GFI MailEssentials for Exchange / SMTP 10.1 with free SPF support – overview

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article i will give you some information about the newest version of GFI MailEssentials 10.1 and how to setup the software with SPF integration. GFI is offering the SPF module as freeware.
GFI MailEssentials for Exchange/SMTP 10.1 is one of the first server based antispam solutions to fight against spam with the well known SPF technology.

Sender Policy Framework (SPF), formerly Sender Permitted From, is an extension to the SMTP standard. SPF makes it easy to counter most forged "From" addresses in email, and thus helps to counter e-mail spam. The combination is also called SMTP+SPF. SPF was originally designed by Meng Weng of POBOX. You can read more about POBOX here.

For more information about SPF, read my article at ww.msexchange.org and for general information about GFI MailEssentials 10.1 and it's SPF integration click here.

Let's begin

Before we start to install GFI MailEssentials and to configure the SPF option, i will give you some information about how SPF works and the GFI MailEssentials key features.

How does SPF work?

SPF is easy to understand. The "Internet" uses DNS (Domain Name System) to resolve Domain Names (as an example www.msexchange.org) into IP addresses. DNS is also used to direct requests for different services like e-mail and Web Servers. For every Domain around the world an MX (Mail Exchanger) record must exist. An MX record tells the e-mail sender where the target server for receiving mail is located.
SPF is publishing "reverse MX" records in DNS which tells the mail sender which machines send mail from the domain.
The recipient of the e-mail can now check these records to ensure that e-mail is coming from a „trusted" sender from this domain.
These "reverse MX" records can be easily published in DNS. It takes only one line in DNS to fullfil all requirements.

Key features of GFI MailEssentials

- ? Server based Anti spam
- ? Freeware SPF integration
- ? Company-wide disclaimer/footer text
- ? Mail archiving to a database
- ? Reporting

- ? Personalized server based auto replies with tracking
- ? POP3 downloader
- ? Mail monitoring
- ? List server (optional)
- ? Highest spam detection rate (98%) using Bayesian filtering
- ? Lowest false positives through a patented automatic whitelist feature and a tailored ham & spam database
- ? Allows users to review mail marked as spam from a folder in their own inbox
- ? Server-based, no client component
- ? Unbeatable pricing: $625 for 100 users, $1250 for unlimited users (as i wrote this article)

System requirements

GFI recommends the following when you install GFI MailEssentials on the Exchange 2000/2003 machine:

- ? Windows 2000/2003 Server or Advanced/Enterprise Server
- ? Microsoft Exchange 2000/2003
- ? Microsoft XML core service (when you want to use the GFI MailEssentials reporter)

GFI recommends the following when you install GFI MailEssentials on a separate machine:

- ? Windows 2000/XP Professional (only up to 10 inbound SMTP connections simultaneously), Windows 2000/2003 Server or Advanced/Enterprise Server
- ? IIS5 SMTP service installed and running as an SMTP relay to your mail server.
- ? Microsoft Exchange 4, 5, 5.5, 2000 oder 2003, Lotus Notes 4.5 and higher, or an SMTP/POP3 mail server.
- ? GFI MailEssentials must be the first server to receive e-mails. I will tell you why later in this article.

Attention:

For both deployment methods you **MUST** disable Anti Virus software from scanning the GFI MailEssentials & IIS directories.

Installation

First, we need to download a trial version of GFI MailEssentials from the GFI website. The download size is about 17,5 MB. You can use the trial version for 30 days. After that time, the software becomes a limited freeware version, unless you enter a 60-day eval key or the purchased license key.

After downloading start the setup by doubleclicking mailesentials101.exe and follow the setup instructions. The configuration of GFI MailEssentials 10.1 is out of the scope of this article.

Attention:

GFI MailEssentials will need to start & Stopp the Exchange services during installation.

Figure 1: Start the installation of GFI MailEssentials

You have two options for installing GFI MailEssentials:

- ? Installing GFI MailEssentials on the Exchange server 2000/2003 machine
- ? Installing GFI MailEssentials on a seperate machine

Installing GFI MailEssentials on the Exchange server 2000/2003 machine

This ist he easiest deployment method. Simply start the setup process and follow the setup instructions. This method is good for small and medium sized organizations which doesn't have a large server infrastructure with Frontend and Backend servers and a complex firewall/DMZ infrastructure. GFI recommends this installation method when you use Exchange 2000/2003.

Installing GFI MailEssentials on a separate machine

If you wish to separate the MailEssentials installation from the Exchange machine, you can install the software on a separate machine. You should prefer this installation method when you want to place the MailEssentials software on a server in your DMZ and to setup the MailEssential Server as a smart host / Mail relay server.

SPF configuration

My focus in this article is the configuration of the Sender Policy Framework settings on the GFI MailEssentials machine.

Attention:

SPF will only function correctly when the machine is configured to receive e-mails directly from the internet. If you have a configuration where e-mails arriving are beeing relayed through another smart host then the SPF checks will fail.
For more information read the following GFI knowledge base article.

