

**"Highest Performance
Lowest Price"**

Microsoft
GOLD CERTIFIED
Partner



**GFI MailSecurity 10.1 for
Exchange/SMTP
User Guide**



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

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

GFI MailSecurity is copyright of GFI SOFTWARE Ltd. © 1999-2009 GFI Software Ltd. All rights reserved.

Document Version: MSEC-UM-EN-1.00.002

Last updated: July 20, 2010

Contents

1	About GFI MailSecurity	1
1.1	Introduction to GFI MailSecurity	1
1.2	Key features of GFI MailSecurity	1
1.3	GFI MailSecurity components	2
1.4	GFI MailSecurity from a user's perspective	3
1.5	Add-ons - GFI MailEssentials.....	3
2	Installing GFI MailSecurity	5
2.1	Introduction.....	5
2.2	Typical deployment scenarios.....	5
2.3	Which installation mode should I use?	9
2.4	Hardware requirements	10
2.5	Software requirements.....	10
2.6	Important installation notes	11
2.7	Preparing to install GFI MailSecurity on an IIS mail relay server	12
2.8	Preparing to install GFI MailSecurity on your mail server	19
2.9	Installing GFI MailSecurity	19
2.10	GFI MailSecurity Post-Installation Wizard	23
2.11	Adding GFI MailSecurity to the Windows DEP Exception List	27
2.12	Securing access to the GFI MailSecurity configuration/quarantine.....	28
2.13	Securing access to the GFI MailSecurity Quarantine RSS feeds	32
2.14	Accessing the GFI MailSecurity Configuration and Quarantine Store.....	34
2.15	Upgrading from GFI MailSecurity 8 to GFI MailSecurity 10.1	36
2.16	Upgrading from GFI MailSecurity 9 to GFI MailSecurity 10.1	39
2.17	Quarantine Upgrade tool.....	39
3	General settings	41
3.1	Introduction to settings.....	41
3.2	Define the administrator's email address	41
3.3	Configuring proxy server settings for automatic updates.....	41
3.4	Adding Local Domains	43
3.5	SMTP server bindings	43
3.6	Managing local users in SMTP mode.....	44
4	Configuring virus checking	47
4.1	Configuring Virus Scanning Engines.....	47

4.2	AVG configuration.....	48
4.3	Kaspersky configuration.....	50
4.4	BitDefender configuration	51
4.5	McAfee configuration	52
4.6	Norman configuration	54
4.7	Virus scanner actions	55
4.8	Virus scanner updates	57
4.9	Setting the Virus Scanning Engines scan priority	58
4.10	Configuring Virus Scanning optimizations	58
4.11	Configuring Information Store Scanning	59
5	Configuring Content Filtering	63
5.1	Introduction.....	63
5.2	Creating a Content Filtering rule	63
5.3	Enabling/disabling rules.....	70
5.4	Removing content filtering rules.....	70
5.5	Modifying an existing rule	70
5.6	Changing the rule priority.....	71
6	Configuring Attachment Filtering	73
6.1	Introduction to Attachment Filtering	73
6.2	Creating an Attachment Filtering rule.....	73
6.3	Removing attachment rules	78
6.4	Make changes to an existing rule.....	79
6.5	Enabling/disabling rules.....	79
6.6	Changing the rule priority.....	79
7	Decompression engine	81
7.1	Introduction to the Decompression engine	81
7.2	Configuring the decompression engine filters	82
7.3	Configuring decompression filter actions	86
7.4	Enable/disable decompression filters.....	87
8	The Trojan & Executable Scanner	89
8.1	Introduction to the Trojan & Executable Scanner	89
8.2	Configuring the Trojan & Executable Scanner	89
8.3	Trojan & Executable Scanner updates.....	91
9	The Email Exploit Engine	95
9.1	Introduction to e-mail exploits	95
9.2	Configuring the Email Exploit Engine	95
9.3	Email Exploit Engine updates	98

10	The HTML Sanitizer	101
10.1	Introduction to the HTML Sanitizer.....	101
10.2	Configuring the HTML Sanitizer	101
11	Patch Checking	103
11.1	Introduction to Patch Checking	103
11.2	Downloading and installing software patches.....	103
12	Quarantine	105
12.1	Introduction to the Quarantine Store	105
12.2	The Quarantine Store	105
12.3	Search Folders	107
12.4	Approving emails from the Quarantine Store	112
12.5	Deleting emails from the Quarantine Store	113
12.6	Rescanning emails from the Quarantine Store.....	114
12.7	View the full security threat report of an email.....	115
12.8	Enable email approval via HTML approval forms.....	117
12.9	Quarantined mail from the user point of view	118
12.10	Enable quarantine RSS feeds.....	119
12.11	Enable the Directory Harvesting filter on quarantined emails	122
13	Reporting	127
13.1	Introduction to GFI MailSecurity Reporting.....	127
14	Realtime Monitor	137
14.1	About the Realtime Monitor	137
14.2	Monitoring email activity.....	137
15	Miscellaneous	139
15.1	Version Information.....	139
16	Advanced topics	141
16.1	Customizing the notification templates.....	141
16.2	Setting Virus Scanning API Performance Monitor Counters.....	144
17	Troubleshooting	148
17.1	Introduction.....	148
17.2	Knowledge Base.....	148
17.3	Web Forum.....	148
17.4	Request technical support	148
17.5	Build notifications.....	148
18	Index	149

