Effective spam filtering with SPAMfighter SMTP Anti Spam Server and Merak Mail Server

This whitepaper describes a “best practice” configuration for SMTP Anti Spam Server when used in conjunction with Merak Mail Server from Icewarp.

Versions this document applies to

- SPAMfighter SMTP Anti Spam Server 2.2.0 – 2.3.0
- Merak Mail Server 8.5.0-9

Assumptions

- SPAMfighter SMTP Anti Spam Server will be installed on the same computer running Merak Mail Server. (If this is not the case, you may still make use of some parts of this document.)
- You have administrative permissions on that computer.
- The computer is using a private, static IP address (not DHCP assigned) and port 25 is being forwarded to it from a public IP address using some router, firewall or gateway device. (If this is not the case, you may still make use of some parts of this document.) You have access to the router’s configuration or can have it reconfigured.
- Incoming mail from the internet is received using the SMTP protocol, not downloaded with ETRN or POP3 (the default).

Conventions

- When asked to “select” or “activate” a button, menu item or list entry, this can usually be done by either clicking the object using a mouse or other pointing device or by pressing the TAB key until the object in question is highlighted followed by pressing the space bar.
- *Italic text like this paragraph requires special attention.*
- `Text in mono-space font like this paragraph illustrates commands or other text that should be entered into an application.`

Table of Contents

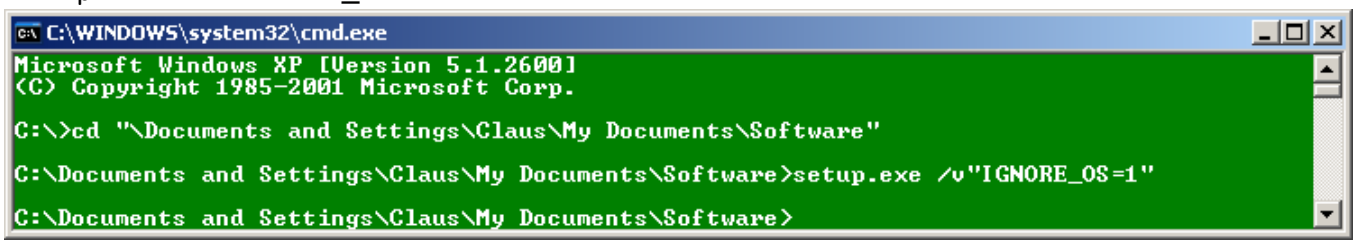
Installing SMTP Anti Spam Server

Installing SMTP Anti Spam Server won't interfere with your current setup. The product does not bind to (listen on) any port until configuration is completed. A reboot is not required by the application itself; however if your computer is missing a Service Pack or the Microsoft .NET Framework 2.0 Runtime, these components might require a reboot.

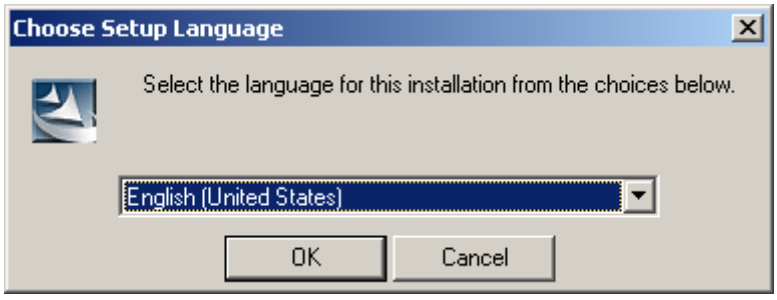
1) Log on to the computer using an Administrator account.

2) Download the latest version of SMTP Anti Spam Server here:
http://www.spamfighter.com/SMTP_Install.asp

3) *If you are running Windows 2000:*
- Make sure that the computer has Service Pack 3 or later installed. If you are unsure, visit Windows Update and install all critical and recommended updates first by clicking here:
http://windowsupdate.microsoft.com/
- Double-click the downloaded file setup.exe to install SMTP Anti Spam Server.
If you are running Windows Server 2003:
- Double-click the downloaded file (setup.exe) to install SMTP Anti Spam Server.
If you are running Windows XP:
- Open a command prompt and navigate to the download directory using the "cd" command, then enter the following command and press Enter/Return:
`setup.exe /v"IGNORE_OS=1"`

