GFI MailEssentials 14

Manual

By GFI Software

http://www.gfi.com
Email: info@gfi.com

Version 14 - Last updated: September 2, 2008

Contents

About GFI MailEssentials

Introduction to GFI MailEssentials

GFI MailEssentials offers server-based anti-spam and other key corporate email 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/whitelists, 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 an email. 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.

Email archiving to a database

With GFI MailEssentials, you can archive all inbound and outbound email. 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 email use, including, daily statistics report, detailed log of emails sent, reports per user or by date range. You can use these reports 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 Microsoft Exchange Server and Lotus Notes are unable to download email from POP3 mailboxes. GFI MailEssentials includes a utility that can forward and distribute email from POP3 mailboxes to mailboxes on your mail server.

Email monitoring

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

GFI MailEssentials components

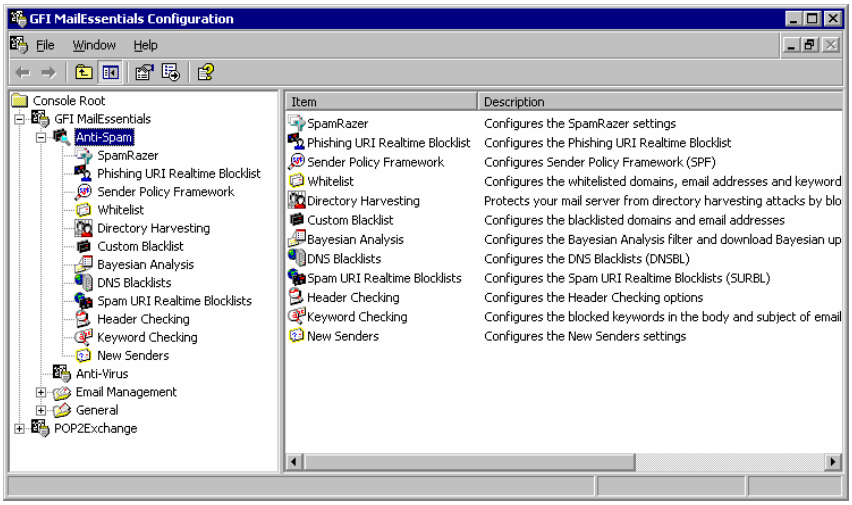
GFI MailEssentials consists of the following parts:

GFI MailEssentials services

The GFI MailEssentials services take care of analyzing and processing all the emails, handle any newsletters and discussion lists you have configured, and perform maintenance tasks that are required by GFI MailEssentials at regular intervals.

GFI MailEssentials configuration

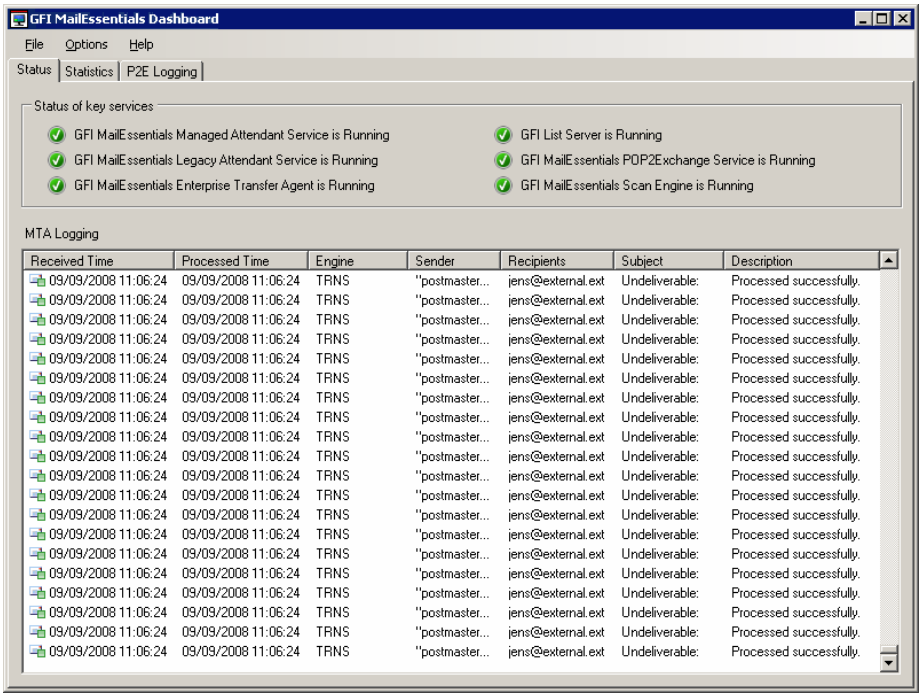
The GFI MailEssentials configuration is hosted in a Microsoft Management Console (MMC) from which you can set up and configure GFI MailEssentials.



Screenshot 1 - GFI MailEssentials configuration

GFI MailEssentials Dashboard

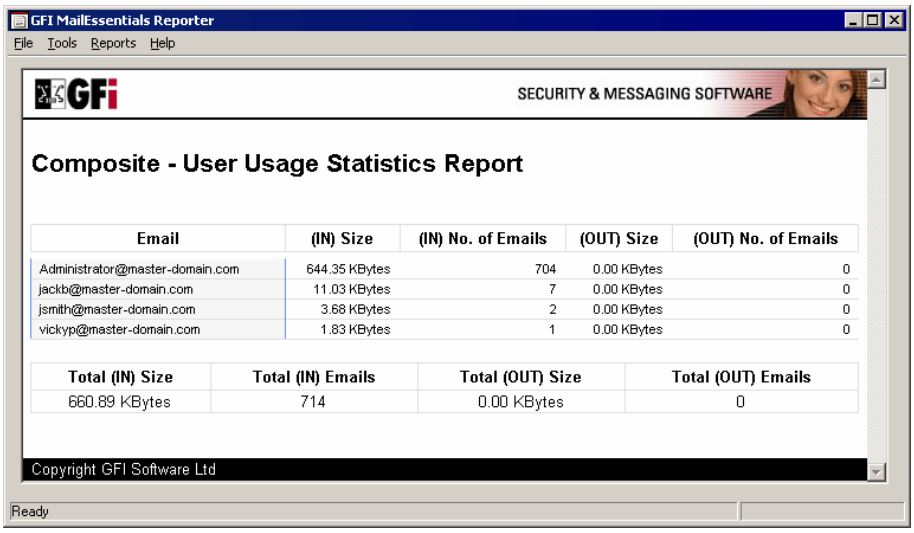
Through the GFI MailEssentials Dashboard, you can view the activity of GFI MailEssentials as well as statistics. The POP collector service can be monitored from the **P2E Logging** tab.



Screenshot 2 - GFI MailEssentials Dashboard

GFI MailEssentials Reporter

The reporting application provides useful reports that give a clear picture of the amount of emails being processed and the effectiveness of GFI MailEssentials in blocking spam email.



Screenshot 3 – GFI MailEssentials Reporter

Installing GFI MailEssentials

Introduction to installing GFI MailEssentials

This chapter shows you how to install and configure GFI MailEssentials. GFI MailEssentials can be installed in two ways:

Installation option 1: Installing GFI MailEssentials on the Microsoft Exchange Server 2000/2003/2007 machine

Simply install GFI MailEssentials on the Microsoft Exchange Server 2000/2003/2007 machine. If you are installing on Microsoft Exchange Server 2007, you either need to have Mailbox Server Role and Hub Transport Server Role installed or Hub Transport Server Role installed. GFI MailEssentials cannot be installed on a Microsoft Exchange Server 2007 machine with only Mailbox Server Role installed. See 'Installing GFI MailEssentials on the Microsoft Exchange Server 2000/2003/2007 machine' for instructions on how to install this deployment option.

NOTE: If you are installing GFI MailEssentials on Microsoft Exchange Server 2000/2003 or Microsoft Exchange Server 2007 with both Mailbox Server Role and Hub Transport Role installed, you can configure GFI MailEssentials to direct email marked as spam directly to the user's junk email folder. This makes it easy for users to periodically review spam email for false positives. If you install GFI MailEssentials in the DMZ, or in front of Microsoft Exchange Server 2000/2003, or on a Microsoft Exchange Server 2007 machine that does not have the Mailbox Server Role installed, this feature will not be available.

Installation option 2: Installing GFI MailEssentials on a separate machine

If you are not running Microsoft Exchange Server 2000/2003/2007 or wish to separate the GFI MailEssentials installation from the Microsoft Exchange Server 2000/2003/2007 machine, you can install GFI MailEssentials on a separate machine.

NOTE: In a Microsoft Exchange Server 2007 environment, the mail relay server in the DMZ can be a machine running Microsoft Exchange Server 2007 with the Edge Transport Server Role installed.

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 specification then the mail server machine and can process email faster
- Additional fault tolerance – if anything happens with your mail server you can still receive email, which is queued on the GFI MailEssentials machine.

NOTE 1: This separate machine does not need to be dedicated to GFI MailEssentials; it can run other applications, such as GFI MailSecurity. If you choose this option, you have to configure IIS before installing GFI MailEssentials.

NOTE 2: If installing on a Microsoft Exchange Server 2007 machine with the Edge Transport Server Role, you do not need to install or configure the IIS SMTP service, since Microsoft Exchange Server 2007 has its own built in SMTP server.

Go to the paragraph 'Installing GFI MailEssentials on a separate machine' for instructions on how to do this.

IMPORTANT: Do not judge the spam detection rate of GFI MailEssentials until you have allowed the Bayesian filter to run for at least one week. GFI MailEssentials can achieve the highest detection rate compared to other anti-spam solutions because it adapts specifically to your emails. Be patient and wait at least a week before you evaluate it.

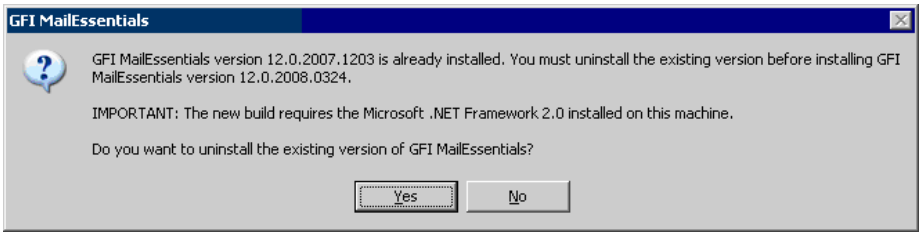
Upgrading from previous versions

If you are currently using a previous version of GFI MailEssentials, you can upgrade your current installation whilst retaining all your existing configuration settings. You will need to enter the fully purchased license key within 10 days of installing the upgrade. For information on how to obtain the new license key, visit http://customers.gfi.com.

NOTE: Only GFI MailEssentials version 9, 10, 11 and 12 can be upgraded to GFI MailEssentials 14. Upgrades cannot be undone i.e. you cannot revert to older versions once you have installed the latest version.

To upgrade:

1. Launch the GFI MailEssentials 14 setup file on the machine on which you have installed GFI MailEssentials. Setup will prompt you whether you wish to remove the current version of GFI MailEssentials and install GFI MailEssentials 14. Click **Yes** to proceed.



Screenshot 4 - Confirm the upgrade

2. Setup will now proceed to install GFI MailEssentials 14 in exactly the same manner as a new installation (for a detailed description, see this chapter), however it will not let you change the destination folder.

This section applies to GFI MailEssentials 9 users only

When the GFI MailEssentials 14 setup has copied all the installation files, it will notify you that it needs to convert the Bayesian weights file to the new format used in GFI MailEssentials 10 onwards. The new format is more compact and uses less memory. During this conversion process, a progress dialog box is displayed on screen. Once the conversion is ready, click **Finish** to complete the upgrade.

Installing GFI MailEssentials on the Microsoft Exchange Server 2000/2003/2007 machine

System requirements

- Windows Server 2008 (x64) or Windows Server 2003 Standard/Enterprise (x86 or x64) or Windows 2000 Professional/Server/Advanced Server (SP1 or higher)
- Microsoft Exchange Server 2007, 2003, 2000 (SP1)

  NOTE 1: GFI MailEssentials also supports Microsoft Exchange Server 2007 (SP1)

  NOTE 2: When using Small Business Server, ensure you have installed Service Pack 2 for Exchange Server 2000 and Service Pack 1 for Exchange Server 2003.

  NOTE 3: To install GFI MailEssentials on Microsoft Exchange Server 2007 you also need to install the Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1.

  NOTE 4: When installing GFI MailEssentials on a Microsoft Exchange Server 2007 machine, only the 64-bit production version of Microsoft Exchange Server 2007 is supported.
- Microsoft .NET Framework 2.0
- If you are going to use 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.
- **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 Microsoft Windows 2000/2003 version, although not always installed by default. For more information on 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.

IMPORTANT: Disable anti-virus software from scanning the GFI MailEssentials, Microsoft IIS, and Microsoft Exchange Server directories. Anti-virus products are known to both interfere with normal operation as well as slow down any software that requires file access. In fact, Microsoft does not recommend running file based anti-virus software on the Microsoft Exchange Server. For more information read the following article: http://kbase.gfi.com/showarticle.asp?id=KBID001824

IMPORTANT: Make sure that backup software is not backing up any of the GFI MailEssentials directories at any point.

NOTE: If you have a cluster please read the following Knowledge Base article prior to installing GFI MailEssentials: http://kbase.gfi.com/showarticle.asp?id=KBID001639

GFI MailEssentials will need to start and stop the Microsoft Exchange Server services during installation.

Running GFI MailEssentials setup

1. On the Microsoft Exchange Server machine, log-on as administrator and run the GFI MailEssentials setup file.

2. Select the language in which you would like to install GFI MailEssentials (English or German).

3. A welcome dialog will appear. Close all the other running Windows programs and click **Next** to continue.

NOTE: At this stage GFI MailEssentials will be performing backend checks such as searching for installed applications and it might take some time for the **Next** button to appear.

4. GFI MailEssentials will prompt you to check for a more recent version or build. Always use the latest version.

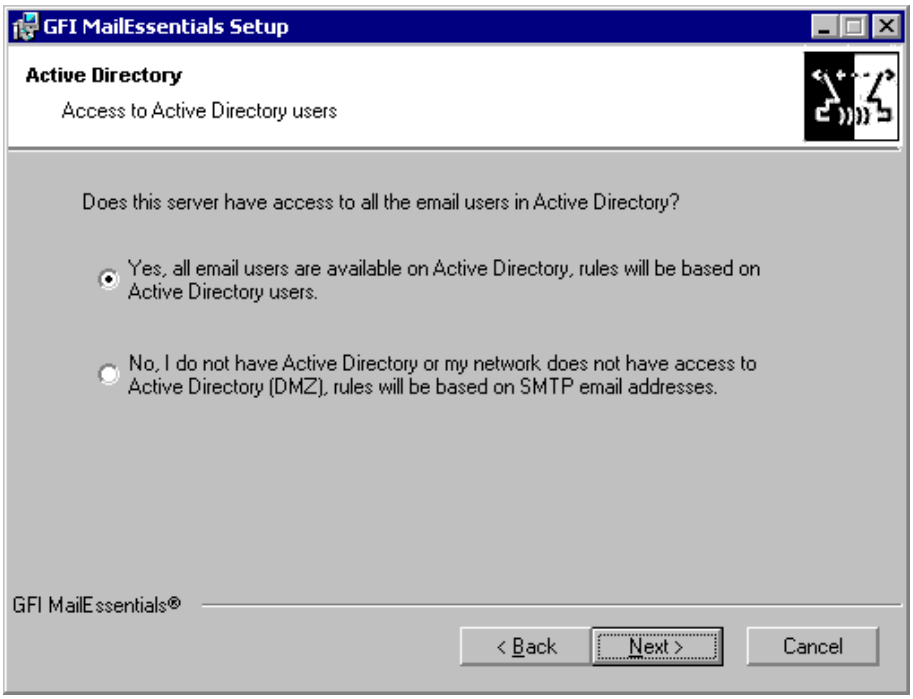
5. Read the licensing agreement carefully. To proceed with the installation, select **I accept the license agreement** and click **Next**.

6. To install GFI MailEssentials to the default location, click **Next** to continue. Alternatively, to specify a custom installation folder click **Browse**, select a new installation path and click **Next** to continue.

7. Enter your name, company name, and license key. If you are evaluating the product, leave the default `'Evaluation'`. Click **Next**.

8. Setup will ask you for the administrator email. GFI MailEssentials will use the administrator email to send critical notifications.

9. If you are installing GFI MailEssentials on a Microsoft Exchange Server 2000/2003 configured as a front-end server, or on a Microsoft Exchange 2007 Edge Transport Server Role machine (i.e. in a DMZ in front of another Microsoft 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, it is better to select SMTP mode, which allows you to input the SMTP email address for user based configuration/rules.



Screenshot 5 - Selecting SMTP mode or Active Directory mode

10. If you do not have Microsoft Message Queuing Services (MSMQ) installed, setup 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 Microsoft 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 Microsoft Windows CD and setup will launch the MSMQ set-up.

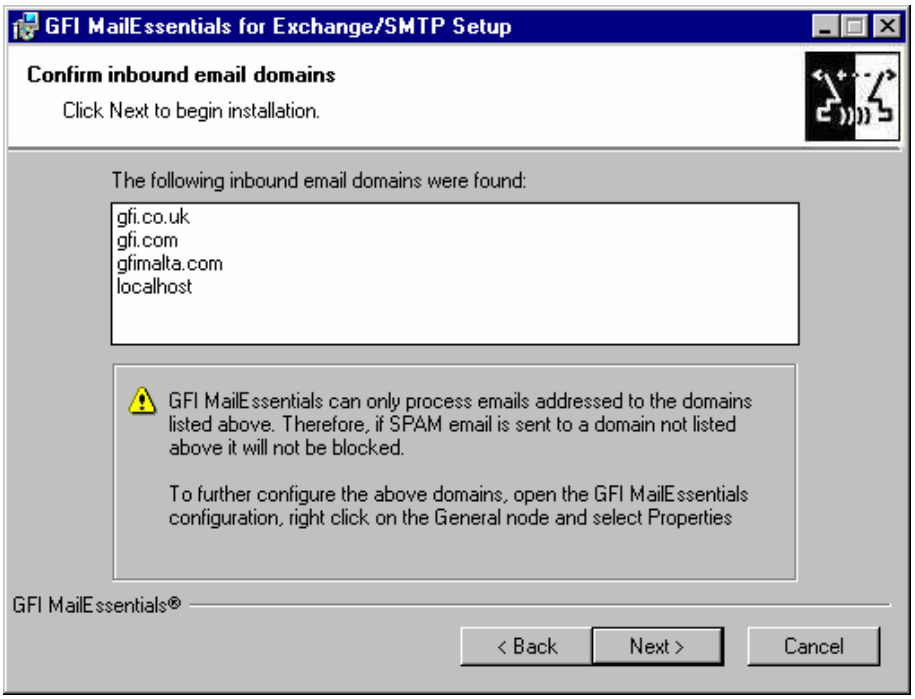
Screenshot 6 - Installing Microsoft Message Queuing Service

11. Setup will now confirm the inbound email domains (e.g. mycompany.com) that you have set up in the IIS/Exchange configuration. It is important to ensure that your inbound email domains are listed correctly.

IMPORTANT: GFI MailEssentials ONLY filters emails destined to your inbound email domain. Therefore, if you do not configure your inbound email domains correctly, no spam will be detected.

NOTE: If you are installing GFI MailEssentials on a Microsoft Exchange Server 2007 machine, the inbound email domains step of the installation wizard is skipped since these are determined from the GFI MailEssentials Post-Installation wizard that is launched when you finish this installation wizard.

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



Screenshot 7 - Configure your inbound email domain

12. Setup will now copy all the 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.

NOTE 1: If you are installing GFI MailEssentials on x64 machine, the files will be installed under the c:\program files (x86)\ folder.

NOTE 2: If you are installing on a Microsoft Exchange Server 2007 machine, you will not be prompted to restart the SMTP service.

13. After the installation, setup will check if you have the Microsoft XML engine installed. If you do not, 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 Microsoft Windows, setup 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 read this Knowledge Base article:

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

NOTE: If you are installing on a Microsoft Exchange Server 2007 machine, the installation will launch the GFI MailEssentials Post-Installation Wizard. Refer to the 'GFI MailEssentials Post-Installation Wizard' section further on in this chapter for information on how to use this wizard.

14. Upon first installation, GFI MailEssentials will display the Quick Start Guide that introduces the GFI MailEssentials Configuration console and explains how to quickly configure/customize the most powerful GFI MailEssentials anti-spam filters.

Installing GFI MailEssentials on a separate machine

If you install GFI MailEssentials on a separate machine that is not your gateway SMTP server, ensure that you configure the **Perimeter SMTP Servers** option in the GFI MailEssentials configuration after you finish the installation. The perimeter SMTP server is the gateway SMTP server which receives your emails directly from the internet and you will have to specify the IP address of your perimeter SMTP server in GFI MailEssentials, especially if you are going to use the SPF filter feature. For more information on how to setup your gateway SMTP server, please refer to the 'Defining your Perimeter (Gateway) SMTP Server' section of the 'Configuring Anti-spam' chapter in this manual. Effectively GFI MailEssentials will act as a mail relay server between the perimeter (gateway) SMTP server and the recipients' inboxes.

System requirements

- Windows Server 2008 (x86 or x64) or Windows Server 2003 Standard/Enterprise (x86 or x64) or Windows 2000 Professional/Server/Advanced Server (Service Pack 1 or higher) or Windows XP

  NOTE: Since the version of Internet Information Services (IIS) included in Windows XP is limited to serving only 10 simultaneous client connections, installing GFI MailEssentials on a machine running Windows XP could affect its performance.

- Microsoft .Net framework 2.0

- Microsoft IIS 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 on how to configure IIS5: http://support.microsoft.com/support/kb/articles/Q293/8/00.ASP.

  NOTE: If you are going to install GFI MailEssentials on the Microsoft Exchange 2007 Edge Transport Server Role, you do not need to install the IIS SMTP service since Microsoft Exchange Server 2007 has its own built in SMTP server.

- If you are going to use 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.

- **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 Microsoft Windows 2000/2003 version, although not always installed by default. For more information on 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.

- Access to a mail server machine such as Microsoft Exchange Server 2007, 2003, 2000 (SP1), 5.5, 5, 4, or Lotus Notes 4.5 and up, or any SMTP/POP3 mail server.

IMPORTANT: Disable anti-virus software from scanning the GFI MailEssentials, Microsoft IIS, and Microsoft Exchange Server directories. Anti-virus products are known to both interfere with normal operation as well as slow down any software that requires file access. In fact, Microsoft does not recommend running file based anti-virus software on the Microsoft Exchange Server. For more information read the following article: http://kbase.gfi.com/showarticle.asp?id=KBID001824

IMPORTANT: Make sure that backup software is not backing up any of the GFI MailEssentials directories at any point.

Installing & configuring IIS SMTP service

GFI MailEssentials uses the Microsoft IIS SMTP service as its SMTP Server and thus the SMTP server must be configured as a mail relay server first.

NOTE: If you have a Microsoft Exchange Server 2007 environment and are going to install GFI MailEssentials on the Microsoft Exchange 2007 Edge Transport Server Role machine, you do not need to install or configure the IIS SMTP service since Microsoft Exchange Server 2007 has its own built in SMTP server.

About the Microsoft IIS SMTP service

The SMTP service is part of Microsoft IIS, which is part of Microsoft Windows 2000/2003. It is used as the message transfer agent of Microsoft Exchange Server, except Microsoft Exchange Server 2007 which has its own built in SMTP server, and has been designed to handle large amounts of email traffic. The Microsoft IIS SMTP service is included in every Microsoft Windows distribution.

NOTE: If you have a cluster please check this Knowledge Base article prior to installing GFI MailEssentials: http://kbase.gfi.com/showarticle.asp?id=KBID001639

To install and configure the Microsoft IIS SMTP service as a mail relay server, follow these steps:

Step 1: Verify the Installation of the SMTP Service

1. From the **Start** menu access the **Control Panel**.

2. Open the **Add or Remove Programs** and click on the **Add or Remove Windows Components**.

3. Click the **Internet Information Services (IIS)** component and click the **Details** button.

4. Verify that the **SMTP Service** checkbox is selected. If it is not selected, click it to select it.

5. Click the **OK** button, and then follow the installation instructions that are displayed.

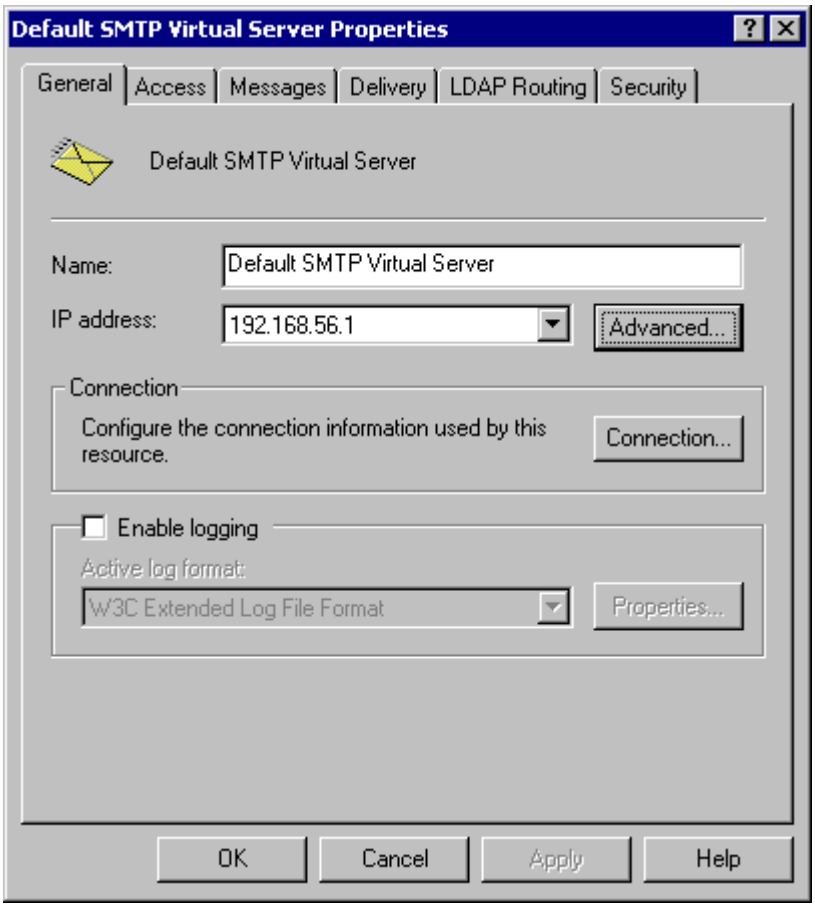
Step 2: Specify mail relay server name and assign an IP

1. From the **Start** menu, access the **Administrative Tools**.

2. Click on the **Internet Information Services (IIS) Manager** icon.

3. Expand the tree under the server name. Right click on the **Default SMTP Virtual Server** and select **Properties**.

4. Assign an IP address to the server and click the **OK** button.



Screenshot 8 - Specify mail relay server name and assign IP

Step 3: Configure the SMTP Service to relay email 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 email

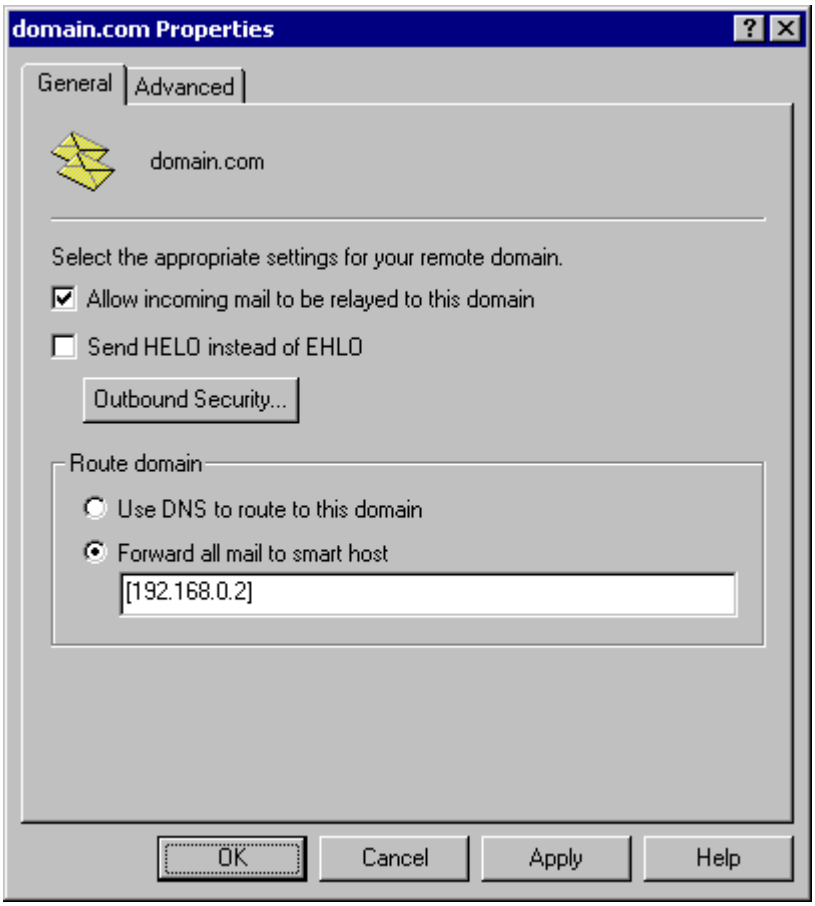
Click the **Start** menu, point to Programs, click **Administrative Tools**, and then click **Internet Services Manager**.

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.

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 9 - Configure the domain

IMPORTANT: Ensure that you add all your inbound email domains, for example 'mycompany.com', otherwise inbound email will not be filtered for spam.

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

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

Configure the domain to relay email to your mail server:

1. Access the **Properties** dialog for the domain that you just created and check the **Allow the Incoming Mail to be Relayed to this Domain** checkbox.

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 mail 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 that this is an IP address, and thus avoids any attempts at performing a DNS lookup.

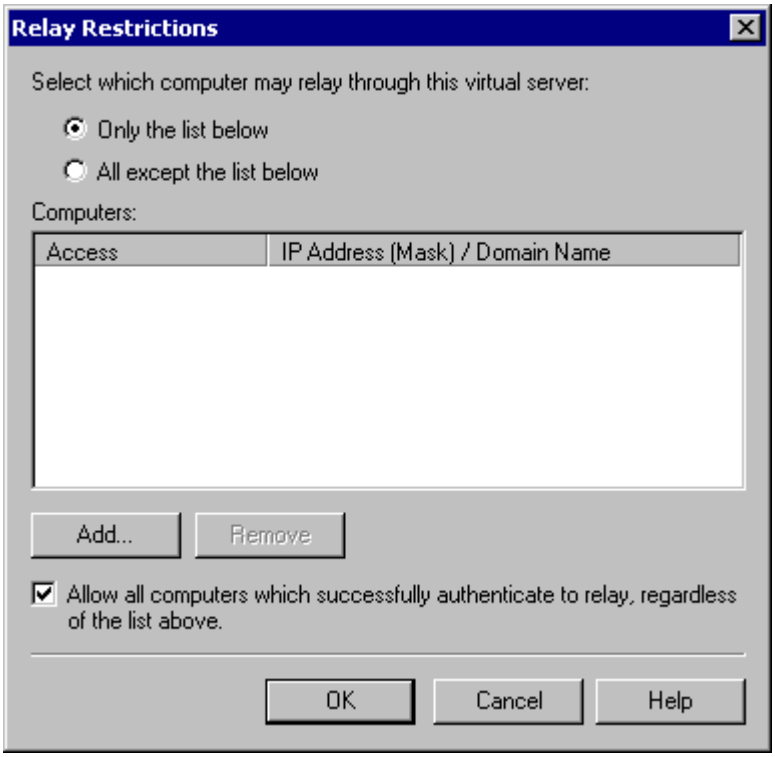
4. Click the **OK** button.

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 email via this mail relay server. Effectively you will limit the servers that can send email to the internet through this server. If you do not create restrictions, anyone can use your mail relay server as an open relay for spamming. To prevent this follow these steps:

1. Open the **Properties** of the **Default SMTP Virtual Server**.

2. On the **Access** tab, click **Relay**.



Screenshot 10 - Relay options

3. Click **Only the list below**.

4. Click the **Add** button, and then add the IP of your mail server that will be forwarding the email to this server. You can specify a single computer, group of computers or a domain:

Single computer - Specify one particular host that you want to relay off from this server. If you click the **DNS Lookup** button, you can lookup an IP address of a specific host.

Group of computers - Specify a base IP address for the computers that you want to relay.

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 email server to relay email via the mail relay server

After you have configured the IIS SMTP service to send and receive email, configure your mail server to relay all email to the mail relay server as follows:

On 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.

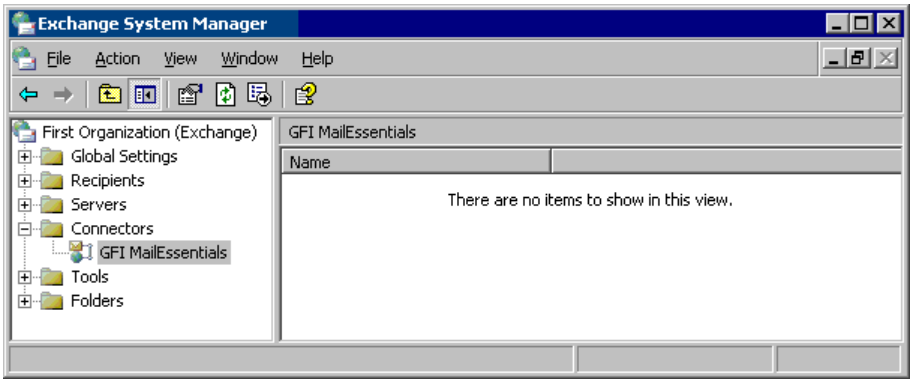
4. In the Message Delivery section, select **Forward all messages to host**. Enter the computer name or IP of the machine running GFI MailEssentials.

5. Click the **OK** button and restart the Microsoft Exchange Server. This can be done from the services applet.

On Microsoft Exchange Server 2000/2003:

You will need to setup an SMTP connector that forwards all email to GFI MailEssentials:

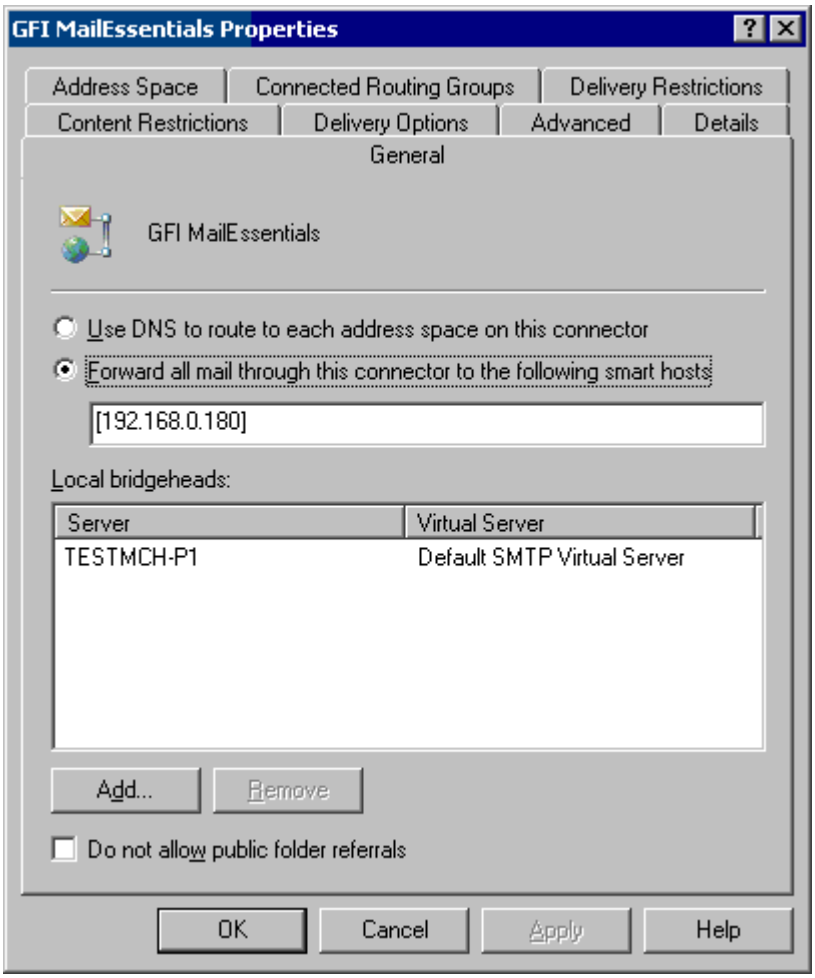
1. Start up Exchange **System Manager**.



Screenshot 11 - Forwarding email to GFI MailEssentials machine

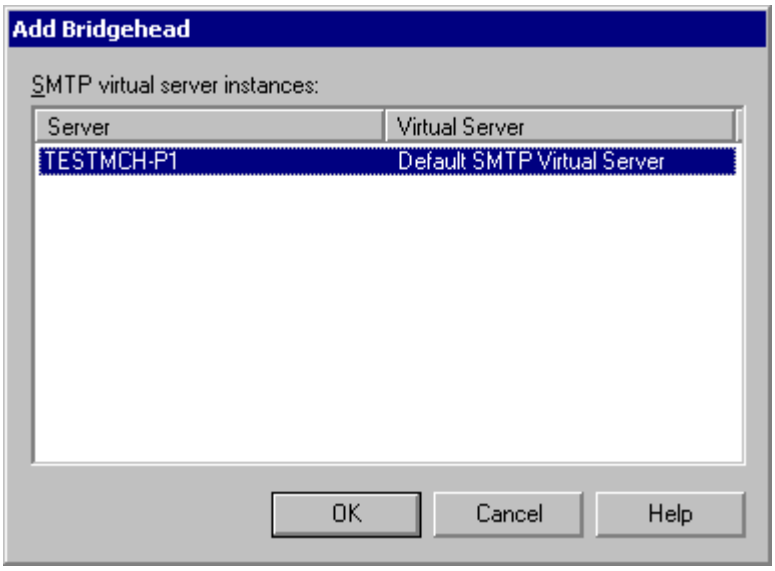
2. Right click on the **Connectors** Node, select **New > SMTP Connector,** and then create a new SMTP connector. You will be prompted for a name.

3. 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, for example: [100.130.130.10].



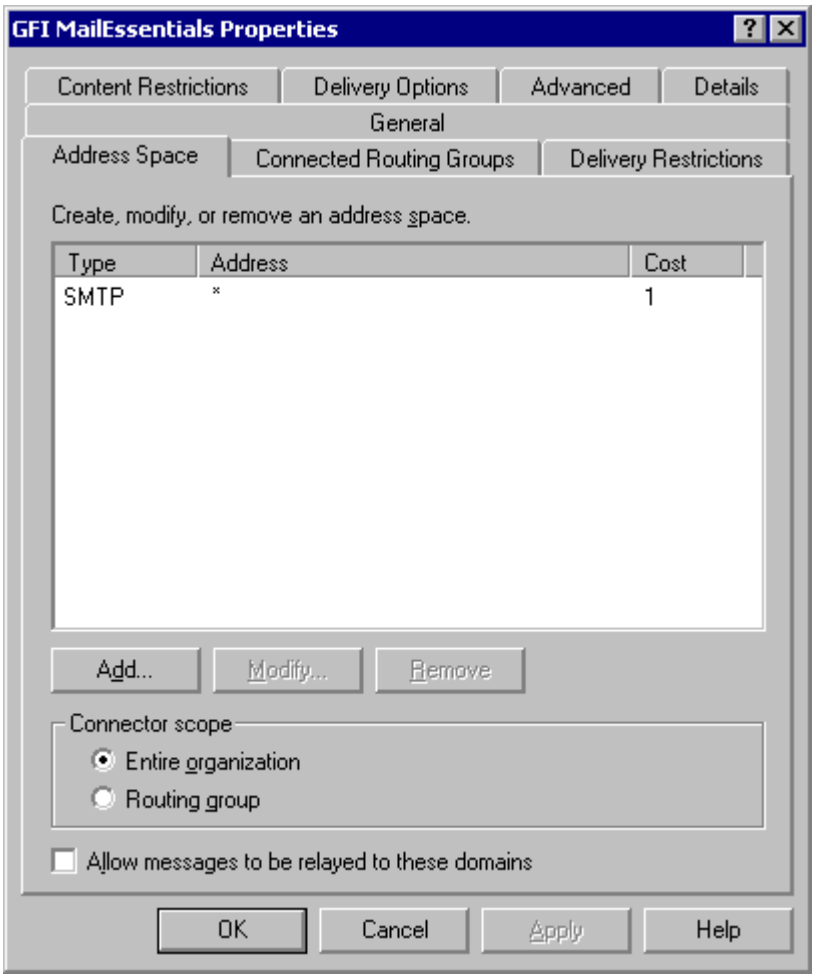
Screenshot 12 - Specifying IP of GFI MailEssentials machine

4. Click **Add** in the **Local bridgeheads** section, and select the appropriate virtual SMTP Server instances that you want to forward email for.



Screenshot 13 - Adding a bridgehead

5. Go to the **Address Space** tab, and click the **Add** button. Select SMTP and click the **OK** button.



Screenshot 14 - Adding SMTP as address space

6. Click the **OK** button to exit. All emails will now be forwarded to the GFI MailEssentials machine.

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

Check the mail server documentation on how to forward email 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 email first, update the MX record of your domain to point to the IP of the new mail relay server. Otherwise, email will continue to go to your mail server and by-pass GFI MailEssentials.

If you run your own DNS server, you need to 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.

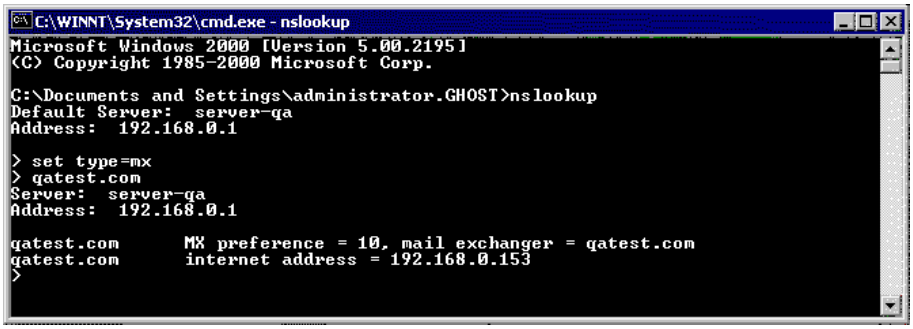
Checking if the MX record for your domain is set correctly

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.



Screenshot 15 - Checking the MX record of your domain

NOTE: If you wish to send out email using a smart host (used when using dial-up) or receive email 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 an email from an external account to an internal user (you can use hotmail, if you do not 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 an email 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 on how to do it:

http://support.microsoft.com/support/kb/articles/Q153/1/19.asp

Step 8: Running GFI MailEssentials setup

1. On the newly configured mail relay machine, log-on as administrator and run the GFI MailEssentials setup file.

2. Select the language in which you would like to install GFI MailEssentials (English or German).

3. A welcome dialog will appear. Close all the other running Windows programs and click **Next** to continue.

NOTE: At this stage GFI MailEssentials will be performing backend checks such as searching for installed applications and it might take some time for the **Next** button to appear.

4. GFI MailEssentials will prompt you to check for a later GFI MailEssentials version. Always use the latest version.

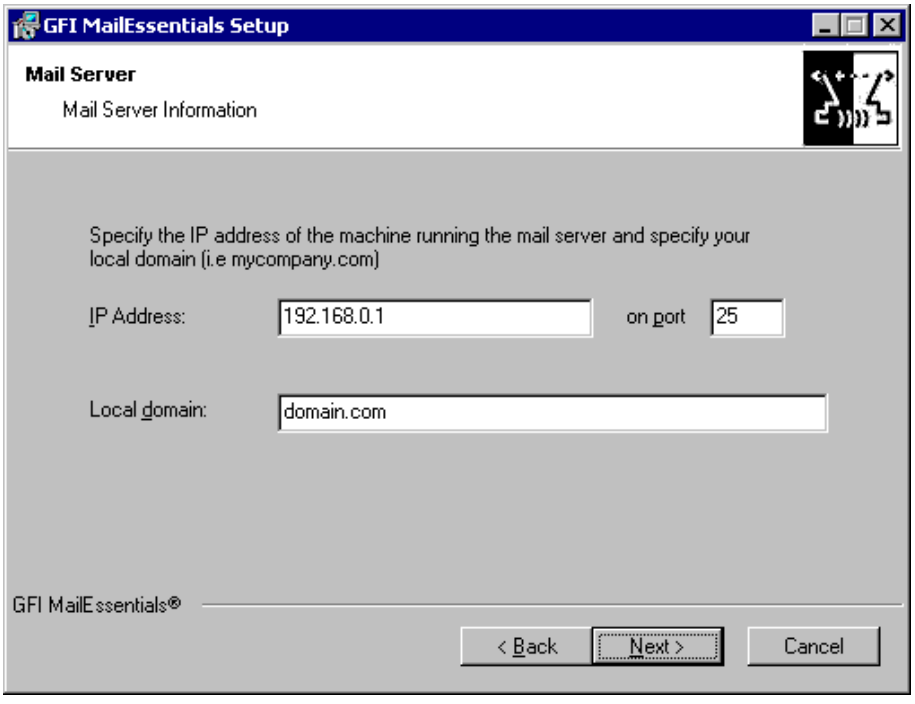
5. Read the licensing agreement carefully. To proceed with the installation, select **I accept the license agreement** and click **Next**.

6. To install GFI MailEssentials to the default location, click **Next** to continue. Alternatively, to specify a custom installation folder click **Browse**, select a new installation path and click **Next** to continue.

7. Enter your name, company, and license key. If you are evaluating the product, leave the default `'Evaluation'`. Click **Next**

8. If you are installing GFI MailEssentials on Microsoft Exchange Server, Setup will now ask you to specify your mail server IP, port and your local domain:

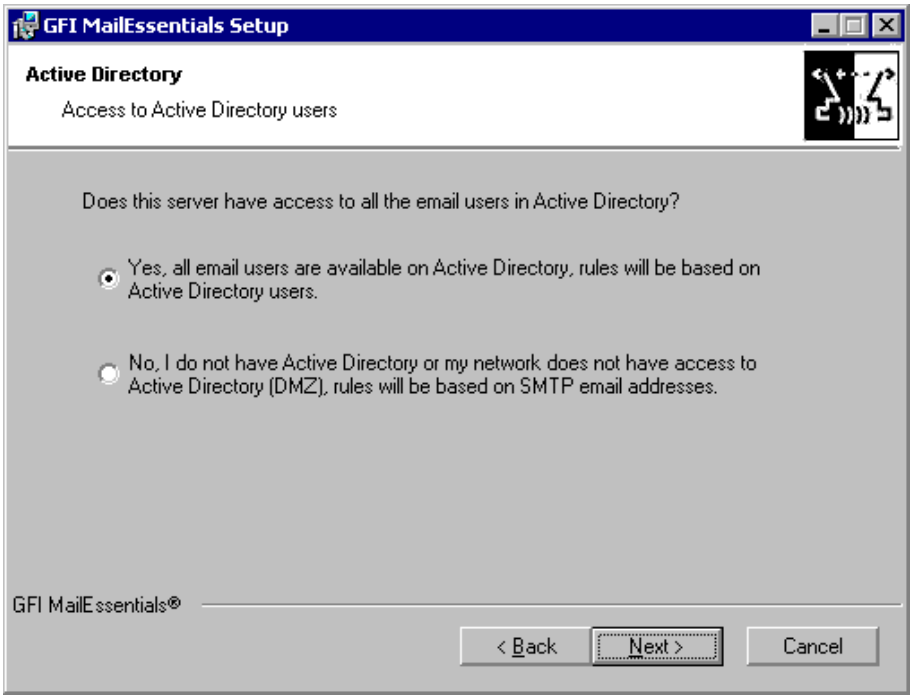
- Specify the IP of your mail server (e.g. Microsoft Exchange Server name) and the port of the mail server.
- Specify your local domain. The local domain is the last part of your internal email address, for example gfi.com.



Screenshot 16 - Specify mail server IP and domain

9. Setup will ask you for the administrator email. GFI MailEssentials will use the administrator email to send critical notifications.

10. If you are installing GFI MailEssentials on a machine that is part of a domain and has Active Directory, setup 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 is better to select SMTP mode. In this mode, all user-based configuration/rules will require you to input the SMTP email address.



Screenshot 17 - Selecting SMTP mode or Active Directory mode

11. If you do not have Microsoft Message Queuing Services (MSMQ) installed, setup 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 Microsoft 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 Microsoft Windows CD and setup will launch the MSMQ setup.

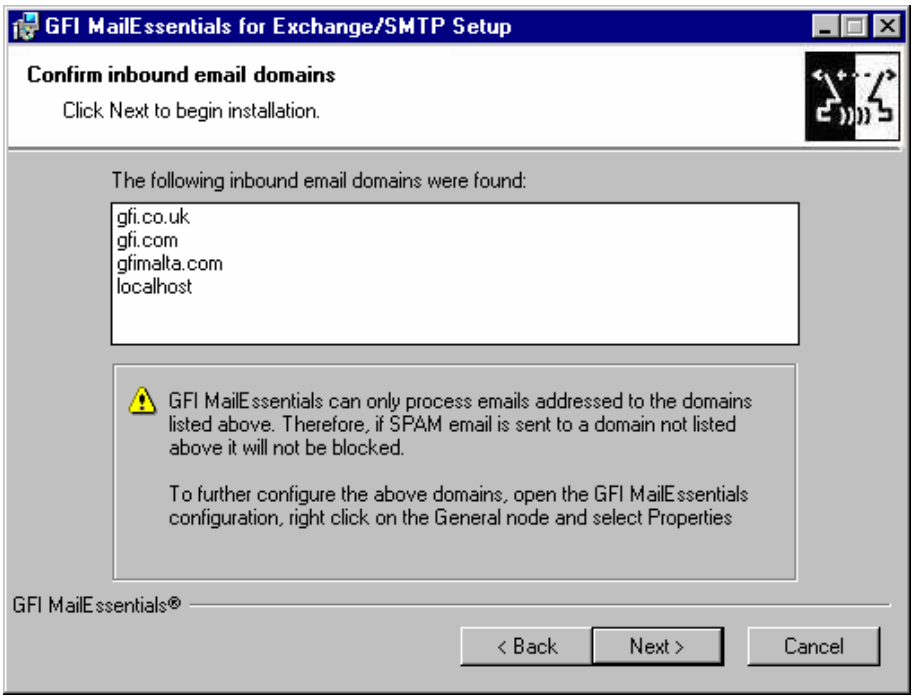
Screenshot 18 - Screenshot 15- Installing Microsoft Message Queuing Service

12. Setup will now confirm the inbound email domains that you have configured. It is important to ensure that your inbound email domains are listed correctly.

IMPORTANT: Ensure that you add all your inbound email domains, for example 'mycompany.com', otherwise inbound email will not be filtered for spam.