Start the GFI MailEssentials SPF configuration by right clicking the „Sender Policy Framework" container – and click „Properties".
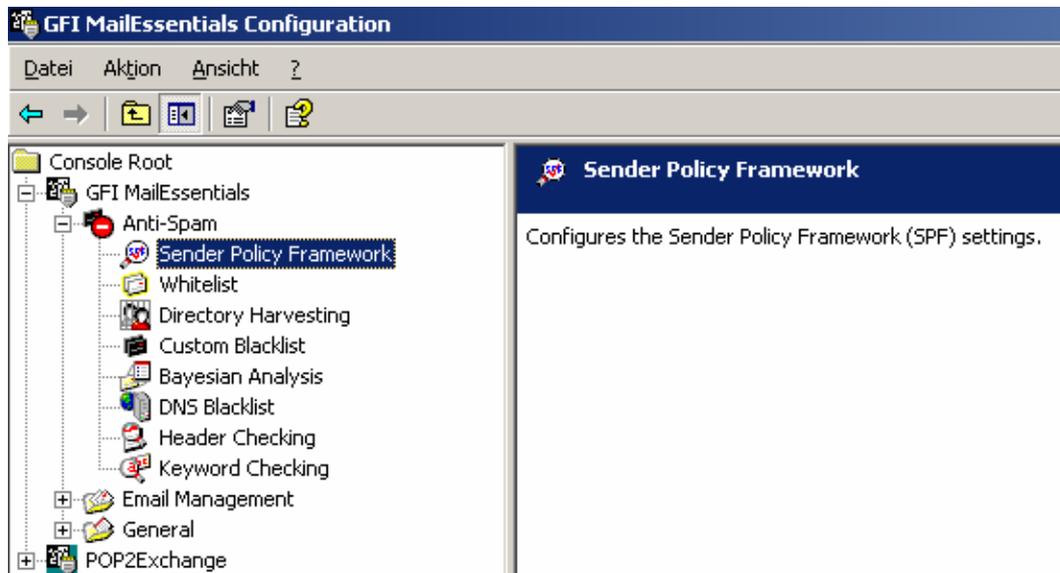

Figure 2: Start configuring the Sender Policy Framework settings

First, we have to setup the SPF Block level which defines how SPF should detect e-mails with forged senders. GFI recommends to set the level to „medium".

Explanation of the four levels:

Never
This setting doesn't block any messages. When you select this option SPF tests are not done for incoming e-mails.

Low
This setting blocks e-mails which are determined to have a forged sender.

Medium
The „medium" setting blocks e-mails which appear to have a forged sender. Choose this option when SPF should treat any messages that appears to have a forged sender as spam.

High
Blocks any message which is not proven to be from the sender. The „High" setting will treat all e-mails as spam with one execption: If it could be proven that the sender is not forged. GFI doesn't recommends to enable this setting because the majority of mail servers today doesn't have an SPF record.
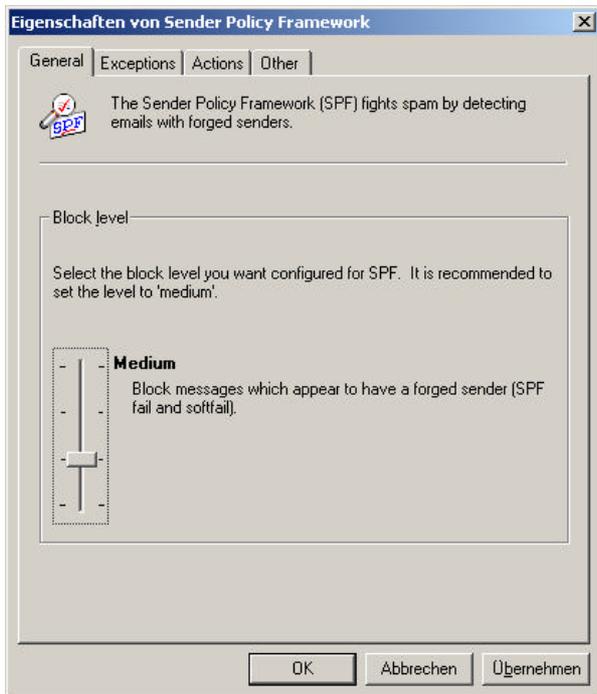
Figure 3: SPF Block level settings