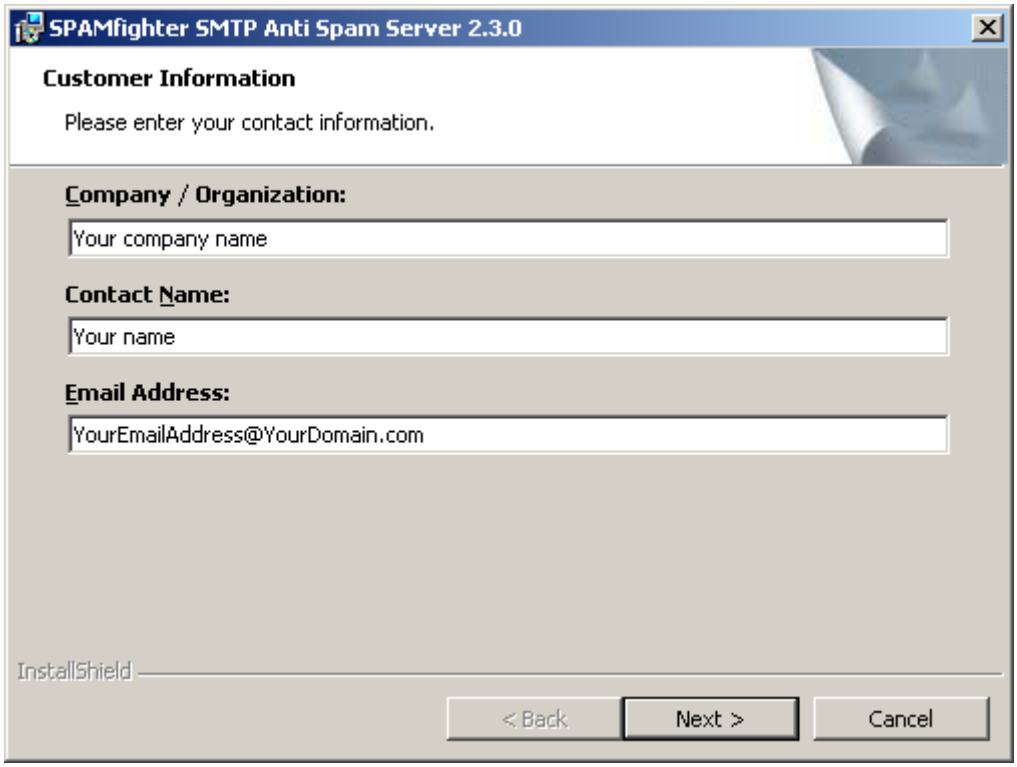


4) Select your preferred language and select "OK":

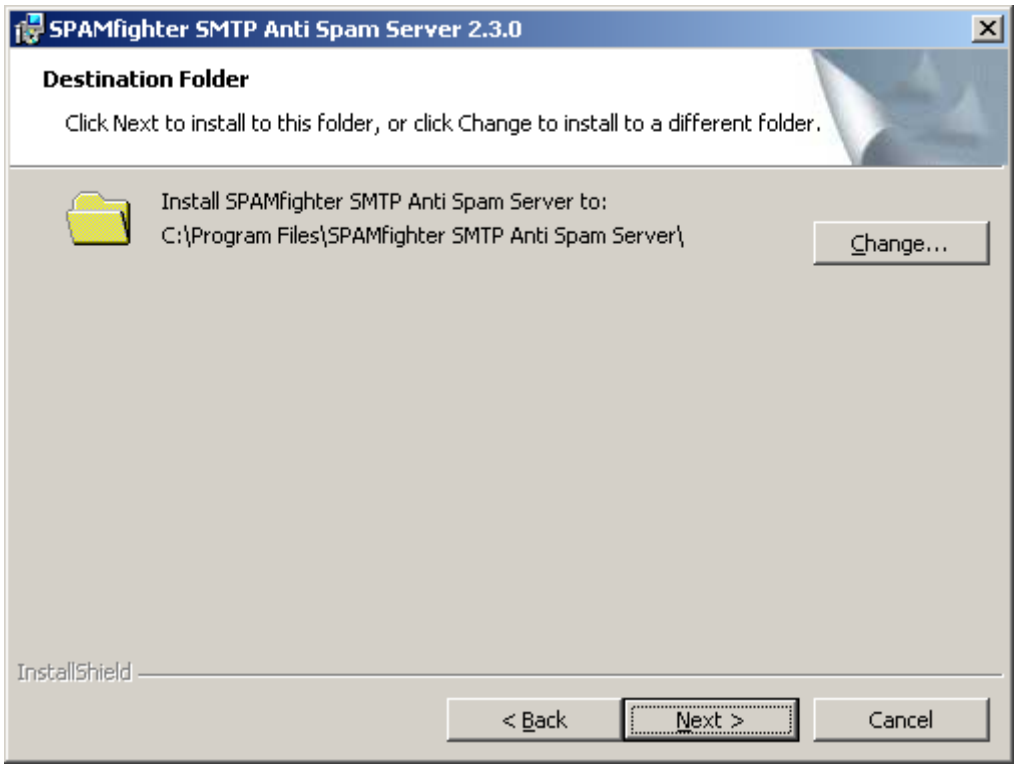


5) When this screen appears, enter your contact details and select "Next". (Are you reinstalling Windows and SMTP Anti Spam Server or moving your existing installation to another server? In this case it is important to enter the exact same details as last time to regain your license(s). If you are unsure, just enter your details

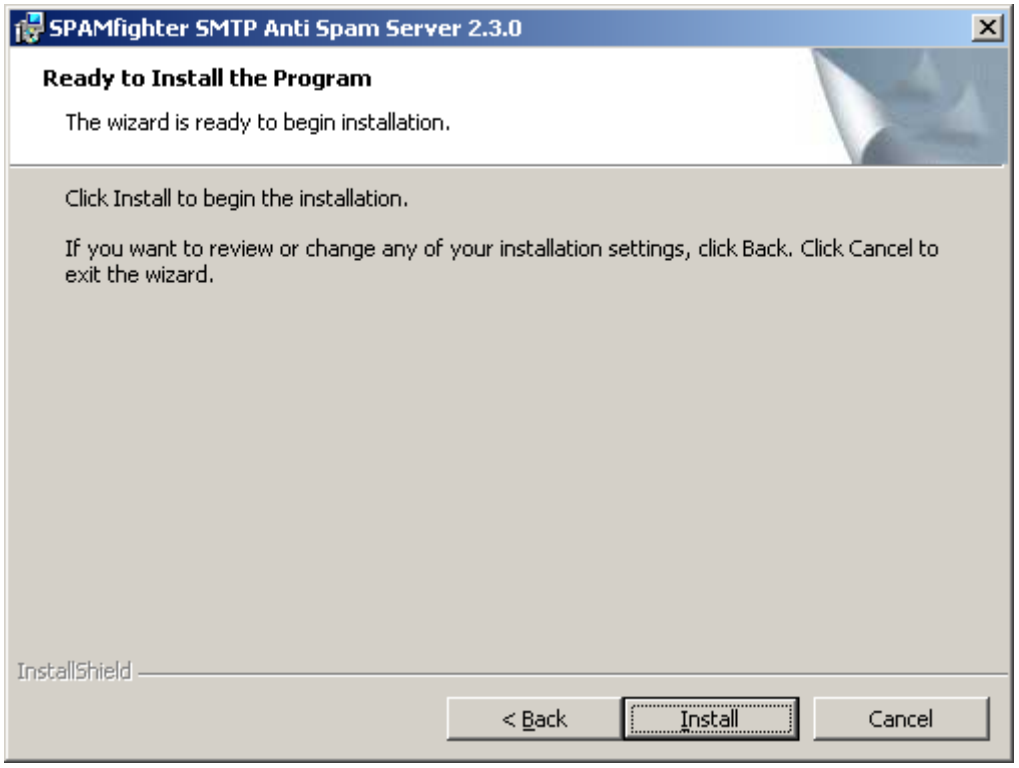
and continue, then contact our support team at smtpsupport@spamfighter.com after the installation.)



