
GFI MailEssentials 10

Manual

By GFI Software Ltd.



<http://www.gfi.com>

E-mail: info@gfi.com

This manual was produced by GFI Software Ltd. Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI Software Ltd.

GFI MailEssentials was developed by GFI Software Ltd. GFI MailEssentials is copyright of GFI Software Ltd. © 1998-2004 GFI Software Ltd. All rights reserved.

GFI MailEssentials is a registered trademark and GFI Software Ltd. and the GFI logo are trademarks of GFI Software Ltd. in the Europe, the United States and other countries.

Version 10.1 last updated: September 28, 2004

Contents

Explaining GFI MailEssentials	1
Introduction to GFI MailEssentials.....	1
Key features of GFI MailEssentials	1
GFI MailEssentials components.....	2
Installing GFI MailEssentials	5
Introduction to installing GFI MailEssentials.....	5
Upgrading from GFI MailEssentials 9 To 10	6
Installing GFI MailEssentials on the Exchange 2000/2003 machine	6
Installing GFI MailEssentials on a separate machine	9
Entering your License key after installation.....	20
Installing the rule manager (sorts spam to junk folder)	20
The Bayesian anti-spam filter	25
Introduction	25
How the Bayesian spam filter works	25
Creating a tailor-made Bayesian word database	25
Creating the ham database (tailored to your company)	26
Creating the spam database	27
How the actual filtering is done	27
Why Bayesian filtering is better	27
What's the catch?	28
Training the Bayesian filter	28
Configuring the Bayesian filter.....	29
Updates	30
Actions.....	31
Configuring Anti-Spam	33
Introduction to Anti Spam	33
White list	34
Auto white list	34
White listed keywords.....	36
Directory harvesting.....	36
Custom Blacklist	37
DNS blacklists (DNSBL)	39
Actions – what to do with spam mail	40
Header checking.....	43
Keyword checking	47
Sender Policy Framework (SPF)	49
How SPF works	49
Configuring the SPF feature	50
Anti Spam global actions	53
Spam management from the user's point of view	55
Introduction	55
Reviewing spam mail.....	55
Adding senders to the white list.....	56

Adding senders to the blacklist.....	56
Adding discussion lists to the white list	56
Adding spam to the SPAM database	57
Adding HAM to the ham database	57
Securing access to the public folders.....	57
Configuring Public folder scanning via IMAP or MAPI	57
Creating a dedicated account to login via IMAP	58
Configuring the GFI AntiSpam folders so that posts are hidden	59
Configuring Disclaimers	61
Introduction to disclaimers.....	61
Configuring disclaimers	61
Configuring Auto replies	65
Introduction to auto replies	65
Configuring Auto replies	65
Configuring Mail Monitoring	69
Introduction to Mail monitoring	69
Configuring Mail monitoring.....	69
Enabling/Disabling mail monitoring	71
Configuring the list server	73
Introduction to list servers.....	73
Requirements of the list server feature	73
Creating a list.....	73
Newsletter properties.....	77
Creating a custom footer for the list	79
Setting permissions to the list.....	80
Adding subscribers to the list	81
Operating the newsletter list	81
Sending a newsletter	81
Subscribing to the list	81
Subscription process	81
Unsubscribing from the list	82
Adding a link to your web site.....	82
Creating a discussion list.....	82
Discussion list properties.....	84
Creating a custom footer for the list	84
Adding subscribers to the list	84
Importing subscribers to the list / Database structure	84
Installing the Message Queuing services (MSMQ) on Windows 2000	85
Configuring Mail Archiving	87
Introduction to Mail archiving.....	87
Configuring Mail archiving	87
Configuring the search page (AWI)	88
Securing the Archive Web Search Interface	91
Generating Mail Reports	95
Introduction	95
Configuring GFI MailEssentials reporter	95
Daily spam report	96
Anti Spam rules report.....	98
User usage statistics	99

Domain usage statistics.....	100
Mail server daily usage statistics.....	101
User communications.....	103
Miscellaneous options.....	104
Printing reports.....	105
Configuring POP3 downloading	107
Should you use POP3 or SMTP to receive mail?.....	107
Configuring the POP3 downloader.....	108
Dial up Connection options.....	110
Miscellaneous options	113
General node.....	113
The GFI MailEssentials monitor.....	113
Configuring a fake Non Delivery Report (NDR).....	113
Adding additional local domains.....	114
Remote commands.....	114
Using remote commands.....	116
Examples.....	117
Remote command logging.....	118
Troubleshooting	121
Introduction.....	121
Knowledgebase.....	121
Request support via e-mail.....	121
Request support via web chat.....	122
Request support via phone.....	122
Web Forum.....	122
Build notifications.....	122
Index	123

Explaining GFI MailEssentials

Introduction to GFI MailEssentials

GFI MailEssentials offers server based anti spam and other key corporate e-mail features for your mail server. Installed as an add-on to your mail server, GFI MailEssentials is totally transparent to your users - no additional user training or administration is needed.

Key features of GFI MailEssentials

Server based Anti spam

With fraudulent, inappropriate and offensive emails being delivered in vast quantities to adults, children and businesses every day, spam protection is an essential component of your network's security strategy. Spam wastes network users' time and network resources, and can be dangerous too. GFI MailEssentials includes an advanced anti-spam module that includes blacklist/white lists, a Bayesian filter, keyword checking and header analysis.

Company-wide disclaimer/footer text

Because companies are effectively responsible for the content of their employees' email messages, it is wise to add a disclaimer to each outgoing email. This disclaimer/footer text can also be used to add a standard corporate message to each email, such as an address or company slogan. Although most employees have their own personal signature, the disclaimer/footer text ensures that the corporate message is always communicated. Disclaimers can be added to the top or the bottom of a mail. In addition, you can include fields/variables in the disclaimer, for example a recipient name or email. This way you can personalize the disclaimer towards the recipient.

Mail archiving to a database

With GFI MailEssentials, you can archive all in- and outbound Internet mail. This allows you to keep a back up of all email communications and easily search for a required message, such as a particular customer's emails. This also enables you to check the content of messages and quality of responses.

Reporting

GFI MailEssentials includes a reporting module that allows you to create reports on Internet mail use, including: daily statistics report, detailed log of sent, reports per user or by date range. These reports can be used for costing purposes.

Personalized server-based auto replies with tracking number

Auto replies can be more than just an 'out of office' reply. With automatic replies, you can let your customers know that their email has been received and that their request is being handled. GFI MailEssentials assigns a unique tracking number to each reply to give your customers and employees an easy point of reference.

POP3 downloader

Some mail servers, such as Exchange Server and Lotus Notes, are unable to download mail from POP3 mailboxes. GFI MailEssentials includes a utility that can forward and distribute mail from POP3 mailboxes to mailboxes on your mail server.

Mail monitoring

The mail monitoring feature allows you to send a copy of mails sent to or from a particular local email address or domain, enabling you to keep a central store of e-mail communications of a particular person or department. Because you can configure the mail to be copied to an email address, all e-mail can be stored in an Exchange or Outlook store, so that you can easily search for e-mail.

List server (Optional)

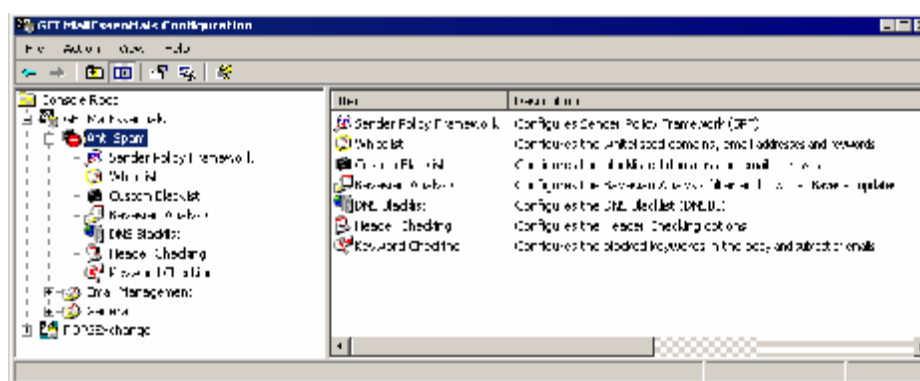
GFI MailEssentials includes a full blown list server, which allows you to easily setup newsletter distribution lists or discussion lists.

GFI MailEssentials components

GFI MailEssentials consists of the following parts:

GFI MailEssentials mail sink

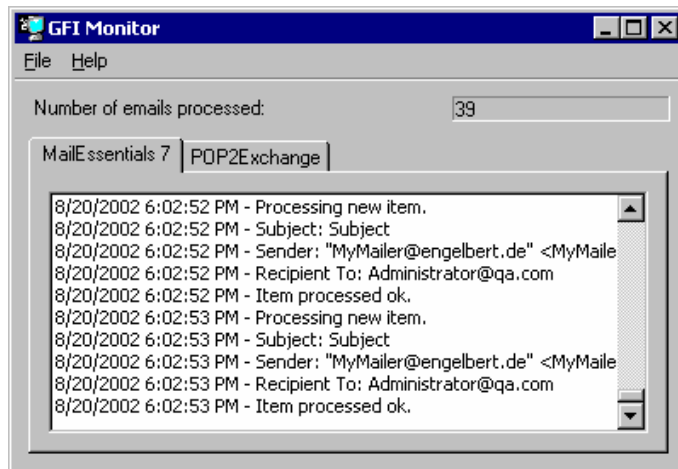
The mail sink installs on the Windows IIS SMTP service and analyses all in- and outbound mail.



Screenshot 1 - GFI MailEssentials configuration

GFI MailEssentials configuration

The configuration program allows you to set up and configure GFI MailEssentials. All configuration can be done from the new MMC console.



Screenshot 2 - GFI Monitor

GFI MailEssentials monitor

This program allows you to monitor the activity of GFI MailEssentials. The POP collector service can be monitored from the POP2Exchange tab.

GFI MailEssentials list server service

The list server is a separate application and runs as a service in the background

GFI MailEssentials attendant service

This service handles a number of GFI MailEssentials tasks and processes.

Installing GFI MailEssentials

Introduction to installing GFI MailEssentials

This chapter explains the procedure how to install and configure GFI MailEssentials. GFI MailEssentials can be installed in 2 ways:

Installation option 1: Installing GFI MailEssentials on the Exchange server 2000/2003 machine

This is a very straightforward and easy deployment mode. Simply install GFI MailEssentials on the Exchange Server 2000/2003 machine. Go to the paragraph 'Installing GFI MailEssentials on the Exchange 2000/2003 machine' for instructions how to install this deployment option.

Note: This installation option allows you to direct mail marked as spam directly to the user's junk mail folder. This makes it easy for users to periodically review spam mail for false positives. If you install GFI MailEssentials in the DMZ, or in front of Exchange 2000/2003, this feature will not be available.

Installation option 2: Installing GFI MailEssentials on a separate machine

If you are not running Exchange 2000/2003 or simply wish to separate the MailEssentials install from the Exchange 2000/2003 machine, you can install MailEssentials on a separate machine. This also allows you to keep your corporate mail server behind the firewall. GFI MailEssentials will act as a smart host/mail relay server in the perimeter network (also known as DMZ, demilitarized zone, and screened subnet).

Additional advantages are:

- You can perform maintenance on your Mail server machine, whilst still receiving email from the Internet.
- You use less resources on your Mail server machine
- The GFI MailEssentials machine can have a lower spec then the Mail server machine and process mail faster
- Additional fault tolerance – if anything happens with your Mail server you still receive mail, which is queued on the GFI MailEssentials machine.

Note: This separate machine does not need to be dedicated to GFI MailEssentials; it can be running other applications, such as GFI MailSecurity.

If you choose this option, you have to configure IIS before installing GFI MailEssentials. Go to the paragraph 'Installing GFI MailEssentials on a separate machine' for instructions how to do this.

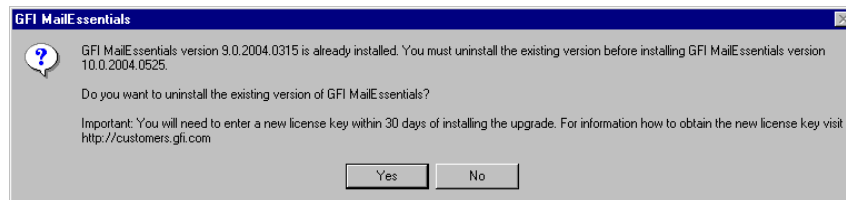
IMPORTANT: Don't judge GFI MailEssentials' spam detection rate until you have allowed the Bayesian filter to run for at least 1 week! GFI MailEssentials can achieve the highest detection rate compared to other anti-spam solutions because it adapts specifically to your mail. Be patient and wait at least a week before you judge it!

Upgrading from GFI MailEssentials 9 To 10

This section applies only to GFI MailEssentials 9 users! Note that an upgrade can not be un-done: I.e. you can not revert back to version 9 once you have installed the upgrade.

If you are currently using GFI MailEssentials 9, you can upgrade your current installation. All version 9 configuration settings will be kept. You will need to enter a new license key within 30 days of installing the upgrade. For information how to obtain the new license key visit <http://customers.gfi.com>.

To upgrade:



Screenshot 3 - Confirm the upgrade

1. Launch the GFI MailEssentials 10 set-up file on the machine on which you have installed GFI MailEssentials 9. Set-up will prompt you whether you wish to remove GFI MailEssentials 9 and install GFI MailEssentials 10.
2. Set-up will now proceed to install GFI MailEssentials 10 in exactly the same manner as a new install (for a detailed description see this chapter). However it will not let you change the destination folder.
3. After set-up has copied the files, set-up will notify you that it will convert the Bayesian weights file to the new GFI MailEssentials 10 format. The new format is more compact and uses less memory. This process may take a while, therefore a progress dialog box is shown.
4. Once the conversion is ready, set-up will show the standard Finish dialog. Click Finish to complete the upgrade.

Installing GFI MailEssentials on the Exchange 2000/2003 machine

This is the recommended mode if you have Exchange 2000/2003!

System requirements

- Windows 2000/2003 Server or Advanced Server
- Microsoft Exchange server 2000/2003
- If using the GFI MailEssentials reporter, Microsoft XML core services is required. This is included in the GFI MailEssentials installation and will be installed automatically if your operating system is UK/US English.

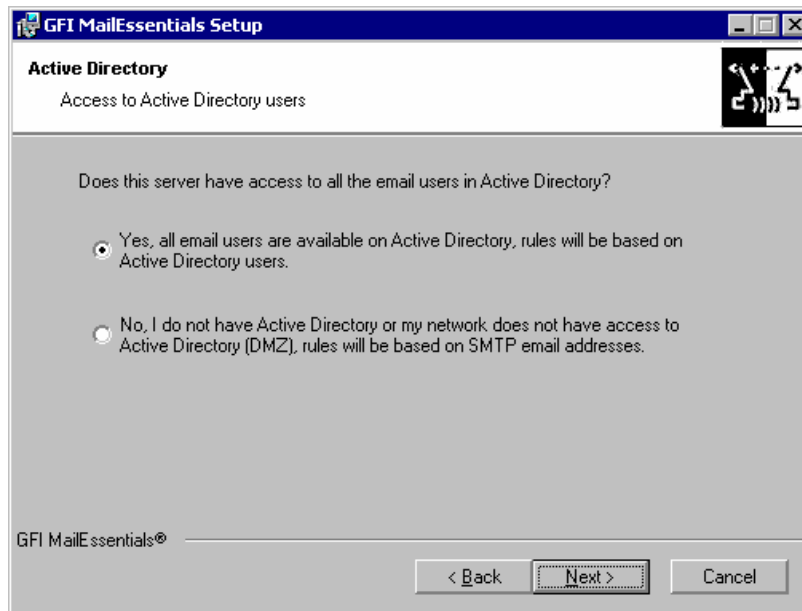
- **IMPORTANT:** Disable Anti Virus software from scanning the GFI MailEssentials & IIS directories! AV products are known to both interfere with normal operation as well as slow down any software which requires file access. In fact Microsoft does not recommend running file based anti virus software on the Exchange Server. For more information: <http://kbase.gfi.com/showarticle.asp?id=KBID001824>
- Make sure that backup software is not backing up any of the GFI MailEssentials directories at any point.
- **For list server only:** The list server feature requires the installation of Microsoft Message Queuing Services. This is a scalable event processing system service developed by Microsoft. It is included with every Windows 2000/2003 and XP version, although not always installed by default. For more information how to install it, please see the chapter 'Configuring the list server' If you do not plan to use the list server feature, you do not need to install Microsoft MSMQ.

Note: If you have a cluster please check this kbase article prior to installation: <http://kbase.gfi.com/showarticle.asp?id=KBID001639>

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

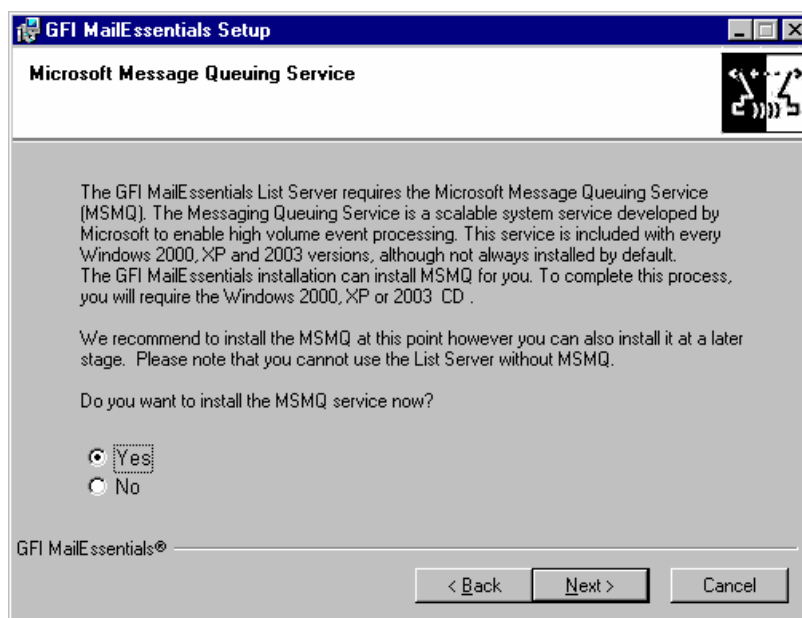
Running GFI MailEssentials set-up

1. On the Exchange machine, Log-on as administrator and run GFI MailEssentials set-up by double-clicking the file **me.exe**. A welcome dialog will appear. Close other Windows programs and click **Next**. GFI MailEssentials will prompt you to check for a later GFI MailEssentials version. Always use the latest version!
2. Read and confirm the License agreement, click Next.
3. Set-up will now ask you where you want GFI MailEssentials to be installed. GFI MailEssentials will need approximately 70 MB of free hard disk space. In addition to this, you must reserve approximately 200 MB for temporary files.
4. Now enter your Name, company, and License key. If you are evaluating the product, leave the default 'Evaluation'. Click **Next**.
5. Set-up will ask you for the administrator e-mail. This e-mail will be used to send critical notifications.



Screenshot 4 - Selecting SMTP mode or Active Directory mode

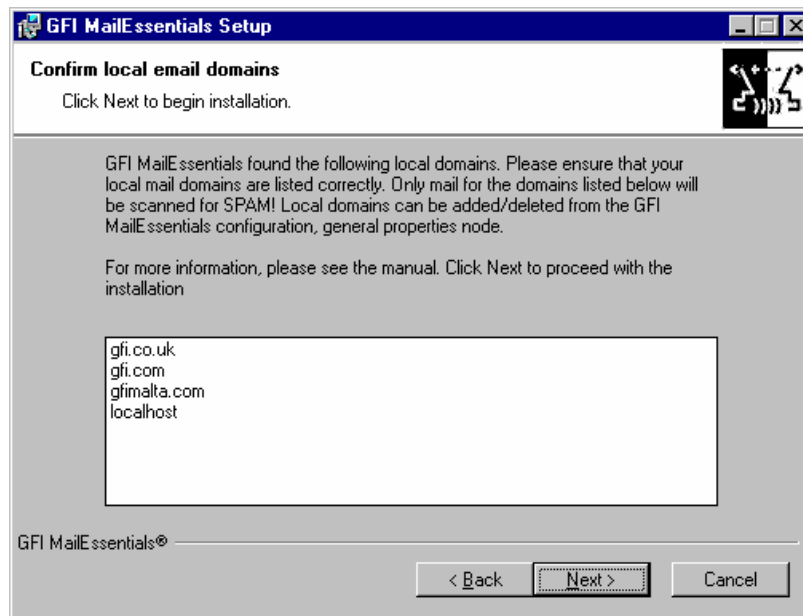
6. If you are installing GFI MailEssentials on an Exchange server configured as a front end server (i.e. in a DMZ in front of another Exchange Server), you can choose whether you want to install GFI MailEssentials in Active Directory mode or in SMTP mode. Active Directory mode allows you to select users present in Active Directory for user based configuration/rules, such as a disclaimer. However, on a front end server not all users are available. In this case its better to select SMTP mode, which allows you to input the SMTP email address for user based configuration/rules.



Screenshot 5 - Installing Microsoft Message Queuing Service

7. If you do not have Microsoft Message Queuing Services (MSMQ) installed, set-up will ask you whether you wish to install it. The list server feature requires this service. Microsoft Message Queuing Service is a scalable event processing system service developed by Microsoft. It is included with every Windows 2000/2003 and XP

version, although not always installed by default. If you do not plan to use the list server feature, or if you wish to install it later, you can click 'No' to continue set-up. If you click 'Yes' you will be prompted for the Windows CD and set-up will launch the MSMQ set-up.



Screenshot 6 - Configure your local domain

8. Set-up will now confirm the local email domains (e.g. mycompany.com) that you have configured. It retrieves the local domains from your IIS/Exchange set-up. Its important to ensure that your local domains are listed correctly. **MailEssentials will ONLY filter mail destined for your local domain** – therefore if you do not configure your local email domain correctly no spam will be detected! You can change these local email domains at a later stage from the GFI MailEssentials configuration.

9. Set-up will now copy all program files to the selected destination, and finish the installation by creating a GFI MailEssentials program group. Click **Finish** to finish setup. After setup has copied all the files, it will ask if it can restart the SMTP service.

10. After installation set-up will check if you have the Microsoft XML engine installed. If you don't, and you are running a US/UK version of Microsoft Windows it will install it for you. If you are NOT running a UK/US version of windows, set-up will prompt you to download and install the appropriate Microsoft XML engine. The XML engine is used by the reporter application and is only 2 megabytes. It is most likely to be used by other applications too. For more information check

<http://kbase.gfi.com/showarticle.asp?id=KBID001584>

Installing GFI MailEssentials on a separate machine

If you install GFI MailEssentials on a separate machine, you must ensure it is the first to receive all mails destined for your mail server and the last 'stop' for outbound mail. In order for this to happen, GFI MailEssentials must act as a gateway for all email. This set-up is also known as 'Smart host' or 'Mail relay' server. Effectively GFI MailEssentials will act as a **mail relay server**.

System requirements

- Windows 2000/2003 - Pro, Server or Advanced Server or Windows XP Professional. (Note that if you use Windows 2000 Pro or XP, you will only be able to accept up to 10 inbound SMTP connections simultaneously, so its better to use Windows 2000/2003 server)
- IIS5 SMTP service installed and running as an SMTP relay to your mail server. This means that the MX record of your domain must be pointing to the machine on which you will install GFI MailEssentials. For more information about configuring IIS5: <http://support.microsoft.com/support/kb/articles/Q293/8/00.ASP>
- Microsoft Exchange server 2000, 2003, 4, 5 or 5.5, Lotus Notes 4.5 and up, or an SMTP/POP3 mail server.
- **IMPORTANT:** Disable Anti Virus software from scanning the GFI MailEssentials & IIS directories! AV products are known to both interfere with normal operation as well as slow down any software which requires file access. In fact Microsoft does not recommend running file based anti virus software on the Exchange Server. For more information: <http://kbase.gfi.com/showarticle.asp?id=KBID001824>
- Make sure that backup software is not backing up any of the GFI MailEssentials directories at any point.
- **For list server only:** The list server feature requires the installation of Microsoft Message Queuing Services. This is a scalable event processing system service developed by Microsoft. It is included with every Windows 2000/2003 and XP version, although not always installed by default. For more information how to install it, please see the chapter 'Configuring the list server' If you do not plan to use the list server feature, you do not need to install Microsoft MSMQ.

Installing & configuring IIS SMTP service

GFI MailEssentials uses the Windows IIS SMTP service as its SMTP server. Because GFI MailEssentials works with this SMTP service, you need to configure this service as a mail relay server first.

About the Windows IIS SMTP service

The Windows SMTP service is part of IIS, which is part of Windows 2000/2003. It is used as the message transfer agent of Microsoft Exchange Server, and has been designed to handle large amounts of mail traffic. The Windows IIS 5 SMTP service is included in every Windows distribution, including Windows professional.

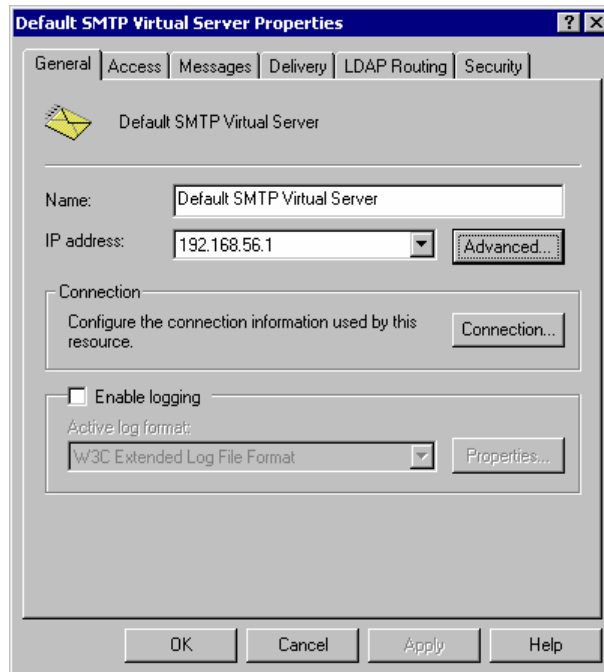
Note: If you have a cluster please check this kbase article prior to installation: <http://kbase.gfi.com/showarticle.asp?id=KBID001639>

To install & configure the IIS SMTP service as a mail relay server:

Step 1: Verify the Installation of the SMTP Service

In Control Panel, open Add/Remove Programs, click Add/Remove Windows Components. Click the Internet Information Services (IIS) component, click Details, and then verify that the SMTP Service check

box is selected. If it is not selected, click to select it, click OK, and then follow the installation directions that are displayed.



Screenshot 7- Specify mail relay server name and assign IP

Step 2: Specify mail relay server name and assign an IP

1. Click Start, point to Programs, click Administrative Tools, and then click Internet Services Manager.
2. Expand the tree under the server name, and then expand the Default SMTP Virtual Server. Right click and select 'Properties'. Assign an IP to it.

Step 3: Configure the SMTP Service to relay mail to your mail server

In this step, you configure the SMTP service to relay inbound messages to your mail server.

Note: During installation, GFI MailEssentials will perform this step for you automatically. GFI MailEssentials will ask for your local domain name, and create it as a remote domain. You will see the domain listed in the right pane. However, if you do this step manually, you can confirm that your relay server is working properly before running the GFI MailEssentials installation.

Creating a local domain in IIS to route mail

1. Click Start, point to Programs, click Administrative Tools, and then click Internet Services Manager.
2. Expand the tree under the server name, and then expand the Default SMTP Virtual Server. By default, you should have a Local (Default) domain with the fully qualified domain name of the server.
3. Configure the domain for inbound:

1. Right-click the Domains icon, click New, and then click Domain.
2. Click Remote, click Next, and then type the domain name in the Name box. Click Finish.



Screenshot 8 - Configure the domain

IMPORTANT NOTE ABOUT LOCAL EMAIL DOMAINS

Ensure that you add all your local email domains (e.g. mycompany.com), otherwise inbound mail will not be filtered for spam!

Note: Upon installation, MailEssentials will import local email domains from the IIS SMTP service. If you want add additional local email domains, you have to add these local domains in the MailEssentials configuration. For more information see 'Adding additional local domains' in the Misc. chapter.

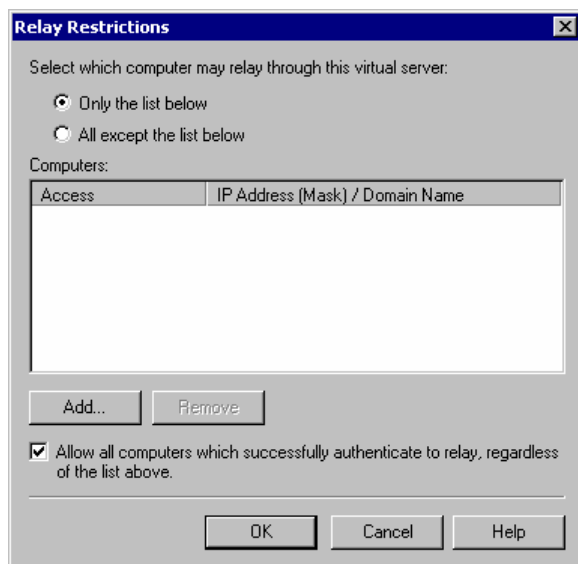
If you add additional local domains in IIS SMTP service, they will not be automatically recognized until you enter them in the MailEssentials configuration. This allows you to setup remote smart hosts for particular domains that are not local.

Configure the domain to relay mail to your mail server:

1. In the properties for the domain that you just created, click to select the Allow the Incoming Mail to be Relayed to this Domain check box.
2. If this is being set up for an internal domain, you should specify the server that receives email for the domain name by the IP address in the Route domain dialog box.
3. Click the forward all email to smart host option, and then type the IP address of the server that is responsible for email for that domain in square brackets. For example:
[123.123.123.123]

Note: Typing the IP address of the server in brackets is necessary so that the server recognizes this is an IP address and not to attempt a DNS lookup.

4. Click OK.



Screenshot 9 - Relay options

Step 4: Secure your mail relay server.

In this step you will specify your mail server name, and any other mail servers that will send mail via this mail relay server. Effectively you will limit the servers that can send mail to the internet through this server. If you don't create restrictions anyone can use your mail relay server as an open relay (i.e. Spamming). To prevent this:

1. Open the properties of the Default SMTP Virtual Server.
2. On the Access tab, click Relay.
3. Click Only the list below, click Add, and then add the IP of your mail server that will be forwarding the mail to this server. You can specify a single computer, group of computer or a domain:
 - a) Single computer: Specify one particular host that you want to relay off of this server. If you click the DNS Lookup button, you can lookup an IP address of a specific host.
 - b) Group of computers: Specify a base IP address for the computers that you want to relay.
 - c) Domain: Select all of the computers in a domain by domain name that will openly relay. This option adds processing overhead, and might reduce the SMTP service performance because it includes reverse DNS lookups on all IP addresses that try to relay to verify their domain name.

Step 5: Configure your mail server to relay mail via the mail relay server

After you have configured the IIS SMTP service to send and receive mail, you must configure your mail server to relay all mail to the mail relay server. To do this;

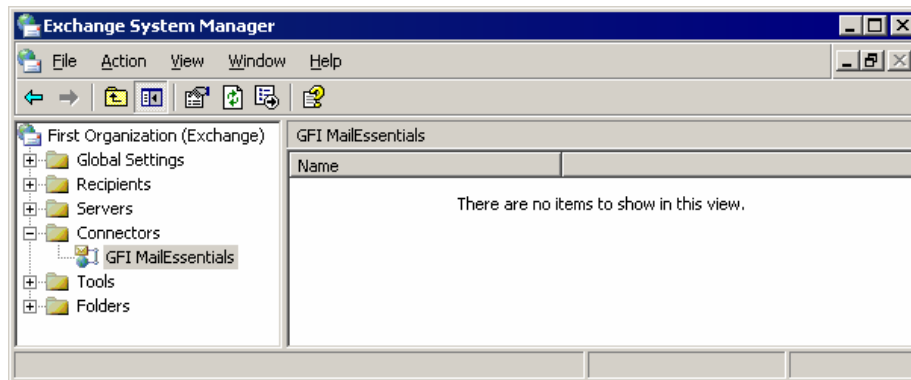
If you have Microsoft Exchange Server 4/5/5.5:

1. Start up **Microsoft Exchange Administrator**.
2. Go to the **Internet Mail Service** and double-click on it to configure its properties.
3. Go to the **Connections** tab.
4. Message Delivery section, select 'Forward all messages to host'. Enter the computer name or IP of the machine running GFI MailEssentials.
5. Click OK and restart Exchange server. This can be done from the services applet.

