BU6NjNAKf01BGHmGwIDAQAB"

 DKIM check details:

Result: pass
 ID(s) verified: header.From=info@arrowmail.co.uk Canonicalized Headers:
 domainkey-signature:a=rsa-
 sha1;'20's=MDaemon;'20'd=arrowmail.co.uk;'20'c=simple;'20'q=dns;'20'h=message-
 id:from;'20'b=teLr7PB0zZVMYooKyYQUdVNBBUaq3Opb+A0eV9MUG78C5ihKZutOTfh7nF2S'20'B
 /elynd+zreZk71nUojwAb331b1Vixh140i6v//fhV1C5v6MPP3yQ/MoS'20'f1SItcbNyW5TT7rkInN
 1RxUyq2aQjNtxM2Tkc3SGT1pR58EEH3aA9c='OD' 'OA'

 Sender-ID check details:

Result: pass
 ID(s) verified: header.From=info@arrowmail.co.uk DNS record(s):
 arrowmail.co.uk. 3600 IN TXT "v=spf1 mx -all"
 arrowmail.co.uk. 3600 IN MX 30 mail3.arrowmail.co.uk.
 arrowmail.co.uk. 3600 IN MX 10 mail1.arrowmail.co.uk.
 arrowmail.co.uk. 3600 IN MX 20 mail2.arrowmail.co.uk.
 mail3.arrowmail.co.uk. 3600 IN A 217.45.193.165
 mail1.arrowmail.co.uk. 3600 IN A 83.245.15.239

What Makes Our Smarthost so Smart?

How come we can get emails delivered successfully when your in-house server can't?

- We have the DNS records for our servers setup properly.
For our main Smarthost, which is called **mail1.arrowmail.co.uk**, this means:-

mail1.arrowmail.co.uk $\xrightarrow[\text{Lookup}]{\text{DNS}}$ **SmartHost's IP Address**

SmartHost's IP Address $\xrightarrow[\text{Lookup}]{\text{Reverse DNS}}$ **mail1.arrowmail.co.uk**

It's often not possible to do this with the IP address you get with a Broadband connection, even if it's a static IP address.

- We have extra DNS records setup to comply with anti-spam initiatives such as SPF and DKIM. Many domain registrars don't yet permit these types of DNS records.
- Some email services block connections from *any* IP address used for Broadband or dial-up connections.
Some mail-server blacklisting services include in their list, whole ranges of addresses in response to complaints about just one address in the range.
The IP addresses we use are reserved for Internet servers.
If we find that any company is blocking emails from our servers we contact them to request that we be whitelisted.
- If we experience problems delivering emails to certain email addresses we route them via other Smarthost partners services in different countries.
- We keep trying to send emails that don't get through straightaway in case the receiving mail-server is having temporary problems.
We try every minute for the first hour then send you back a warning - it often transpires that you've made an error in the email address.
We continue to try to send the email, once an hour, for the next 5 days before finally sending you a "we've given up" message.