The „Exceptions" field allows you to configure any IP addresses and recipients that should be excluded from SPF checks. This setting is useful when you want to allow special IP addresses and recipients which shouldn't be blocked.
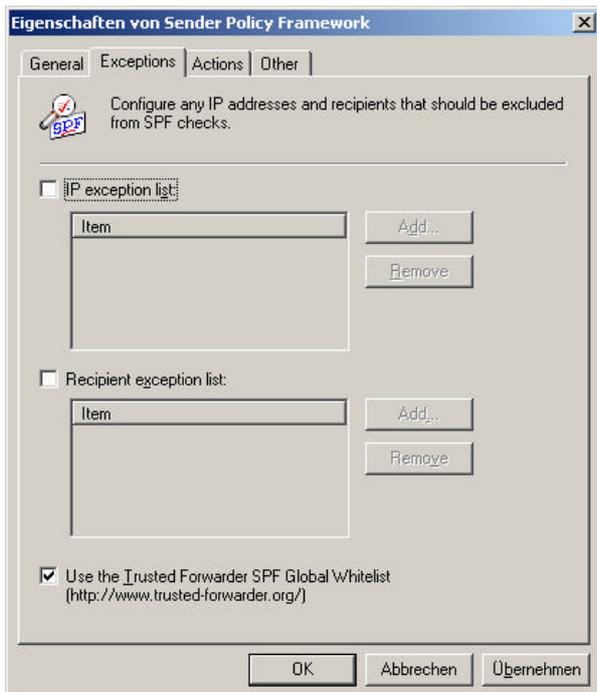

Figure 4: SPF exceptions settings

The Trusted Forwarder Global Whitelist (www.trusted-forwarder.org) provides a global whitelist for SPF users. This setting is useful because it provides a solution to allow legitimate email that is sent through well known and trusted e-mail forwarders from being blocked by SPF. This setting is enabled by default. GFI recommends to always leave this option enabled.

The „Actions" container allows you to configure the action to perform when a spam e-mail is detected. If you are using Exchange 2003, i recommend to select „Move to user's junk mail folder (Exchange 2003 only)". With this setting enabled, GFI MailEssentials forwards the spam mails to the user's junk mail folder. You have to activate this feature manually on the Exchange server. For more information about Exchange servers IMF options, read the following article written by Henrik Walther.
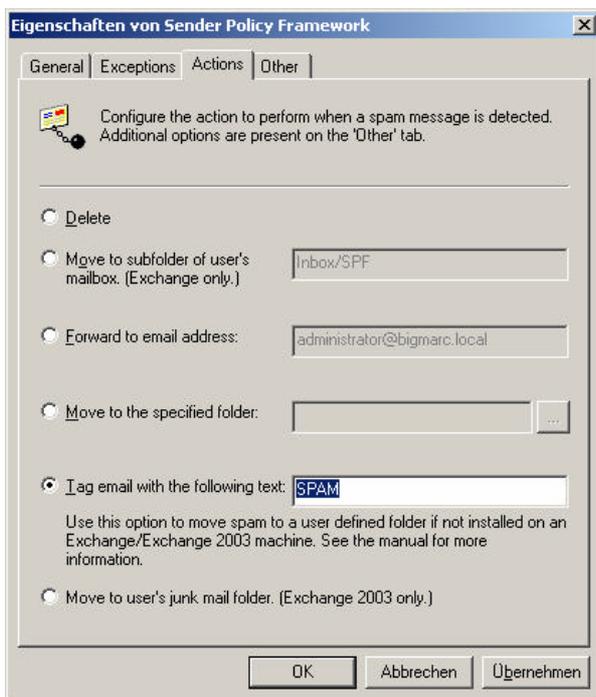

Figure 5: SPF Action settings

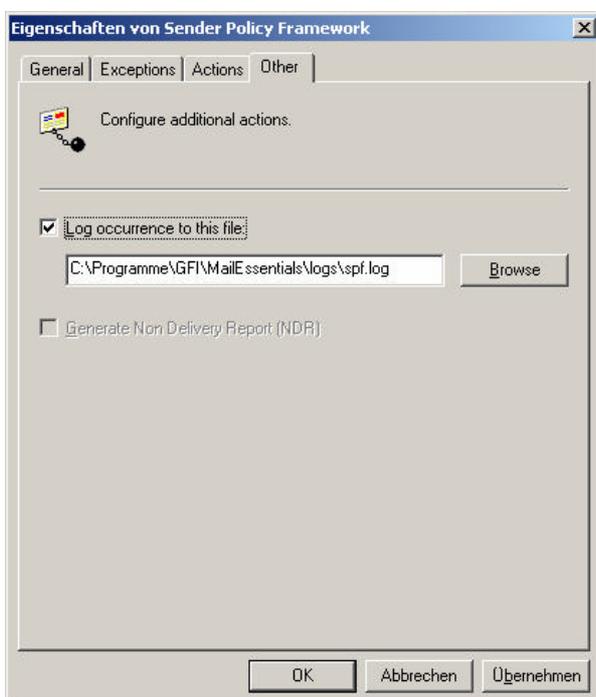The last option is to configure the logging of SPF settings.

Figure 6: SPF Log settings

Conclusion

GFI MailEssentials 10.1 is a great solution to fight against spam and one of the first vendors with SPF support. I love the product because GFI offers the SPF addon as freeware.

Related Links

General information about GFI
http://www.gfi.com/mes
GFI MailEssentials Download Link
http://www.gfi.com/downloads/downloads.asp?pid=11&lid=1
News about GFI MailEssentials 10.1
http://www.gfi.com/news/en/mes101launch.htm
SPF in general
http://spf.pobox.com
Free SPF Filter for Windows – bought by GFI
http://www.michaelbrumm.com/smtpspffilter.html