If you have Microsoft Exchange Server 2000/2003:

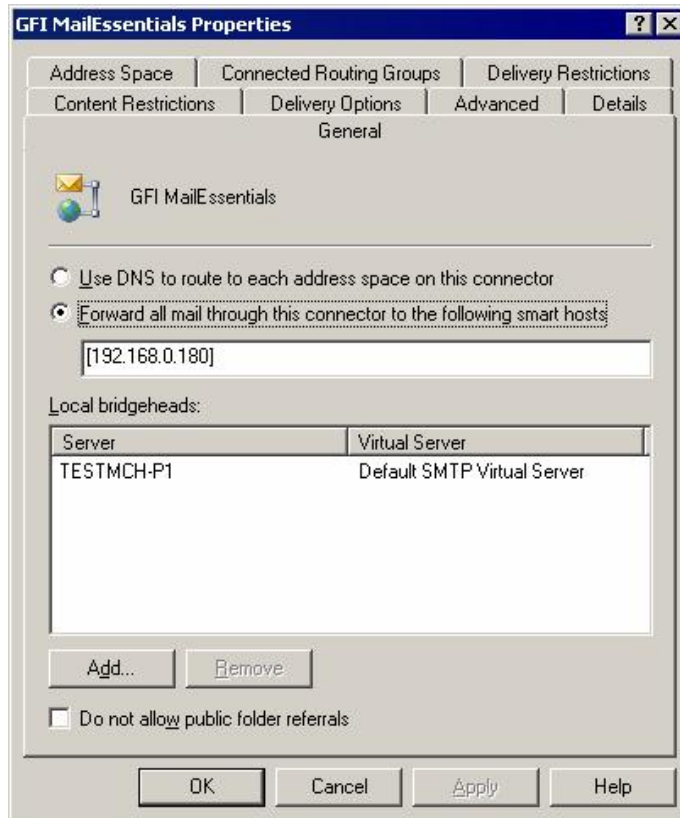
You will need to set-up an SMTP connector that forwards all mail to GFI MailEssentials:

1. Start up Exchange System Manager



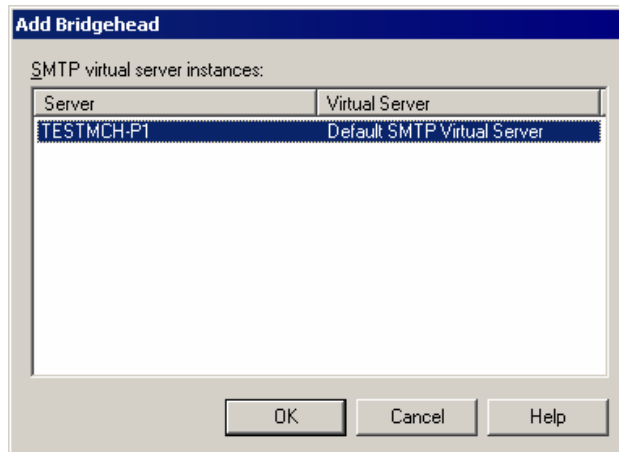
Screenshot 10 - Forwarding mail to GFI MailEssentials machine

2. Right-click on the Connectors Node->New->SMTP Connector and create a new SMTP connector. You will be prompted for a name.



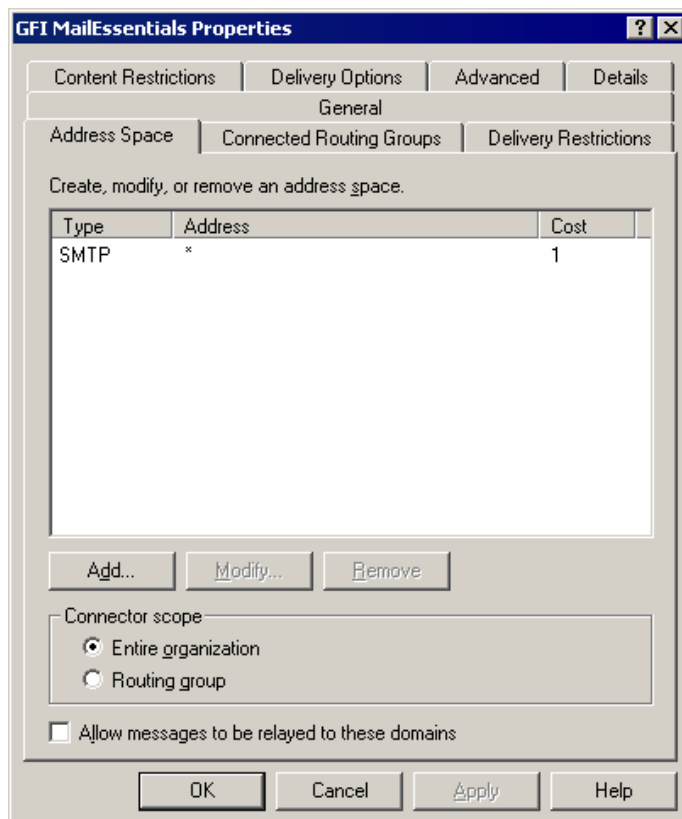
Screenshot 11 - Specifying IP of GFI MailEssentials machine

- Now select the option "Forward all mail through this connector to the following smart host", and type in the IP of the GFI MailEssentials server (the mail relay server) enclosed within square brackets [] (e.g.: [100.130.130.10]).



Screenshot 12 - Adding a bridgehead

- Now click on the 'Add' button in the local bridgeheads section, and select the appropriate virtual SMTP Server instances that you want to forward mail for.



Screenshot 13 - Adding SMTP as address space

5. Go to the Address Space tab, and click Add. Select SMTP and click OK.
6. Click OK to exit. All mails will now be forwarded to the GFI MailEssentials machine.

If you have Lotus Notes or an SMTP/POP3 server:

Check the mail server documentation how to forward mail to the GFI MailEssentials machine.

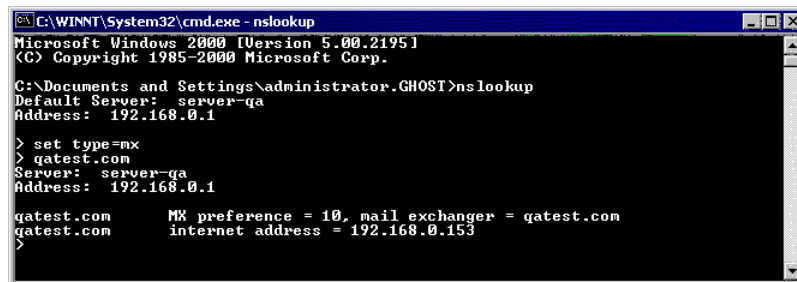
Step 6: Point the MX record of your domain to the mail relay server.

Since the new mail relay server must receive all inbound mail first, you must update the MX record of your domain to point to the IP of the new mail relay server. Otherwise mail will continue to go to your mail server and by-pass GFI MailEssentials.

If you run your own DNS server you need update this in your DNS server. If your ISP manages it for you, you need to ask your ISP to update the MX record for you. After you have done this, check if the MX record is correct using the following procedure.

Checking if the MX record for your domain is set correctly

1. Open command prompt. Type nslookup
2. Now type 'set type=mx'
3. Enter your mail domain.
4. The MX record should return a single IP. This IP must be the mail relay server!



```
C:\WINNT\System32\cmd.exe - nslookup
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator.GHOST>nslookup
Default Server:  server-qa
Address: 192.168.0.1

> set type=mx
> gatest.com
Server:  server-qa
Address: 192.168.0.1

gatest.com      MX preference = 10, mail exchanger = gatest.com
gatest.com      internet address = 192.168.0.153
>
```

Screenshot 14 - Checking the MX record of your domain

Note: If you wish to send out mail using a smart host (used when using dial-up) or receive mail using ETRN, you will need to perform additional steps to configure IIS 5 as a mail relay server. For more information refer to the IIS 5 documentation.

Step 7: Test your new mail relay server!

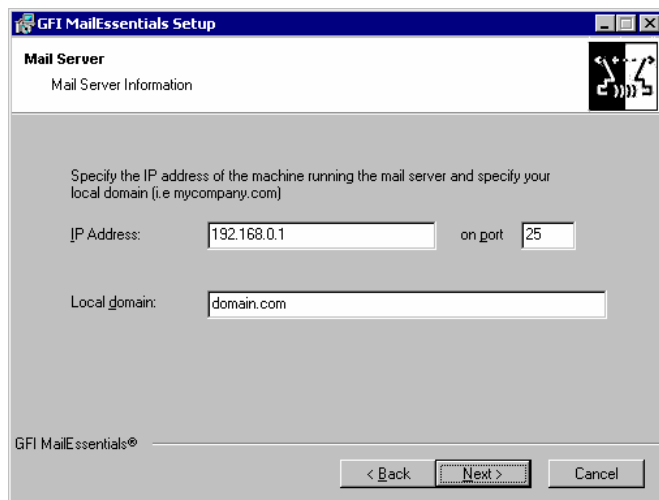
Before you proceed to install GFI MailEssentials, verify that your new mail relay server is working correctly.

1. Test IIS 5 SMTP inbound connection of your mail relay server by sending a mail from an external account to an internal user (you can use hotmail, if you don't have an external account available). Verify that the mail client received the email.
2. Test IIS 5 SMTP outbound connection of your mail relay server by sending a mail to an external account from an internet email client. Verify that the external user received the email.

Note: Instead of using an email client, you can use Telnet and manually send an email. This will give you more troubleshooting information. Here is the link to the Microsoft KB article how to do it: <http://support.microsoft.com/support/kb/articles/Q153/1/19.asp>

Step 8: Running GFI MailEssentials set-up

1. On the newly configured mail relay machine, Log-on as administrator and run GFI MailEssentials set-up by double-clicking the file **me.exe**. A welcome dialog will appear. Close other Windows programs and click **Next**. GFI MailEssentials will prompt you to check for a later GFI MailEssentials version. Always use the latest version!
2. Read and confirm the License agreement, click Next.
3. Set-up will now ask you where you want GFI MailEssentials to be installed. GFI MailEssentials will need approximately 70 MB of free hard disk space. In addition to this, you must reserve approximately 200 MB for temporary files.
4. Now enter your Name, company, and License key. If you are evaluating the product, leave the default 'Evaluation'. Click **Next**.



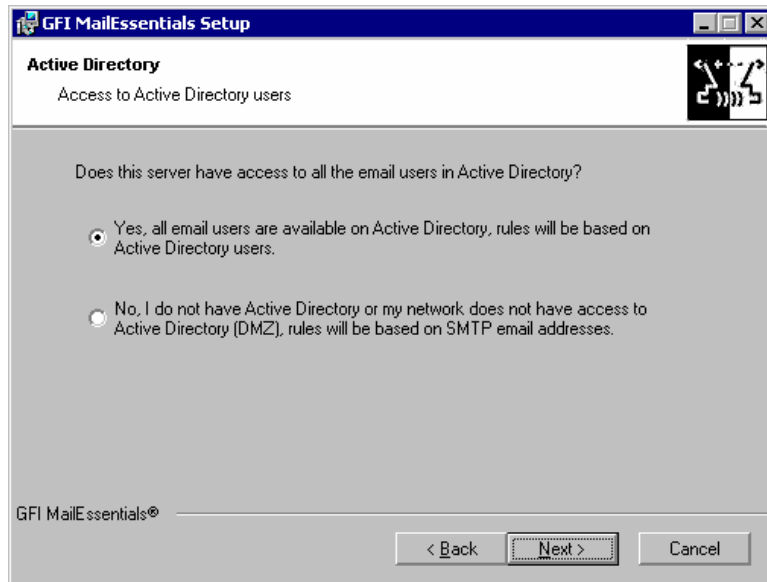
Screenshot 15 - Specify mail server IP & domain

5. Set-up will now ask you to specify your mail server IP, port and your local domain:

- Specify the IP of your Mail server (e.g. Exchange server name) and the port of the mail server
- Specify your local domain.

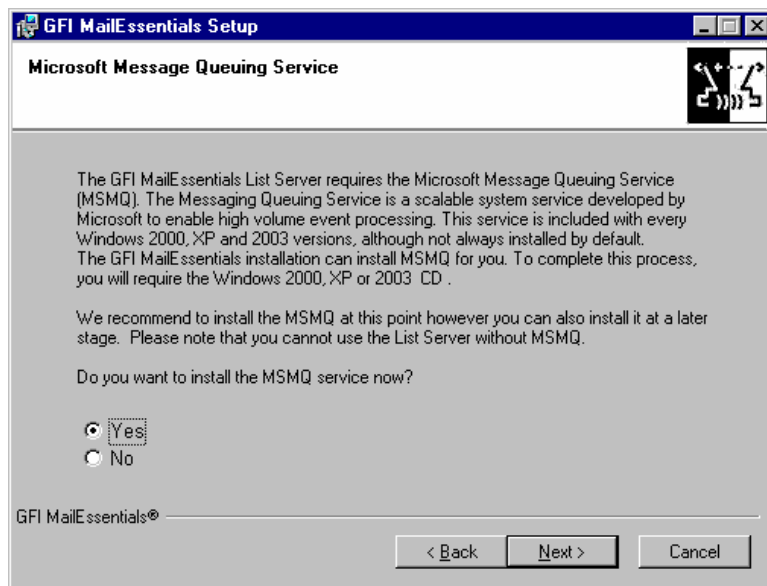
The local domain is the last part of your internal e-mail address, for example gfi.com.

6. Set-up will ask you for the administrator e-mail. This e-mail will be used to send critical notifications.



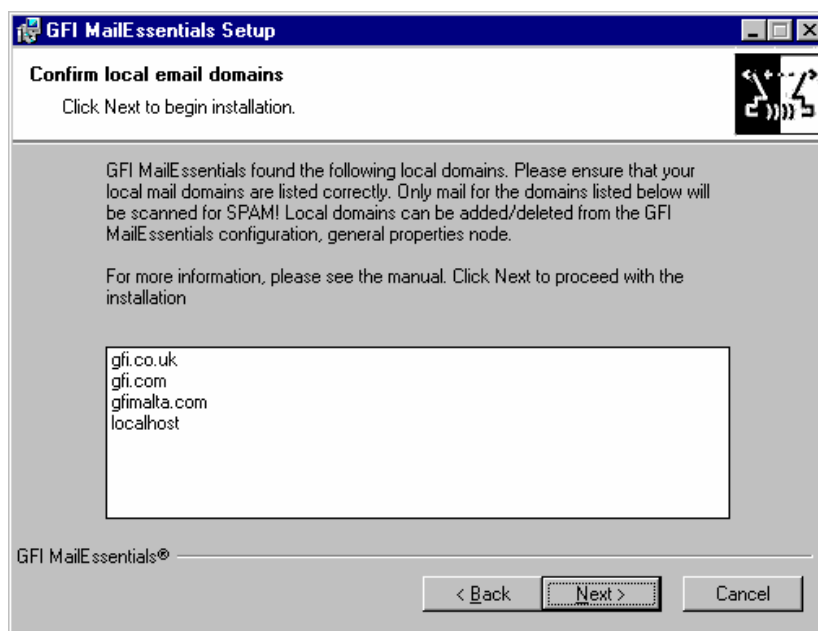
Screenshot 16 - Selecting SMTP mode or Active Directory mode

If you are installing GFI MailEssentials on a machine that is part of a domain and has Active Directory, set-up will ask you whether you want to install in Active Directory mode or in SMTP mode. Active Directory mode allows you to select users present in Active Directory for user based configuration/rules, such as a disclaimer. However, if your machine is in the DMZ, then it's better to select SMTP mode. In this mode all user based configuration/rules will require you to input the SMTP email address.



Screenshot 17 - Screenshot 15- Installing Microsoft Message Queuing Service

7. If you do not have Microsoft Message Queuing Services (MSMQ) installed, set-up will ask you whether you wish to install it. The list server feature requires this service. Microsoft Message Queuing Service is a scalable event processing system service developed by Microsoft. It is included with every Windows 2000/2003 and XP version, although not always installed by default. If you do not plan to use the list server feature, or if you wish to install it later, you can click 'No' to continue set-up. If you click 'Yes' you will be prompted for the Windows CD and set-up will launch the MSMQ set-up.



Screenshot 18 - Confirm your local domain

8. Set-up will now confirm the local domains that you have configured. It retrieves the local domains from your IIS set-up. Its important to ensure that your local domains are listed correctly. **MailEssentials will ONLY filter mail destined for your local domain** – therefore if you do not configure your local domain correctly no spam will be

detected! You can change these local email domains at a later stage from the GFI MailEssentials configuration.

9. Set-up will now copy all program files to the selected destination, and finish the installation by creating a GFI MailEssentials program group. Click **Finish** to finish setup. After setup has copied all the files, it will ask if it can restart the SMTP service.

10. After installation set-up will check if you have the Microsoft XML engine installed. If you don't, and you are running a US/UK version of Microsoft Windows it will install it for you. If you are NOT running a UK/US version of windows, set-up will prompt you to download and install the appropriate Microsoft XML engine. The XML engine is used by the reporter application and is only 2 megabytes. It is most likely to be used by other applications too. For more information check

<http://kbase.gfi.com/showarticle.asp?id=KBID001584>

If you have IIS services running, GFI MailEssentials will need to stop these services during installation to install certain files. After it has done that, it will offer to restart these services.

Entering your License key after installation

If you have purchased GFI MailEssentials, you can enter your License key in the General > Licensing node.

If you are evaluating GFI MailEssentials, it will time out after 60 days (with evaluation key). If you then decide to purchase GFI MailEssentials, you can just enter the License key here without having to re-install.

You must license MailEssentials for the amount of users that you have on your mail server.

Entering the License key should not be confused with the process of registering your company details on our website. This is important, since it allows us to give you support and notify you of important product news. Register on:

<http://www.gfi.com/pages/regfrm.htm>

Installing the rule manager (sorts spam to junk folder)

Note: The rule manager will only run on Windows 2000 and up. It will not run on Windows NT.

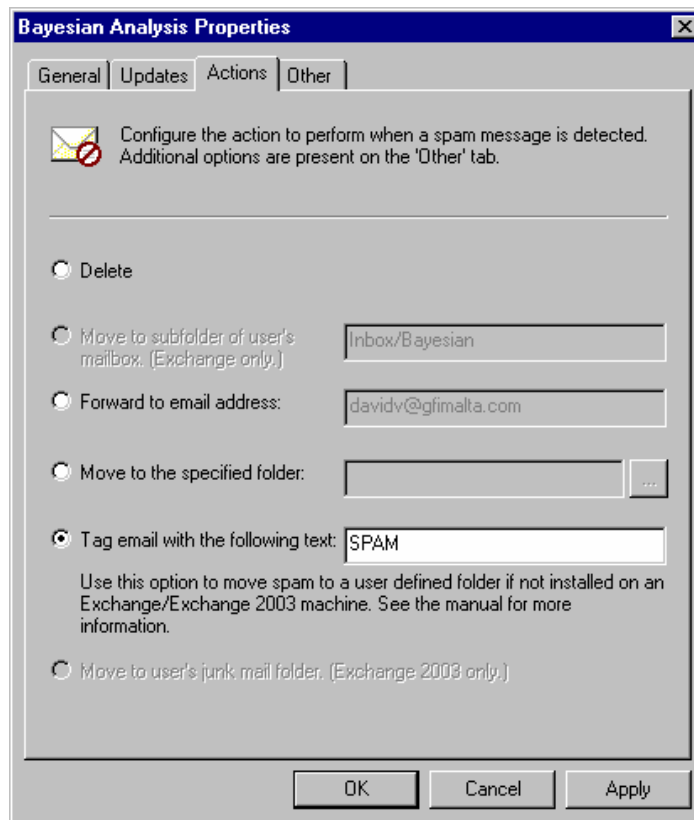
The mailbox rule manager

The mailbox rule manager is a utility which allows you to setup rules for user's mailboxes, so that mails marked as spam can be automatically moved to the users junk mail folder for easy review by the user.

How it works

Basically, you install the rule manager on the Exchange Server and specify the mailboxes which you wish to install the rule on. Then you specify in the MailEssentials configuration that all spam mail must be tagged.

If you want to use the rule manager, you must select TAG, and NOT block and delete or move. The latter will mean that no mail will reach the mailbox of the user, and therefore the rule will never be activated!



Screenshot 19 - Tag mail, NOT block and delete!

This way all spam will be tagged as [SPAM], and subsequently the rules installed on the mailbox will then move the mail tagged as [SPAM] to another folder of choice, for example the users junk mail folder. The mailbox rule manager is applicable to:

- Companies who have not installed GFI MailEssentials on the Exchange Server 2000/2003, but rather installed it as a mail relay, for example in the DMZ
- Companies using Exchange 5.5

If you have installed GFI MailEssentials on the Exchange 2000/2003 machine itself, there is no need to run the mailbox rule manager, because GFI MailEssentials will be able to route the mail itself to the user's junk mail folder.

Installing the rule manager and the Bayesian wizard

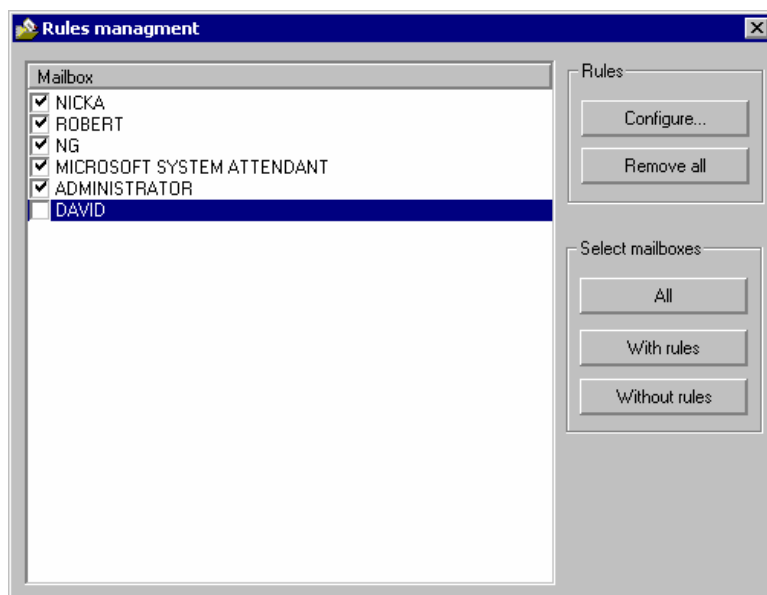
To install the rule manager and the Bayesian wizard:

1. Copy the file bayesianwiz.exe, located in the MailEssentials\bsw folder, to the machine on which you wish to install these utilities.
2. Run bayesianwiz.exe.

Configuring the rules on user's mailboxes

To configure the rules on users mailboxes:

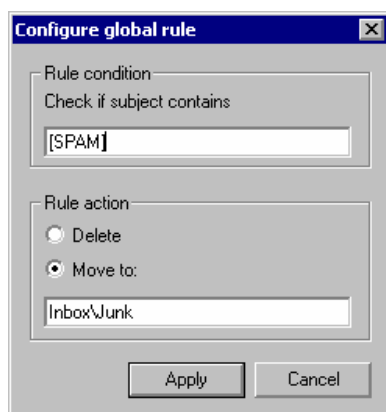
1. Run the rule manager application from the GFI MailEssentials program folder



Screenshot 20 - The rules manager

2. The main screen will show all the mailboxes it found on your server. Now select the mailboxes which you want to install a rule on. You can create 2 types of rules:

- A rule which moves mail marked as spam to the users junk mail folder
- A rule which deletes mail marked as spam (This rule can be used for users who wish to delete their spam automatically)



Screenshot 21 - Create a rule

3. Click configure. By default the rule will check for [SPAM] in the subject. **Note that if you change this, you will have to change the tag appended by MailEssentials at server level too!** Then select whether to delete the mail, or move the spam to a separate folder. You can specify the folder name. If you specify for example inbox\junk, then the folder will be created under the inbox folder. If you specify just 'junk', then the folder will be created at the top level, i.e. next to the inbox for example.

4. You can select multiple mailboxes and configure rules for all of them in one go (as long as the same rule applies to all)

5. All mailboxes for which you have configured a rule will be marked as blue.

The Bayesian anti-spam filter

Introduction

The Bayesian filter is the main 'Spam fighting' technology of GFI MailEssentials. Whilst the other anti spam features are important too and complementary to the Bayesian filter, it is the Bayesian filter that will allow you to virtually eliminate spam from your network.

Bayesian filtering technology is an adaptive, 'artificial intelligence' technique that is much harder to circumvent by spammers.

However it pays administrators to take a moment to understand the Bayesian filtering technology, in order to be able to gain the most from it.

This chapter explains how the Bayesian filter works, how it can be configured and how it can be trained.

IMPORTANT: Don't judge GFI MailEssentials' spam detection rate until you have allowed the Bayesian filter to run for at least 1 week! GFI MailEssentials can achieve the highest detection rate compared to other anti-spam solutions because it adapts specifically to your mail. Be patient and wait at least a week before you judge it!

How the Bayesian spam filter works

Bayesian filtering is based on the principle that most events are dependent and that the probability of an event occurring in the future can be inferred from the previous occurrences of that event. (More information about the mathematical basis of Bayesian filtering is available at [Bayesian Parameter Estimation](http://www-ccrma.stanford.edu/~jos/bayes/Bayesian_Parameter_Estimation.html) and [An Introduction to Bayesian Networks and their Contemporary Applications](http://www.niedermayer.ca/papers/bayesian/bayes.html))

(http://www-ccrma.stanford.edu/~jos/bayes/Bayesian_Parameter_Estimation.html & <http://www.niedermayer.ca/papers/bayesian/bayes.html>.)

This same technique can be used to classify spam. If some piece of text occurs often in spam but not in legitimate mail, then it would be reasonable to assume that this email is probably spam.

Creating a tailor-made Bayesian word database

Before mail can be filtered using this method, the user needs to generate a database with words and tokens (such as the \$ sign, IP addresses and domains, and so on), collected from a sample of spam mail and valid mail (referred to as 'ham').

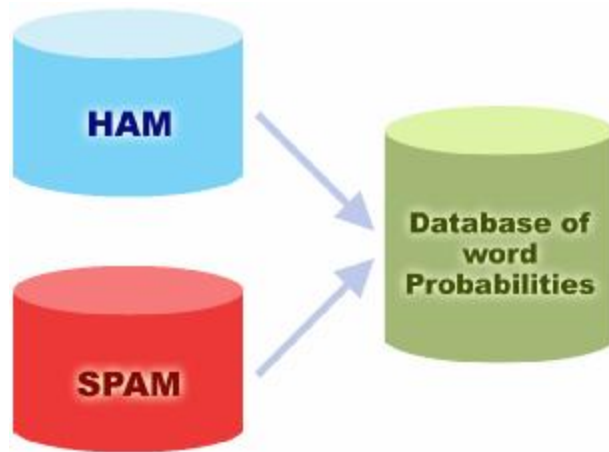


Figure 1 - Creating a word database for the filter

A probability value is then assigned to each word or token; the probability is based on calculations that take into account how often that word occurs in spam as opposed to legitimate mail (ham). This is done by analyzing the users' outbound mail and by analyzing known spam: All the words and tokens in both pools of mail are analyzed to generate the probability that a particular word points to the mail being spam.

This word probability is calculated as follows: If the word "mortgage" occurs in 400 of 3,000 spam mails and in 5 out of 300 legitimate emails, for example, then its spam probability would be 0.8889 (that is, $[400/3000]$ divided by $[5/300 + 400/3000]$).

Creating the ham database (tailored to your company)

It's important to note that the analysis of ham mail is performed on the company's mail, and is therefore tailored to that particular company. For example, a financial institution might use the word "mortgage" many times over and would get a lot of false positives if using a general anti-spam rule set. On the other hand, the Bayesian filter, if tailored to your company through an initial training period, takes note of the company's valid outbound mail (and recognizes "mortgage" as being frequently used in legitimate messages), and therefore has a much better spam detection rate and a far lower false positive rate.

Note that some anti-spam software with very basic Bayesian capabilities, such as the Outlook spam filter or the Internet Message Filter in Exchange Server, does not create a tailored ham data file for your company, but ships a standard ham data file with the installation. Although this method does not require an initial learning period, it has 2 major flaws:

1. The ham data file is publicly available and can thus be hacked by professional spammers and therefore bypassed. If the ham data file is unique to your company, then hacking the ham data file is useless. For example, there are hacks available to bypass the Microsoft Outlook 2003 or Exchange Server spam filter. For more information about this, see [Microsoft Outlook 2003 Spam Filter: Under the hood](#)

2. Secondly the ham data file is a general one, and thus not tailored to your company, it cannot be as effective and you will suffer from noticeably higher false positives.

Creating the spam database

Besides ham mail, the Bayesian filter also relies on a spam data file. This spam data file must include a large sample of known spam and must be constantly updated with the latest spam by the anti-spam software. This will ensure that the Bayesian filter is aware of the latest spam tricks, resulting in a high spam detection rate (note: this is achieved once the required initial two-week learning period is over).

How the actual filtering is done

Once the ham and spam databases have been created, the word probabilities can be calculated and the filter is ready for use.

When a new mail arrives, it is broken down into words and the most relevant words - i.e., those that are most significant in identifying whether the mail is spam or not - are singled out. From these words, the Bayesian filter calculates the probability of the new message being spam or not. If the probability is greater than a threshold, say 0.9, then the message is classified as spam.

This Bayesian approach to spam is highly effective - a May 2003 BBC article reported that spam detection rates of over 99.7% can be achieved with a very low number of false positives!

Why Bayesian filtering is better

1. The Bayesian method takes the whole message into account - It recognizes keywords that identify spam, but it also recognizes words that denote valid mail. For example: not every email that contains the word "free" and "cash" is spam. The advantage of the Bayesian method is that it considers the most interesting words (as defined by their deviation from the mean) and comes up with a probability that a message is spam. The Bayesian method would find the words "cash" and "free" interesting but it would also recognize the name of the business contact who sent the message and thus classify the message as legitimate, for instance; it allows words to "balance" each other out. In other words, Bayesian filtering is a much more intelligent approach because it examines all aspects of a message, as opposed to keyword checking that classifies a mail as spam on the basis of a single word.

2. A Bayesian filter is constantly self-adapting - By learning from new spam and new valid outbound mails, the Bayesian filter evolves and adapts to new spam techniques. For example, when spammers started using "f-r-e-e" instead of "free" they succeeded in evading keyword checking until "f-r-e-e" was also included in the keyword database. On the other hand, the Bayesian filter automatically notices such tactics; in fact if the word "f-r-e-e" is found, it is an even better spam indicator, since its unlikely to occur in a ham mail. Another example would be using the word "5ex" instead of "Sex". You would probably not have a word 5ex in a ham mail, and therefore the likelihood that its spam increases.

3. The Bayesian technique is sensitive to the user – It learns the email habits of the company and understands that, for example, the word 'mortgage' might indicate spam if the company running the filter is, say, a car dealership, whereas it would not indicate it as spam if the company is a financial institution dealing with mortgages.

4. The Bayesian method is multi-lingual and international - A Bayesian anti-spam filter, being adaptive, can be used for any language required. Most keyword lists are available in English only and are therefore quite useless in non English-speaking regions. The Bayesian filter also takes into account certain languages deviations or the diverse usage of certain words in different areas, even if the same language is spoken. This intelligence enables such a filter to catch more spam.

