Subscription Procedure to

Email Filtering
&
Managed Messaging Services

VERSION 3.8

Introduction

This document describes the different steps required for initializing the processing of your messages by the **Email Filtering Service**. You have subscribed to the **Email Filtering Service** and signed up on-line to enjoy this service and get an access to the online administration console.

The service will be fully operative after you have completed the following steps:

1. Modify the MX records in the Internet DNS of your company's domain so that incoming messages are processed by the **Email Filtering Service**;
2. Optional, restrict connections to your messaging server so that emails sent and received by your company must pass through the **Email Filtering Service**;
3. Optional, modify the configuration of the SMTP relay of your messaging server so that your outgoing emails are processed by the **Email Filtering Service**;
4. Optional, if you subscribed to the **Managed Messaging Service**, you just have to create and manage your Mailboxes (see the Managed Messaging Service Guide).

The rest of this document describes these steps in details. If you need help, feel free to contact the technical support team of the **Email Filtering Service** or your reseller.

Step 0: Preliminary subscription to the Email Filtering Service

You filled in the registration form (available on-line). Once you have submitted this form, a member of our technical staff will get in touch with you to create an account on the administration system of the **Email Filtering Service** with a default configuration corresponding to your wishes. He will also make sure the technical information you gave is correct.

Now that your account has been created you can access the administration console from the Web site **https://www.security-mail.net**

You should save this URL in your bookmarks to get a quick access to the administration console homepage.

Step 1: Modifying the MX records in the DNS of your company's domain

The protocol routing emails on the Internet uses information in your DNS: the MX records. They are sorted according to their preference value from the lowest to the highest. Record with the **lowest value** is generally your messaging server while **higher values** correspond to your ISP **mail relays**. If your server is not responding, your messages will be received thanks to those relays as long as your servers are unavailable. We are going to use this property and assign the lowest value to the **Email Filtering Service** to give him priority with regards to receiving emails. After having processed your messages, the **Email Filtering Service** will send them to your messaging server.

This is usually done by the person managing your DNS – most of the times your Internet service provider (ISP). You need to send this person a request for change. An example of such a request, which you can print on headed notepaper and send to the person in charge of your DNS, is included in the appendices. It usually takes several hours to propagate the changes throughout the Internet, but you will receive your first secure messages right after the modification.

Here is an example; the DNS table extract shows the MX records of the domain "company.com":

company.com. IN MX 5 mailgate.company.com.
company.com. IN MX 40 smtp.isp.net.
company.com. IN MX 40 secours.isp.net.

mailgate.company.com is the domain messaging server (value = 5).
smtp.isp.net and **secours.isp.net** are SMTP relays (value = 40).
According to this table if the message cannot be sent to mailgate.company.com, for whatever reason, it will be routed towards one of the SMTP relays with a preferential value of 40. These hosts will then try on a regular basis to send the email to a host with a lower preferential value: the messaging server mailgate.company.com.

To analyze and filter messages before they reach the mailgate.company.com server, we set the preferential values of the **Email Filtering Service** servers as follows:

company.com. IN MX 3 france.security-mail.net.
company.com. IN MX 4 europe.security-mail.net.
company.com. IN MX 5 asia.security-mail.net.

You should give the priority to relays corresponding to your geographical area.

Step 2 (Optional): Restricting connections to your messaging server

Because of the way the Internet messaging protocols operate the only modification of the MX records does not assure you that your servers will only receive messages from our servers. To make sure only secure messages are received, we suggest you restrict email delivery to messages coming from the servers of the **Email Filtering Service** only. This will strengthen your messaging server security by hiding it.

Do not hesitate to contact the technical support of the **Email Filtering Service** or your reseller, to confirm the IP addresses to be typed.

You can set up this restriction at the level of your company firewall by implementing safety rules authorizing only the **Email Filtering Service** servers to interact with your server using SMTP.

You can also use the security features of your messaging server (if you use MS Exchange 5.5, you can do it via Accept Connections|Specify by Host…on the configuration screen of the Internet mail connector).

Step 3 (optional): Modifying the SMTP relay configuration of your messaging server

Follow this step if you wish to filter your outgoing messages, from your server to the outside world.

