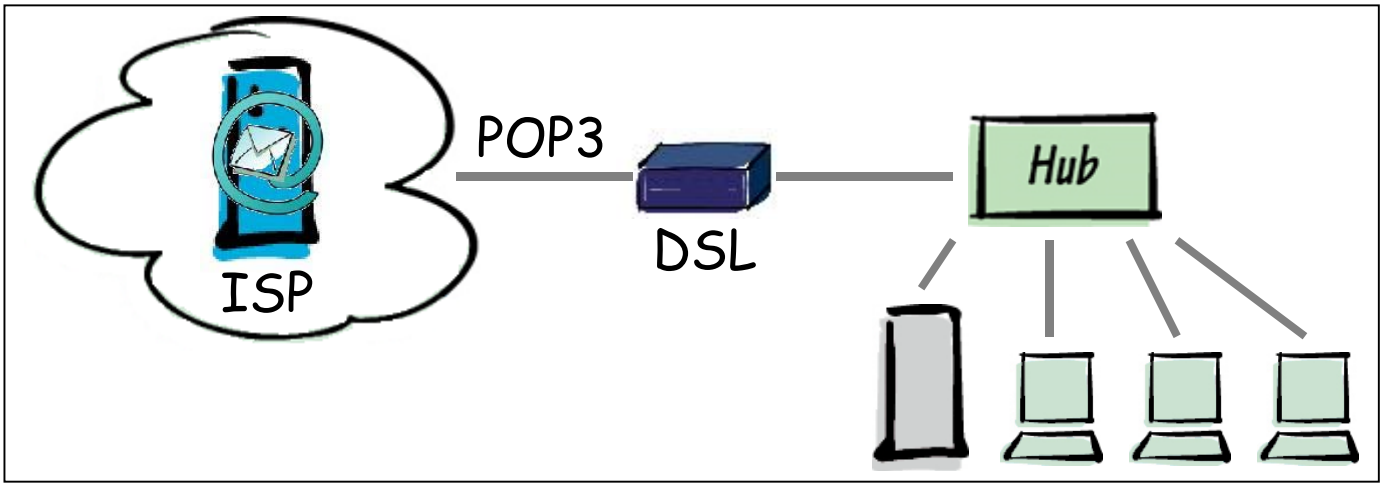
Centralized Anti-Spam with POP3 Downloads

created by: Rainer Bemsel – **Version** 1.0 – **Dated:** Dec/21/2003

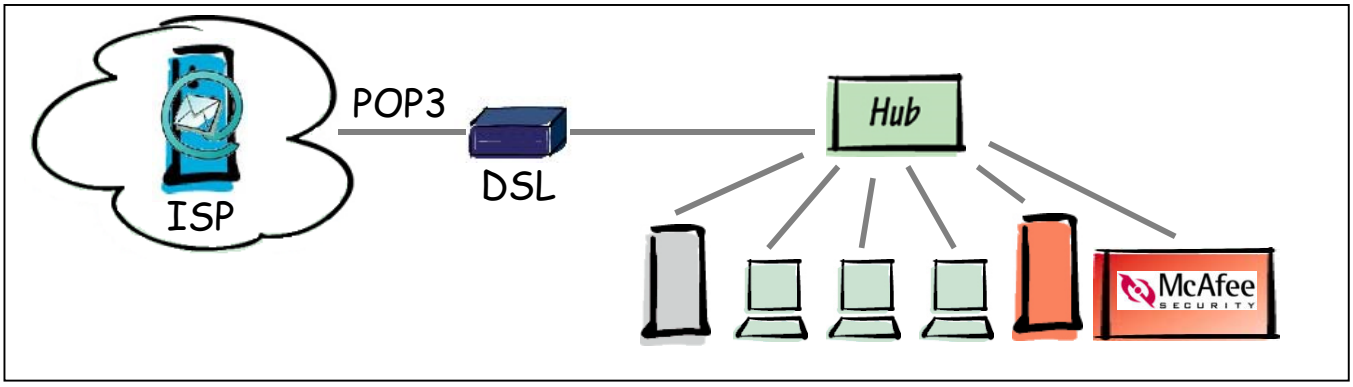
If you have evaluated different centralized Anti-Spam & Anti-Virus Solutions you mostly stuck with one criteria. Email delivery has to be done via SMTP and MX Records. So far so good, but what to do, when having ISP taking care of all your email routing and your company is not big enough to maintain an own Email Service, like Lotus Domino or an Exchange environment. This works only, when your ISP is able to catch all in one single mailbox. When running a different environment, you may consider another POP3 Download Proxy, which is able to forward internally via SMTP.

A typical environment looks like this:



In this scenario, all client retrieves their emails via POP3 from an external Email Server, hosted by an ISP. Anti-Spam can only work, if they are located on each client and this to be administered could cause nightmares. There are good solutions out there, like McAfee Security's WebShield Appliance with Anti-Spam and Anti-Virus, but solutions like that works only when SMTP delivery is in place. This won't be the way in this environment.

To make this run, I've added another service and McAfee Security WebShield Appliance.



The Red Server hosts now a kind of POP3 Retriever and SMTP Forwarder. The Grey Server has been added with a freeware SMTP Server. Between them, McAfee Security WebShield Appliance is scanning for Anti-Virus, Anti-Spam & Email Content Filtering.

There are several products out there, doing the Email Retrieval Job. In this scenario I used following products, which may be easily copied for your demands.

ISP hosting Emails:

EMAIL RETRIEVAL: EFS Standard Email Forwarding System by
http://www.chimeracomputing.com/

Local SMTP Server: Mail Enable Standard Edition by
http://www.mailenable.com

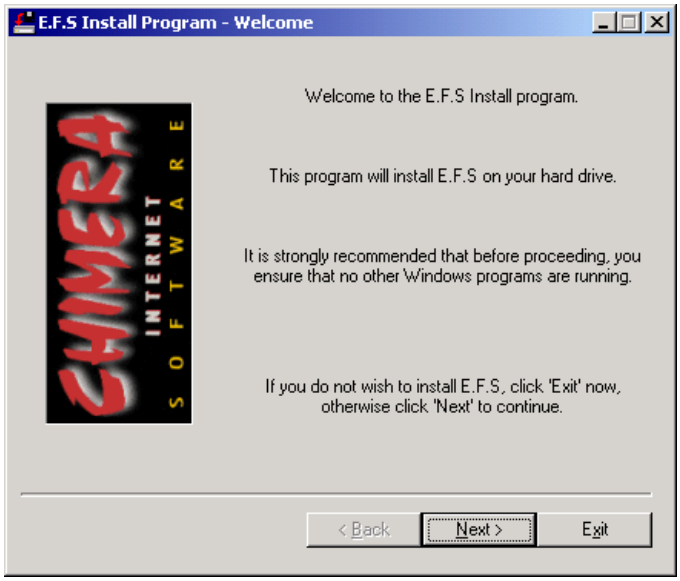
ANTI-Virus & Anti-Spam: McAfee Security WebShield Appliance
http://www.nai.com/us/products/mcafee/antispam/spk_webshield_appliances.htm