5. A Bayesian filter is difficult to fool, as opposed to a keyword filter - An advanced spammer who wants to trick a Bayesian filter can either use fewer words that usually indicate spam (such as free, Viagra, etc), or more words that generally indicate valid mail (such as a valid contact name, etc). Doing the latter is impossible because the spammer would have to know the email profile of each recipient - and a spammer can never hope to gather this kind of information from every intended recipient. Using neutral words, for example the word "public", would not work since these are disregarded in the final analysis. Breaking up words associated with spam, such as using "m-o-r-t-g-a-g-e" instead of "mortgage", will only increase the chance of the message being spam, since a legitimate user will rarely write the word "mortgage" as "m-o-r-t-g-a-g-e".

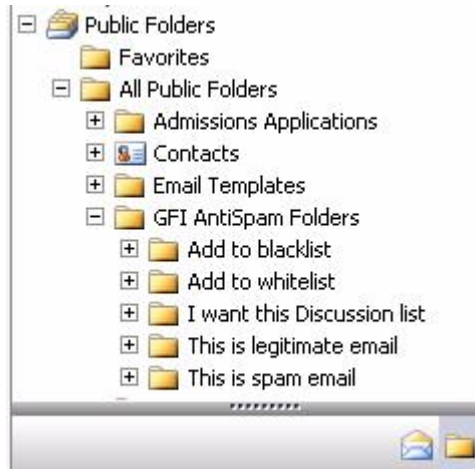
What's the catch?

Bayesian filtering, if implemented the right way and tailored to your company is by far the most effective technology to combat spam. Is there a downside? Well, in a way there is one downside, but this can easily be overcome: Before you can use and judge the Bayesian filter, you have to wait for it to learn for at least two weeks - that or create the ham or spam databases yourself. This task can be quite complex, so it is best to wait until the filter has had time to learn. Over time, the Bayesian filter becomes more and more effective as it learns more about your organization's email habits. To quote the old saying, good things come to he who waits.

Training the Bayesian filter

When you first install GFI MailEssentials, the Bayesian filter will be disabled. GFI MailEssentials ships with a default HAM (2000 ham e-mails) and SPAM database, however its better if you train the Bayesian filter with your specific 'email profile' before switching it on. This training can be done in 2 ways:

1. Automatically by collecting outbound e-mails. GFI MailEssentials will collect legitimate mail (HAM) by scanning outbound mail. You can enable the Bayesian filter after it has collected at least 500 outbound emails (If you send out mainly English mail) or 1000 outbound mails (If you send out non-English mail). Normally this amount of mail is collected in a matter of days.

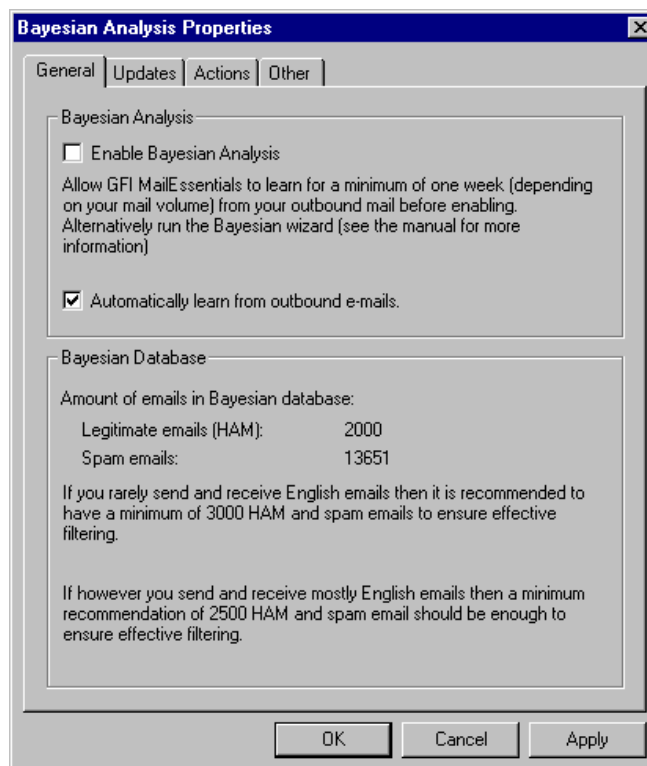


Screenshot 22 - Supplying ham to the Bayesian filter

2. By supplying ham to the Bayesian filter by copying between 500-1000 mails from your sent items to the **'This is legitimate email'** sub folder in the GFI AntiSpam public folders. For more information see paragraph 'Adding HAM to the ham database' in the chapter 'Spam management from the user's point of view'.

Configuring the Bayesian filter

After the Bayesian filter has been trained you can enable the Bayesian filter:

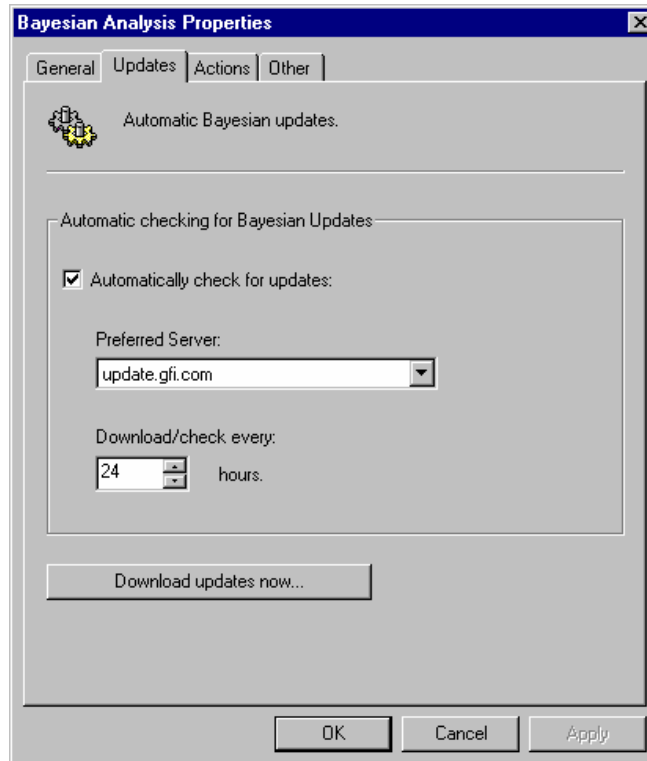


Screenshot 23 - Bayesian analysis properties

1. In the GFI MailEssentials configuration, select the Anti Spam > Bayesian filter node, right-click and select properties. This brings up the Bayesian filter properties. Click 'Enable Bayesian analysis'.

2. Ensure that the 'Automatically learn from outbound e-mails' option is ticked. This option will continuously update the legitimate mail database with outbound mails.

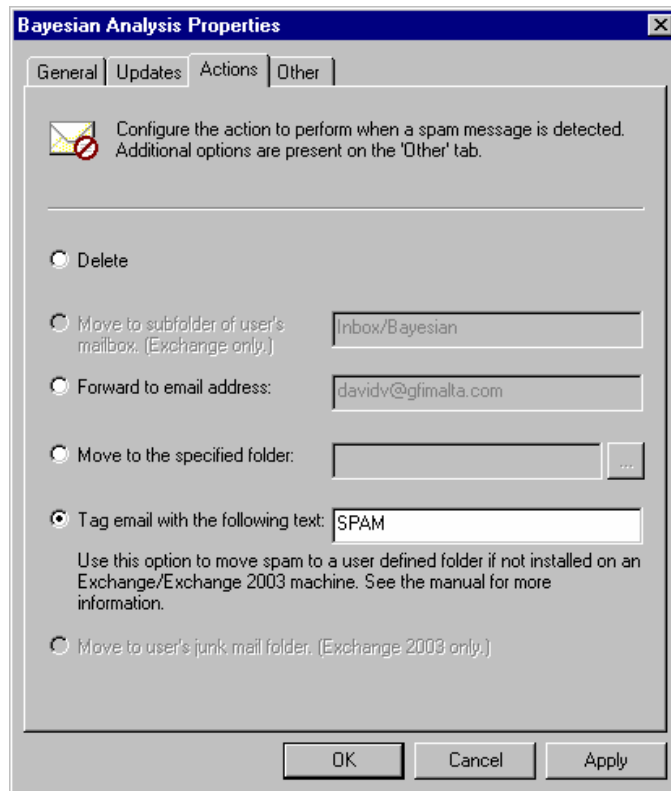
Updates



Screenshot 24 - Bayesian updates

3. In the updates tab you can specify how frequently GFI MailEssentials should check for updates to the spam database. You can also trigger an instant download by clicking on the 'Download Updates Now' button.

Actions



Screenshot 25 - What to do with mail tagged as spam

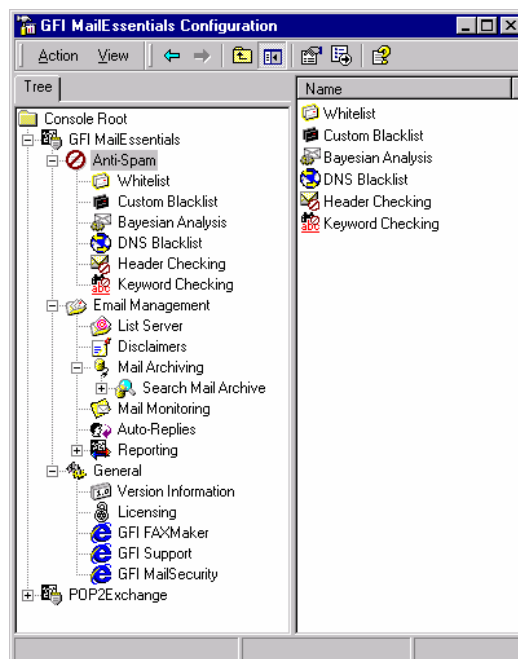
After you have configured the Bayesian filter, you can configure what you wish to do with mail marked as Spam. Please see the actions paragraph in the configuring Anti Spam chapter.

Configuring Anti-Spam

Introduction to Anti Spam

GFI MailEssentials tackles spam protection at server level and eliminates the need to install and update anti-spam software on each desktop. GFI MailEssentials uses various methods to identify spam:

1. **White lists** – White lists are lists of email addresses and phrases/words from which you always wish to receive mail. GFI MailEssentials will automatically build a white list for you from outbound mail.
2. **Custom black lists** – This feature allows you to specify domains and email addresses from which you do not wish to receive mail.
3. **DNS black list** - this allows you to configure GFI MailEssentials to query whether the email sender is on a public DNS black list of known spammers such as ORDB.
4. **Bayesian analysis** – this method analyses the content of the inbound mail and based on mathematical rules decides if the mail is spam or not. The Bayesian filter is discussed in the chapter 'The Bayesian anti-spam filter'.
5. **Header checking** – this method analyses the header of the mail to detect whether a mail is spam or not.
6. **Keyword checking** – this method allows you to configure keywords which indicate if a mail is spam.



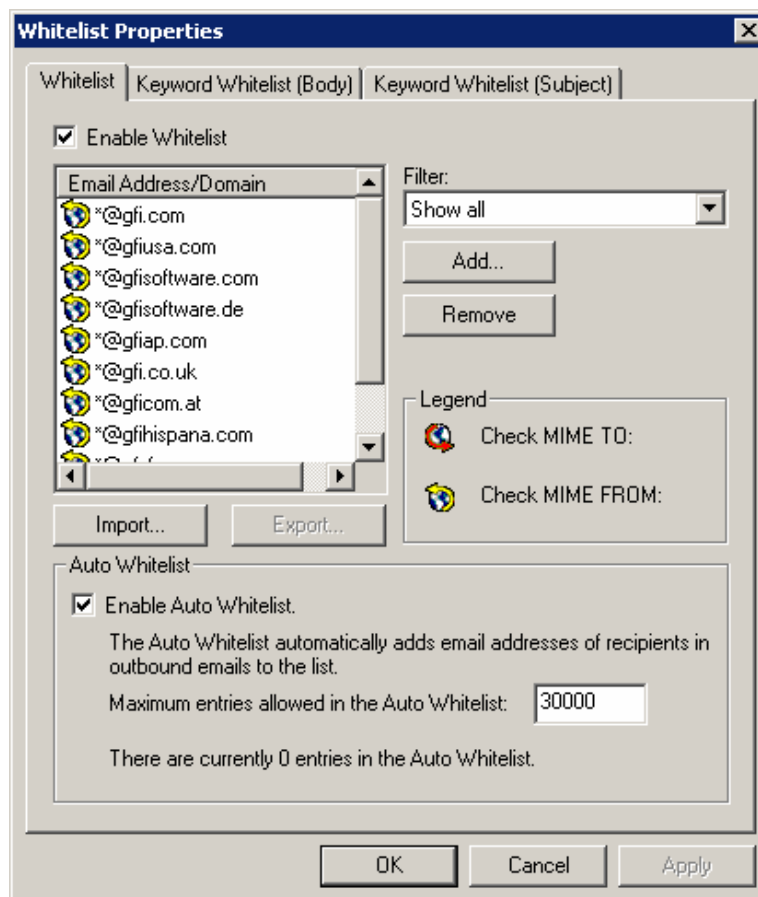
Screenshot 26 - Anti spam configuration

When GFI MailEssentials finds a spam message, it can delete the message, move it to a central folder, forward it to an e-mail address, tag the e-mail or move it to a users junk mail folder.

Note: To stop spammers from relaying their mail through your mail server, you need configure your mail server to disallow mail relaying. For more information on this, consult the mail server documentation.

White list

The White list is a list of email addresses & domains from which you always wish to receive emails. I.e. mails sent from these email addresses or domains will never be marked as spam. You can also configure keywords, which if found in the body or subject, will automatically white list the email.



Screenshot 27 - White listed domains

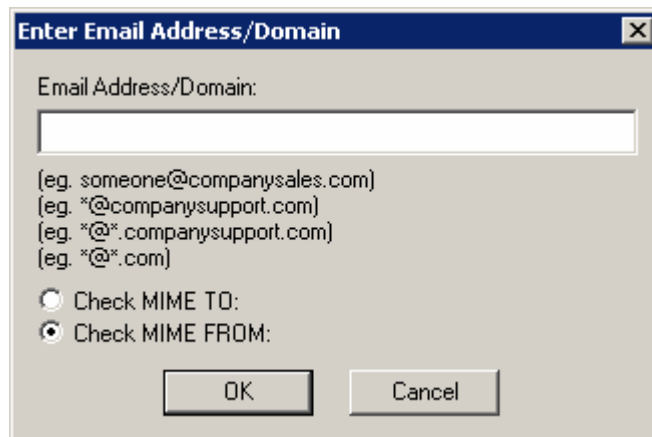
The configuration of the White list is done from the Anti Spam > White list node. Right-click on this node to bring up the White list properties. The first tab is the White list configuration.

Auto white list

This feature automatically white lists email addresses to which you send mail. Clearly you will want to receive an answer from anyone you send a mail, so white listing them automatically makes a lot of sense. The process is completely automatic - you will have a reliable and constantly updated white list in no time and without any administration!

The white list can store up to 30,000 email addresses. After that the oldest records get replaced.

We highly recommend using this feature, since it allows GFI MailEssentials to achieve a very low rate of false positives.



Screenshot 28 - Adding a white listed email entry

To add a white listed domain or email address:

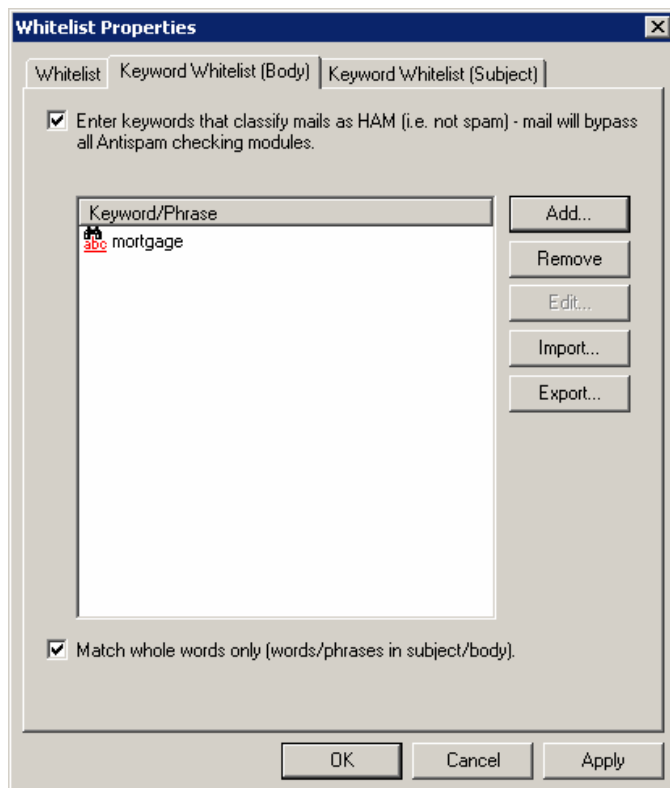
1. Click 'Add' and specify the full email address. If you wish to specify an entire domain, specify it as follows `*@companysupport.com`. The `*` is a wildcard to include all email addresses from that domain. You can also specify wildcards and white list entire domain suffixes, for example `*@*.mil` or `*@*.edu`. The latter will for example ensure that mail sent from military or educational domains will never be marked as spam.

2. Specify 'Check Mime to:' OR 'Check Mime from:'. This option allows you to white list an email recipient. The MIME TO: is the email address to which the email is addressed. To find out the MIME TO: open up a copy of the list mail/newsletter and double click on the to: field. Enter the email address shown in the 'Add List' dialog.

Some newsletters use mailers that do not address the sender in the MIME to field, causing the GFI MailEssentials header checking feature to mark it as spam. These should be white listed with the MIME TO: option

Note: If you want to exclude a user from spam filtering, simply enter the e-mail address of the user, and select MIME TO:

White listed keywords



Screenshot 29 - White listing keywords

GFI MailEssentials allows you to specify keywords, which cause the mail to be flagged as HAM (valid mail). If a keyword configured in the keyword white list is found in a mail, then GFI MailEssentials will automatically allow the mail to skip all anti spam filters and deliver the mail directly the user's inbox.

Use this option carefully, since entering too many keywords will allow too much spam to skip the spam filters. You can configure white listed keywords for body and subject:

1. To configure white listed keywords in the body, click on the White listed keywords (body) tab and select add
2. To Configure white listed keywords in the subject, click on the white listed keywords (subject) tab and select add.

Directory harvesting

Note: The directory harvesting feature makes use of Active Directory to search for known users within the organization. If GFI MailEssentials is not installed in Active Directory user mode this feature will not be available. If you have installed GFI MailEssentials on a demilitarized zone (DMZ) and Active Directory is behind a firewall this feature will not work and should be disabled.

Directory harvesting attacks occur when a spammer uses known email addresses to generate other valid e-mail addresses from corporate or ISP mail servers. This technique allows the spammer to send e-mails to randomly generated e-mail addresses. Some of these e-mail addresses are real users in the organization however many of them are bogus addresses that flood the victim mail server.

The directory harvesting attacks feature in GFI MailEssentials stops these types of attacks by blocking emails addressed to users that do not exist on the organizations email server.



Screenshot 30 - The directory harvesting feature

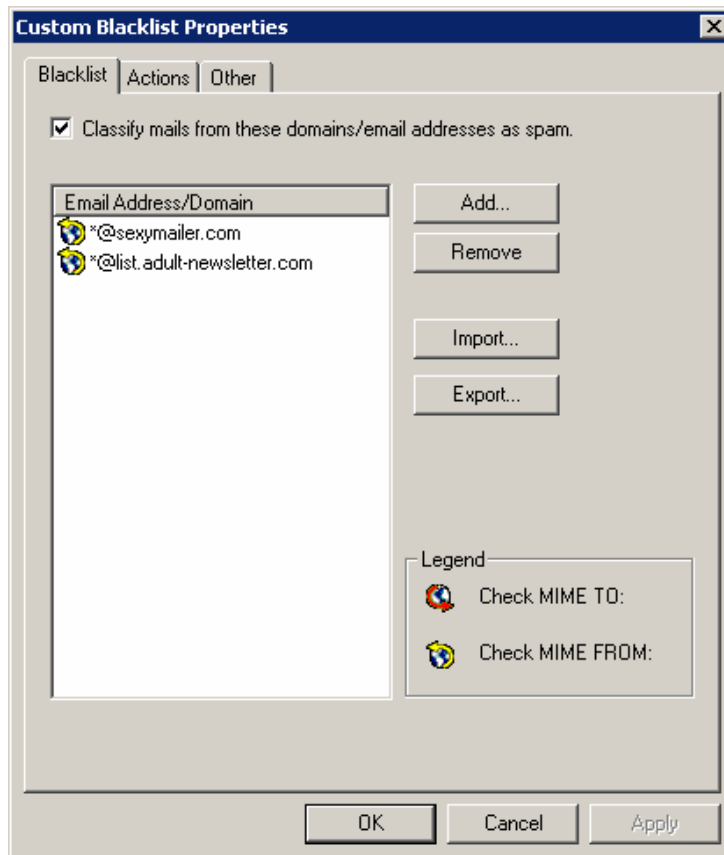
Configuration is done from the Anti Spam -> Directory Harvesting node. Right-click on this node to bring up the Directory Harvesting properties. Check the 'Enable directory harvesting protection' option to enable this feature then click 'OK' or 'Apply' to save the settings.

Actions

After you have configured directory harvesting, you can configure what you wish to do with mail marked as Spam. Please see the actions paragraph for more information on the actions tab.

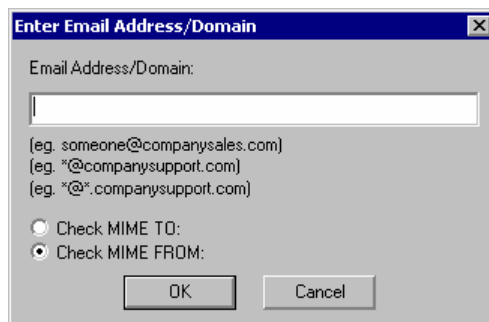
Custom Blacklist

The Black list is a custom database of email addresses & domains from which you never wish to receive emails. I.e. mails sent from these email addresses or domains will always be marked as spam.



Screenshot 31 - The custom blacklist

The configuration of the blacklist is done from the Anti Spam > Custom Blacklist list node. Right-click on this node to bring up the Custom Blacklist properties.



Screenshot 32 - Adding a blacklisted email entry

To add a blacklisted domain or email address, click 'Add'. Specify the full email address. If you wish to specify an entire domain, specify it as follows `*@spammer.com`. The `*` is a wildcard to include all email addresses from that domain.

You can also blacklist entire domain suffixes, for example `*@*.jp`. This will for example ensure that mail sent from Japan is automatically marked as spam. Clearly you have to use these entries with care.

Then specify whether you want the blacklist entry to apply to the MIME TO: field or the MIME FROM: field. The MIME TO option allows you to blacklist email sent to a non existing email address. This could be handy if you want to avoid an NDR being sent and just want the

email to be automatically deleted (for example mail sent to ex employees).

DNS blacklists (DNSBL)

Note: **This feature requires a properly configured DNS server.** If the DNS server is not properly configured (and we have seen this many times), a time out will occur and mail will be processed slowly and in addition a lot of valid mail will be tagged as spam. For more information see the GFI Knowledgebase article 'KBID001770'.

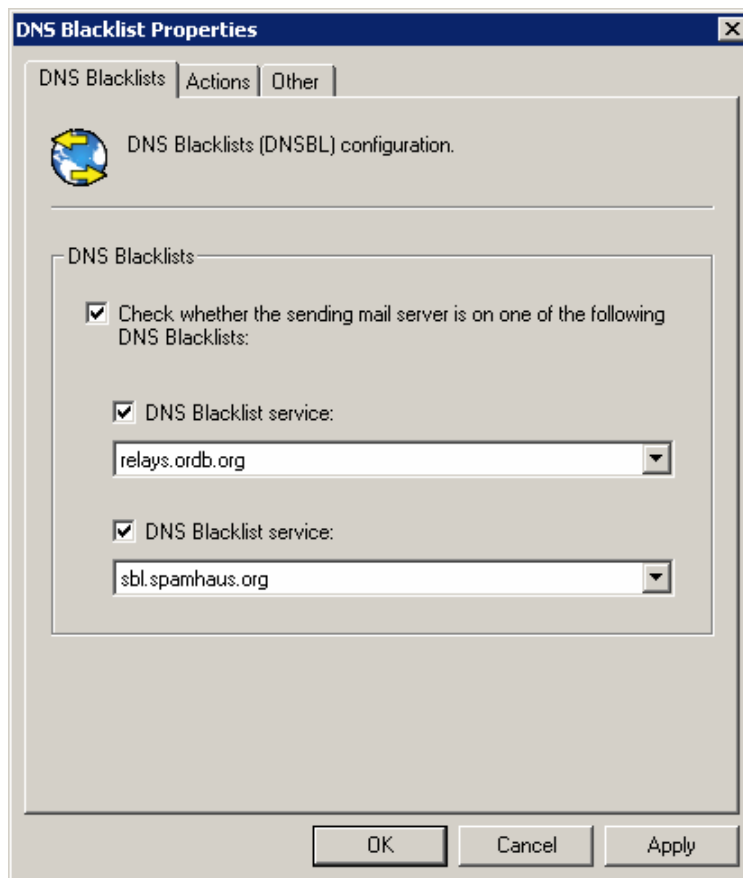
GFI MailEssentials supports a number of DNS blacklists, which can be configured from the DNS blacklists node. DNS blacklists are databases of SMTP servers that have been used for spamming. These databases are queried 'DNS style'. There are quite few third party DNS blacklists available, ranging from reliable lists that have clearly outlined procedures for getting on or off the DNS blacklist to less reliable lists.

When an email is sent, it is passed through a number of SMTP servers until it reaches the final destination. The ip address of each of these SMTP servers is recorded in the email header. GFI MailEssentials will check all the public ip's found in the message header with the DNSBL database configured (example: ordb.org).

The ORDB list is an Open Relay Database maintained by ORDB.org. ORDB.org is a non-profit organization, which stores an IP-addresses of verified open SMTP relays. These relays are, or are likely to be, used as conduits for sending unsolicited bulk email, also known as spam. By accessing this list, system administrators are allowed to choose to accept or deny email exchange with servers at these addresses.

How it works

GFI MailEssentials will check all the public ip's found in the message header with the DNSBL database configured (example: ordb.org). GFI MailEssentials will record all the ip's checked in an internal database and will not perform further checks with the DNSBL for the same ip's. The ip addresses are kept in the database for 4 days, or until the Simple Mail Transport Protocol service is restarted



Screenshot 33 - The DNS blacklist properties

To enable the DNS blacklist:

1. Right-click on the Anti Spam > DNS Blacklist node and select properties.
2. Click on '**Check whether the sending mail server is on this DNSBL**'.
3. Now select the appropriate DNS blacklist you wish to check incoming mail against. For example relays.ordb.org
4. Optionally you can select a second DNS blacklist, for example SpamHaus.

Note that querying a DNS blacklist can be slow (depending on your connection), so mail can be slowed down a little bit, especially if you query against 2 DNS blacklists.

Actions – what to do with spam mail

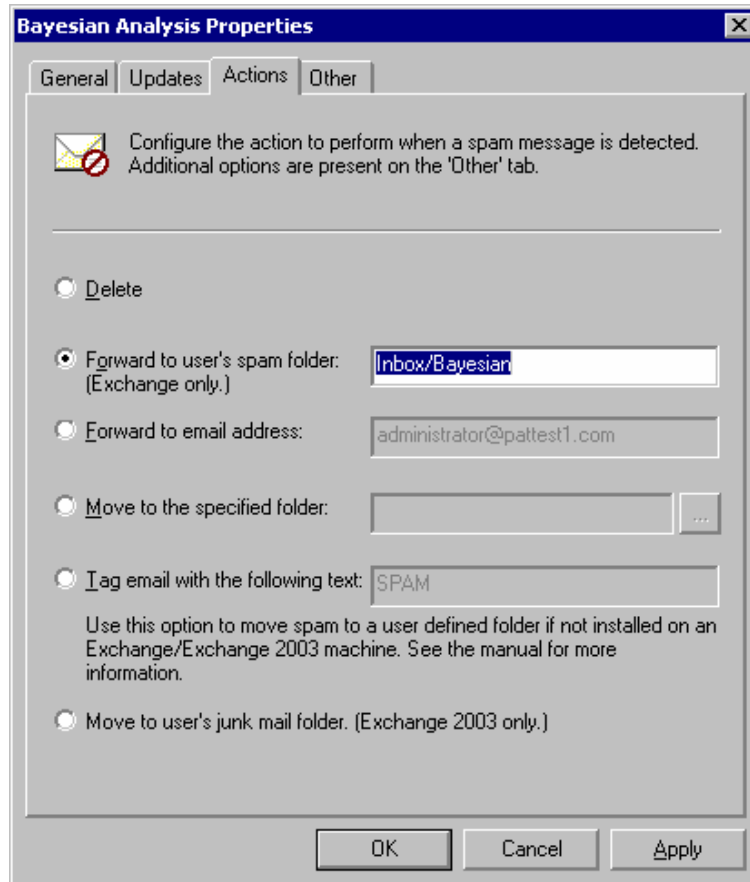
The properties of each spam filter (i.e. the nodes white list, custom blacklist, DNS blacklist, Bayesian analysis, header checking and keyword checking) have an actions tab to enable you to specify what should be done with mail marked as spam by that module.

The reason that you can specify this per filter is:

- If you sort mail to the users junk mail folder, you can create folders for each filter, so that the user can immediately identify why the mail was marked as spam.

- Secondly, you might want to delete mail marked by the blacklist spam filter, but do something else with mail marked as spam by the keyword checking filter.

The options in the actions tab are identical for each spam filter.



Screenshot 34 - Configuring the action that should be taken

You can specify that mail marked as spam should be:

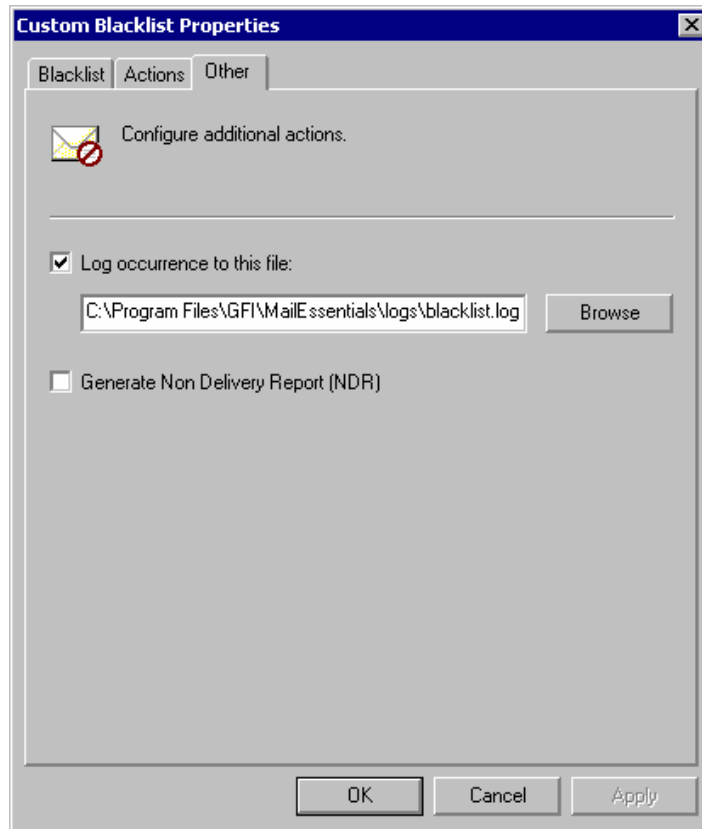
- Deleted
- Forwarded to subfolder of user's mailbox – this option will cause spam mail to be sent to a set of subfolders in the user's mailbox. GFI MailEssentials will create a folder according to the name you specify and sort all mail marked as spam to this folder. This way users can periodically check mail marked as spam, and identify mail that might have been wrongly marked as spam. If you enter **inbox/junk mail**, then the folder will be created under the inbox folder. If you don't it will be created 'next to' the inbox, i.e. at the same level. By using a different folder name for the Bayesian, keyword and header checking filters, spam is automatically sorted to a different folder depending on which filter identified it as spam. This further eases the spam reviewing process.