Emails sent by your company must be routed by the **Email Filtering Service**. Procedures vary according to the messaging servers and SMTP gateways of your organization.

You first need to find the last of your organization servers through which your emails pass before being sent across the Internet: usually, your messaging server. It usually routes emails directly towards the destination SMTP server checking the address in the DNS MX records. It can also route messages to an SMTP relay of your Internet service provider.

The **Email Filtering Service** will act as an SMTP relay; it receives the emails sent by your organization at the address: **smtp.security-mail.net**

Do not use IP address instead of names because IP addresses can change without advance notice.

You will have to change the configuration of your last server or SMTP gateway so that emails are routed towards the **Email Filtering Service.** Before this, we advise you to check that none of the intermediary firewalls (which could be present) prevent connections to this address. On your server, type command:

telnet france.security-mail.net 25

You should see something similar to this:

220 E-securemail 3.0 ESMTP running on ……

*(To exit from telnet type **quit)***

If this is the case, you can now change the configuration of your SMTP relay. For MS Exchange and Lotus Notes, procedures are detailed in the appendices. Once you have changed your SMTP relay configuration, make sure emails sent via the **Email Filtering Service** are correctly delivered. To do so, send a message to an autoresponder, for instance **ping@oleane.net**. Your email will be echoed and you will get the answer in your mailbox within a few minutes.

You can now proceed to the next step which consists in routing messages received via the **Email Filtering Service**.

Glossary

DNS
The DNS or Domain Name System is a distributed database used on the Internet and private networks to associate names with addresses.

A-records of the DNS
A-records ("address records") are entries in the DNS that map names to IP addresses. There can be several A-records for a single name so that it corresponds to several IP addresses.

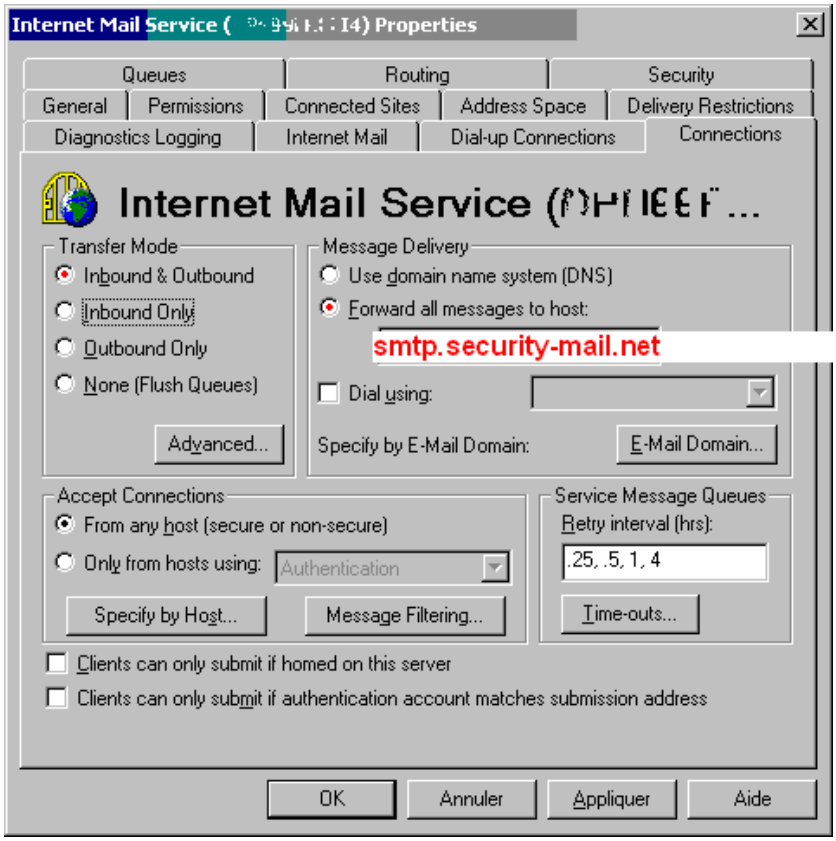
MX-records of the DNS
MX records ("Mail exchanger records") are entries in the DNS that set the part of a specific domain messages will be routed to. For instance, messages sent to company.co.uk must be routed to the host inrelkay1.e-scan.net before being delivered to the company. If this is not possible, messages are routed to a backup host for later delivery via the wished host. MX records specify how messages must be routed by SMTP servers. Most of the very small businesses store their MX records in the DNS of their Internet service provider. Big companies usually operate their own DNS and, thus, have a more direct control over their MX records.