1 About GFI MailSecurity

1.1 Introduction to GFI MailSecurity

The need to monitor email messages for dangerous, offensive or confidential content has never been more evident. The most deadly viruses, able to cripple your email system and corporate network in minutes, are being distributed worldwide via email in a matter of hours (for example, the MyDoom worm). Products that perform single vendor anti-virus scanning do not provide sufficient protection. Worse still, email is likely to become the means for installing backdoors (Trojans) and other harmful programs to help potential intruders break into your network. Products restricted to a single anti-virus engine will not protect against email exploits and attacks of this kind.

Your only defense is to install a comprehensive email content checking and anti-virus solution to safeguard your mail server and network. GFI MailSecurity acts as an email firewall and protects you from email viruses, exploits and threats, as well as email attacks targeted at your organization.

GFI MailSecurity is totally transparent to your users and does not require additional user training.

1.2 Key features of GFI MailSecurity

Virus checking using multiple virus engines

GFI MailSecurity scans email for viruses using multiple anti-virus engines. Scanning email at the gateway and at mail server level prevents viruses from entering and/or spreading within your network. Furthermore, you can avoid the embarrassment of sending infected emails to customers as GFI MailSecurity also checks outgoing mail for viruses. GFI MailSecurity includes the industrial strength Norman and BitDefender anti-virus engines that have received various awards. You also have the option to add the AVG, McAfee and Kaspersky anti-virus engines. Multiple anti-virus engines give you a higher level of security since anti-virus engines complement each other and lower the average response time to a virus outbreak. GFI MailSecurity also includes an auto-update facility that allows you to configure the anti-virus engines so that they automatically check and download any available updates without administrator intervention.

Email attachment checking/filtering

GFI MailSecurity's key feature is the ability to check all inbound and outbound email. It can quarantine all email with dangerous attachments, such as *.exe, *.vbs and other files. Such attachments are more likely to carry a virus, worm or email attack. Since email viruses can spread so quickly and cause immense damage, it is best to quarantine such emails before they are distributed to your email users. When GFI MailSecurity quarantines an email, the administrator can review it and then delete or approve the message.

Furthermore, you might choose to quarantine mails carrying *.mp3 or *.mpg files, as these hog bandwidth and can needlessly burden a mail server's disk space.

The Attachment Checking module has effectively saved thousands of companies from the LoveLetter virus.

Trojan and Executable Scanner

GFI MailSecurity is able to analyze incoming executables and rate the risk-level of an executable through a GFI patented process. Through the Trojan and Executable Scanner, GFI MailSecurity can detect and block potentially dangerous and unknown Trojans before they enter your network.

HTML Sanitizer

The advent of HTML email has made it possible for hackers/virus writers to trigger commands by embedding them in HTML mail. GFI MailSecurity scans the email body parts and any .htm/.html attachments for scripting code, and cleans up the HTML by removing all the scripting code. The HTML Sanitizer thus protects you from potentially malicious HTML email, containing HTML viruses and attacks launched via HTML email.

Decompression filter

The decompression filter is used to decompress and analyze compressed files (archives) attached to emails. This filter is able to check for and block password-protected archives, corrupted archives and recursive archives. Furthermore, this engine can also monitor the size and amount of the files included in an archive. You can configure this filter to quarantine or delete archives that exceed the specified file count or file size.

1.3 GFI MailSecurity components

GFI MailSecurity scan engine

The GFI MailSecurity scan engine analyzes the content of all inbound and outbound email. If you install GFI MailSecurity on the Microsoft Exchange machine, it will also scan the information store. If installed on a Microsoft Exchange 2007/2010 machine, GFI MailSecurity will scan the information store only if the Mailbox Server Role is installed. If you install GFI MailSecurity on a Microsoft Exchange 2007/2010 machine with the Hub Transport Server Role, it will also analyze internal email. When GFI MailSecurity quarantines an email, it informs the appropriate supervisor/administrator via Email/RSS feed, depending on the options you configure.