NOTE: If you are installing GFI MailEssentials on a Microsoft Exchange 2007 Edge Transport Server Role machine, the inbound email domains step of the installation wizard is skipped since these are determined from the GFI MailEssentials Post-Installation wizard that is launched when you finish this installation wizard.

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



Screenshot 19 - Confirm your inbound email domain

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

NOTE 1: If you are installing GFI MailEssentials on a x64 machine with Microsoft Exchange Server 2007, the files will be installed under the c:\program files (x86)\ folder.

NOTE 2: If you are installing on a Microsoft Exchange 2007 Edge Transport Server Role machine, you will not be prompted to restart the SMTP service.

14. After installation, setup will check if you have the Microsoft XML engine installed. If you do not, 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 Microsoft Windows, setup 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 read the following Knowledge Base article:

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.

NOTE: If you are installing on a Microsoft Exchange 2007 Edge Transport Server Role machine, the installation will launch the GFI MailEssentials Post-Installation Wizard. Refer to the following section for information on how to use this wizard.

15. Upon first installation, GFI MailEssentials will display the Quick Start Guide that introduces the GFI MailEssentials Configuration console and explains how to quickly configure/customize the most powerful GFI MailEssentials anti-spam filters.

GFI MailEssentials Post-Installation Wizard

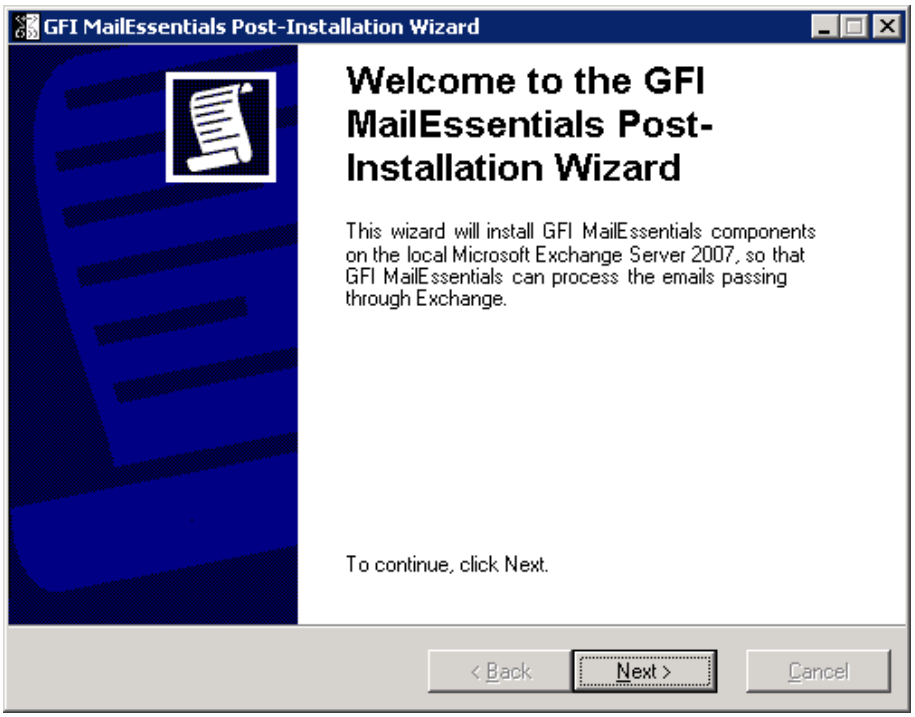
NOTE: This section applies only when installing GFI MailEssentials on a Microsoft Exchange Server 2007 machine.

IMPORTANT: You need to complete this wizard for GFI MailEssentials to work with Microsoft Exchange Server 2007.

The GFI MailEssentials installation wizard launches the GFI MailEssentials Post-Installation Wizard when you click **Finish**. The GFI MailEssentials Post-Installation Wizard registers GFI MailEssentials with the local installation of Microsoft Exchange Server 2007 so that it can process the emails passing through the server.

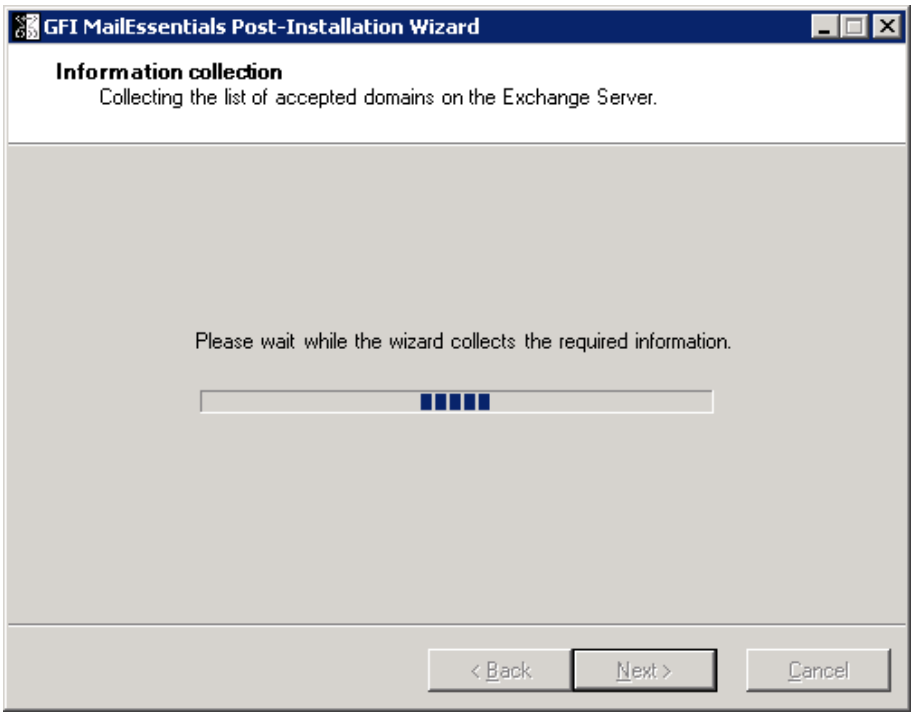
To complete the GFI MailEssentials Post-Installation Wizard, follow these steps:

1. Click **Next** in the welcome page.



Screenshot 20 - GFI MailEssentials Post-Installation Wizard welcome page

2. The wizard will collect information from the Microsoft Exchange Server 2007 installation, such as the list of inbound email domains and the server roles installed, for example Hub Transport Server Role.



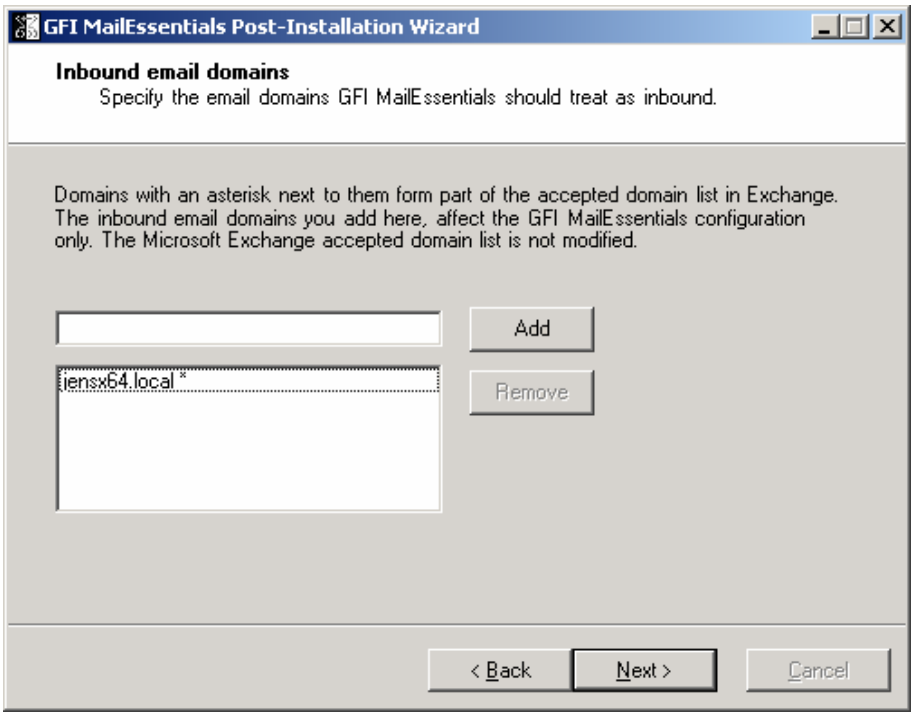
Screenshot 21 - Collecting information from Microsoft Exchange Server 2007

3. The wizard will display the accepted domain list collected from Microsoft Exchange Server 2007. If you need to specify another local domain, type it in the **Inbound email domains** box and click **Add**. If you want to remove a domain that you added from this page, click on it from the list, and then click **Remove**.

NOTE 1: The inbound email domains you add from this page affect the GFI MailEssentials installation only. The Microsoft Exchange Server 2007 accepted domains list is not modified.

NOTE 2: GFI MailEssentials does not support the use of wildcards when specifying inbound email domains. Thus, for example, specifying **.gfimalta.com* as an inbound email domain is not supported.

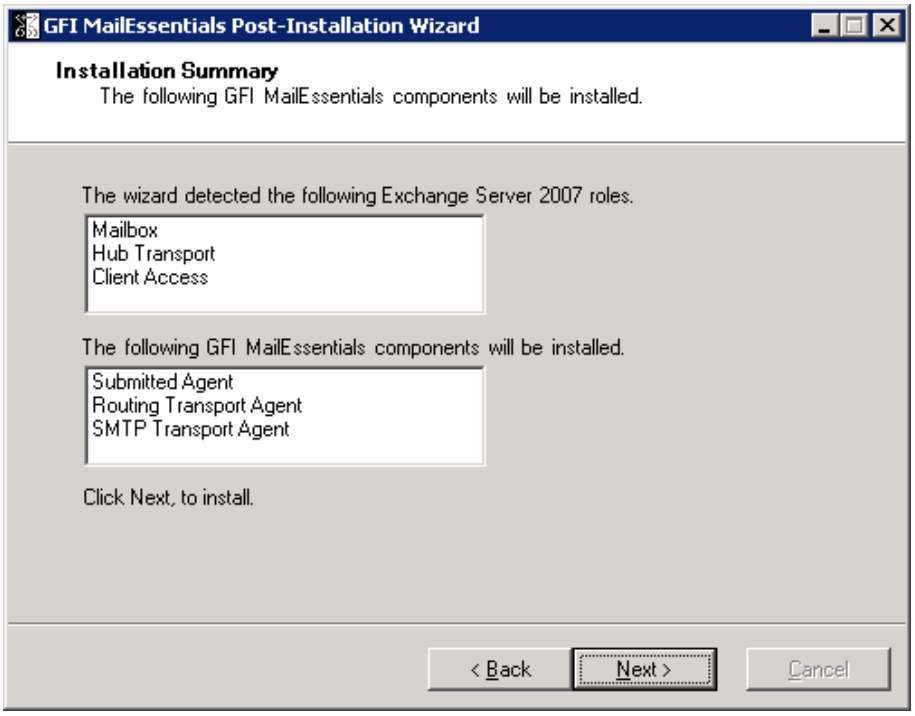
NOTE 3: An asterisk (*) next to an inbound email domain is used to differentiate between domains detected by Microsoft Exchange, and those added manually. Inbound email domains shown with an asterisk next to them are domains detected by Microsoft Exchange.



Screenshot 22 – Inbound email domains list

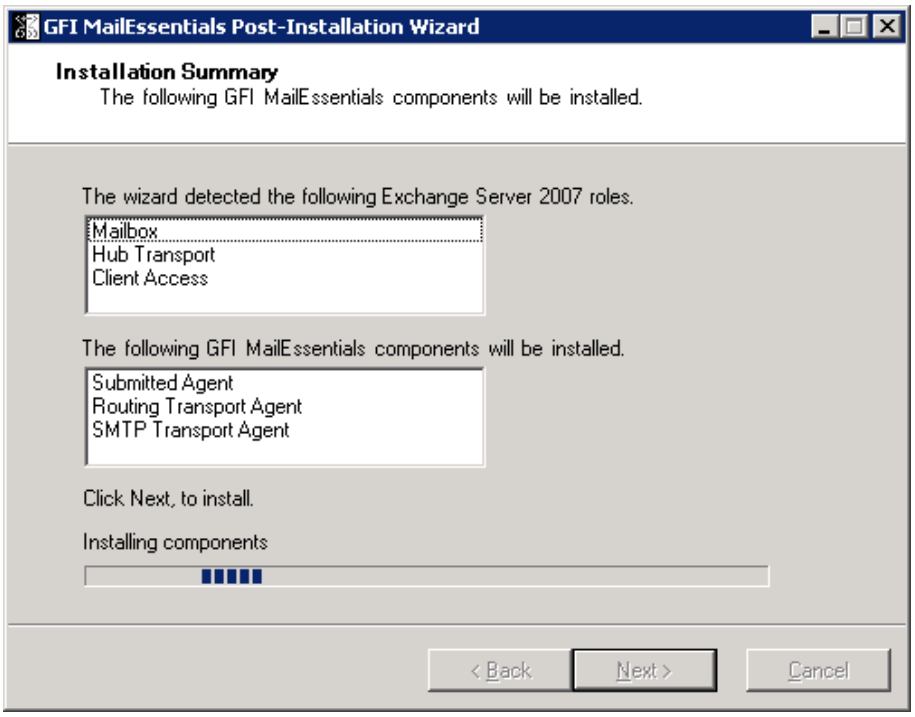
4. Click **Next** to continue.

5. The wizard displays a list of the Microsoft Exchange Server 2007 server roles detected on this machine, and a list of the GFI MailEssentials components it needs to register for it to be able to process and scan emails passing through the server.



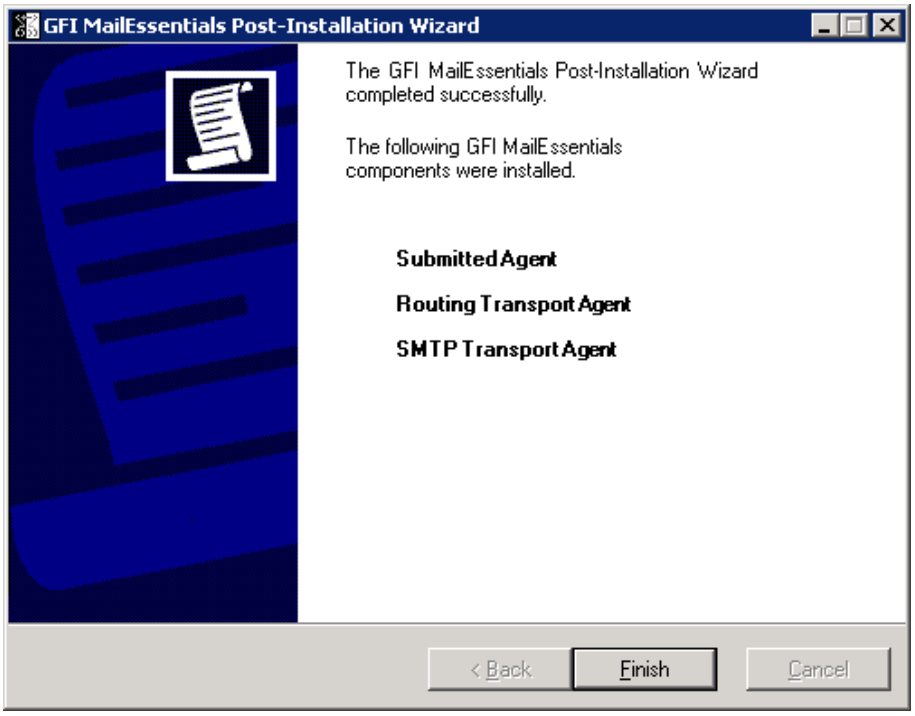
Screenshot 23 - Server roles detected and list of components to install.

6. Click **Next** to install the required GFI MailEssentials components.



Screenshot 24 - Installing the required GFI MailEssentials components

7. In the finish page, the GFI MailEssentials Post-Installation wizard will list the GFI MailEssentials components that it successfully installed. Click **Finish** to close the wizard and complete the installation of GFI MailEssentials on a Microsoft Exchange Server 2007 machine.

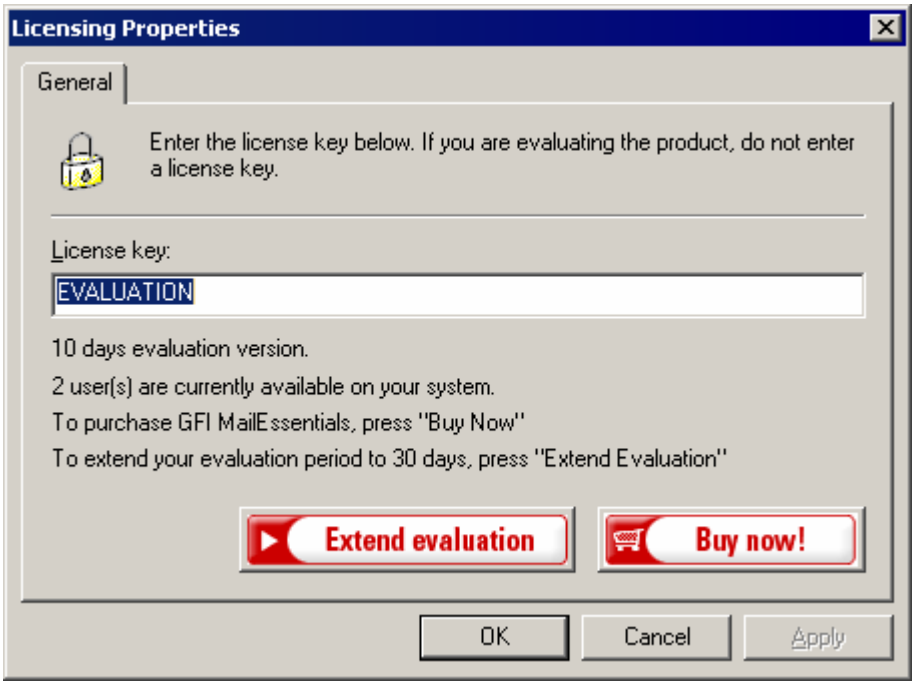


Screenshot 25 - GFI MailEssentials Post-Installation Wizard finish page

Entering your license key after installation

The unregistered, evaluation version of GFI MailEssentials expires after 10 days.

You must license GFI MailEssentials for the amount of mailboxes that you have on your mail server. For more information on GFI MailEssentials licensing visit: http://www.gfi.com/pricing/pricelist.aspx?product=me.



Screenshot 26 – General licensing node

When you obtain the 30-day evaluation key or the purchased licensed key, you can enter your license key in the **General** > **Licensing node**, without having to re-install the product.

NOTE: 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://customers.gfi.com.

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 rule manager does not support Microsoft Exchange Server 2007. If you have a Microsoft Exchange Server 2007 environment, and GFI MailEssentials is not installed on the Microsoft Exchange 2007 Mailbox Server Role machine, you can configure Transport rules from the Microsoft Exchange Server 2007 configuration. To do this, configure GFI MailEssentials to tag spam email in the subject with a keyword, for example, [SPAM]. Then configure a transport rule to set the SPAM confidence level to 9 on emails with the [SPAM] keyword in the subject. The transport rule will then move the spam email detected by GFI MailEssentials to the users' junk mail folder.

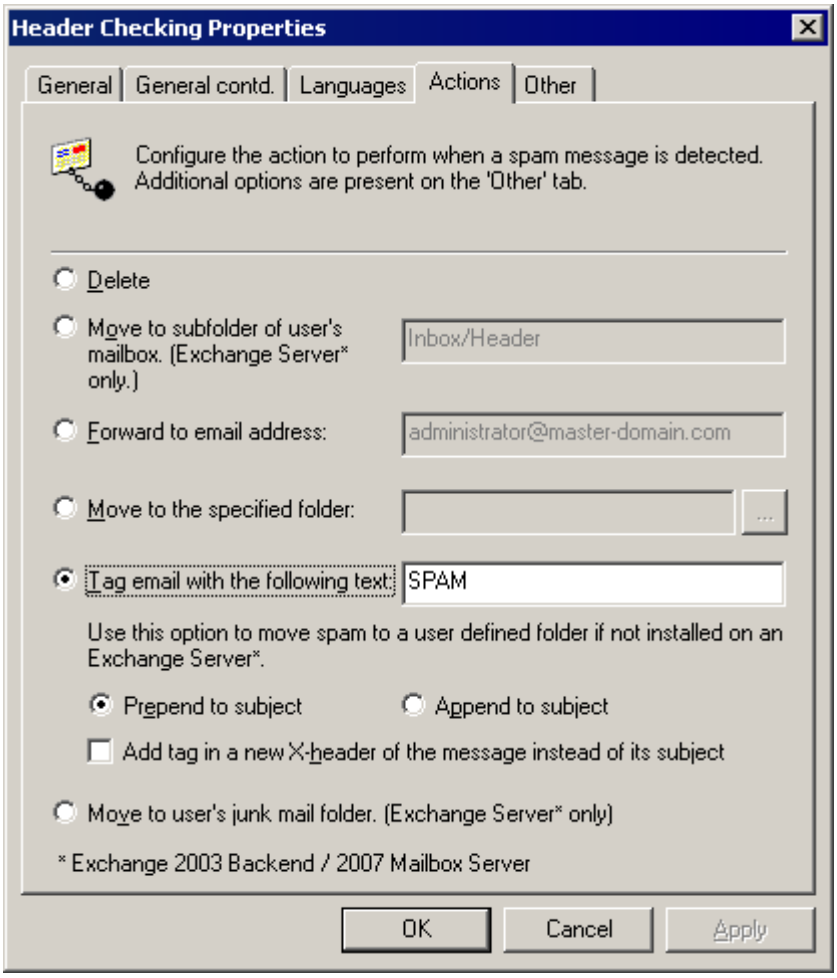
The mailbox rule manager

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

How it works

You need to install the rule manager on the Microsoft Exchange Server and specify the mailboxes which you wish to install the rule on. Then you specify in the GFI MailEssentials configuration that all spam email must be tagged.

NOTE: If you want to use the rule manager, select the TAG action only. If you select any other type of action, the emails detected as spam will not reach the mailbox of the user, and therefore the rule will never be activated.



Screenshot 27 - Tag email to work in conjunction with Rules Manager

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

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

If you have installed GFI MailEssentials on the Microsoft Exchange Server 2000/2003 machine itself, you do not need to run the mailbox rule manager, because GFI MailEssentials will be able to route the email 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**, click **Next** and specify the path were the Bayesian wizard and rule manager files will be extracted.

3. Click **Yes** to start installing the Bayesian Wizard.

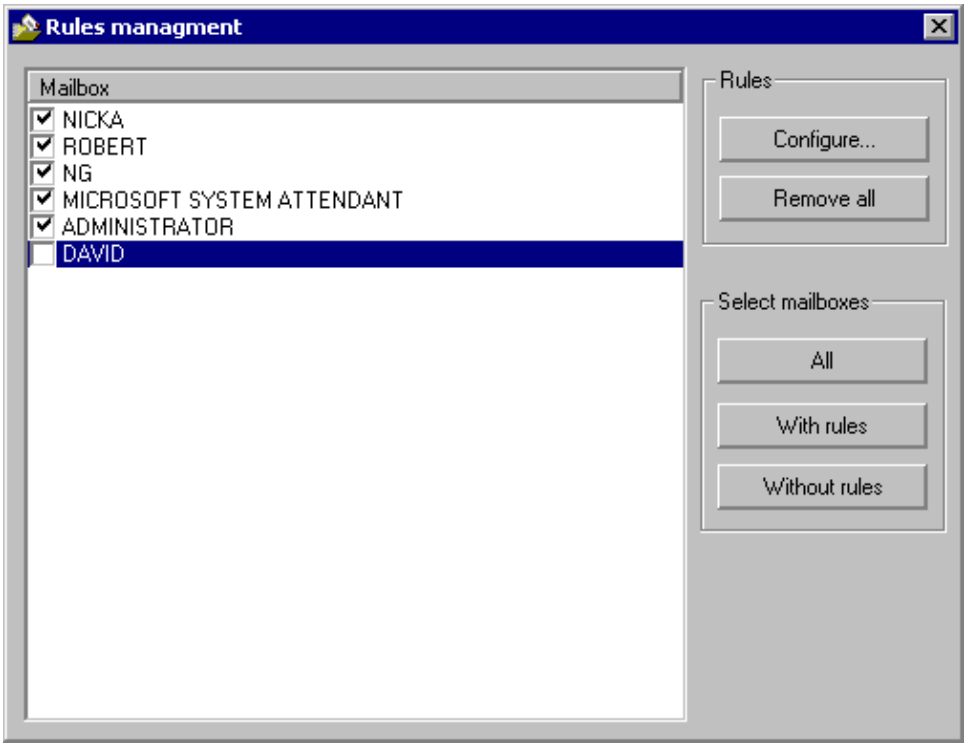
NOTE: The Bayesian Wizard can only be installed on a separate machine as a stand-alone tool. The server version of GFI MailEssentials includes the Bayesian wizard by default, and thus can be used without further configurations.

NOTE: The Bayesian wizard (bayesianwiz.exe) installation **does not** create any icon or additional components in the GFI MailEssentials program group. In order to launch the rule manager, run **rulemgmt.exe**.

Configuring the rules on user's mailboxes

To configure the rules on users' mailboxes:

1. Run the rule manager application (**rulemgmt.exe**) from the GFI MailEssentials program folder (by default C:\Program Files\GFI\MailEssentials).



Screenshot 28 - 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 two types of rules:

- A rule which moves email marked as spam to the user's junk mail folder

- A rule which deletes email marked as spam (This rule can be used for users who wish to delete their spam automatically).

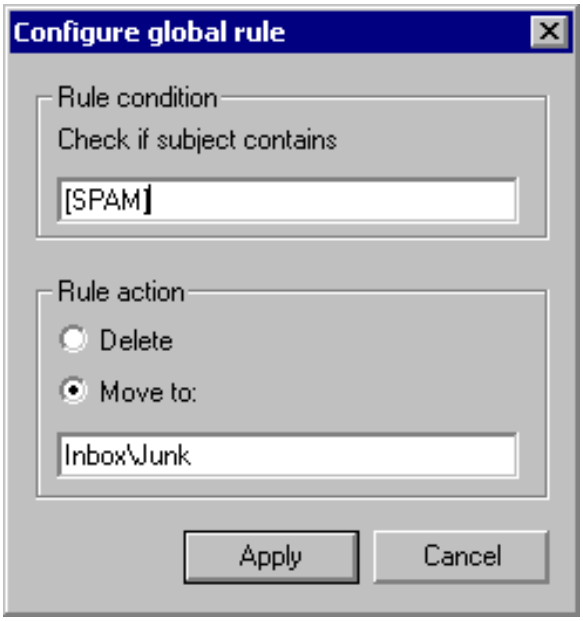
NOTE: You can select multiple mailboxes and configure rules for all of them in one go (as long as the same rule applies to all).

3. Click **Configure**. By default, the rule will check for [SPAM] in the subject. You should enter the exact phrase you configured in the GFI MailEssentials configuration tag action box.

NOTE: If you change this, you will have to change the tag appended by GFI MailEssentials at server level too.

4. Select whether you want to delete the spam emails or move the spam emails to a separate folder. If you select to move spam email, you will need to specify the folder name. If you specify for example inbox\junk, then that 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.

5. Click **Apply**.



Screenshot 29 - Create a rule

6. All the 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 and complementary to the Bayesian filter, it is the Bayesian filter that makes it possible to eliminate spam from your network.

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

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

IMPORTANT: Do not judge the spam detection rate of GFI MailEssentials until you have allowed the Bayesian filter to run for at least one week. GFI MailEssentials can achieve the highest detection rate compared to other anti-spam solutions because it adapts specifically to your email. Be patient and wait at least a week before you evaluate 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 and An Introduction to Bayesian Networks and their Contemporary Applications.

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

Creating a tailor-made Bayesian word database

Before email 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 email and valid email (referred to as 'ham').

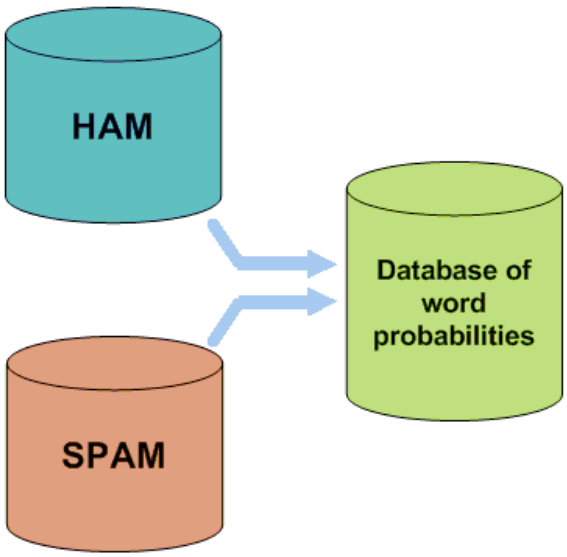


Figure 1 - Creating a word database for the filter

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 email (ham). This is done by analyzing the users' outbound email and by analyzing known spam: All the words and tokens in both pools of email are analyzed to generate the probability that a particular word points to the email being spam.

This word probability is calculated as follows: If the word ‘mortgage’ occurs in 400 of 3,000 spam emails 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 is important to note that the analysis of ham email is performed on the company's email, and is therefore tailored to that particular company. For example, a financial institution might use the word ‘mortgage’ many times over and would get many 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 email (and recognizes ‘mortgage’ as being frequently used in legitimate messages), it will have a much better spam detection rate and a far lower false positive rate.

Creating the spam database

Besides ham email, the Bayesian filter also relies on a spam data file. This spam data file must include a large sample of known spam. Additionally, it 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.

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 email arrives, it is broken down into words and the most relevant words - i.e., those that are most significant in identifying whether the email 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, the message is classified as spam.

Why Bayesian filtering is better

1. The Bayesian method considers the whole message - It recognizes keywords that identify spam, but it also recognizes words that denote valid email. 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 that sent the message and thus classify the message as legitimate, for instance; it allows words to ‘balance’ each other out.

2. A Bayesian filter is constantly self-adapting - By learning from new spam and new valid outbound emails, 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 it is unlikely to occur in a ham email.

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 nearly useless in non English-speaking regions. The Bayesian filter also takes into account certain language deviations or the diverse usage of certain words in different areas, even if the same language is spoken.

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 or Viagra), or more words that generally indicate valid email (such as a valid contact name). 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’.

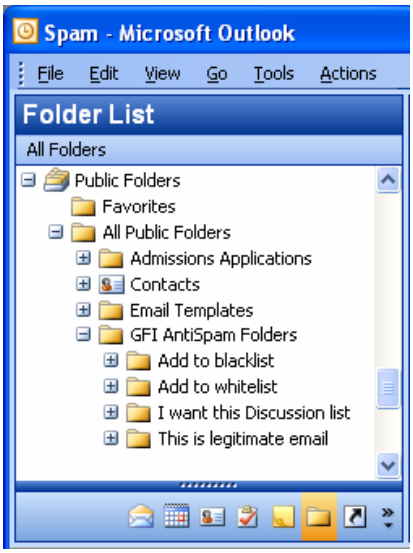
What is the catch?

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 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 two ways:

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

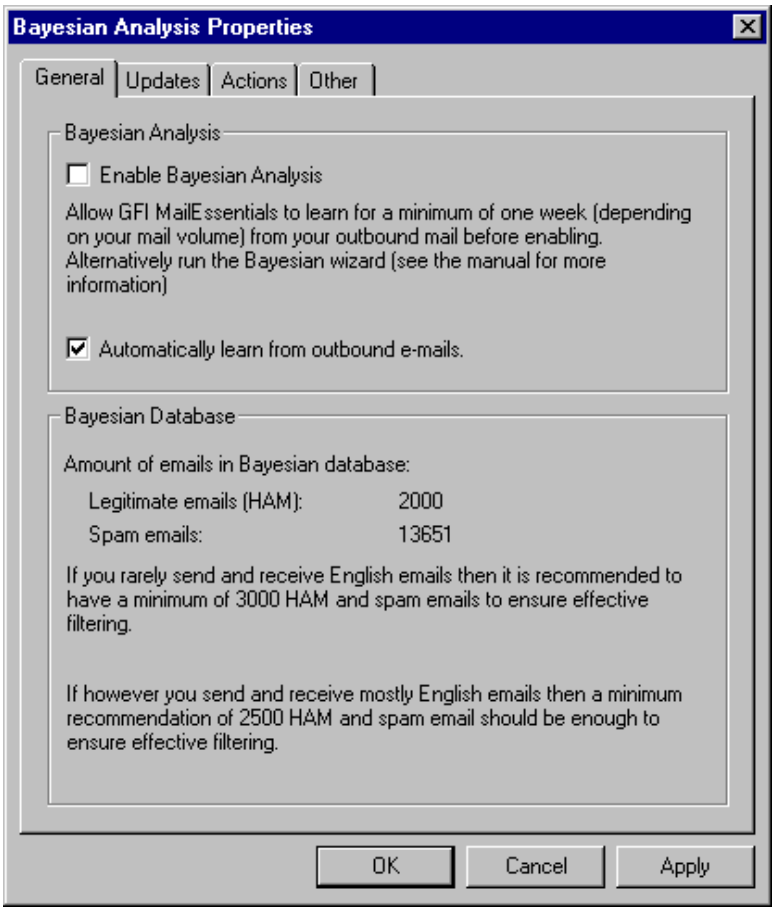


Screenshot 30 - Supplying ham to the Bayesian filter

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 Folders** public folders. For more information, see the 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 by following these steps:

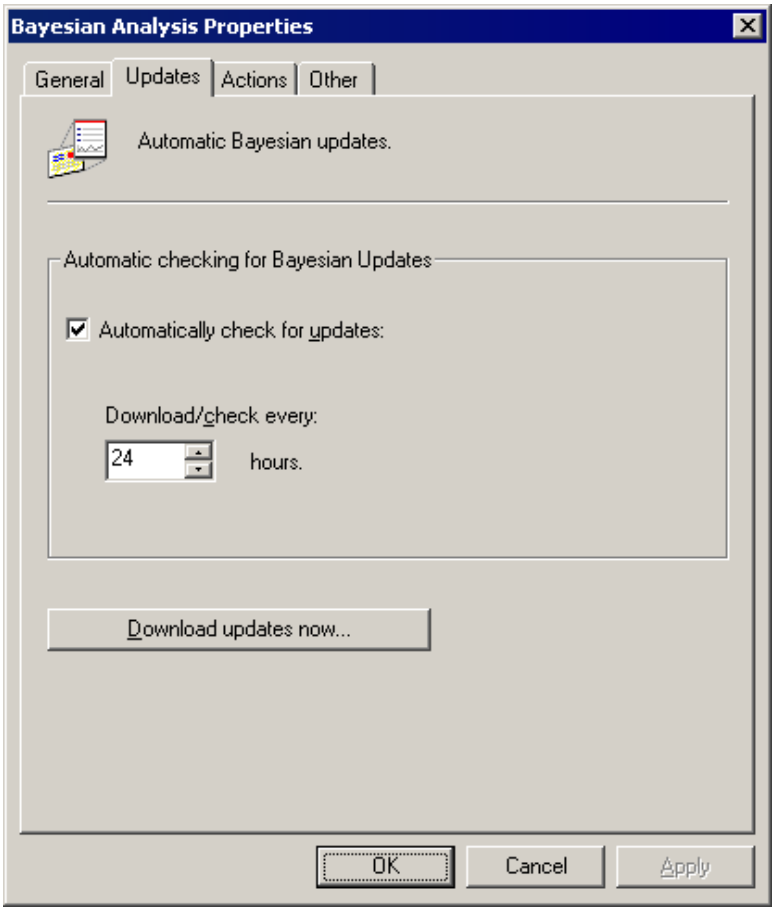


Screenshot 31 - Bayesian analysis properties

1. In the GFI MailEssentials configuration, select the **Anti-Spam > Bayesian Analysis** node, right-click and select **Properties**. This brings up the **Bayesian Analysis Properties** dialog. From the **General** tab, select the **Enable Bayesian Analysis** checkbox.

2. Ensure that the **Automatically learn from outbound emails** option is checked. This option will continuously update the legitimate email database with outbound emails.

Updates



Screenshot 32 - Bayesian updates

3. From the **Updates** tab, you can specify how frequently GFI MailEssentials should check for updates to the spam database. To do this, select the **Automatically check for updates** checkbox and specify an interval in hours in the **Download/check every** field. If you want to trigger an instant download, click the **Download updates now** button. The updates will be downloaded from the preferred server selected. For more information on how to select the preferred server, refer to the 'Selecting the server from where to download updates' section of the 'Miscellaneous Options' chapter.

Actions

After you have configured the Bayesian filter, you can configure what you wish to do with email marked as Spam. For more information refer to the 'Actions – what to do with spam email' section of 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:

SpamRazer

SpamRazer is a secondary anti-spam engine that uses various technologies such as email reputation, message fingerprinting and heuristics to block spam.

Phishing URI Realtime Blocklists (PURBL)

This feature will extract links from the message body and check if they point to known phishing sites or contain typical phishing keywords.

Sender Policy Framework (SPF)

SPF works by publishing a text record in the DNS of domains that indicates which machines send email from that domain. GFI MailEssentials supports SPF and fights spam by checking the SPF record in the received messages. This feature allows you to define the SPF test sensitivity that will be used when processing emails with forged senders (e.g. Block only messages that are determined to have a forged sender).

Whitelists

Whitelists are lists of email addresses, IP addresses and phrases/words from which you always wish to receive email. GFI MailEssentials will automatically build a whitelist for you from outbound email.

Directory Harvesting

This feature blocks emails addressed to users that do not exist on the organization's mail server. Such email attacks occur when spammers try to send messages, using details from known email addresses together with the most common usernames or possible alphanumeric combinations (brute force approach) that could be used for the username part of an email. This is done in order to try to discover other email accounts present on the same server.

Custom blacklist

This feature allows you to specify domains and email addresses from which you do not wish to receive email.

Bayesian analysis

This feature analyses the content of the inbound email and based on mathematical rules decides if the email is spam or not. The Bayesian filter is discussed in the chapter 'The Bayesian anti-spam filter'.

DNS blacklists

This feature allows you to configure GFI MailEssentials to query whether the email sender is on a public DNS blacklist of known spammers. You can also choose to block emails sent from botnet/zombie machines that have their IP listed on SORBS.net.

NOTE: This feature is enabled by default upon installation.

Spam URI Realtime Blocklists (SURBL)

This feature will extract links or domains from the message body and query whether these are listed on public Spam URI Blocklists such as sc.surbl.org

Header checking

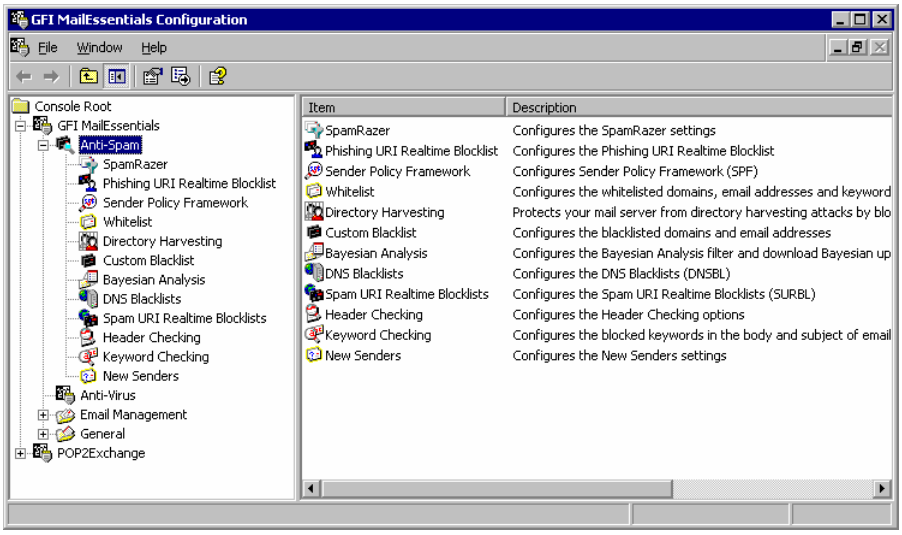
This feature analyses the header of the email to detect whether an email is spam or not.

Keyword checking

This feature allows you to configure keywords that indicate if an email is spam.

New Senders

This feature automatically identifies emails that have been sent from senders to whom you have never sent emails. These emails could be from legitimate senders as well as spam which where not detected by the GFI MailEssentials spam filter.



Screenshot 33 - 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 email address, tag the email or move it to a user's junk mail folder.

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

Defining your Perimeter (Gateway) SMTP Server

The perimeter SMTP server is the Mail server gateway that processes emails received directly from the Internet.

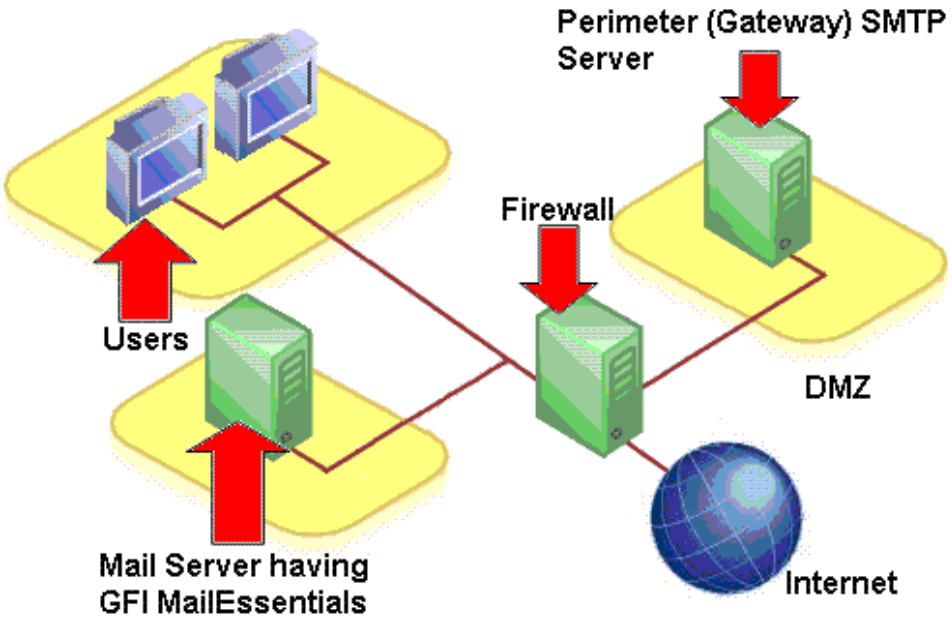
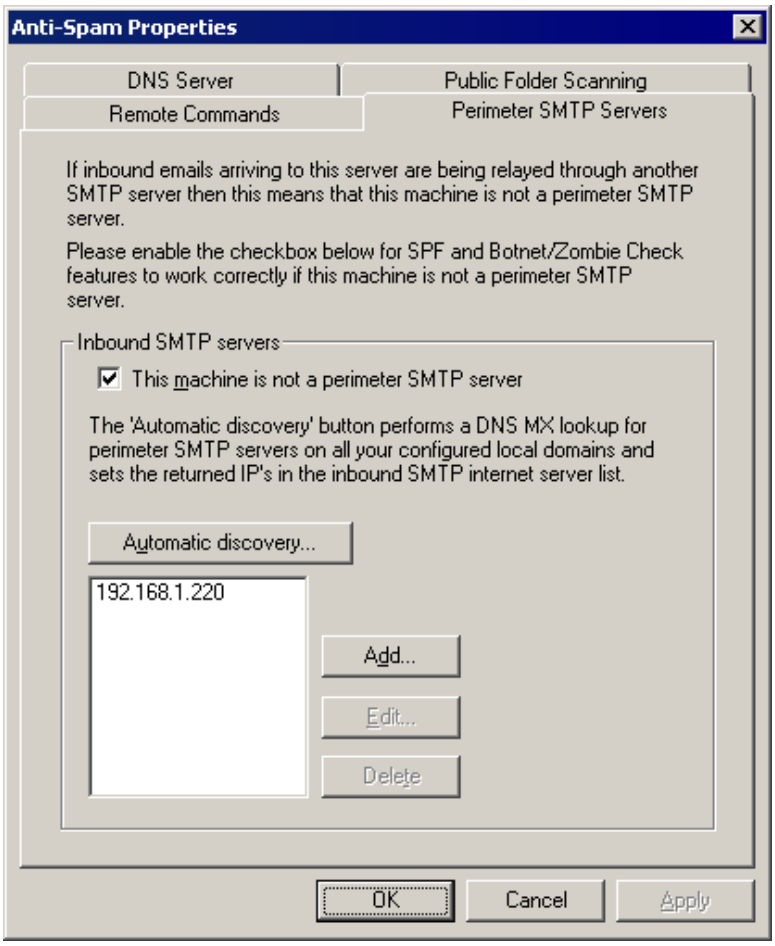


Figure 2 – A typical Perimeter SMTP Relay Server setup

Such gateway SMTP servers are generally specified and configured in the DNS MX records of a domain and are often setup on a De-Militarized Zone (DMZ). The DMZ (see figure above) is a public internal network typically used exclusively for servers that are accessed by external clients on the Internet, such as Web, FTP and Mail servers.

If the inbound emails arriving to the server on which GFI MailEssentials is installed are being relayed from another gateway server, then specify your gateway SMTP server details using the Perimeter SMTP Servers tab in the Anti-spam properties in order for the SPF filter and Botnet/Zombie Check features to work correctly. For example, let us take into account a company in England, which receives all its emails on an SMTP server located in the USA. Since the SMTP server in the USA will relay all emails received to the SMTP server in England, the SMTP server in the USA is the perimeter gateway server for the company in England. That is, when the company in England installs GFI MailEssentials on its local SMTP server, they must enable the option in the perimeter SMTP servers page and specify the details of the SMTP server in the USA for the SPF filter and Botnet/Zombie Check features to work correctly.



Screenshot 34 – Perimeter SMTP Server Setup

When GFI MailEssentials is not installed on the perimeter SMTP server, you must:

1. Right click on the **Anti-Spam** node and select **Properties**.

2. Click on the **Perimeter SMTP Servers** tab and enable the **This machine is not a perimeter SMTP server** option.

3. Click on the **Add** button and specify the IP address of your perimeter (gateway) SMTP server. Repeat the same process if you want to specify alternative perimeter SMTP servers which you might have available. Please make sure to specify your perimeter SMTP servers in their order of preference, with the actual perimeter server being the one at the top of your list, followed by its alternatives.

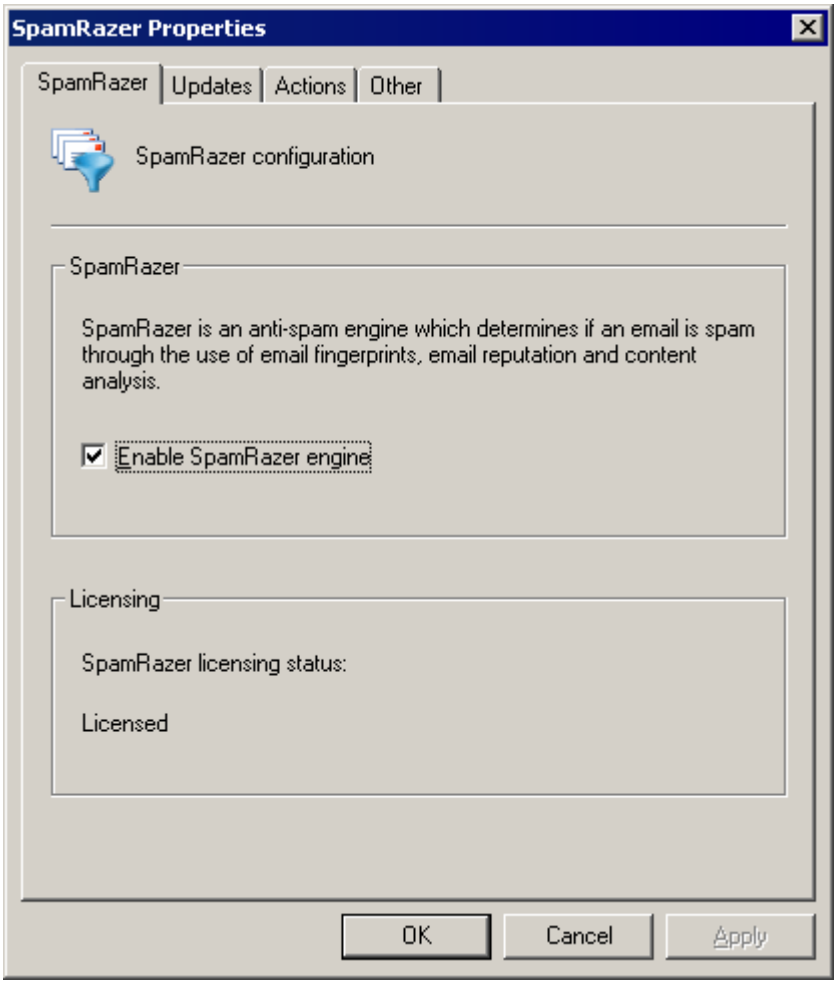
NOTE: You can click **Automatic discovery** to perform a DNS MX lookup to automatically search and retrieve the IP's of perimeter SMTP servers configured on your inbound email domains.

SpamRazer

SpamRazer is a secondary anti-spam engine that uses various technologies such as email reputation, message fingerprinting and heuristics to block spam. Frequent updates are released for SpamRazer that will further increase the response time to new trends of spam.

To enable the SpamRazer check:

1. Right click on the **Anti-Spam > SpamRazer** node and select **Properties**.



Screenshot 35 – SpamRazer Properties

2. In **SpamRazer** tab, select the **Enable SpamRazer engine** option.

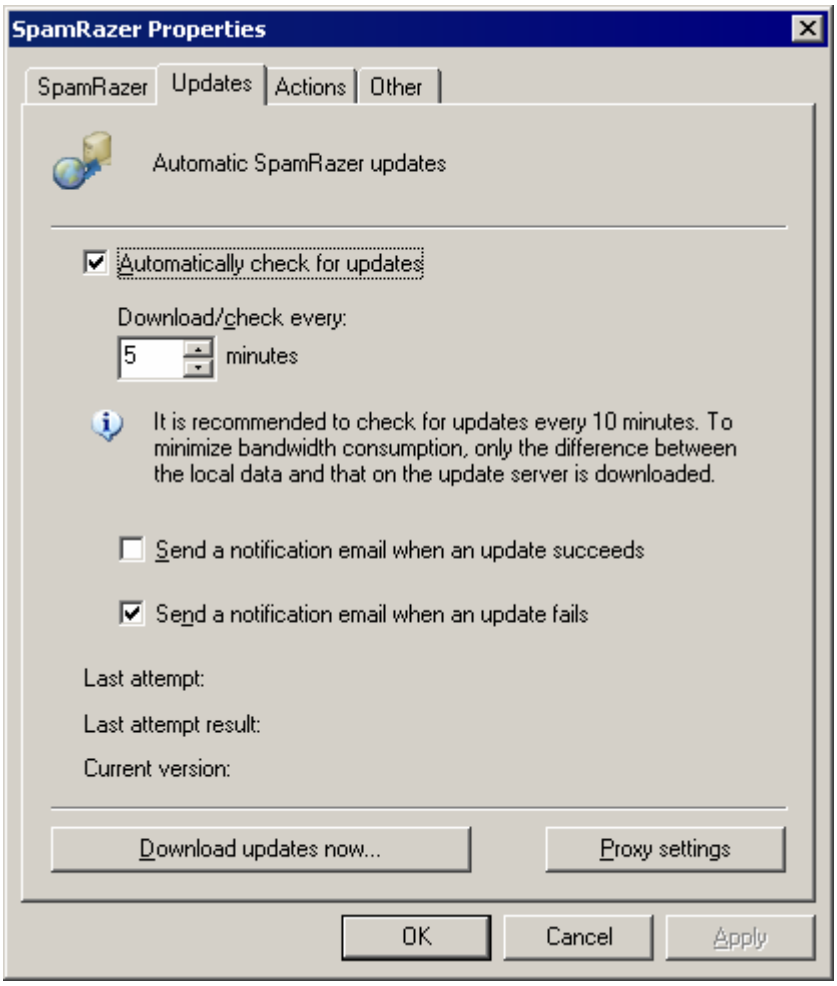
Updates tab

In the **Updates** tab, you can configure GFI MailEssentials to automatically check for and download any SpamRazer updates available. Since new spam techniques are introduced daily, it is recommended to leave the automatic checking and downloading option enabled so that the SpamRazer feature will be more effective in detecting the latest spam emails.