ISP
Your Internet service provider is the company providing you an access to the Internet. It is usually a leased line or a dial-up access. In addition to supplying the Internet access, ISP often hosts your company's DNS.

SMTP
The Simple Mail Transfer Protocol defines how emails should be formatted and routed from one messaging server to another across the Internet.

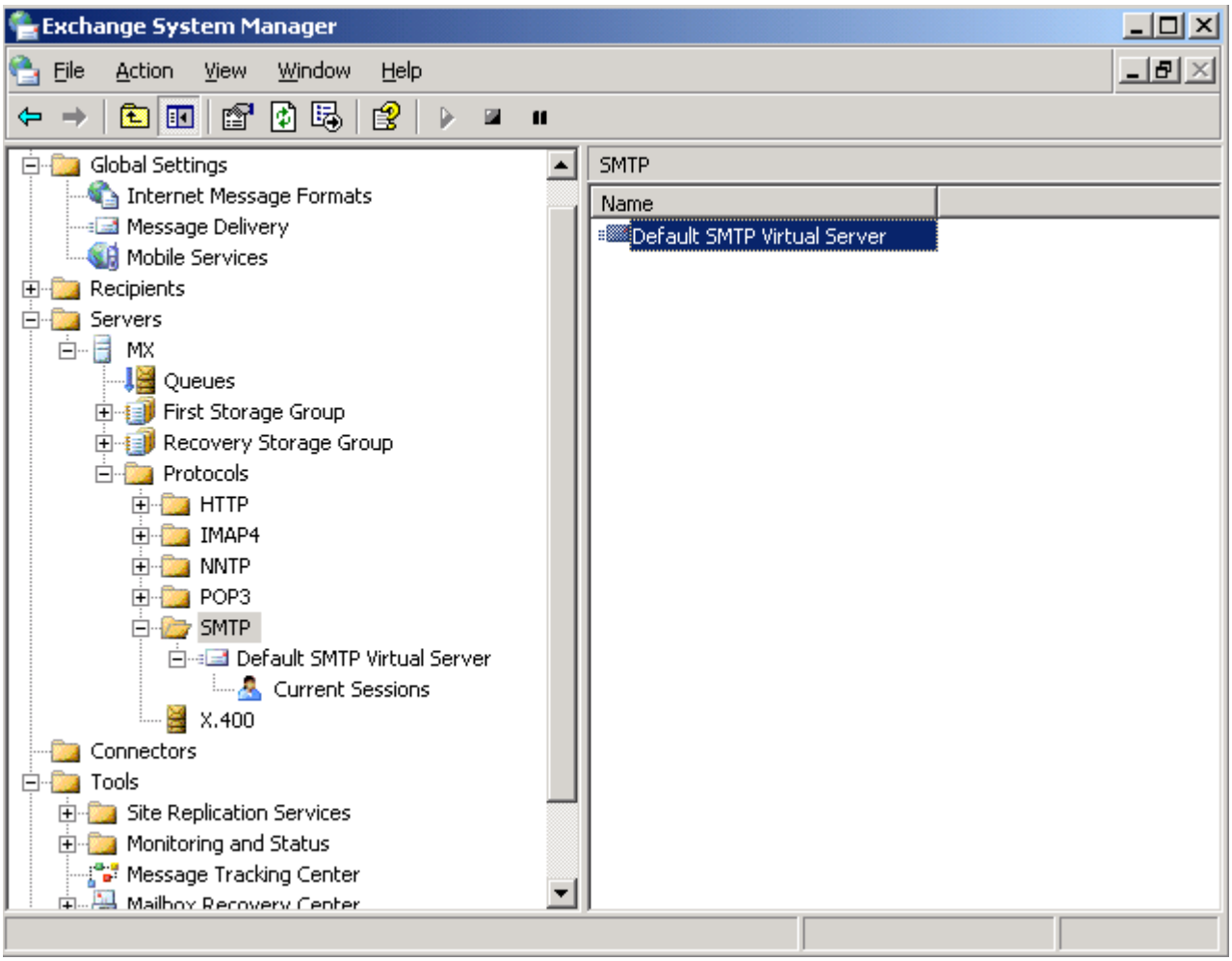
Configuring your MS Exchange Server 5.5

On the Microsoft Exchange administrator program open the configuration screen of the Internet mail connector in:
Organisation\Site\Configuration\Connections\Internet Mail Service (Server). Select the tab "**Connections**", following screen will appear (screen shot from MS Exchanges 5.5):
Choose **Forward all messages to host** and type the address of the mail relay **smtp.security-mail.net** in the text box. Click “Apply” and then “OK” to save the configuration. You will then be asked to restart the Internet messaging system. This can be done thanks to the **Control Panel Services** applet.