Email Client: Microsoft Outlook Express

Installation Steps

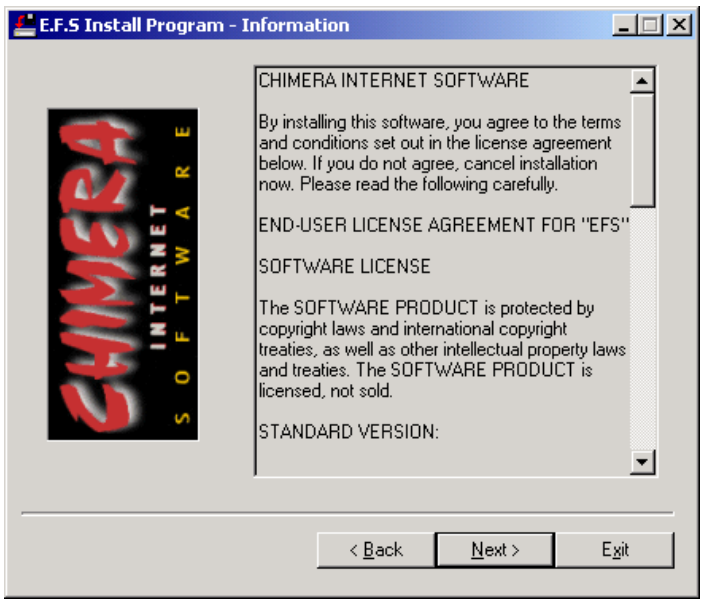
EFS Standard Email Forwardung System

Download Product from http://www.chimeracomputing.com/ and run efs3full.exe

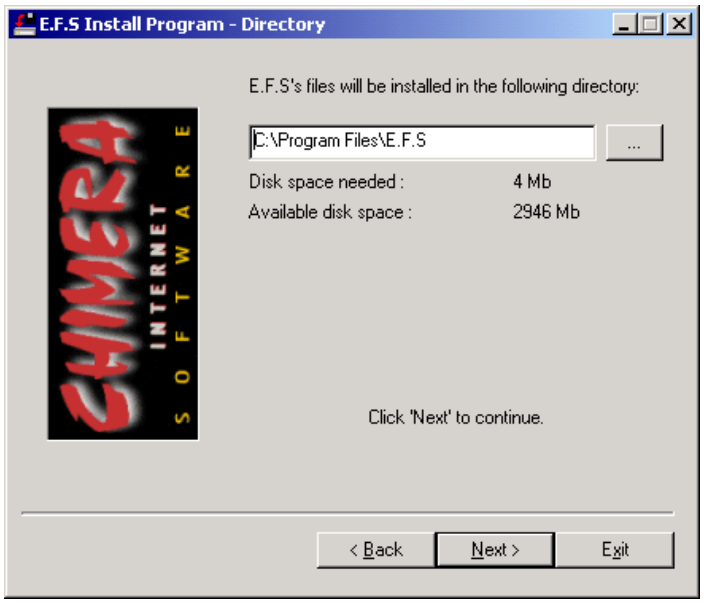


Click on **NEXT**

License Agreement will show up

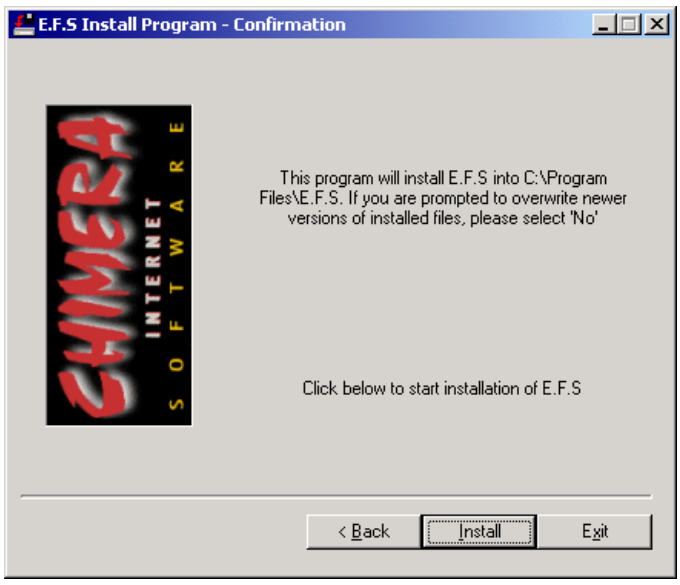


Click on **NEXT** – Here you can change Default Directory. I recommend to leave default settings

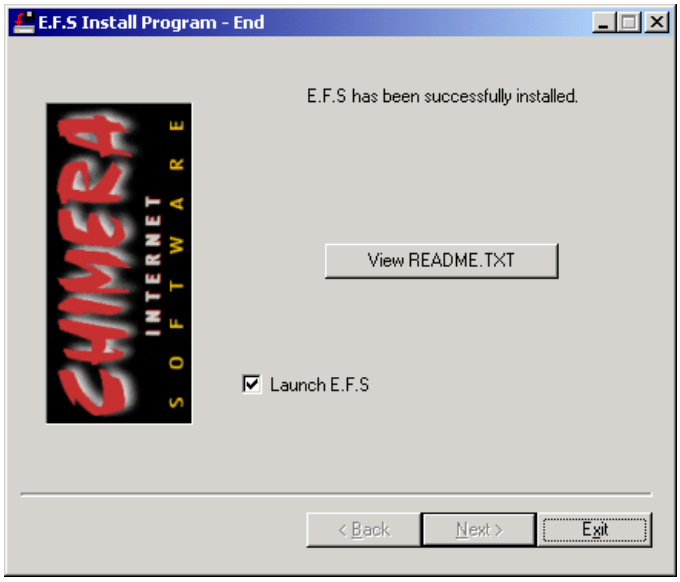


Click on **NEXT**

Once confirmation windows appears, you have the last change to stop the installation. To continue, you have to click **INSTALL**