Note that this option requires that GFI MailEssentials is installed on the Exchange Server machine, in Active Directory mode, and that you are running Exchange 2000/2003. However if you are running Exchange 5.5 or are not running GFI MailEssentials on the Exchange server machine, you can

still achieve the same thing with the Tag email feature and the Rules manager (see installation chapter)

- Forwarded to another email address – In this case the email will be sent to a central email address. You can specify the email address of a public folder. The subject of the mail will be in the format [recipient] [subject]. This way a person can be assigned to periodically check mail marked as spam, and identify mail that might have been wrongly marked as spam. This feature can also be used to further improve the spam rules.
- Moved to specified folder – In this case the mail will be saved as a file in the specified folder. The file name will be as follows: **[Sender_recipient_subject_number_.eml]**
This allows you to quickly sort spam based on sender.
- Tagged: This option allows you to tag a spam mail. It does not block or delete the spam. This option can be used in combination with the Rules manager application, which allows you to easily setup sorting rules for all mailboxes on your Exchange Server machine. Then all mail tagged as spam will be sorted into the users junk mail folder. (location and name of folder is customizable)
- Move to user's junk mail folder (Exchange 2003) only. If you have Exchange 2003, GFI MailEssentials can tag spam in such a way that Outlook will sort the mail to the user's junk mail folder. However we recommend using the move to users spam folder feature instead, since this allows you to use a different folder name for the Bayesian, keyword and header checking filters. Spam mail is then automatically sorted to a different folder depending on which filter identified it as spam, greatly easing the spam reviewing process.

Other



Screenshot 35 - The other actions tab

In the other tab, you can specify a number of optional actions:

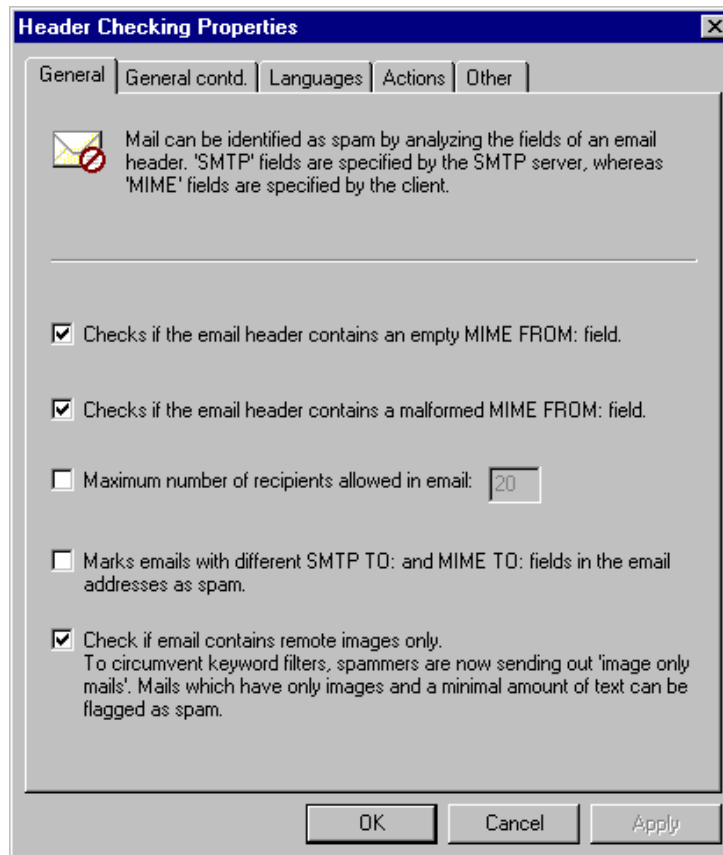
- The '**Log occurrence to this file**' feature allows you to log the spam mail occurrence to a log file of your choice.
- The Generate Non Delivery Report (NDR) feature allows You to create a fake Non Delivery Report (NDR). This will cause most bulk mailing software to remove your address from their database. In addition you can use this feature to notify the sender that his email has been considered spam. This feature can be handy to use whilst in initial training phase.

Note: If you wish you can customize the NDR. Go to the chapter Miscellaneous options for more information on this.

Header checking

The header checking module analyses the individual fields in a header. This module makes reference to SMTP and MIME fields. SMTP fields are specified by the mail server, whereas the MIME fields are specified by the email client (which encodes the mail to MIME).

The configuration of anti spam identification based on e-mail headers is done from the Anti Spam > Header Checking node. Right-click on this node to bring up the Header checking properties.



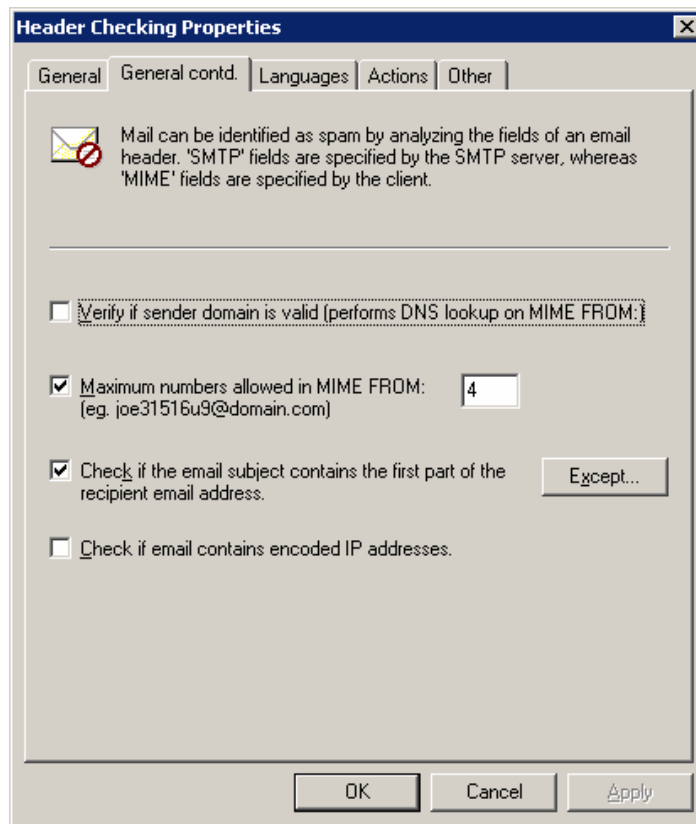
Screenshot 36 - Header checking properties (1)

General anti spam header checking options

The General tab in the Header Checking Properties dialog contains the following options:

1. **'Checks if the email header contains empty MIME From field':** This feature checks if the sender has identified himself in the From: field. If this field is empty it's an almost sure sign that the mail is sent by a spammer.
2. **'Checks if the email header contains a malformed MIME from: field'**. This feature checks if the MIME from field is a correct notation, i.e. it matches the RFC. Spammers often include a wrong or wrongly specified from address.
3. **'Marks emails with recipient lists of more than X recipients as spam'**. This feature marks mails with large recipient lists as spam. Mails with large recipient lists tend to be joke lists, chain e-mails or simply 'junior' or inadvertent spammers.
4. **'Marks email with different SMTP to: and MIME to: fields in the email addresses as spam'**. Checks whether the SMTP to: and MIME to: fields are the same. The spammers email server always has to include an SMTP to: address. However, the MIME to: email address is often not included or is different. This feature catches a lot of spam, however some list servers don't include the MIME to: either. Therefore to use this feature, you must white list the newsletter sender address if it gets marked as spam by this feature. This can be done from the white list node or by dragging the newsletter in the GFI AntiSpam public folders 'I want this newsletter' node.

5. **Check if email contains remote images only:** To circumvent keyword filters, spammers are now sending out 'image only mails'. GFI MailEssentials can flag mails which have only have images and a minimal amount of text as spam.



Screenshot 37 - Header checking continued

6. **'Verify if sender domain is valid'** This feature will do a DNS lookup on the domain specified in the MIME from field and verify if the domain is valid. If the domain is not valid it's a sure sign of spam.

Note: **This feature requires a properly configured DNS server.** If the DNS server is not properly configured (and we have seen this many times), a time out will occur and mail will be processed slowly and in addition a lot of valid mail will be tagged as spam.

7. **Check if emails contain more than X numbers in the MIME from.** Frequently, more than 3 numbers in the mime from means that the sender is a spammer. The reason for this is that spammers often use tools to automatically create reply-to: addresses on hotmail and other free email services. Frequently they use 3 or more numbers in the name to make sure the reply-to: is unique.

8. **'Checks if email subject contains first part of recipient email address'** To 'personalize' a spam mail, spammers frequently include the first part of the recipient email address in the subject. Be careful using this feature with generic email addresses such as sales@company.com. A customer that replies to an auto-reply with a subject 'Your mail to sales', would be marked as spam. To avoid this, you can specify email addresses for which this check should not be done, using the Except button.



Screenshot 38 - Excluding an email address

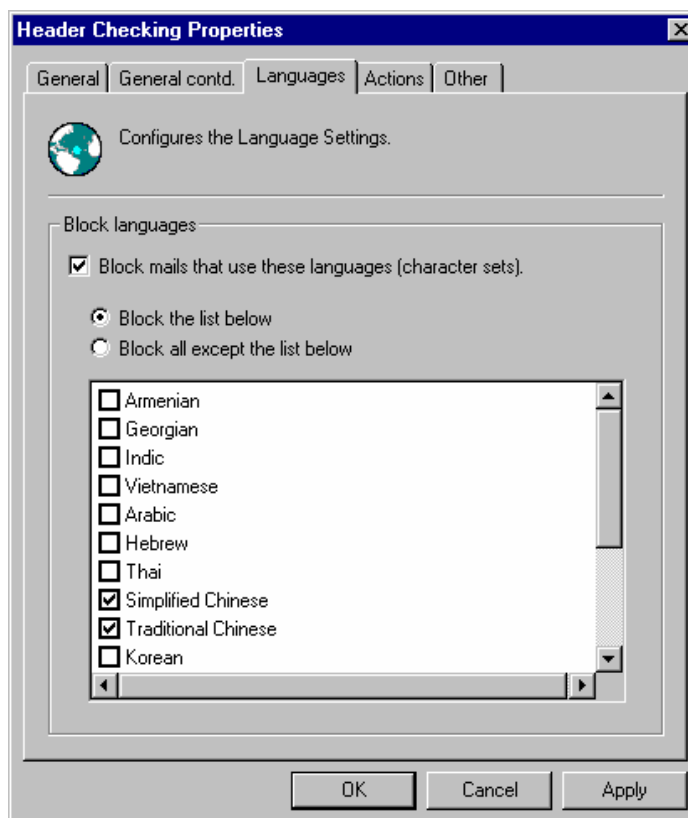
9. **Check if email contains encoded IP addresses** – This check looks for a url which has a hex/octal encoded IP (<http://0072389472/hello.com>) or which has a username/password combination in it (e.g. www.citibank.com@scammer.com).

These practices are often used by spammers as well as hackers. Examples which will be flagged as spam:

<http://12312>

www.microsoft.com:hello%01@123123

Language detection



Screenshot 39 - Language detection

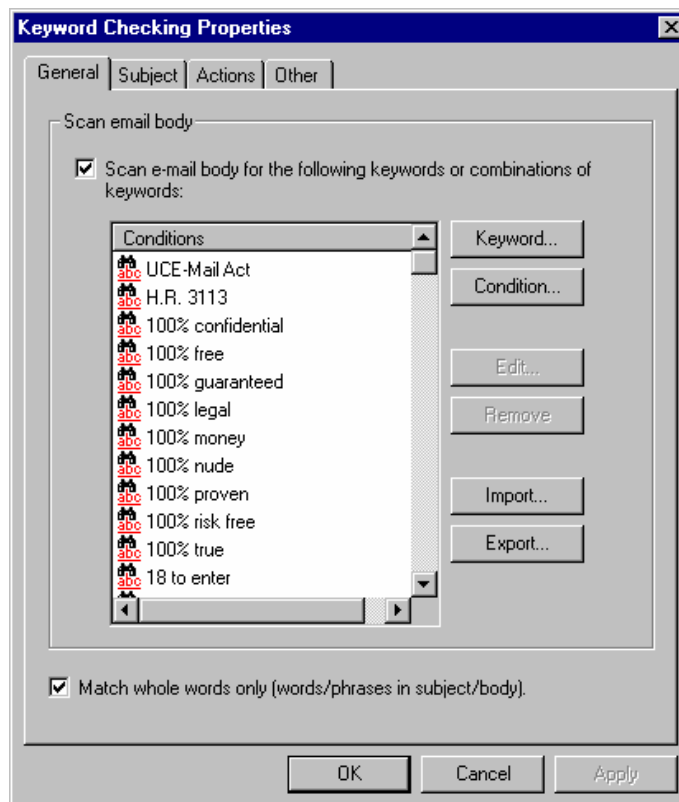
The languages tab in the Header Checking Properties dialog contains the language detection options. Many spam mails are not even in your language, meaning that you can greatly reduce spam simply by blocking mail written in say Chinese or Vietnamese. Using the Languages tab you can block mail using certain character sets. (GFI MailEssentials can not distinguish between Italian or French for example because they use the same character set) MailEssentials can only detect languages written in different character sets.

Actions

After you have configured the header checking filter, you can configure what you wish to do with mail marked as Spam. Please see the actions paragraph for more information on the actions tab.

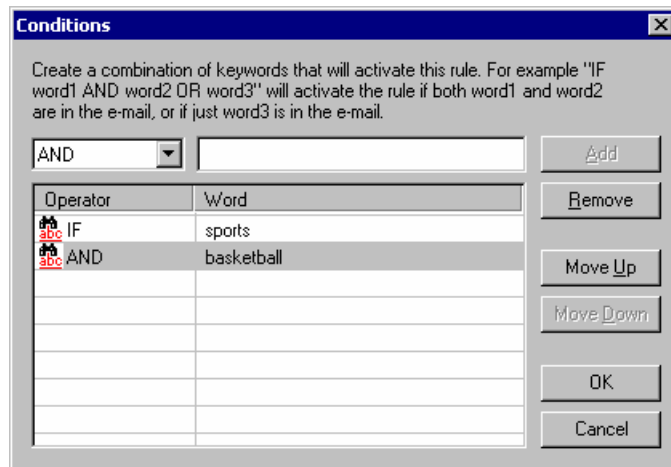
Keyword checking

The configuration of anti spam identification based on keywords is done from the Anti Spam > Keyword Checking node. Right-click on this node to bring up the Keyword checking properties.



Screenshot 40 - Anti Spam keyword checking properties

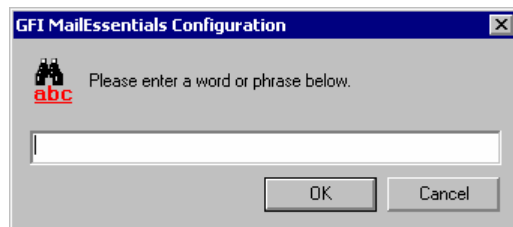
1. Enable 'Scan e-mail body'. Now you can enter keywords & conditions that identify spam. Select either 'Add Condition' to enter a condition, which uses operands, or select 'Add Keyword' to enter a single keyword or a phrase.



Screenshot 41 - Adding a condition

Adding conditions

Conditions are combinations of keywords using the operands IF, AND, AND NOT, OR or OR NOT. Using conditions, you can specify combinations of words that must appear in the e-mail. For example a condition "If Word1 AND Word2" will check for Word1 and Word2. Both words would have to be present in the mail to activate the rule. To add a condition, select 'Add Condition'



Screenshot 42 - Adding a keyword or phrase

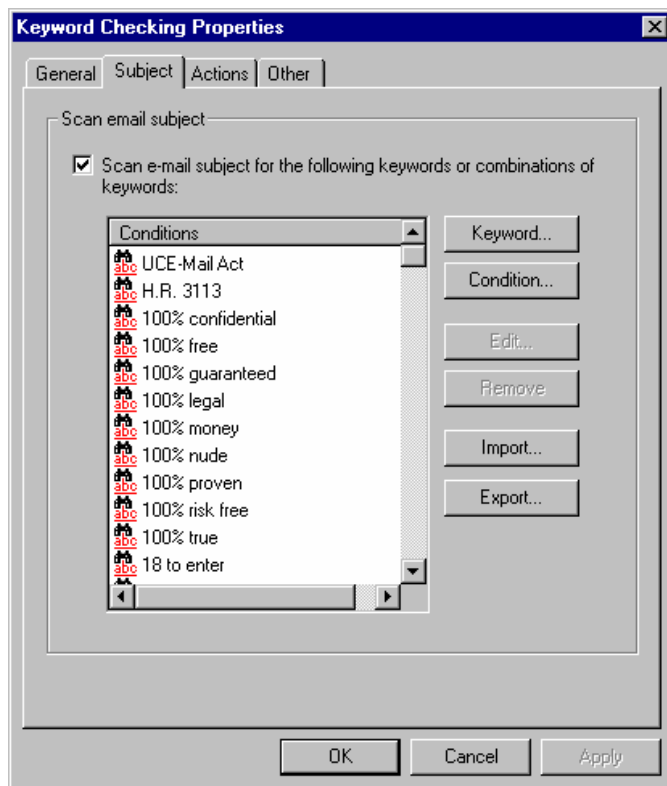
Adding keywords

If you only wish to check for single words or phrases, you do not need to create a condition. In this case you can just add a keyword. Select 'Add Keyword' to do this. If you enter multiple words, then MailEssentials will search for that phrase. For example if you enter Basketball sports, then MailEssentials will check for the phrase 'Basketball sports'. Only this phrase would activate the rule, not only the word basketball OR sports.

Match whole words only: Enabling this option allows you to ensure that GFI MailEssentials will only block mails where the word you specify is a whole word. For example, if you specify the word 'sport', an email with the word 'sport' will be blocked, but not an email with the word 'Allsports'.

Subject

2. To scan for words in the subject, enable 'Scan e-mail subject'. Now you can specify words that you wish to check for in the subject of the message. You can specify keywords and conditions.



Screenshot 43 - Looking for keywords in the subject tab

Actions

After you have configured the keyword checking filter, you can configure what you wish to do with mail marked as Spam. Please see the actions paragraph for more information on the actions tab.

Sender Policy Framework (SPF)

GFI MailEssentials supports the Sender Policy Framework (SPF). The Sender Policy Framework allows you to check whether a particular email sender is forged or not. Most of today's spammers use forged email addresses.

SPF is a community effort that is rapidly gaining ground. SPF requires that the company of the sender has published its mail server in an SPF record. For example if an email is sent from xyz@CompanyABC.com then companyABC.com must publish an SPF record in order for SPF to be able to determine if the email was really sent from the companyABC.com network or whether it was forged. If an SPF record is not published by CompanyABC.com the SPF result will be 'unknown'.

How SPF works

Domains use public records (DNS) to direct requests for different services (web, email, etc.) to the machines that perform those services. All domains already publish email (MX) records to tell the world what machines receive mail for the domain.

SPF works by domains publishing a text record in the DNS of those domains to tell the world what machines send mail from the domain. When receiving a message from a domain, GFI MailEssentials can

check those records to make sure mail is coming from where it should be coming from.

GFI MailEssentials does not require you to publish any SPF records yourself. If you would like to do this then you can use the SPF wizard at: <http://spf.pobox.com/wizard.html>

An example

Suppose a spammer forges CompanyABC.com and tries to spam you. He connects from somewhere other than CompanyABC.

When his message is sent, you see MAIL FROM: <forged_address@CompanyABC.com>, but you don't have to take his word for it. You can ask CompanyABC if the IP address comes from their network.

In this example CompanyABC publishes an SPF record. That record tells GFI MailEssentials how to find out if the sending machine is allowed to send mail from CompanyABC.

If CompanyABC says they recognize the sending machine, it passes, and you can assume the sender is who they say they are. If the message fails the SPF tests, it's a forgery. That's how you can tell it's probably a spammer.

For more information on SPF and how it works, please visit the Sender Policy Framework Web Site at <http://spf.pobox.com>.

SPF on the gateway machine

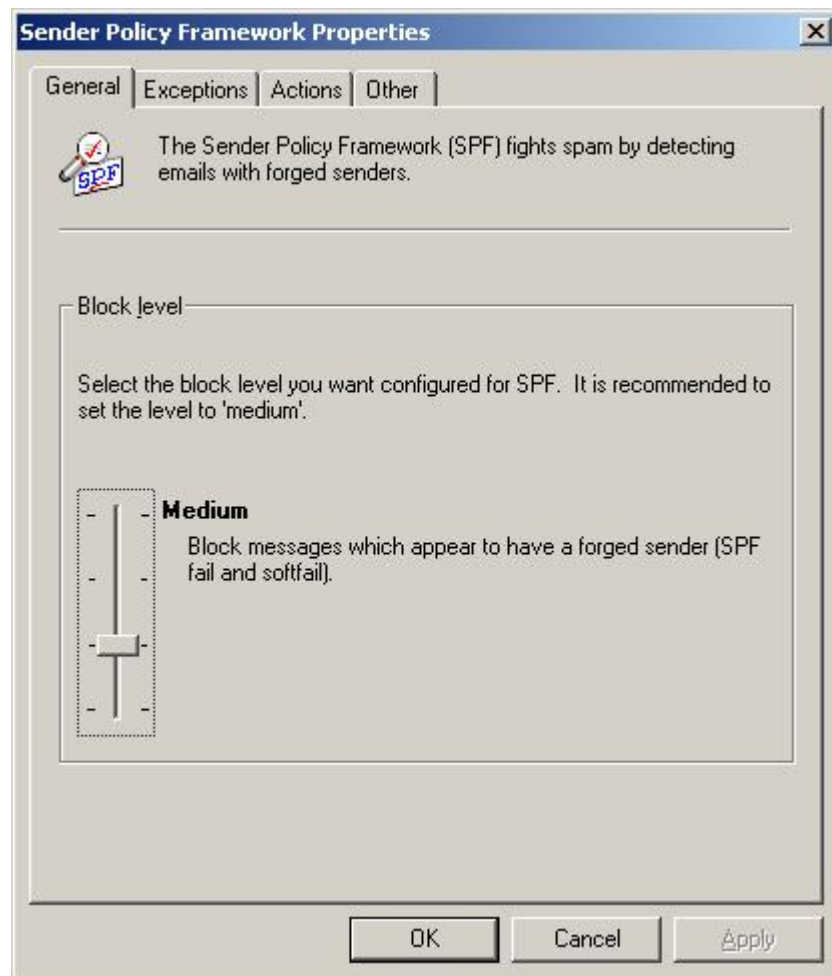
For SPF to function correctly the mail server must receive emails directly from the Internet. If inbound emails arriving are being relayed through via another server then the SPF checks will fail. If you are unsure whether mail reaches this server via a relay, set the rejection level to 'low' and configure the actions to TAG the email rather than block it.

Please see this KB article for more information: <http://kbbase.gfi.com/showarticle.asp?id=KBID002159>.

Configuring the SPF feature

The configuration of SPF is done from the Anti Spam -> Sender Policy Framework node. Right-click on this node to bring up the SPF properties.

SPF block level



Screenshot 44 - Configuring the SPF block level

The rejection level allows you to set the sensitivity of the SPF test. You can choose from 4 levels:

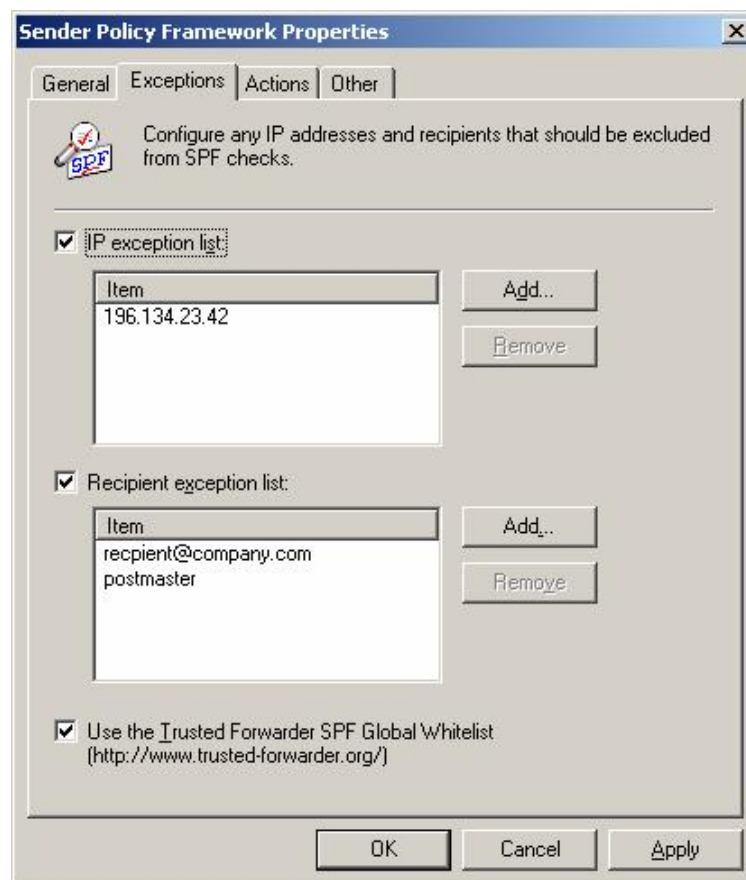
Never: Never block any messages. When this option is selected SPF tests are not done on incoming emails.

Low: Only block messages which are determined to have a forged sender. This option will treat any message with a forged sender as spam.

Medium: Block messages which appear to have a forged sender. This option will treat any messages that appear to have a forged sender as spam. This is the default and recommended setting.

High: Block any message which is not proven to be from the sender. This option will treat all mail as spam unless it could be proven that the sender is not forged. Since the majority of mail servers do not yet have an SPF record this option is not recommended.

Configuring Exceptions



Screenshot 45 - Configuring the SPF exceptions

This page allows you to configure the IP addresses and recipients that should be excluded from SPF checks.

IP exception list: IP addresses in this list will automatically pass SPF checks. Click on 'Add...' to add a new IP address. To remove an IP address, select it from the list and click on 'Remove'. To disable the IP exception list uncheck the 'IP exception list' checkbox.

Recipient exception list: This option allows certain recipients to always receive their e-mail, even if the messages should be rejected. A recipient exception can be entered in one of three ways:

- localpart - "abuse" (matches "abuse@abc.com", "abuse@xyz.com", etc...)
- domain - "@abc.com" (matches "john@abc.com", "jill@abc.com", etc...)
- complete - "joe@abc.com" (only matches "joe@abc.com")

To disable the recipient exception list uncheck the 'Recipient exception list' checkbox.

Trusted Forwarder Global Whitelist: The Trusted Forwarder Global Whitelist (www.trusted-forwarder.org) provides a global whitelist for SPF users. It provides a way of allowing legitimate email that is sent through known, trusted email forwarders from being blocked by SPF checks because the forwarders do not use some sort of envelope-from rewriting system. By default this setting is enabled. It is recommended to always leave this option enabled.

Actions

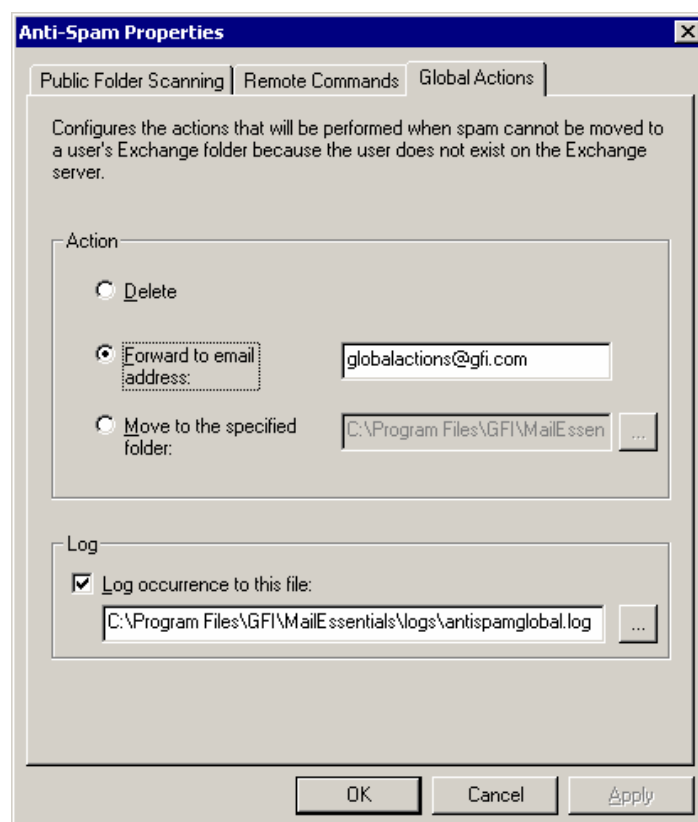
After you have configured the SPF feature, you can configure what you wish to do with mail marked as Spam. Please see the actions paragraph for more information on the actions tab.

Anti Spam global actions

This section applies only to users who have installed GFI MailEssentials **on the Exchange 2000/2003 machine** and who are using the 'Forward to user's spam folder function'. If you have not installed on the Exchange 2000/2003 machine, the anti spam global actions will not appear.

A lot of spam is sent to email addresses that no longer exist on your server. Therefore, once you start sorting mail marked as spam to user's junk mail folders, you will end up with a relatively large percentage of mail that can not be sorted into someone's mailbox. Generally, you will simply want to delete these mails. However for troubleshooting or evaluation purposes, you might want to move these mails to a folder or forward them to a particular email address. This can be done from the global actions tab in the Anti Spam properties. To configure the global actions:

1. Right clicking on the Anti Spam node and selecting properties.



Screenshot 46 - Global actions

2. Now select whether to:
 - Delete the mail
 - Forward it to an email address
 - Move it to a specified folder.

Additionally, using the '**Log occurrence to this file**' feature, you can log the spam mail occurrence to a log file of your choice.

Spam management from the user's point of view

Introduction

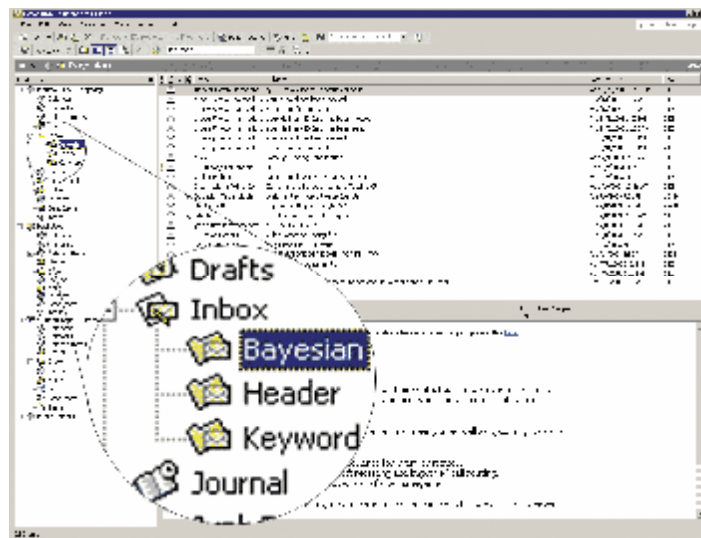
This chapter describes how users can manage their spam. First and foremost, it needs to be pointed out that GFI MailEssentials has been designed to minimize spam management by the user. Its pointless flagging mail as spam if the user has to spend a lot of time managing his spam. That said, there are some valid actions that a user can perform to increase the effectiveness of GFI MailEssentials. These include:

1. Training the Bayesian filter with valid mail, flagged erroneously as spam by GFI MailEssentials
2. Training the Bayesian filter with spam, flagged erroneously as valid mail.
3. Adding mail senders and newsletters to the white list

In addition, users will tend to blame the anti spam package for not receiving certain mails. Therefore, especially just after the deployment of GFI MailEssentials, it pays administrators to give users control and allow them to see what has been flagged as spam.