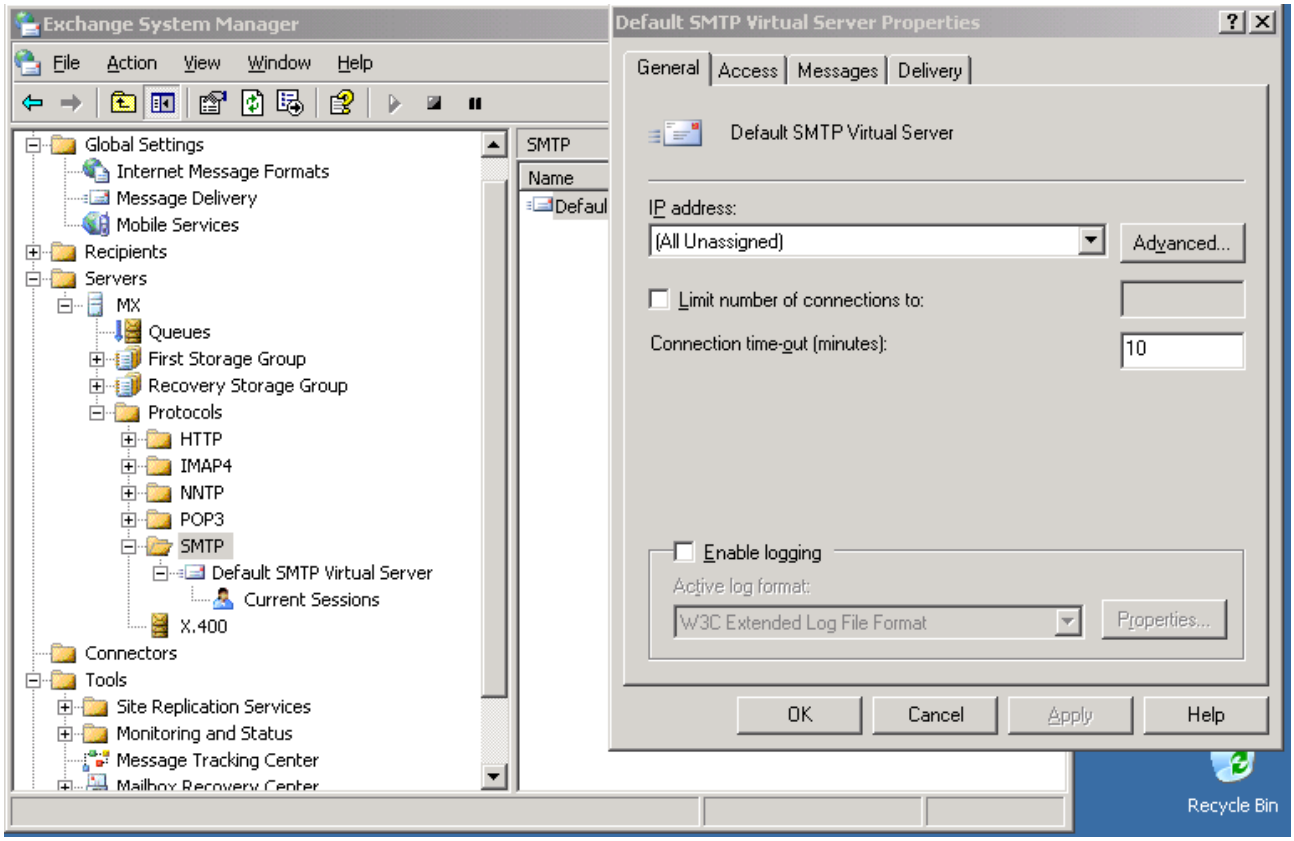


Configuring your MS Exchanges Server 2003

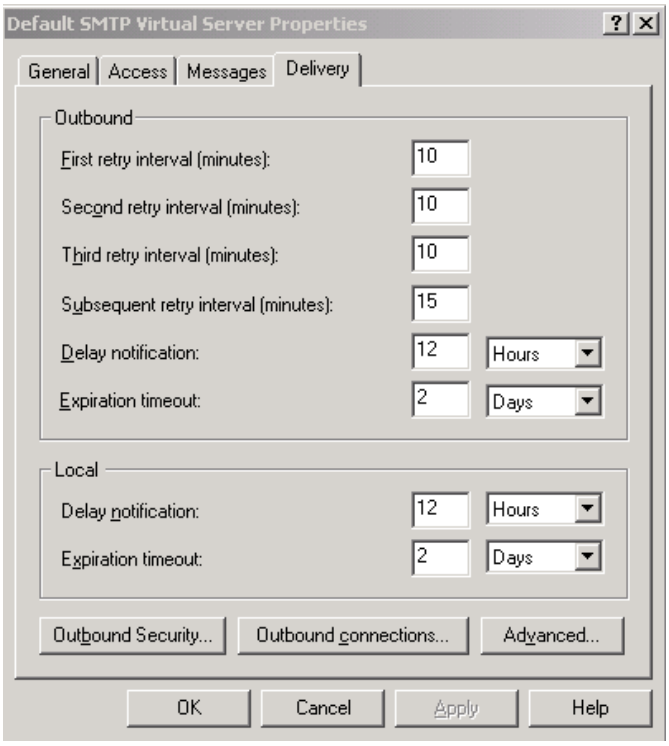
On the Microsoft Exchange administrator program open the configuration screen of the Internet mail connector in:
Servers\MX\Protocols\SMTP\Default SMTP Virtual Server:



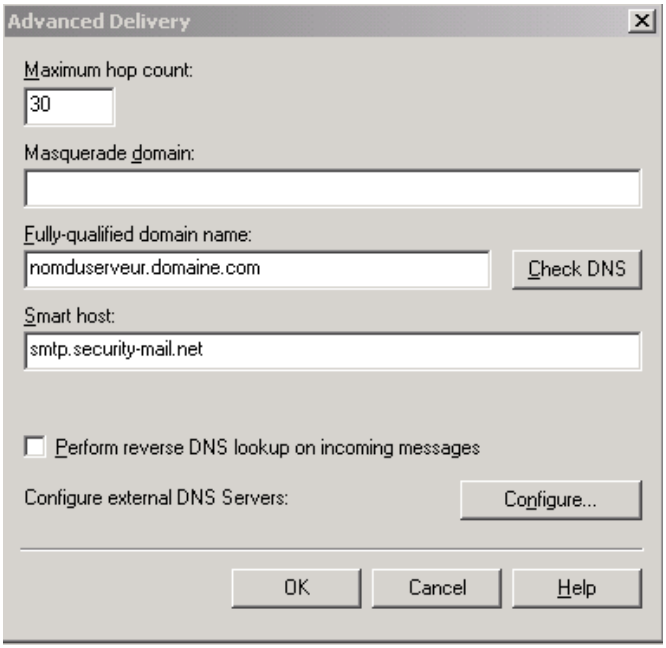
Right click on “Default SMTP Virtual Server” then select "**properties**":



Now, go to “**Delivery**”