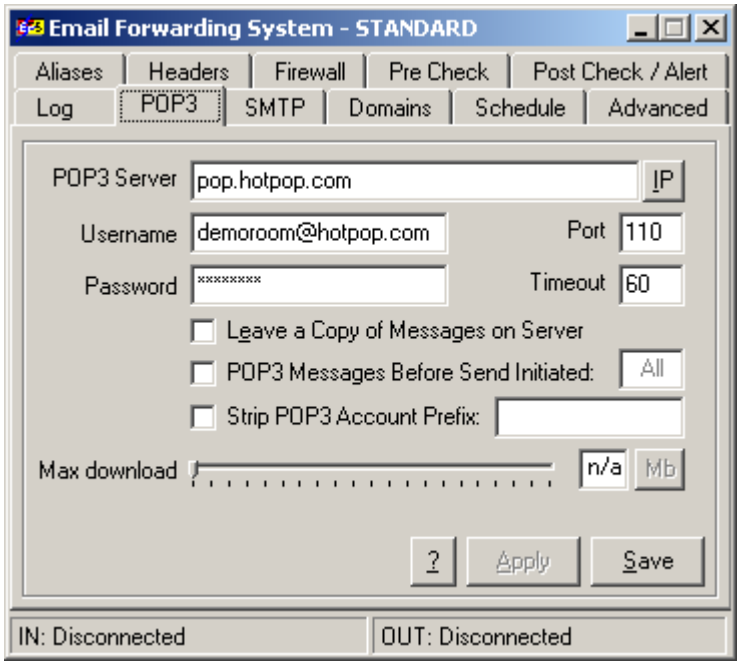
After a short moment, when installation has been performed you'll get a notification, that EFS has successfully installed. Now, it's time to view the readme.txt



When having Launch E.F.S. be marked, the application will start automatically.

Launch EFS by right click on  at the taskbar

Configure E.F.S

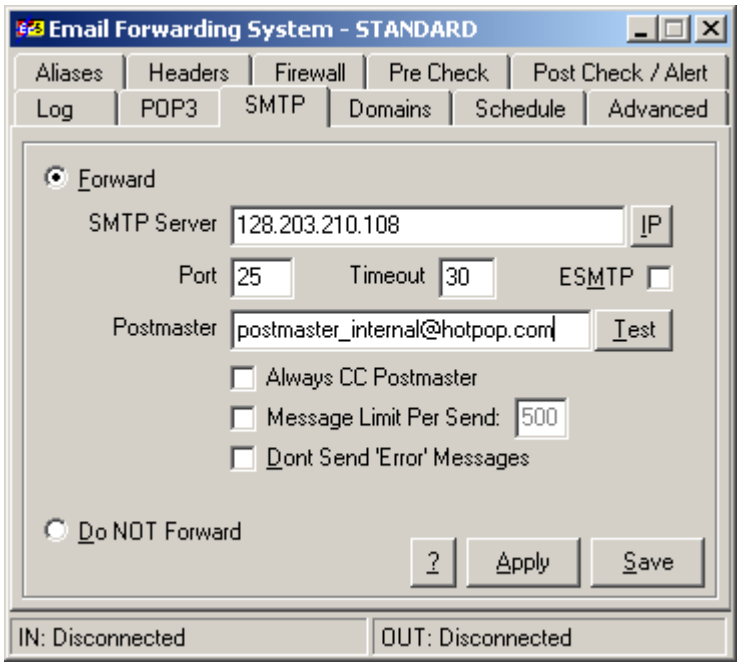


Add following minimum values:

POP3 Server
Username
Password

Verify by clicking on IP, if DNS Lookup works.

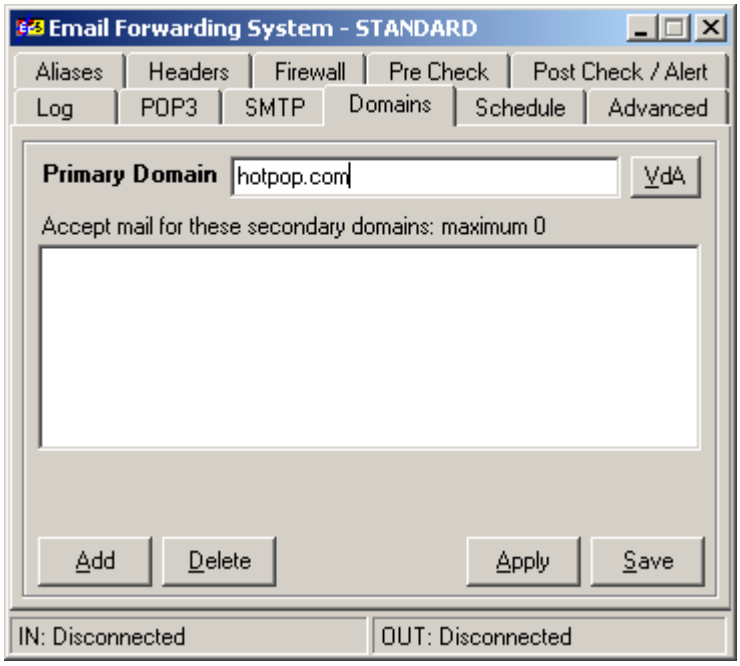
Setup POP3 (incoming mail) settings and test mail downloads correctly and Enter the domain you accept mail for under the Domains tab



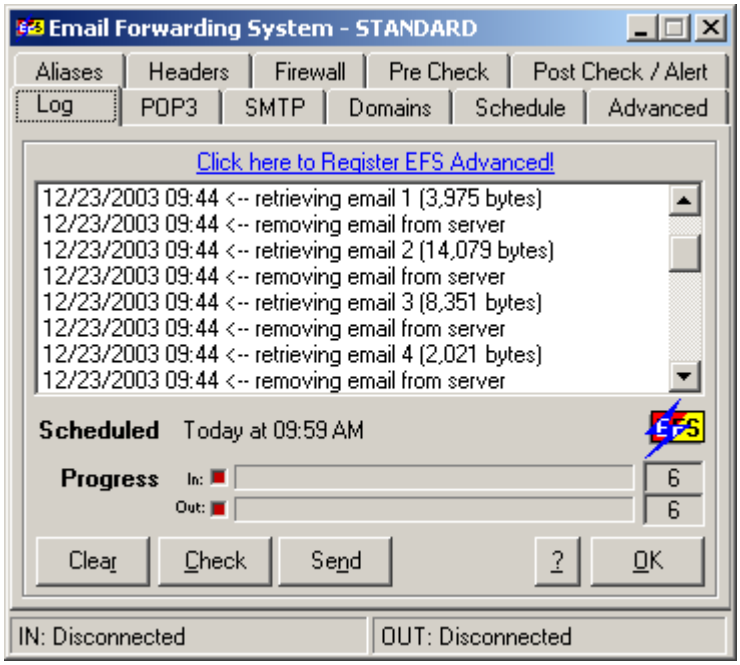
This SMTP Server is the IP Address of my McAfee Security Webshield Appliance, where all POP3 retrieved Emails will be forwarded. How WebShield has been configured, you will find later on this document.