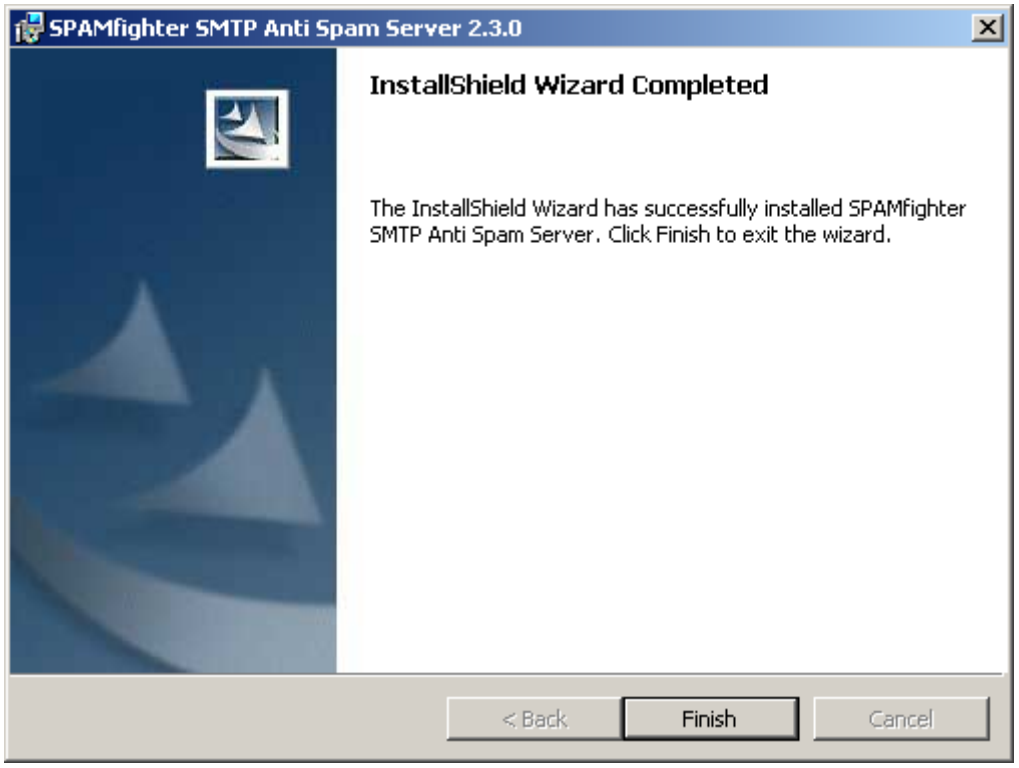
6) Choose the installation directory (it is recommended to install into the pre-entered directory) and select "Next":



7) Select “Install”:



8) Select “Finish” to exit the installation:



Configuring Windows

The following task has to be completed to setup Windows for SMTP Anti Spam Server:

- Add another local IP address for SMTP Anti Spam Server.

Add another local IP address for SMTP Anti Spam Server

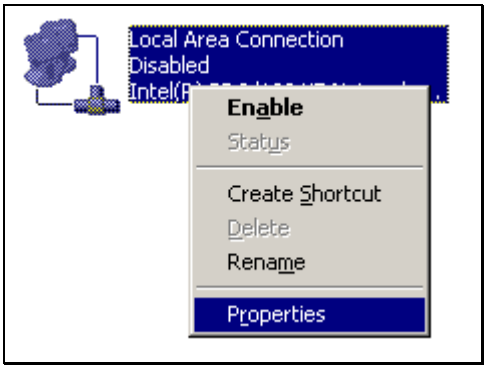
Please note that all numbers and values displayed in the following images are *meant as examples only* and likely need to be adapted to your specific network environment.

1) Select “Start” > “Control panel”.

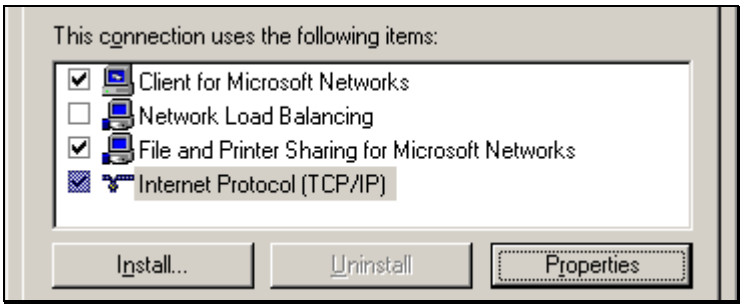
2) If the modern view is displayed, “Switch to classic view” on the upper left.

3) Activate “Network connections”.