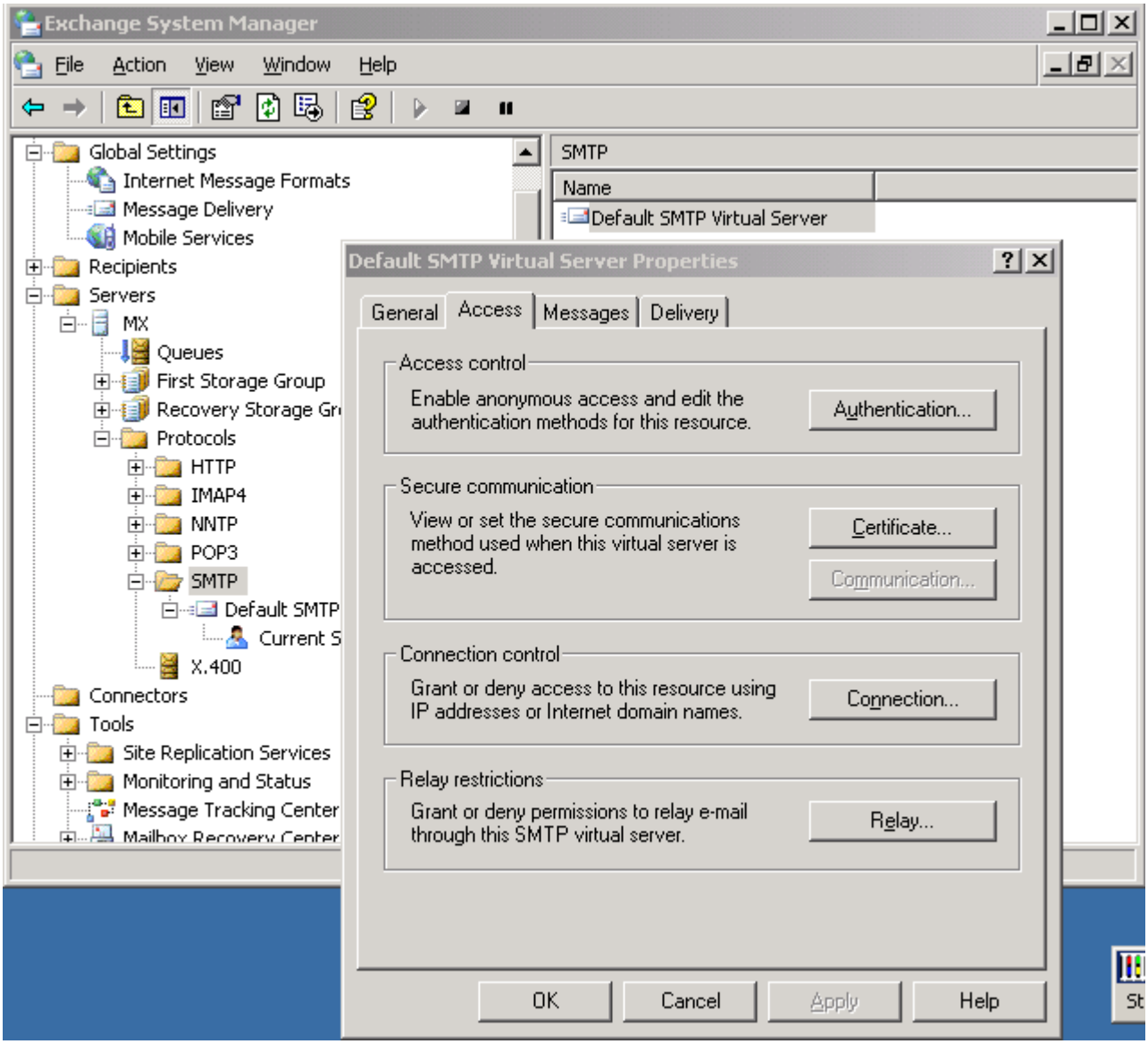


Then, click “Advanced” and fill text boxes with appropriate data. To use our SMTP servers to send emails type the address of the mail relay **smtp.security-mail.net** in the "**Smart Host**" text box. Click “OK” to save configuration. You will then be asked to restart the Internet messaging system. This can be done thanks to the **Control Panel Services** applet.