Reviewing spam mail

The recommended way to configure GFI MailEssentials is to forward mail marked as spam by the Bayesian, keyword and header checking spam filters to a separate subfolder in the user's mailbox.

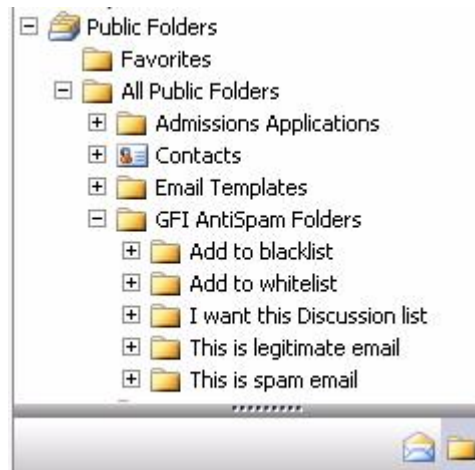


Screenshot 47 - Spam is sorted to a subfolder

This way users can periodically check mail in these folders marked as spam, and identify mail that might have been wrongly marked as spam. Using separate subfolders for each filter allows the user to immediately understand which spam filter flagged the mail as spam.

For more information on how to configure this, see the chapter configuring anti spam.

Adding senders to the white list



Screenshot 48 - White listing an email

If a user wants to add a specific email address to the company white list, all he needs to do is drag and drop the mail to the Public folder "Add to white list", located under the GFI AntiSpam public folders.

GFI MailEssentials will retrieve the mail, and add the MIME FROM Email address (whole email not domain) to the white list.

Use this same procedure for newsletters that you wish to receive, simply drop them in the 'Add to white list' folder.

Note: When dragging and dropping mail, by default Outlook will move the mail. To retain a copy of the mail, hold down the CTRL key, which copies the mail rather than moves it.

Adding senders to the blacklist

To add the sender of a spam mail to the company blacklist, drag and drop the mail to the Public folder "Add to blacklist", located under the GFI AntiSpam public folders. GFI MailEssentials will retrieve the mail, and add the MIME FROM Email address (whole email not domain) to the blacklist

Adding discussion lists to the white list

Often discussion lists (**NOT newsletters**) are sent out without including the recipient email address in the MIME TO and are therefore marked as spam. If you want to receive these discussion lists, you need to white list the email addresses of these valid list mailers.

To add the newsletter to the company white list, drag and drop the discussion list to the Public folder "I want this discussion list", located under the GFI AntiSpam public folders. GFI MailEssentials will retrieve

the mail, and add MIME TO, CC and BCC (whole email not domain) to the white list.

Adding spam to the SPAM database

When a spam mail arrives in the user's inbox, which has therefore not been flagged as spam, users should notify GFI MailEssentials of this. Dragging the mail to the Public folder "This is spam email", will cause GFI MailEssentials to retrieve the mail and add it to the SPAM database. This further improves the performance of the Bayesian filter.

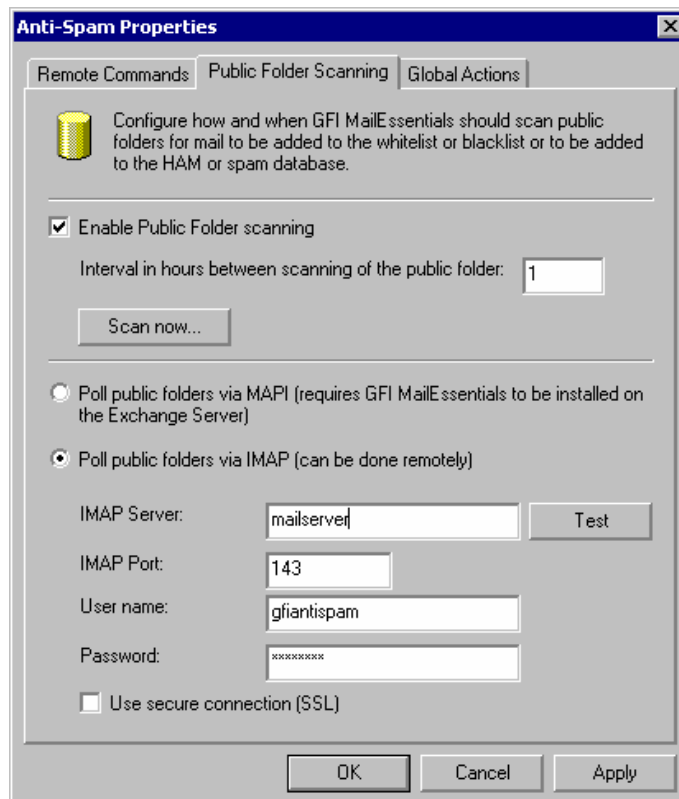
Adding HAM to the ham database

If, whilst reviewing a spam mail a user finds a valid mail, the user should add the mail to the ham database. To do this, the user simply drags the mail to the Public folder "This is legitimate email". Doing this will cause GFI MailEssentials to retrieve the mail and add it to the HAM database, thus further tuning the Bayesian filter and avoiding it being flagged as spam in the future.

Securing access to the public folders

If you don't want to allow all users in your company to add email to the ham, spam or white list database, simply limit access to the public folder from Exchange server.

Configuring Public folder scanning via IMAP or MAPI



Screenshot 49 - Configuring Public folder scanning

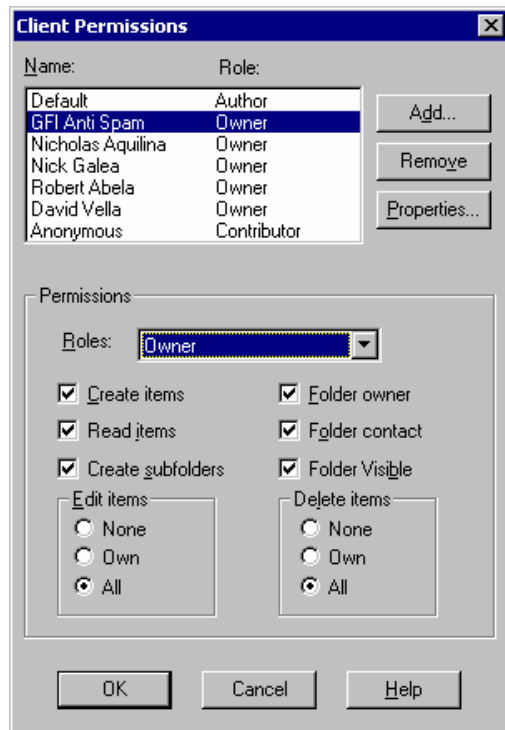
To use the public folder scanning feature, you must configure GFI MailEssentials to scan the public folders. To do this:

1. In the GFI MailEssentials configuration, right-click on the anti-spam node and select properties.
2. Tick the option 'Enable public folder scanning'.
3. Now choose how GFI MailEssentials will retrieve the mails from the public folders:
 - Via MAPI (requires that GFI MailEssentials is installed on the Exchange Server machine itself)
 - Via IMAP (requires that the Ms Exchange IMAP service is started). IMAP allows you to scan the public folders remotely and also works well across firewalls. It can also be used with other mail servers that support IMAP.
4. If you select IMAP, you must specify the mail server name, port (default IMAP port is 143) as well as an account and password. You can also use a secure connection.
5. Click Test. If everything went OK, the public folders will be created automatically. If they do not appear, check the credentials and re-test.

Creating a dedicated account to login via IMAP

If GFI MailEssentials is installed in a DMZ, for security reasons it is recommended to create a dedicated user account to retrieve the mail from the public folders. This user would only have access to the GFI Anti Spam folders. To do this on Exchange 2003:

1. Before you proceed to create the user, use admin credentials and click test to ensure that IMAP is working properly and that the public folders have been created.
2. Create a new user. This user can have limited rights.
3. Open the Exchange System manager and go to Administrative groups > Folders > Public Folders. Right-click on the GFI AntiSpam public folders to bring up its properties
4. Go to the permissions tab and click on the client permissions button.
5. Click 'Add' and select the user you created in step 2 and click OK.



Screenshot 50 - Setting user role

6. Click on the user you just added to the client permissions list and set its role to owner. Make sure all check boxes are enabled and the radio buttons are set to all.
7. Click OK twice to return to Exchange System manager
8. Now right-click on the 'GFI AntiSpam Folders', select 'All tasks' > 'Propagate settings'. Enable the 'Folder rights' checkbox and click OK.
9. Now enter the user name you have created in the GFI MailEssentials configuration and click test to ensure the permissions have been set correctly.

Configuring the GFI AntiSpam folders so that posts are hidden

If desired, you can hide the posts that users make from other users by configuring Exchange Server to hide them.

1. Open the Exchange System manager and go to Administrative groups > Folders > Public Folders. Right-click on the GFI AntiSpam public folders to bring up its properties
2. Go to the permissions tab and click on the client permissions button.
3. Click 'Add' and select the user/group you want to hide the posts from and click OK.
4. Click on the user/group you just added to the client permissions list and set its role to contributor. Make sure that only the 'Create items' check box is enabled and the radio buttons are set to 'none'.
5. Click OK twice to return to Exchange System manager
6. Now right-click on the 'GFI AntiSpam Folders', select 'All tasks' > 'Propagate settings'. Enable the 'Folder rights' checkbox and click OK.

Note: Users will only be able to post to the GFI AntiSpam folders. They will not be able to view any mails, not even the ones they posted themselves.

Configuring Disclaimers

Introduction to disclaimers

What are e-mail disclaimers?

Disclaimers are standard text added to the bottom or top of each outbound e-mail. They can be used for legal and/or marketing reasons

Legal reasons to use a disclaimer

E-mail disclaimers are a good start in helping companies protect themselves from potential legal threats resulting from the contents of an e-mail.

Basically, adding a standard disclaimer to each e-mail will help in case you ever get sued over the content of an e-mail.

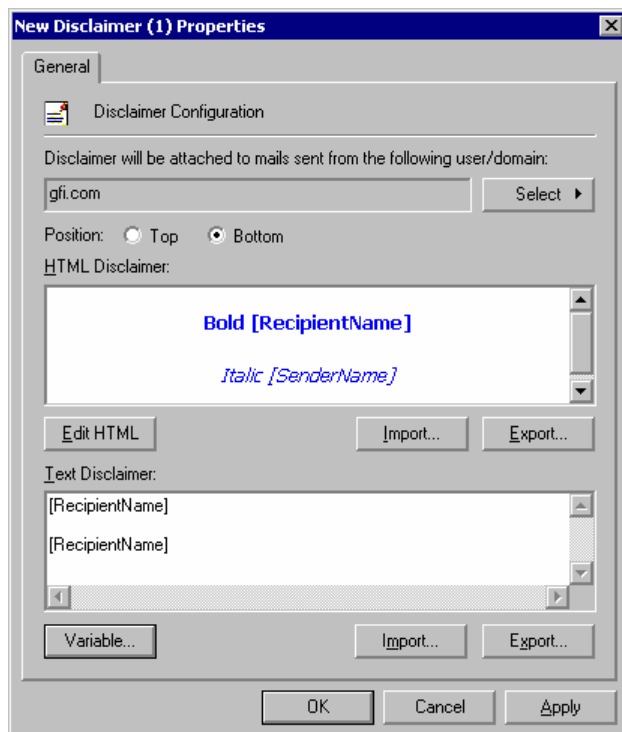
Marketing reasons to use a disclaimer

You can also use a disclaimer to add a description about the products/services your company provides.

Note that disclaimers are only added to outbound mail.

Configuring disclaimers

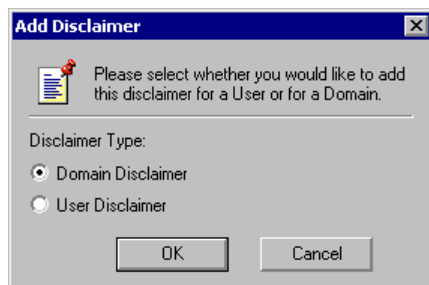
To add disclaimers to your outbound e-mail, go to the disclaimer node in the GFI MailEssentials configuration. You can add different disclaimers for different domains and users.



Screenshot 51 - Adding a disclaimer

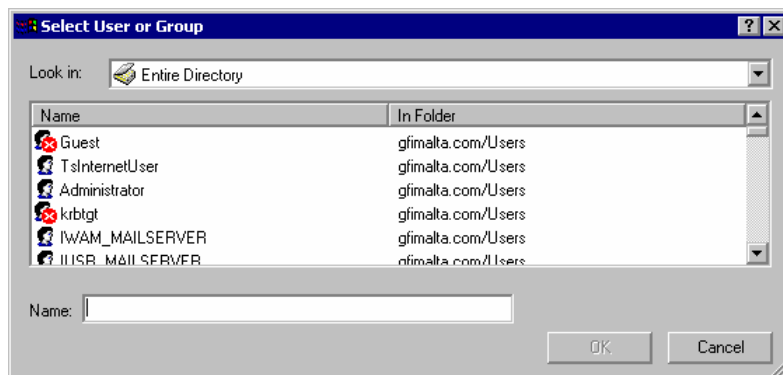
To add a disclaimer:

1. Highlight the Email management > Disclaimer node in the GFI MailEssentials configuration. Right click the mouse, and select **New > Disclaimer**.



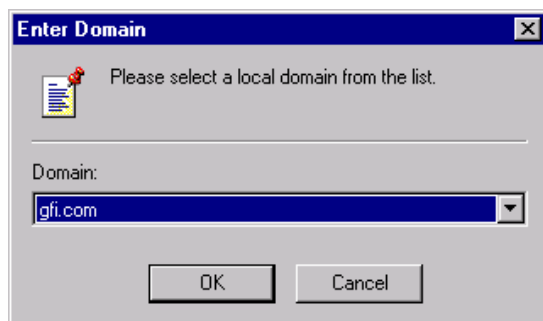
Screenshot 52 - Selecting a user or domain disclaimer

2. Now you can specify whether you wish to add a user based disclaimer or a domain based disclaimer. If you select domain, you can choose the appropriate domain from the list of configured domains. All mails sent FROM that domain will have the disclaimer added. If you select user, you can specify a user or a group of users, and the disclaimer will be added ONLY to mails sent FROM that user or group of users.



Screenshot 53 - Selecting the user or group for which the user based disclaimer will apply

3. If you selected a user based disclaimer, you have to specify the user. If you have installed GFI MailEssentials in active directory mode, you will be able to pick users or groups of users directly from active directory. If you have not installed in Active Directory mode, you have to specify the SMTP email address of the user.



Screenshot 54 - Specifying the domain for a domain based disclaimer

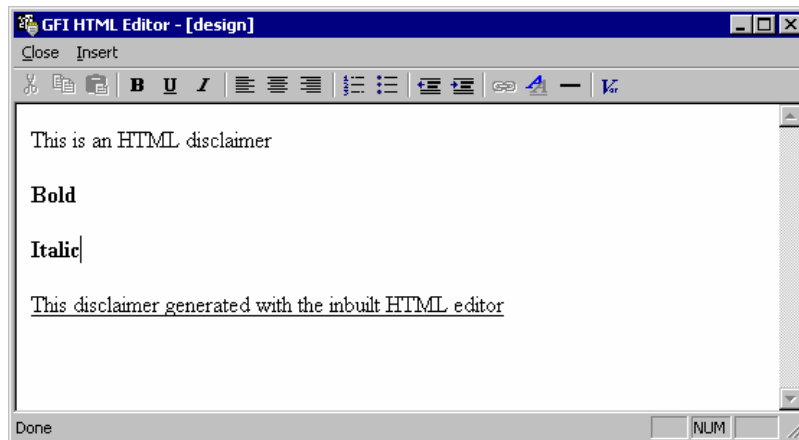
4. If you selected a domain based disclaimer, you have to specify the domain. Note that the disclaimer will only be added if the from address specified in the mail includes the domain you specified! If you use multiple email addresses with different domains, setup the disclaimers for all domains that you use.

5. A new disclaimer will be listed in the right pane. You can now double-click on the disclaimer to bring up the disclaimer properties.

6. You can specify whether the disclaimer should be put at the bottom of the mail or at the top of the mail using the top/bottom 'Position' radio button. You can also change to which mail the disclaimer is added, by clicking on the Select button and selecting the user/group or domain.

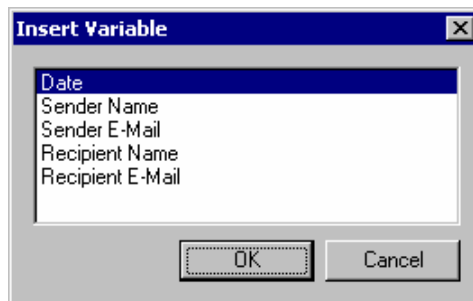
7. You can now create your disclaimer. You can create both an HTML disclaimer and a text only disclaimer. To create an HTML disclaimer, click on 'Edit HTML' to bring up the HTML disclaimer editor. Now enter your disclaimer. You can insert variables using the 'Insert' menu. You can format text and variables using the formatting toolbar at the top. Variables are fields, which will be replaced with the real recipient or sender name in the e-mail. You can include the following fields in a disclaimer text: [recipient display name], [recipient email address], [date], [sender display name] and [sender email address].

After you are ready, click on 'Close'. This will add the disclaimer to the disclaimer properties dialog.



Screenshot 55 - The disclaimer editor

8. You can include a text based version of your disclaimer (for text only emails) directly from the disclaimer properties dialog. Simply insert the text directly into the Text Disclaimer edit field. You can insert variables using the 'Variable' button.



Screenshot 56 - Including variables in your disclaimer

9. If you wish you can import or export your disclaimer using the import and export buttons.

10. Click OK to exit the dialog.

Note: The recipient display name and recipient email address variables will only be replaced if the mail is sent to a single recipient. If a mail is sent to multiple recipients, the variable will be replaced with 'recipients'

Configuring Auto replies

Introduction to auto replies

The Auto reply feature allows you to send automated replies to certain incoming e-mails. You can specify a different auto reply for each e-mail address or subject. You can use variables in an auto reply to personalize an email.

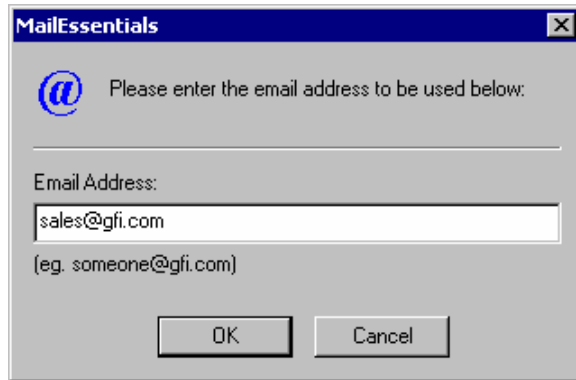
Configuring Auto replies



Screenshot 57 - Auto-reply properties

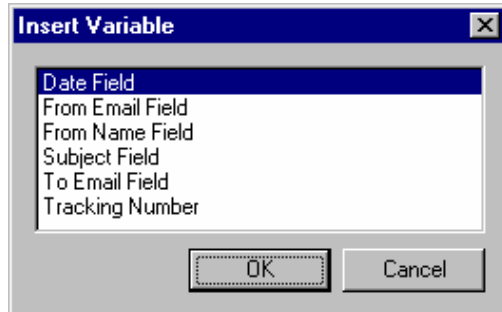
To create an auto reply:

1. Highlight the Email management > Auto replies node in the GFI MailEssentials configuration. Right click the mouse, and select **New > Auto reply**.



Screenshot 58 - Creating a new auto reply

2. Enter the email address for which you wish to create an auto reply. That means that for email sent to this email address, for instance sales@company.com, this auto reply will be sent. Click OK. The auto reply options dialog will now come up.
3. At the top of this dialog you can specify a subject, which the mail must include in order to trigger the auto reply. This is optional. To enable this, specify a subject in the edit box '**And subject contains**'.
4. Now you must specify the auto reply text: Enter the text that you wish to be sent. To import a text file, click '**Import...**'. If you wish to include an attachment, click on '**Add...**' and choose the file you wish to send.
5. You can personalize the auto reply by adding variables. To do this click on '**Variable**'. The following fields are available:



Screenshot 59 - Variables dialog

- Date Field: This will insert the date that the e-mail was sent.
- From Email Field: This will insert the e-mail address of the sender.
- From Name Field: This will insert the name of the sender.
- Subject Field: This will insert the subject of the e-mail.
- To Email Field: This will insert the recipient's e-mail address.
- To Name Field: This will insert the recipient's name.
- Tracking Number: This will insert the tracking number.

Select the variable(s) you wish to insert and click **OK**.

6. When you have prepared the auto reply click OK to activate it.

Other options:

Generate Tracking Number in subject: Activate this option if you wish the auto reply to include a tracking number in the subject. The

tracking number can be used as a point of reference for the recipient and your company. The tracking number will be added to the auto reply and also to the subject of the original mail. Therefore, if you route the mail to a public folder, you can easily search for a customer's email based on the tracking number.

Include email sent: Activate this option if you wish the auto reply to include the e-mail text that was sent.

Auto reply from: You can specify a from email address for your auto reply.

Auto reply subject: You can specify a fixed subject for your auto-reply.

Note: When creating auto reply text, be sure not to format the body text beyond 30-40 characters per line. Alternatively do not include carriage returns. This is because some older mail servers will truncate the line at 30-40 characters. If your text is longer than that and contains a return at the end of the line, your message will be truncated as follows:

Example:

This is a long text line with a return at the end. It looks fine in my editor
This is the next line

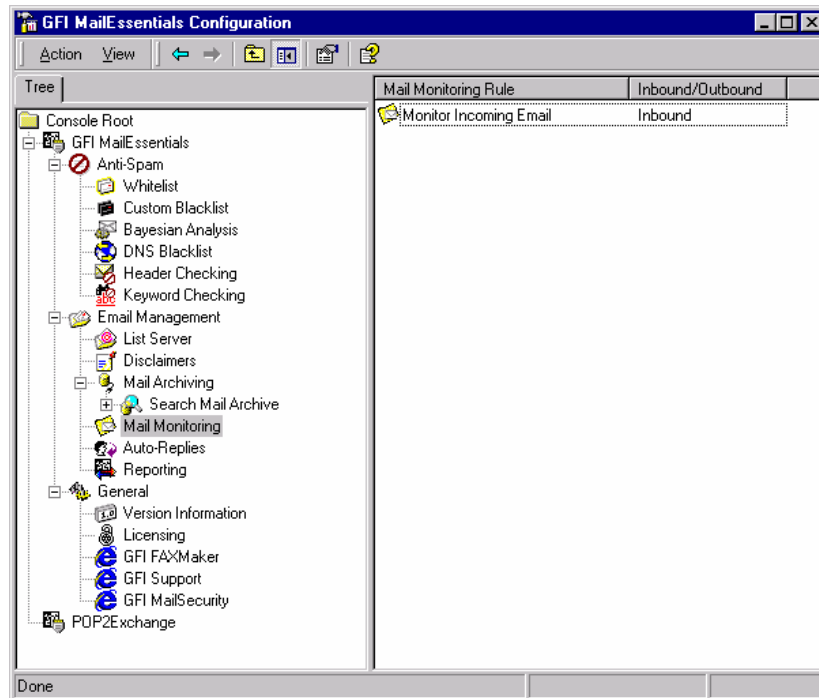
Might look like this:

This is a long text line with a return at the end. It looks
fine in my
editor
This is the next line

Therefore many newsletters that you receive are formatted to avoid this.

Configuring Mail Monitoring

Introduction to Mail monitoring



Screenshot 60 - Monitor specific email addresses

The mail monitoring feature allows you to send a copy of mails sent to or from a particular LOCAL email address to another email address. This allows you to keep a central store of e-mail communications of a particular person or department.

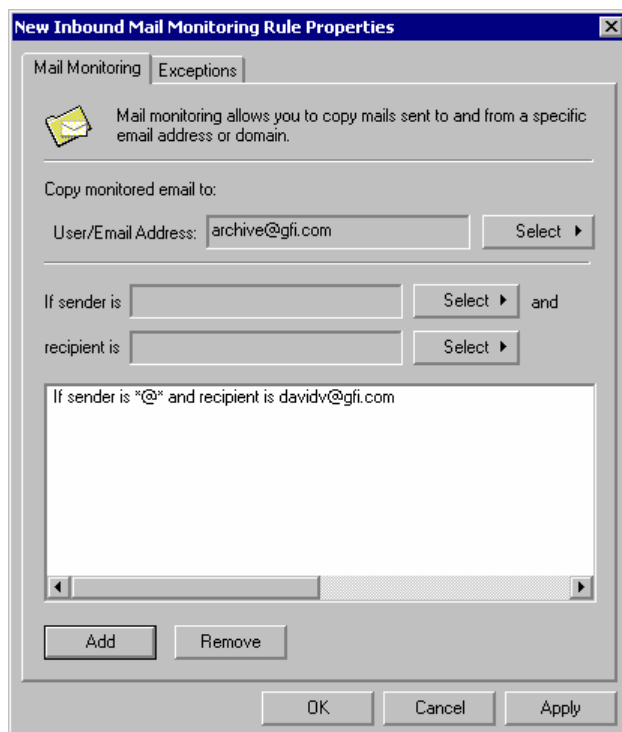
Because you can configure the mail to be copied to an email address, all e-mail can be stored in an Exchange or Outlook store, so that you can easily search for e-mail. Mail monitoring can therefore be used as a replacement for Mail archiving.

Configuring Mail monitoring

Mail monitoring can be configured from the Mail monitoring node. To monitor a particular email address or domain:

1. Highlight the Mail monitoring node in the GFI MailEssentials configuration. Right click the mouse, and select **New > Inbound mail monitoring rule** or **New > Outbound mail monitoring rule**, depending on whether you want to monitor outbound mail or inbound mail with this rule.
2. You will be asked for the email address/mailbox to which you wish to copy the mail. You can specify the email address of a manager or

specify an email address associated with for example a public folder. Click OK. The monitoring rule properties will appear.



Screenshot 61 - Configuring mail monitoring

3. Now specify which email correspondence you wish to monitor by clicking on the sender and the recipient buttons respectively. Click 'Add' to add the mail monitoring filter. You can specify multiple filters.

You can specify both the sender and the recipient of an email, meaning that you can monitor rules from one person to another person. You can also monitor mail from one person to an entire company (domain), or monitor all mail of a particular user. To monitor:

All mail sent by a particular user: Create outbound rule, specify sender email or select user (if using AD) in the sender field and specify the 'all mail' (*@*) in the recipient field.

All mail sent to a particular user: Create inbound rule, specify recipient email or select user (if using AD) in the recipient field and specify 'all mail' (*@*) in the sender field.

Mail sent by a particular user to an external recipient: Create an outbound rule, specify sender or select user (if using AD) in the sender field. Then enter external recipient email in the recipient field.

Mail sent to a particular user by an external sender: Create an inbound rule, specify external sender email in the sender field. Then enter the user name or user email address in the recipient field.

Mail sent by a particular user to a company or domain: Create an outbound rule, specify sender or select user (if using AD) in the sender field. Then specify the domain of the company in the recipient field. To do this select 'domain' when clicking on the recipient button.

Mail sent to a particular user by a company or domain: Create an inbound rule, specify domain of the company in the sender field. To do this select 'domain' when clicking on the sender button. Then enter the user name or user email address in the recipient field.

Exceptions

You can configure exceptions to the rule from the exceptions tab. Here you can exclude mails sent from or to the CEO for example.



Screenshot 62 - Creating an exception

Note that the exceptions are both applied. E.g. all senders listed in the sender exception list and all recipients listed in the recipient list will NOT be monitored.

Enabling/Disabling mail monitoring

You can enable/disable all mail monitoring rules temporarily by switching off inbound/outbound mail monitoring. This can be done from the Mail monitoring properties dialog, which can be accessed by right-clicking on the mail monitoring node



Screenshot 63 - Enable or disable mail monitoring

You can also disable an individual mail monitoring rule temporarily, by right clicking on the rule and selecting disable.

Configuring the list server

Introduction to list servers

List servers allow you to create two types of distributions lists:

1. A newsletter subscription list. – this type of list can be used for a company or product newsletter. The big advantage over using normal emailing software, is that creating a list allows users to unsubscribe or subscribe to the list.
2. A discussion list – this type of list allows a group of people to hold a discussion via email, with each member of the list receiving the mail that a user sends to it.

Typically, list server software is very expensive. Furthermore it required that you run the list server on a separate machine from the Exchange server, since port 25 is already taken by Exchange.

GFI MailEssentials now brings powerful list server capabilities to Exchange Server users, at a small price and without the need to dedicate an additional machine for the list server alone.

Requirements of the list server feature

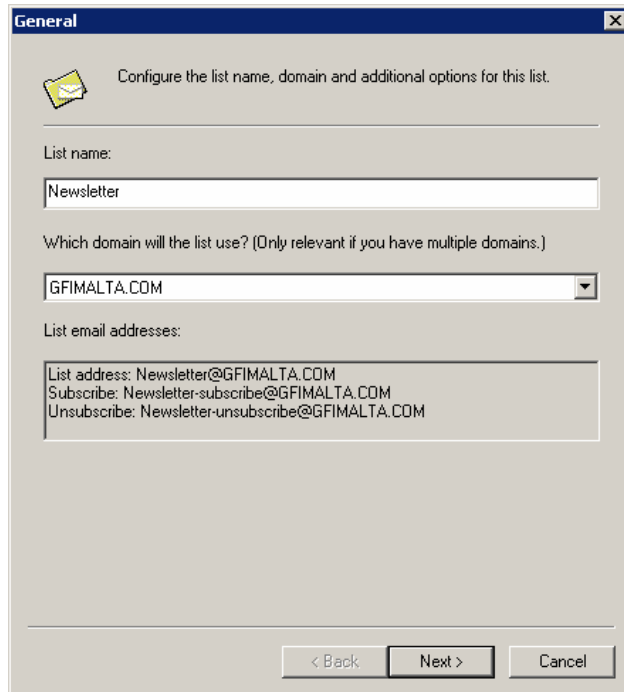
The list server feature requires the installation of Microsoft Message Queuing Services. This is a scalable system service developed by Microsoft to enable high volume event processing. GFI MailEssentials 10 uses this service. It is included with every Windows 2000/2003 and XP version, although not always installed by default.

To check whether it is installed and if not how to install it, see the last paragraph of this chapter.