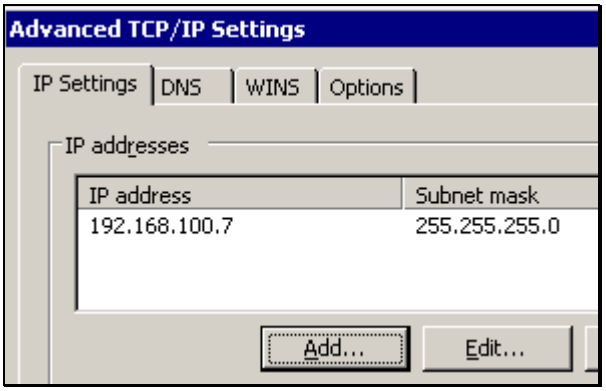
4) Right-click the LAN connection to your router or gateway device and select “Properties”:



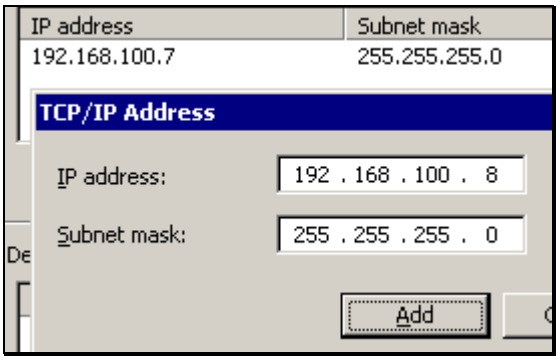
5) Select “Internet Protocol (TCP/IP)” and then “Properties”:



6) Note the existing IP address(es) and select “Add…”:



7) Add a new unoccupied IP address from the same subnet (if you are unsure, consult your network administrator) and click “Add”:



8) Write both IP addresses down – you will need them later.
In the following text we will refer to the example address “192.168.100.8” as the “new IP address” and to the example address “192.168.100.7” as the “old IP address”.

9) Select “OK” three times.

Configuring Merak Mail Server

The following tasks have to be completed to setup Merak Mail Server for interopability with SMTP Anti Spam Server:

- Unbind Merak Mail Server from the newly added IP address.
- Disable relaying access for the newly added IP address.
- Disable SPF sender filtering (only if previously activated).
- Disable intrusion prevention (only if previously activated).
- Disable “catch-all” functionality (optional, only if previously activated).

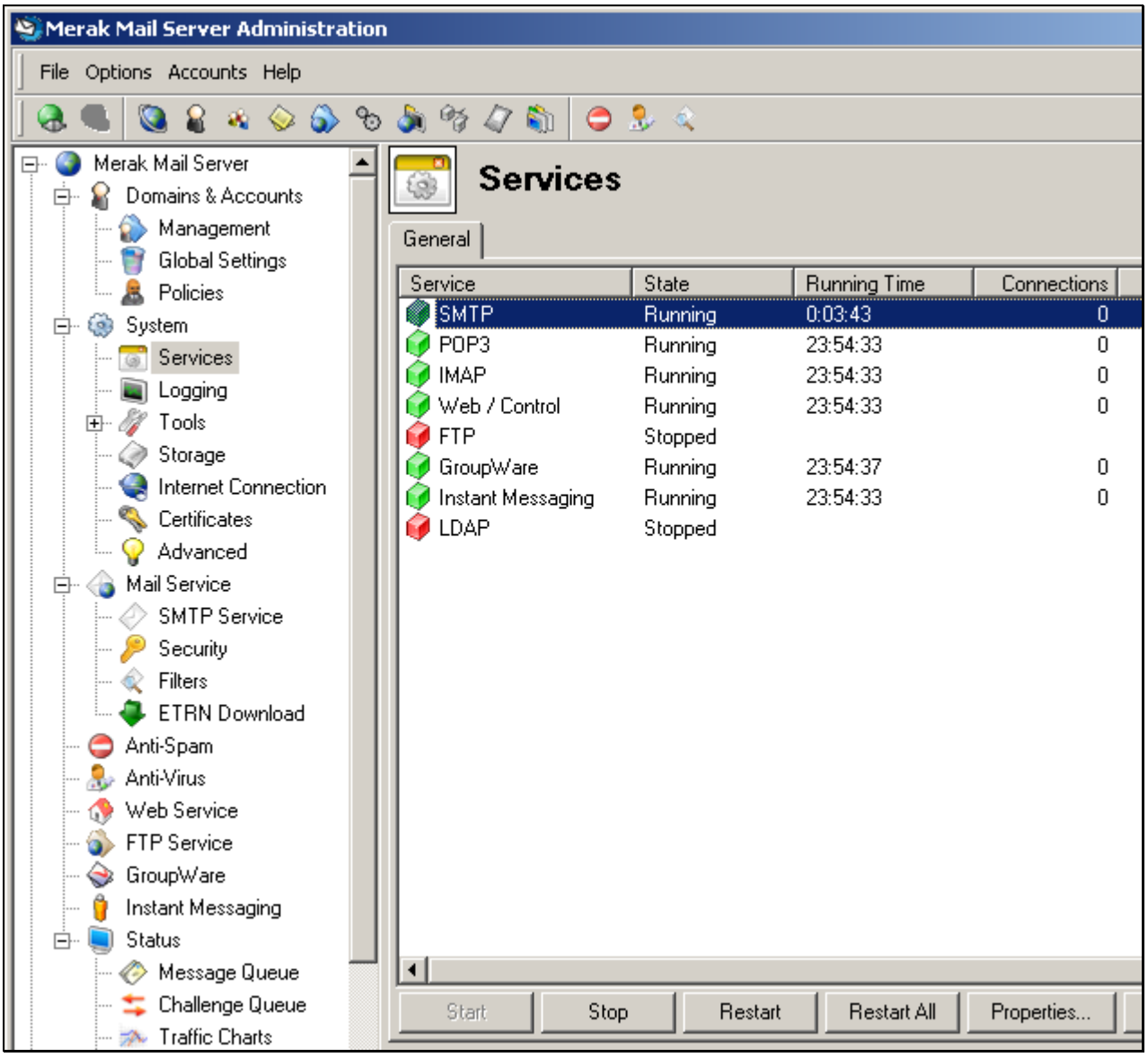
1) Start Merak Mail Server Administration by clicking “Start” > “All programs” > “Merak Mail Server” > “Merak Mail Server Administration”.