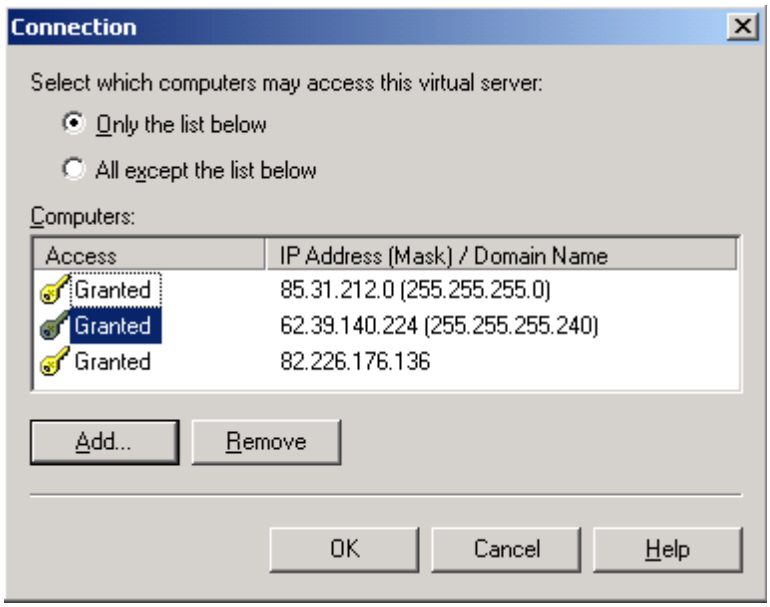


Authorizing only the "Security-mail.net" servers to access your domain

Select the tab "Access"



Click "**Connection**", then authorize only the “security-mail.net” servers to send you e-mails.



Do not hesitate to contact the technical support of the **Email Filtering Service** or your reseller, to confirm the IP addresses to be typed above.

Configuring your Lotus Notes Server

Open the **configuration screen** of the SMTP messaging system, in the Public Address Book of the server. Change the configuration of the SMTP connection; the dialog box looks like the following screen (this screen shot is from Lotus Notes 5):

Type the address of the mail relay **smtp.security-mail.net** in the "**Relay host**" field. Save configuration. You should now restart SMTP connection.

Standard Letter to the Attention of your DNS Operator

<Your company>
<First name>
<Surname>

<place and date>

DNS management service
<Operator>
<Address>
<fax>

You are currently hosting our domain < your domain >.....……..…….....
Our messages will now be filtered by the company …….....
the main servers of which are called **france.security-mail.net** and secondary servers **europe.security-mail.net**.

Would you, please, modify the existing MX records and replace them by the following ones? Could you also give these MX records the highest priorities, so that messages sent to the domain ..... are received by these servers?

france.security-mail.net

europe.security-mail.net

asia.security-mail.net

We look forward to hearing from you.

Checking your Domain MX Records

Follow the procedure below to see the MX records of your company's DNS. Use a computer with Windows NT or Unix and which has access to the public DNS.

Type the command-line:

nslookup

Now, type the command:

set type=MX

Then, type your domain name and press Return. Once you are done, type "exit" to terminate program. In the example below, this procedure will return results similar to the followings:

C:\>nslookup
Default Name Server: res1.dns.uk.isp.net
Address: 154.32.105.18
> set type=MX
> company.com.
Name Server: res1.dns.uk.isp.net
Address: 154.32.105.18
Answer from not allowed source:
company.com preference = 40, mail exchanger = relay1.isp.net
company.com preference = 40, mail exchanger = relay2.isp.net
company.com preference = 5, mail exchanger = france.security-mail.net
company.com preference = 10, mail exchanger = europe.security-mail.net
company.com preference = 15, mail exchanger = asia.security-mail.net

You can also find your MX records thanks to the following commands:

company.com nameserver = pri1.dns.uk.isp.net
company.com nameserver = pri2.dns.uk.isp.net
relay1.isp.net internet address = 154.32.111.6
smtp.security-mail.net internet address = 62.39.140.224
relay2.isp.net internet address = 154.32.105.6
> exit
C:\>