If you want to be informed via email whenever a new SpamRazer update is downloaded and installed, select the **Send a notification email when an update succeeds** checkbox.

If you want to be informed via email whenever a failure occurs, select the **Send a notification email when an update fails** checkbox.

To download through a proxy server, click on the **Proxy settings** button and specify the proxy server.



Screenshot 36 - Automatic SpamRazer updates

Actions tab

After you have enabled SpamRazer checks, click on the **Actions** tab to specify what you want to do with emails marked as spam by this filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

Other tab

Please refer to the 'Other options' section in this chapter.

Phishing URI Realtime Blocklist (PURBL)

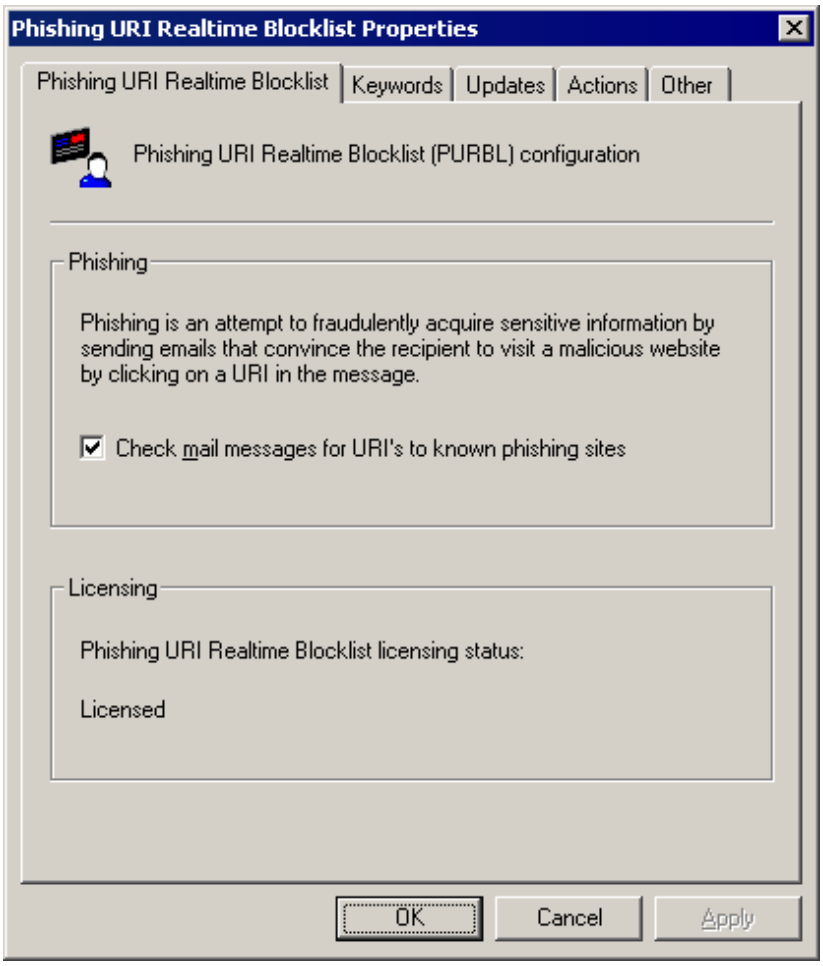
Phishing is a technique used to perform social engineering through emails. A phishing email will be crafted to look like an official email coming from a reputable business, for example a bank. Phishing emails will contain instructions, for example that a bank requires you to reconfirm your online banking username and password or credit card information. The phishing email will include a phishing Uniform Resource Identifier (URI) that the user is supposed to follow to enter some sensitive information on a site, such as the username and password in the example used before. The site pointed to by the phishing URI will look like the official site, but in reality it is controlled by whoever sent the phishing emails. When the user enters the sensitive information on the phishing site, the data will be collected

and is then used for example to withdraw money from your bank account.

The Phishing URI Realtime Blocklist (PURBL) feature of GFI MailEssentials detects phishing emails by comparing URIs present in the email to a database of URIs that are known to be used in phishing attacks, and also by looking for typical phishing keywords in the URIs.

To enable the PURBL check:

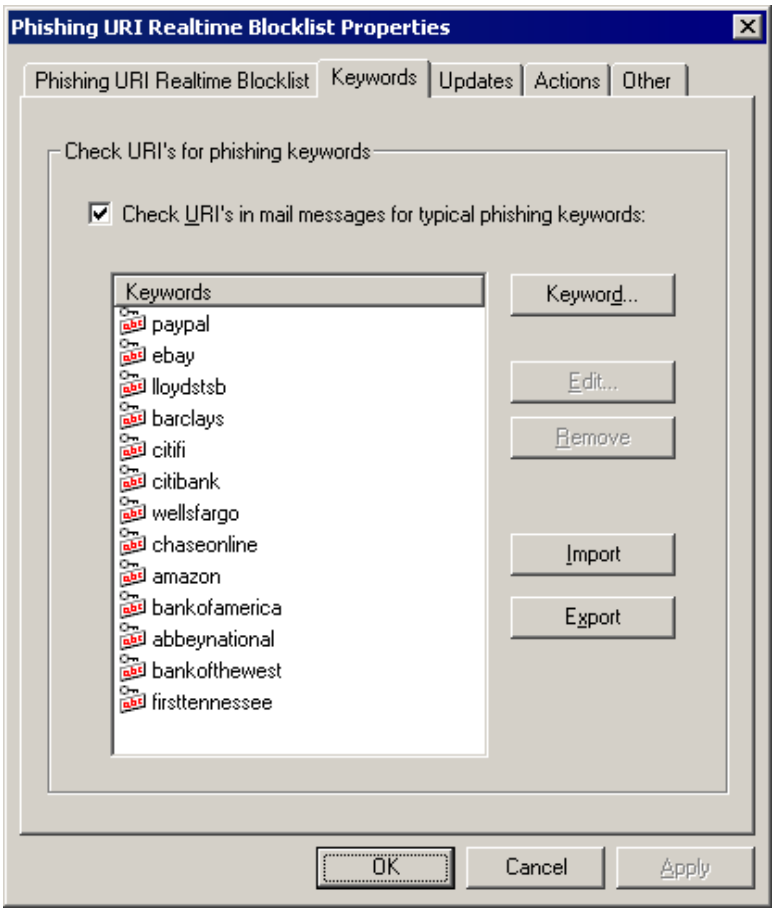
1. Right click on the **Anti-Spam > Phishing URI Realtime Blocklist** node and select **Properties**.



Screenshot 37 – Phishing URI Realtime Blocklist Properties

2. In **Phishing URI Realtime Blocklist** tab, select the **Check mail messages for URI's to known phishing sites** option. This option will instruct GFI MailEssentials to look at the URIs present in an email, perform a lookup of those URIs in a database of URIs that are known to be used to point to phishing sites, and if a match is found, the email containing those URIs will be marked as SPAM email.

3. If you also want to check for phishing keywords in the URIs present in the email, which would be a good indicator that the email is a phishing email, access the **Keywords** tab and select the **Check URI's in mail messages for typical phishing keywords** option.



Screenshot 38 - Phishing keywords

4. To add phishing keywords, click the **Keyword** button. In the **Enter a keyword** dialog specify the phishing keyword and click the **OK** button. The phishing keyword is added to the **Keywords** list.

NOTE: To edit/remove a phishing keyword, select it from the list and click the **Edit** or **Remove** button respectively.

5. When ready, click on the **Apply** button to save the new settings.

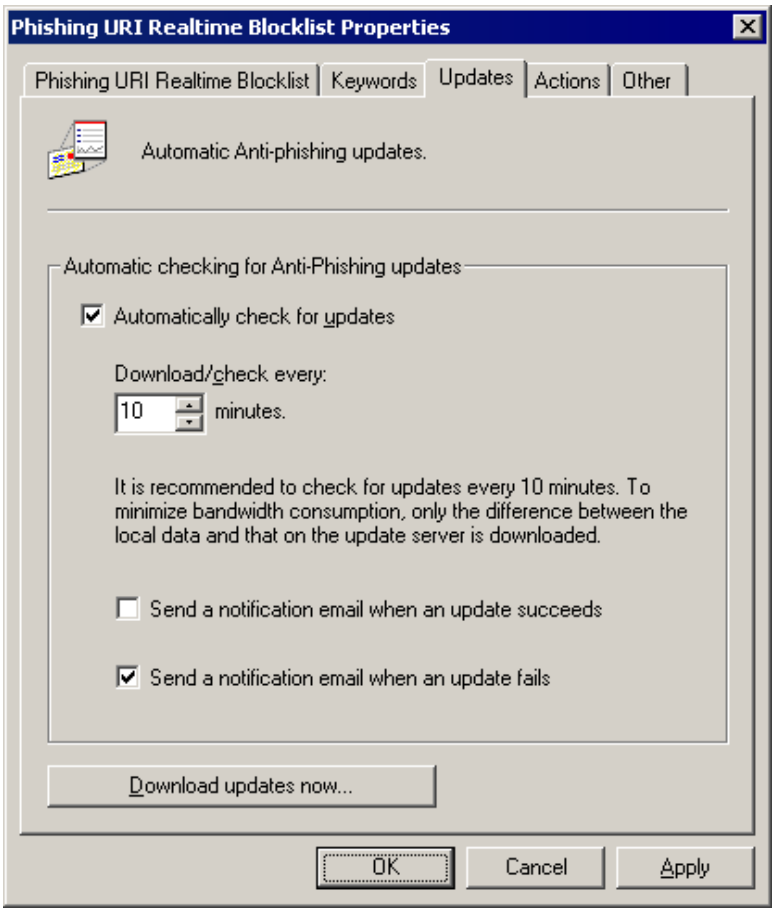
Updates tab

In the **Updates** tab, you can configure GFI MailEssentials to automatically check for and download any anti-phishing updates available. Since new phishing URIs are discovered daily, it is recommended to leave the automatic checking and downloading option enabled so that the PURBL feature will be more effective in detecting the latest phishing email attempts.

If you want to be informed via email whenever a new anti-phishing update is downloaded and installed, select the **Send a notification email when an update succeeds** checkbox.

If you want to be informed via email whenever a failure occurs, select the **Send a notification email when an update fails** checkbox.

The anti-phishing updates will be downloaded from the preferred server selected. For more information on how to select the preferred server, refer to the 'Selecting the server from where to download updates' section of the 'Miscellaneous Options' chapter.



Screenshot 39 - Automatic anti-phishing updates

Actions tab

After you have specified which PURBL checks to perform, click on the **Actions** tab to specify what you want to do with emails marked as spam by this filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

Other tab

Please refer to the 'Other options' section in this chapter.

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 to the machines that perform services (web, email, etc.). All domains already publish email (MX) records to publish the machines that receive email for the domain.

For SPF to work, domains need to publish a text record in the DNS of those domains to publish the machines that send email from the domain. When receiving a message from a domain, GFI MailEssentials can check those records to make sure email is coming from where it should be.

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://www.openspf.org/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 do not 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 email 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 is a forgery. That is how you can tell it is probably a spammer.

For more information on SPF, and how it works, visit the Sender Policy Framework website at http://www.openspf.org.

SPF on a perimeter (Gateway) SMTP server

The perimeter SMTP server is the machine that receives emails directly from the Internet. If you have installed GFI MailEssentials on a perimeter SMTP server, you do not need configure any settings on GFI MailEssentials (i.e. you do not need to configure the perimeter [gateway] SMTP server options in the Perimeter SMTP Servers tab of the Anti-spam properties).

SPF on a non-perimeter (Gateway) SMTP server

If GFI MailEssentials is NOT installed on a perimeter SMTP server, configure the 'Perimeter SMTP Servers' option in the Anti-spam node properties. To setup this option, right click on the Anti-spam node > select **Properties** and click on the Perimeter SMTP Servers tab.

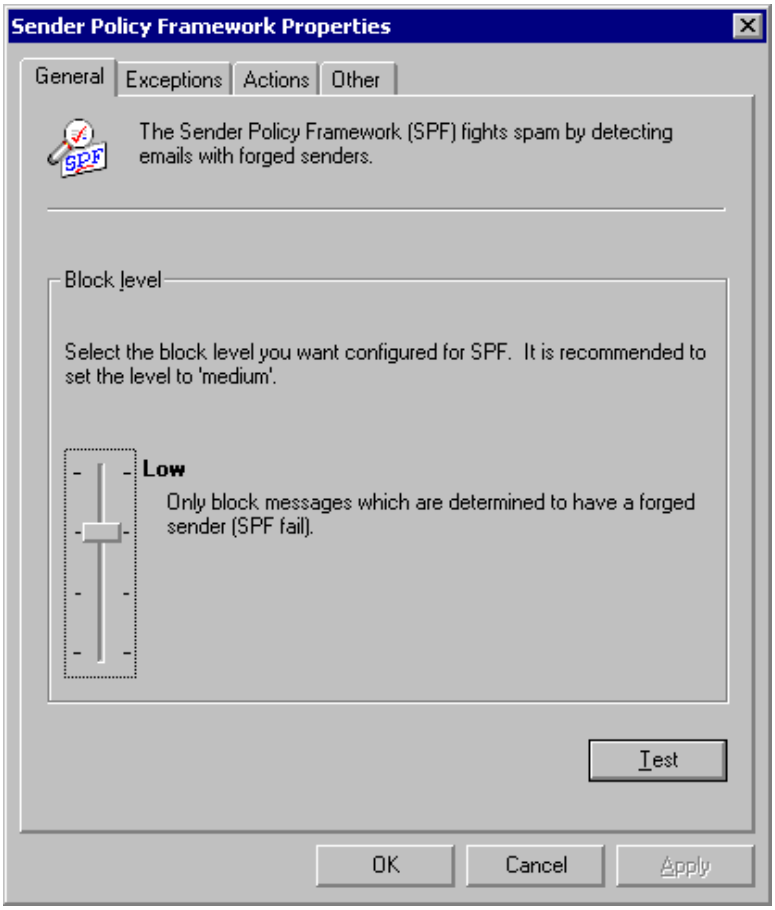
If you are not sure if you have installed GFI MailEssentials on your perimeter SMTP server, you can make use of the 'Auto Discovery' button in the Perimeter SMTP setup option to perform a DNS MX lookup and automatically define the IP address of your perimeter SMTP server.

For further details on how to configure your perimeter SMTP server option, please refer to the 'Defining your Perimeter (Gateway) SMTP Server settings' section in this chapter.

Configuring the SPF feature

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

SPF block level



Screenshot 40 - Configuring the SPF block level

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

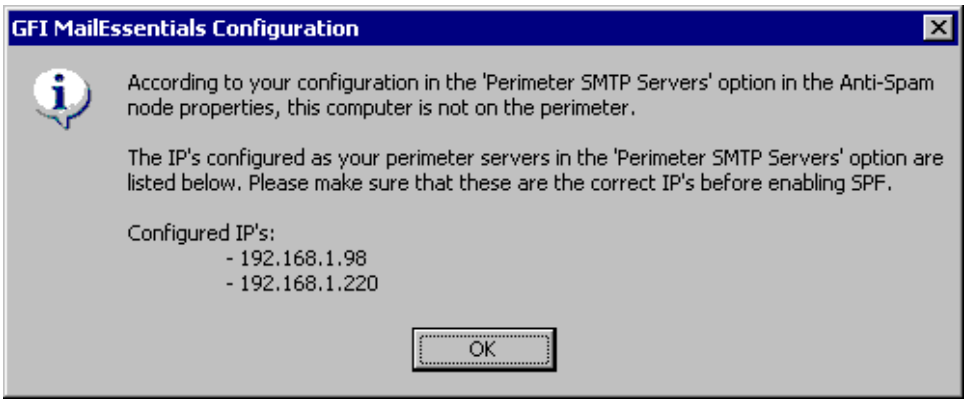
Never: Never block any messages. When this option is selected, SPF tests are not done on incoming emails.

Low: Only block messages that 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.

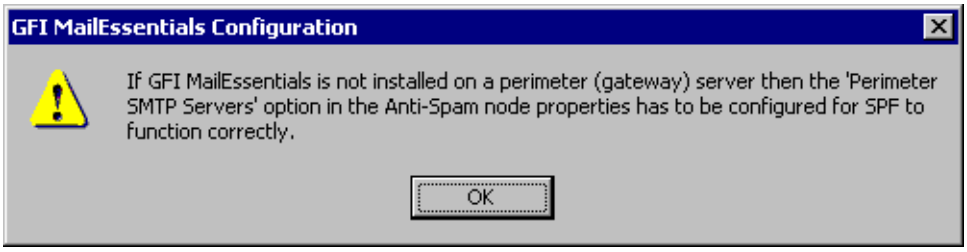
High: Block any message that is not proven to be from the sender. This option will treat all email as spam unless it could be proven that the sender is not forged. Since the majority of mail servers do not yet have an SPF record, this option is not yet recommended.

After you define the sensitivity required for your SPF test, click on the **Apply** button to save this configuration. If you have already specified in GFI MailEssentials that this computer is not your perimeter SMTP server (refer to 'Defining your perimeter (gateway) SMTP server' section in this chapter), a dialog box similar to the one shown below will pop up. This dialog box shows the perimeter SMTP server settings that you have configured in GFI MailEssentials (i.e. the IPs specified for your perimeter SMTP server).



Screenshot 41 – Current Perimeter SMTP Server setup

If GFI MailEssentials is installed on your perimeter SMTP server or if you have not yet specified that the mail server on which GFI MailEssentials is installed is not a perimeter SMTP server (refer to 'Defining your perimeter (gateway) SMTP server' section in this chapter), the dialog box shown below will pop up.



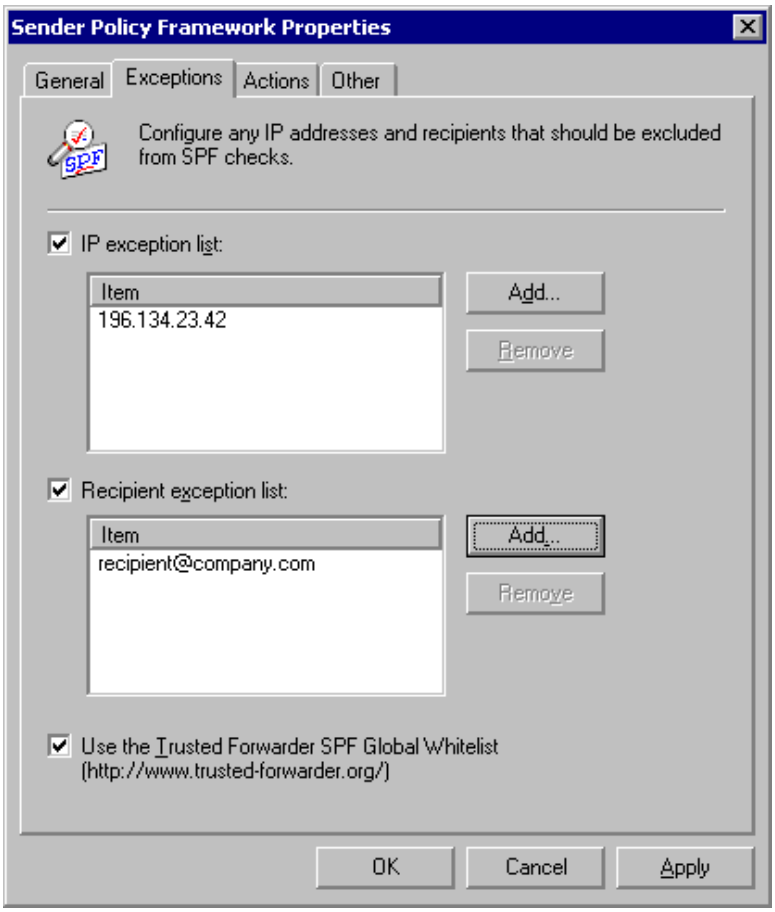
Screenshot 42 - Reminder: SPF must be installed on the perimeter SMTP server.

This dialog box will remind you that if this computer is not a perimeter server, configure the **Perimeter SMTP Servers** option in the Anti-spam node properties (right click on the **Anti-Spam** node and select **Properties**. Click on the **Perimeter SMTP Servers** tab). For further information on how to configure your perimeter SMTP server, please refer to the 'Defining your perimeter (gateway) SMTP Server' section in this chapter.

Click on the **OK** button. If you wish to test your DNS settings/services, click on the **Test** button located on top of the **Apply** button.

Configuring Exceptions

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



Screenshot 43 - Configuring the SPF exceptions

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

Recipient exception list: With this option you can ensure that certain recipients always receive their email, 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 leave this option enabled always.

Actions tab

After you have configured the SPF feature, click on the **Actions** tab to specify what you want to do with emails marked as Spam by the SPF filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

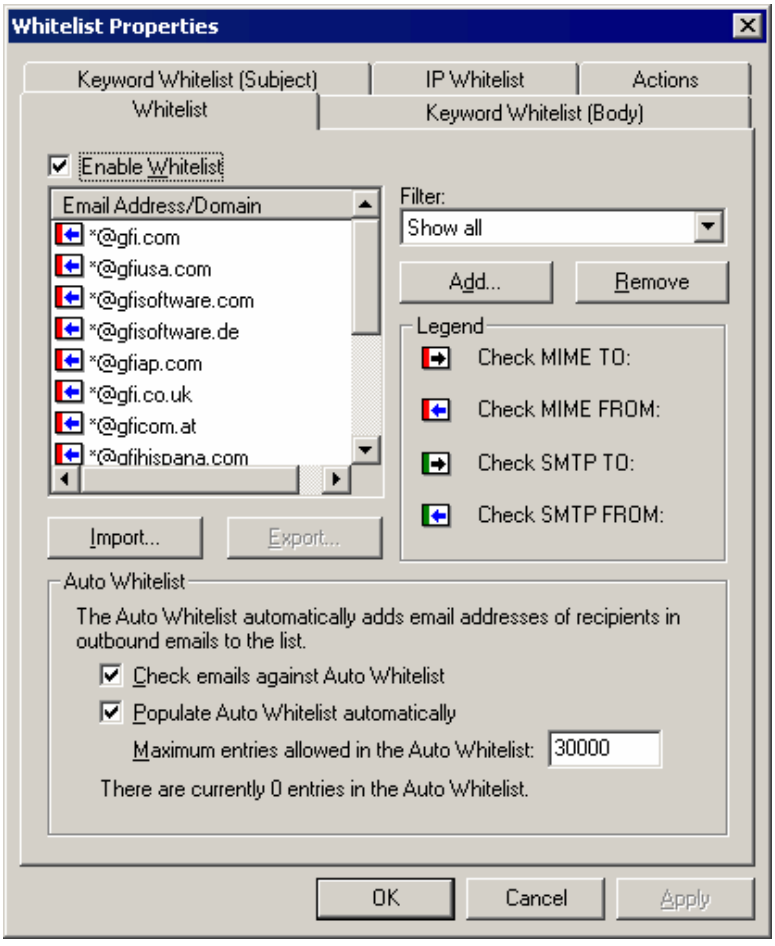
Other tab

Please refer to the 'Other options' section in this chapter.

Whitelist

The Whitelist is a list of email addresses and domains from which you always wish to receive emails. i.e., emails 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 whitelist the email.

To configure the Whitelist, right click on the **Anti-Spam > Whitelist** node and select **Properties** from the context menu. The first tab is the **Whitelist** configuration.



Screenshot 44 - Whitelisted domains

To add a whitelisted domain or email address:

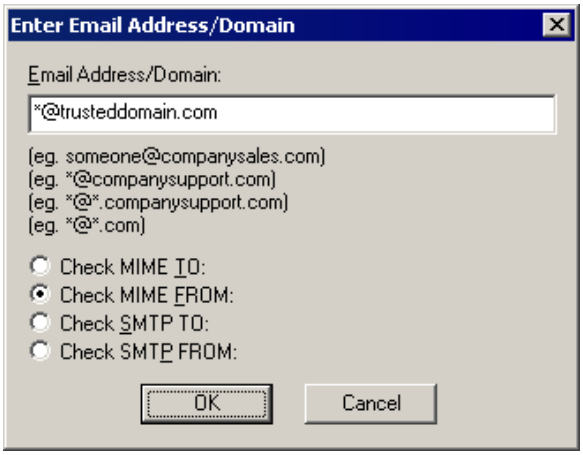
1. Click the **Add** button. The **Enter Email Address/Domain** dialog is displayed.

2. In the **Email Address/Domain** edit box you can specify a full email address, emails from an entire domain, for example '*@companysupport.com' or else whitelist an entire domain suffix, for example *@*.mil or *@*.edu. The latter will for example ensure that email sent from military or educational domains will never be marked as spam.

3. To specify in which email header field this entry should be matched, so as to whitelist the email, select one of the **Check…** options. For example, to whitelist all inbound email sent by a specific user, select the **Check MIME FROM:** option.

NOTE 1: 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 whitelisted with the **Check MIME TO:** option.

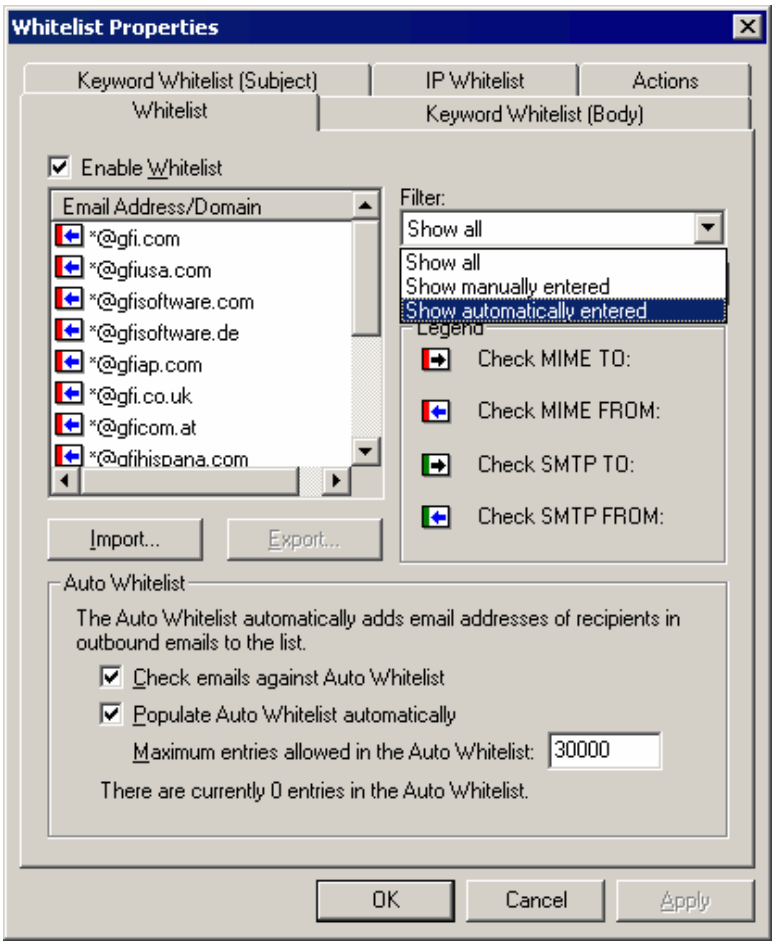
NOTE 2: To exclude a local user from spam filtering, simply enter the email address of the user, and select the Check MIME TO: option.



Screenshot 45 - Adding a whitelisted email entry

Auto whitelist

This feature, when enabled, automatically whitelists email addresses to which you send email. Clearly, you will want to receive a reply from anyone you send an email to; automatic whitelisting therefore makes a lot of sense. The process is completely automatic - you will have a reliable and constantly updated whitelist in no time and without any administration. You can specify the total amount of email addresses to be stored in the whitelist up to a maximum of 30,000 addresses. After the maximum amount is reached, the oldest records are replaced.

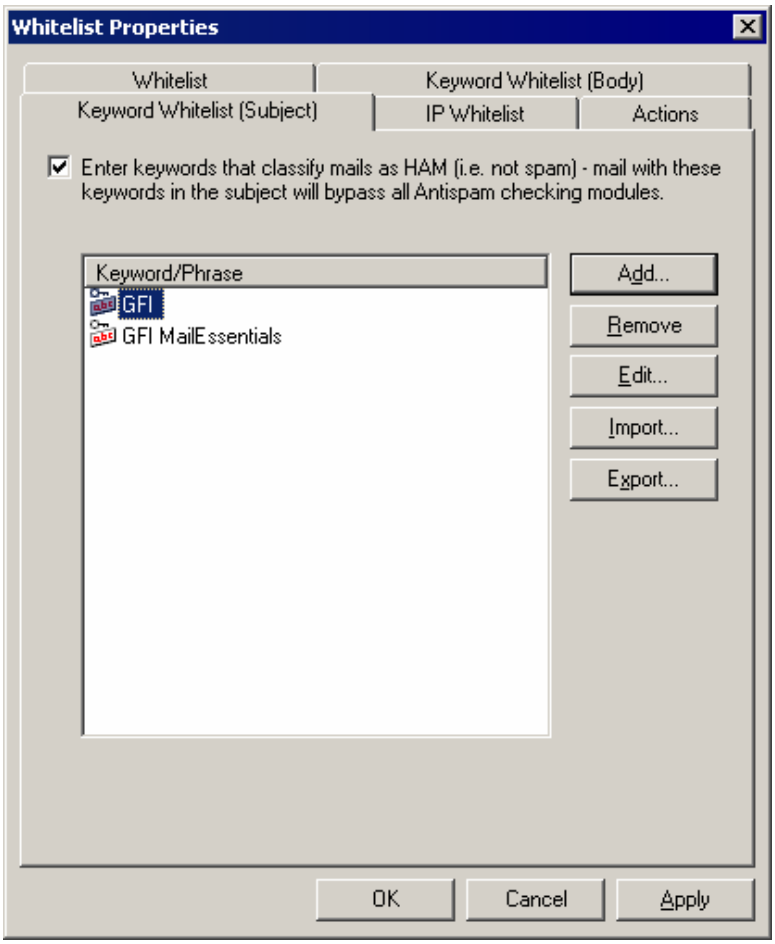


Screenshot 46 - Auto Whitelist options

The Auto Whitelist is made up of two components. One component scans incoming emails and matches their senders against the auto whitelist. If the sender is present in the list, the email will be passed on directly to the recipient's inbox without applying further spam checking. This feature is by default enabled, but you can still disable it by unmarking the **Check emails against Auto Whitelist** option in the whitelist properties page. The second component extracts the destination email addresses from outbound emails and automatically adds them to the autowhitelist.mdb for use by the first component. This feature is also enabled by default, but you can still disable it by unmarking the **Populate Auto Whitelist automatically** option in the whitelist properties page. You can view auto whitelist entries by selecting the **Show automatically entered** option from the **Filter** dropdown located at the top (right) of the page, near the **Email Address/Domain** display list.

We highly recommend using these features, since they allow GFI MailEssentials to achieve a very low rate of false positives.

Whitelisted keywords



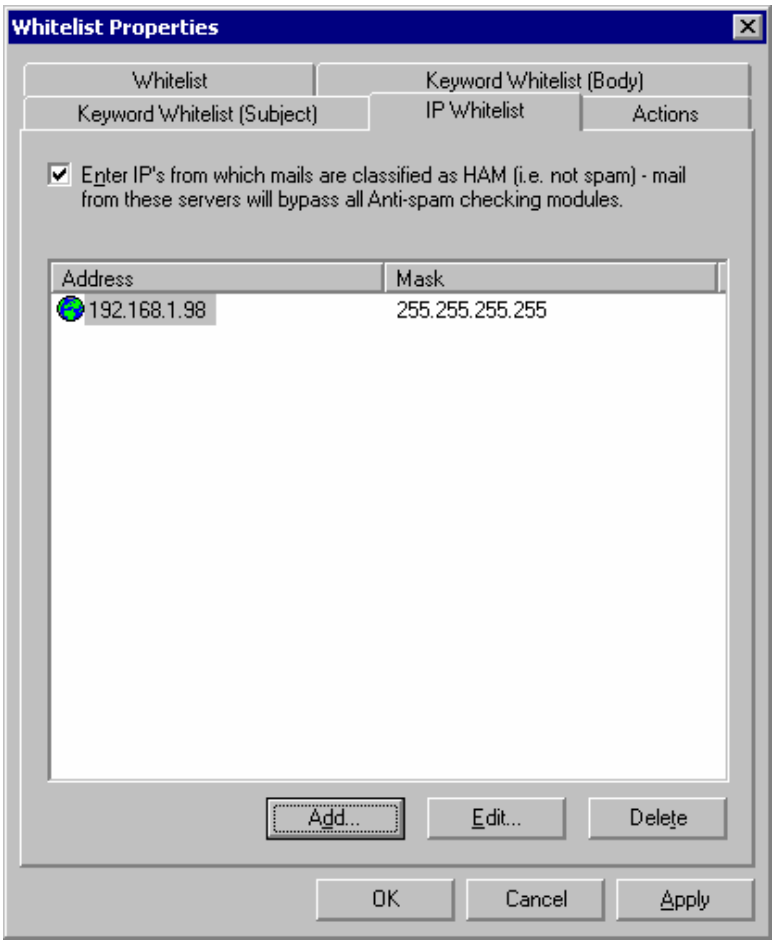
Screenshot 47 - Whitelisting keywords

GFI MailEssentials allows you to specify keywords, which cause the email to be flagged as ham (valid email). If a keyword configured in the keyword whitelist is found in an email, then GFI MailEssentials will automatically allow the email to skip all anti-spam filters and deliver the email directly in 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 whitelisted keywords for body and subject:

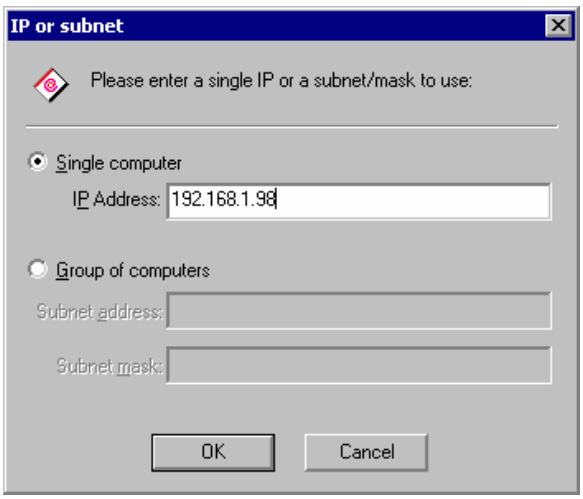
1. To specify whitelisted keywords in the message body, click on the **Keyword Whitelist (Body)** tab and select **Add**.
2. To specify whitelisted keywords in the subject, click on the **Keyword Whitelist (Subject)** tab and select **Add**.

IP Whitelist



Screenshot 48 – Whitelisting IPs

GFI MailEssentials allows you to bypass anti-spam checks on emails sent from servers whose IP address is specified in the IP Whitelist. Mails sent from listed servers are automatically classified as valid email and are directly delivered in the user's inbox. To enable this feature, click on the **IP Whitelist** tab in the **Whitelist Properties** dialog and check the **Enter IP's from which mails are classified as HAM…** option. In this page, you can also specify IPs to be added to the whitelist, as well as delete or make changes to the IP details already available.



Screenshot 49 - IP entry dialogue

To add IP's to the whitelist, click on the **Add** button. In the IP entry dialog box on display, you can specify the IP of a single computer as well as a range of IP's for a group of computers, by marking the **Group of computers** option and entering the relative subnet address and subnet mask.

Actions tab

After you have configured the Whitelist feature, click on the **Actions** tab to specify what you want to do with emails marked as Spam by the Whitelist. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

Directory harvesting

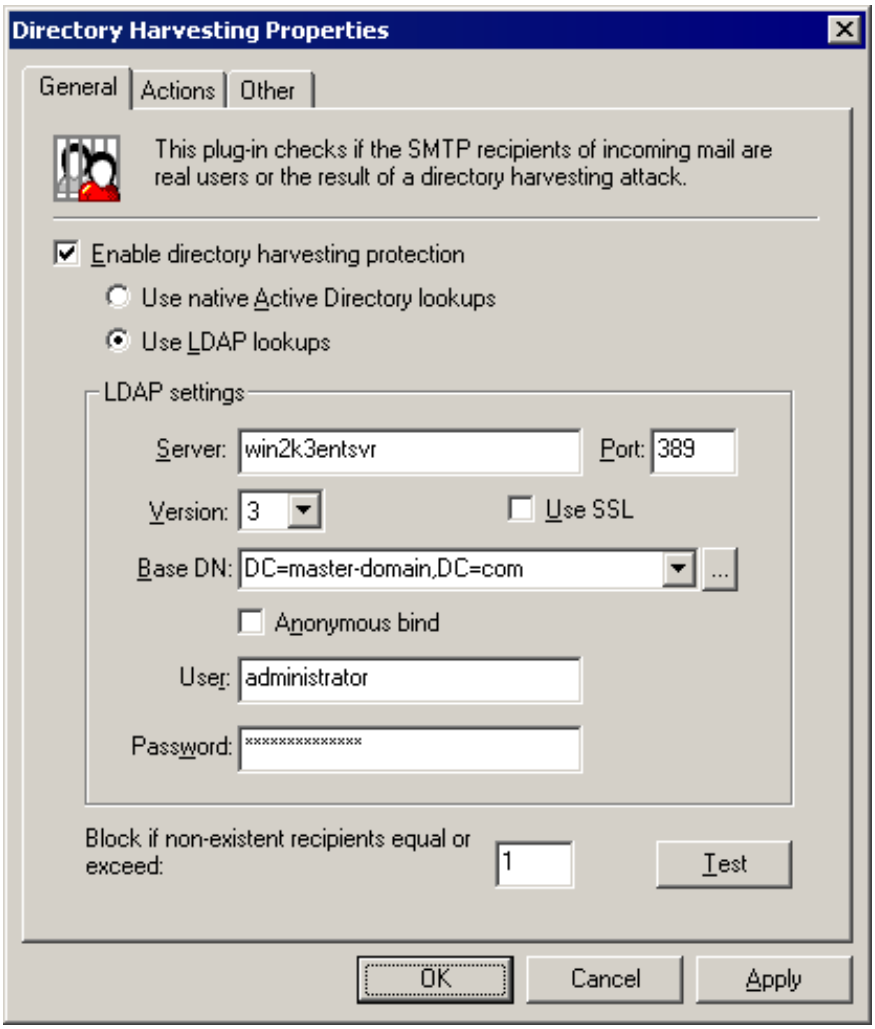
Directory harvesting attacks occur when a spammer uses known email addresses to generate other valid email addresses from corporate or ISP email servers. This technique allows the spammer to send emails to randomly generated email addresses. Some of these email addresses are real users in the organization however many of them are bogus addresses that flood the victim's email 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' Active Directory or email server. This feature makes use of the Active Directory or LDAP server to search for known users within the organization.

Configuration is done from the **Anti-Spam > Directory Harvesting** node. Right click on this node to bring up the **Directory Harvesting Properties** dialog. Mark the **Enable directory harvesting protection** option to enable this feature.

NOTE: To avoid false positives, specify a reasonable number in the **Block if non-existent recipients equal or exceed** edit box. One should keep in mind that sometimes users send legitimate emails with mistyped email addresses or to users no longer employed with the company.

If the amount of non-existent recipients is equal to or above the number specified, the action configured is triggered. If the total amount of recipients is less than the number specified, the action configured is triggered only if ALL the recipients do not exist, otherwise the email is not marked as SPAM.



Screenshot 50 - The directory harvesting feature

If GFI MailEssentials is installed in SMTP mode, fill in your LDAP server detail (i.e. server name, the rest can be left as default). If your LDAP server requires authentication, unmark the **Anonymous bind** option and enter the authentication details that will be used by this feature. You can test your LDAP configuration settings by clicking on the **Test** button or click on the **Apply** button to save the current settings.

If GFI MailEssentials is installed in Active Directory user mode, define the type of user lookup which best suits your company's setup i.e., enable the **Use native Active Directory lookups** option to search for user information in the Active Directory or enable the **Use LDAP lookups** option and specify your LDAP setting to search for user information on your LDAP server.

NOTE 1: If GFI MailEssentials is installed in Active Directory user mode on a DMZ, the Active Directory of a DMZ, normally, does not include all the network users (i.e. email recipients) and as a result, you will be getting many false positives. In such cases, it is recommended that you perform Directory Harvesting checks using LDAP lookups (i.e. enable the **Use LDAP lookups** option and specify your LDAP server details).

NOTE 2: When GFI MailEssentials is setup behind a firewall, the Directory Harvesting feature will not be able to connect directly to the

internal Active Directory because of the Firewall. In this case, although both options will be available, make use of LDAP lookups in order to enable the Directory Harvesting feature to connect to the internal Active Directory of your network (i.e., pass through your Firewall). Make sure to enable default port 389 on your Firewall

NOTE 3: When connecting to an Active Directory using LDAP (i.e. when GFI MailEssentials in installed on a DMZ or behind a Firewall), you have to specify the authentication credentials in this form: Domain\User (e.g. master-domain\administrator).

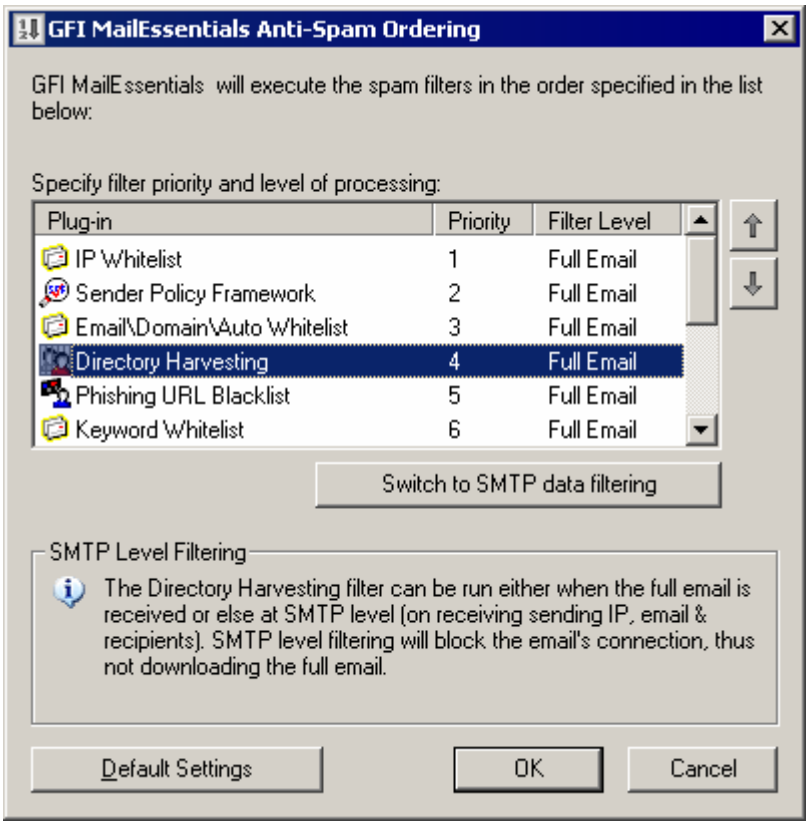
NOTE 4: In an Active Directory, normally the LDAP server is the Domain Controller.

Processing at Transport or SMTP protocol sink level

Directory harvesing can either run when the full email is received (Transport sink) or at SMTP level i.e. on receiving the sending IP, email and recipients (SMTP protocal sink). SMTP level filtering will block the email's connection and will therefore stop from downloading the full email whilst economizing on bandwith. When Directory Harversting runs at SMTP protocol sink level subsequent actions cannot be performed on the spam email given that emails are rejected.

To enable Directory Harvesting at SMTP protocal sink level:

1. Right click on **Anti-spam** > **Order module priorities**. This will open the Anti-Spam Ordering dialog.



Screenshot 51 – Anti-spam ordering dialog

2. In the plug-in list, select **Directory Harvesting**.
3. Click on **Swith to SMTP data filtering**.

NOTE: To switch back to full email filtering click on **Switch to full email filtering**.

Actions tab

After you have configured Directory Harvesting, click on **Actions** to specify what you want to do with emails marked as spam by this filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

NOTE: If Directory Harvesting is running at SMTP protocal sink level, only the Log Occurrence option will be available in the Actions tab.

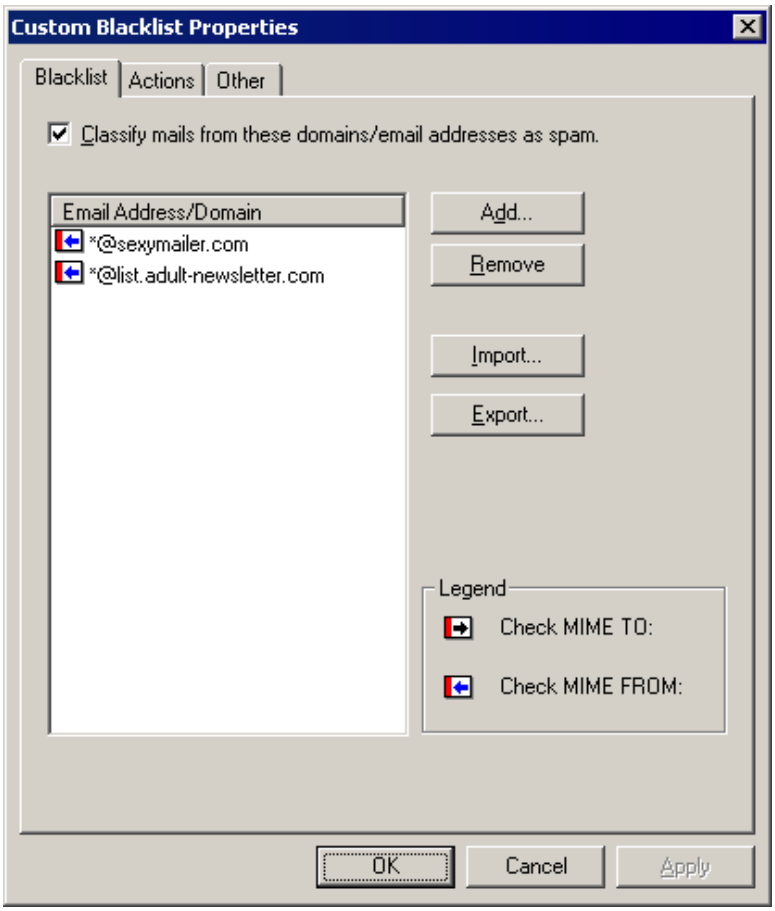
Other tab

Please refer to the 'Other options' section in this chapter.

Custom Blacklist

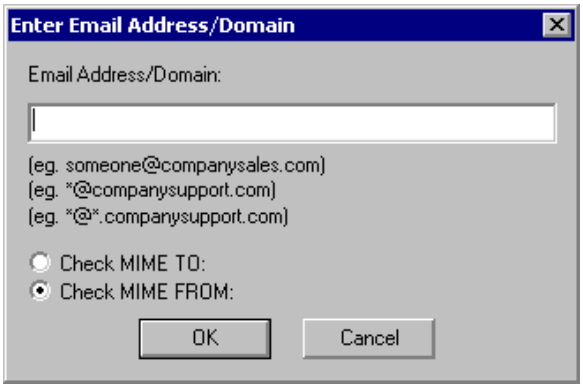
The Blacklist is a custom database of email addresses and domains from which you never wish to receive emails. i.e., emails sent from these email addresses or domains will always be marked as spam.

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



Screenshot 52 - The custom blacklist

To add a blacklisted domain or email address, click the **Add** button. In the **Enter Email Address/Domain** dialog box, specify the full email address or an entire domain, for example '*@spammer.com'. The '*' is a wildcard to include all email addresses from that domain.



Screenshot 53 - Adding a blacklisted email entry

You can also blacklist entire domain suffixes, for example *@*.jp. This will for example ensure that email 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 email sent to ex employees).

Actions tab

After having specified your custom blacklist, click on the **Actions tab** to specify what you want to do with emails marked as spam by this filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

Other tab

Please refer to the 'Other options' section in this chapter.

DNS blacklists (DNSBL)

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. 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.

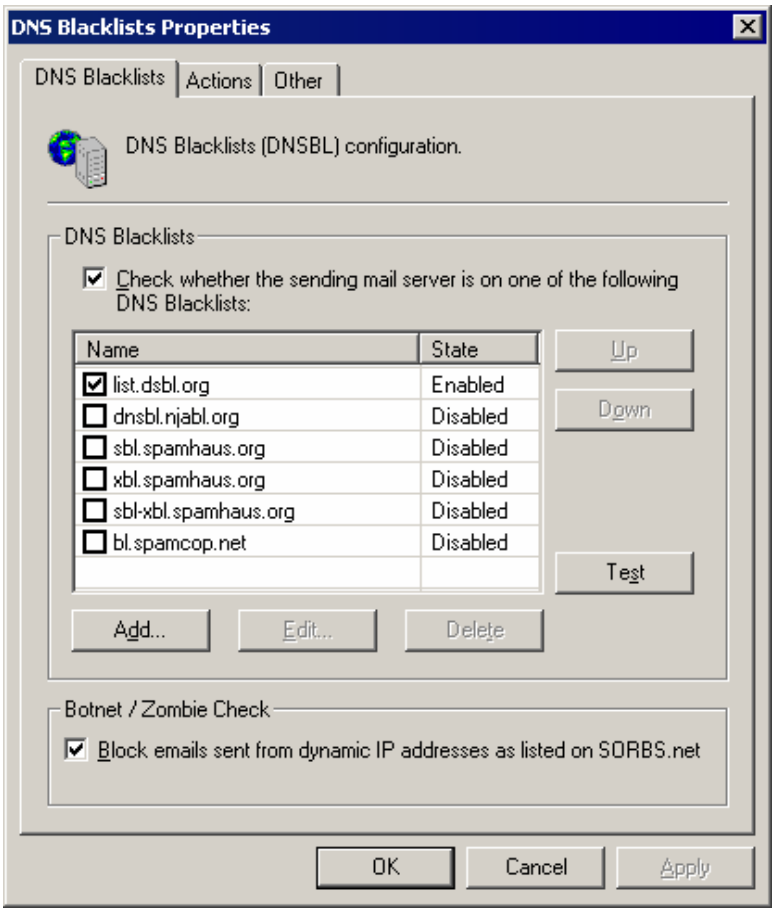
When an email is sent, it is passed through a number of SMTP servers until it reaches the final destination. The IP address of each of these SMTP servers is recorded in the email header. GFI MailEssentials will check all the public IPs found in the message header with the DNSBL database configured.