Unbind Merak Mail Server from the newly added IP address

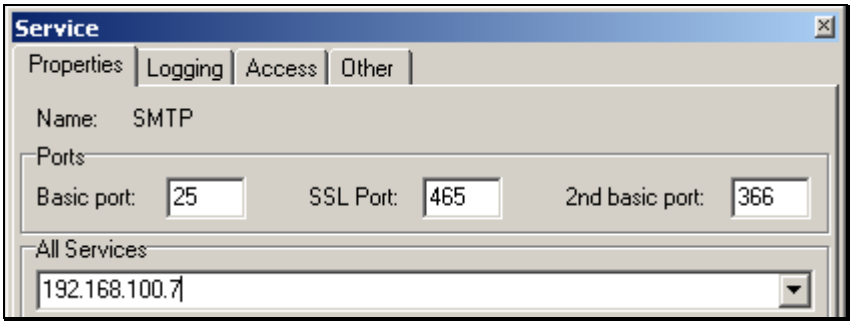
We need to prevent Merak Mail Server from listening on the new IP address in order to allow the SMTP Anti Spam Server to use it.

2) Expand the “System” icon in the tree on your left hand and select “Services”.

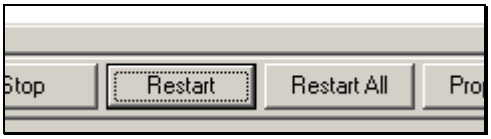
3) On the right, select “SMTP”, then activate the “Properties…” button below:



4) From the “All Services” dropdown, select the old IP address, then “OK”:



5) With the SMTP service still selected, press “Restart” to restart this service:



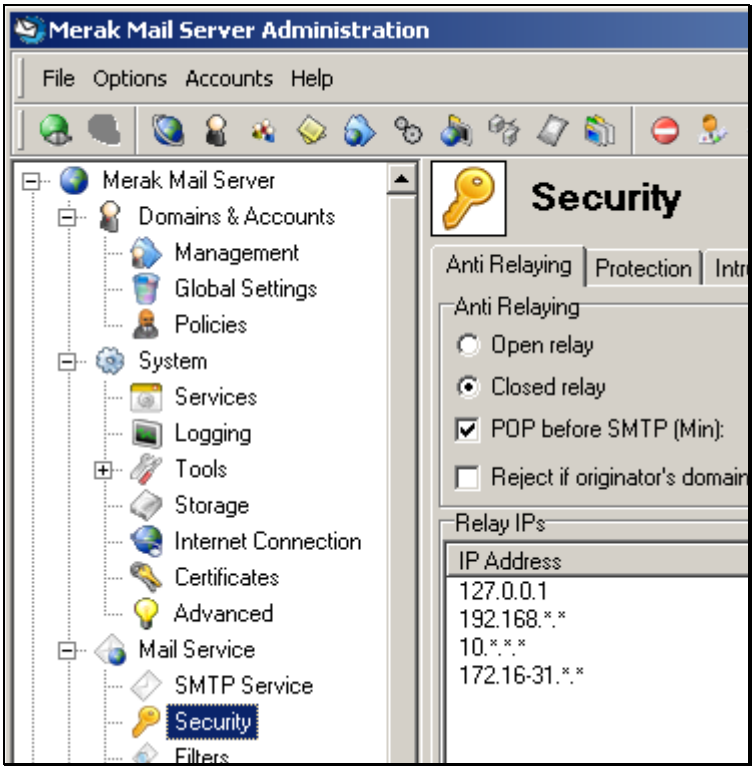
6) You have now freed the new IP address for use with SMTP Anti Spam Server.

Disable relaying access for the newly added IP address

The relaying list in Merak Mail Server determines which computers may use your connection to send e-mail to external domains. By default Merak Mail Server won't relay e-mails for unauthenticated users; however you might have changed this setting previously in order to simplify client configuration. *Because the IP address used by SMTP Anti Spam Server represents external, unauthenticated clients, it is extremely important to disable relaying access from the new IP address.*

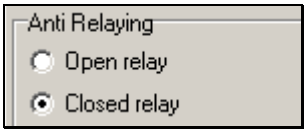
7) Enable the Advanced interface by selecting "Options" > "Interface mode" > "Advanced":

8) Expand the "Mail Service" icon in the tree on your left hand and select "Security", then switch to the "Anti Relaying" pane on the right, unless it already is being displayed:

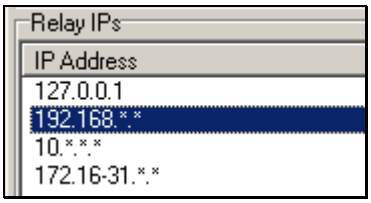


9) If the "POP before SMTP" checkbox has a checkmark in front of it, you can skip the rest of this chapter and jump to "Disable SPF sender filtering".

10) If "Open relay" is selected, change this to "Closed relay":

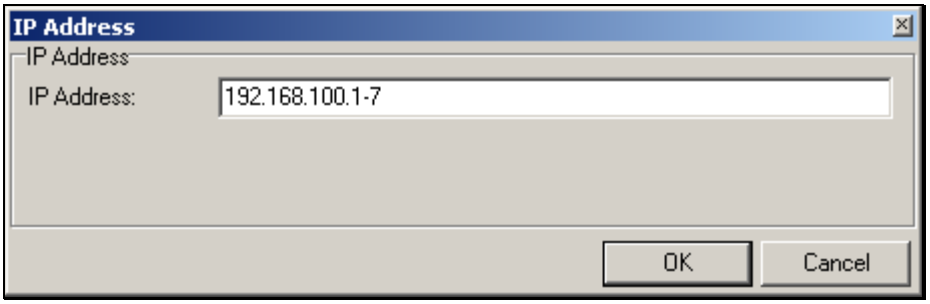


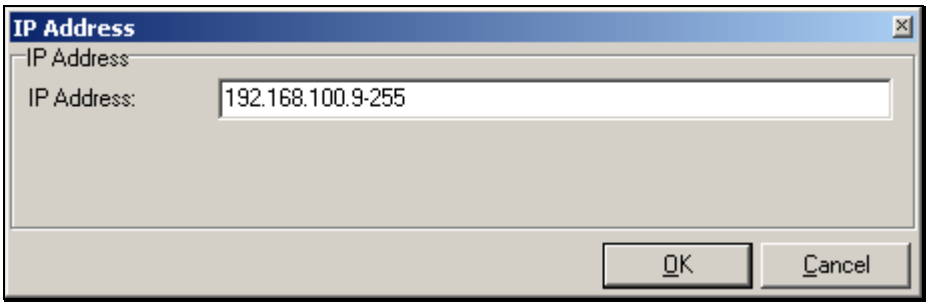
11) In the list of "Relay IPs", find the one range which contains the newly added IP address:



Following the example the new IP address is “192.168.100.8”, which is contained in the range “192.168.*.*” selected above. *Don’t modify the range yet.*

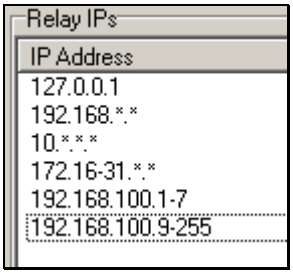
12) Add two or more new ranges by activating the “Add…” button below the list. For example, if all your computers are located in the range 192.168.100.*, you will need to add two ranges, which contain all IP addresses *except* the newly added IP address:



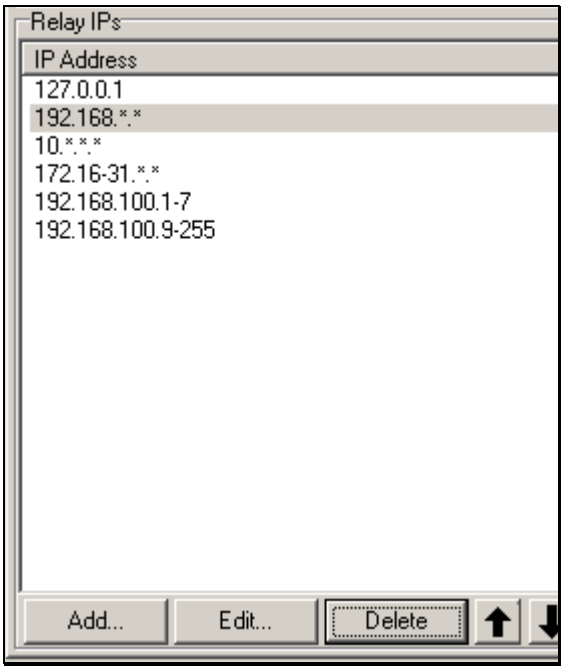


Remember, this is just an example – the actual values to be entered will most likely differ, depending on the IP addresses in use at your site.

13) After adding the new ranges the “Relay IPs” box might look like this:



14) Now that we have ensured relaying access for all computers except the IP address previously added to this server, remove the original range by selecting it and pressing “Delete”:



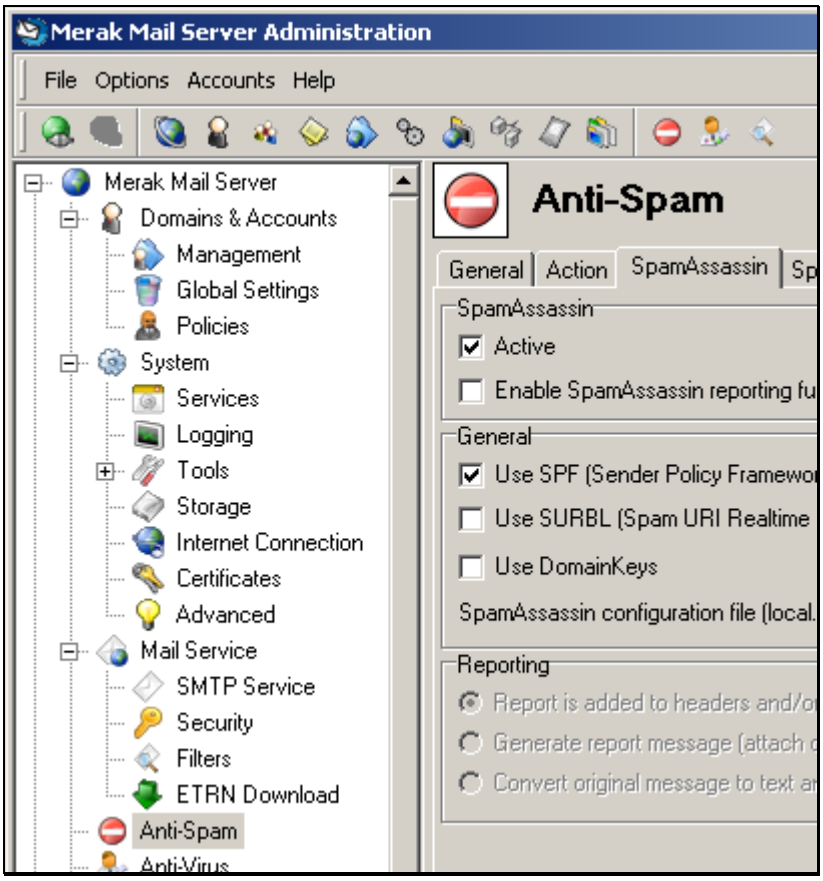
15) Finally save your changes by activating the “Apply” button at the bottom right.

Disable SPF sender filtering

The Sender Policy Framework (SPF), also known as “Sender ID”, is a technology which prevents phishing attacks from spoofed, well-known domain names. Due to little industry recognition its current effects are rather scant, and using SPF and a tunneling filter such as SMTP Anti Spam Server at the same time can prevent legitimate e-mails from being delivered.