If your WebShield is already be setup, you should verify, if you can reach McAfee WebShield Appliance via Telnet on Port 25 (for SMTP)

The disclaimer for SMTP has been modified, so you might have a different disclaimer. Now, you should enter the Primary Domain.

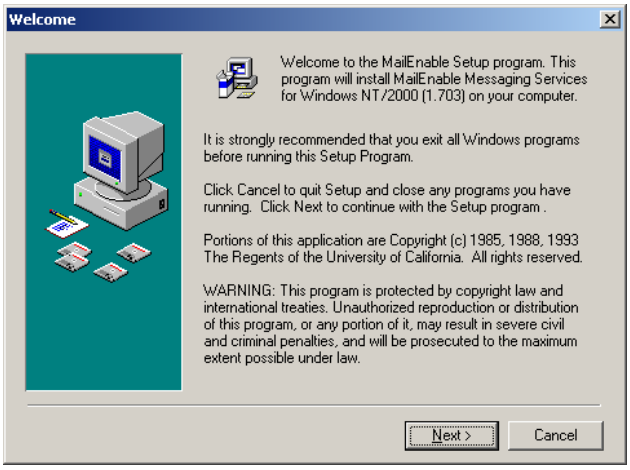


Change to LOG tab and click on CHECK. If there are any emails already with your ISP, you should get a retrieval

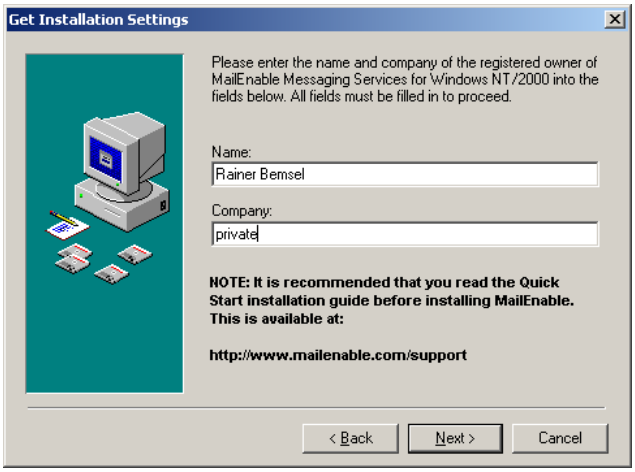


Mail Enable Standard Edition

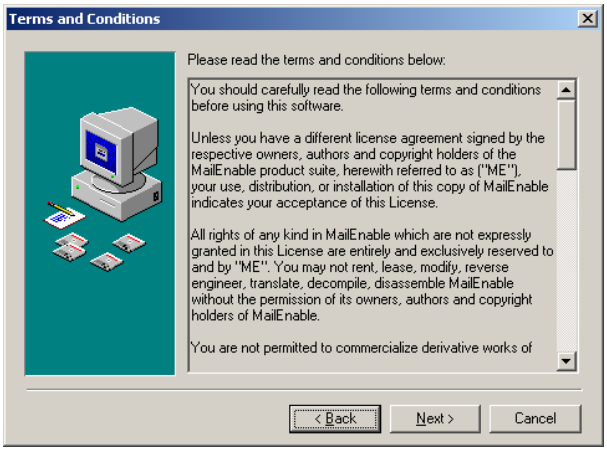
Start the installation by double-click on mailenablestandard.exe. You should **not** install this mail server not on the same server as E.F.S has been installed.



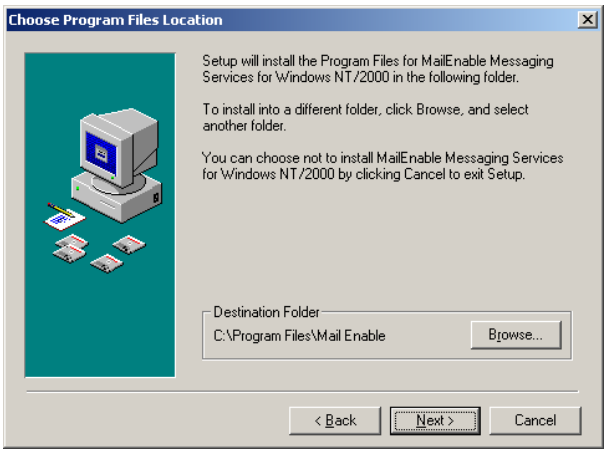
Click on **NEXT**



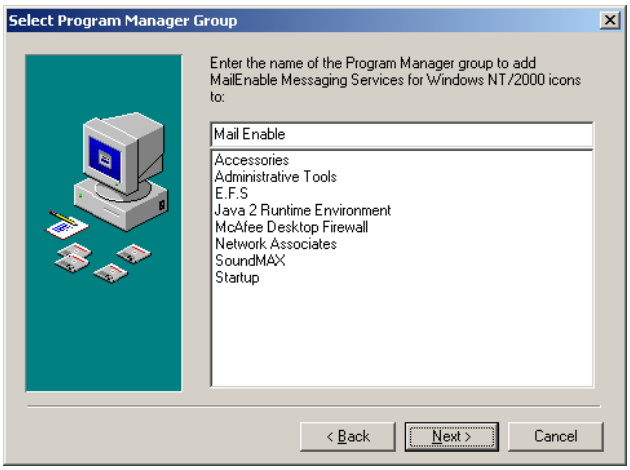
Type your name and Company. Click on **NEXT**



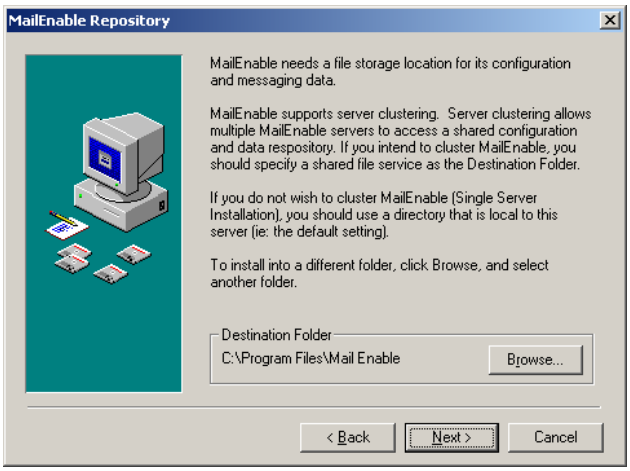
Read the terms and conditions and click on **NEXT**