NOTE: This feature is enabled by default upon installation. For this feature to work, the DNS server needs to be properly configured. If the DNS server is not properly configured, a time out will occur and email

will be processed slowly. For more information, see the GFI Knowledge Base article KBID001770.

How it works

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



Screenshot 54 - The DNS Blacklist properties

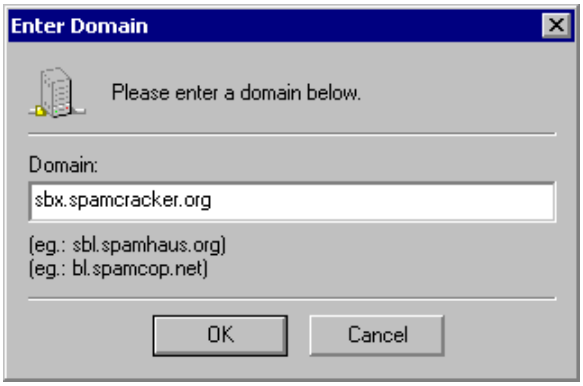
To enable the DNS blacklist:

1. Right click on the **Anti-Spam > DNS Blacklists** node and select **Properties**.
2. Check the **Check whether the sending mail server is on one of the following DNS Blacklists:** checkbox.
3. Select the appropriate DNS blacklists that you wish to check incoming email against.

NOTE 1: You can click on the **Test** button to check if the selected blacklists are available.

NOTE 2: Querying a DNS blacklist can be slow (depending on your connection), so email can be slowed down a little bit, especially if you query against multiple DNS blacklists.

You can also add more DNS Blacklists to the ones already listed by clicking on the **Add** button.



Screenshot 55 - Adding more DNS blacklists

Specify the domain containing the DNSBL (e.g. sbl.spahaus.org) in the dialog box on display and click on the **OK** button.

To change the order of reference for an enabled DNS blacklist, click on the relative blacklist and then click on the **Up** or **Down** buttons to move it up or down in the list according to the required priority. The DNSBL feature will reference enabled blacklist starting from the top.

To edit or delete a blacklist from GFI MailEssentials, click on the required blacklist and subsequently click on the **Edit** or **Delete** button accordingly.

Botnet / Zombie Check

Increasingly, spammers are distributing spyware and bots to infect home-user machines. The home-user machines then end up being used by the spammer as botnets or zombies, to send millions of spam emails.

Most home-user machines are assigned a dynamic IP from their Internet Service Provider (ISP).

When a home-user sends a legitimate email, the home-user machine (dynamic IP) connects to the ISP's mail server (fixed IP) which in turn then forwards the email to the destination.

On the other hand, when a zombie home-user machine (dynamic IP) wants to send a SPAM email, it connects directly to the victim SMTP server to send the SPAM email.

Thus, GFI MailEssentials can use these facts to detect spam email sent from a botnet/zombie machine by looking up the connection IP in the SORBS.net list of dynamically allocated IP address space.

To block emails sent from a dynamic IP address, which is a good indication that the email is spam being sent from a botnet/zombie machine, select the **Block emails sent from dynamic IP addresses as listed on SORBS.net** check box.

Botnet / Zombie Check on a perimeter (Gateway) SMTP server

The perimeter SMTP server is the machine that receives emails directly from the Internet. If you have installed GFI MailEssentials on a perimeter SMTP server, you do not need to configure the perimeter

[gateway] SMTP server options in the Perimeter SMTP Servers tab of the Anti-spam properties.

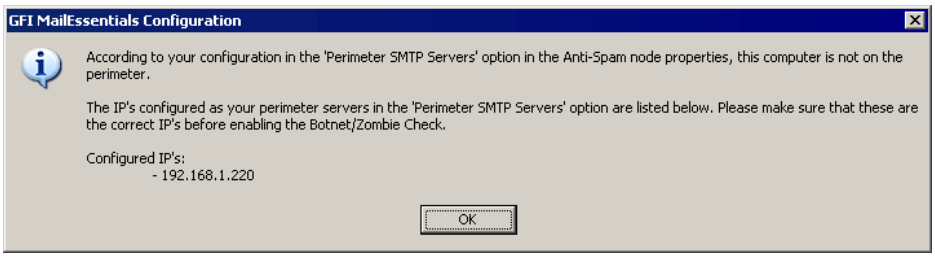
Botnet / Zombie Check on a non-perimeter (Gateway) SMTP server

If GFI MailEssentials is NOT installed on a perimeter SMTP server, configure the 'Perimeter SMTP Servers' option in the Anti-spam node properties. To setup this option, right click on the Anti-spam node, select **Properties** and click on the Perimeter SMTP Servers tab.

If you are not sure if you have installed GFI MailEssentials on your perimeter SMTP server, you can make use of the **Auto Discovery** button in the Perimeter SMTP setup option to perform a DNS MX lookup and automatically define the IP address of your perimeter SMTP server.

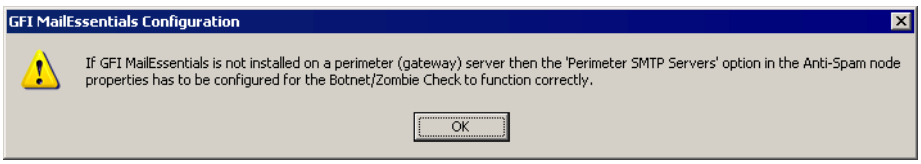
For further details on how to configure your perimeter SMTP server option, please refer to the 'Defining your Perimeter (Gateway) SMTP Server settings' section earlier in this chapter.

Click **Apply** to save the configuration. If you have already specified in GFI MailEssentials that this computer is not your perimeter SMTP server (refer to 'Defining your perimeter (gateway) SMTP server' section earlier in this chapter), a dialog box similar to the one shown below will pop up. This dialog box shows the perimeter SMTP server settings that you have configured in GFI MailEssentials (i.e. the IPs specified for your perimeter SMTP server).



Screenshot 56 – Current Perimeter SMTP Server setup

If GFI MailEssentials is installed on your perimeter SMTP server or if you have not yet specified that the mail server on which GFI MailEssentials is installed is not a perimeter SMTP server (refer to 'Defining your perimeter (gateway) SMTP server' section in this chapter), the dialog box shown below will pop up.



Screenshot 57 - Reminder: SPF must be installed on the perimeter SMTP server.

This dialog box will remind you that if this computer is not a perimeter server, configure the **Perimeter SMTP Servers** option in the Anti-spam node properties (right click on the **Anti-Spam** node and select **Properties**. Click on the **Perimeter SMTP Servers** tab). For further information on how to configure your perimeter SMTP server, please refer to the 'Defining your perimeter (gateway) SMTP Server' section earlier in this chapter.

Click **OK**.

Actions tab

After you have specified which DNS blacklists will be referenced click on the **Actions tab** to specify what you want to do with emails marked as spam by this filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

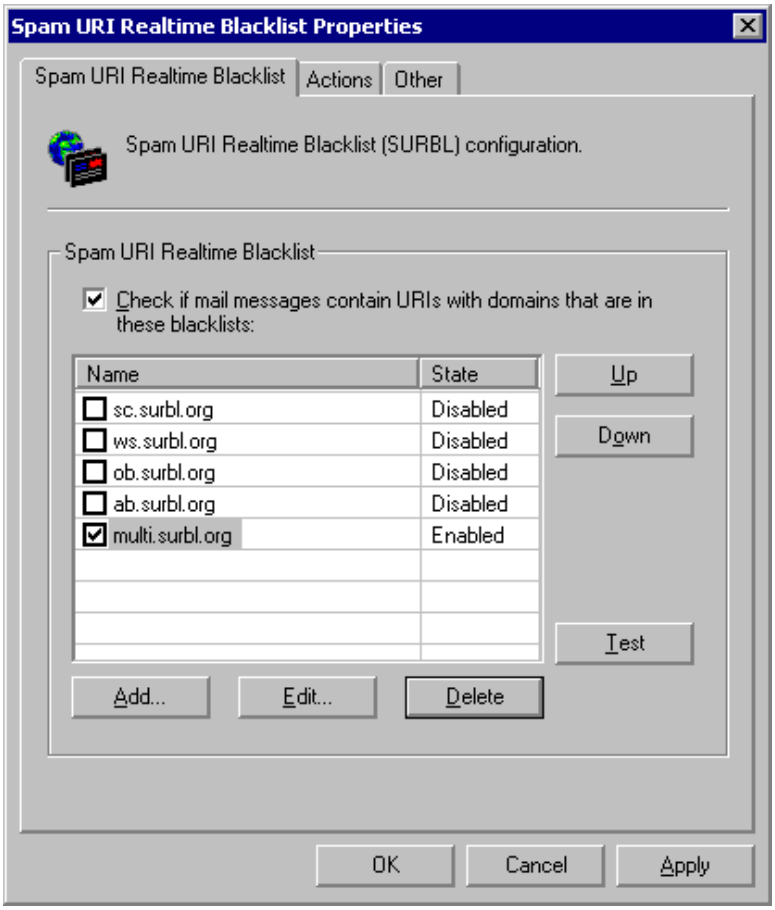
Other tab

Please refer to the 'Other options' section in this chapter.

Spam URI Realtime Blocklists (SURBL)

A Universal Resource Identifier (URI) is a standard means of addressing resources on the Web. Common URIs such as Uniform Resource Locators (URLs) and Uniform Resource Names (URNs) are used to identify the destination of hypertext links as well as the sources of images, information and other objects in a Web Page. URLs are most generally used in websites but can also be included as part of an email message body e.g. to attract new visitors to a website.

SURBLs differ from most other RBLs in that they are used to detect spam based on message body URIs. Unlike most other RBLs, SURBLs are not used to block spam senders. Instead, they allow you to block messages that have spam hosts (e.g. web servers, domains, websites) which are mentioned in message bodies.



Screenshot 58 – Spam URI Realtime Blacklist properties

To enable the SURBL check:

1. Right click on the **Anti-Spam > Spam URI Realtime Blocklists** node and select **Properties**.
2. In the default opening page, check the **Check if mail message contains URIs with domains that are in these blacklists:** checkbox to enable the SURBL check on inbound messages.
3. Mark on the available list, the blacklists that will be used as reference when checking messages using the SURBL function. (e.g., if you mark sc.surbl.org, the domains (URLs) in the message body will be compared to the blacklist present (sc.surbl.org). If the message contains URLs with domains that are on the selected blacklist, it will be marked as spam).
4. When ready, click on the **Apply** button.

NOTE 1: You can test the connection to the selected SURBL providers by clicking on the **Test** button.

NOTE 2: To add more SURBLs, click on the **Add** button, specify the full name of the domain (e.g. URIBL.com) containing the blacklist and click on the **OK** button to accept the new entry.

TIP: Multi.surbl.org combines the following lists in a unique list:

- sc.surbl.org
- ws.surbl.org
- phishing data source from mailsecurity.net.au
- phishing data source from fraud.rhs.mailpolice.com
- ob.surbl.org
- ab.surbl.org
- jp data source

This means that Multi.surbl.org includes all other SURBL Lists already listed in GFI MailEssentials, as well as two other sources. Hence, you can enable multi.surbl.org only for SURBL checks since this leads to the following advantages:

- You need to click only one blacklist.
- You would have two extra sources against which the URLs/domains are being checked.
- Multi.surbl.org has a unique list with no re-occurrence (i.e. a domain will appear only once in multi.surbl.org even if it is found in more than one list) thus it is faster than using the other four lists simultaneously (due to re-occurrence).

NOTE 1: When enabling multi.surbl.org it is recommended to disable all other SURBL lists from the configuration, otherwise the same scan will be performed more than once (in deferent lists) leading to lengthy email processing.

NOTE 2: The disadvantages of using multi.surbl.org only are:

- You might have a higher rate of false positives since more blacklists are present.
- The entries present in multi.surbl.org list have a higher (6 hours) TTL (Time to live) than those present in other lists (sc.surbl.org

entries TTL is 10 minutes). This means that you might encounter some false positives.

- If for some reason the multi.surbl.org list is not reachable, no checks will be performed.

TIP: If SURBL is giving many false positives, it is suggested that you try to disable multi.surbl.org and enable the other four SURBL lists. You can attempt reducing the amount of lists enabled in SURBL filter every time a high rate of false positives is present.

For more information on SURBL lists, please refer to http://www.surbl.org/lists.html.

Actions tab

After you have specified which SURBLs will be referenced, click on the **Actions tab** to specify what you want to do with emails marked as spam by this filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

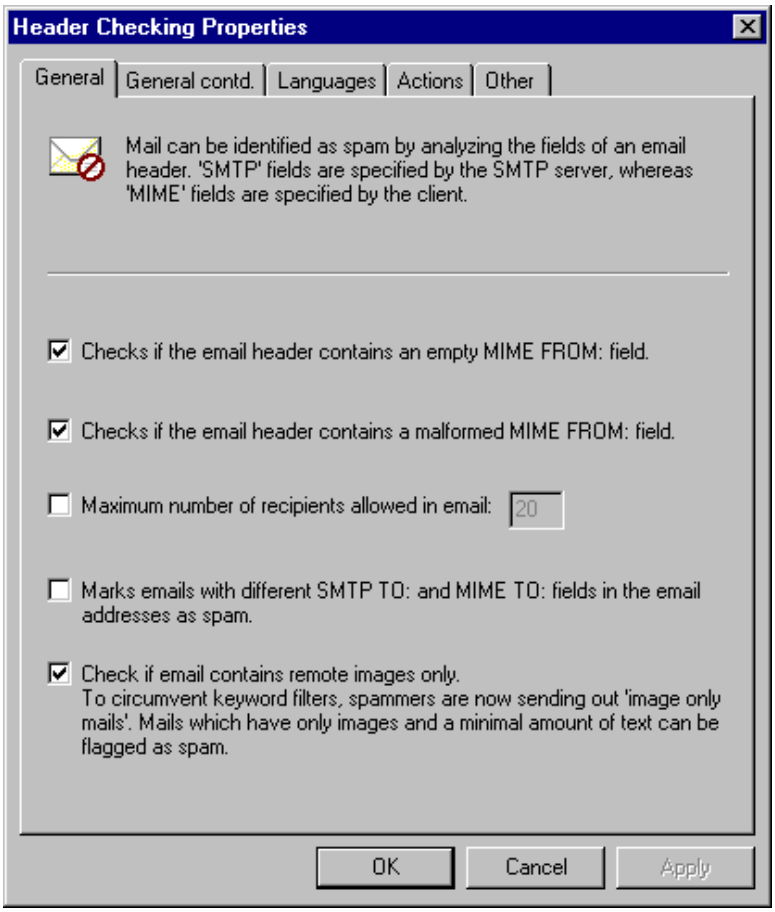
Other tab

Please refer to the 'Other options' section in this chapter.

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 email to MIME).

The configuration of anti-spam identification based on email headers is done from the **Anti-Spam > Header Checking** node. Right click on this node to bring up the **Header Checking Properties** dialog box.



Screenshot 59 - Header checking general tab

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 an empty MIME FROM field:** This feature checks if the sender has identified himself in the From: field. If this field is empty, it is an almost sure sign that the email is sent by a spammer.

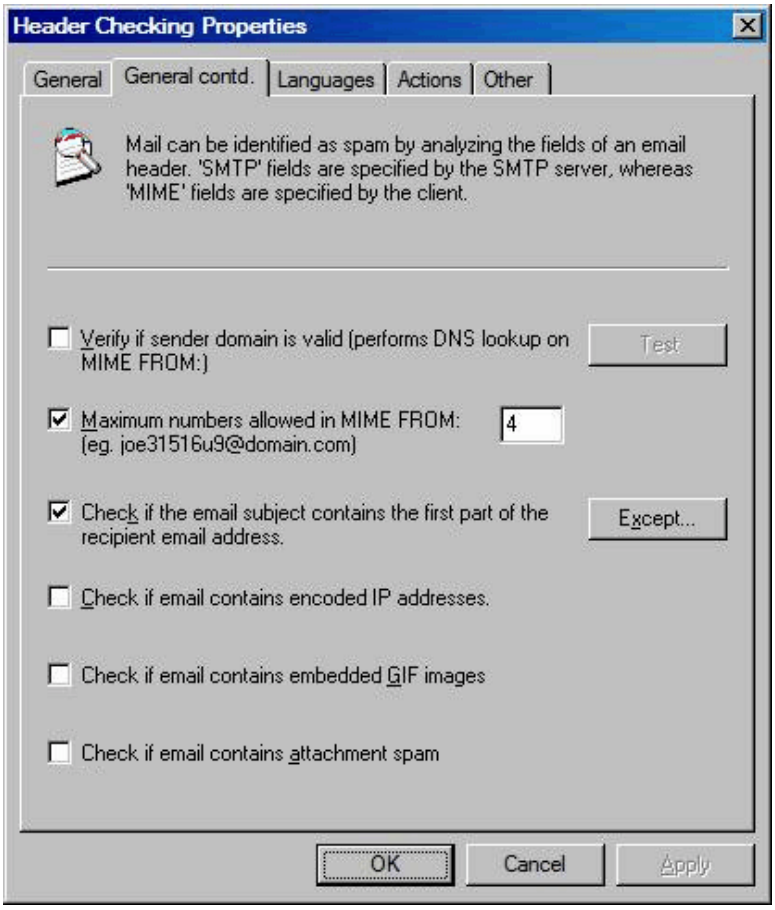
2. **Checks if the email header contains a malformed MIME FROM: field:** This feature checks if the MIME from field is a correct notation, i.e. it matches the RFC. Spammers often include a wrong or wrongly specified From address.

3. **Maximum number of recipients allowed in email:** This feature marks emails with large recipient lists as spam. Emails with large recipient lists tend to be joke lists, chain emails 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 captures a lot of spam, however some list servers do not include the MIME to: either. Therefore, to use this feature, whitelist the newsletter sender address if it gets marked as spam by this feature. This can be done from the

Whitelist node or by dragging the newsletter in the GFI Anti-spam public folders **I want this Discussion list** node.

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



Screenshot 60 - Header checking continued general tab

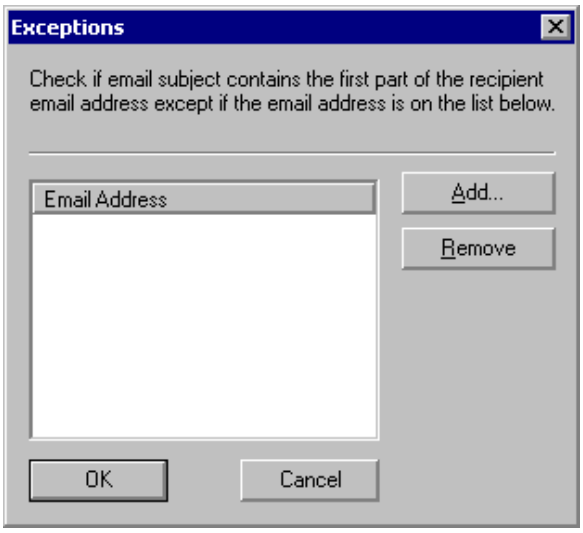
6. **Verify if sender domain is valid:** This feature will perform a DNS lookup on the domain specified in the MIME from field and verify if the domain is valid. If the domain is not valid, it is a sure sign of spam.

NOTE: This feature requires a properly configured DNS server, otherwise, a time out will occur and emails will be processed slowly. In addition, a lot of valid email will be tagged as spam. After enabling this feature, you can test your DNS server/services by clicking on the adjacent **Test** button. A dialog box will subsequently inform you if the DNS test has been successful or not.

7. **Maximum numbers allowed in 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 the email subject contains the first part of the recipient email address:** To 'personalize' a spam email, 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 email to sales', would be marked as spam. To avoid this, you can specify email addresses for which this check should not be done, by clicking on the **Except…** button.



Screenshot 61 - Excluding an email address

9. **Check if email contains encoded IP addresses:** Checks the message header and body for URLs which have a hex/octal encoded IP (http://0072389472/hello.com) or which have a username/password combination in it (e.g. www.citibank.com@scammer.com).

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

http://12312

www.microsoft.com:hello%01@123123

10. **Check if email contains embedded GIF images:** Checks if the email contains one or more embedded GIF images. Spammers are increasingly using embedded GIF images to circumvent spam filters. Since some legitimate emails do contain embedded GIF images, for example, a company or product logo in the email signature, this option is prone to false positives.

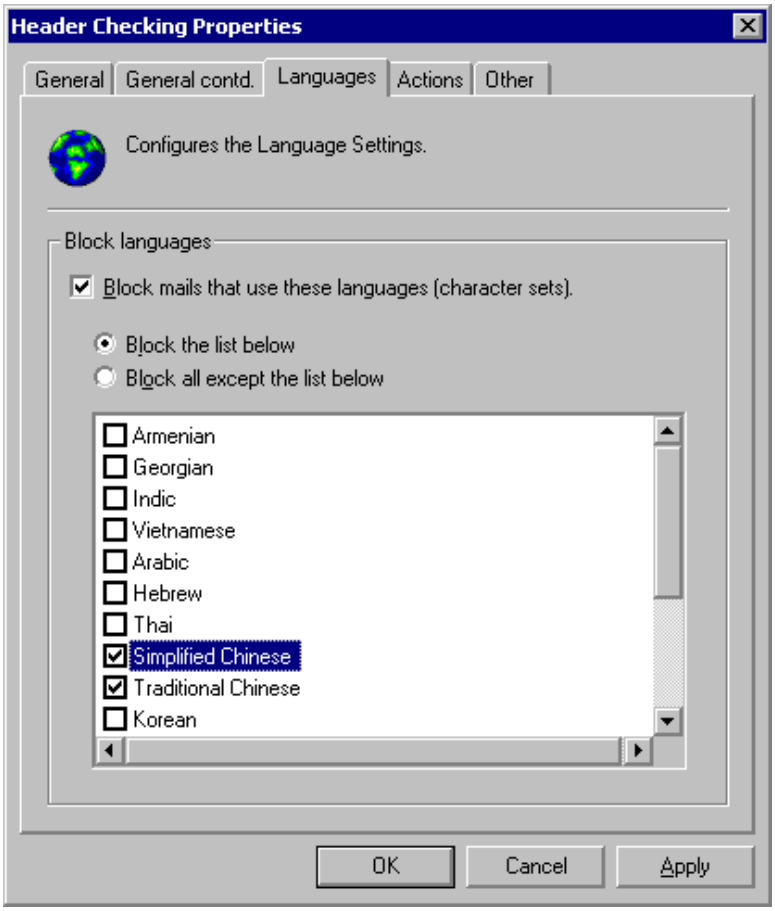
11. **Check if email contains attachment spam:** Checks the email attachments for properties that are common to attachments sent in spam email. Spammers are choosing to send attachment spam since all the other methods used, such as embedded images, are these days very well known and can be blocked easily. This new check will help you keep up with the latest techniques used by spammers and thus further protect your network from spam email.

Language detection

The languages tab in the Header Checking Properties dialog contains the language detection options. Many spam emails are not even in your language, meaning that you can greatly reduce spam simply be blocking email written in say Chinese or Vietnamese. Using the **Languages** tab you can block email using certain character sets.

NOTE: GFI MailEssentials cannot distinguish between Italian and French for example because they use the same character set. GFI

MailEssentials can only detect languages written in different character sets.



Screenshot 62 - Language detection

Actions tab

After you have configured the header checking filter, click on the **Actions tab** to specify what you want to do with emails marked as Spam by this filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

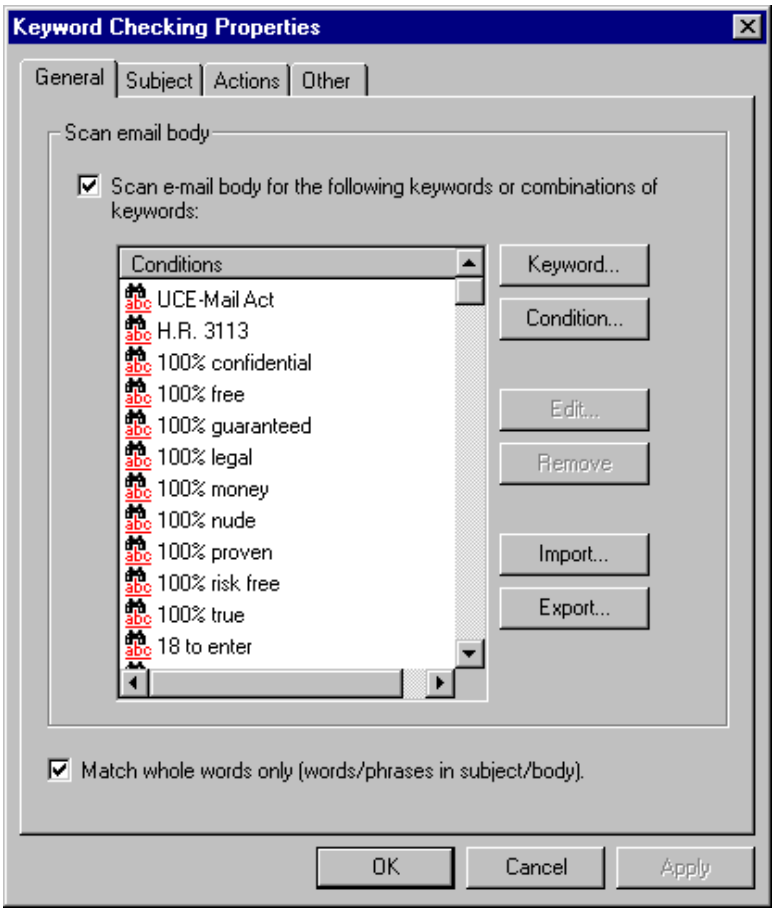
Other tab

Please refer to the 'Other options' section in this chapter.

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** dialog box.

1. Check the **Scan email body for the following keywords or combinations of keywords:** checkbox. To enter keywords combined with logical operators click the **Condition…** button. To enter single words or phrases without logical operators, click the **Keyword…** button.

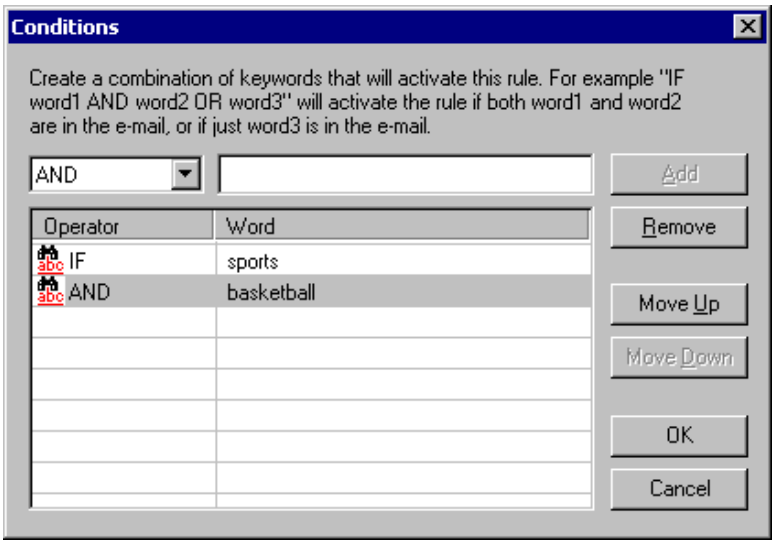


Screenshot 63 – Anti-spam keyword checking properties

Match whole words only: Enabling this option allows you to ensure that GFI MailEssentials will only block emails 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'.

Adding conditions

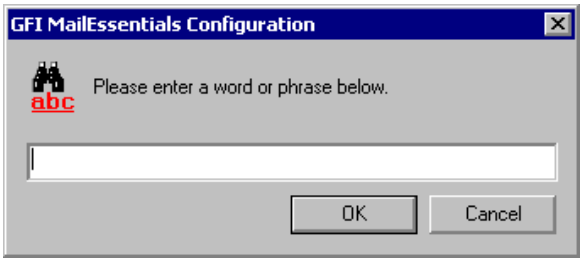
Conditions are combinations of keywords using the operands IF, AND, AND NOT, OR, OR NOT. Using conditions, you can specify combinations of words that must appear in the email. For example a condition 'If Word1 AND Word2' will check for Word1 and Word2. Both words would have to be present in the email to activate the rule. To add a condition, click the **Condition…** button.



Screenshot 64 - Adding a condition

Adding keywords

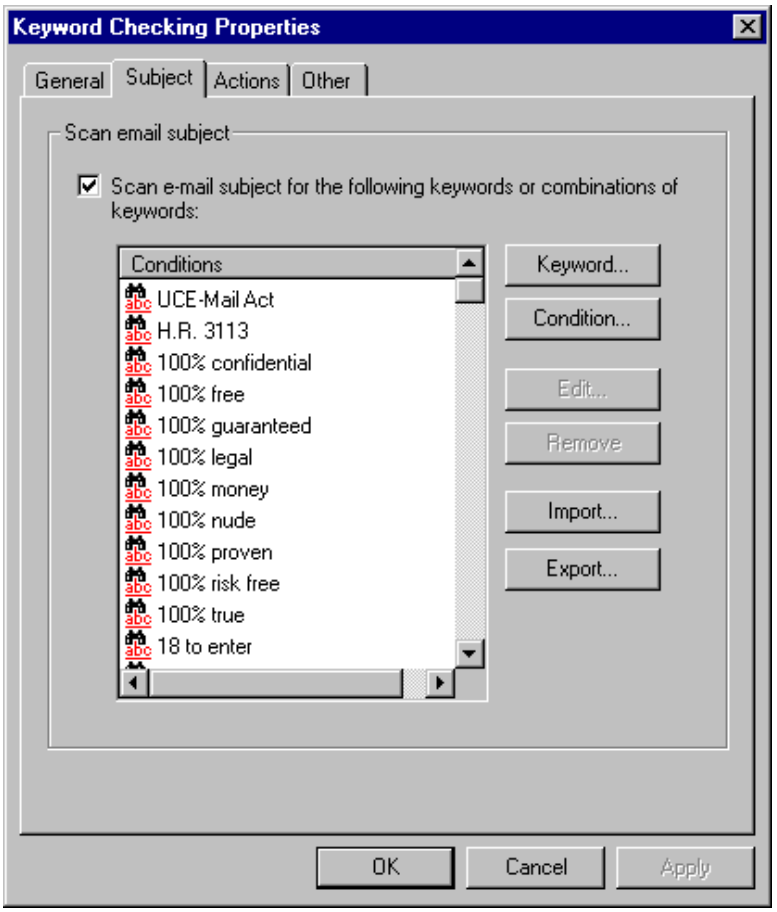
If you only wish to check for single words or phrases, you do not need to create a condition. In this case you can just add a keyword. Click the **Keyword…** button to do this. If you enter multiple words, then GFI MailEssentials will search for that phrase. For example, if you enter 'Basketball sports',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



Screenshot 65 - Adding a keyword or phrase

Subject

2. To scan for words in the subject, access the **Subject** tab and check the **Scan email subject for the following keywords or combinations of keywords** checkbox. Now you can specify the words that you wish to check for in the subject of the message. To enter keywords combined with logical operators click the **Condition…** button. To enter single words or phrases without logical operators, click the **Keyword…** button.



Screenshot 66 - Looking for keywords in the subject tab

Actions tab

After you have configured the keyword checking filter, click on the **Actions tab** to specify what you want to do with emails marked as Spam by this filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

Other tab

Please refer to the 'Other options' section in this chapter.

New Senders check

GFI MailEssentials can automatically identify emails which have been sent from senders to whom you have never sent emails before. Such senders are identified by referencing the data collected in the Whitelists.

NOTE: ONLY emails in which no spam was detected and whose senders are not present in any Whitelist are delivered in the New Senders folder.

Since such emails could be sent from legitimate users as well as undetected spam, GFI MailEssentials collects them into a dedicated folder. This feature conveniently separates such emails from the rest of the filtered messages in your inbox, in order to make them easily

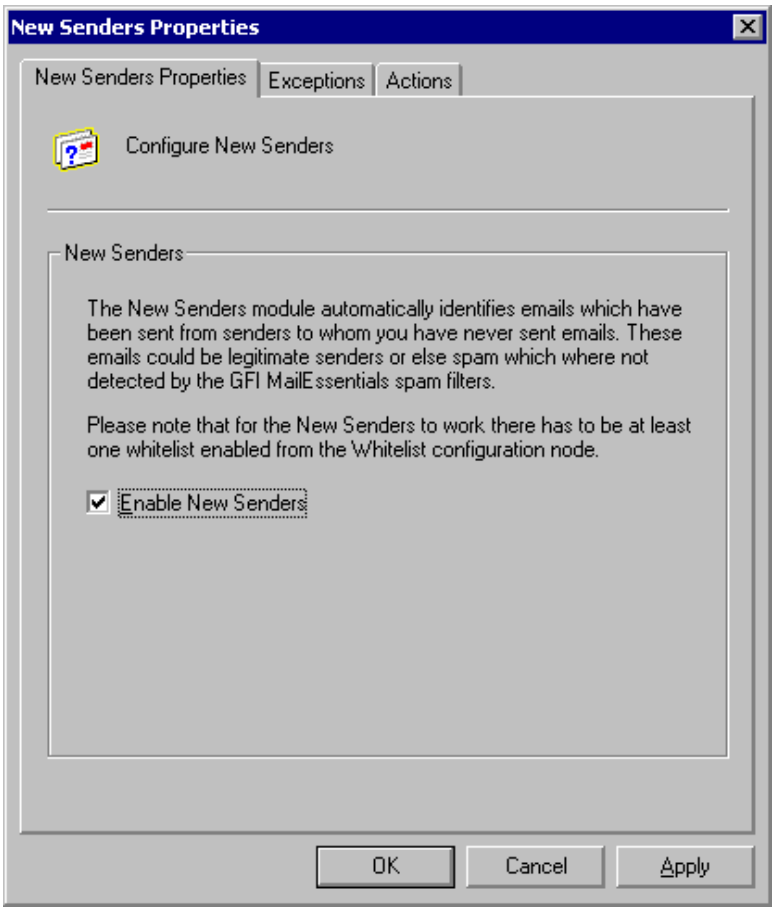
identifiable. Subsequently, you can review such emails and add any undetected spam present in this folder to the custom blacklist.

NOTE: You must enable at least one of the available Whitelists in order to be able to use the New Senders function. In the absence of the Whitelist functions (should no spam be detected by the other filters) received messages will be delivered to the recipient's inbox. i.e. ONLY emails in which no spam was detected and whose senders are not present in the Whitelist are delivered in the New Senders folder.

To activate the new senders filter:

1. Right click on the **Anti-Spam > New Senders** node and select **Properties**.

2. In the **New Senders Properties** tab, check the **Enable New Senders** checkbox to enable the check for new senders on all inbound messages and click on the **Apply** button.



Screenshot 67 - New Senders properties

Exceptions tab

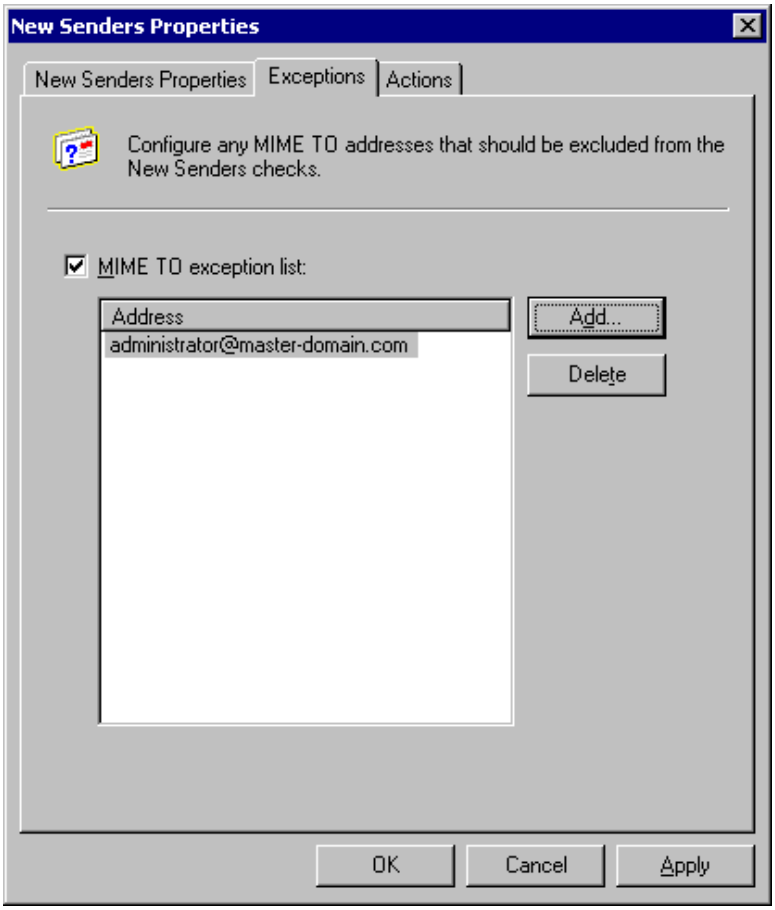
In the **New Senders Properties** dialog you can specify the address (MIME TO) of any local recipients whose emails should be excluded from the New Senders check.

To setup your exception list:

1. Click on the **Exceptions** tab and check the **MIME TO exception list:** checkbox.

2. Click on the **Add…** button and specify the email address of the sender, for example administrator@master-domain.com. Repeat the same procedure for each address that needs to be added, and then click on the **Apply** button to save these entries.

TIP: If you want to temporarily disable your exception list, there is no need to delete all address entries made, but you only need to uncheck the **MIME TO exception list:** checkbox.



Screenshot 68 - New Senders Exception setup

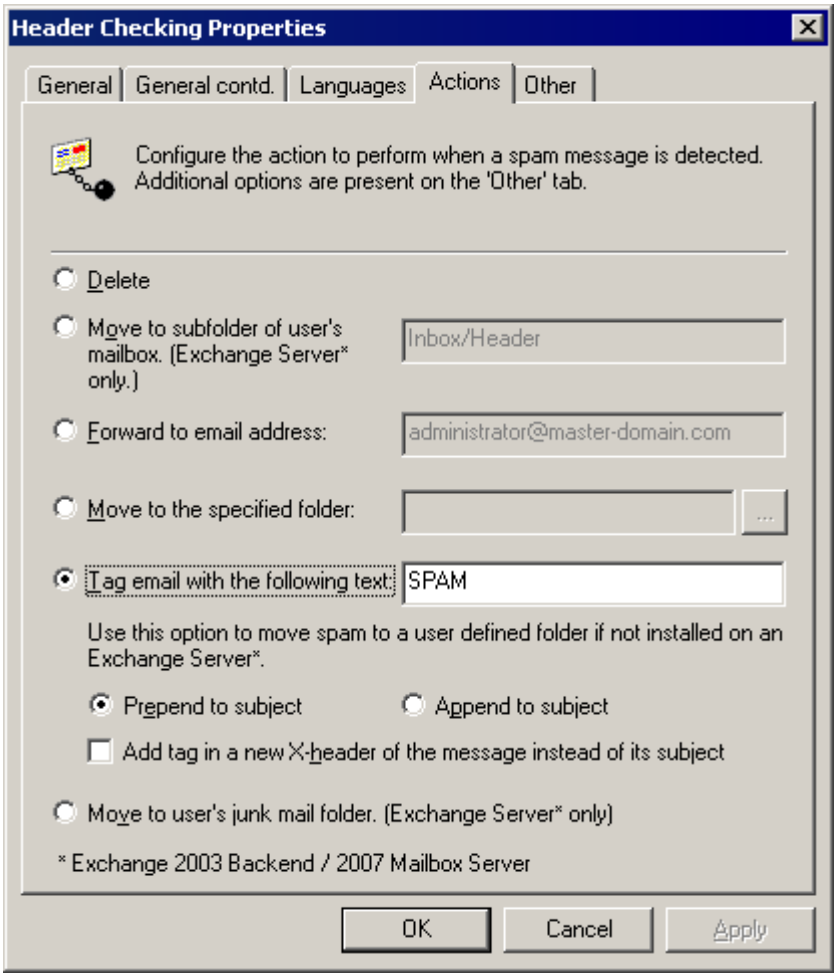
Actions tab

After you have enabled the New Senders feature, click on the **Actions tab** to specify what you want to do with emails marked as spam by this filter. For more information on possible actions, please refer to the 'Actions – what to do with spam email' section in this chapter.

Actions – what to do with spam email

In GFI MailEssentials, actions define what should be done with emails marked as spam. You can configure different actions for each of the available spam filter nodes. This feature conveniently enables you to use separate folders for storing spam email detected by each filter. This would help you to immediately identify why the email was marked as spam as well as makes it easier to perform operations on emails blocked by a particular filter. For example, you might want to delete emails marked by the blacklist spam filter, but do something else with emails marked as spam by the keyword checking filter.

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



Screenshot 69 - Configuring the action that should be taken

Select one of the following options to specify what you want to do with email marked as spam:

- **Delete** – This option will cause spam email to be deleted.
- **Move to subfolder of user's mailbox** – This option will cause spam email 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 store all email marked as spam by this anti-spam filter to this folder. This way, users can periodically check email marked as spam, and identify email that might have been wrongly marked. If you enter **inbox/junk mail**, then the folder will be created under the inbox folder. If you do not, it will be created at the same nesting level of the inbox folder. 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: This option requires that GFI MailEssentials is installed on the Microsoft Exchange Server machine, in Active Directory mode, and that you are running Microsoft Exchange Server 2000/2003 or Microsoft Exchange Server 2007 with the Mailbox Server Role installed. However if you are running Microsoft Exchange 5.5 or are not running GFI MailEssentials on the Microsoft Exchange

Server machine, you can still achieve the same behavior with the Tag email feature in conjunction with the Rules manager. For further information on the Rules manager refer to the 'Installing the rule manager (sorts spam to junk folder)' section of the 'Installing GFI MailEssentials' chapter.

- **Forward to email address** – This option will instruct GFI MailEssentials to send email detected as spam by the particular anti-spam filter you are configuring to the email address specified. For example, you can specify the email address of a public folder. The subject of the email will be in the format [recipient] [subject]. This way a person can be assigned to periodically check email marked as spam, and identify email that might have been wrongly marked as spam. This feature can also be used to further improve the spam rules.
- **Move to the specified folder** – This option will instruct GFI MailEssentials to save email detected as spam by the particular anti-spam filter you are configuring to the path specified, for example, 'C:\GFI MailEssentials\DetectedSpam'. The file name will have the following format: **`[Sender_recipient_subject_number_.eml]`**; this allows you to quickly sort spam based on sender.

  (e.g. C:\My Spam\ jim@gfi.com_bob@gfi.com_MailOffers_1_.eml)
- **Tag Email with the following text** - This option allows you to tag a spam email but does not block or delete it. You can also specify where to insert this tag by selecting:
  - **Prepend to subject** – to insert the specified tag at the start (i.e. as a prefix) of the email subject text. For example, '[SPAM]Free Web Mail)'.
  - **Append to subject** – to insert the specified tag at the end (i.e. as a suffix) of the email subject text. For example, 'Free Web Mail[SPAM])'.
  - **Add tag in a new X-header…** - to add the specified tag as a new X-header to the email. In this case, the X-Header will have the following format :

    `X-GFIME-SPAM: [TAG TEXT]`

    `X-GFIME-SPAM-REASON: [REASON]`

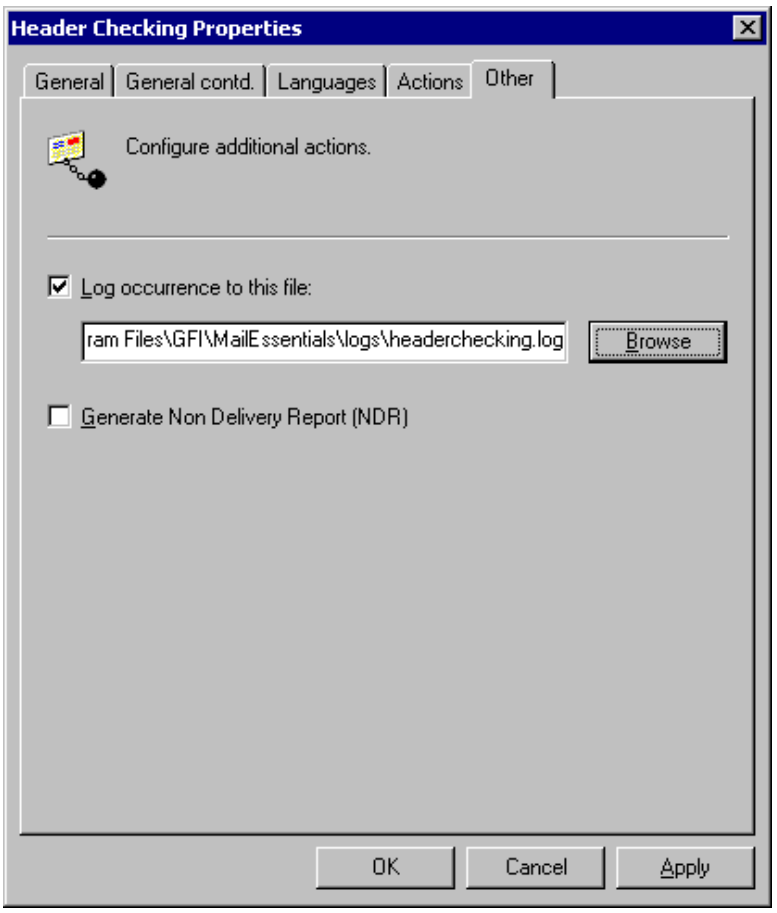
    E.g.

    ```
    X-GFIME-SPAM: [This is SPAM]
    X-GFIME-SPAM-REASON: [DNSBL Check failed – Sent from Blacklisted Domain]
    ```

  The tag email option can be used in conjunction with the Rules manager application, which allows you to easily setup sorting rules for all mailboxes on your Microsoft Exchange Server machine. All email tagged as spam will be subsequently sorted into the user's junk mail folder. (Location and name of folder is customizable)
- **Move to user's junk mail folder** - If you have Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007 with the Mailbox Server Role installed, GFI MailEssentials can tag spam in such a way that Microsoft Outlook will sort the email 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 email is then automatically sorted to a different folder depending on which filter identified it as spam, greatly easing the spam reviewing process.

Other options



Screenshot 70 - The other actions tab

From the **Other** tab, you can specify a number of optional actions:

- The **Log occurrence to this file** feature allows you to log the spam email 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 as spam. This feature can be convenient to use during the initial training phase.

NOTE: If you wish you can customize the NDR. For information on how to achieve this, refer to the 'Configuring a fake Non Delivery Report (NDR)' section in the 'Miscellaneous options' chapter.

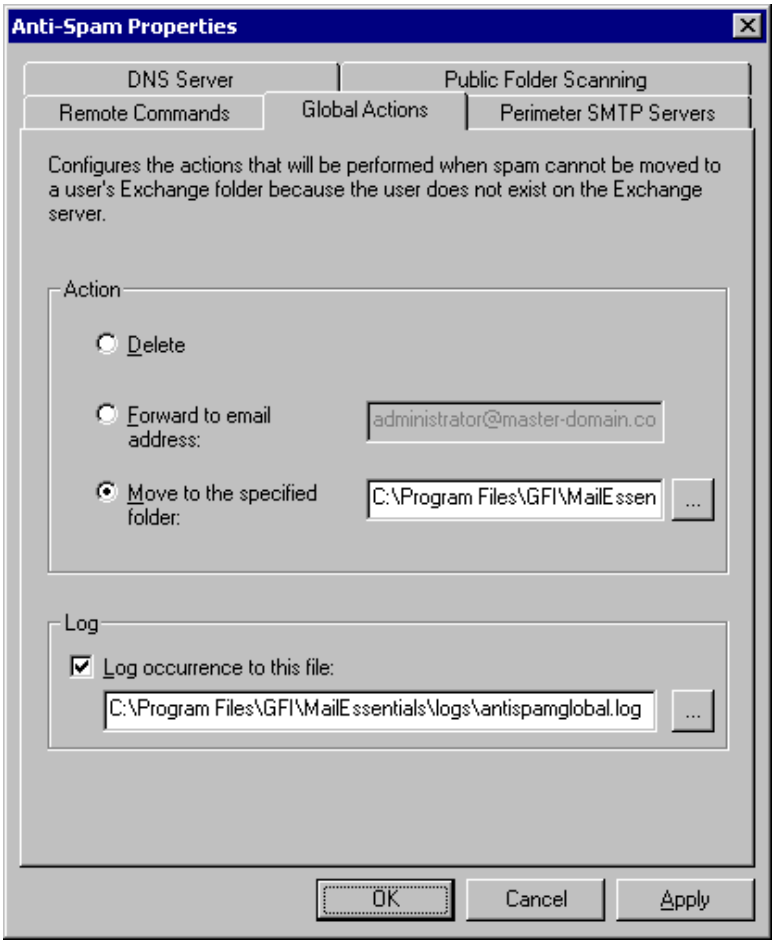
Anti-spam global actions

This section applies only to users who have installed GFI MailEssentials **on the Microsoft Exchange Server 2000/2003/2007 machine** and who are using the **Forward to user's spam folder function**. If you have not installed on the Microsoft Exchange Server

2000/2003/2007 machine, the anti-spam global actions tab will not appear.

A lot of spam is sent to email addresses that no longer exist on your server. Therefore, once you start sorting email marked as spam to user's junk mail folders, you will end up with a relatively large percentage of email that cannot be sorted into someone's mailbox. Generally, you will simply want to delete these emails. However for troubleshooting or evaluation purposes, you might want to move these emails 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** dialog. To configure the global actions:

1. Right click on the **Anti-Spam** node and select **Properties**.



Screenshot 71 - Global actions

2. Click on the **Global Actions** tab and select whether to:

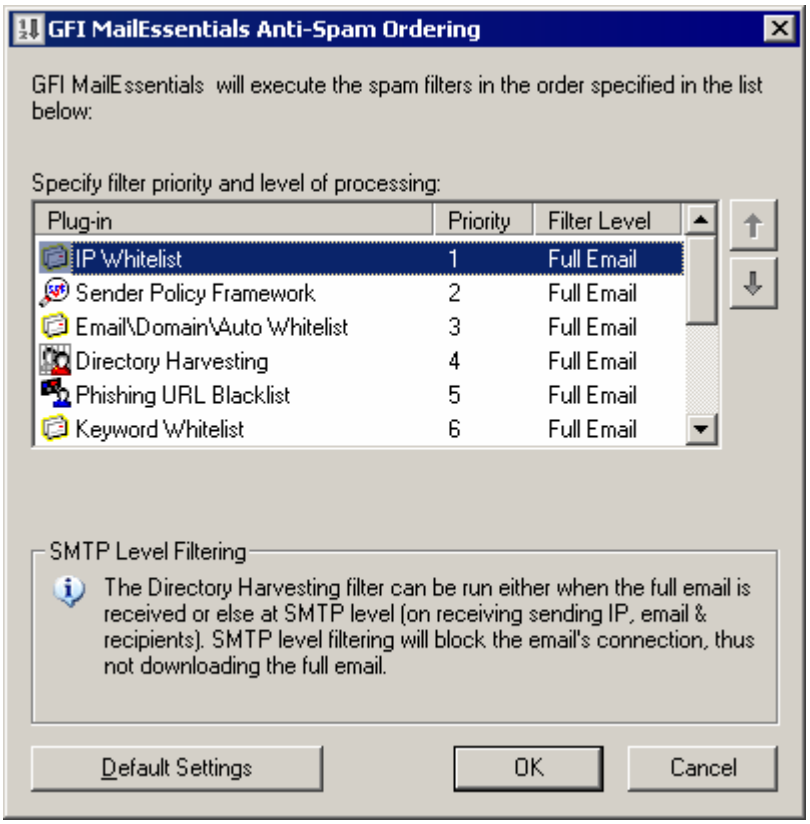
- Delete the email
- Forward it to an email address
- Move it to a specified folder.