If you previously enabled the SPF functionality in Merak Mail Server (not enabled by default), follow these steps to disable it:

16) Select the “Anti-Spam” icon in the tree on your left hand, then switch to the “SpamAssasin” pane on the right, unless it already is being displayed:



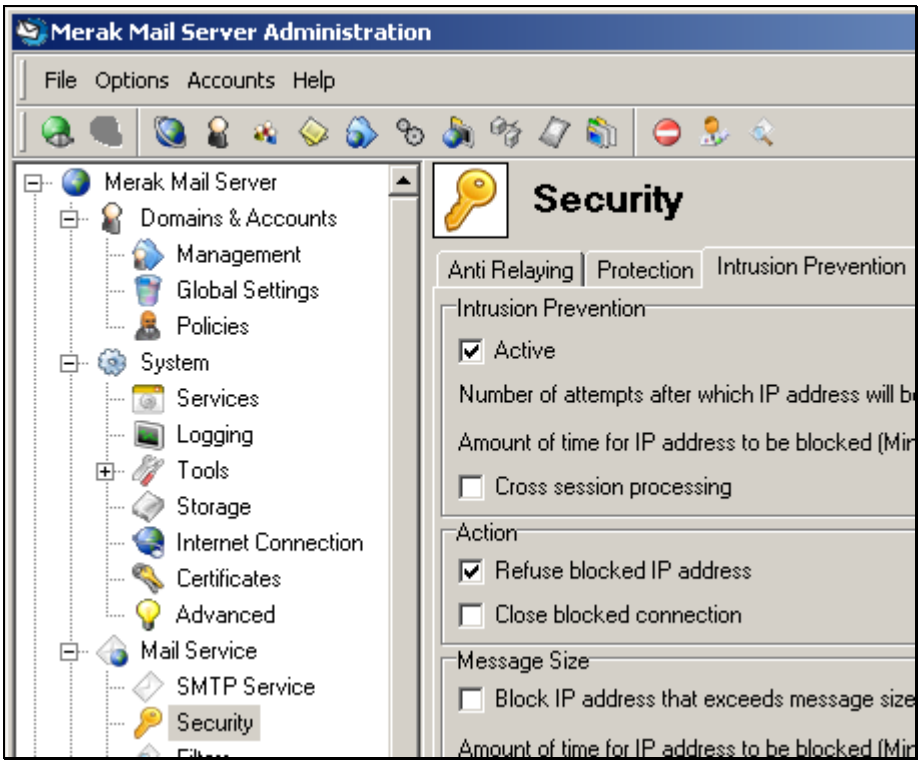
17) Remove the checkmark in front of “Use SPF (Sender Policy Framework)” and activate the “Apply” button at the bottom right.

Disable intrusion prevention

The intrusion prevention feature in Merak Mail Server allows you to block access from IP addresses with several failed delivery attempts for a certain time. This functionality is neither useful nor compatible with SMTP Anti Spam Server; nor is it enabled by default.

If you previously enabled the intrusion prevention functionality in Merak Mail Server, follow these steps to disable it:

18) Expand the “Mail Service” icon in the tree on your left hand and select “Security”, then switch to the “Intrusion prevention” pane on the right, unless it already is being displayed:



19) Remove the checkmark in front of “Active” and activate the “Apply” button at the bottom right.

Disable “catch-all” functionality (optional)

If you never enabled “catch-all” functionality in Merak Mail Server, jump to “Configuring SMTP Anti Spam Server”.

When a mail server that is responsible for some domain receives mail for an unknown user at that domain (an e-mail address without a corresponding mailbox) it’s usual action will be to reject that e-mail. Common causes leading to this scenario are: the sender misspelled the recipient’s address; the sender is a spammer just “trying out” lots of recipients in the hope of finding a victim; or the recipient’s mailbox has been removed from the system. Most mail servers including Merak Mail Server (where this functionality isn’t enabled by default though) sport a feature called “catch-all”. If “catch-all” functionality is enabled for a domain, instead of rejecting mails to unknown recipients the mail server accepts them and consolidates them into a single mailbox. This can be very useful, especially if there are only few users on the server. In most cases though enabling the “catch-all” feature is counterproductive, as it can demand lots of bandwidth and increase the number of spam mails received tremendously.

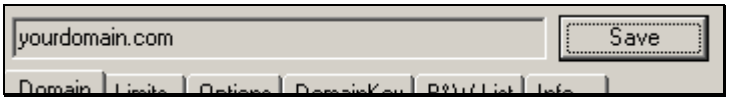
If you enabled the “catch-all” feature and your company’s e-mail infrastructure relies on it, don’t change it either.

In case you enabled the “catch-all” feature in Merak Mail Server previously, but aren’t using it, we recommend to follow these steps to disable it:

20) Expand the “Domains & Accounts” icon in the tree on your left hand and select “Management”, then select your domain on the right and switch to the “Domain” pane, unless it already is being displayed:

21) Under “Unknown users”, in the “Action” dropdown, change “Forward to email address (Catch-all)” to “Reject mail”:

22) Activate the “Save” button on the upper right:



Configuring SMTP Anti Spam Server

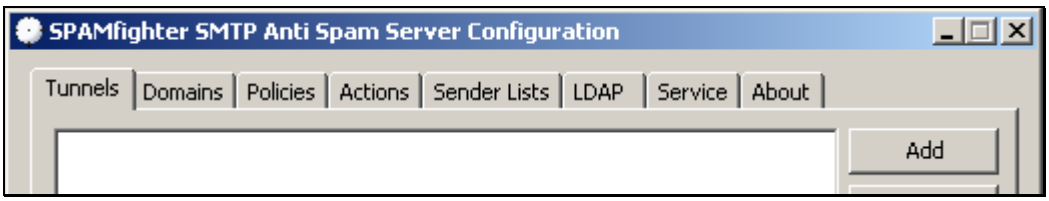
The following tasks have to be completed to setup SMTP Anti Spam Server for interopability with Merak Mail Server:

- Establish a tunnel between the new and old IP address.
- Decide on a policy for spam handling.
- Apply the policy to domains.

1) Start the SMTP Anti Spam Server configuration utility by choosing “Start” > “All programs” > “SPAMfighter SMTP Anti Spam Server” > “Configure Anti Spam Server”.