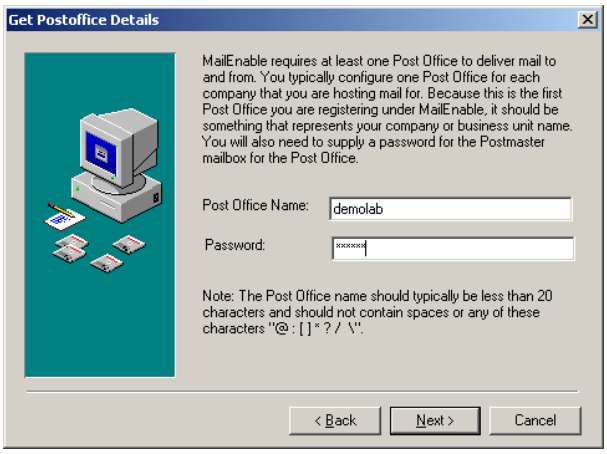
You can change the folder by clicking on **BROWSE**. However, I recommend to keep default settings. Click on **NEXT**



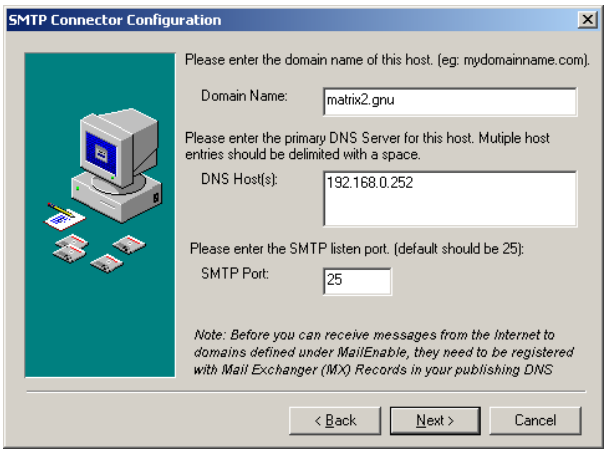
Again, keep default settings and click on **NEXT**



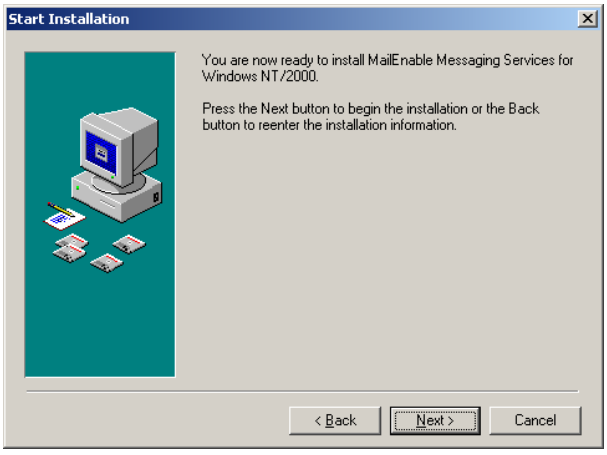
Click on **NEXT**



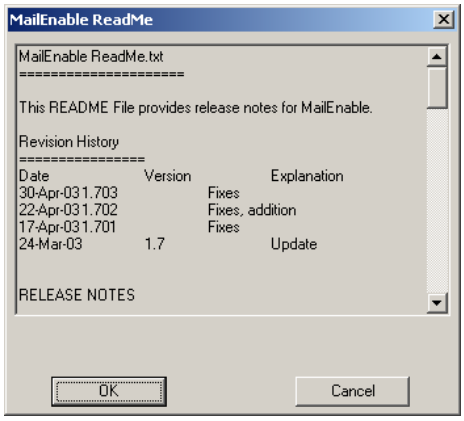
This is where you can add your own domain. I've added another Post Office later on at MailEnable Administrator. Click on **NEXT**



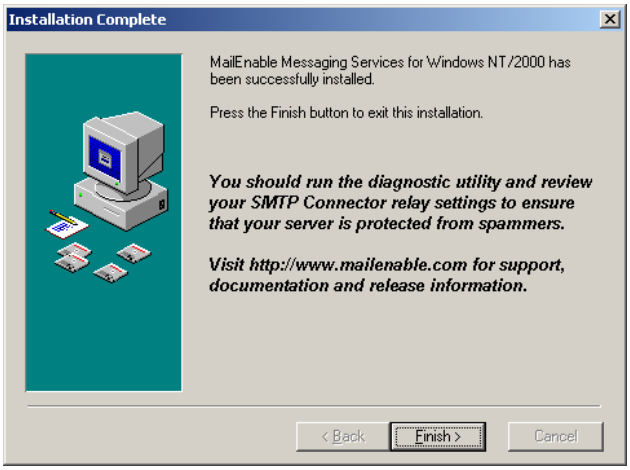
Change the values to meet your requirements and click on **NEXT**



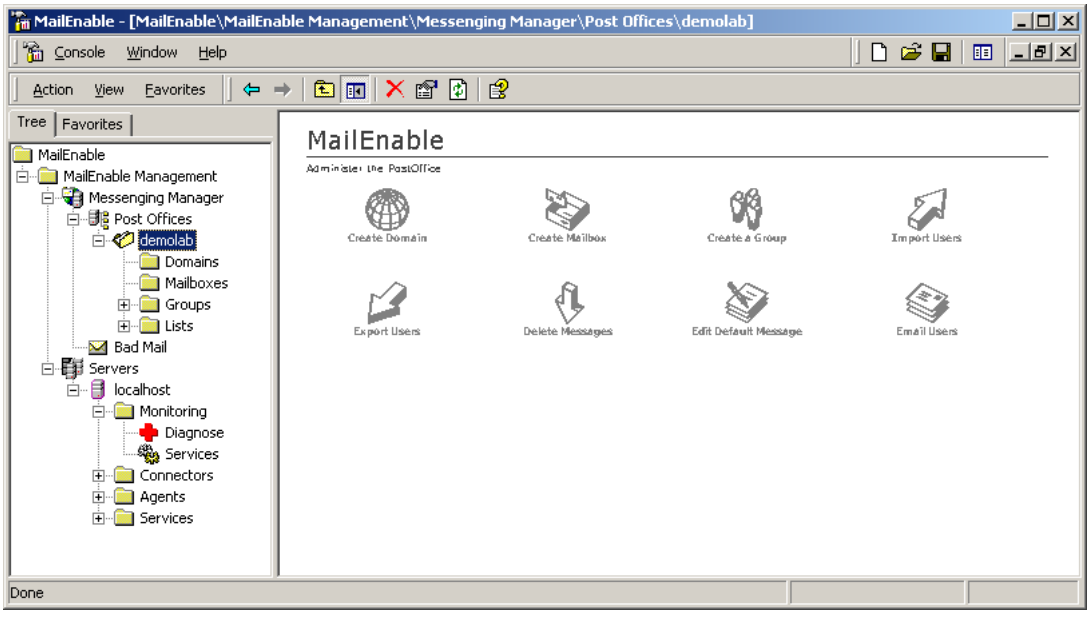
To start the installation click on **NEXT** and progress bar will appear.