Additionally, by checking the **Log occurrence to this file** checkbox**,** you can log the spam email occurrence to a log file of your choice.

Sorting anti-spam filters by priority

In GFI MailEssentials, you can define the order in which your anti-spam checks will be applied to your inbound messages (i.e. you can define the priority of each anti-spam filter).

NOTE: You can sort the priority of all available filters except for the New Senders filter, which is always automatically set to the lowest priority. This is because this filter depends on the results of the Whitelist checks and the other anti-spam filters.



Screenshot 72 – Assigning filter Priorities

To define the order of the anti-spam filters:

1. Right click on the **Anti-Spam** node and select **Order module Priorities**.

2. Click on the required filter and click on the (up) button on the right of the list to assign a higher priority to the selected filter (i.e. move the filter up in the list) or click on the (down) button on the right of the list to assign a lower priority to the selected filter (i.e. move the filter down in the list).

NOTE: Clicking on the **Default Settings** button will setup the filter priorities to the order recommended by GFI.

3. When you have finished sorting your anti-spam filter priorities, click on the **OK** button. Changes will take effect immediately.

Spam management from the user's point of view

Introduction

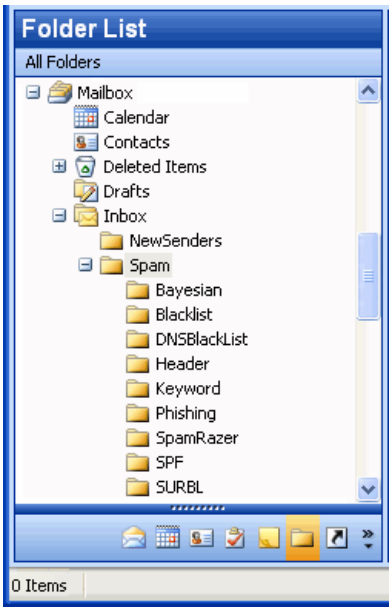
This chapter describes how users can manage their spam. GFI MailEssentials has been designed to minimize spam management by the user. It is pointless to flag email as spam if the user has to spend a lot of time managing his spam. That said, there are some valid actions that a user can perform to increase the effectiveness of GFI MailEssentials. These include:

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

In addition, users will tend to blame the anti-spam package for not receiving certain emails. 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 email

It is recommended that you configure GFI MailEssentials to forward email marked as spam by the different anti-spam filters to separate subfolders in the user's mailbox.



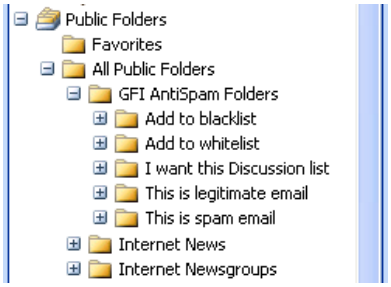
Screenshot 73 - Spam is sorted to a subfolder

This makes it easier for you to carry out periodical email checks and identify any emails that might have been wrongly marked as spam. Using separate subfolders for each filter allows the user to immediately understand which filter has flagged the email as spam.

For more information on how to configure and setup spam filters, please refer to the 'Configuring anti-spam' chapter.

Adding senders to the whitelist

To add a specific email address to the company whitelist, you need to drag and drop the email to the **Add to whitelist** Public folder, located under the **GFI AntiSpam Folders** public folders.



Screenshot 74 - Whitelisting an email

NOTE: To automatically create the **GFI AntiSpam Folders** public folders on your Microsoft Exchange Server, refer to the "Configuring Public folder scanning" further on in this chapter.

GFI MailEssentials will retrieve the email, and add the MIME FROM email address (whole email not domain) to the whitelist.

Use this same procedure for newsletters that you wish to receive, simply drop them in the **Add to whitelist** public folder.

NOTE: When dragging and dropping email, by default Microsoft Outlook will move the email. To retain a copy of the email, hold down the CTRL key, which copies the email rather then moves it.

Adding senders to the blacklist

To add the sender of a spam email to the company blacklist, drag and drop the email to the Public folder **Add to blacklist**, located under the **GFI AntiSpam Folders** public folder.

NOTE: To automatically create the **GFI AntiSpam Folders** public folders on your Microsoft Exchange Server, refer to the "Configuring Public folder scanning" further on in this chapter.

GFI MailEssentials will retrieve the email, and add the MIME FROM email address (whole email not domain) to the blacklist

Adding discussion lists to the whitelist

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 whitelist the email addresses of these valid list mailers.

To add the discussion list to the company whitelist, drag and drop the discussion list to the Public folder **I want this discussion list**, located under the **GFI AntiSpam Folders** public folder. GFI MailEssentials will retrieve the email, and add MIME TO, CC and BCC (whole email not domain) to the whitelist.

NOTE: To automatically create the **GFI AntiSpam Folders** public folders on your Microsoft Exchange Server, refer to the "Configuring Public folder scanning" further on in this chapter.

Adding spam to the spam database

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

NOTE: To automatically create the **GFI AntiSpam Folders** public folders on your Microsoft Exchange Server, refer to the "Configuring Public folder scanning" further on in this chapter.

Adding ham to the ham database

If, whilst reviewing a spam email a user finds a valid email, the user should add the email to the ham database. To do this, the user simply needs to drag and drop the email to the public folder **This is legitimate email**. Doing this will prompt GFI MailEssentials to retrieve the email and add it to the ham database, thus further tuning the Bayesian filter and avoiding it being flagged as spam in the future.

NOTE: To automatically create the **GFI AntiSpam Folders** public folders on your Microsoft Exchange Server, refer to the "Configuring Public folder scanning" further on in this chapter.

Securing access to the public folders

If you do not want to allow all users in your company to add email to the **GFI AntiSpam Folders**, simply limit access to the public folder from the Microsoft Exchange System Manager.

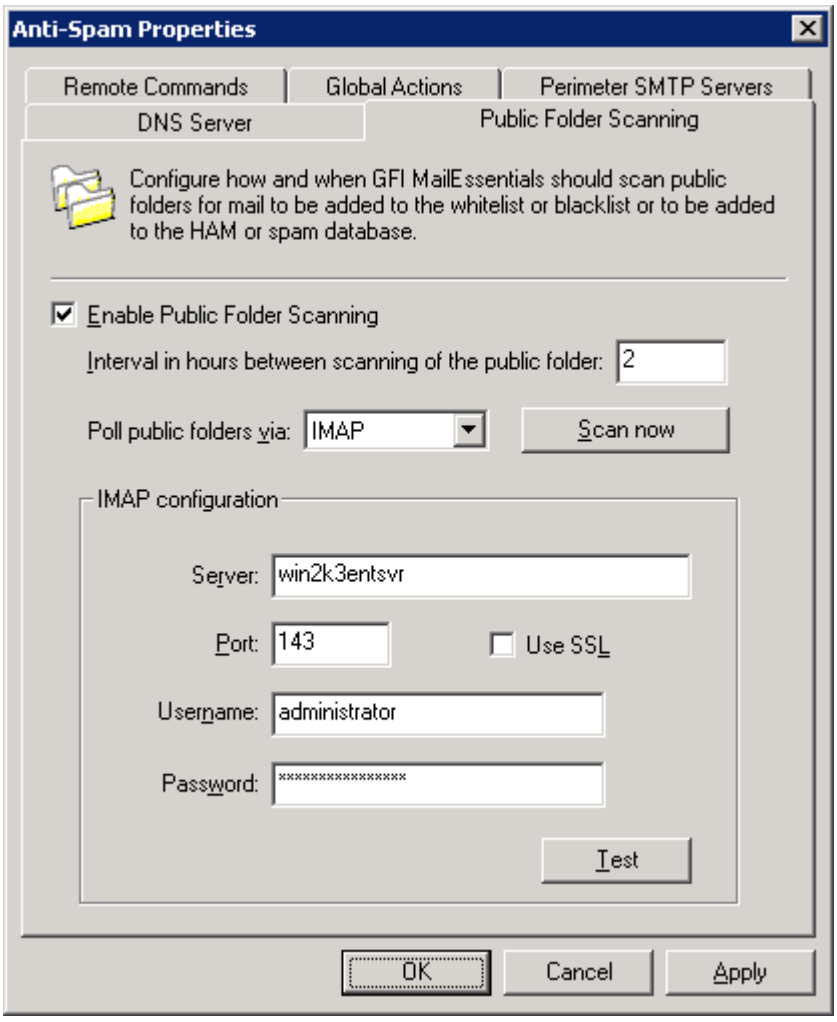
NOTE: To automatically create the **GFI AntiSpam Folders** public folders on your Microsoft Exchange Server, refer to the "Configuring Public folder scanning" further on in this chapter.

Configuring Public folder scanning

To use the public folder scanning feature, 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. Select the **Public Folder Scanning** tab.



Screenshot 75 - Configuring Public folder scanning

3. Select the **Enable Public Folder scanning** checkbox.

4. From the **Poll public folders via** list choose how GFI MailEssentials will retrieve the emails from the public folders:

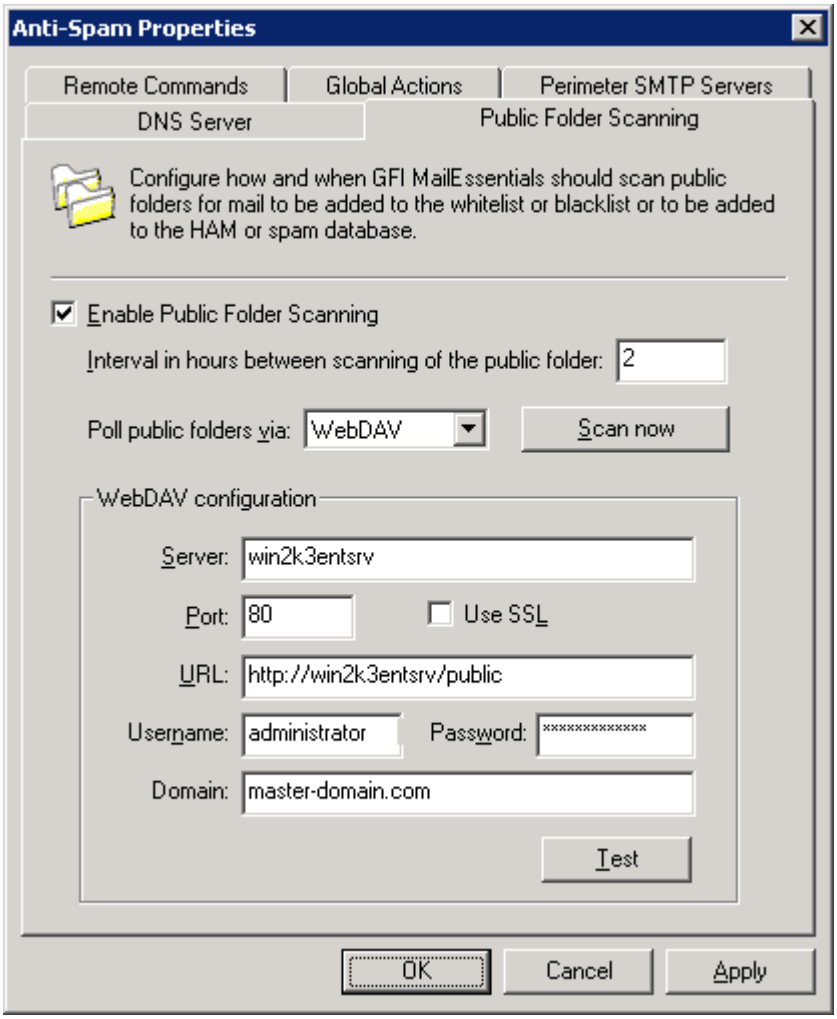
- Via MAPI (requires that GFI MailEssentials be installed on the Microsoft Exchange Server machine itself). If you select MAPI you do not need to configure other settings.

  NOTE: MAPI cannot be used to poll emails from Microsoft Exchange Server 2007 public folders.

- Via IMAP (requires that the Microsoft 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.

  NOTE: IMAP cannot be used to poll emails from Microsoft Exchange Server 2007 public folders.

  If you select IMAP, specify the Mail server name, port (default IMAP port is 143) as well as a username and password. You can also use a secure connection by selecting the **Use SSL** checkbox.

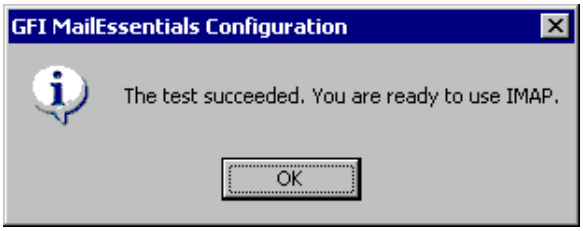


Screenshot 76 - Using WebDAV for public folder scanning

- Via WebDAV - If you select WebDAV, specify the Mail server name, port (default WebDAV port is 80), a username and password, as well as the domain. You can also use a secure connection by selecting the **Use SSL** checkbox. By default, public folders are accessible under the 'public' virtual directory. If you changed this to something else, specify the correct virtual directory

name to access the public folders by editing the text in the **URL** box.

5. If you selected IMAP or WebDAV, click **Test**. If everything works, the public folders will be created automatically and a dialog box as shown below will be displayed. If the test fails, check the credentials and re-test.



Screenshot 77 – Public folder scanning test succeeded

Creating a dedicated account to login via IMAP

NOTE: IMAP cannot be used to poll emails from Microsoft Exchange Server 2007 public folders.

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

1. Before you proceed to create the user, use administrator credentials and click **Test** to ensure that IMAP is working properly and that the public folders have been created.

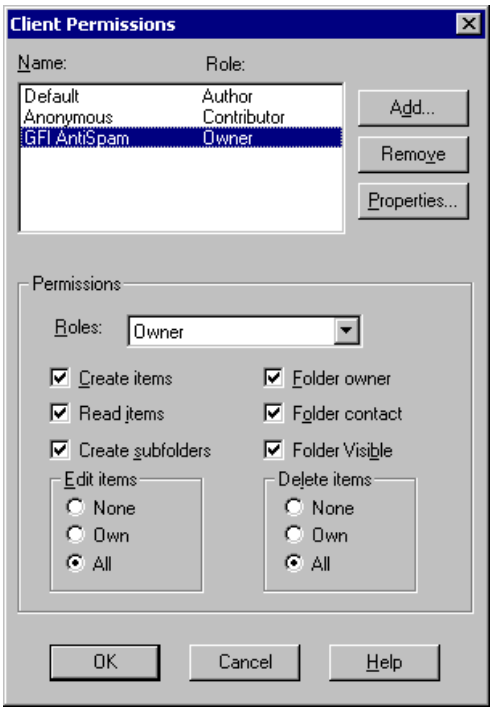
2. Create a new Active Directory (AD) user. This user can have limited rights.

3. Open the Microsoft Exchange System Manager and expand the **Folders > Public Folders** node. Right click on the **GFI AntiSpam Folders** public folder and select **Properties** from the context menu.

4. In the **Properties** dialog box, click the **Permissions** tab and then click **Client permissions**.

5. Click **Add…**, select the user you created in step 2, and then click **OK**.

6. Click on the user you just added to the client permissions list and set its role to owner from the **Roles** list. Make sure all checkboxes are selected and the radio buttons are set to **All**.



Screenshot 78 - Setting user role

7. Click **OK** twice to return to Microsoft Exchange System Manager.

8. Now right click on the **GFI AntiSpam Folders** and from the context menu select **All tasks > Propagate settings**.

9. In the **Propagate Folder Settings** dialog box, select the **Folder rights** checkbox and click **OK**.

10. Finally enter the username you have created in the GFI MailEssentials configuration and click **Test** to ensure the permissions have been set correctly.

Configuring the GFI anti-spam folders so that posts are hidden

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

1. Open the Microsoft Exchange System Manager and expand the **Folders > Public Folders** node. Right click on the **GFI AntiSpam Folders** public folder and select **Properties** from the context menu.

2. In the **Properties** dialog box, click the **Permissions** tab and then click **Client permissions**.

3. Click **Add…** and select the user/group you want to hide the posts from and then 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** checkbox is selected and the radio buttons are set to **None**.

5. Click **OK** twice to return to the Microsoft Exchange System Manager.

6. Now right click on the **GFI AntiSpam Folders** and from the context menu select **All tasks > Propagate settings**.

7. In the **Propagate Folder Settings** dialog box, select the **Folder rights** checkbox and click **OK**.

NOTE: Users will only be able to post to the GFI anti-spam folders. They will not be able to view any emails, not even the ones they posted themselves.

Configuring disclaimers

Introduction to disclaimers

What are email disclaimers?

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

Legal reasons to use a disclaimer

Email disclaimers are a good start in helping companies protect themselves from potential legal threats resulting from the contents of an email.

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

Marketing reasons to use a disclaimer

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

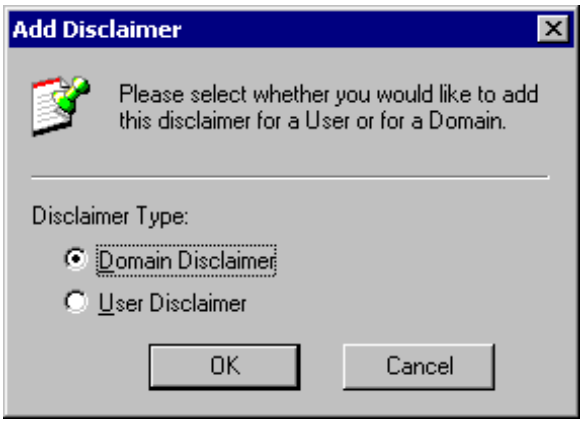
NOTE: Disclaimers are only added to outbound email.

Configuring disclaimers

To add a disclaimer:

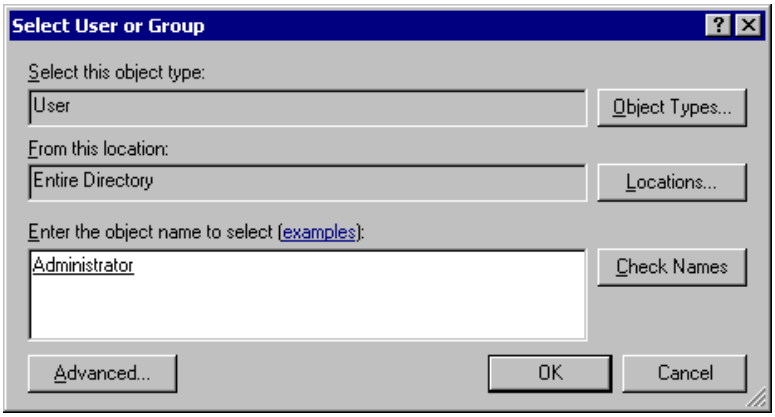
1. Right click on the **Email Management > Disclaimers** node in the GFI MailEssentials configuration. From the context menu select **New > Disclaimer**.

2. Now you need to 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 emails 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 emails sent FROM that user or group of users.



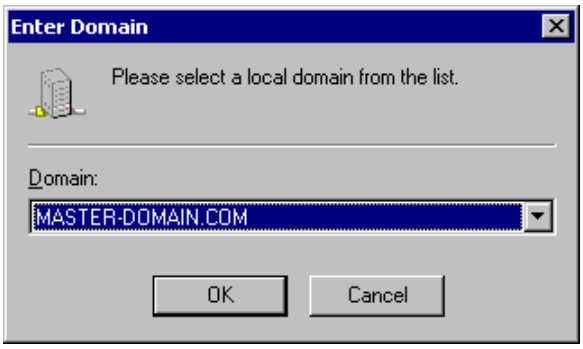
Screenshot 79 - Selecting a domain or user disclaimer

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 80 - Selecting the user/group for whom the user based disclaimer applies

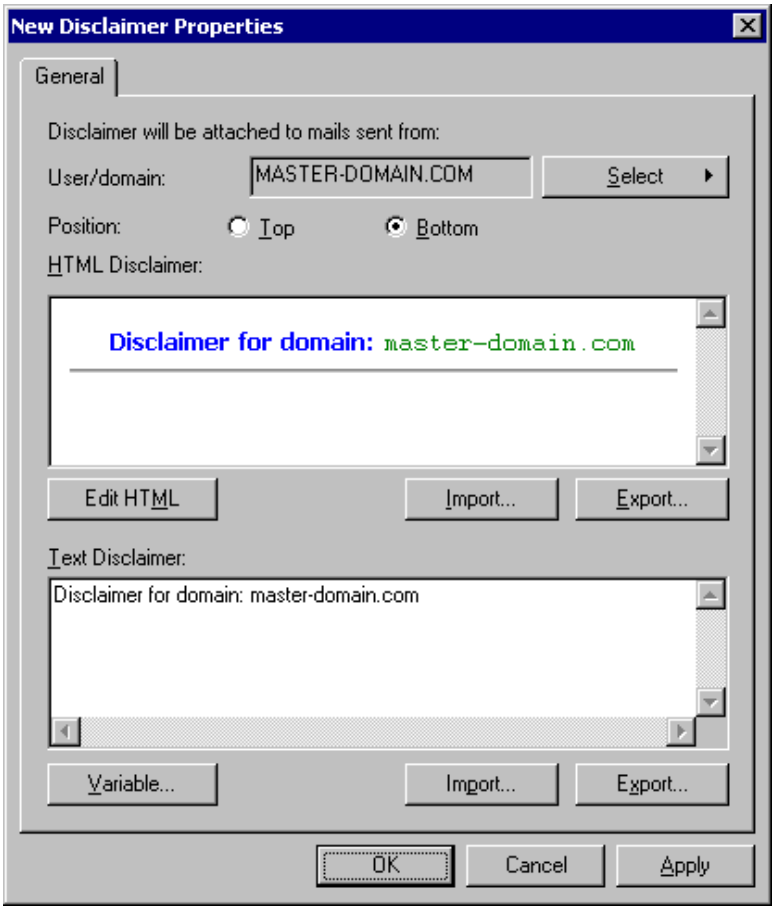
4. If you selected a domain based disclaimer, you have to specify the domain. Note that the disclaimer will only be added if the from address specified in the email includes the domain you specified. If you use multiple email addresses with different domains, setup the disclaimers for all domains that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



Screenshot 81 - Specifying the domain for a domain based disclaimer

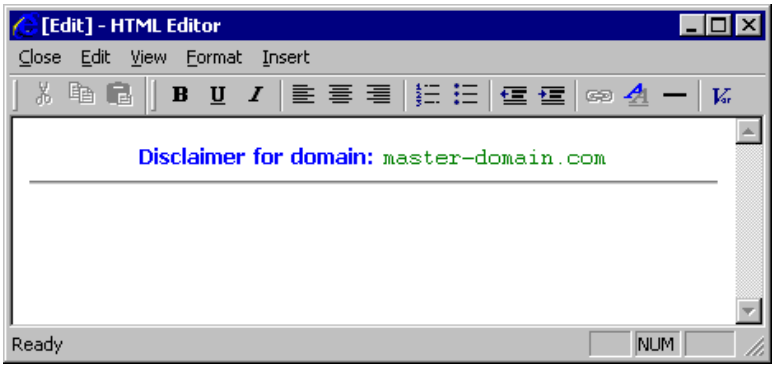
5. The new disclaimer properties dialog is displayed. From the **Properties** dialog, you can specify whether the disclaimer should be put at the top or bottom of the email, by selecting the respective option

from **Top** or **Bottom**. If you want to change the type of the disclaimer, from domain to user/group or vice versa, or you want to specify a different domain/user/group, click the **Select** button.



Screenshot 82 - Adding a disclaimer

6. 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.

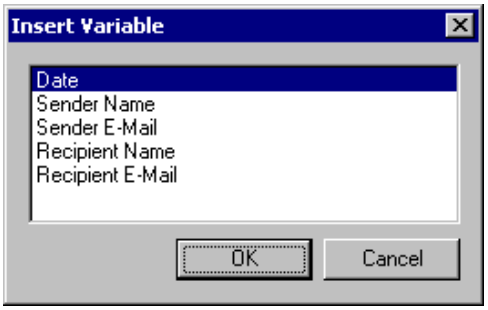


Screenshot 83 - The HTML disclaimer editor

7. The HTML disclaimer editor allows you to specify different font styles. You use the HTML disclaimer editor just like a simple word processing application. In the disclaimer text, you can insert variables using the **Insert** menu. Variables are fields, which will be replaced with the real recipient or sender name in the email. You can include the following fields in the disclaimer text: [recipient display name],

[recipient email address], [date], [sender display name] and [sender email address]. When you finish from editing the disclaimer, click on **Close** from the top menu. This will add the disclaimer to the disclaimer properties dialog.

8. You can include a text based version of your disclaimer, to be used in plain 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 84 - Including variables in your disclaimer

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

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

10. Click the **OK** button to exit the dialog.

11. The new disclaimer is displayed in the right pane of the GFI MailEssentials configuration. To give the new disclaimer a more useful name then just ‘New Disclaimer’, click on the disclaimer and press the F2 key. The disclaimer name will be highlighted allowing you to rename it in place. When you finish renaming the disclaimer press the Enter key.

Configuring spam digests

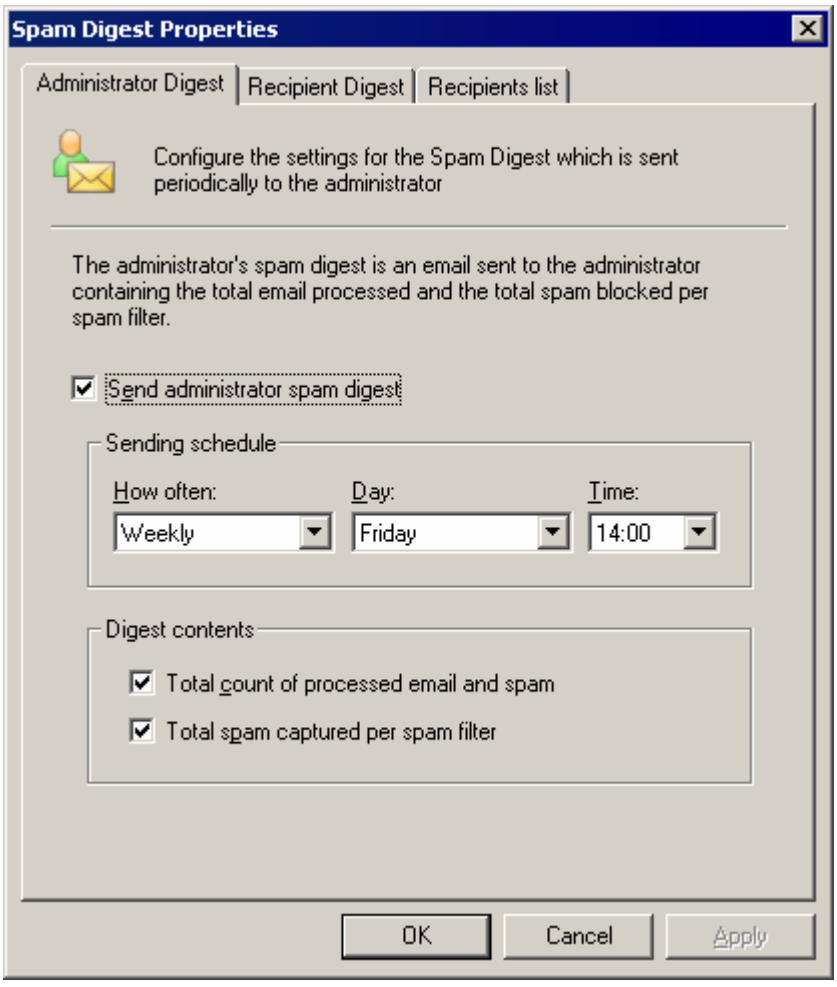
Introduction to the spam digest

The spam digest is a short report that is sent to the administrator or a user via email. This email will outline the total number of emails that have been processed by GFI MailEssentials and the number of spam emails that have been blocked over a specific period of time.

Configuring the administrator spam digest

To configure the spam digest:

1. Right click on the **Email Management > Spam Digest** node in the GFI MailEssentials configuration. From the context menu select **Properties**.



Screenshot 85 – Spam digest properties/Administrator spam digest

2. In the dialog, select **Spam administrator spam digest**.

3. Specify the desired sending frequency (Daily, Weekly or Monthly) through the **Sending schedule** drop-down.

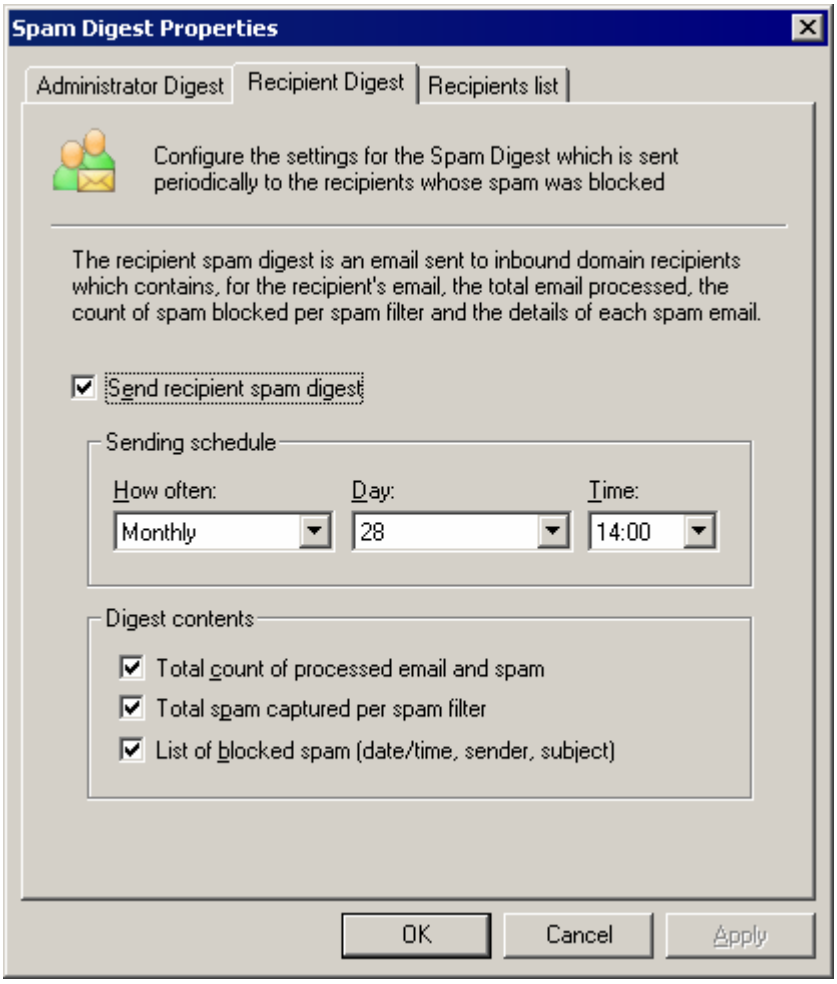
4. Confirm the digest content that will be sent in the email. By default, the digest will contain information on the total count of processed emails including spam emails and the total spam captured by spam filter. To remove any of this content, uncheck the appropriate checkbox from the **Digest contents** area.

5. To finalize your settings, select **Apply** and **OK**.

Configuring the recipient spam digest

To configure the spam digest:

1. Right click on the **Email Management > Spam Digest** node in the GFI MailEssentials configuration. From the context menu select **Properties**.



Screenshot 86 – Recipient spam digest

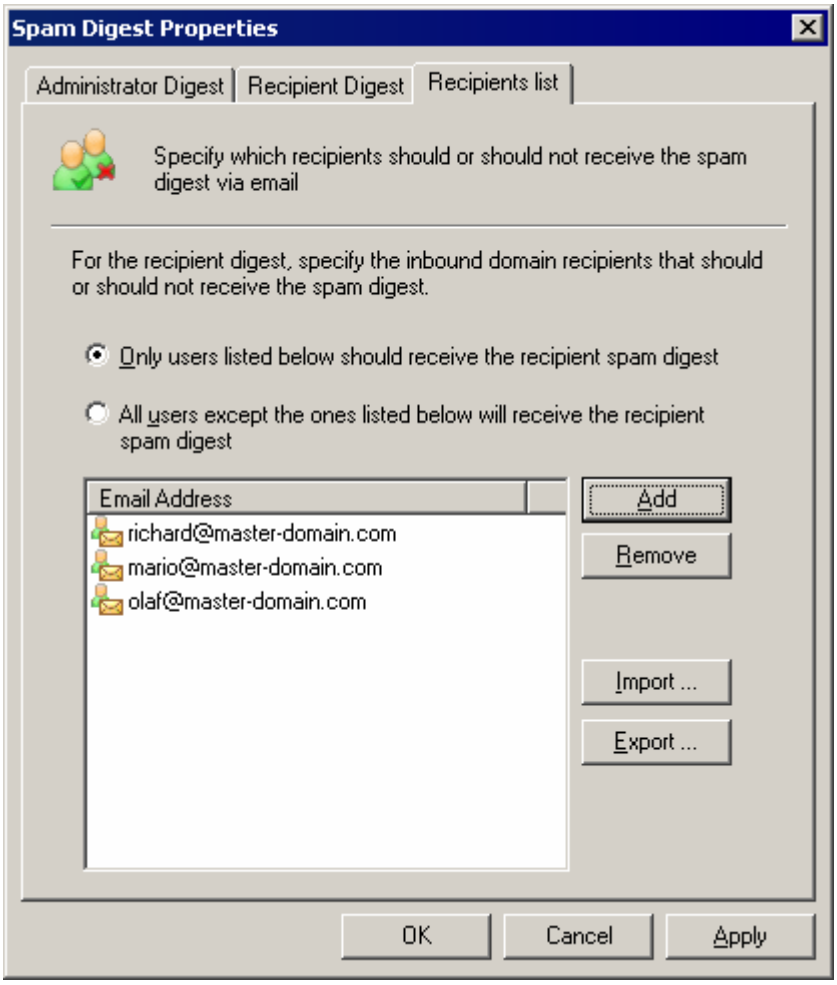
2. Click on the **Recipient Digest** tab.

3. Select **Spam recipient spam digest**.

4. Specify the desired sending frequency (Daily, Weekly or Monthly) through the **Sending schedule** drop-down.

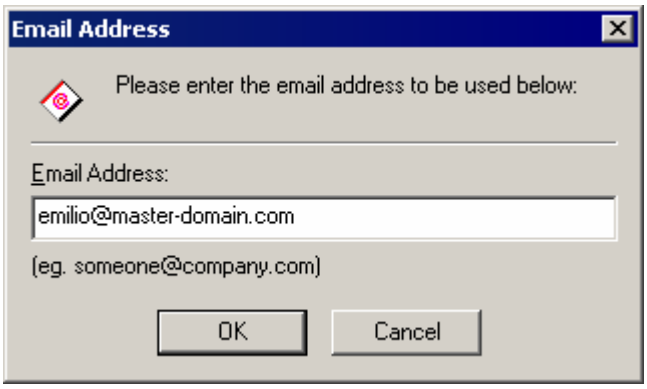
5. Confirm the digest content that will be sent in the email. By default, the digest will contain information on the total count of processed emails including spam emaills, the total spam captured per spam filter

and a list of blocked spam emails. To remove any of this content, uncheck the appropriate checkbox from the **Digest contents** area.



Screenshot 87 – Spam digest recipient list

6. To configure the list of recipients that should receive the spam digest, click on the **Recipients list** tab.



Screenshot 88 – Adding a spam digest recipient

7. To add specific users that should receive the spam digest, select **Only users listed below should receive the recipient spam digest**. Alternatively, if you would like all the users listed in your inbound domain to receive a spam digest, select **All users except the ones listed below will receive the recipient spam digest**.

8. Click on **Add** and enter the email address of the desired recipient in the checkbox provided and click **OK**. Repeat this procedure for the desired amount of users.

NOTE: The required list of users can be imported from a file in XML format in the same structure that GFI MailEssentials would export files.

9. To finalize your settings, select **Apply** and **OK**.

Configuring auto-replies

Introduction to auto-replies

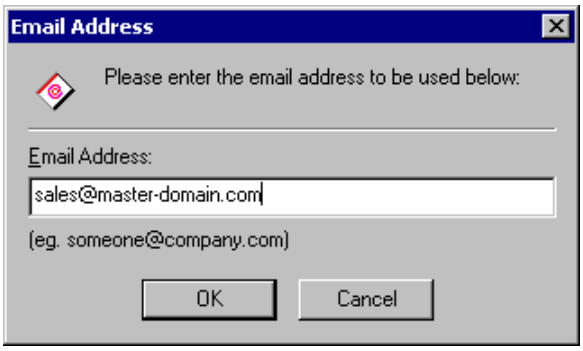
The Auto reply feature allows you to send automated replies to certain incoming emails. You can specify a different auto reply for each email address or subject. You can use variables in an auto reply to personalize an email.

Configuring auto-replies

To create an auto reply:

1. Right click on the **Email management > Auto-Replies** node in the GFI MailEssentials configuration and select **New > Auto-Reply**.

2. In the **Email Address** dialog box specify for which email address you are configuring this auto reply. If for example you specify 'sales @master-domain.com', the sender of an inbound email sent to this email address will receive an auto reply. Click the **OK** button. The auto reply options dialog will be displayed.



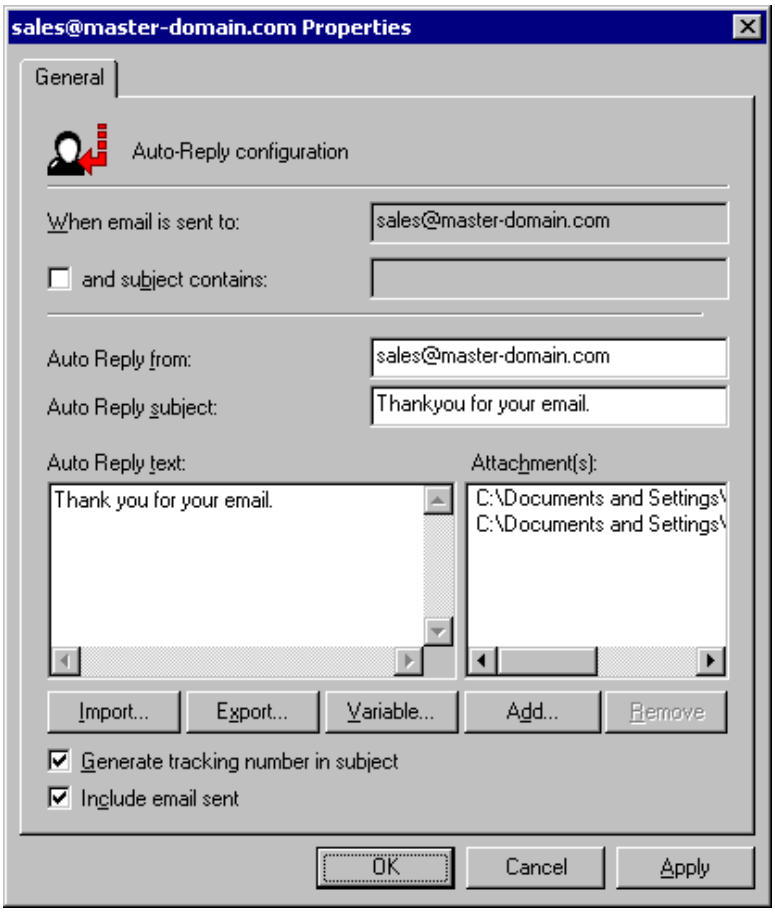
Screenshot 89 - Creating a new auto reply

3. If you want to send an auto reply only when the inbound email contains a certain subject, check the **and subject contains** checkbox, and in the edit box to the right specify the subject.

4. By default the auto reply will be sent from the same email address you specified in step 2 above. If you want to send the auto reply using a different email address in the From field, you can specify it in the **Auto Reply from:** field.

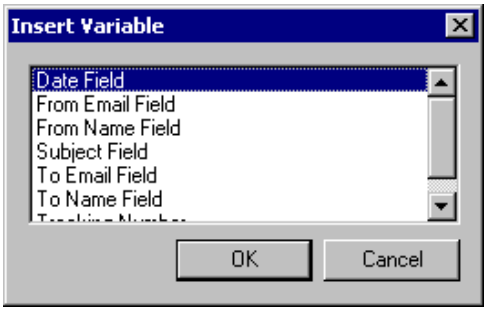
5. You can specify the subject of the auto reply email in the **Auto Reply subject** field.

6. In the **Auto Reply text** edit box, you can specify the text you want to be displayed in the auto reply email. If you have a text file which contains the auto reply email you want to send, you can import its contents by clicking on the **Import…** button.



Screenshot 90 - Auto-reply properties

7. You can personalize the auto reply by adding variables. To do this click on the **Variable…** button. From the **Insert Variable** dialog select the variable field you want to insert, and click the **OK** button. Repeat this step until you have inserted all the variable fields you require.



Screenshot 91 - Variables dialog

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

8. To send file attachments with the auto reply email, such as sales brochures for example, click on the **Add…** button and choose the file you wish to attach. To remove attachments, click on the attachment you want to remove from the **Attachments** list, and then click on the **Remove** button.

9. If you want to quote the inbound email in the auto reply, check the **Include email sent** checkbox.

10. To make it easier for you to track auto-replies, you can specify that the auto reply should include a unique tracking number. Customers for example could reply back to you and quote that tracking number. To generate a tracking number in the subject of both the original inbound email and the auto reply email sent, check the **Generate tracking number in subject** checkbox.

11. To save the auto reply email settings, click the **OK** button.

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 email monitoring

Introduction to email monitoring

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

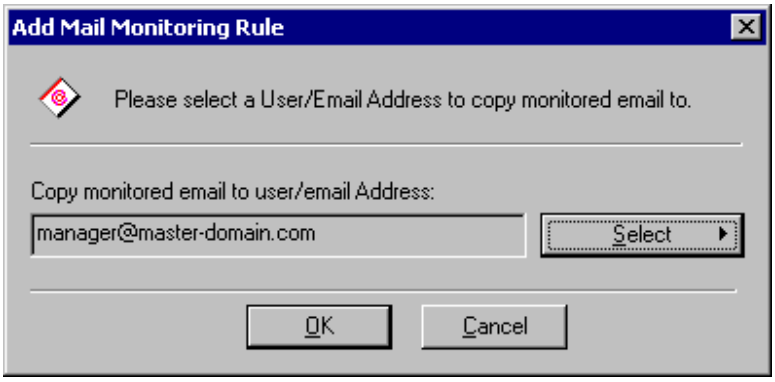
Because you can configure the email to be copied to an email address, all email can be stored in an Microsoft Exchange Server or Microsoft Outlook store, so that you can easily search for email. Mail monitoring can therefore be used as a replacement for Mail archiving.

Configuring email monitoring

To confiture mail monitoring:

1. Right click on the **Email management > Mail Monitoring** node in the GFI MailEssentials configuration and select **New > Inbound Mail Monitoring Rule** or **New > Outbound Mail Monitoring Rule**, depending on whether you want to monitor inbound or outbound email respectively.

2. An **Add Mail Monitoring Rule** dialog box is displayed. Specify the email address/mailbox to which you wish to copy the emails being monitored by the rules you will specify later on. You can specify the email address of a manager or specify an email address associated with for example a public folder. Click the **OK** button to continue.



Screenshot 92 – Add Mail Monitoring rule

3. The monitoring rule properties dialog will be displayed. To specify which email correspondence this monitoring rule should monitor, you need to specify the sender and recipient filter by clicking on the sender and the recipient **Select** buttons respectively. To add the filter to the list, click the **Add** button. To specify multiple filters, repeat this step.

To monitor:

All email 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.

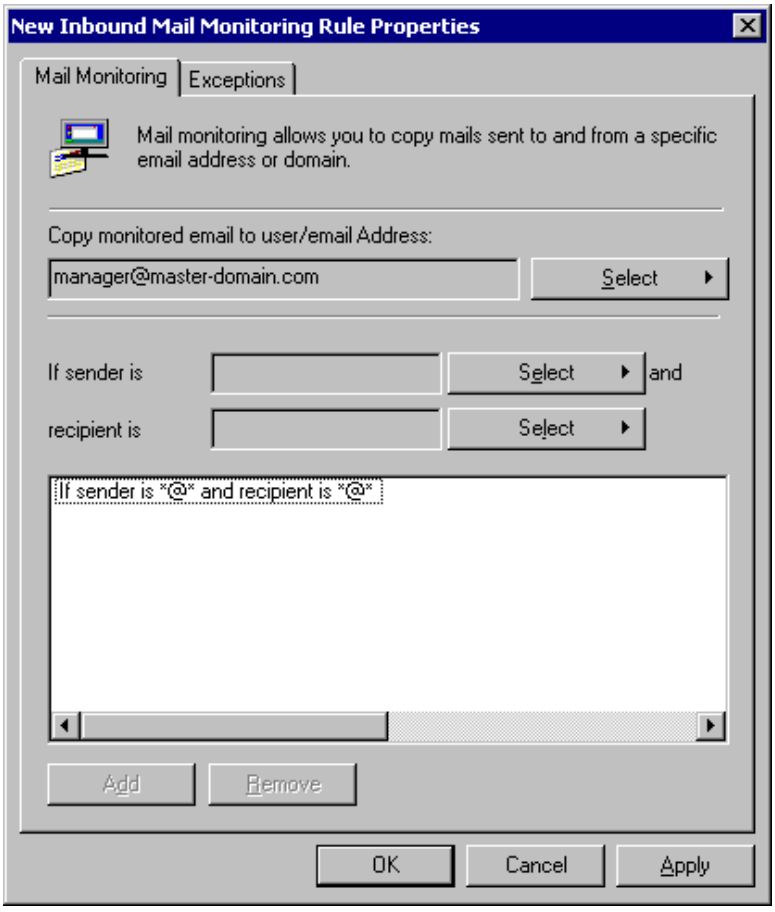
All email sent to a particular user: Create inbound rule, specify recipient email or select user (if using AD) in the recipient field and specify 'all mail' (*@*) in the sender field.

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 username 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 username or user email address in the recipient field.



Screenshot 93 - Configuring email monitoring

4. To configure exceptions to the rule, for example you do not want to monitor the emails of the CEO, access the **Exceptions** tab. Add all the users that you do not want to be monitored by this rule by clicking the **Add…** button to the right of the **Sender** or **Recipient** list. When

specifying exceptions for an inbound monitoring rule, the **Sender** list contains non-local email addresses, and the **Recipient** list addresses are all local. When specifying exceptions for an outbound monitoring rule, the **Sender** list contains local email addresses, whilst the **Recipient** list contains only non-local email addresses.

Screenshot 94 - Creating an exception

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

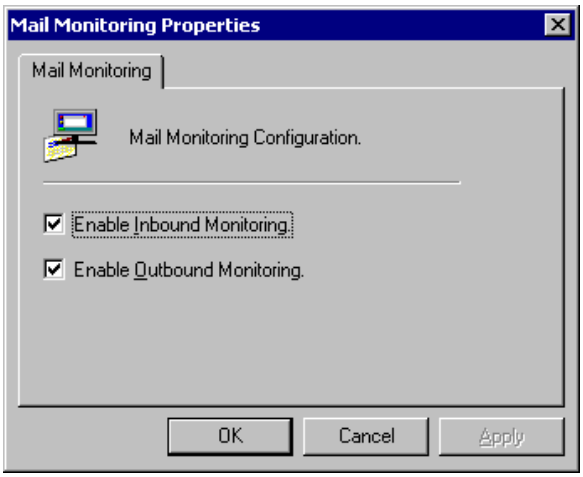
5. Click the **OK** button to add the new email monitoring rule. The new email monitoring rule is displayed in the right pane of the GFI MailEssentials configuration. To give the new email monitoring rule a more descriptive name, for example 'Monitor new employee', click on the email monitoring rule and press the F2 key. The email monitoring name will be highlighted allowing you to rename it in place. When you finish renaming the email monitoring rule, press the Enter key.

Enabling/Disabling email monitoring

If you want to enable/disable all email monitoring rules, follow these steps:

1. Right click on the **Email management > Mail Monitoring** node in the GFI MailEssentials configuration and select **Properties**.

2. The **Mail Monitoring Properties** dialog box is displayed.



Screenshot 95 - Enable or disable email monitoring

3. To enable/disable all inbound email monitoring rules, check/uncheck the **Enable Inbound Monitoring** checkbox respectively.

4. To enable/disable all outbound email monitoring rules, check/uncheck the **Enable Outbound Monitoring** checkbox respectively.

5. Click the **OK** button to accept the changes.

NOTE: To enable/disable an individual email monitoring rule, right click on the email monitoring rule in the right pane of the GFI MailEssentials configuration and select **Enable/Disable** from the context menu.

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 email that a user sends to it.

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

GFI MailEssentials now brings powerful list server capabilities to Microsoft 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 uses this service. It is included with every Windows 2000/2003 and XP version, although not always installed by default.

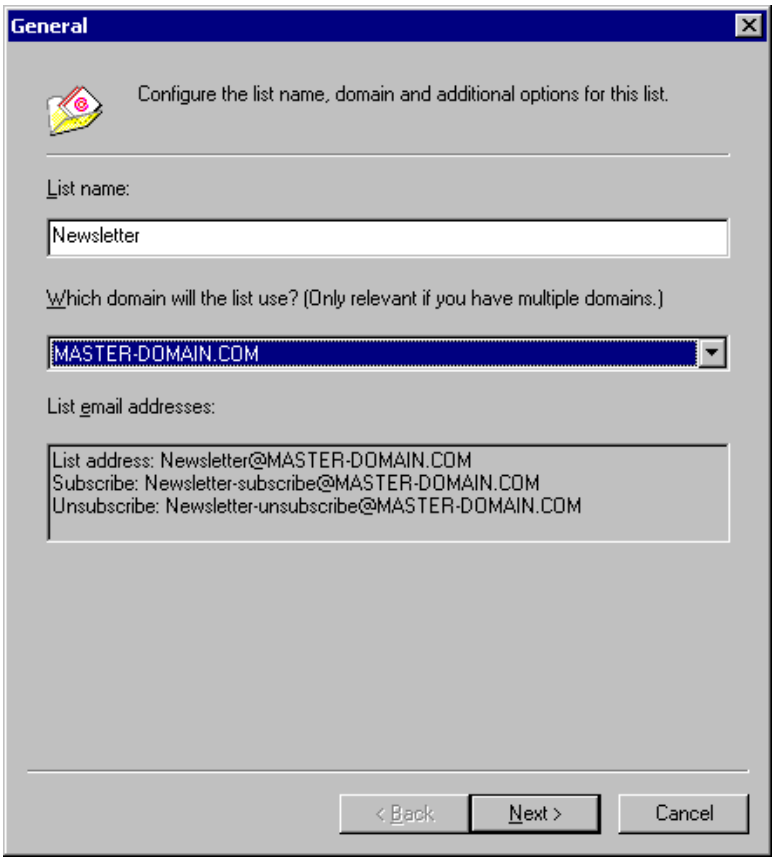
To check whether it is installed and if not how to install it, see the 'Installing the Message Queuing services (MSMQ) on Windows 2000' and 'Installing the Message Queuing services (MSMQ) on Windows 2003' sections of this chapter.