Creating a list

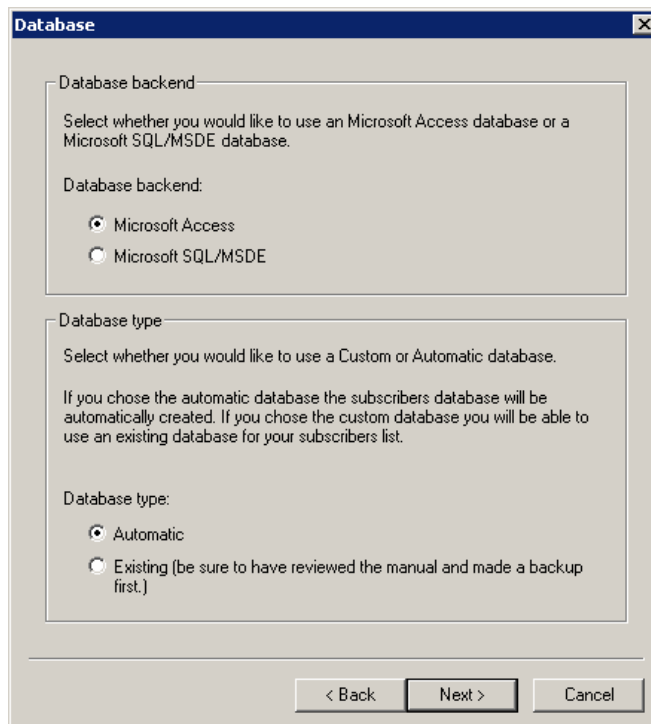
To create a newsletter list:

1. Right-click on the email management > list server node and select New > Newsletter



Screenshot 64 - Creating a new newsletter list

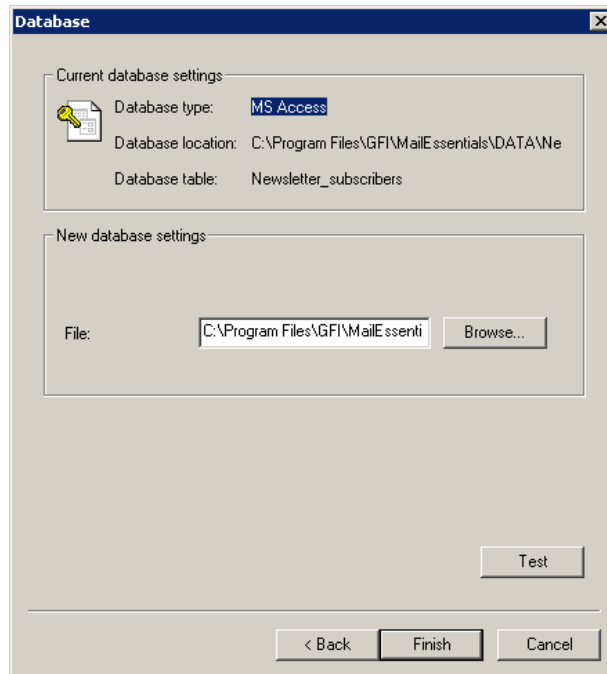
2. The general list dialog will appear. Here you can enter a name for the list, and also specify the domain of the list (if you have multiple domains). Click Next to continue



Screenshot 65 - Specifying database backend

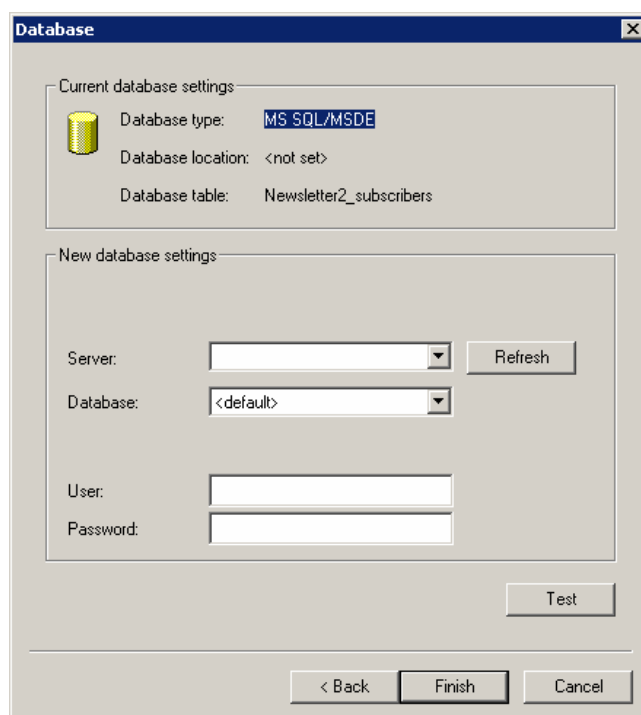
3. Next you need to specify the type of database backend. For smaller lists of up to 5000 members, you can use Microsoft Access as a backend.

4. You can specify whether GFI MailEssentials should create a new database or connect to an existing database. The latter allows you to use an existing customer database for the newsletter list. Click Next



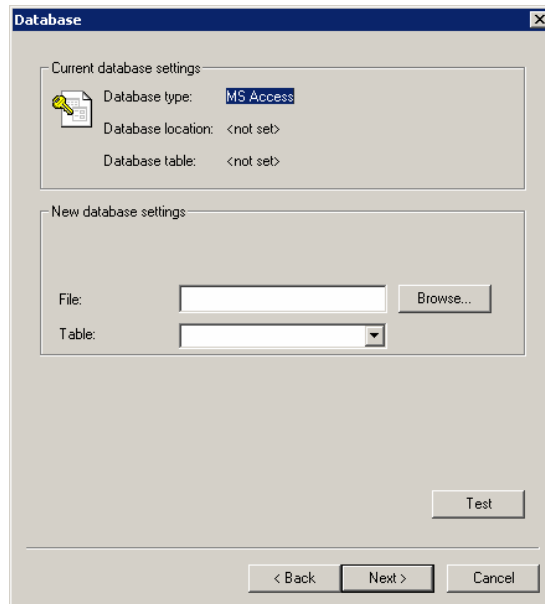
Screenshot 66 - Specifying Microsoft Access details

5. If you selected 'Automatic' and selected Microsoft Access as the database backend, you have to configure a file name and location for the database. Click Finish to end the wizard. The wizard will confirm creation of database and table. The newsletter list will now be created in the right hand pane and you can further configure its options by right clicking on the list and selecting properties



Screenshot 67 - Specifying SQL server details

If you selected 'Automatic' and selected Microsoft SQL server, you can configure the SQL server name, the database and the credentials. Click Finish to end the wizard. The wizard will confirm creation of the table. The newsletter list will now be created in the right hand pane and you can further configure its options by right clicking on the list and selecting properties

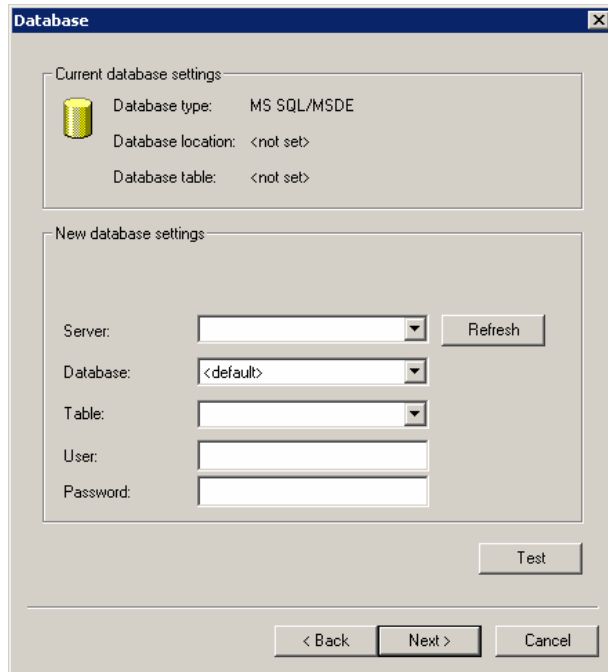


Screenshot 68 - Specifying existing Microsoft Access database file and table

6. If you selected 'Existing database' and selected Microsoft Access as the database backend, you have to enter the path to the file name and enter the table name which contains the subscriber members.

Then you have to map the EMAIL field to a string value field containing the email address. In addition you have to map the UNSUBSCRIBE field to an integer (or Boolean) value field which will be used to define whether the user is subscribed to the list or not. This field is there so that when a user unsubscribes from the list we do not delete the user's entry, but rather just unsubscribe them from the list.

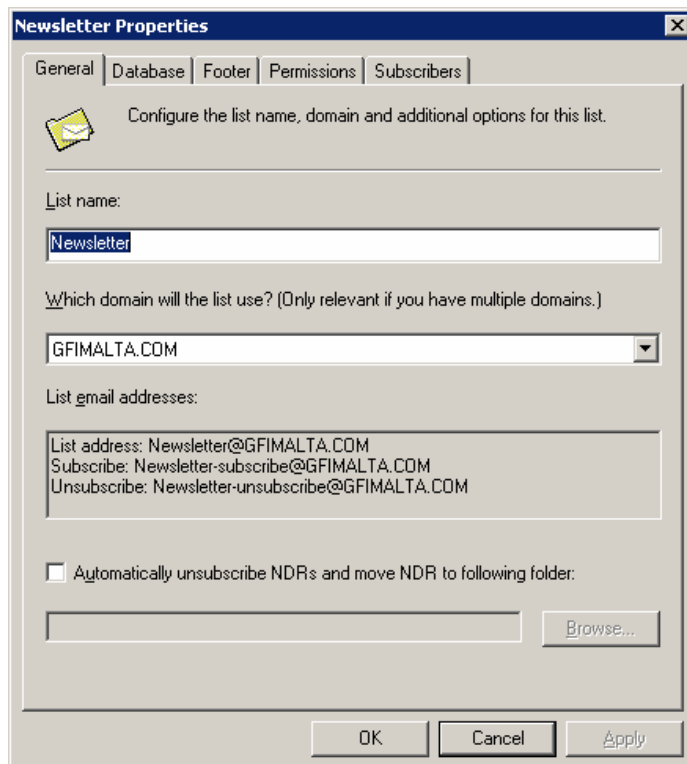
If you selected Existing database and selected Microsoft SQL server as the database backend, you have to enter the SQL server details, as well as the table name which contains the subscribers and the credentials to logon to the database. Then you have to map the fields as described above.



Screenshot 69 - Specifying existing SQL server table

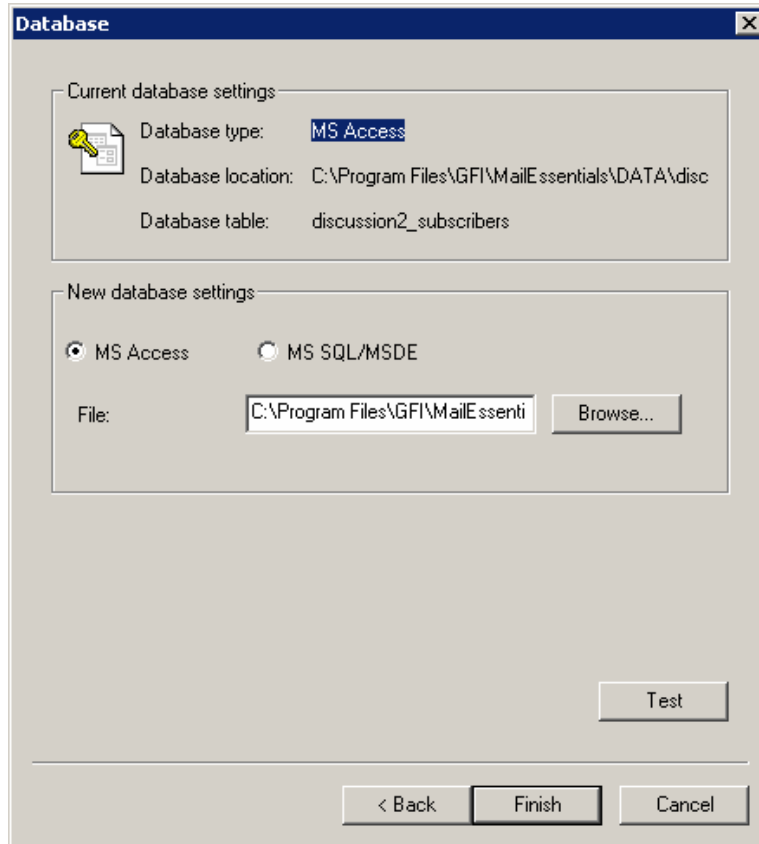
Newsletter properties

After you have created the newsletter list, you can further configure its properties. To do this, right click on the newsletter in the right hand pane and select 'Properties'. This brings up the newsletter properties dialog.



Screenshot 70 - General newsletter properties

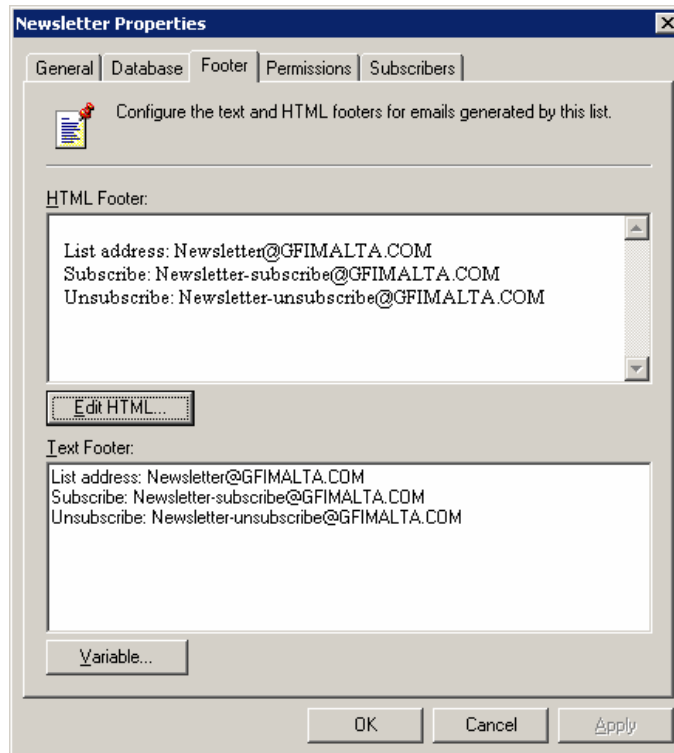
The general newsletter properties dialog allows you to change the list name, as well as its domain. In addition you can specify that if the list server receives an NDR, it automatically unsubscribes the user.



Screenshot 71 - Database newsletter properties

In the database tab, you can modify the database settings of the list.

Creating a custom footer for the list

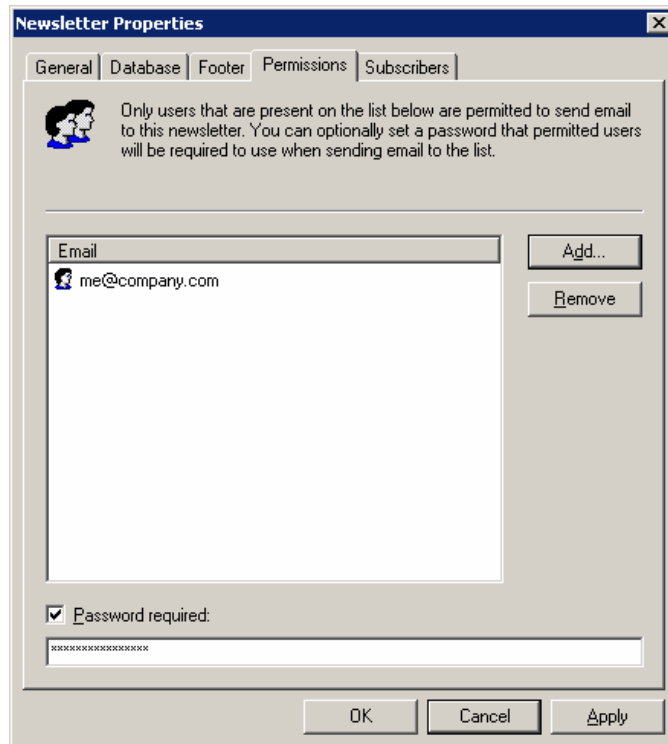


Screenshot 72 - Footer newsletter properties

The footer tab allows you to configure a custom HTML or text footer. This footer will be added to each mail. Click Edit HTML to create an HTML footer.

Use the footer to communicate how users can subscribe to the list and unsubscribe from the list.

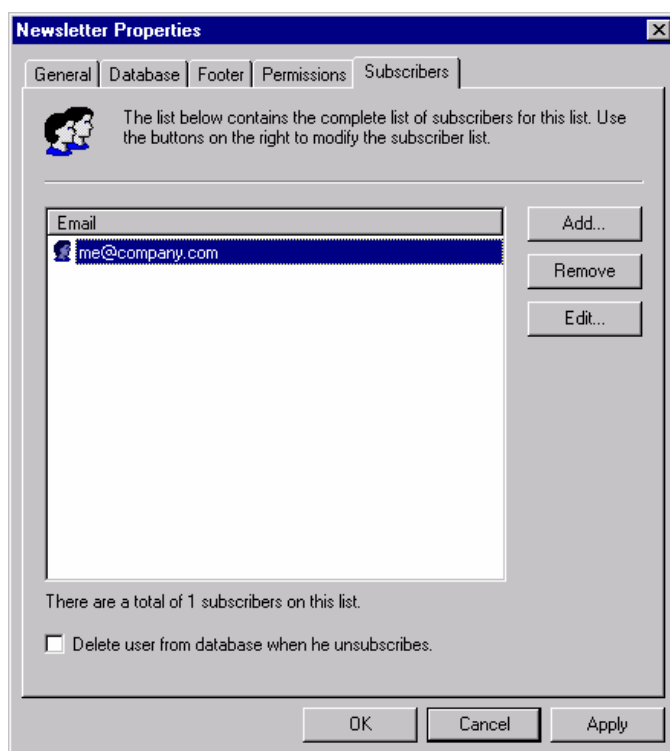
Setting permissions to the list



Screenshot 73 - Setting permissions to the newsletter

The permissions tab allows you to specify who can submit a mail to the list. If you do not secure the list, anybody can send a mail to the entire list by sending a mail to the list address! Click Add to specify a user with permissions to submit a mail to the list.

Adding subscribers to the list



Screenshot 74 - Entering subscribers to the newsletter

The subscribers tab allows you to add/remove users to the list manually. However, we recommend that you allow users to subscribe specifically to the list. If you import users, and have not specifically asked their permission to be added to the list, you might get spam complaints. Therefore if anything send out a mailing asking them to subscribe at newsletter-subscribe@yourdomain.com

Operating the newsletter list.

Sending a newsletter

Sending a mail to the entire list is very easy. Members who have permission to send a mail to the list (This is configured from the permission tab in the newsletter properties), just send the mail to the newsletter list mailing address, which is <newslettername>@yourdomain.com

Subscribing to the list

We recommend that you allow users to subscribe specifically to the list. If you add users to the list without specifically asking their permission, you might get spam complaints. Therefore we recommend sending out a mailing and asking them to subscribe by sending a mail to <newslettername>-subscribe@yourdomain.com

Subscription process

To subscribe to a newsletter, a user has to send a subscription request to <newslettername>-subscribe@yourdomain.com. Upon receiving the request, the list server will send a confirmation email to

the user. Only after confirming his subscription by replying to the confirmation email, will the user be added as a subscriber. The confirmation email is required and can not be turned off. It will save you a lot of spam complaints.

Unsubscribing from the list

To unsubscribe from the list, users simply send a mail to <newslettername>-unsubscribe@yourdomain.com

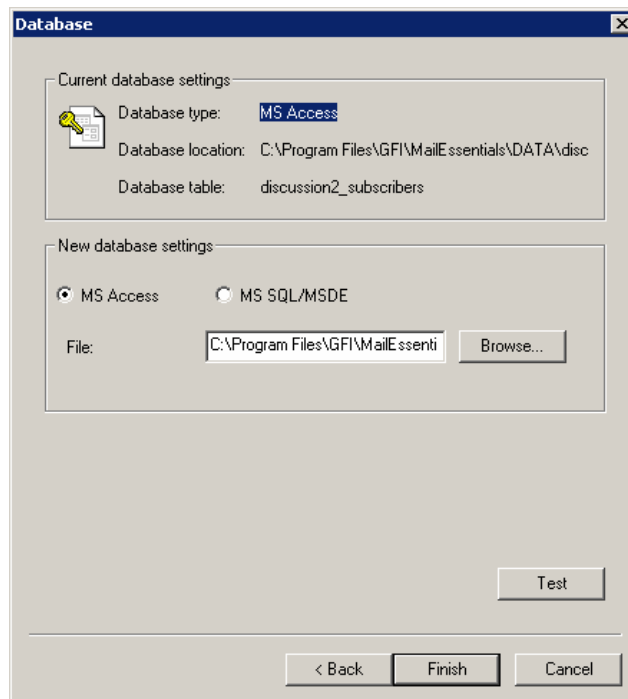
Adding a link to your web site

To allow users to easily subscribe to your newsletter, simply add a small web form which asks for name and email address and direct the output to the <newslettername>-subscribe@yourdomain.com

Creating a discussion list

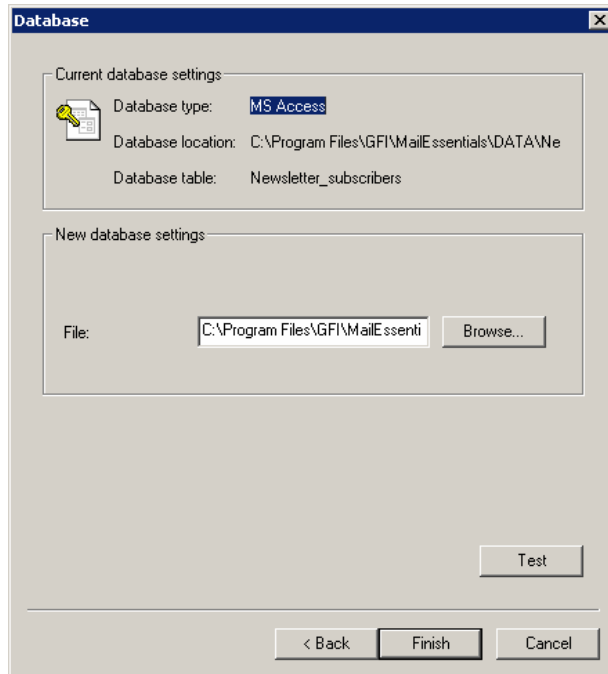
Creating a discussion list is largely the same as a newsletter list. To create a discussion list:

1. Right-click on the Email management > list server node and select New > Discussion list
2. The general list dialog will appear. Here you can enter a name for the list, and also specify the domain of the list (if you have multiple domains). Click Next to continue



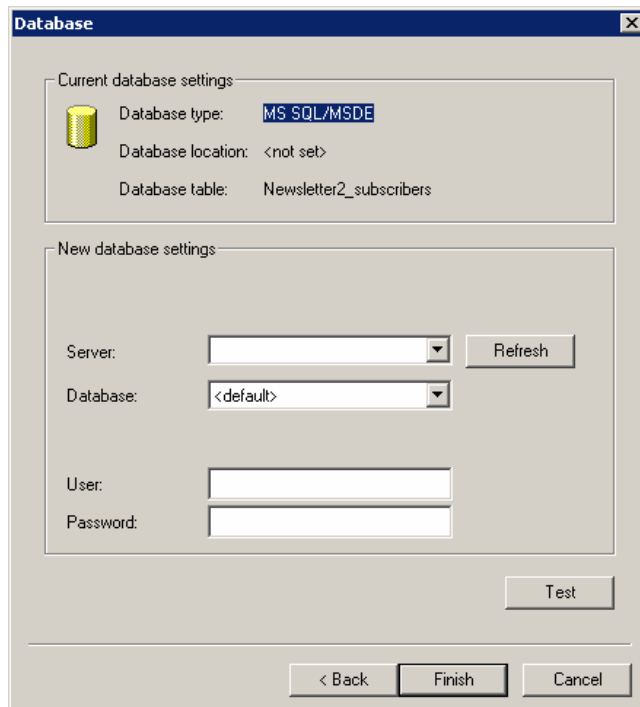
Screenshot 75 - Specifying database backend

3. Next you need to specify the type of database backend. In general, we recommend using Microsoft SQL server if you have more then 5 lists OR one of the lists has more then 1000 members.



Screenshot 76 - Specifying Microsoft Access details

4. If you selected Microsoft Access, you can configure a file name and location for the database. Click Finish to end the wizard. The wizard will confirm creation of database and table. The discussion list will now be created in the right hand pane and you can further configure its options by right clicking on the list and selecting properties



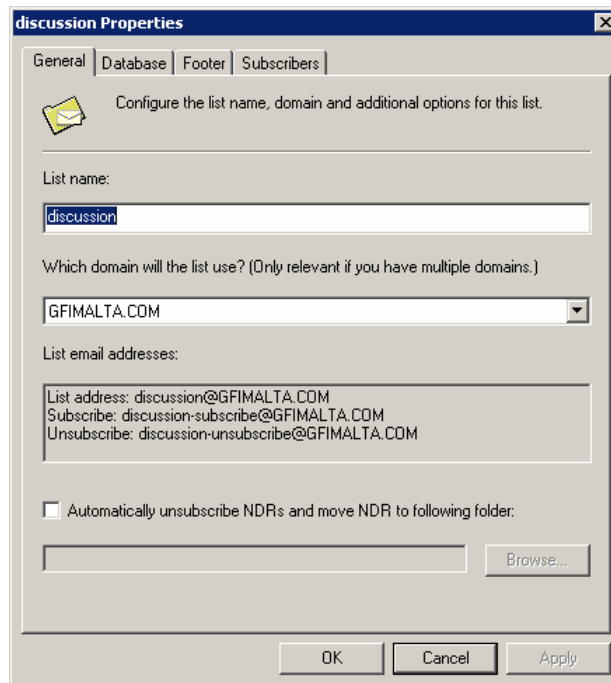
Screenshot 77 - Specifying SQL server details

If you selected Microsoft SQL server, you can configure the SQL server name, the database and the credentials. Click Finish to end the wizard. The wizard will confirm creation of the table. The list will now

be created in the right hand pane and you can further configure its options by right clicking on the list and selecting properties

Discussion list properties

After you have created the discussion list, you can further configure its properties by right clicking on the discussion list and selecting 'Properties'. This brings up the discussion list properties dialog.



Screenshot 78 - General discussion list properties

The general tab allows you to change the list name, as well as its domain. In addition you can specify that if the list server receives an NDR, it automatically un-subscribes the user. In the database tab, you can modify the database settings of the list.

Creating a custom footer for the list

The footer tab allows you to configure a custom HTML or text footer. This footer will be added to each mail. Click Edit HTML to create an HTML footer. Use the footer to communicate how users can subscribe to the list and unsubscribe from the list.

Adding subscribers to the list

Adding subscribers to the list is identical to adding subscribers for a newsletter list. The subscribers tab allows you to add/remove users to the list manually.

Importing subscribers to the list / Database structure

When you create a new newsletter OR discussion list, the configuration will create a table called 'listname_subscribers' with the following fields as shown in the table below.

If you wish to import data into the list, simply ensure that the database is populated with the correct data in the correct fields.

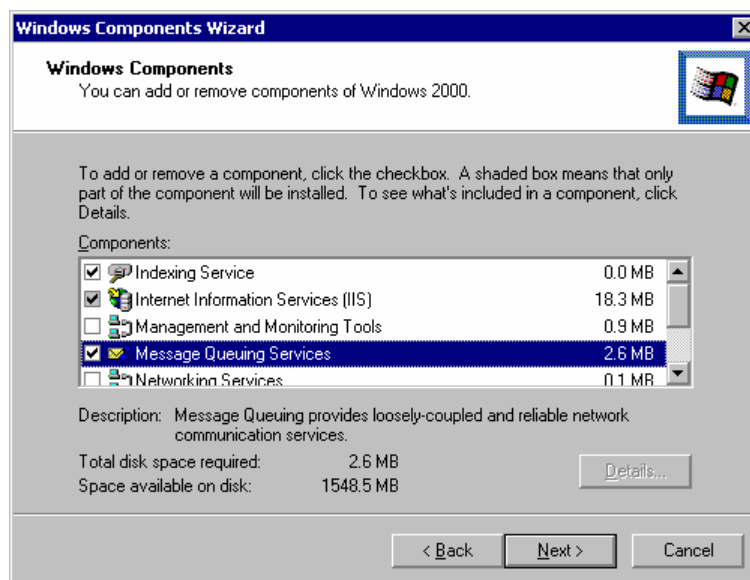
Field name	Type	Default Value	Flags	Description
Ls_id	Varchar(100)		PK	Subscriber ID
Ls_first	Varchar(250)			First name
Ls_last	Varchar(250)			Last name
Ls_email	Varchar(250)			Email
Ls_unsubscribed	Int	0	NOT NULL	Unsubscribe flag
ls_company	Varchar(250)			Company name

Table 1 - Fields automatically created for the list

Installing the Message Queuing services (MSMQ) on Windows 2000

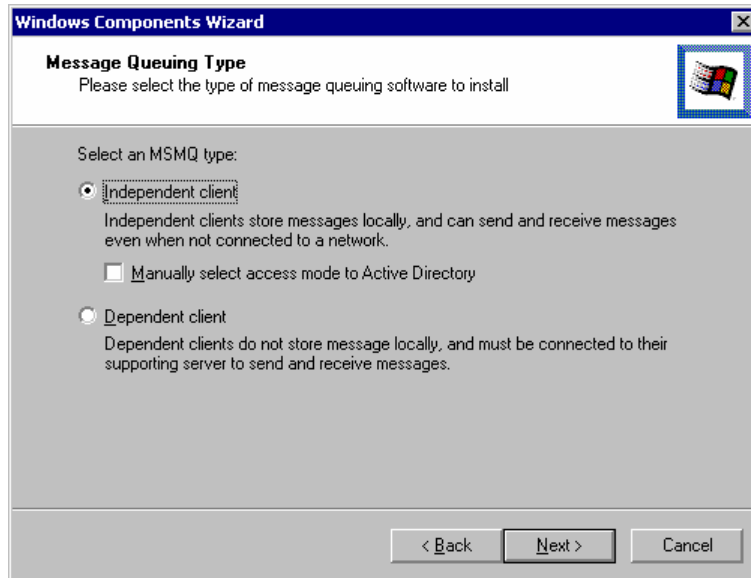
The Messaging queue is a scalable system service developed by Microsoft to enable high volume event processing. GFI MailEssentials uses this service. It is included with every Windows 2000/2003 and XP version, although not always installed by default. To check whether it is installed or install it;

1. To check if it is installed, simply go to Control Panel > Add/Remove Programs > Windows Components. The Windows components wizard will appear. Now check if a tick mark is present next to 'Message Queuing Service'.



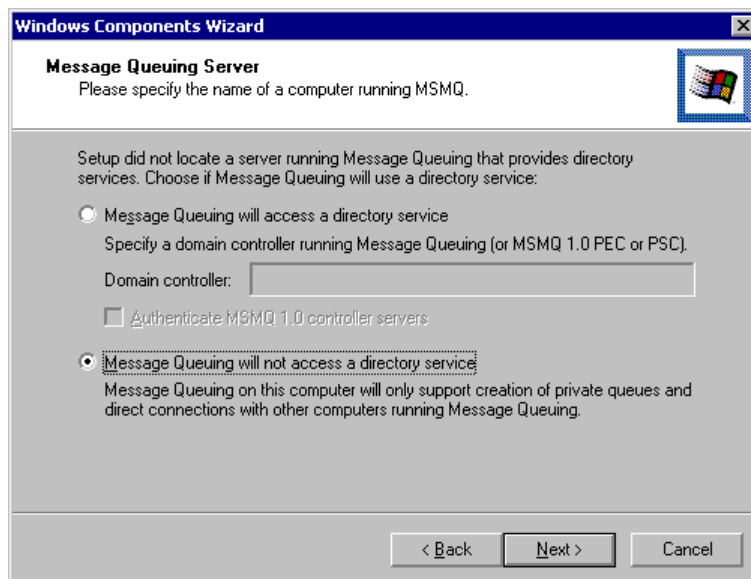
Screenshot 79 - The Windows components wizard

2. If there is no check mark selected, you need to install the Message queuing service. To do this, select the checkbox and click Next. You will need to have your Windows 2000 CD handy.