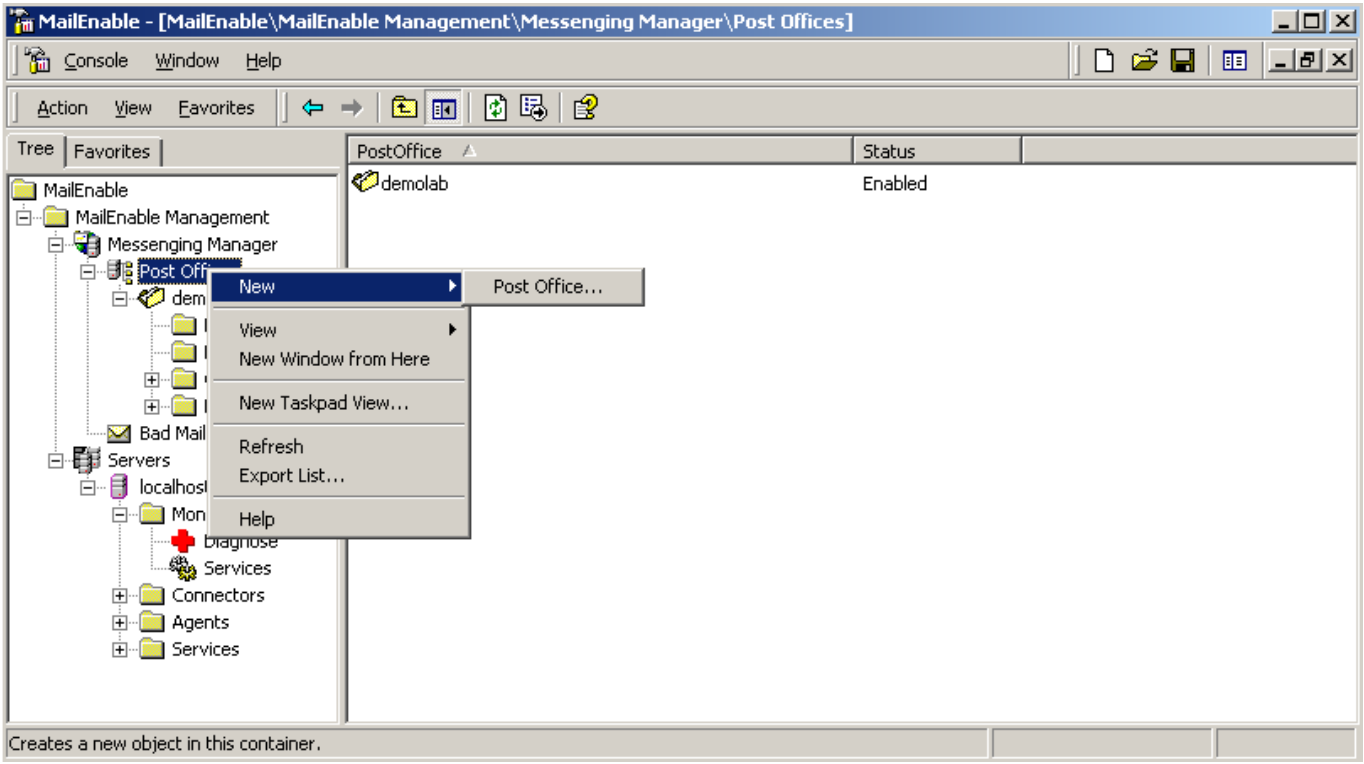
You will get a readme. Click on **OK**



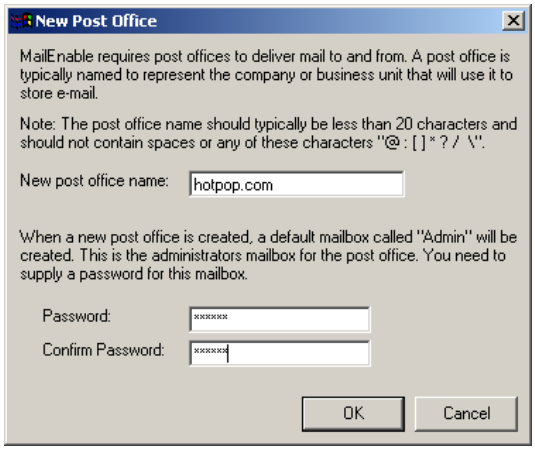
Installation is complete. Click on FINISH and allow PC to restart. When PC has been restarted, logon again and start Mailenable



Create a new Post Office, if necessary



Type a New post office name (incl. Domain extension)