Creating a list

To create a newsletter list:

1. Right-click on the **Email Management > List Server** node and select **New > Newsletter**.

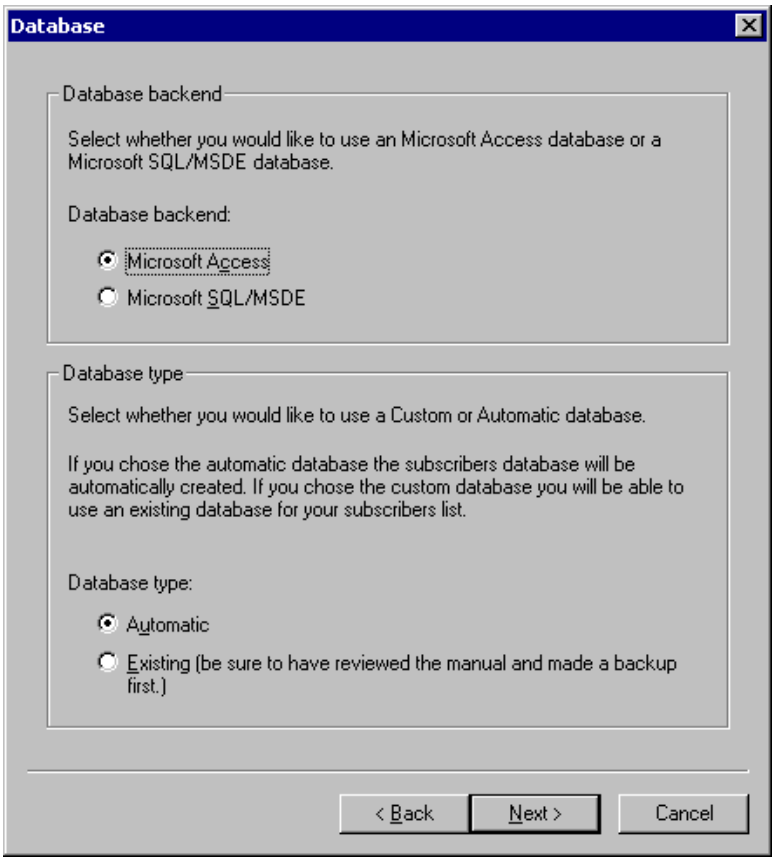
2. The **General** dialog will be displayed. Here you need to specify a list name in the **List name:** edit box and a domain for the list (if you have multiple domains). Click the **Next** button to proceed.



Screenshot 96 - Creating a new newsletter list

3. Next you need to specify whether you want to use a Microsoft Access or Microsoft SQL Server database as the backend for the newsletter. For small lists of up to 5000 members, you can use Microsoft Access as a backend.

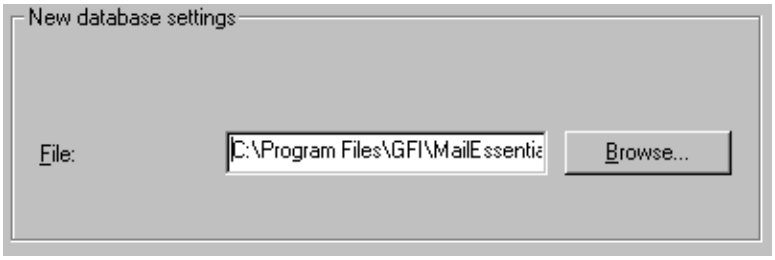
From the **Database type** group, you can specify whether GFI MailEssentials should create a new database or connect to an existing database. The latter allows you to use an existing customer database for the newsletter list. To create a new database, select the **Automatic** option. Click the **Next** button to continue.



Screenshot 97 - Specifying database backend

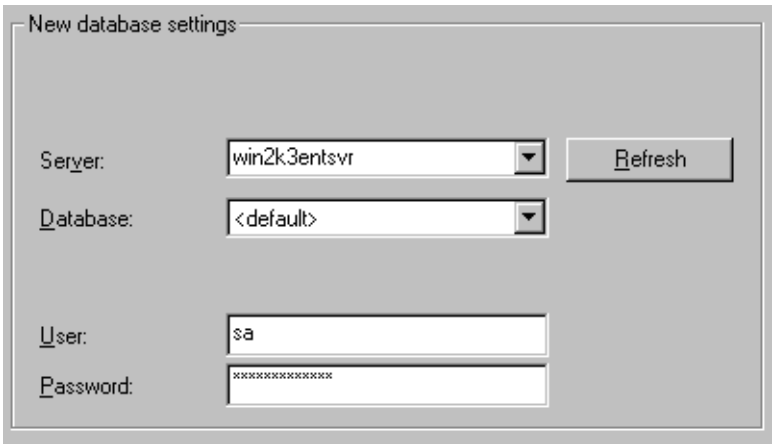
4. You now need to specify which database to use to store the newsletter subscribers list based on the settings you selected in the previous step.

Microsoft Access with Automatic option - You need to specify the location where you want to create the new database to store the newsletter subscribers in the **File** edit box.



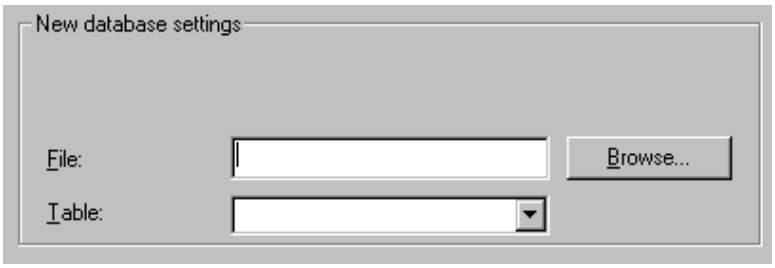
Screenshot 98 - Specifying Microsoft Access details

Microsoft SQL Server with Automatic option – You need to configure the SQL server name, logon credentials and database to use to store the newsletter subscribers list.



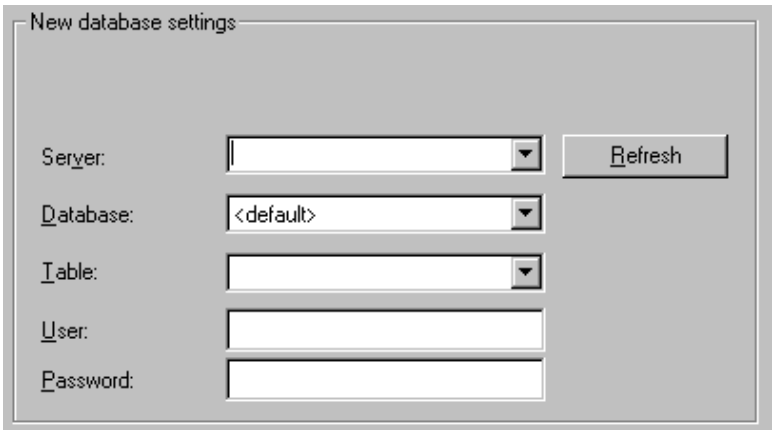
Screenshot 99 - Specifying SQL server details

Microsoft Access with Existing option - You need to enter the path to your existing Microsoft Access database containing the newsletter subscribers in the **File** edit box. From the **Table** drop down list you need to select the table where the subscribers list is stored.



Screenshot 100 - Specifying existing Microsoft Access database file and table

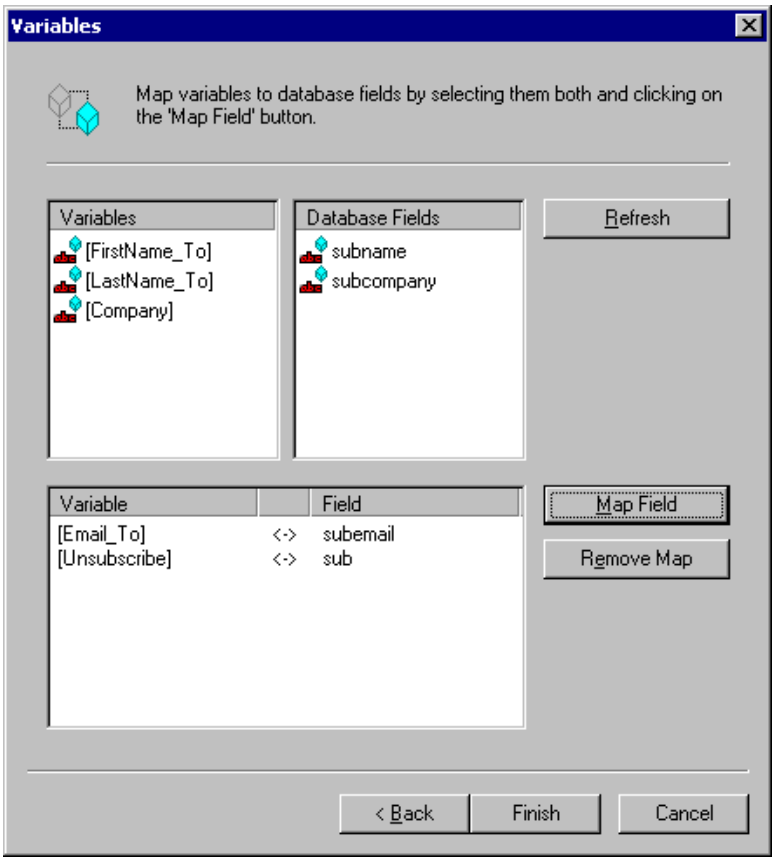
Microsoft SQL Server with Existing option – You need to configure the SQL server name and logon credentials, then select the database and table where the subscribers list is stored.



Screenshot 101 - Specifying existing SQL server table

5. If you selected any database type with the **Automatic** option, you only need to click the **Finish** button to end the wizard.

6. If on the other hand you selected the **Existing** option, you will need to click on the **Next** button and then map the required fields with the custom fields found in the database and table you selected in the **Variables** dialog.



Screenshot 102 – Mapping custom fields

The [Email_To] and [Unsubscribe] fields need to be mapped. The [Email_To] field should be mapped to a string field containing the email address of a subscriber. The [Unsubscribe] field should be mapped 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 used so that when users unsubscribe from the list we do not delete the actual entries, but rather just flag them as no longer subscribed to the list.

To map fields you need to select a field from the **Variables** list and the corresponding field from the **Database Fields** list, and then click the **Map Field** button. To remove mapped entries, select them from the bottom list and click the **Remove Map** button.

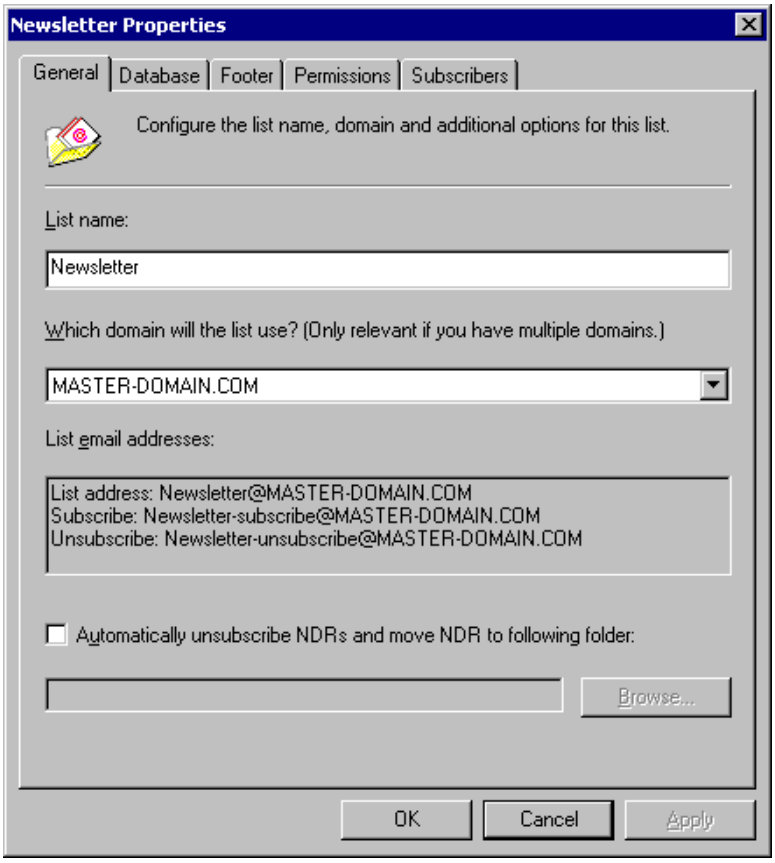
When you map the required fields, click the **Finish** button to end the wizard.

7. When the wizard completes, the newsletter list will be created in the right hand pane of the GFI MailEssentials configuration and you can further configure its options by right clicking on the list name and selecting **Properties** from the context menu.

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** from the context menu. This brings up the newsletter properties dialog.

From the **General** tab you can change the list name, as well as its domain. In addition you can specify that if the list server receives an NDR, the user will be automatically unsubscribed.

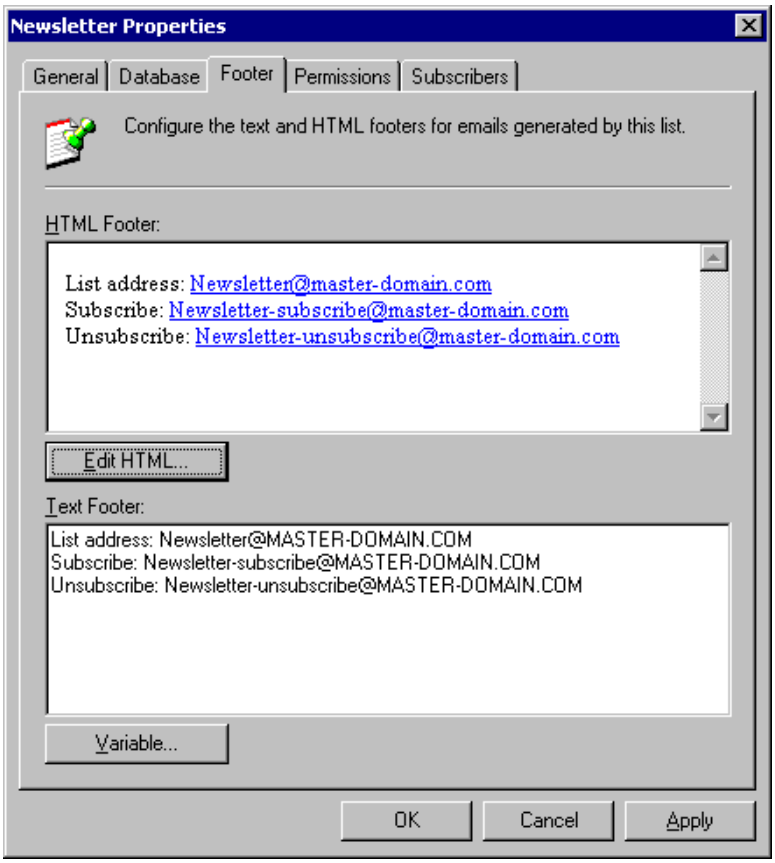


Screenshot 103 - General newsletter properties

From 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 email. Click the **Edit HTML** button to create an HTML footer. You can use the footer to communicate how users can subscribe to the list and unsubscribe from the list.



Screenshot 104 – Newsletter footer properties

Setting permissions to the list

The permissions tab allows you to specify who can submit an email to the list.

NOTE: If you do not secure the list, anybody can send an email to the entire list by sending an email to the list address.

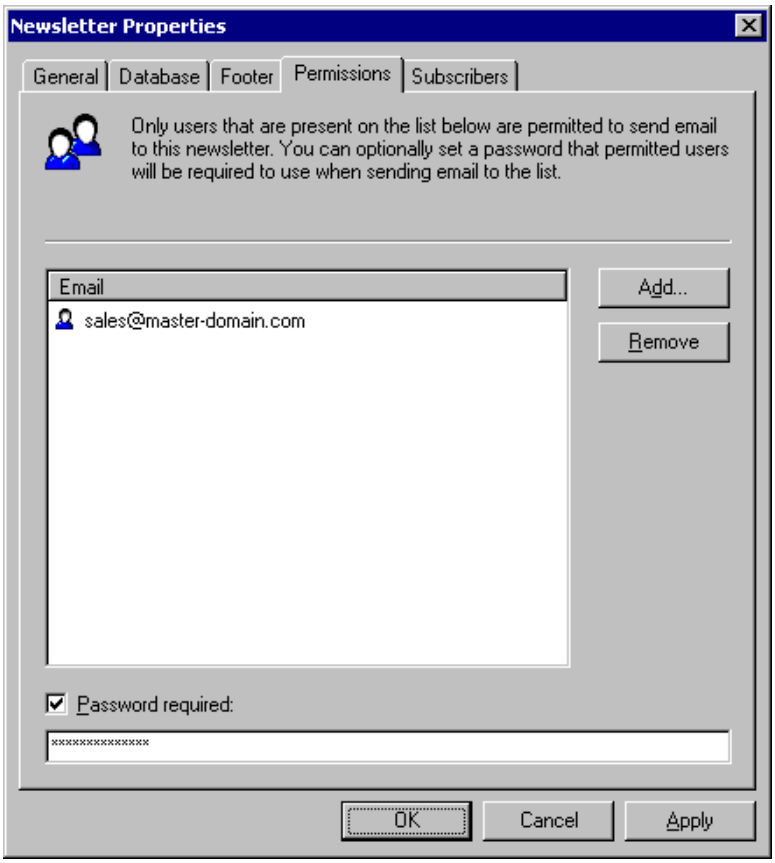
To configure who can post emails to the newsletter list, access the **Permissions** tab. Click the **Add** button and in the **Email Address** dialog box specify the user with permissions to submit an email to the list. Click the **OK** button. The email address will be added to the **Email** list.

You can optionally set a password, which secures access to this newsletter in case someone else makes use of the email client or account details of a permitted user (e.g. email client sharing between employees, computers left unlocked by permitted users, spoofing, etc..). When this option is enabled, permitted users must authenticate themselves by including this password in the email **subject** field when sending emails to the newsletter. The password must be specified in the subject field as follows:

[PASSWORD:<*configured password*>**]**<*The Subject of the email!*>

For example: [PASSWORD:letmepost]Special Offer.

If the password is correct, the list server will remove the password details from the subject and relay on the email to the specified list address (i.e. to the Newsletter).



Screenshot 105 - Setting permissions to the newsletter

To enable password authentication, check the **Password required** checkbox and specify the password in the text box at the bottom of the page.

Adding subscribers to the list

We recommend that you allow users to subscribe specifically to the list, by sending an email themselves to the subscribe newsletter address.

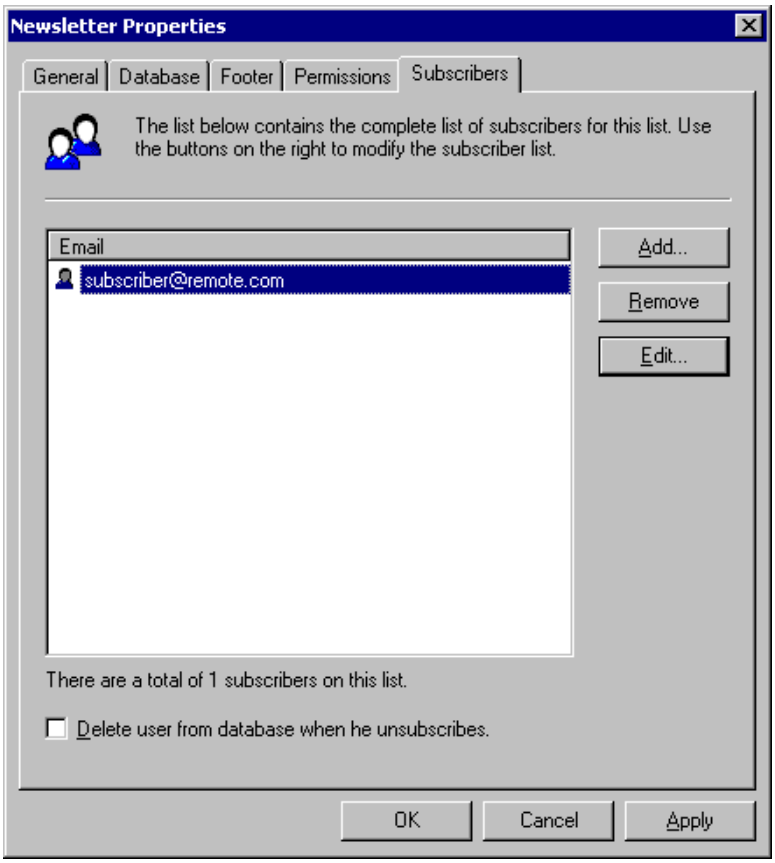
If however you have a list of users you want to add to the newsletter yourself, you can do this via the **Subscribers** tab.

NOTE: If you add users, and you have not specifically asked their permission to be added to the list, you might get spam complaints. Therefore we suggest you send out a mailing asking them to subscribe at < newslettername>-subscribe@yourdomain.com

To add a user to the newsletter subscription list, click the **Add** button. In the **Subscriber** dialog, specify the **Email Address** field. The **First name**, **Last name** and **Company** fields are optional. Click the **OK** button. The new subscriber email address will be added to the **Email** list.

To remove subscribers from the list select them and click the **Remove** button and click **Yes** in the prompt.

To edit an existing subscriber details, select the email address from the **Email** list and click the **Edit…** button.



Screenshot 106 - Entering subscribers to the newsletter

NOTE: If you want the user details to be removed from the subscription list table when unsubscribing from the list, and not just flag it as unsubscribed, check the **Delete user from database when he unsubscribes** checkbox.

Operating the newsletter list

Sending a newsletter

Sending email to the entire list is very easy. Members who have permission to send email to the list (this is configured from the **Permissions** tab in the newsletter properties), can just send the email 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 an email 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 cannot be turned off. It will save you a lot of spam complaints.

Unsubscribing from the list

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

Adding a link to your website

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 need to specify a name for the list, and also the domain of the list (if you have multiple domains). Click the **Next** button to continue.

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.

4. If you selected Microsoft Access, you need to enter the full path where you want to create the new database in the **File** edit box. If you selected Microsoft SQL server, you need to configure the SQL server name, logon credentials and the database.

5. Click the **Finish** button to end the wizard. The wizard will confirm the creation of the 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 discussion list name and selecting **Properties** from the context menu.

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** from the context menu. This brings up the discussion list properties dialog.

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 will automatically unsubscribe 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 email. 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 subscribes 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

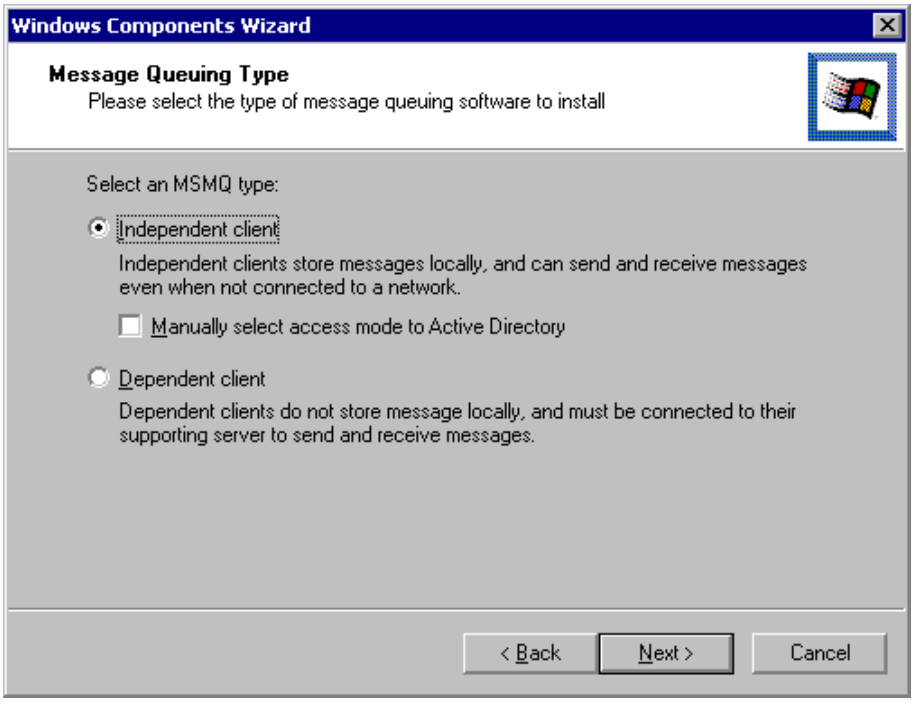
The message queuing service is a scalable system service developed by Microsoft to enable high volume event processing. GFI MailEssentials uses this service for the list server. The message queuing service is included with every Windows 2000/2003 and XP version, although not always installed by default.

To check whether MSMQ is installed and to install it if it is not:

1. Open the Windows Control Panel from the start menu, double-click on Add/Remove Programs and then click on the Windows Components tab to launch and display the Windows components wizard. Now check if the 'Message Queuing Service' checkbox is selected.

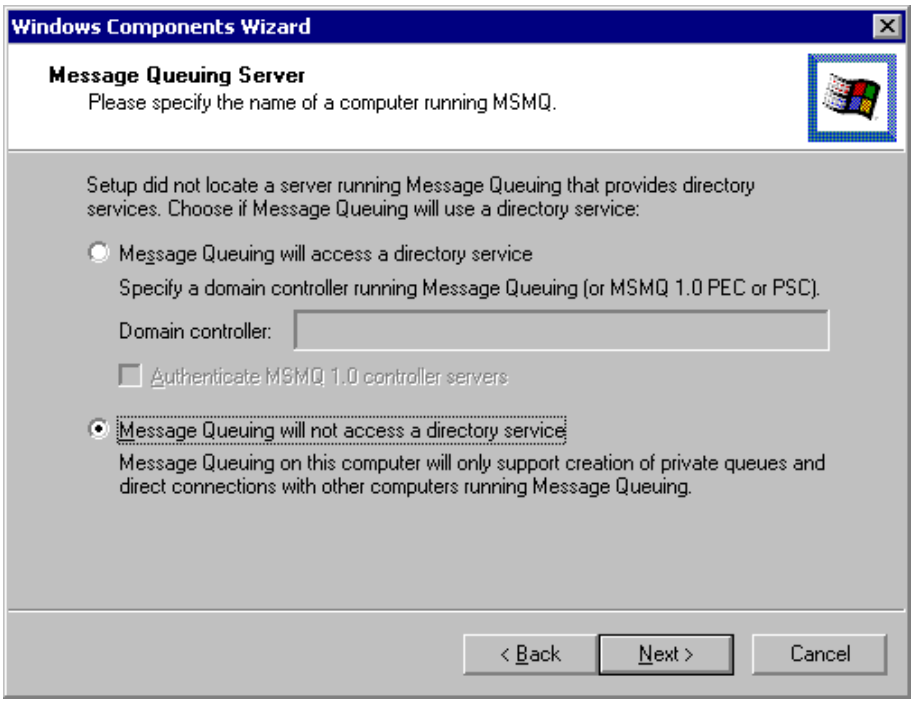
Screenshot 107 - The Windows components wizard

2. If the Message Queuing Services checkbox is not selected, you need to install the Message Queuing Service. To do this, select the checkbox and click **Next**. You need to have your Windows 2000 CD handy.



Screenshot 108 - Selecting the Message Queuing type

3. You will now be asked to select what type of queue to install. Click on **Independent client** and then click **Next**.



Screenshot 109 - 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. Click on the **Message Queuing Service will not access a directory service** option and then click **Next**. The Message Queuing Service will now be installed.

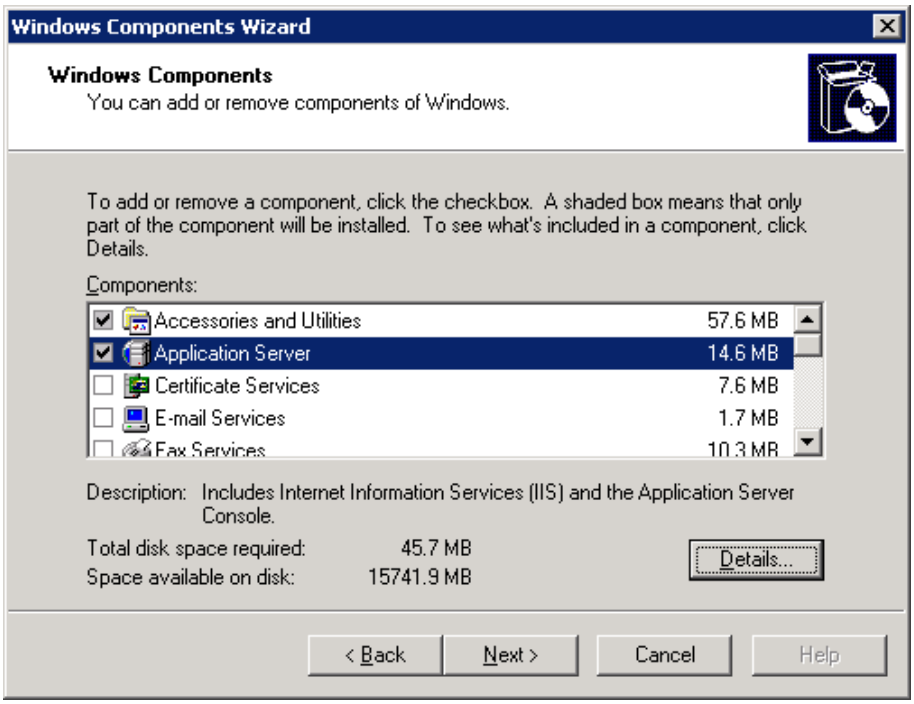
Installing the Message Queuing services (MSMQ) on Windows 2003

The message queuing service is a scalable system service developed by Microsoft to enable high volume event processing. GFI MailEssentials uses this service for the list server. The message queuing service is included with every Windows 2000/2003 and XP version, although not always installed by default.

To check whether MSMQ is installed and to install it if it is not:

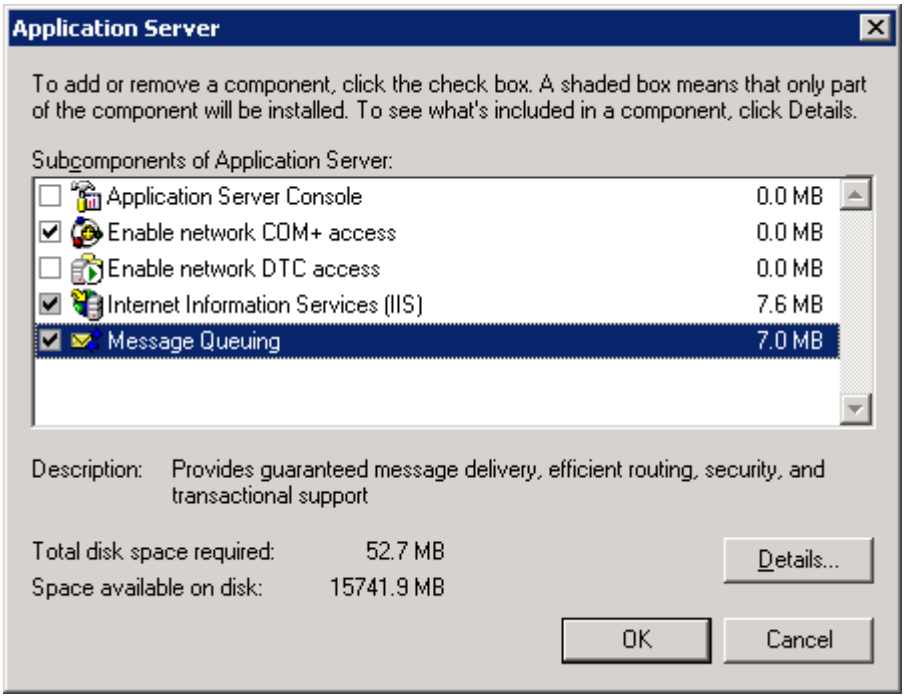
1. Open the Windows Control Panel from the start menu, double-click on Add/Remove Programs and then click on the Windows Components tab to launch and display the Windows components wizard.

2. Click on **Application Server** and then click **Details**.



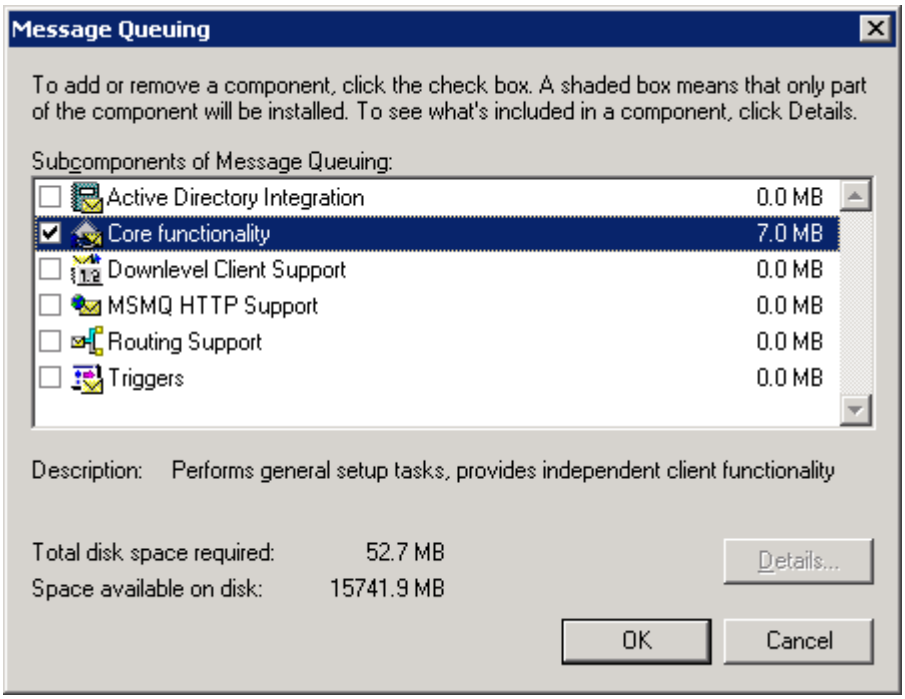
Screenshot 110 - Windows Components Wizard

3. If the **Message Queuing** checkbox is selected it means the service is already installed and you can thus skip the rest of this section. If it is not, then you need to follow the rest of the steps below to install the message queuing service. In the **Application Server** dialog click on **Message Queuing** and then click **Details**.



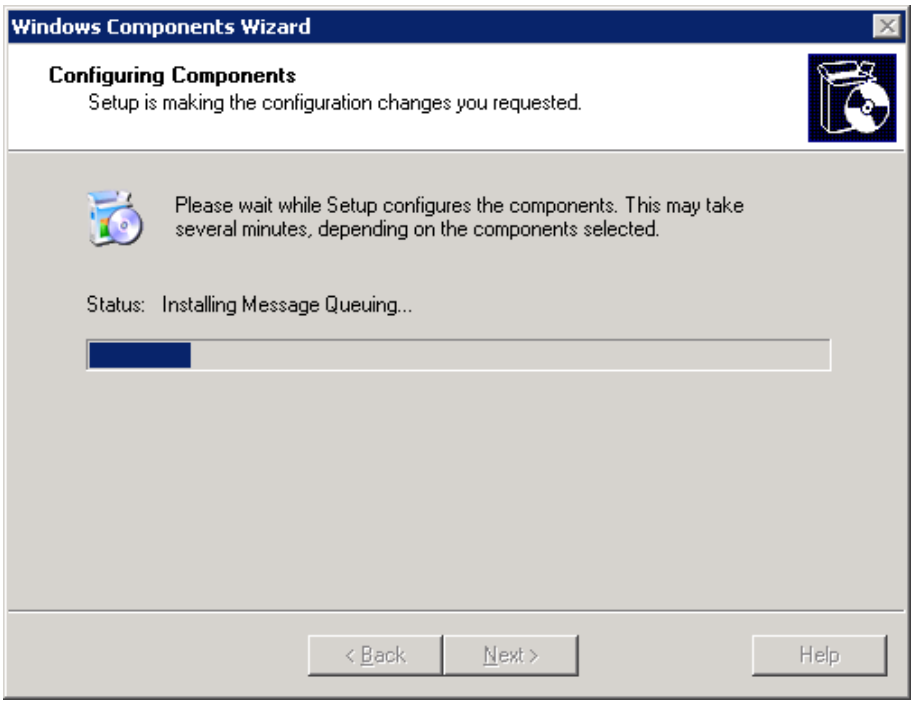
Screenshot 111 - Message Queuing component

4. In the **Message Queuing** dialog select the **Core functionality** checkbox and then click **OK**.



Screenshot 112 - MSMQ Core functionality

5. In the **Application Server** dialog click **OK** and then click **Next** in the **Windows Components Wizard** window to start installing the message queuing service.



Screenshot 113 - Installing the Message Queuing service

6. When the installation of the message queuing service is complete, you need to click **Finish** in the **Windows Components Wizard**. The Message Queuing Service is now installed.

Configuring email archiving

Introduction to email archiving

NOTE: For full-featured email archiving, we recommend GFI MailArchiver, which allows users to search, view and restore emails through a single web-based location, significantly reduces storage requirements and helps in regulatory compliance.

For more information on GFI MailArchiver, visit:

http://www.gfi.com/mailarchiver/

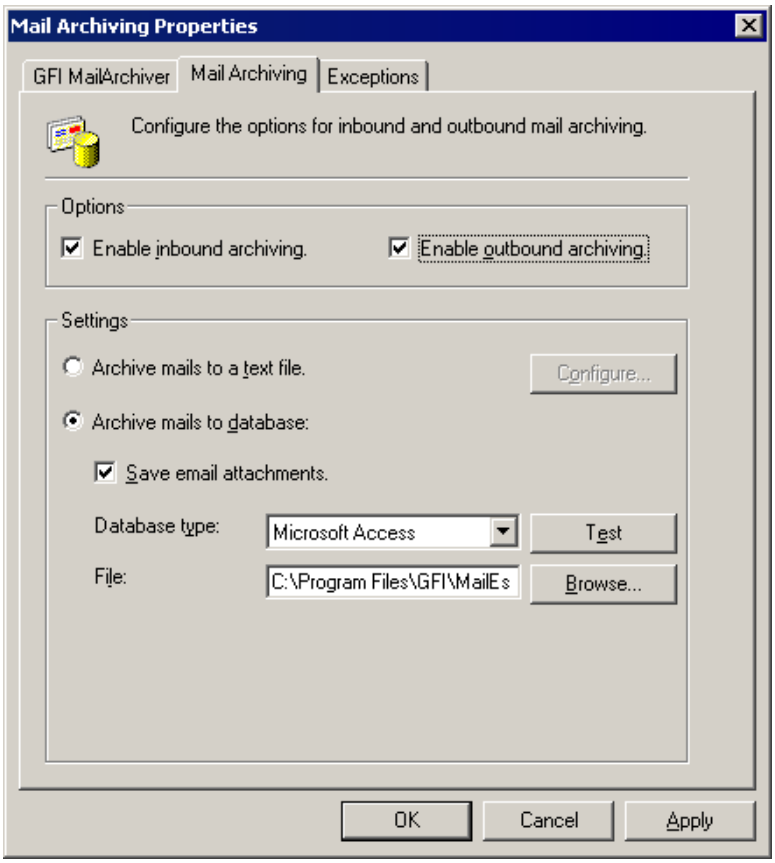
The GFI MailEssentials archiving feature allows you to archive all inbound and outbound email. This feature can be used to store a history of your email communications. In some countries and industries this is required by law.

Configuring email archiving

To archive email:

1. Right click on the **Email Management > Mail Archiving** node and select **Properties** from the context menu. The **Mail Archiving Properties** dialog is displayed.

2. Select the **Mail Archiving** tab.



Screenshot 114 - Archiving properties

3. Select whether you want to archive inbound and outbound emails.

Enable Inbound archiving: Check this checkbox to enable archiving of inbound email.

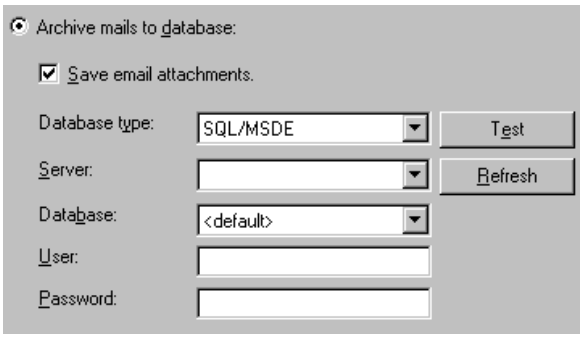
Enable Outbound archiving: Check this checkbox to enable archiving of outbound email.

4. Then choose whether you want to archive email to a database or to a text file.

5. If you want to archive email to a text file, select the **Archive mails to a text file** option and click on the **Configure** button to select the location and filename to which GFI MailEssentials should archive the emails. Be sure to select a drive with ample disk space.

NOTE: If you archive to a text file, attachments will not be archived.

6. If you want to archive email to a database, select the **Archive mails to database** option and select which database you wish to use. Although you can archive email to an access database file, this is not recommended, considering the amount of data that will be archived.



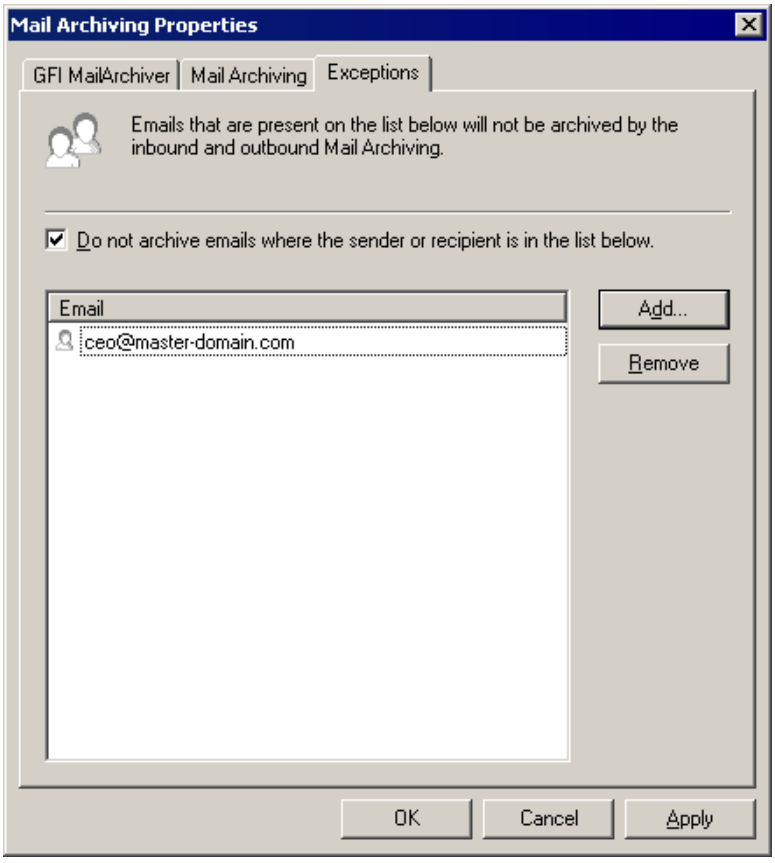
Screenshot 115 - SQL server settings

7. Select SQL/MSDE from the **Database type** drop down list and specify the server name, logon credentials and database.

NOTE: If you select MSDE there is a limit of 2 gigabytes.

8. If you want to exclude certain users from having their emails archived, you can specify an exception list in the **Exceptions** tab. Click the **Add** button to add a new user email address in the **Email** list. To remove users from the exception list, select the email address from the list and click the **Remove** button.

9. To save the email archiving settings, click the **OK** button.



Screenshot 116 – Mail Archiving exception list

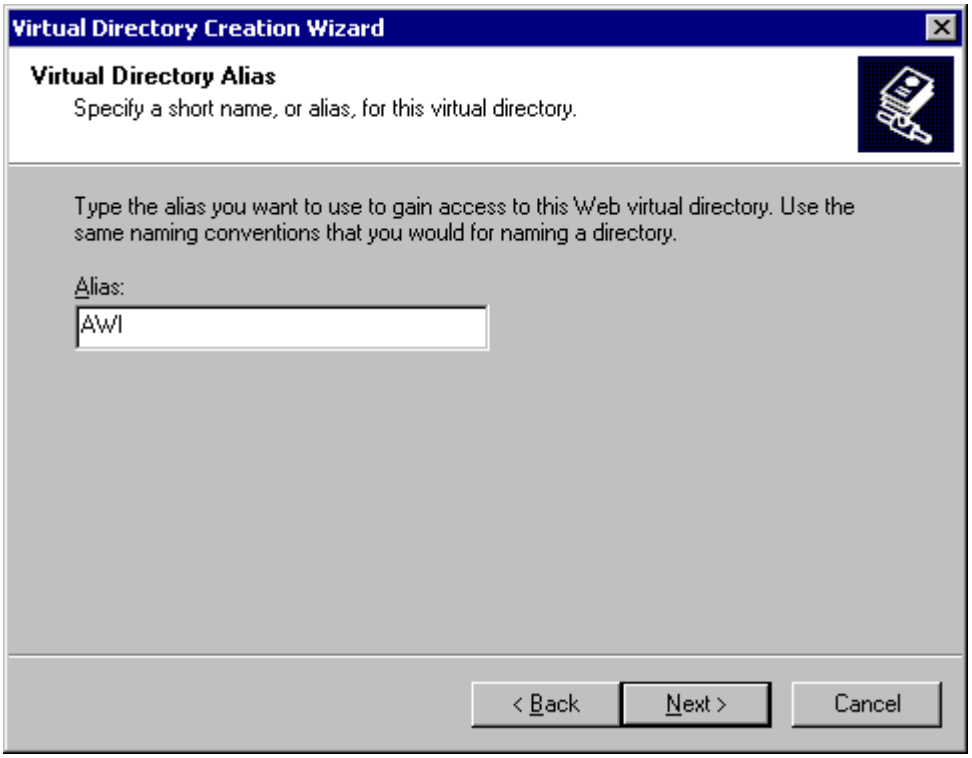
Configuring the IIS to access the Archive Web Interface (AWI)

NOTE: If you installed GFI MailEssentials on a Microsoft Exchange Server 2007 machine, you cannot configure the **Archive Web Interface (AWI)** feature on IIS, since the **AWI** is not compatible with x64 machines.

Mail archived by the Mail Archiving feature to a database, 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. To do this follow these steps:

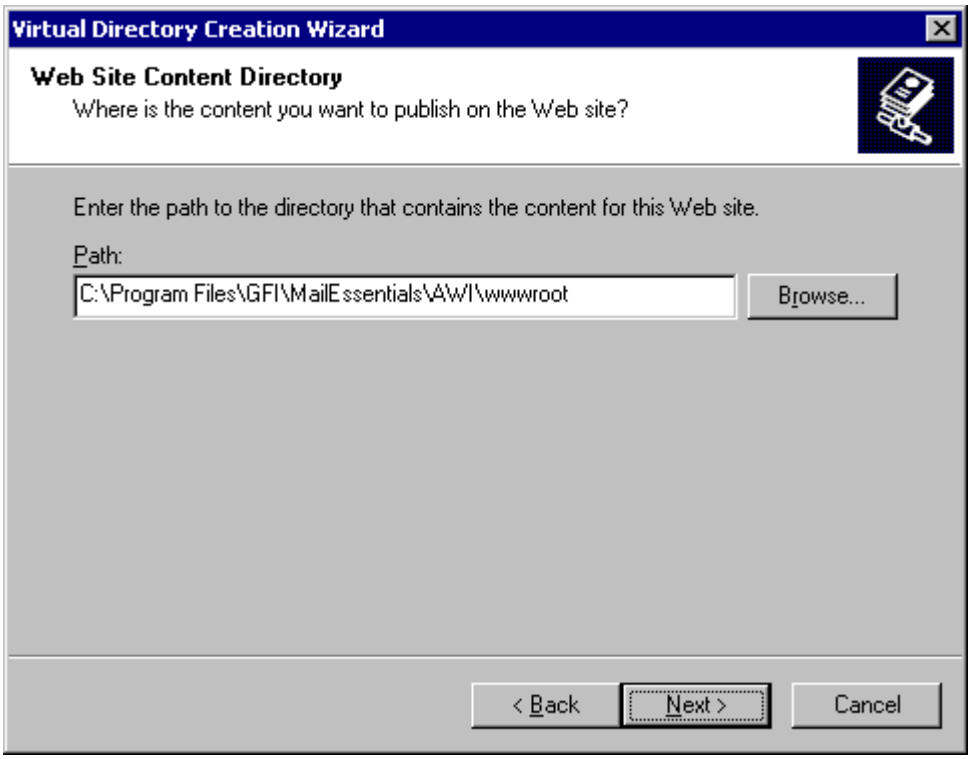
1. Start up Internet Services Manager, right click on the Website node, and from the popup menu select **New – Virtual Directory**. The **Virtual Directory Creation Wizard** is displayed. Click the **Next** button to continue.

2. 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.