Screenshot 80 - Selecting the Message Queuing type

3. You will now be asked to select what type of queue to install. Select 'independent client'.



Screenshot 81 - Message queue will not access a directory service

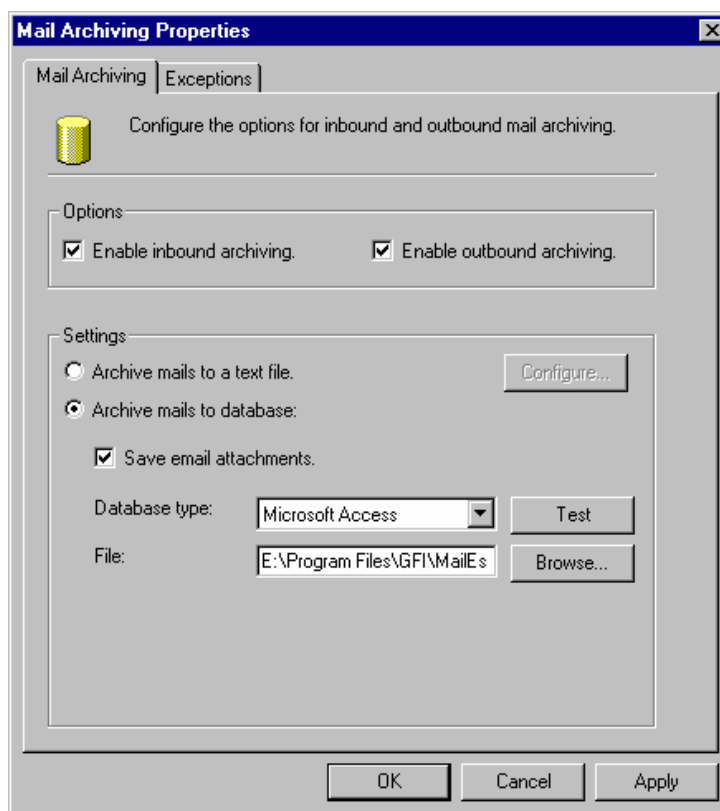
4. After you select independent, you will be asked if the Message Queue will be connecting to a directory service. Select 'Message Queuing service will not access a directory service'. Select Next. The Message Queuing service will now be installed.

Configuring Mail Archiving

Introduction to Mail archiving

The archiving feature allows you to archive all in- and outbound mail. This feature can be used to store a history of your email communications. In some countries and industries this is required by law.

Configuring Mail archiving



Screenshot 82 - Archiving properties

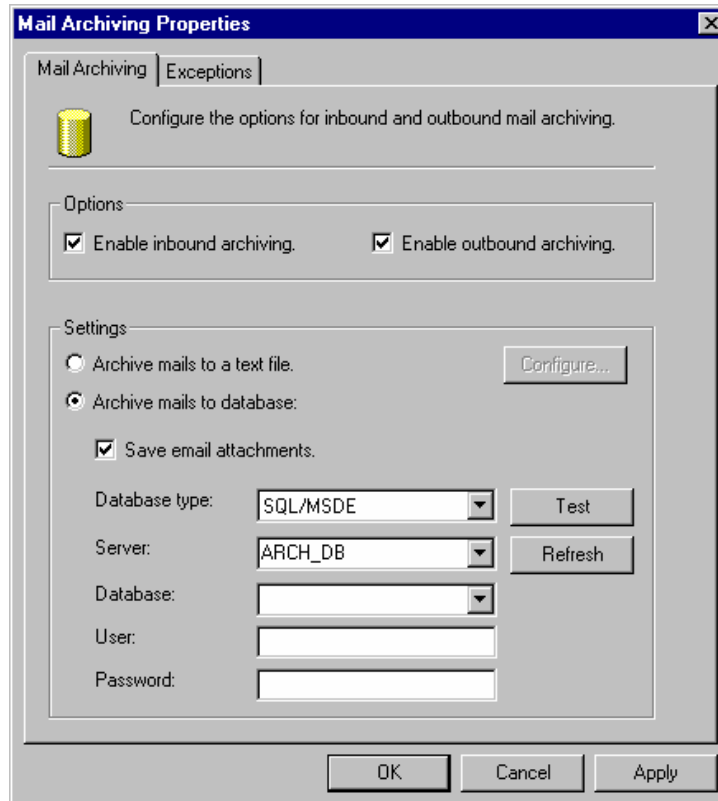
To archive mail:

1. In the GFI MailEssentials configuration, highlight the mail archiving node, right click and select properties. This brings up the Mail Archiving properties dialog.
2. You can now specify to archive inbound and/or outbound mail.

Enable Inbound archiving: Select this option to enable archiving of inbound mail.

Enable Outbound archiving: Select this option to enable archiving of Outbound mail.

3. Then choose whether to archive mail to a database or to a text file.
4. If you want to archive mail to a text file, click on the button 'Configure' to select the location and filename to which MailEssentials should archive the mail. Be sure to select a drive with ample disk space! Note: If you archive to a text file, attachments will not be archived.
5. If you want to archive mail to a database you have to select which database you wish to use. Although you can archive mail to an access database file, this is not very practical, considering the amount of data that will be archived.



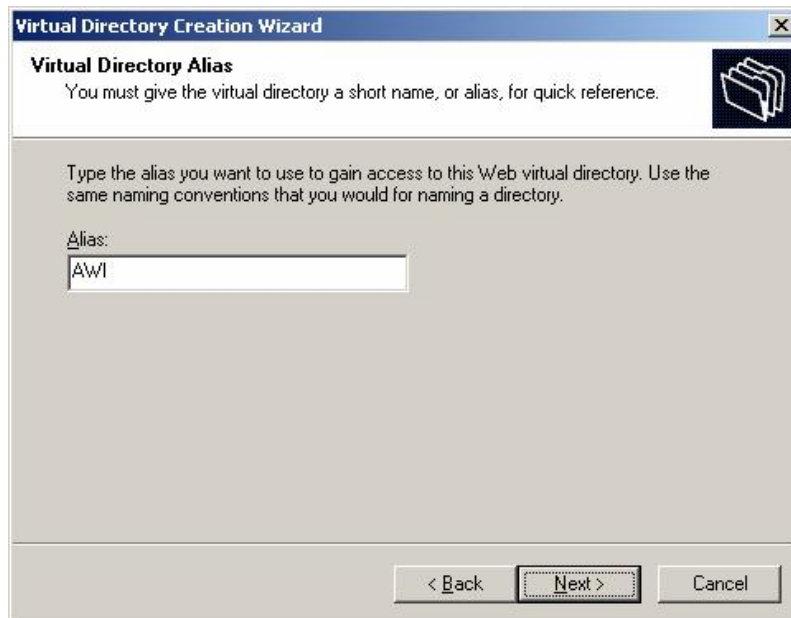
Screenshot 83 - SQL server settings

6. Select SQL/MSDE (note that if you select MSDE there is a limit of 2 gigabyte) and specify server name, database and credentials.

Configuring the search page (AWI)

Mail archived by the archiving module can be searched using a web based front end, called the Archive Web Interface (AWI). To use this front end, you have to configure IIS and configure the asp search page included with GFI MailEssentials. To do this:

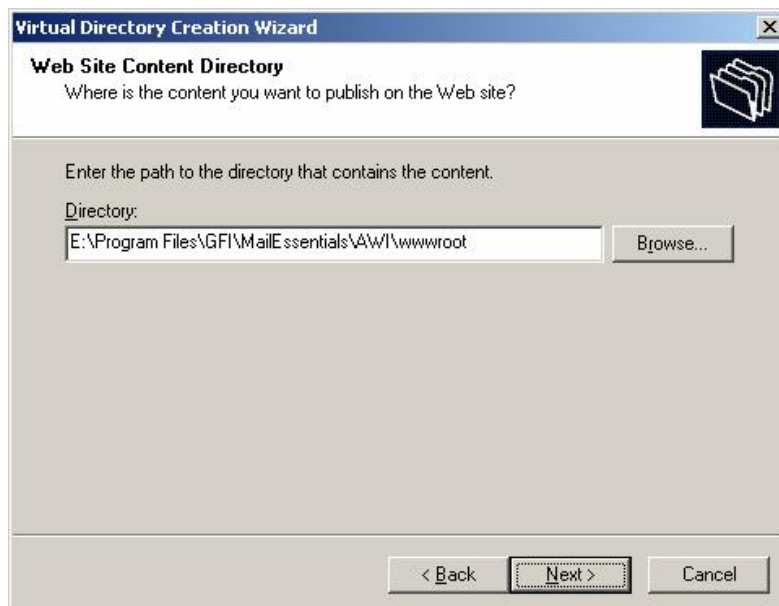
1. Start up Internet Services Manager, right click on the Web Site node, and from the popup menu select New – Virtual Directory.



Screenshot 84 - Specifying an alias for the virtual directory

2. This will start the Virtual Directory Creation Wizard. Click Next to continue. Now you need to enter an alias for the virtual directory. In this case it is AWI, but you can enter whatever name you like, as long as it follows the folder naming conventions used in Microsoft Windows.

3. Now enter the path where the content is located. Select browse, and select the folder AWI\wwwroot in the MailEssentials installation path.

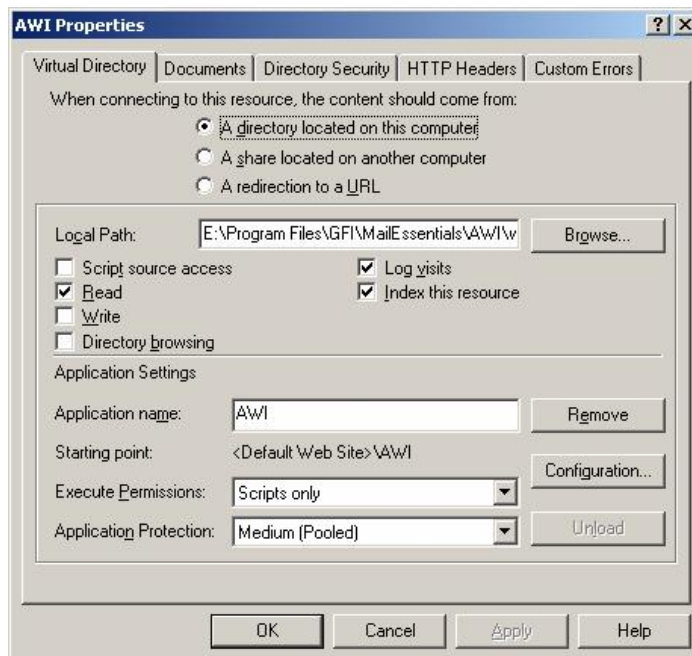


Screenshot 85 - Pointing to the AWI web folder



Screenshot 86 - Setting permissions

4. Next we need to set the access permissions. Tick 'Read' and Run Scripts only. Do not tick any of the other check boxes. Now click next to finish the Virtual Directory Creation Wizard.
5. Right-click on the newly created virtual directory, located under the web root of your web site server and select properties.
6. In the Virtual Directory tab of the properties dialog, tick the 'Read', the 'Log Visits' and the 'Index this resource' check boxes. For Execute Permissions, select Scripts Only.
7. Press OK to close the properties dialog. The Virtual Directory has been set-up and you can now test access to it.



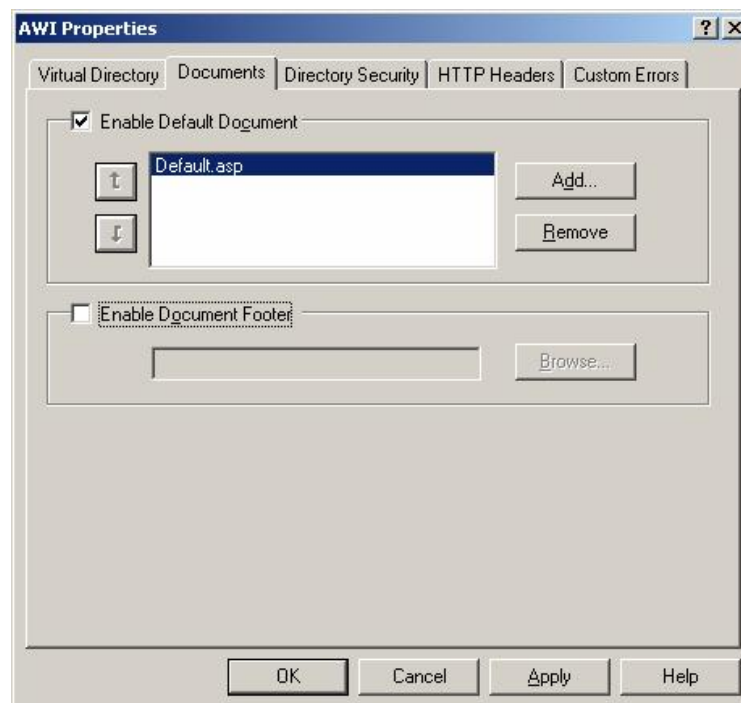
Screenshot 87 - Setting Virtual Directory properties

Securing the Archive Web Search Interface

Since the Archive Web Interface provides access to all the emails archived by MailEssentials, it is important to setup proper authentication and security for this web server and virtual directory. There are three ways to secure the Search Interface. These are Basic Authentication, Digest and Integrated Windows Authentication. Integrated Windows Authentication is the preferred choice in an Active Directory environment, because it makes the authentication process seamless, since initially it does not prompt users for their user name or password information. Rather, it uses the current Windows user information on the client computer for authentication. If you are installing GFI MailEssentials in a DMZ, you must use Basic authentication.

The following steps show how to secure access to AWI:

1. Open up Internet Services Manager. Right click on the Archive Web Interface virtual directory under your server web site and select properties.
2. Under the Virtual Directory tab make sure to deselect Directory Browsing.
3. Select the Documents tab and remove all the default documents except for default.asp



Screenshot 88 - Specify default document

4. Next select the Directory Security tab and click on the Edit button for the Anonymous access and authentication control group.
5. Select Integrated Windows authentication (recommended if installed on the internal network) OR Basic Authentication check box (if installed in the DMZ). Ensure Anonymous access is deselected.

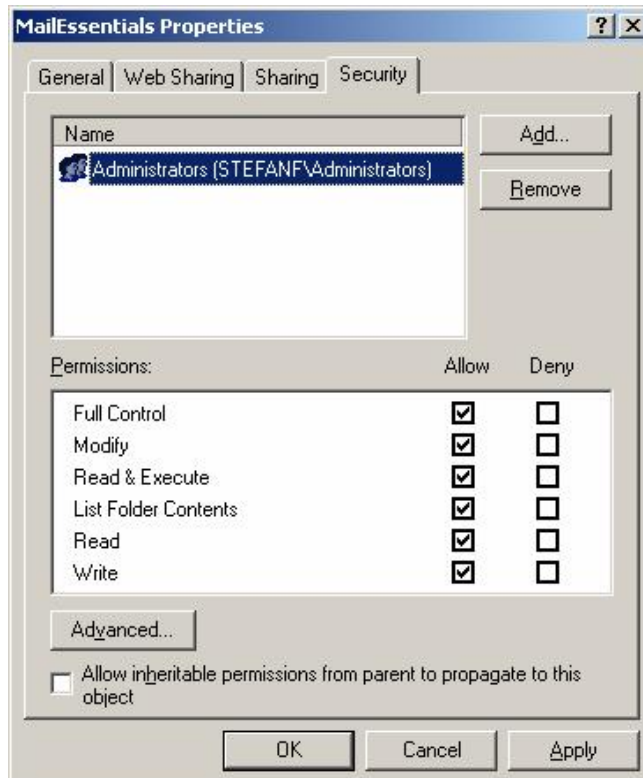


Screenshot 89 - Select authentication method

If using Integrated Windows authentication, then authentication will occur against Active Directory. This means you do not need to configure additional users. If you use basic authentication, authentication will occur against the local user database on the machine. In this case you must create user names and passwords on that local machine. For more information on securing IIS, please review the IIS documentation.

Be sure not to allow anonymous access!

6. Now restrict access to the accounts you want by using NTFS permissions. Open up Explorer and navigate to the MailEssentials folder. Right click on the MailEssentials folder and select properties and then the Security tab.



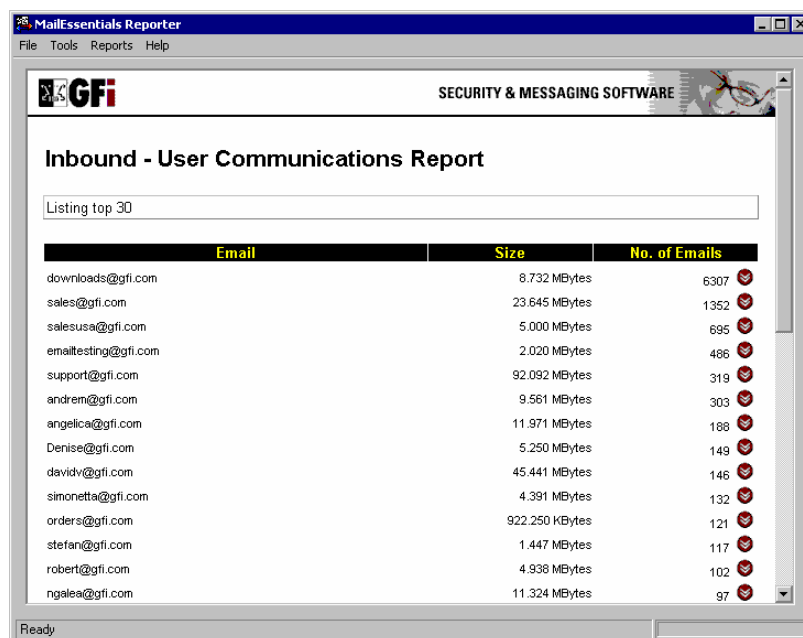
Screenshot 90 - Setting permissions

7. Add / remove the users / groups you want to allow access to the Archive Web Interface. To allow access only to users forming part of the administrators group you would set the security tab as in the screenshot. Click OK. You have now secured the Archive Web Interface.

Generating Mail Reports

Introduction

The GFI MailEssentials Mail reporter allows you to generate useful reports regarding inbound and outbound mail traffic. For example, you can generate reports on number of mails sent per user, per domain, or just daily statistics of mail traffic.



The screenshot shows the GFI MailEssentials Reporter application window. The title bar reads 'MailEssentials Reporter'. The menu bar includes 'File', 'Tools', 'Reports', and 'Help'. The main window displays the GFI logo and 'SECURITY & MESSAGING SOFTWARE'. The report title is 'Inbound - User Communications Report'. Below the title is a search box containing 'Listing top 30'. A table lists the top 30 email addresses with their respective sizes and the number of emails sent. Each row has a small red icon to its right.

Email	Size	No. of Emails
downloads@gfi.com	8.732 MBytes	6307
sales@gfi.com	23.645 MBytes	1352
salesusa@gfi.com	5.000 MBytes	695
emailtesting@gfi.com	2.020 MBytes	486
support@gfi.com	92.092 MBytes	319
andrem@gfi.com	9.561 MBytes	303
angelica@gfi.com	11.971 MBytes	188
Denise@gfi.com	5.250 MBytes	149
davidv@gfi.com	45.441 MBytes	146
simonetta@gfi.com	4.391 MBytes	132
orders@gfi.com	922.250 KBytes	121
stefan@gfi.com	1.447 MBytes	117
robert@gfi.com	4.938 MBytes	102
ngalea@gfi.com	11.324 MBytes	97

Screenshot 91 - The MailEssentials reporter

Configuring GFI MailEssentials reporter

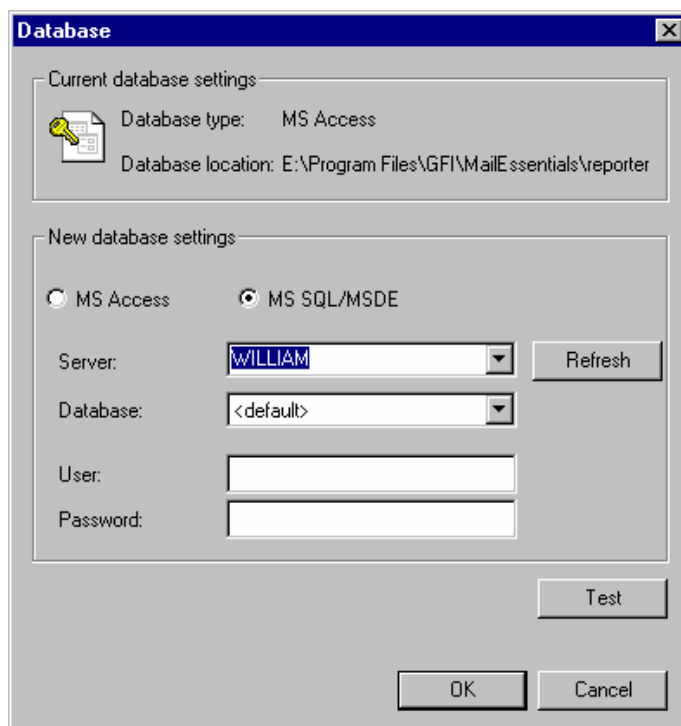
Reporting data is generated from data logged to a database. GFI MailEssentials can log data to a Microsoft Access file or to a Microsoft SQL server database.

For larger networks, we recommend using Microsoft SQL server. If you do not have Microsoft SQL server, or if the database server is not accessible from where you have installed GFI MailEssentials, you can use the Microsoft Access format to log data to. This capability is built in to the operating system and does not require the installation of Microsoft Access. Note however that a file limit of 2 gigabytes is imposed on the file. Before the file reaches that size you need to start logging to a new database.

To configure the database type to which GFI MailEssentials should log to:

1. In the GFI MailEssentials configuration, go to the Email management > Reporting node.

2. Right click on the node and select properties. This will bring up the reporting properties dialog. Click on the configure button.
3. Specify Microsoft Access or Microsoft SQL server.
4. If you specify Microsoft Access, specify the file name and location.



Screenshot 92- Configure database

5. If you specify Microsoft SQL server, specify the server name and the credentials.
6. Click Test to ensure you have configured the database correctly. Click OK to exit.

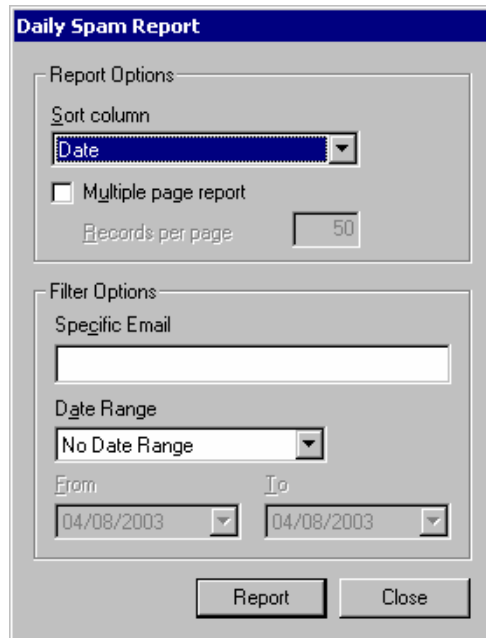
Daily spam report

Day	Total Processed	Total Spam	Keyword Checking	Header Checking	Blacklist	Spam Percentage
6/12/2003	4293	830	366	450	14	19%
6/13/2003	7484	1916	788	1101	27	26%
6/14/2003	4775	1648	710	914	24	35%
6/15/2003	3081	1458	567	867	24	47%
6/16/2003	4495	1253	504	730	19	28%
Total Processed	24126	7105	2935	4062	108	29%

Screenshot 93 - Daily spam report

The Spam report shows you how much spam MailEssentials caught as a percentage of total mails received.

The daily spam report can be generated via the Reports > Daily Spam menu option. This will bring up the report options dialog. You can specify the following options for the report:



Report Options

'Sort column' allows you to specify whether the report should be sorted by date, total spam processed, keyword checking etc. For example, if you sort on keyword checking, it will list the days on which most emails were caught via keyword checking at the top.

'Multi Page report' allows you to specify the number of days you wish to display on each page.

Filter options

'Specific email' This filter option allows you to limit the report to a specific email address.

'Date range' This filter option allows you to limit the report to a specific date range.

When you have specified the report options, click on the 'Report' button to start generating the report. The report will be shown in the main window.

Anti Spam rules report

Anti-Spam Rules Report	
Blacklist	108
Recipient blacklisted	94
Sender blacklisted	14
Header Checking	4062
Character set not allowed	417
Email contains remote images	1640
Email found in subject	395
Email has different SMTP TO: and MIME TO: fields in the email addresses	565
Email header contains a malformed MIME From: field	277
From field empty	13
Number of numbers in MIME From exceeds maximum threshold	755
Keyword Checking	2935
Found word(s) in the HTML body	1750
Found word(s) in the subject	349
Found word(s) in the Text body	836

Copyright GFI Software Ltd

Ready

Screenshot 94 - Anti Spam rules report

The Anti spam rules report shows you how much spam each anti-spam method caught.

The anti spam rules report can be generated via the Reports > Anti Spam rules menu option. This will bring up the report options dialog. You can specify the following options for the report:

'Specific email' This filter option allows you to limit the report to a specific email address.

'Date range' This filter option allows you to limit the report to a specific date range.

When you have specified the report options, click on the 'Report' button to start generating the report. The report will be shown in the main window.

User usage statistics

User Usage Statistics

Report Type
 Inbound Only Outbound Only Both Directions

Report Options
Sort column: Email Address Email Direction: Inbound
 Highlight user records when the following conditions match
Direction: Received mail Amount more than: 1 MBytes
 Display top records only for current sort column
Top: 1
 Multiple page report
Records per page: 50

Filter Options
Specific Email:
Date Range: No Date Range
From: 04/08/2003 To: 04/08/2003

Report Close

Screenshot 95 - User usage statistics filter dialog

The user usage statistics report gives you an overview of how many emails users send or receive and how large their sent or received emails are.

The user usage statistics report can be generated via the Reports > User usage statistics menu option. This will bring up the User usage statistics report options dialog. You can specify the following options for the report:

Report Type

'Report Type': Allows you to specify whether you wish to report on inbound or outbound emails, or both.

Report Options

'Sort by' allows you to specify whether the report should be sorted by email address, by number of emails, or by the total size of the emails. For example, if you sort on number of emails, the users which send/receive most emails will be listed at the top of the report. If you are reporting on both inbound and outbound emails, you can specify this sort option for inbound or outbound.

'Highlight users' allows you to highlight those users that send or receive more than X number of emails or X number of megabytes of mail.

'List top' allows you to list only the top X number of users in the report. This can be very handy if you have a lot of users on your mail server.

'Multi Page report' allows you to specify the number of users you wish to display on each page.

Filter options

'Specific email' This filter option allows you to limit the report to a specific email address.

'Date range' This filter option allows you to limit the report to a specific date range.

When you have specified the report options, click on the 'Report' button to start generating the report. The report will be shown in the main window.

Domain usage statistics

The screenshot shows a dialog box titled "Domain Usage Statistics". It is divided into three main sections: "Report Type", "Report Options", and "Filter Options".

- Report Type:** Three radio buttons are present: "Inbound Only", "Outbound Only", and "Both Directions". The "Both Directions" option is selected.
- Report Options:**
 - "Sort column": A dropdown menu with "Domain" selected.
 - "Email Direction": A dropdown menu with "Inbound" selected.
 - A checkbox "Highlight domain records when the following conditions match" is unchecked.
 - Below this checkbox are two dropdowns: "Direction" (set to "Mail To Domain (OUT)") and "Amount more than" (set to "1 MBytes").
 - A checkbox "Display top records only for current sort column" is unchecked.
 - Below it is a "Top" input field with the value "1".
 - A checkbox "Multiple page report" is unchecked.
 - Below it is a "Records per page" input field with the value "50".
- Filter Options:**
 - "Specific Domain": An empty text input field.
 - "Date Range": A dropdown menu with "No Date Range" selected.
 - "From": A date dropdown menu with "04/08/2003" selected.
 - "To": A date dropdown menu with "04/08/2003" selected.

At the bottom right of the dialog are two buttons: "Report" and "Close".

Screenshot 96 - Domain usage statistics filter dialog

The domain usage statistics report gives you an overview of how many emails are sent or received for a particular domain. This report is handy if manage multiple domains.

The domain usage statistics report can be generated via the Reports > Domain usage statistics menu option. This will bring up the Domain usage statistics report options dialog. You can specify the following options for the report:

Report Type

'Report Type': Report data for domain usage statistics is always for both inbound and outbound emails.

Report Options

'Sort by' allows you to specify whether the report should be sorted by domain name, by number of emails, or by the total size of the emails.

For example, if you sort on domain name, the report will be sorted in alphabetical order.

'Highlight domains' allows you to highlight those domains that send or receive more than X number of emails or X number of megabytes of mail.

'List top' allows you to list only the top X number of domains in the report. This can be very handy if you have a lot of domains.

'Multi Page report' allows you to specify the number of domains you wish to display on each page.

Filter options

'Specific domain' This filter option allows you to limit the report to a specific domain.

'Date range' This filter option allows you to limit the report to a specific date range.

When you have specified the report options, click on the 'Report' button to start generating the report. The report will be shown in the main window.

Mail server daily usage statistics

The screenshot shows a dialog box titled "Mail Server Daily Usage Statistics". It is divided into three main sections: "Report Type", "Report Options", and "Filter Options".

- Report Type:** Three radio buttons are present: "Inbound Only", "Outbound Only", and "Both Directions". "Both Directions" is selected.
- Report Options:**
 - Sort column:** A dropdown menu set to "Date".
 - Email Direction:** A dropdown menu set to "Inbound".
 - Highlight days when the following conditions match:** A checkbox that is unchecked. Below it, "Direction" is set to "Received mail" and "Amount more than" is set to "1 MBytes".
 - Display top records only for current sort column:** A checkbox that is unchecked. Below it, "Top" is set to "1".
 - Multiple page report:** A checkbox that is unchecked. Below it, "Records per page" is set to "50".
- Filter Options:**
 - Specific Email:** An empty text input field.
 - Date Range:** A dropdown menu set to "No Date Range".
 - From:** A date dropdown menu set to "04/08/2003".
 - To:** A date dropdown menu set to "04/08/2003".

At the bottom right, there are two buttons: "Report" and "Close".

Screenshot 97 - Mail server daily usage statistics filter dialog

The mail server daily usage statistics report gives you an overview of how many emails, per day, are sent or received on the mail server on which GFI MailEssentials is installed.

The mail server daily usage statistics report can be generated via the Reports > Mail server daily usage statistics menu option. This will bring up the Mail server daily usage statistics report options dialog. You can specify the following options for the report:

Report Type

'Report Type': Report data for Mail Server Daily usage statistics is always for both inbound and outbound emails.

Report Options

'Sort by' allows you to specify whether the report should be sorted by date (since the report is per day), by number of emails, or by the total size of the emails.

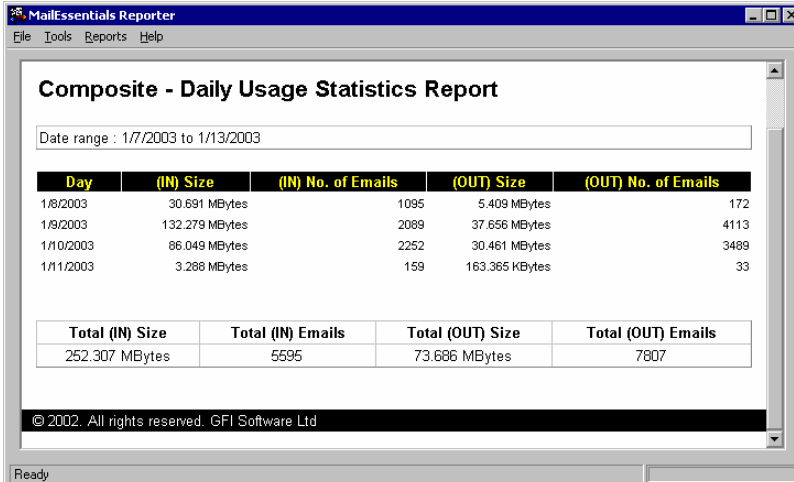
For example, if you sort on number of emails, the days on which you sent or received most e-mail will be listed at the top.

You can specify this sort option for inbound or outbound.

'Highlight days' allows you to highlight those days on which you sent or received more than X number of emails or X number of megabytes of mail.

'List top' allows you to list only the top X number of days in the report.

'Multi Page report' allows you to specify the number of days you wish to display on each page.



MailEssentials Reporter

File Tools Reports Help

Composite - Daily Usage Statistics Report

Date range : 1/7/2003 to 1/13/2003

Day	(IN) Size	(IN) No. of Emails	(OUT) Size	(OUT) No. of Emails
1/8/2003	30.691 MBytes	1095	5.409 MBytes	172
1/9/2003	132.279 MBytes	2089	37.656 MBytes	4113
1/10/2003	86.049 MBytes	2252	30.461 MBytes	3489
1/11/2003	3.288 MBytes	159	163.365 KBytes	33

Total (IN) Size	Total (IN) Emails	Total (OUT) Size	Total (OUT) Emails
252.307 MBytes	5595	73.686 MBytes	7807

© 2002. All rights reserved. GFI Software Ltd

Ready

Screenshot 98 - The daily usage statistics report

Filter options

'Specific email' This filter option allows you to limit the report to a specific domain.