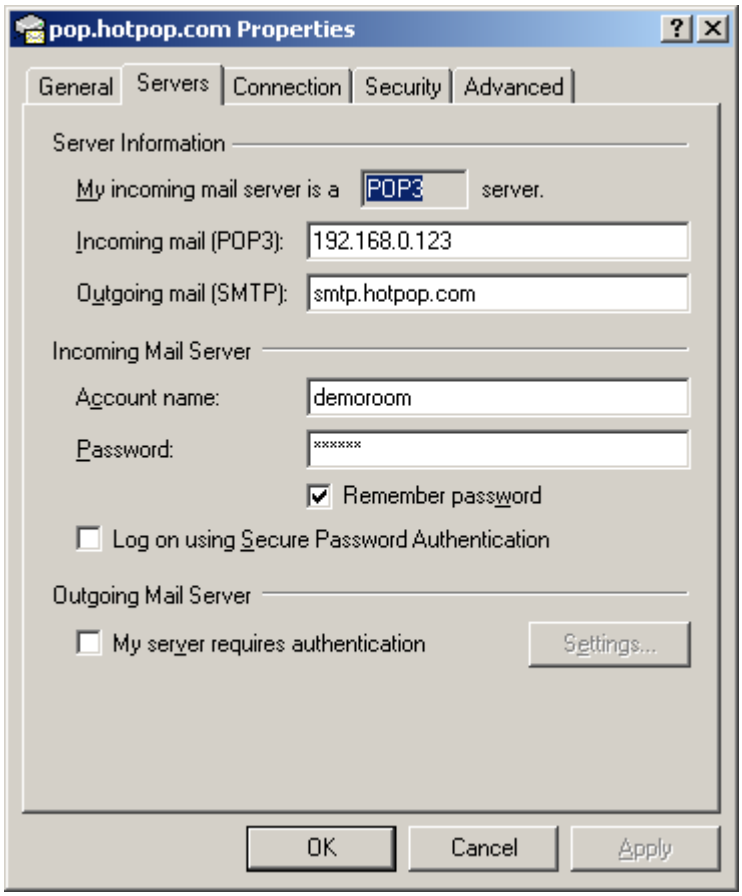
The password is for the administrator's mailbox, also knows as postmaster.

Similar to Post Office, create mailboxes if necessary.

Outlook Express Configuration

Because EFS is a POP3 Download Service only, you will have to use to different server for routing emails in and out.

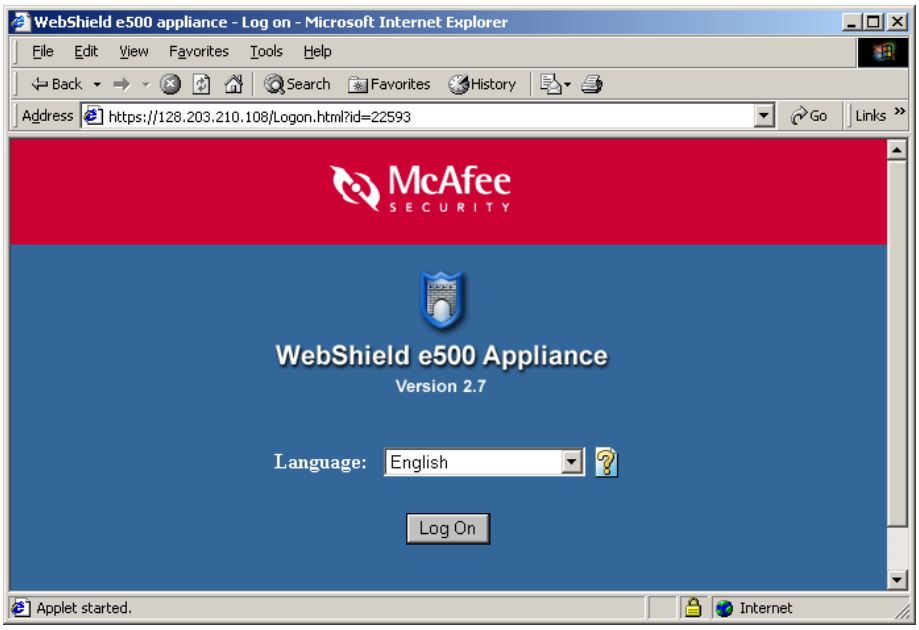
In my example, incoming Mail Server is located on “grey server” (based on my network layout on page one). For Outgoing mail, you may have to send emails directly to your ISP.



On the next pages, you’ll find some screenshots, where to add parameters to have appliance be able to scan for Spammails.

McAfee Security WebShield Appliance

1. Connect WebShield Appliance on LAN **2** with your Administration Computer. https://10.1.2.108

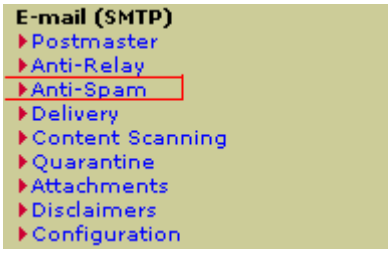


2. Default User Name: **webshield** – Default Password: **webshieldchangeme**
   If you have Java Runtime Version other than 1.31_04, please uninstall Java Runtime first, and let WebShield serve you with the proper Java Runtime Version. Allow installation and grant access.

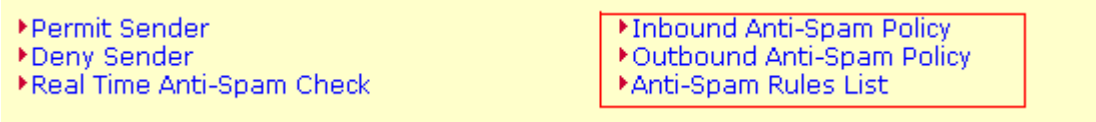
3. Assign Basic Settings:
   As I decided to run WebShield Appliance in Proxy Mode, you only need to change IP Address for LAN 1. LAN 2 is used for administration only and can be deactivated after basic settings have been configured.

4. Reboot WebShield Appliance and log on again by using new assigned IP Address and reconnected to LAN 1

5. Under SMTP, click on Anti-Spam.



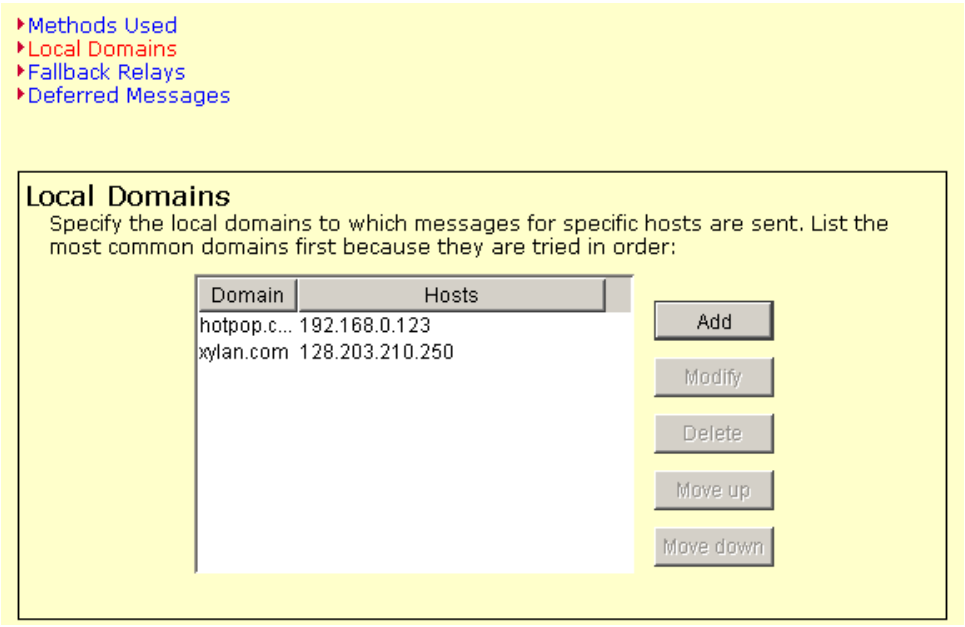
6. E-Mail Anti-Spam pane will open.