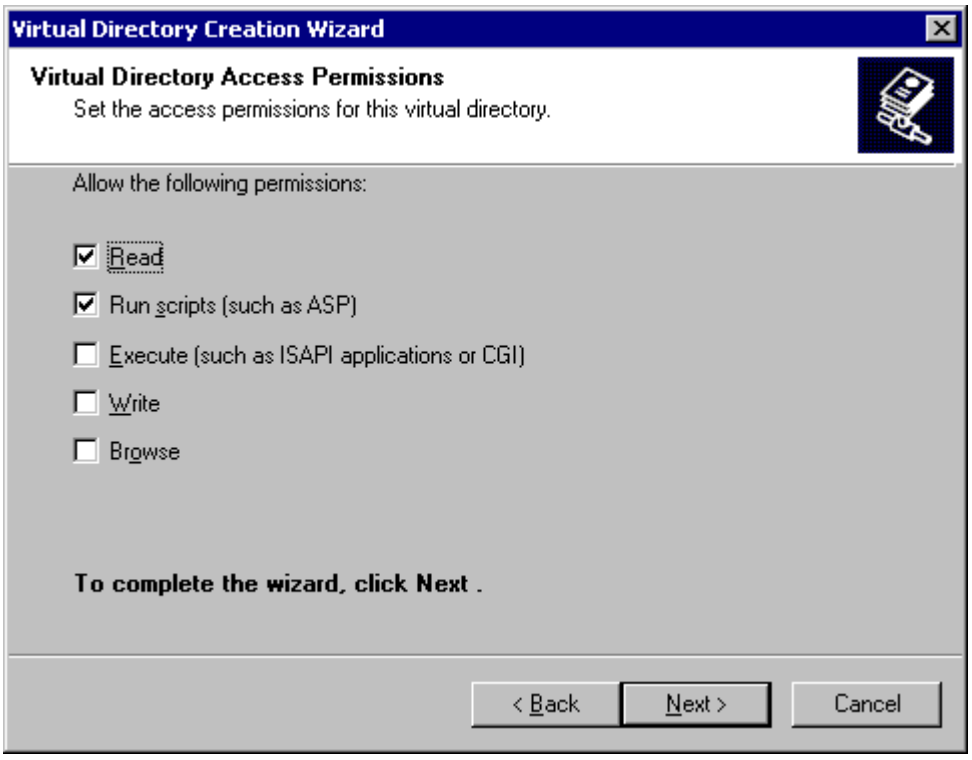
Screenshot 117 - Specifying an alias for the virtual directory

3. You now need to enter the path where the content is located. Click on the **Browse** button, and select the folder AWI\wwwroot in the GFI MailEssentials installation path.



Screenshot 118 - Pointing to the AWI web folder

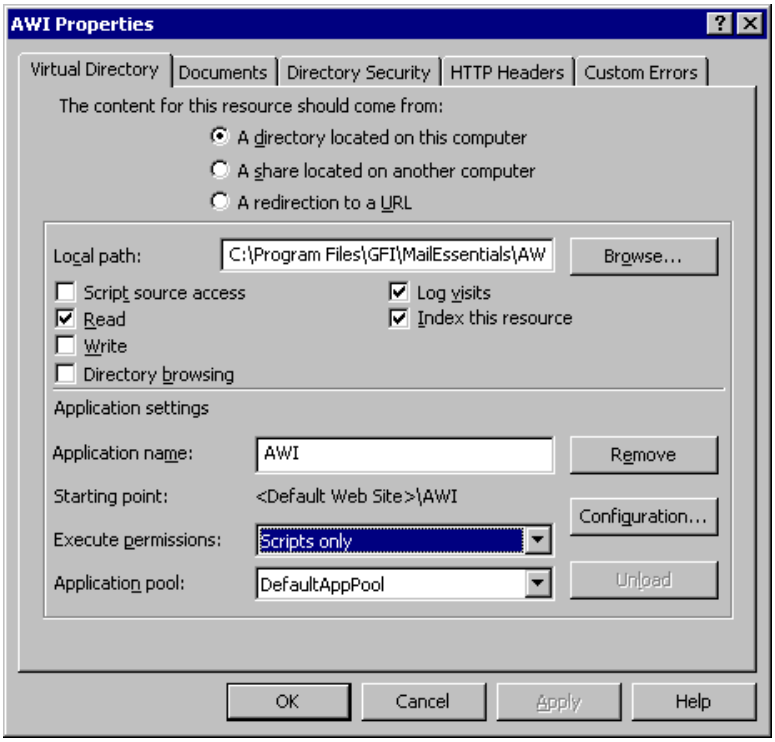
4. Next you need to set the access permissions. Check the **Read** and **Run Scripts (such as ASP)** checkboxes only. Make sure all the other checkboxes are unchecked. Click the **Next** button and on the finish page click the **Finish** button to finish the Virtual Directory Creation Wizard.



Screenshot 119 - Setting permissions

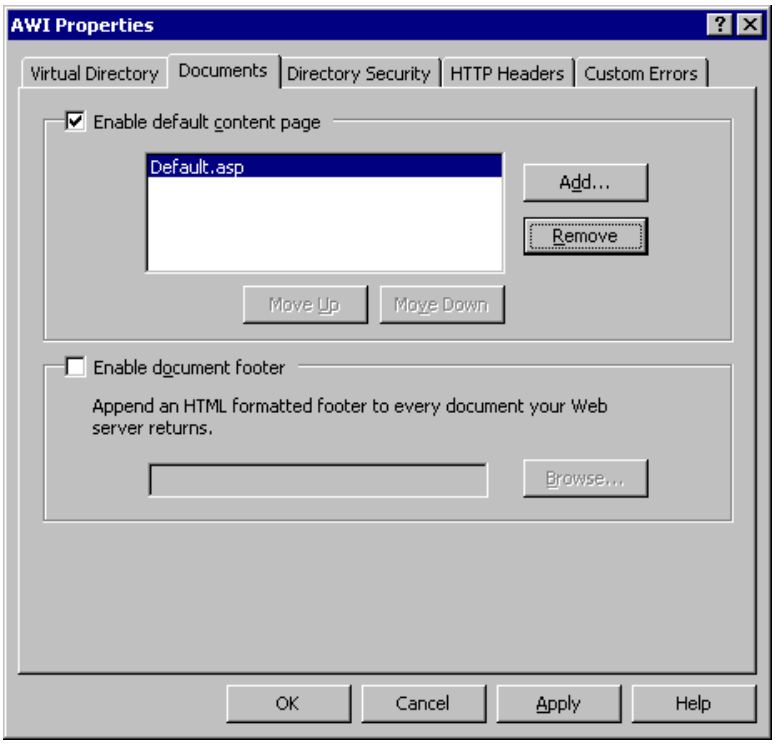
5. Right click on the newly created virtual directory, located under the web root of your website server and select **Properties** from the context menu.

6. In the **Virtual Directory** tab of the **Properties** dialog, check the **Read**, **Log Visits** and **Index this resource** checkboxes. Make sure that all the other checkboxes are unchecked. In the **Execute Permissions** list box, select **Scripts only**.



Screenshot 120 - Setting Virtual Directory properties

7. Access the **Documents** tab. Remove all the default documents except for **default.asp**.



Screenshot 121 - Specify default document

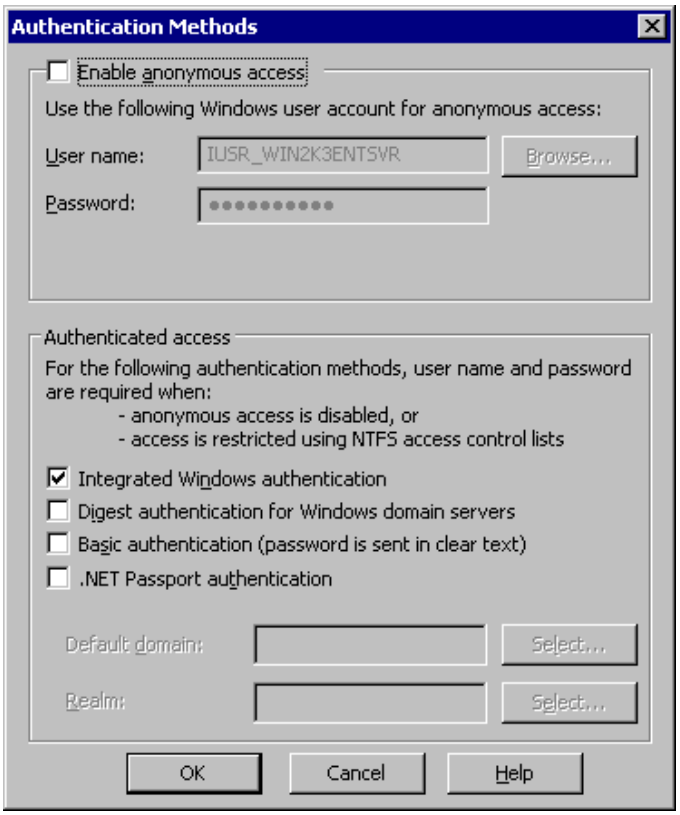
8. Access the **Directory Security** tab and click on the **Edit** button in the **Authentication and access control** group.

NOTE: Since the Archive Web Interface provides access to all the emails archived by GFI 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 the users for their username 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, use Basic authentication.

9. Check the **Integrated Windows authentication** checkbox (recommended if installed on the internal network) OR **Basic Authentication** checkbox (if installed in the DMZ). Ensure that the **Enable anonymous access** checkbox is unchecked.

NOTE 1: 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 create usernames and passwords on that local machine. For more information on securing IIS, please review the IIS documentation.

NOTE 2: Be sure not to allow anonymous access.



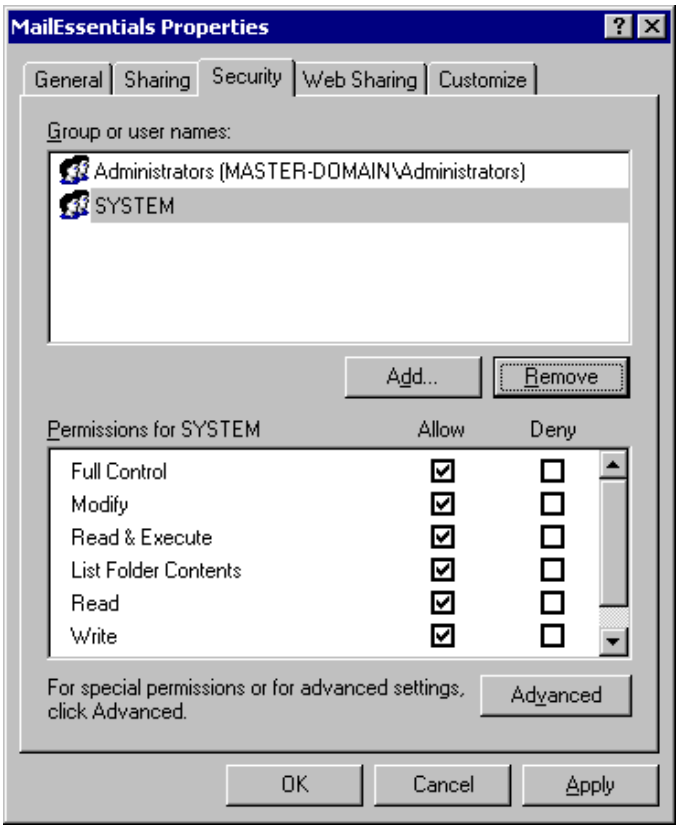
Screenshot 122 - Select authentication method

10. Press the **OK** button to close the properties dialog. The Virtual Directory has been setup and you can now test access to it.

Restrict access to the AWI by using NTFS permissions

The following steps show how to secure access to AWI:

1. Open up Explorer and navigate to the GFI MailEssentials folder. Right click on the GFI MailEssentials folder and select **Properties** and then the **Security tab**.



Screenshot 123 - Setting permissions

2. 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 screenshot 100. Click the **OK** button. You have now secured the Archive Web Interface.

NOTE: Since GFI MailEssentials services (attendant and engine) and IIS services all run using the localsystem account, please make sure to include the **SYSTEM** account in the list of users/groups allowed to access the Archive Web Interface. Also make sure that the permissions for the SYSTEM account are set to Full Control, otherwise the required services will fail to start (i.e. GFI MailEssentials will not work).

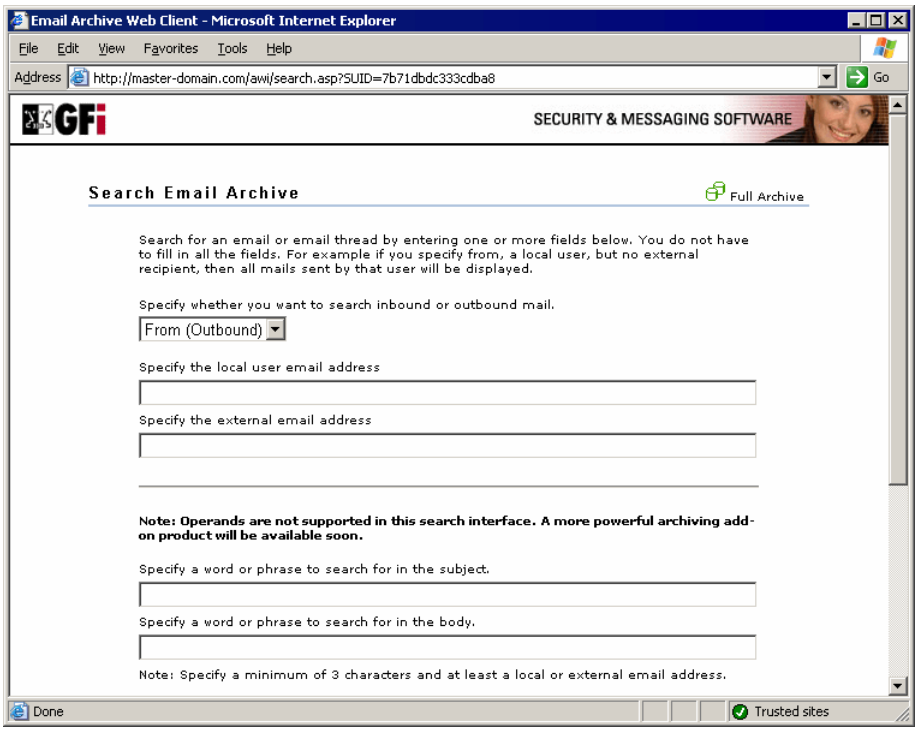
Accessing the AWI

To access the AWI you need to configure IIS as outlined in the previous section, and then load Microsoft Internet Explorer. In the address bar enter the following and press the Enter key:

http://<machine_name>/<awi_virtual_folder_name>

For example: http://master-domain.com/awi/

By default the AWI will load the search page. To access the full archive click on the **Full Archive** link in the top right corner.



Screenshot 124 – Archive Web Interface (AWI) search page

Configuring the Search Mail Archive node

NOTE: The **Search Mail Archive** node feature is disabled if you installed GFI MailEssentials on a Microsoft Exchange Server 2007 machine, since the **Archive Web Interface (AWI)** feature is not compatible with x64 machines.

To configure the **Search Mail Archive** node, so as to be able to access the AWI from the GFI MailEssentials configuration, follow these steps:

1. Make sure that you have configured IIS correctly as outlined in the previous sections to access the AWI.

2. Right click on the **Email Management > Mail Archiving > Search Mail Archive** node and select **Properties** from the context menu.

3. In the **Search Mail Archive Properties** dialog, specify the address to access the AWI in the **Archive Web Interface address** edit box using the following format:

http://<machine_name>/<awi_virtual_folder_name>

For example: http://master-domain.com/awi/

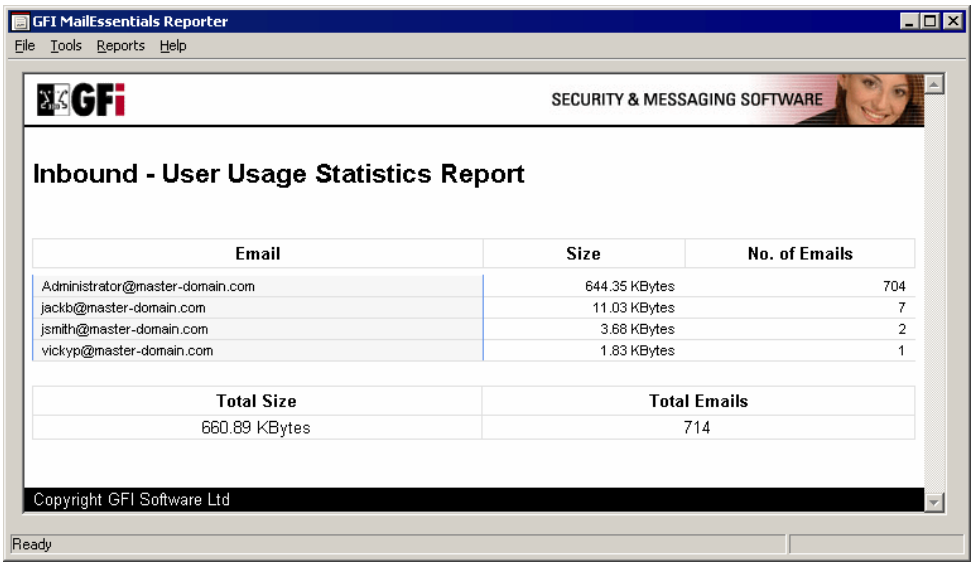
4. Click the **OK** button.

5. The **Search Mail Archive** node will load the AWI in the right pane of the GFI MailEssentials configuration.

Generating email reports

Introduction

The GFI MailEssentials Reporter allows you to generate useful reports regarding inbound and outbound email traffic. For example, you can generate reports on the number of emails sent per user, per domain, or just daily statistics of email traffic.



Screenshot 125 - 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 database 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, right click on the **Email Management > Reporting** node and select **Properties** from the context menu.

2. The **Reporting Properties** dialog is displayed. Click on the **Configure** button.

3. Specify Microsoft Access or Microsoft SQL server.

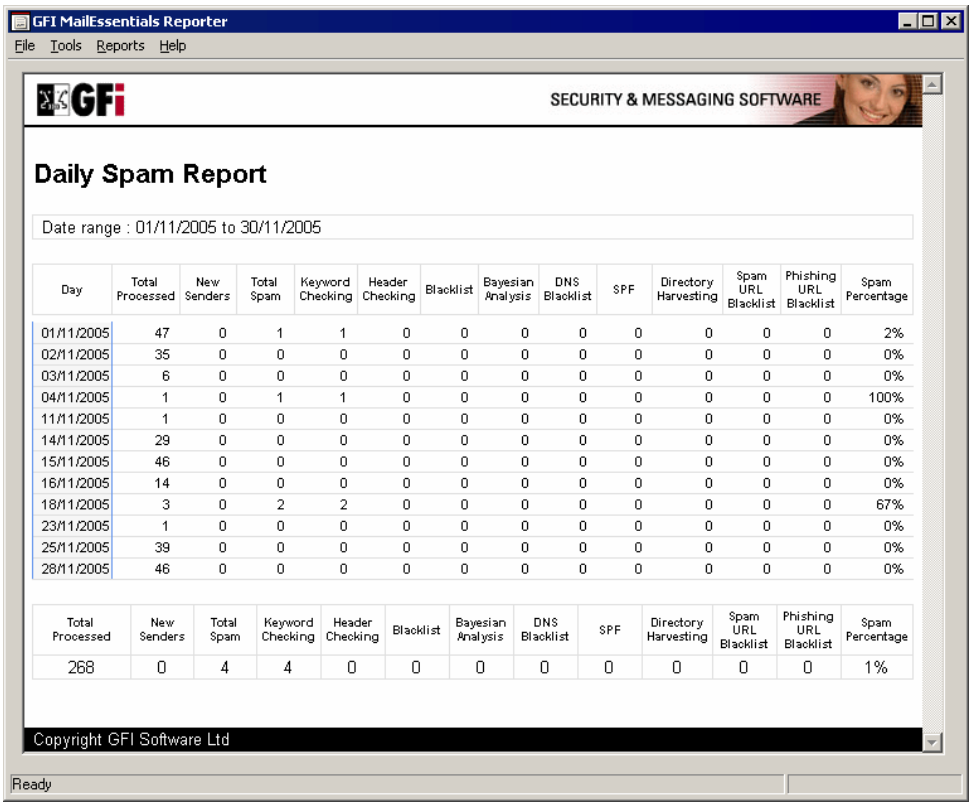
4. If you specify Microsoft Access, specify the file name and location.

5. If you specify Microsoft SQL server, specify the server name, logon credentials and database.

6. Click the **Test** button to ensure you have configured the database correctly. Click the **OK** button to save your settings.

Daily spam report

The Daily Spam Report shows you the total emails processed, total spam email caught, the spam percentage of total emails processed and how many spam emails were caught by each individual anti-spam feature. Each row in the report represents a day.



Day	Total Processed	New Senders	Total Spam	Keyword Checking	Header Checking	Blacklist	Bayesian Analysis	DNS Blacklist	SPF	Directory Harvesting	Spam URL Blacklist	Phishing URL Blacklist	Spam Percentage
01/11/2005	47	0	1	1	0	0	0	0	0	0	0	0	2%
02/11/2005	35	0	0	0	0	0	0	0	0	0	0	0	0%
03/11/2005	6	0	0	0	0	0	0	0	0	0	0	0	0%
04/11/2005	1	0	1	1	0	0	0	0	0	0	0	0	100%
11/11/2005	1	0	0	0	0	0	0	0	0	0	0	0	0%
14/11/2005	29	0	0	0	0	0	0	0	0	0	0	0	0%
15/11/2005	46	0	0	0	0	0	0	0	0	0	0	0	0%
16/11/2005	14	0	0	0	0	0	0	0	0	0	0	0	0%
18/11/2005	3	0	2	2	0	0	0	0	0	0	0	0	67%
23/11/2005	1	0	0	0	0	0	0	0	0	0	0	0	0%
25/11/2005	39	0	0	0	0	0	0	0	0	0	0	0	0%
28/11/2005	46	0	0	0	0	0	0	0	0	0	0	0	0%

Total Processed	New Senders	Total Spam	Keyword Checking	Header Checking	Blacklist	Bayesian Analysis	DNS Blacklist	SPF	Directory Harvesting	Spam URL Blacklist	Phishing URL Blacklist	Spam Percentage
268	0	4	4	0	0	0	0	0	0	0	0	1%

Screenshot 126 - Daily spam report

The daily spam report can be generated via the **Reports > Daily Spam** menu option. This will bring up the **Daily Spam 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 and so on. For example, if you sort on keyword checking, it will list the days on which most emails were caught via the keyword checking at the top.

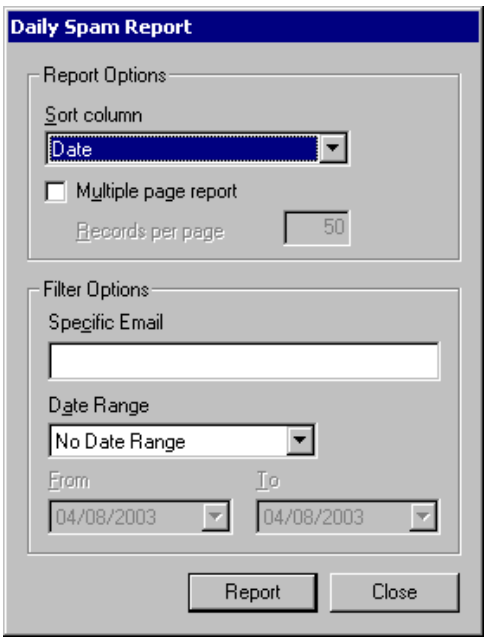
Multi Page report: allows you to specify the number of days you wish to display on each page.

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.

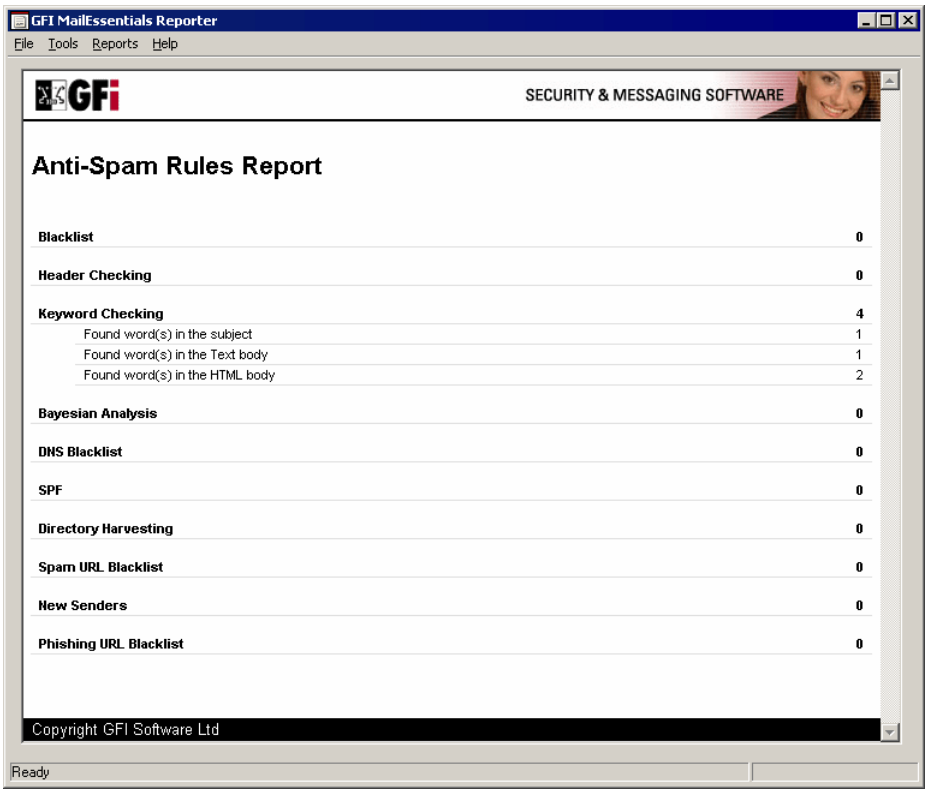
When you have specified the report options, click on the **Report** button to start generating the report. The report will be shown in the main window.



Screenshot 127 – Daily Spam Report options dialog

Anti-Spam rules report

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



Screenshot 128 – Anti-spam rules report

The Anti-spam rules report can be generated via the **Reports > Anti-Spam** rules menu option. This will bring up the **Anti-Spam Rules 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.

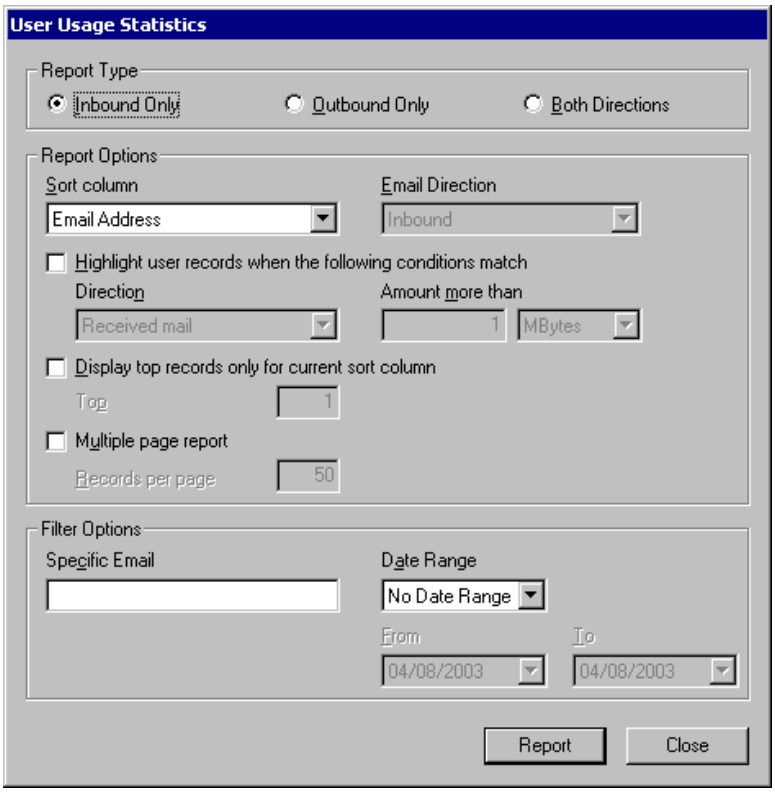
Date range: This filter option allows you to limit the report to a specific date range.

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.

Screenshot 129 – Anti-Spam Rules Report options dialog

User usage statistics

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.



Screenshot 130 - User usage statistics filter dialog

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 then X number of emails or X number of megabytes of email.

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

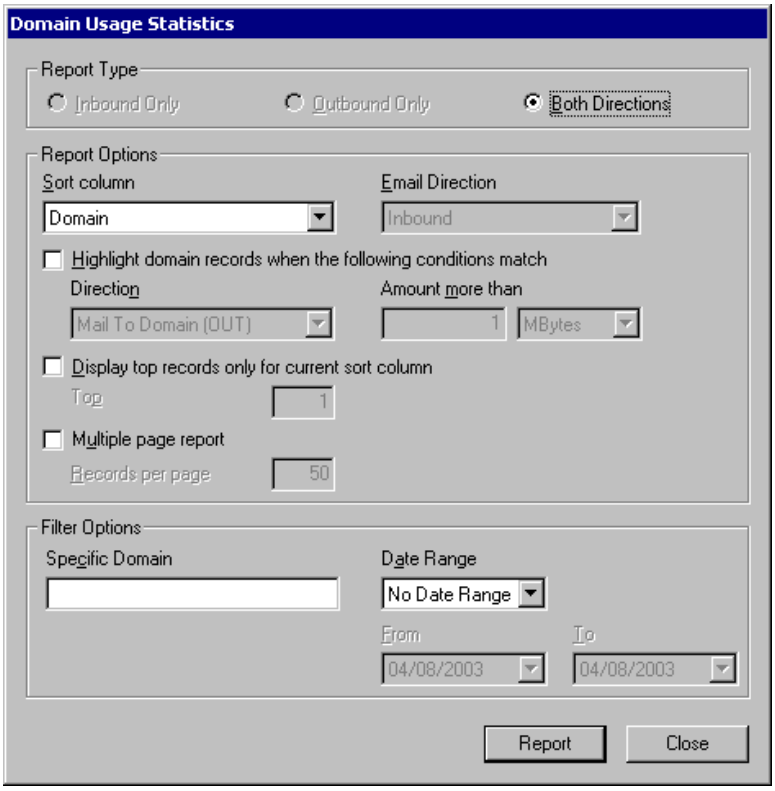
Specific email: Allows you to limit the report to a specific email address.

'Date range': 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 domain usage statistics report gives you an overview of how many emails are sent or received to non-local domains.



Screenshot 131 - Domain usage statistics filter dialog

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 then X number of emails or X number of megabytes of email.

List to: Allows you to list only the top X number of domains in the report.

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

Filter options

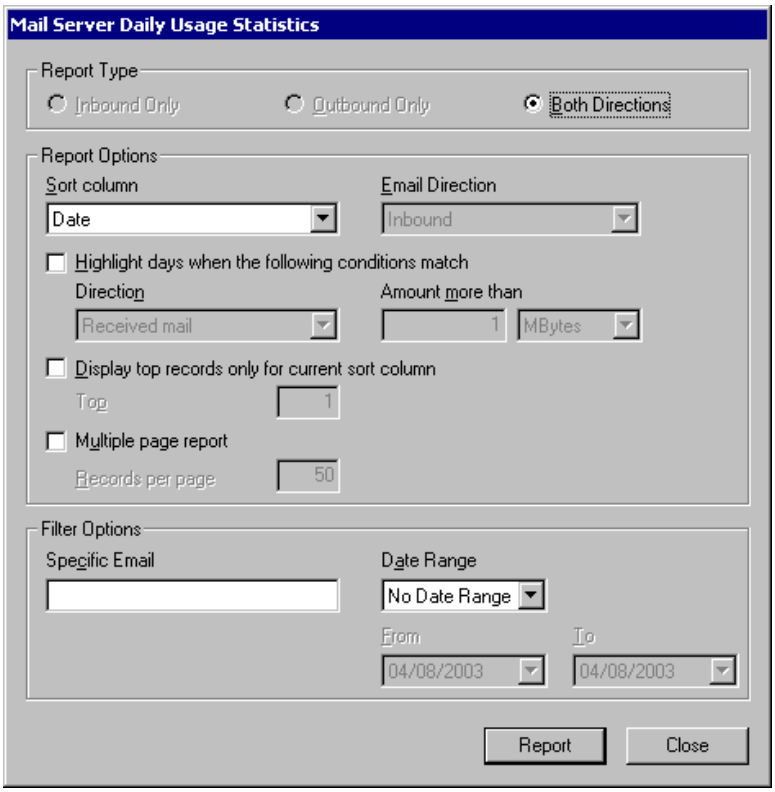
Specific domain: Allows you to limit the report to a specific domain.

Date range: 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 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.



Screenshot 132 - Mail server daily usage statistics filter dialog

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.

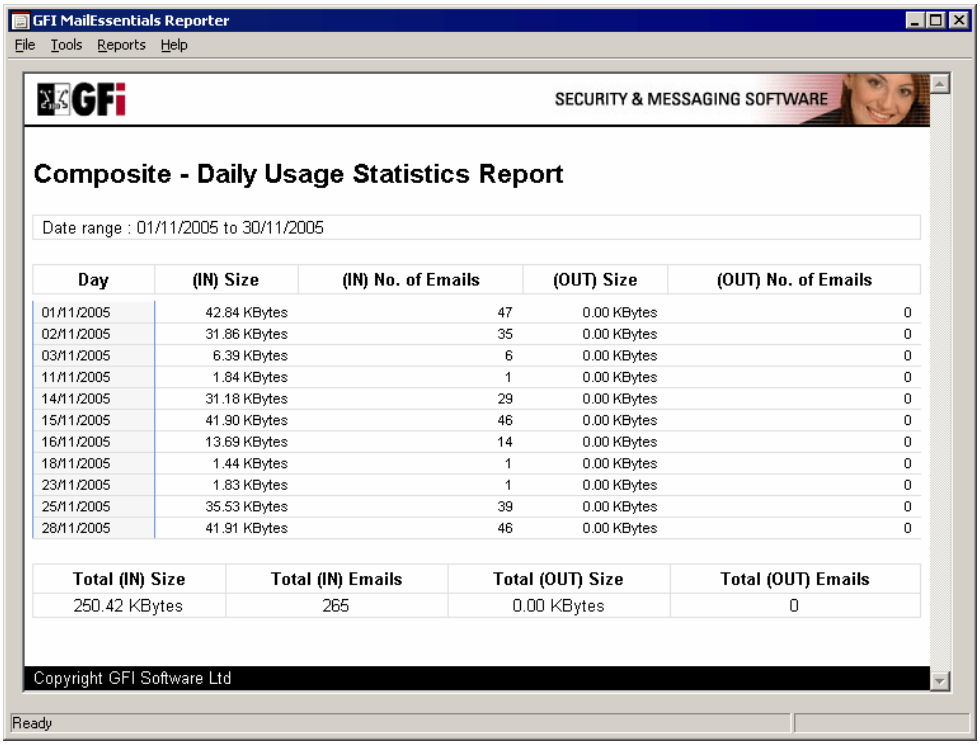
For example, if you sort on number of emails, the days on which you sent or received most email will be listed at the top.

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 then X number of emails or X number of megabytes of email.

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.



Screenshot 133 - The daily usage statistics report

Filter options

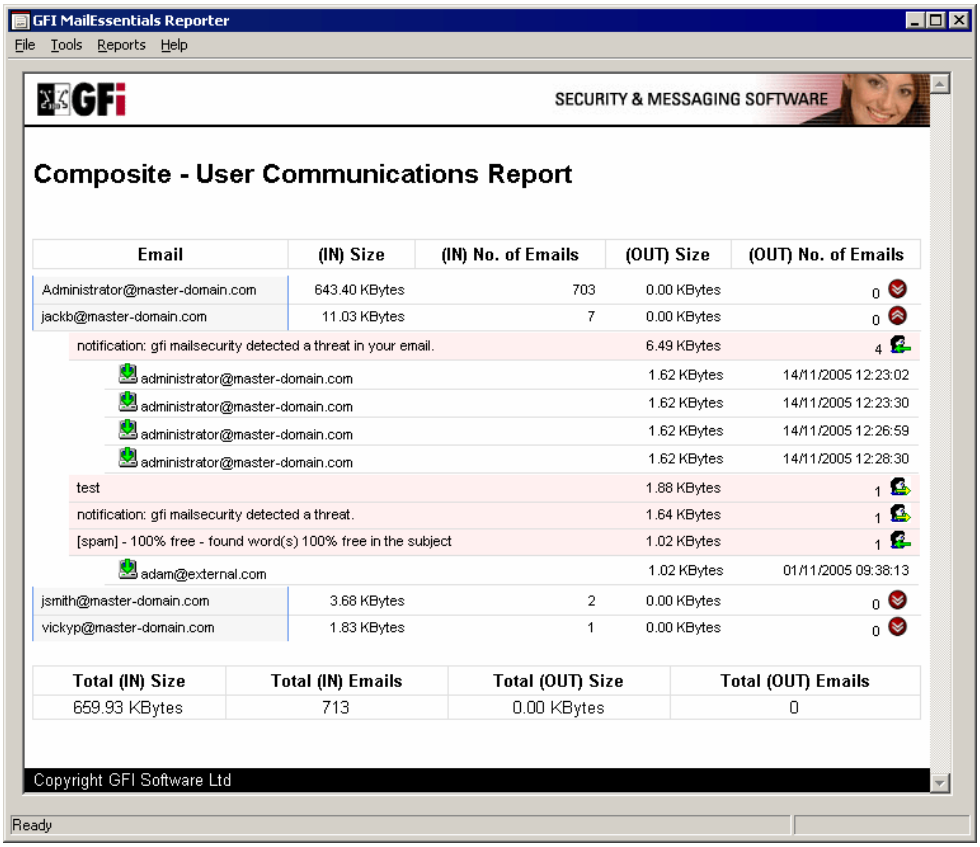
Specific email: Allows you to limit the report to a specific domain.

Date range: 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

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 emails. Mail with the same subject is grouped. These emails can be further expanded to reveal when and to whom, email with that subject was sent.



Screenshot 134 - The user communications report shows exact email trail

The User communications report can be generated via the **Reports > User Communications** menu 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 email 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 email 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 then X number of emails or X number of megabytes of email.

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.

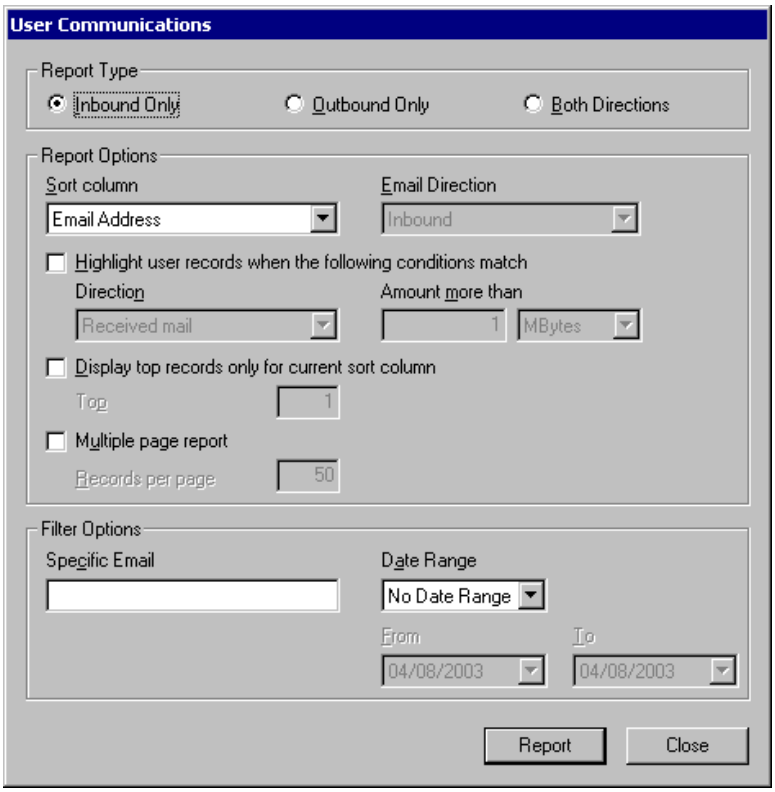
Filter options

Specific email: Allows you to limit the report to a specific email address.

Date range: 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 you limit the user communications report to a specific user or to a particular date range.



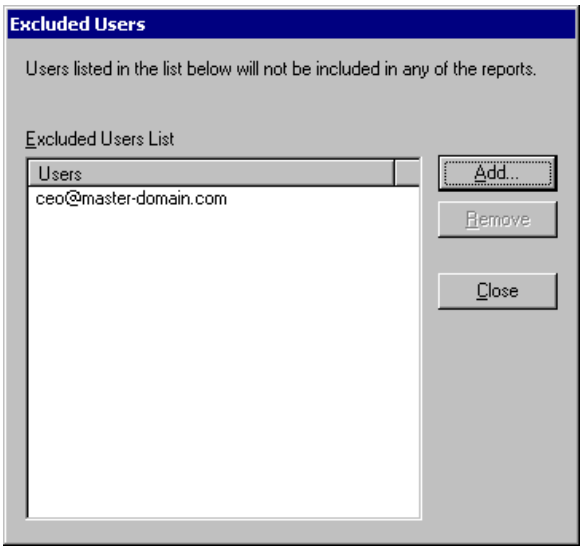
Screenshot 135 - User communications filter dialog

Miscellaneous options

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

Excluded users

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 List** menu option.



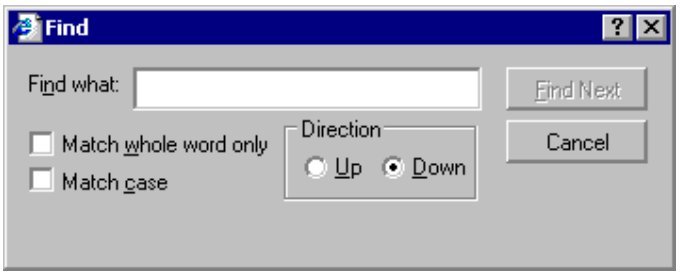
Screenshot 136 - Excluded users dialog

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.

To remove a user from the exclusion list, select it from the list and click on the **Remove** button.

Find

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



Screenshot 137 - Find dialog

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. Before you print the report, you can preview how it will look like on paper by using the print preview, accessible from the **File > Print Preview** menu option.

Saving reports

The GFI MailEssentials Reporter allows you to save reports generated to a desired location. To save reports follow these steps:

1. Generate the report you want by using the options under the **Reports** menu.

2. Click on **File > Save As** menu option.

3. A dialog is displayed. Select the location where you want to save the report and in the **File name** edit box specify the name you want to give this report.

4. Click the **Save** button.

5. The report will be saved to the location you selected inside a folder with the name you specified for the report. The folder contains two sub-folders, ‘graphics’ and ‘report’. The ‘report’ sub-folder contains the report files in HTML format. The ‘graphics’ sub-folder contains graphics which are displayed in the HTML report.

Configuring POP3 downloading

Should you use POP3 or SMTP to receive email?

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

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

Using POP3 to receive email

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 ISPs support POP3.

Advantages of using POP3 to retrieve email

- 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 Microsoft 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 email 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 email message's header For a single recipient, this is not a problem. If the email is in your mailbox, you know it is for you. However, if all email directed at a specific domain goes into the same mailbox, there may be no way of determining who the email 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 email 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 email

Simple Mail Transport Protocol (SMTP(RFC821)) is a server-to-server protocol for sending email across the Internet. Briefly, an email client will make a TCP connection to an ISP's SMTP server and upload an email 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.

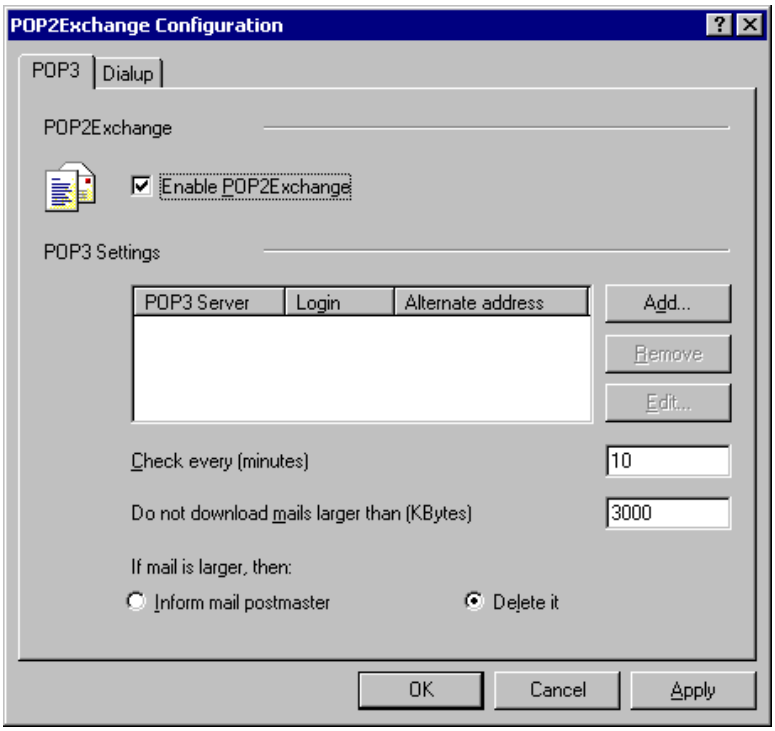
Disadvantages of using SMTP

- You need a public IP

Configuring the POP3 downloader

If you wish to receive email by downloading email from one or more POP3 mailboxes, you need to setup the POP3 downloader. To do this, follow these steps:

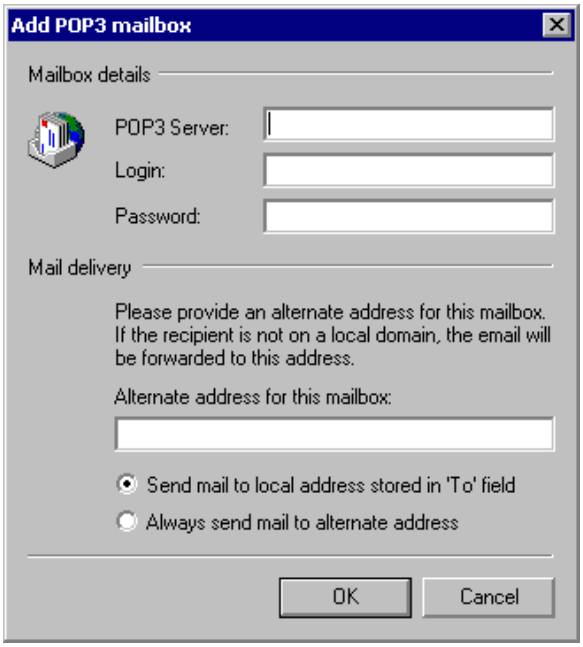
1. Highlight the **POP2exchange** node in the GFI MailEssentials configuration. In the right pane, double click on the **General** item. This will bring up the **POP2Exchange Configuration** dialog.



Screenshot 138 - The GFI MailEssentials pop3 downloader

2. Enable the POP3 downloader by checking the **Enable POP2Exchange** checkbox.

3. To add a POP3 mailbox from which you wish to download email, click the **Add** button. The **Add POP3 mailbox** dialog is displayed.



Screenshot 139 - 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

email accordingly. If the email analyzing fails, the email will be sent to the email address specified in the alternate address.

- **Send mail to alternate address:** Activate this option if you wish all email 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 email, or if you specified to forward all email to address.

4. When you are ready, click the **OK** button. 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

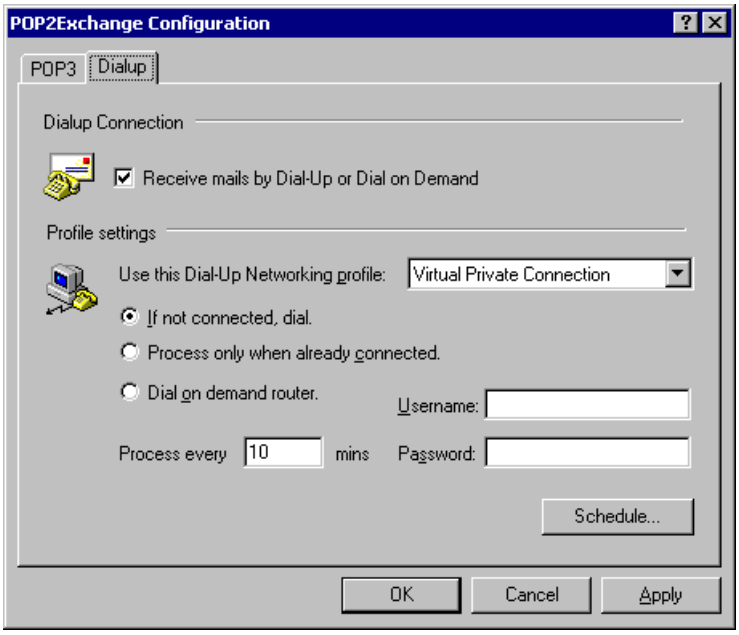
Check every .. minutes: Specify the download interval.

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

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

Dial up Connection options

To receive emails by dial-up, go to dial-up tab in the POP2Exchange dialog. Check the **Receive mails by Dial-Up or Dial on Demand** checkbox.



Screenshot 140 - 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

stating when the email should be sent / picked up. The dial-up networking profiles are setup 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.

Username: Enter the username 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 email 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 prompt GFI MailEssentials to pick up email at the specified interval, but without triggering a dial-up connection.

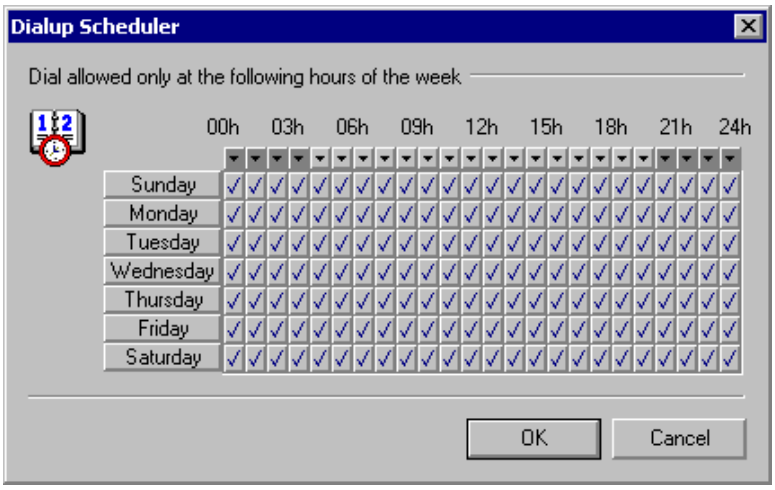
Process every (minutes): Enter the interval at which GFI MailEssentials must either dial-up or check if a connection already exists (depends on whether you set GFI MailEssentials to dial-up or to only process email when already connected).

Scheduler

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

1. Click on **Schedule**

2. Specify the hours when GFI MailEssentials should dial-up. A check mark indicates that GFI MailEssentials will dial out. A cross indicates that GFI MailEssentials will not dial out at this hour.



Screenshot 141 - Configuring when GFI MailEssentials should pick up email

Synchronizing configuration data

Introduction

If you have installed GFI MailEssentials on more than one server, you will want to keep the anti-spam and configuration data synchronized between the servers, so that email caught as spam on one server, would be caught as spam on another server as well if it passes through it.

To perform this synchronization procedure manually between the servers hosting GFI MailEssentials, is both tedious and error prone. For this reason, two new features have been introduced that make it really easy to keep multiple GFI MailEssentials installations synchronized. The new features are the following:

- Anti-spam Synchronization Agent: This service takes care of keeping anti-spam settings such as the Bayesian filter database, whitelist, auto whitelist and blacklist, synchronized between GFI MailEssentials installations using the Microsoft BITS service.
- GFI MailEssentials Configuration Export/Import Tool: This application allows you to export or import all the GFI MailEssentials configuration settings.