'Date range' This filter option allows you to limit the report to a specific date range.

When you have specified the report options, click on the 'Report' button to start generating the report. The report will be shown in the main window.

User communications

User Communications

Report Type
 Inbound Only Outbound Only Both Directions

Report Options
Sort column: Email Direction:
 Highlight user records when the following conditions match
Direction: Amount more than: MBytes
 Display top records only for current sort column
Top:
 Multiple page report
Records per page:

Filter Options
Specific Email:
Date Range:
From: To:

Screenshot 99 - User communications filter dialog

The User communications report allows you to view what kind of emails each user has sent. Once you generate a user communications report, you can expand the user record to list the subject of sent or received mails. Mail with the same subject is grouped. These mails can be further expanded to reveal when and to whom, mail with that subject was sent.

From	Size	Count
angelica@gfi.com	11.971 MBytes	188
mike & lara's engagement photos	4.447 MBytes	1
mpbal@fastnet.net.nt	4.447 MBytes	1/10/2003 8:47:21 PM
oops - 4got to attach!	1.683 MBytes	1
corp id notes /heed your feedback on stationery!	1.308 MBytes	7
dlipak@mac.com	115.637 KBytes	1/9/2003 2:37:20 PM
dlipak@mac.com	35.949 KBytes	1/9/2003 4:06:23 PM
dlipak@mac.com	43.519 KBytes	1/9/2003 4:25:05 PM
dlipak@mac.com	1.017 MBytes	1/10/2003 12:10:33 AM
dlipak@mac.com	45.808 KBytes	1/10/2003 10:33:35 AM
dlipak@mac.com	2.118 KBytes	1/10/2003 10:42:39 AM
dlipak@mac.com	54.591 KBytes	1/10/2003 11:59:28 AM
new year	739.709 KBytes	1
thought you might like to have a look at these	644.080 KBytes	1

Screenshot 100 - The user communications report shows exact email trail

The User communications report can be generated via the Reports > User communications option. This will bring up the User communications report options dialog. You can specify the following options for the report:

Report Type

'Report Type': Allows you to specify whether you wish to report on inbound or outbound emails, or both.

Report Options

'Sort by' allows you to specify whether the report should be sorted by e-mail address, by number of emails, or by the total size of the emails.

For example, if you sort on number of emails, the days on which you sent or received most e-mail will be listed at the top.

You can specify this sort option for inbound or outbound.

'Highlight users' allows you to highlight those users who sent or received more than X number of emails or X number of megabytes of mail.

'List top' allows you to list only the top X number of users in the report.

'Multi Page report' allows you to specify the number of users you wish to display on each page.

Filter options

'Specific email' This filter option allows you to limit the report to a specific email address.

'Date range' This filter option allows you to limit the report to a specific date range.

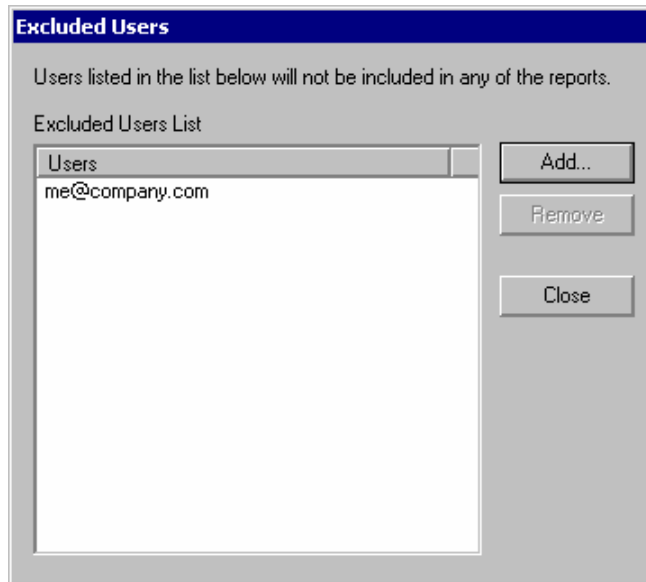
When you have specified the report options, click on the 'Report' button to start generating the report. The report will be shown in the main window.

Note: The user communications report is a complex report that takes time to generate. Therefore, if you have large logs, we recommend that limit the user communications report to specific users or to a particular date range.

Miscellaneous options

The following additional options are available from the tools menu of the GFI MailEssentials reporter.

Excluded users

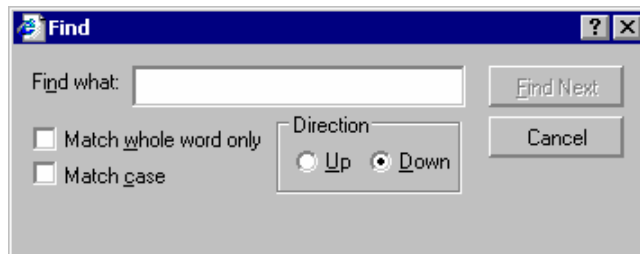


Screenshot 101 - Excluded users dialog

The exclude users tool allows you to specify email addresses that should be excluded from the reports. The excluded users dialog can be accessed from the Tools > Excluded users menu option.

To exclude a user, simply click on the add button and specify the SMTP email address of the user to be excluded from the reports.

Find



Screenshot 102 - Find dialog

The find tool allows you to find a string in a report. The find dialog can be accessed from the Tools > Find menu option.

Printing reports

After you have generated a report, you can choose to print it. You can print a report from the File > Print menu option. You can preview the report using the print preview option.

Configuring POP3 downloading

Should you use POP3 or SMTP to receive mail?

We recommend using SMTP. This is the proper protocol for receiving mail. If you have a continuous line or dial on demand router, use SMTP. POP3 was meant only for e-mail clients, not for mail servers to retrieve mail.

However, in some cases you might not have a choice and you have to use POP3 to download your mail.

Using POP3 to receive mail

Post office protocol (POP3 (RFC 1225)) is a client/server protocol for storing email so that the client can connect to the POP3 server at any time and read the email. A mail client will make a TCP/IP connection with the server and by exchanging a series of commands, read the email. All ISP's support POP3.

Advantages of using POP3 to retrieve mail

- Simple
- Any ISP can support it
- No need for fixed IP address.

Disadvantages

- BCC messages are not routed within your organization.
- If you use a POP3 mailbox for each user, you have to create mailboxes twice – once at the ISP and once on Exchange server.
- If you use one POP3 mailbox for multiple users, messages sent by list servers are not always routed correctly. If your ISP mail server does not support the 'for' clause, messages from some mailing lists will not be routed. This is because when mail is sent via SMTP, the actual recipient is provided by the sender on the "RCPT" command. This information is called part of the "envelope" (since it is outside of the message), and is sometimes not included in the actual mail message's header. For a single recipient, this is not a problem. If the mail is in your mailbox, you know it is for you. However, if all mail directed at a specific domain goes into the same mailbox, there may be no way of determining who the mail should be delivered to. This is most often the case for messages from mailing lists or if the BCC: field was used. There is however a solution for this problem. The most common is in the Received: line. According to page 32 of RFC 821, the Received: line should look something like this:
 - Received: from sender.com by yourisp.com for you@yourdomain.com

- The "for" clause is derived directly from the envelope information, so even if the To: and Cc: lines make no mention of "you@yourdomain.com", the true recipient can be found here. Thus, any POP to Exchange solution must (at least) be able to parse the Received: lines in the header in order to forward the mail to the correct local recipient.

Note: An easy way around the above problem is to create dedicated POP3 mailboxes for lists. Then route the lists to a public mailbox, so that other users can also benefit from the lists.

Using SMTP to receive mail

Simple Mail Transport Protocol (SMTP(RFC821)) is a server-to-server protocol for sending e-mail across the Internet. Briefly, a mail client will make a TCP connection to an ISP's SMTP server and upload a mail message (complete with headers) and instructions to whom the message should be delivered. The SMTP server will then either deliver the message (if it knows the final recipient) or pass it along to another SMTP server. SMTP works best when all servers are connected all the time. If the receiving server is not available, then the sender will have to queue the message and try later. Eventually, the sender will either make it through or give up and return the message to its originator. In the case of dial-up connections, the receiver may be unavailable more often than not.

Advantages of using SMTP

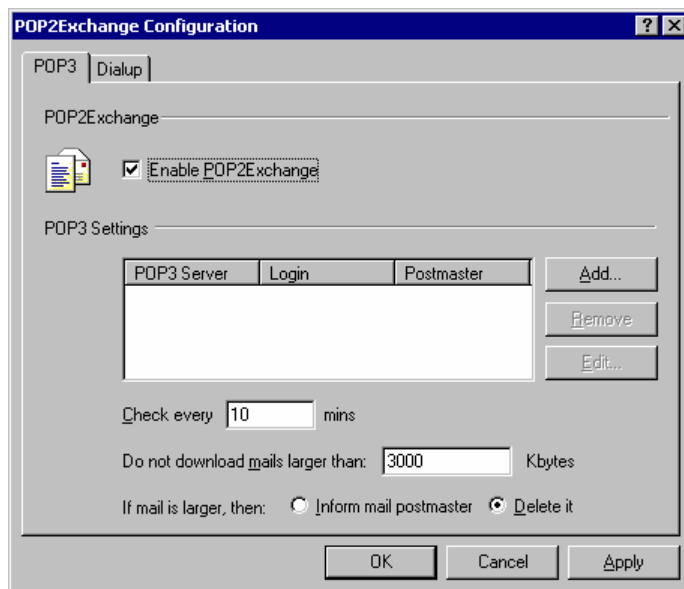
- Server protocol, not client protocol
- Allows you to create an unlimited amount of email addresses on your mail server, without having to worry about aliases etc.

Disadvantages using of SMTP

- You need a public IP

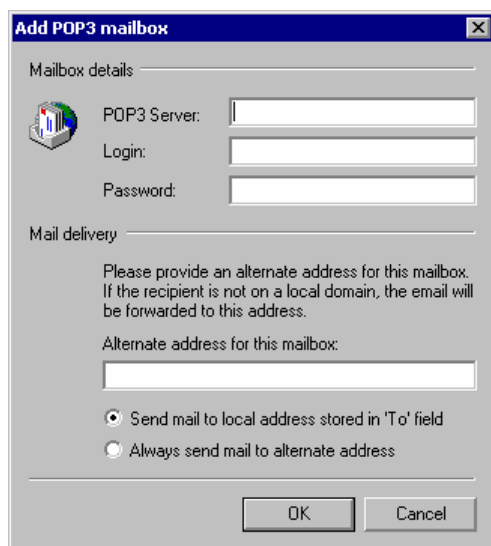
Configuring the POP3 downloader

If you wish to receive mail by downloading mail from one or more POP3 mailboxes, you need to set-up the POP3 downloader. To do this:



Screenshot 103 - The GFI MailEssentials pop3 downloader

1. Highlight the 'POP2exchange' node in the GFI MailEssentials configuration. In the right pane, a node 'general' will appear. Double-click on general. This will bring up the POP2Exchange configuration dialog.
2. Enable the POP3 downloader by ticking the 'Enable POP2Exchange'.
3. To add a POP3 mailbox from which you wish to download mail, click Add.



Screenshot 104 - Adding a POP3 mailbox

Enter the POP3 server name, for example mail.myisp.com, the POP3 mailbox/login name and the password of the mailbox. Then choose between two options:

- **Send mail to address stored in To field:** Activate this option if you wish GFI MailEssentials to analyze the header and route the mail accordingly. If the mail analyzing fails the mail will be sent to the mail address specified in the alternate address.

- **Send mail to alternate address:** Activate this option if you wish all mail from this mailbox to be forwarded to one email address. Enter the full SMTP address in the 'Email address' box, for example john@company.com

Now specify the alternate address. Mail will be sent to this email address if it can not be 'resolved' from the to: header of the mail, or if you specified to forward all mail to address.

4. When you are ready, click **OK**. You can add as many POP3 mailboxes as you wish.

Note: When specifying the destination email address (the address where GFI MailEssentials will forward the email to), be sure that you have set up a corresponding SMTP address on your mail server.

Other POP3 downloading options

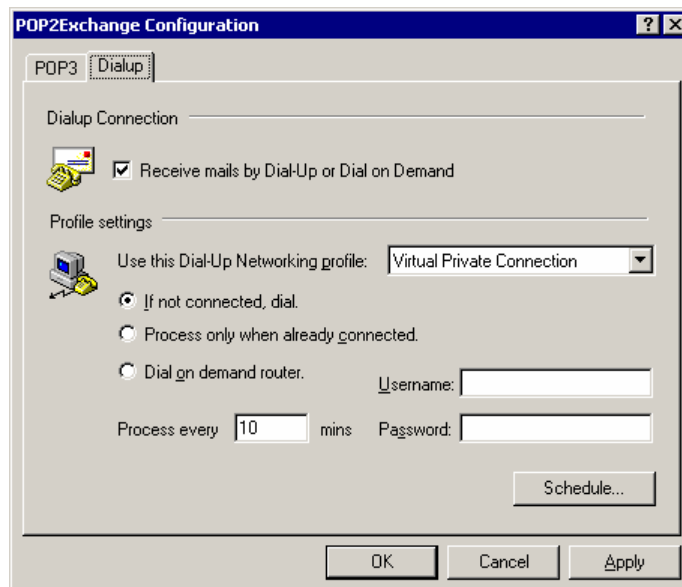
Check every .. minutes: Specify the download interval.

Do not download mail larger than: Here you can specify a maximum download size. If mail exceeds this size, it will not be downloaded.

If mail is larger, then: You can either choose to delete mail larger than the maximum allowed size, or send a message to the postmaster.

Dial up Connection options

To receive mails by dial-up, go to dialup tab in the POP2Exchange dialog. Tick the option 'Receive mails by dial-up'.



Screenshot 105 - Dial-up options

In this dialog, you can specify where and when GFI MailEssentials should dial up to pick up email. You must specify a dial up networking profile and specify a login name and password, as well as a schedule when the mail should be sent/ picked up. The dial up networking profiles are set up from RAS. The following options are available:

Use this Dial-Up Networking profile: Choose the Dial up Networking profile you wish to use from the drop down list.

If not connected dial: If you tick this option GFI MailEssentials will only dial up if there is no connection.

User name: Enter the user name used to logon to your ISP.

Password: Enter the password used to logon to your ISP.

Process only when already connected: If you tick this option, GFI MailEssentials will only process mail if a connection already exists.

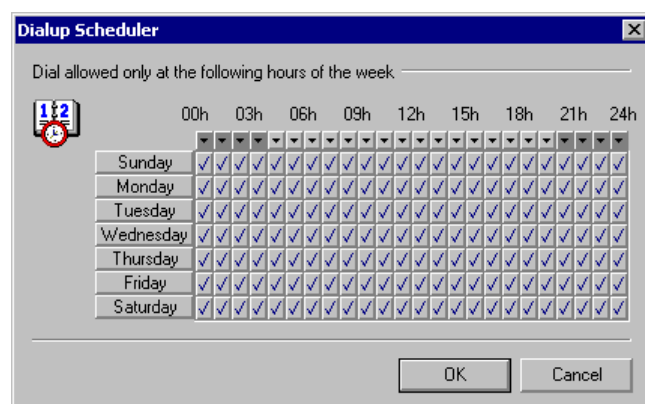
Dial on demand router: If you have an internet connection that gets automatically established, such as a dial on demand router, select this option. This will cause GFI MailEssentials to pick up mail at the specified interval, but without triggering a dial up connection.

Process every .. minutes: Enter the interval at which GFI MailEssentials must either dial up or check if a connection already exists (depends on whether you set GFI MailEssentials to dial up or to only process mail when already connected).

Scheduler

Use the scheduler to specify when GFI MailEssentials should dial up to pick up mail:

1. Click on schedule
2. Specify the hours when GFI MailEssentials should dial up. A 'V' indicates that GFI MailEssentials will dial out. An 'X' indicates that GFI MailEssentials will not dial out at this hour.



Screenshot 106 - You can configure the act schedule when GFI MailEssentials should pick up mail

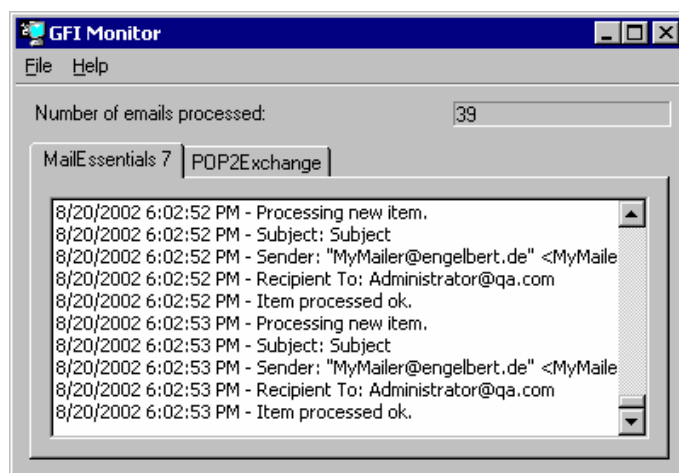
Miscellaneous options

General node

Under the general node in the MailEssentials configuration you will find general information regarding GFI MailEssentials.

1. Version Information – allows you to check what version you have installed and whether it's the latest.
2. Licensing – use this node to enter your License key.
3. Product patches – shows you patches available
4. GFI MailSecurity – link to the product information page of GFI MailSecurity, GFI MailEssentials companion product.
5. GFI FAXmaker – link to the product information page of GFI FAXmaker, GFI MailEssentials companion product.
6. Support – takes you directly to the GFI MailEssentials support page, which lists the most frequently asked questions. Also allows you to search the GFI knowledge base

The GFI MailEssentials monitor



Screenshot 107 - The MailEssentials monitor

The monitor shows you the current activity of GFI MailEssentials. You can use it to check how MailEssentials is processing mails. The POP collector service can be monitored from the POP2Exchange tab.

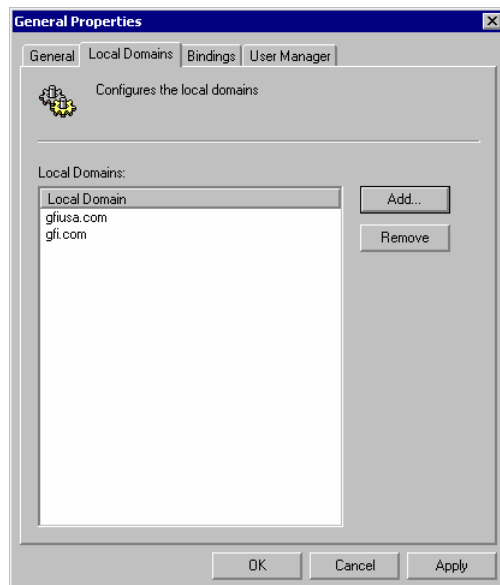
Configuring a fake Non Delivery Report (NDR)

In anti spam actions, you can enable a fake NDR to be sent once a spam mail is detected. If you wish to customize this NDR, you can do so by editing the file ndr.xml, located in MailEssentials\templates

directory. You can edit the file with notepad as well as with an XML editor.

Adding additional local domains

GFI MailEssentials needs to know what your local domains are to distinguish between inbound or outbound email. During installation, GFI MailEssentials will import local domains from the IIS SMTP service. If however you wish to add or remove local domains afterwards, you can do so from the local domains tab in the general node properties:



Screenshot 108 - Adding a local domain

1. Right-click on the general node and select properties to access this dialog.
2. Now enter the local domain

This feature is handy because in some cases you might want to configure local mail routing in IIS differently, as in add domains which are local for mail routing purposes but are not local for your mail server.

Remote commands

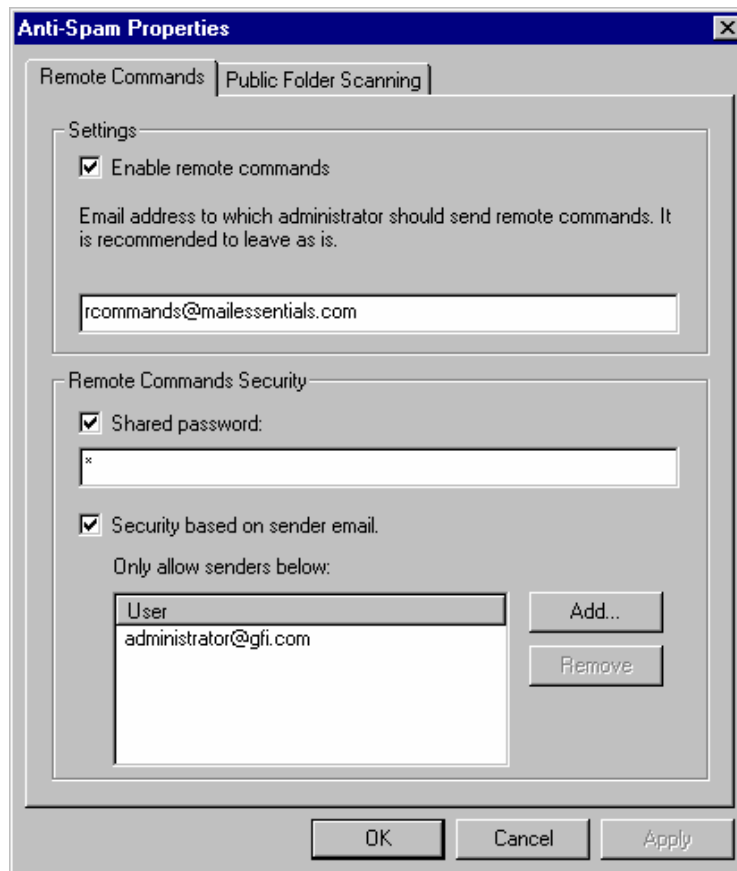
Remote commands make it easy to add domains or email addresses to the spam blacklist, as well as update the Bayesian filter with spam or ham (valid mails).

Remote commands function by sending a mail to GFI MailEssentials: Simply address a mail to rcommands@mailessentials.com (configurable) and GFI MailEssentials will recognize the mail as containing remote commands and process the remote commands.

With remote commands, you can do the following:

1. Add Spam or ham to the Bayesian module
2. Add keywords either to the subject keyword checking feature or to the body keyword checking feature.
3. Add email addresses to the blacklist feature.

Configuring remote commands



Screenshot 109 - Remote commands configuration

To configure remote commands:

1. Go to the Anti Spam node, right click and select properties. This brings up the anti spam properties dialog.
2. Now enable remote commands
3. You can edit the email address to which the remote commands should be sent. However it should not be a local domain. We suggest using rcommands@mailessentials.com. A mailbox for the configured address does not need to exist, but the domain-part of the address must consist of a real email address domain which returns a positive result to an MX-record lookup via DNS.
4. Optionally you can configure some basic security for the remote commands: You can do any of the following:
 - Specify a shared password which should be included in the mail as follows (see next section for information how to create a mail with remote commands)
 - In addition, you can specify which users are able to send mails with remote commands. Note that a user could fake this by faking the from address.

The password is specified as a separate command with the following syntax:

PASSWORD: <shared password>;

Using remote commands

Once you have configured remote commands, you can send mails with remote commands. The remote commands must follow the following syntax:

<command> : <param1>, [<param2>, <param3>, ...];

There can be more than one command in the body of an email, each of them must be separated by a semi-colon (;). Each command name is case-sensitive and should be written in capital letters. The following commands are available:

Keyword checking commands

NOTE: The robot can only add keywords, but not delete or modify them. Conditions are not supported.

ADDSUBJECT – this command adds keywords specified to the subject keyword checking database.

Example: ADDSUBJECT: sex, porn, spam;

ADDBODY – this command adds keywords specified to the body keyword checking database.

Example: ADDBODY: free, “100% free”, “absolutely free”;

NOTE: when you need to specify a phrase rather than a single word, enclose the phrase into double quotes.

Blacklist commands

With blacklist commands you can add a single email address or an entire domain to the custom black list. To add an entire domain to the blacklist, one must specify a wildcard before the domain, e.g. *@domain.com.

ADDBLIST: <email>;

Example: ADDBLIST: user@somewhere.com;

ADDBLIST: *@domain.com;

NOTE: For security reasons, there can be only one ADDBLIST command in an email, and only one address can be specified as the command parameter. The parameter is either a user email, e.g. spammer@spam.com, or a domain, e.g. *@spammers.org. Please note that you cannot use wildcards in domain name, that is, an email like *@*.domain.com will be rejected as invalid.

Bayesian filter commands


With these commands you can add spam mail or good mail (ham) to the Bayesian filter database. Simply forward the mail with one of the following remote commands in them.

ADDASSPAM – instructs the Bayesian module to classify given email as spam.

ADDASGOODMAIL – instructs the Bayesian module to classify given email as good email.

These commands do not have parameters – rather the rest of the mail is the parameter.

Examples



From: max@max.com (192.168.206.1)

To: rcommands@mailessentials.local

Cc:

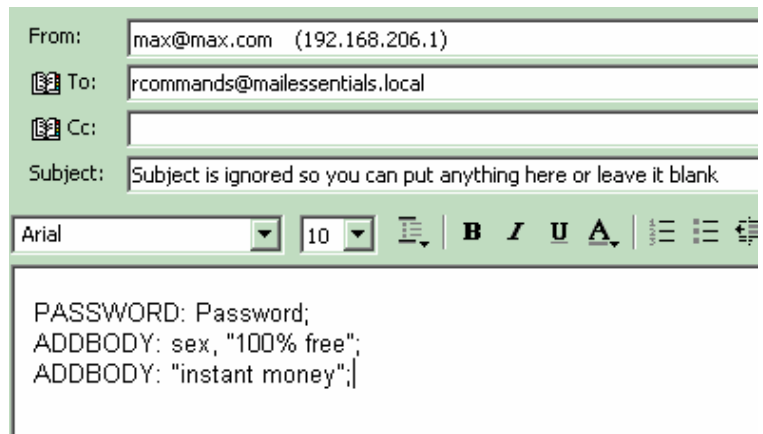
Subject: Subject is ignored so you can put anything here or leave it blank

Arial 10

PASSWORD: Password;
ADDBLIST: spammer@spamhouse.com;
ADDSUBJECT: sex, "100% free";

Screenshot 110 - Adding an email address to the blacklist & keywords

Example 1 - By sending this email, the user adds spammer@spamhouse.com to blacklist and also adds a few keywords to subject keyword checking database.



From: max@max.com (192.168.206.1)

To: rcommands@mailessentials.local

Cc:

Subject: Subject is ignored so you can put anything here or leave it blank

Arial 10

PASSWORD: Password;
ADDBODY: sex, "100% free";
ADDBODY: "instant money";

Screenshot 111 - Specifying the same commands more than once

Example 2: You can specify the same command more than once. (in this case ADDBODY). The result is cumulative, that is, in this case the keywords added to body checking database are: sex, 100% free and instant money.

To...	rcommands@maillessentials.local
Cc...	
Bcc...	
Subject:	FW: Depressed? ap

PASSWORD: Password;
ADDASSPAM

-----Original Message-----

From: Ty Westbrook [mailto:266e5ohfrhww@excite.com]
Sent: Thursday, June 12, 2003 9:38 PM
To: 20orders@gfi.com
Cc: Alexander Zammit; bcdefbk@gfi.com; Brian Azzopardi; David Farinic; David Vella; Downloads
Subject: Depressed? ap

Human Growth Hormone

As seen on NBC, CBS, and CNN, and even Oprah! The health discovery that actually reverses aging while burning fat, without dieting or exercise! And it's Guaranteed!

Doctor Formulated HGH

- * Enhance sexual performance
- * Remove wrinkles and cellulite
- * Restore hair color and growth
- * Strengthen the immune system
- * Increase energy and cardiac output

Screenshot 112 - Adding a spam to the Bayesian filter database

Example 3: A spam email is added using the ADDASSPAM command. Note that a colon is not required for this type of command – everything immediately after this command is treated as data for the Bayesian filter.

To...	rcommands@maillessentials.local
Cc...	
Bcc...	
Subject:	

ADDBLIST: spamsender@spam.com;

Screenshot 113 - Sending remote commands without security

Example 4: When “Disable Password” checkbox is checked, you can send remote commands without specifying a password.

Remote command logging

In order to keep track of changes made to configuration database via remote commands, each email with remote commands (even if email with remote commands was invalid) is saved under ADBRProcessed subfolder which is located under product's main folder. The file name of each email is formatted according to the following format:

<sender_email_address>_SUCCESS_<timestamp>.eml – in case of successful processing.

<sender_email_address>_FAILED_<timestamp>.eml – in case of failure.

Timestamp is formatted as yyyyddmmhhmmss.

Troubleshooting

Introduction

The troubleshooting chapter explains how you should go about resolving issues you have. The main sources of information available to users are:

1. The manual – most issues can be solved by reading the manual.
2. The GFI knowledgebase – accessible from the GFI website.
3. The GFI support site.
4. Contacting the GFI support department by email at support@gfi.com
5. Contacting the GFI support department using our live support service at <http://support.gfi.com/livesupport.asp>
6. Contacting our support department by telephone.

Knowledgebase

GFI maintains a knowledgebase, which includes answers to most common problems. If you have a problem, please consult the knowledgebase first. The knowledgebase always has the most up-to-date listing of support questions and patches.

The knowledgebase can be found on <http://kbase.gfi.com>

Request support via e-mail

If, after using the knowledgebase and this manual, you have any problems that you cannot solve, you can contact the GFI support department. The best way to do this is via e-mail, since you can include vital information as an attachment that will enable us to solve the issues you have more quickly.

The **Troubleshooter**, included in the program group, generates automatically a series of files needed for GFI to give you technical support. The files would include the configuration settings etc. To generate these files, start the troubleshooter and follow the instructions in the application.

In addition to collecting all the information, it also asks you a number of questions. Please take your time to answer these questions accurately. Without the proper information it will not be possible to diagnose your problem.

Then go to the support directory, located under the main program directory, **ZIP the files**, and send the generated files to support@gfi.com.

Ensure that you have registered your product on our website first, at <http://www.gfi.com/pages/regfrm.htm>!

We will answer your query within 24 hours or less, depending on your time zone.

Request support via web chat

You may also request support via Live support (web chat). You can contact the GFI support department using our live support service at <http://support.gfi.com/livesupport.asp>

Ensure that you have registered your product on our website first, at <http://www.gfi.com/pages/regfrm.htm>!

Request support via phone

You can also contact GFI by phone for technical support. Please check our support website for the correct numbers to call, depending on where you are located, and for our opening times.

Support website:

<http://support.gfi.com>

Ensure that you have registered your product on our website first, at <http://www.gfi.com/pages/regfrm.htm>!

Web Forum

User to user support is available via the web forum. The forum can be found at:

<http://forums.gfi.com/>

Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, go to:

<http://support.gfi.com>

Index

A

Anti-Spam 1, 33–47
Archiving 87
Attachments 88
Auto replies 2, 65

B

blacklist 34–39

D

Dial on demand 107, 111
dial up 110–11
disclaimers 61, 63
DNS lookup 13
DNSbl 39

E

Exchange Server 2000 5–10,
14

G

gateway 9

H

header 33, 43–47, 107, 109
header checking 43–44, 47

I

IIS5 SMTP 10

L

Lotus Notes 2, 10, 16

M

mail monitoring 2, 69, 71
mail relay server 5, 9–11,
13–17
mail reports 3
mail sink 2
MailEssentials reporter 3, 6,
104
MX record 10, 16

N

newsletter 56

non delivery report 43, 113

O

ORDB 39

P

POP2exchange' 109
POP3 2, 10, 16, 107–9
POP3 downloading 107, 110

S

Scheduler 111
sink 2
SMTP 2, 10–18, 107–10
System requirements 6

W

whitelist 34–35

X

XML 6–9, 20, 113