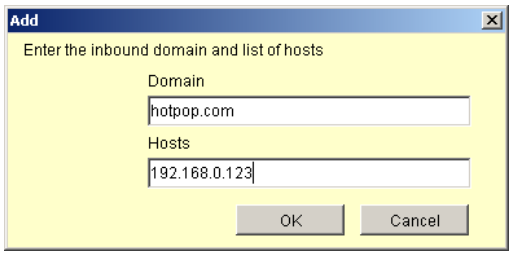
When running a configuration from scratch, click on **EVALUATE** and Anti-Spam Policy

7. Now, click on Delivery

Click on Local Domains. If you haven't added any local domains, now it's time to do.

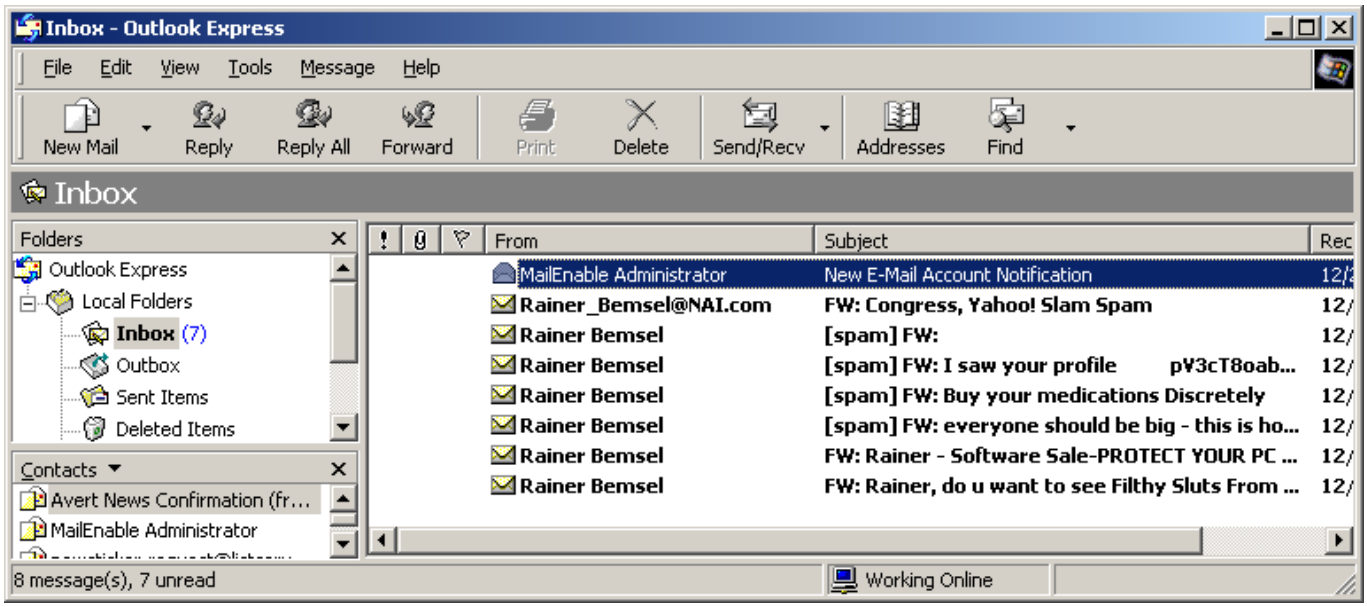


Click on Add and enter the values for Domain and internal SMTP Server

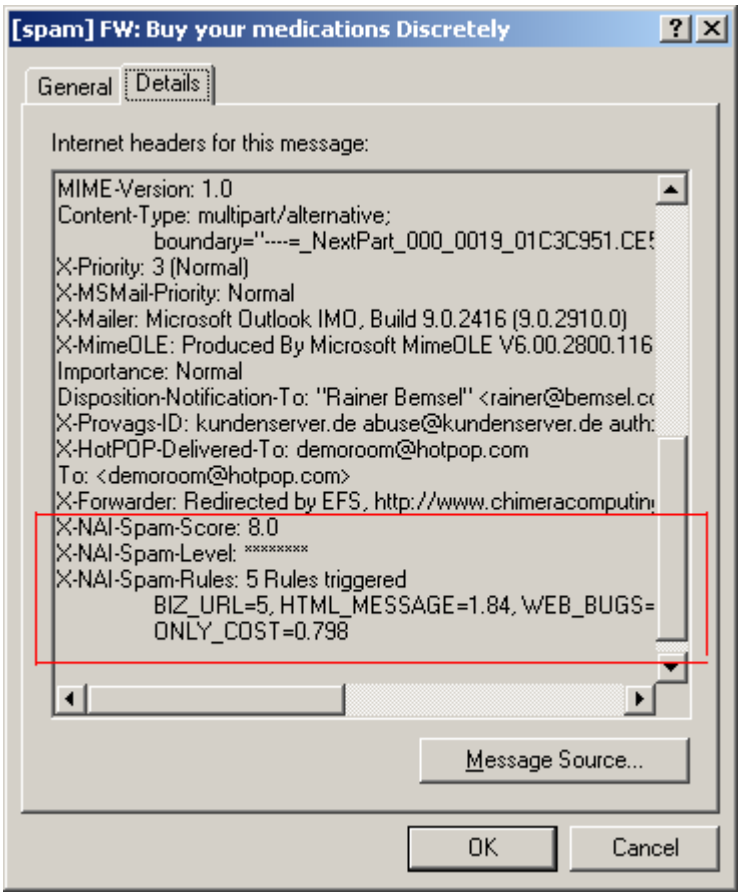


That's pretty much for the basics. I've sent a couple of caught spam mails to my demoroom Pop Account and run this scenario all the way through. On the next pages, you will see some screenshots of the positiv result.

Outlook Express Inbox View



Picking one of the emails, marked with SPAM. By verifying the properties, I could see all X-Headers, added by Spamkiller



With a setup similar to this, you can use a global Anti-Spam Solution, based on SMTP.