Anti-spam synchronization agent

The Anti-Spam Synchronization Agent works in the following manner:

1. A server machine hosting GFI MailEssentials is configured as the master server.

2. The other server machines, where GFI MailEssentials is installed, are configured as slave servers.

3. The slave servers upload an archive file, containing the anti-spam settings, to an IIS virtual folder hosted on the master server via the BITS service.

4. When the master server has collected all the slave servers anti-spam data, the data is extracted from the individual archives and merged into a new up to date anti-spam settings archive file.

5. The slave servers download this updated anti-spam settings archive file and take care of extracting it and updating the local GFI MailEssentials installation to make use of the new settings.

The next sections will thus show you how to prepare and configure the server machines hosting GFI MailEssentials, to be able to use the Anti-Spam Synchronization Agent feature.

NOTE 1: The servers that collaborate in the synchronization of anti-spam settings must all have GFI MailEssentials 14 installed.

NOTE 2: The files uploaded and downloaded by the anti-spam synchronization agent are compressed archives so as to limit the traffic on the network.

NOTE 3: The BITS service uses spare bandwidth to upload and download files, thus further reducing the impact on network traffic.

Configuring the master server

One of the server machines hosting GFI MailEssentials must be configured as the master server. The master server will host an IIS virtual folder, which will be used by the slave servers to upload and download an anti-spam settings archive file via the BITS service.

NOTE: Only one server can be configured as master server at any one time.

To configure a server as a master server, it must meet one of the following system specifications:

- Microsoft Windows 2003 with SP1 or later and IIS6.0 with BITS server extension installed. (Further information on how to install the BITS server extension is provided below)
- Microsoft Windows 2000 with SP3 or later and IIS5.0 with BITS server extension installed. (Further information on how to install the BITS server extension is provided below)

NOTE: A Microsoft Windows XP machine cannot be configured as master since Microsoft BITS server extension is not supported.

To configure a server as the master server, follow these steps:

1. First you need to install the Microsoft BITS server extension. For further information refer to the 'Installing BITS Server Extension on the master server' section later on.

2. Next you need to configure a virtual directory which will be used by the slave machines to upload and download anti-spam settings archive files. Load the **Internet Information Services (IIS) Manager** console from the **Administrative Tools** group.

3. Right click on the website of your choice and select **New > Virtual Directory** from the context menu.

4. Follow the **Virtual Directory Creation Wizard** steps to create the new virtual directory. You basically need to give a sensible name for the virtual directory, choose a location on disk where the contents for this virtual directory will be stored and in the permissions stage, check only the **Read** and **Write** checkboxes. All other checkboxes must be unchecked.

5. When the new virtual directory is created, right click on it and select **Properties** from the context menu. Access the **Directory Security** tab from the **Properties** dialog, and click on the **Edit** button in the **Authentication and access control** group.

6. Check the **Basic Authentication** checkbox and specify the **Default domain** and **Realm** to which the username and password used for authentication by the slave machines belong.

NOTE: Make sure that all other checkboxes are unchecked, especially Enable anonymous access.

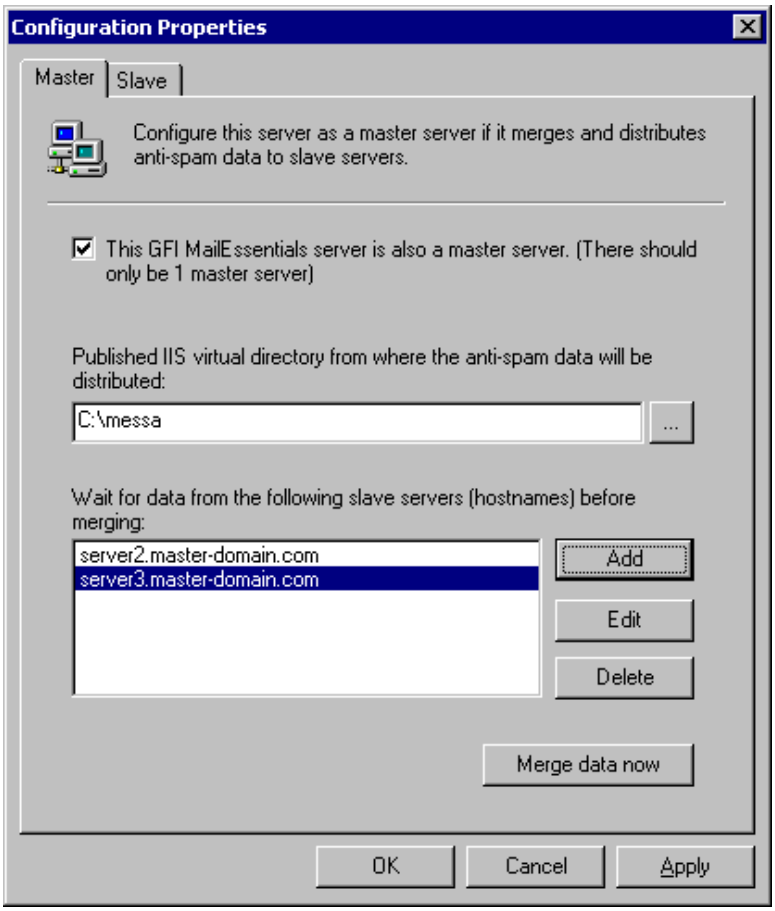
7. Click the **OK** button to close the **Authentication Methods** dialog.

8. Access the **BITS Server Extension** tab and check the **Allow clients to transfer data to this virtual directory** checkbox.

9. You now need to load the **Anti-Spam Synchronization Agent** configuration console. To do this, click on the **MailEssentials Anti-Spam Synchronization Agent** shortcut from the **GFI MailEssentials** program group in the **Start** menu.

10. Right click on the **Anti-Spam Synchronization Agent > Configuration** node and select **Properties** from the context menu.

11. The **Configuration Properties** dialog is displayed. From the **Master** tab check the **This GFI MailEssentials server is also a master server** checkbox.



Screenshot 142 – Configuring a master server

12. In the edit box specify the full path of the folder configured to hold the contents of the virtual directory created in step 3 above.

13. You now need to add the machine names of the slave servers which are going to be configured later on to upload to this master server. To add a slave server, click the **Add** button and enter the hostname in the **Server** edit box of the **Enter Server** dialog displayed. Click the **OK** button to add it to the list. Repeat this step to add all the other slave servers you have configured.

NOTE 1: Make sure that you configure all the machines you add to this list as slave servers. If not, the anti-spam synchronization agent on the master server will never merge the data, since it only merges the data when all the slave servers configured have uploaded their anti-spam settings archive file.

NOTE 2: You can configure the master to be slave at the same time. This means that the server will merge its own anti-spam settings data to the ones uploaded by the other slave servers. If this is the case, you need to add the master server hostname to the list of slave servers as well. For further information on how to configure a server machine to be a slave, refer to the 'Configuring a slave server' section.

To edit a slave server hostname, select it from the list and click the **Edit** button.

To remove a slave server hostname from the list, select it from the list and click the **Delete** button.

14. Click the **OK** button to save the settings.

Installing BITS Server Extension on the master server

This section will show you how to install the Microsoft Background Intelligent Transfer Service (BITS) Server Extension on the server machine you will configure as master for the Anti-spam Synchronization Agent feature.

To install BITS Server Extension on Microsoft Windows 2000 follow these steps:

1. Download the BITS v1.5 Server Component from the following Microsoft link and execute it on the master server:

http://www.microsoft.com/downloads/details.aspx?FamilyID=17967848-be86-4cd6-891c-ec8241611ad4&displaylang=en

2. Follow the **BITS Server Setup Wizard** instructions to finish the installation.

To install BITS Server Extension on Microsoft Windows 2003 follow these steps:

1. Load **Add or Remove Programs** from the **Control Panel**.

NOTE: Keep the Windows Server 2003 installation CD handy since you will be asked for it to perform the installation of the BITS server extension.

2. Click on the **Add/Remove Windows Components** tab.

3. In the **Windows Components Wizard** dialog select **Application Server** from the **Components** list and click the **Details** button.

4. From the **Application Server** dialog, select **Internet Information Services (IIS)** from the **Subcomponents of Application Server** list and click the **Details** button.

5. Check the **Background Intelligent Transfer Service (BITS) Server Extension** checkbox from the **Subcomponents of Internet Information Services (IIS)** list and click the **OK** button.

6. Click the **OK** button once more to close the **Application Server** dialog.

7. In the **Windows Components Wizard** dialog click the **Next** button. The installation process will start copying the required files.

8. When the installation is ready click the **Finish** button to close the **Windows Components Wizard**.

Configuring a slave server

A server machine hosting GFI MailEssentials, which is configured as a slave server, will upload and download anti-spam settings archive files from the master server using the BITS service.

To configure a server as a slave server, it must meet one of the following system specifications:

- Microsoft Windows 2003 - It is recommend that you download the BITS 2.0 client update from the following Microsoft link:

  http://www.microsoft.com/downloads/details.aspx?familyid=3FD31F05-D091-49B3-8A80-BF9B83261372&displaylang=en

- Microsoft Windows 2000 with SP3 or later – You need to download and install the BITS 2.0 client from the following Microsoft link:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=3ee866a0-3a09-4fdf-8bdb-c906850ab9f2&DisplayLang=en

- Microsoft Windows XP Professional – You need to download and install the BITS 2.0 client from the following Microsoft link:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=b93356b1-ba43-480f-983d-eb19368f9047&DisplayLang=en

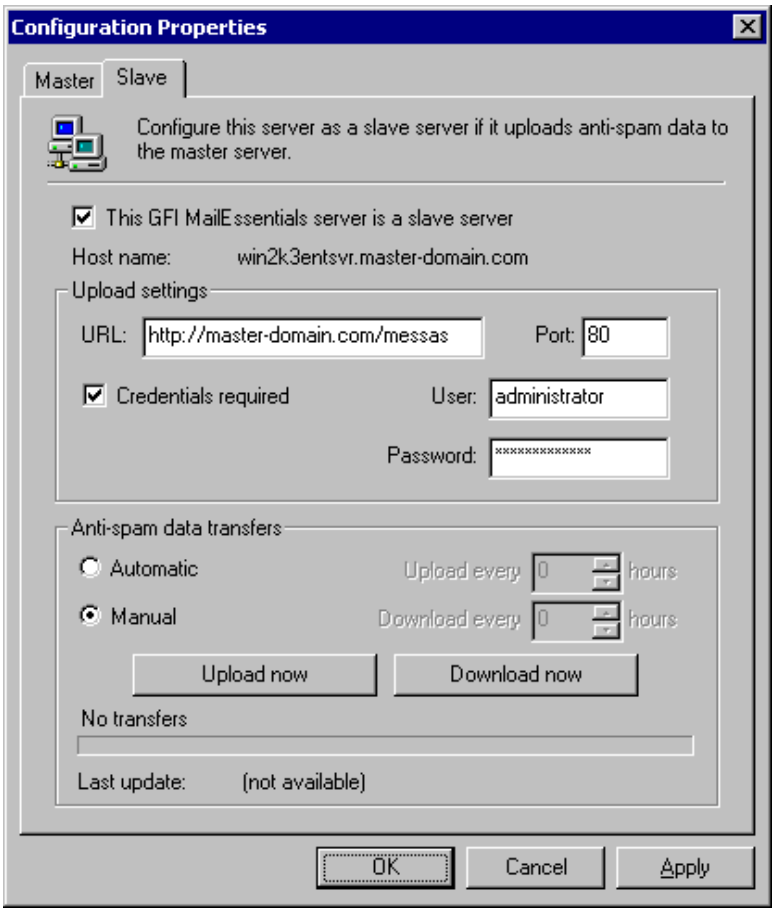
To configure a server as a slave server you need to do the following:

1. Meet the system requirements outlined above and have the latest BITS client installed on the server machine.

2. Click on the **GFI MailEssentials Anti-Spam Synchronization Agent** shortcut from the **GFI MailEssentials** program group in the **Start** menu, so as to load the **Anti-Spam Synchronization Agent** configuration console.

3. Right click on the **Anti-Spam Synchronization Agent > Configuration** node and select **Properties** from the context menu.

4. The **Configuration Properties** dialog is displayed. Access the **Slave** tab and check the **This GFI MailEssentials server is a slave server** checkbox.



Screenshot 143 – Configuring a slave server

5. In the **URL** edit box specify the full URL to the virtual directory hosted on the master server, as you configured in steps 2 to 8 of the 'Configuring the master server' section.

For example: 'http://master-domain.com/messas'

In the **Port** field you need to specify the port on which the master server accepts HTTP communications. By default it is set to port 80 which is the standard port used for HTTP.

6. Check the **Credentials required** checkbox and specify the user and password you want to use to authenticate with the master server, in the **User** and **Password** edit boxes respectively.

7. You now need to decide whether you want the anti-spam data to be synchronized automatically or manually via this tab.

8. If you want to upload and download the anti-spam settings archive file manually, select the **Manual** option. To upload the anti-spam settings of the slave server to the master server, you need to click the **Upload now** button. To download the updated merged anti-spam settings from the master server, you need to click the **Download now** button.

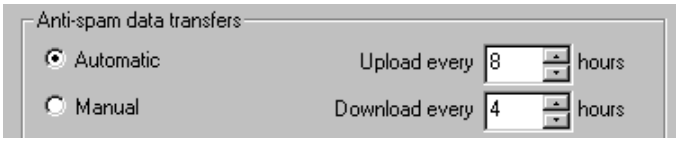
9. To configure the anti-spam synchronization to occur automatically, select the **Automatic** option. In the **Upload every** field specify the upload interval in hours, which determines how often you want the slave server to upload its anti-spam settings to the master server. In the **Download every** field you need to specify the download interval in

hours, which determines how often the slave server checks for updates on the master server and downloads them if any.

NOTE 1: The hourly interval for upload and download cannot be set to the same value. The hourly interval can be set to any value between 1 and 240 hours.

NOTE 2: It is suggested that you configure the download interval to a smaller value than the upload interval. So for example the download interval is set to 3 hours, while the upload interval is set to 4 hours. This way downloads are more frequent than uploads.

NOTE 3: It is suggested that you set the same interval settings for all the slave servers you have configured.



Screenshot 144 – Upload / download hourly interval setting

10. Click the **OK** button to save the settings.

GFI MailEssentials Configuration Export/Import Tool

The GFI MailEssentials Configuration Export/Import Tool is useful when you want to configure a new GFI MailEssentials installation with the same exact settings of an already working GFI MailEssentials installation.

The above procedure can be accomplished in three easy steps:

1. Run the GFI MailEssentials Configuration Export/Import Tool on the working GFI MailEssentials machine, to export all the configuration settings to a destination folder you choose.

2. Copy the exported settings to the machine where you have recently installed GFI MailEssentials.

3. Run the GFI MailEssentials Configuration Export/Import Tool and choose to import the settings you have just copied.

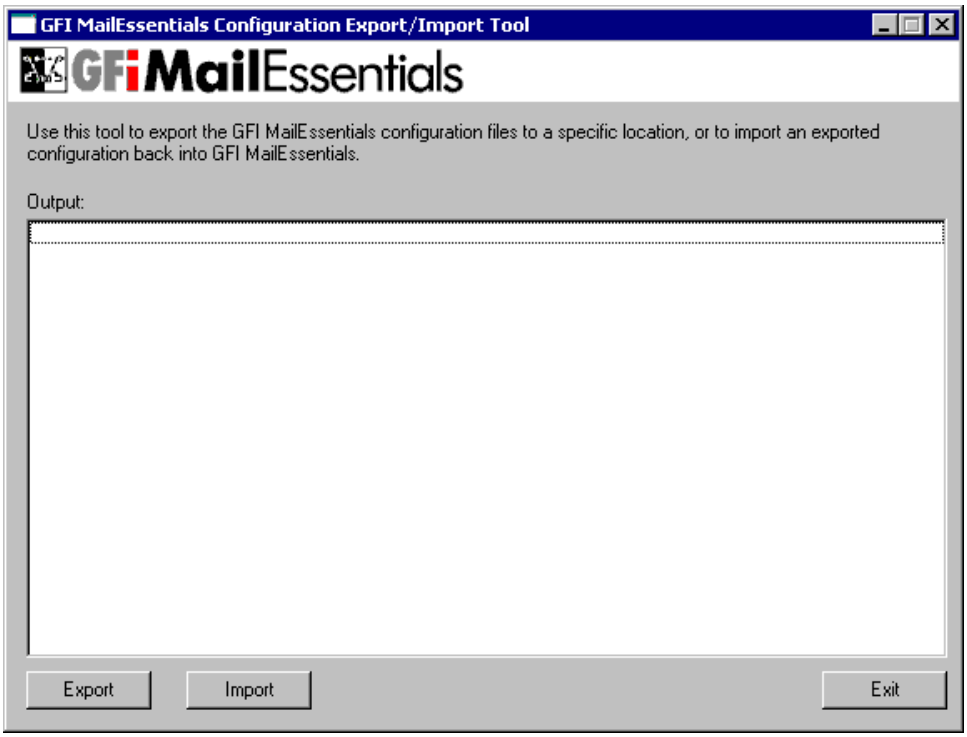
NOTE: When importing settings, the current GFI MailEssentials installation settings will be overwritten.

Exporting GFI MailEssentials configuration settings

To export the configuration settings of a GFI MailEssentials installation, follow these steps:

1. Double click on the 'meconfigmgr.exe' executable, found in the root folder of the GFI MailEssentials installation.

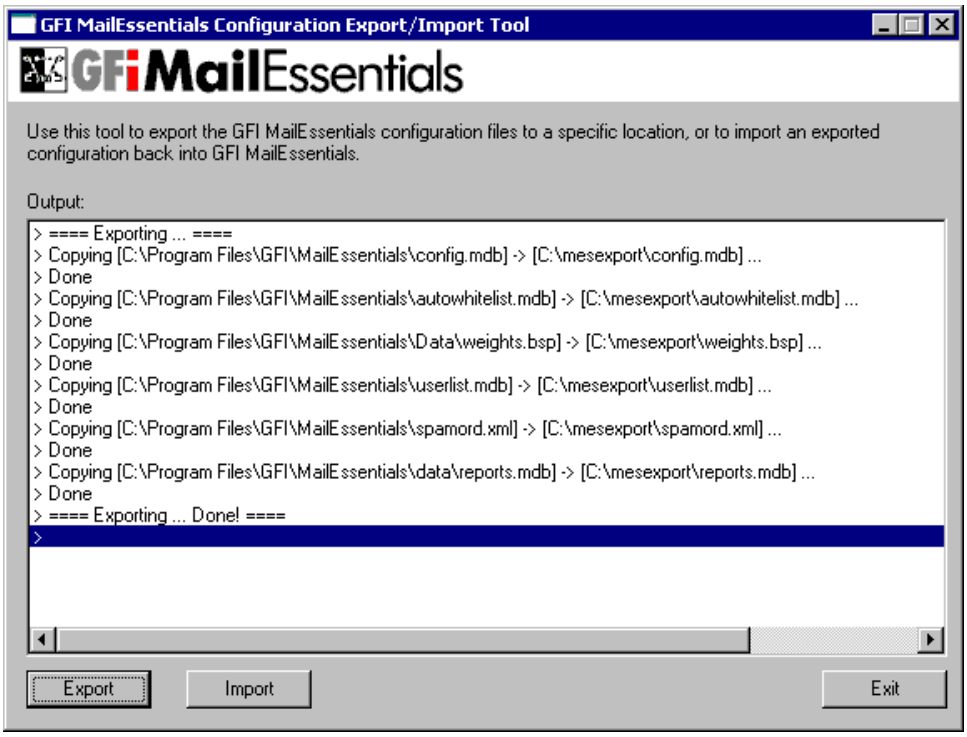
2. The GFI MailEssentials Configuration Export/Import Tool will load. Click the **Export** button.



Screenshot 145 – GFI MailEssentials Configuration Export/Import Tool

3. The **Browse for Folder** dialog is displayed. Choose an empty folder where you want to export the GFI MailEssentials configuration settings and click the **OK** button.

4. The GFI MailEssentials configuration files will be copied to the destination you selected. The tool will display the export progress.



Screenshot 146 – Configuration settings exported successfully

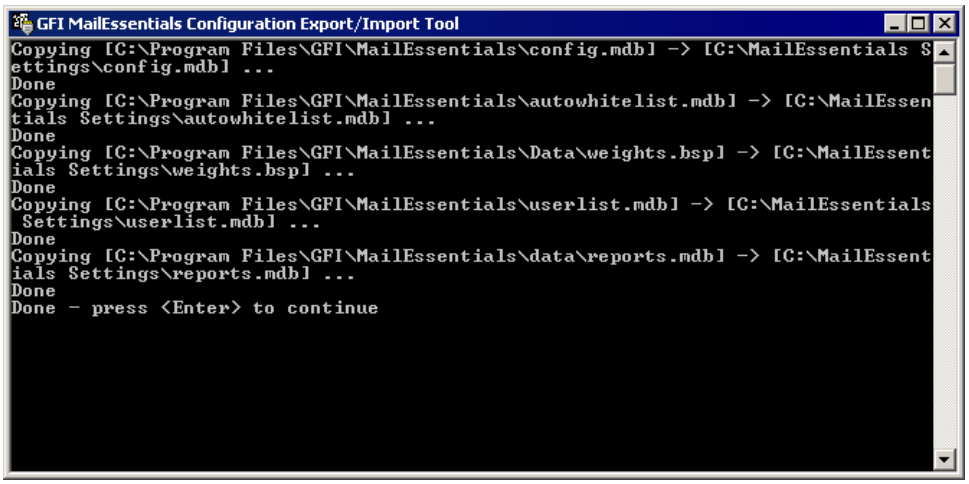
5. When **Exporting… Done** is displayed, all the settings have been exported. Click the **Exit** button. When prompted click the **Yes** button to close the export tool.

Exporting settings via the command line

You can also export the GFI MailEssentials settings via command line. From a command prompt, browse to the GFI MailEssentials installation root folder, then enter the following command:

```
meconfigmgr /export:"c:\MailEssentials Settings" /verbose /replace
```

The GFI MailEssentials settings will be copied to the "MailEssentials Settings" folder on drive C. Replace "C:\MailEssentials Settings" with the desired destination path. The /verbose switch instructs the tool to display progress while copying the files as shown in the screenshot below.



Screenshot 147 - Exporting settings via command line

The /replace switch instructs the tool to overwrite existing files in the destination folder.

Importing GFI MailEssentials configuration settings

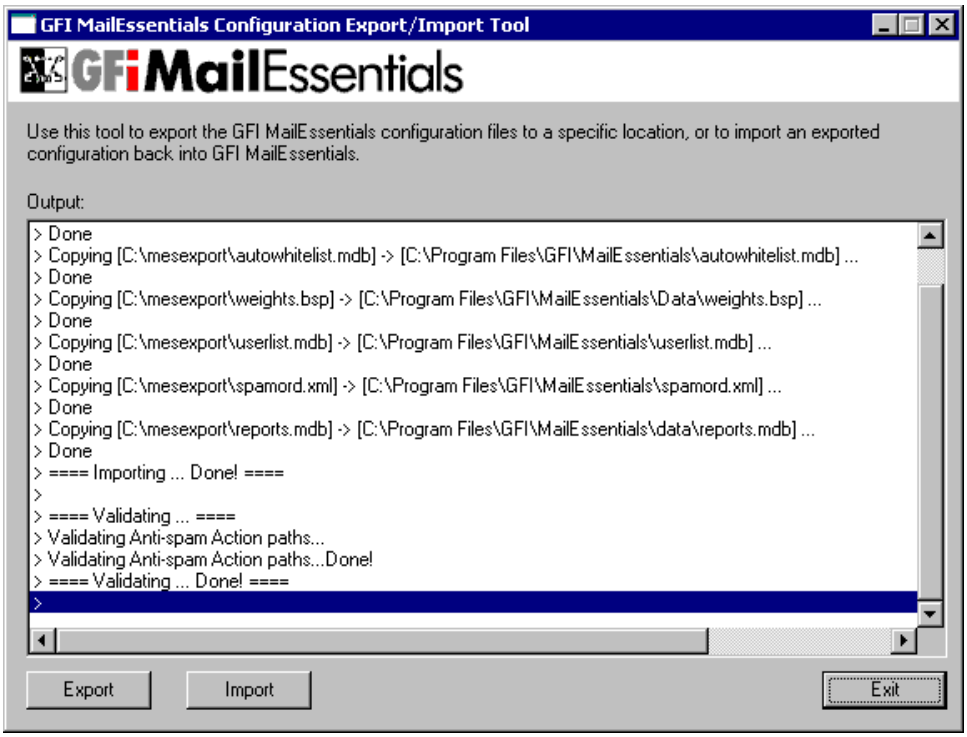
To import the configuration settings exported from another GFI MailEssentials installation, follow these steps:

1. Double click on the 'meconfigmgr.exe' executable, found in the root folder of the GFI MailEssentials installation.

2. The GFI MailEssentials Configuration Export/Import Tool will load. Click the **Import** button.

3. The **Browse for Folder** dialog is displayed. Choose the folder that contains the exported GFI MailEssentials configuration settings and click the **OK** button.

4. The tool will start the importation process, overwriting the local GFI MailEssentials configuration files with the ones in the folder you selected in step 3 above. The tool will display the import progress.



Screenshot 148 – Configuration settings imported successfully

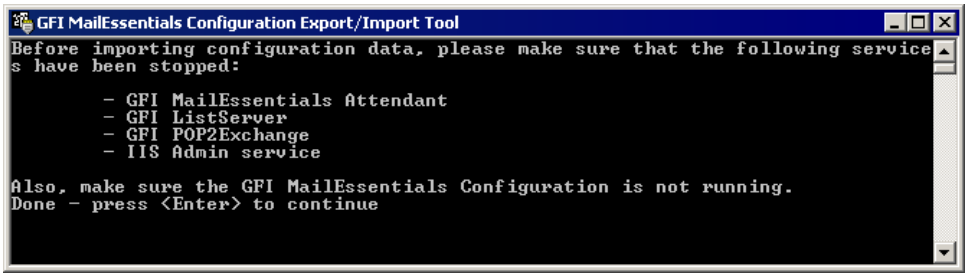
5. When **Validating… Done** is displayed, all the settings have been imported. Click the **Exit** button. When prompted click the **Yes** button to close the import tool.

Importing settings via the command line

You can also import the GFI MailEssentials settings via command line. From a command prompt, browse to the GFI MailEssentials installation root folder, then enter the following command:

```
meconfigmgr /import:"c:\MailEssentials Settings" /verbose /replace
```

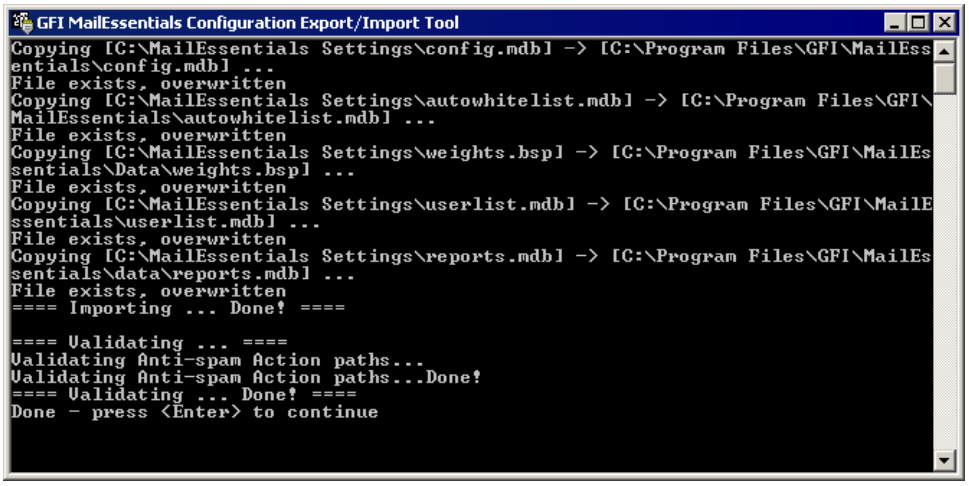
NOTE: To import settings, you first need to stop the IIS Admin Service and the GFI MailEssentials Attendant service. You also need to close any instance of the GFI MailEssentials Configuration. If you try to run the import tool and the above-mentioned services are not yet stopped, the prompt shown in the screenshot below is displayed.



Screenshot 149 - Stop these services before starting the import process.

The GFI MailEssentials settings will be copied from the "MailEssentials Settings" folder on drive C: to the proper location in the GFI MailEssentials installation path. Replace "C:\MailEssentials Settings" with the desired source path. The /verbose switch instructs

the tool to display progress while copying the files as shown in the screenshot below.



Screenshot 150 - Importing settings via command line

The /replace switch instructs the tool to overwrite existing files in the destination folder.

Miscellaneous options

General node

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

Version Information: Allows you to check what version you have installed and whether it's the latest.

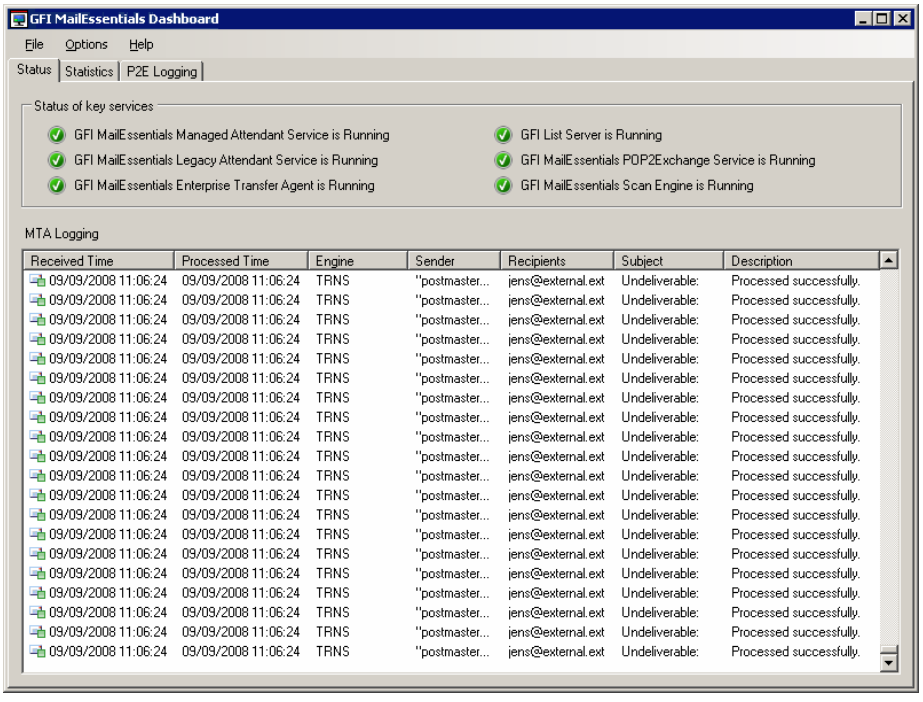
Licensing: Use this node to enter your License key.

Product patches: Shows you patches available.

GFI 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.

GFI MailEssentials Dashboard

Through the GFI MailEssentials Dashboard, you can view the activity of GFI MailEssentials as well as statistics. The POP collector service can be monitored from the **P2E Logging** tab.



Screenshot 151 - GFI MailEssentials Dashboard

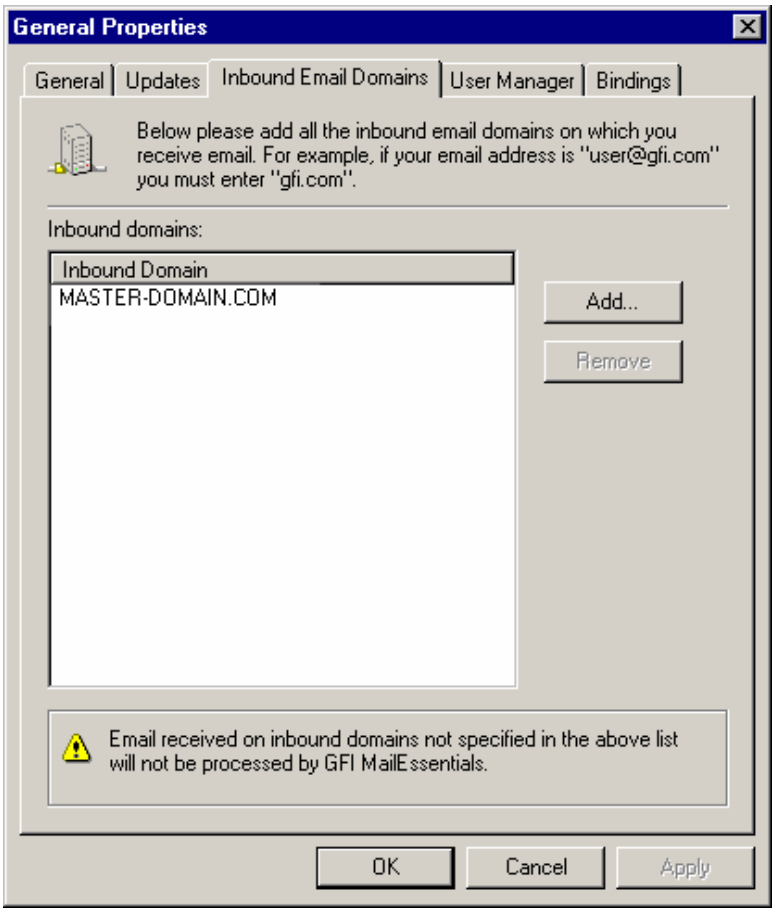
Configuring a fake Non Delivery Report (NDR)

In anti-spam actions, you can enable a fake NDR to be sent once a spam email 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 inbound email domains

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



Screenshot 152 - Adding an inbound email domain

1. Right click on the **General** node and select **Properties** from the context menu to access the **General Properties** dialog.

2. Access the **Inbound email domains** tab.

3. To add new inbound email domains, click the **Add…** button. Specify a domain in the **Enter Domain** dialog and click on the **OK** button.

4. To remove inbound email domains, select the domain you want to remove from the **Local Domain** list, and click on the **Remove** button. Click the **Yes** button in the confirmation dialog.

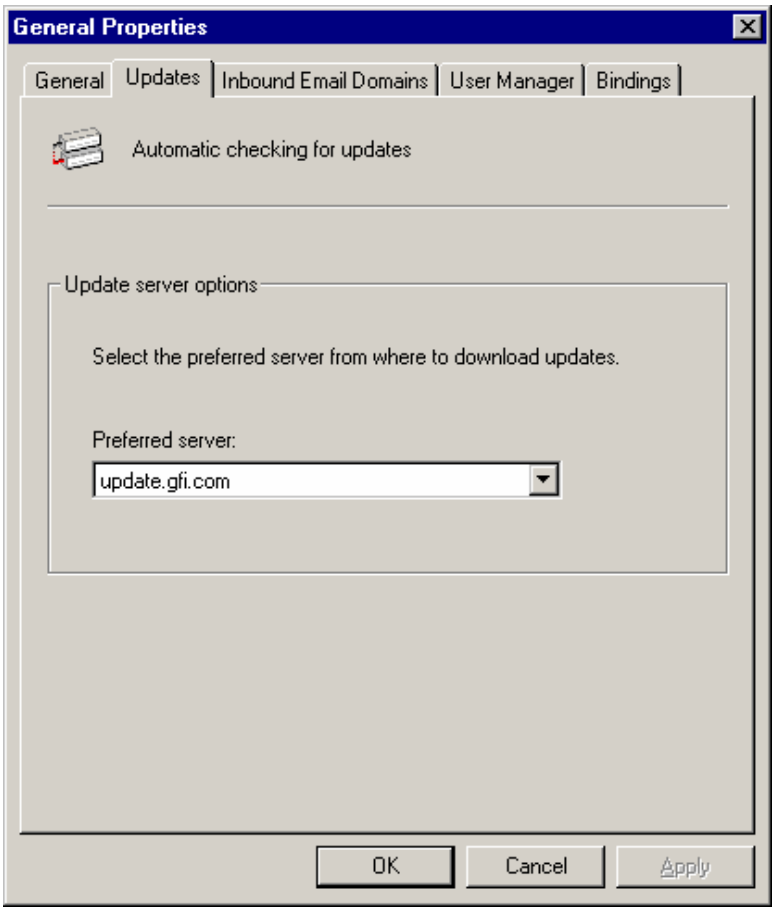
This feature is handy because in some cases you might want to configure local email routing in IIS differently, i.e. add domains which are local for email routing purposes but are not local for your mail server.

Selecting the server from where to download updates

The updates server is the server GFI MailEssentials uses to check for and download any Bayesian spam filter updates and Anti-Phishing updates. To select the updates server you want GFI MailEssentials to use, follow these steps:

1. Right click on the **General** node and select **Properties** from the context menu to access the **General Properties** dialog.

2. Access the **Updates** tab.



Screenshot 153 - Selecting the updates server

3. Select a server from the **Preferred server** list.

4. Click the **OK** button to save the new settings and close the **General Properties** dialog.

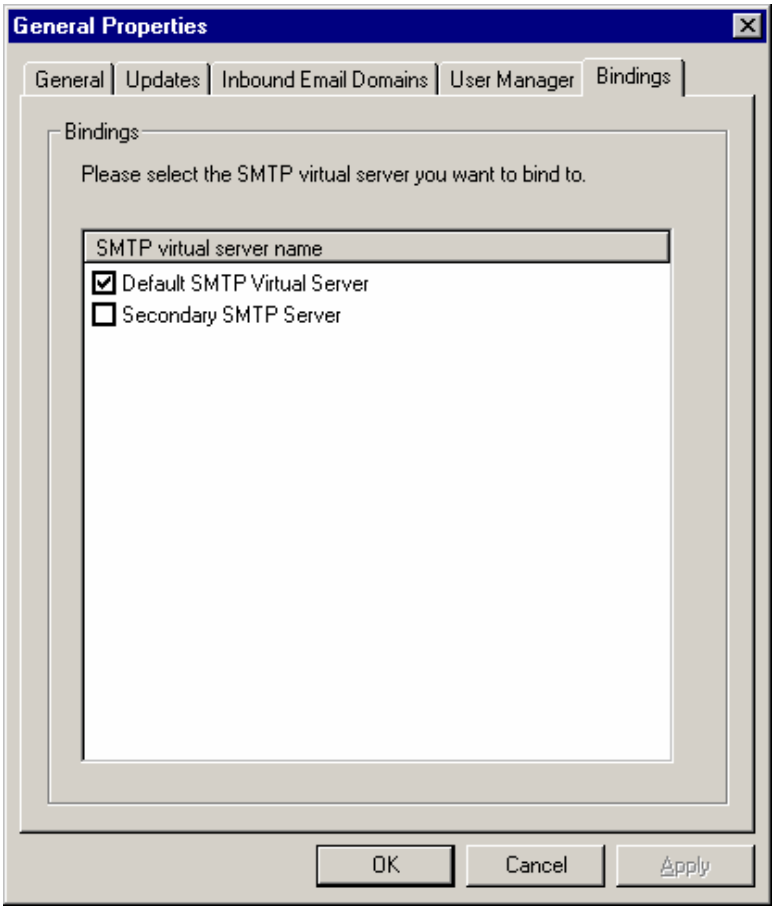
Selecting the SMTP Virtual Server to bind GFI MailEssentials

NOTE: The SMTP Virtual Server **Bindings** tab is not displayed if you installed GFI MailEssentials on a Microsoft Exchange Server 2007 machine.

If you have more than one SMTP Virtual Server configured and you want GFI MailEssentials to bind to a different SMTP Virtual Server, follow these steps:

1. Right click on the **General** node and select **Properties** from the context menu to access the **General Properties** dialog.

2. Access the **Bindings** tab.

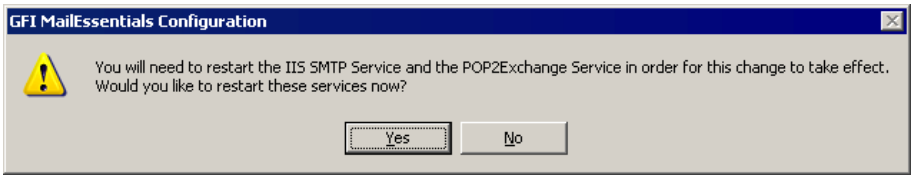


Screenshot 154 - SMTP Virtual Server Bindings

3. Select the checkbox of the SMTP Virtual Server you want GFI MailEssentials to bind to, from the **SMTP virtual server name** list.

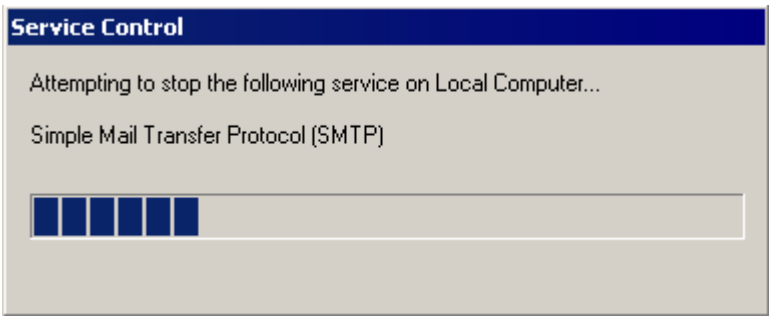
4. Click the **OK** button to save the new settings and close the **General Properties** dialog.

5. The GFI MailEssentials configuration will prompt you that certain services, such as the IIS SMTP Service, need to be restarted for the new settings to take effect. Click the **Yes** button to restart the required services now.



Screenshot 155 - Restart services prompt

6. A progress dialog will keep you informed of the services being restarted. When all the required services are restarted, GFI MailEssentials will be bound to the new SMTP Virtual Server you selected.



Screenshot 156 - Services restart progress

Remote commands

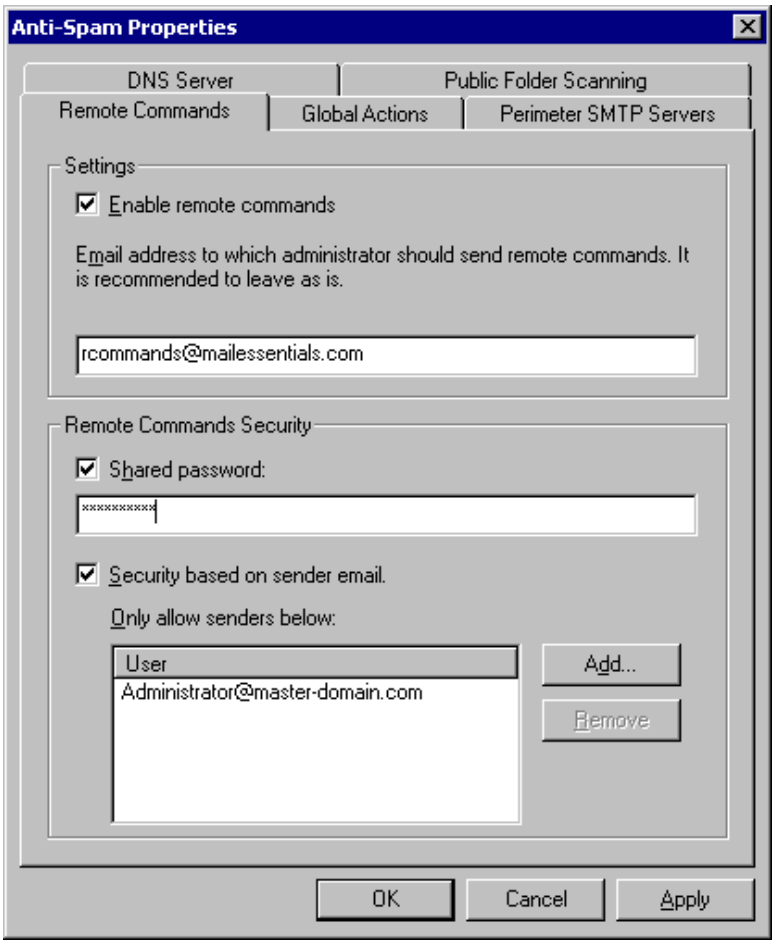
Remote commands make it easy to add domains or email addresses to the spam blacklist, as well as update the Bayesian filter with spam or ham (valid emails).

Remote commands function by sending an email to GFI MailEssentials: Simply address an email to rcommands@mailessentials.com (configurable) and GFI MailEssentials will recognize the email as containing remote commands and will 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 157 - Remote commands configuration

To configure remote commands:

1. Right click on the **Anti-Spam** node and select **Properties** from the context menu. This brings up the **Anti-Spam Properties** dialog.

2. Access the **Remote Commands** tab and check the **Enable remote commands** checkbox.

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 email. See the next section for information how to create an email with remote commands.
- In addition, you can specify which users are able to send emails 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 emails 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 UPPER CASE. 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 in double quotes (“ “).

Blacklist commands

With blacklist commands you can add a single email address or an entire domain to the custom blacklist. 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 email or good email (ham) to the Bayesian filter database. Simply forward the email with one of the following remote commands in them.

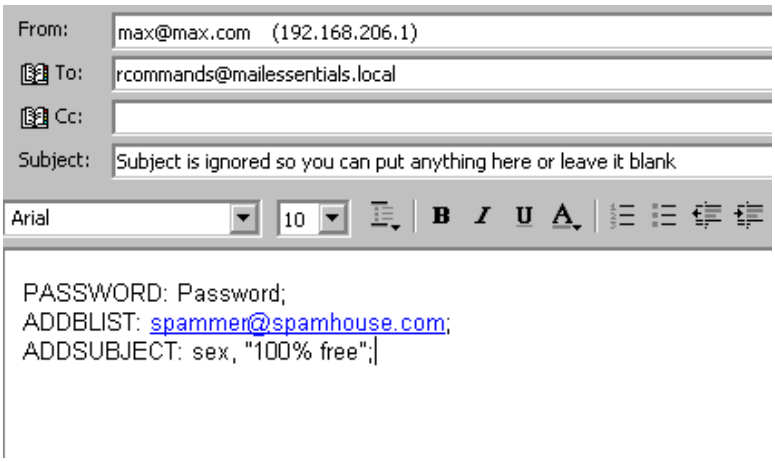
ADDASSPAM – instructs the Bayesian module to classify given email as spam.

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

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

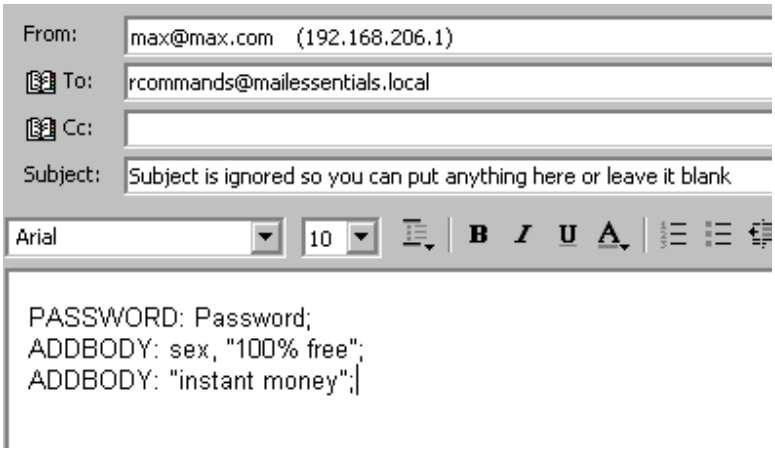
Examples

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



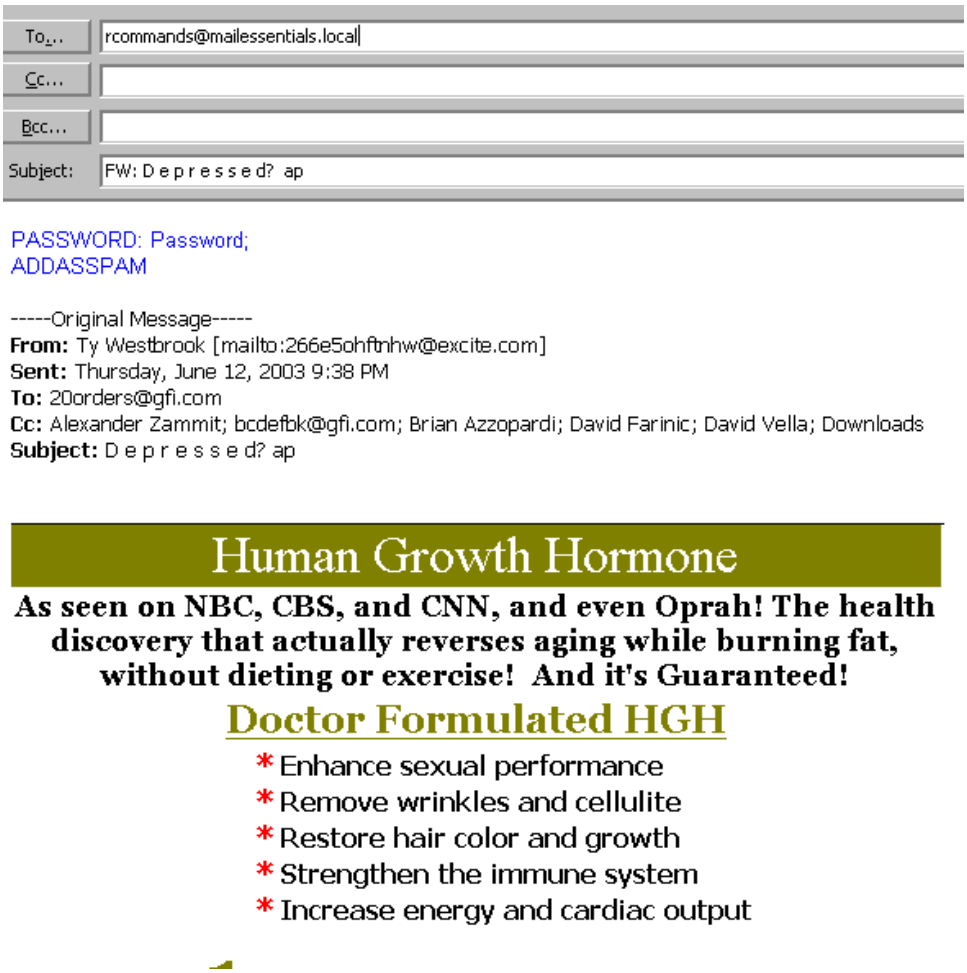
Screenshot 158 - Adding an email address to the blacklist and keywords

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



Screenshot 159 - Specifying the same commands more than once

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.



Screenshot 160 - Adding a spam to the Bayesian filter database

Example 4: When **Shared Password** checkbox is unchecked, you can send remote commands without specifying a password.

Screenshot 161 - Sending remote commands without security

Remote command logging

In order to keep track of changes made to the configuration database via remote commands, each email with remote commands (even if the email with remote commands was invalid) is saved under ADBRProcessed subfolder which is located under the GFI MailEssentials root 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 any software issues that you might encounter. The main sources of information available to users are:

- The manual – most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit http://kbase.gfi.com/.

Web Forum

User to user technical support is available via the web forum. The forum can be found at: http://forums.gfi.com/.

Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online:** Fill out the support request form on: http://support.gfi.com/supportrequestform.asp. Follow the instructions on this page closely to submit your support request.
- **Phone:** To obtain the correct technical support phone number for your region please visit: http://www.gfi.com/company/contact.htm.

NOTE: Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: http://customers.gfi.com.

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

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, visit: http://www.gfi.com/pages/productmailing.htm.