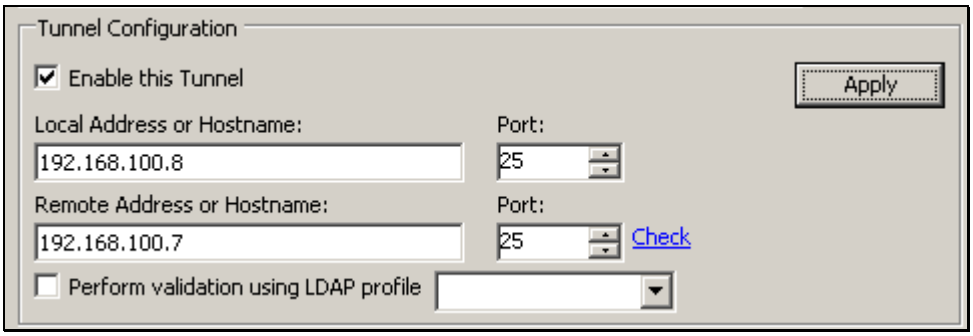
Establish a tunnel between the new and old IP address

2) On the “Tunnels” pane, select “Add” to create a new tunnel:

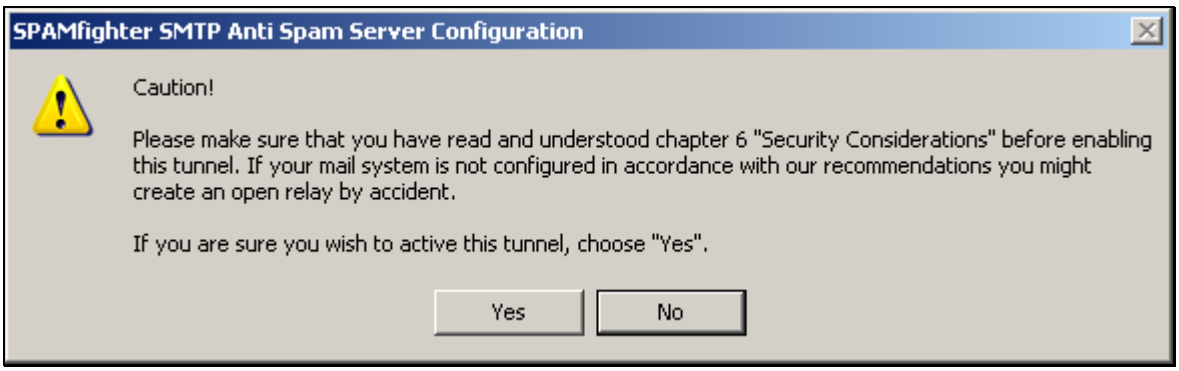


3) Select the “New tunnel” that appeared in the list.

4) For “Local Address or Hostname”, enter the new IP address you added to the server previously.
For “Remote Address or Hostname”, enter the old IP address used by Merak Mail Server.
Put a checkmark in the “Enable this Tunnel” box and activate the “Apply” button:



5) If you receive a security warning, confirm it by selecting “Yes”:



Decide on a policy for spam handling

SMTP Anti Spam Server enables different scenarios depending on the control you and your users require over filtered spam mails. Among the possible spam handling actions are:

- Reject delivery (the default)

- Redirect them to a collection mailbox
- Deliver them to the intended recipient and:
    - Insert “SPAM” or other text in the subject
    - Insert a header line in the mail

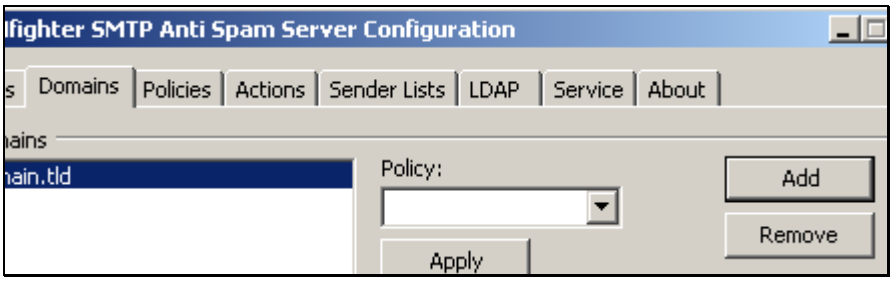
  for further sorting in the mail server or mail application.

These “actions” can be applied to one or more “policies” that in turn can be applied to one or more domains and/or recipients.

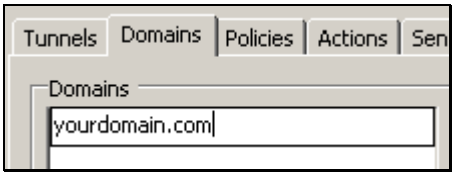
In the following steps we will apply the “Default policy”, which is a basic policy configured to reject mails with a high spam probability. For more information on configuring actions, policies and other advanced features of SMTP Anti Spam Server please refer to the manual included with your installation or available for separate download here.

Apply the policy to domains

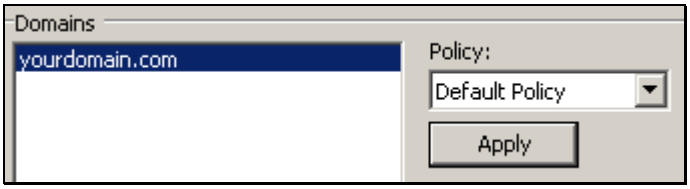
6) On the “Domains” pane, select “Add” to add your first domain:



7) Double-click (or select and press F2) the new domain “domain.tld” added to the list, rename it to your real domain name and press Enter:



8) With the domain still selected, choose the “Default Policy” from the dropdown and activate the “Apply” button:



After having verified that the setup is working you might want to customize your policy and spam handling actions further. Please refer to the manual included with your installation or available for separate download here for further instructions at that time.

Configuring your router, firewall or gateway device

The last step will be to configure your router, so incoming mail from the internet is sent through the tunnel before being delivered to your Merak Mail Server.

How to do this depends on the hard- and software to use. Usually you would change the port forwarding setting for port 25 (SMTP) from the old IP address to the new one (following our example, you would change 192.168.100.7 to 192.168.100.8 in the router's port forwarding configuration). If in doubt, please ask your network administrator or consult the manuals included with your hard- or software.