GFI MailSecurity configuration

Through the GFI MailSecurity configuration, you can configure GFI MailSecurity to fit your needs.



Screenshot 1 - GFI MailSecurity Configuration

1.4 GFI MailSecurity from a user's perspective

GFI MailSecurity is totally transparent to the user. This means that the user will not notice that GFI MailSecurity is active until it blocks an email that triggers a rule, for example, an email that contains a forbidden attachment or a virus.

In the case of a suspicious attachment, GFI MailSecurity will quarantine the email for review by the administrator. Optionally, the recipient will receive a message indicating that the mail is awaiting administrator review. As soon as the administrator approves the email, GFI MailSecurity will forward the email to the recipient.

1.5 Add-ons - GFI MailEssentials

A companion product to GFI MailSecurity is GFI MailEssentials. GFI MailEssentials adds a number of corporate email features to your mail server, notably:

- Anti-spam, using a variety of methods including Bayesian analysis



- Email management, including disclaimers, POP3 downloader and server-based auto replies and more.

For more information, please visit the GFI website at <http://www.gfi.com>.

NOTE: GFI MailEssentials is available at a bundle price if purchased in combination with GFI MailSecurity.

2 Installing GFI MailSecurity

2.1 Introduction

This chapter explains how to install and configure GFI MailSecurity. You can install GFI MailSecurity directly on your mail server or you can choose to install it on a separate machine configured as a mail relay/gateway server. When installing on a separate machine, you must first configure the machine to relay the inbound and outbound emails to your mail server prior to installing this mail security software.

In order to function correctly, GFI MailSecurity requires access to the complete list of all your email users and their email addresses. This is required in order to configure content policy rules such as attachment checking and content checking. GFI MailSecurity can access the list of email users in two ways: either by querying your Active Directory (requires installing this software in **Active Directory mode**) or by importing the list from your SMTP Server (requires installing this software in **SMTP mode**). The mode to be used depends entirely on your network setup and the machine on which you will be installing this mail security software. You can choose the required access mode during the installation of GFI MailSecurity.

2.2 Typical deployment scenarios

Installing GFI MailSecurity on your mail server

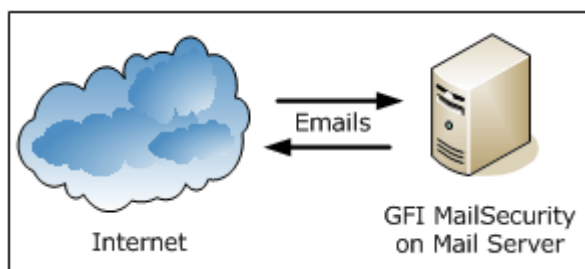


Figure 1 - Installing GFI MailSecurity on your mail server

You can install GFI MailSecurity directly on your mail server, without any additional configuration required. Moreover you can also choose any of the two installation modes (i.e., Active Directory mode or SMTP mode) to define how GFI MailSecurity will retrieve the list of email users since your mail server will have access to both the Active Directory as well as to the list of SMTP users which is contained on the mail server itself.

NOTE: GFI MailSecurity can be only installed in the following Microsoft Exchange 2007/2010 installations:

- Edge Server Role
- Hub Transport Role (and any other Microsoft Exchange 2007/2010 server roles which are irrelevant to GFI MailSecurity)
- Mailbox and Hub Transport Server Role (and any other Microsoft Exchange 2007/2010 server roles which are irrelevant to GFI MailSecurity)

Installing GFI MailSecurity on a mail relay server

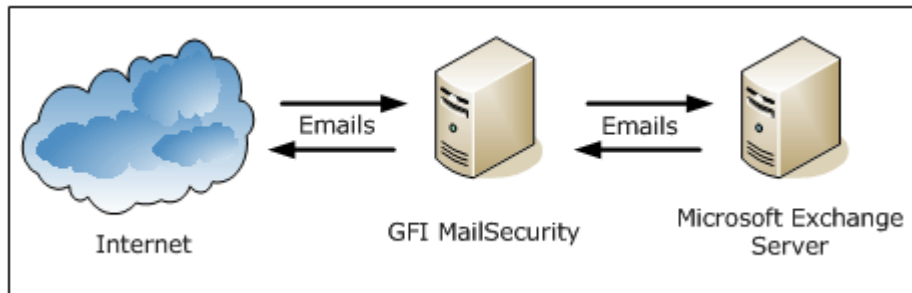


Figure 2 - Installing GFI MailSecurity on a mail gateway/relay server

When installing on a separate server (i.e., on a server which is not your mail server), you must first configure that machine to act as a gateway (also known as “Smart host” or “Mail relay” server) for all your email. This means that all inbound email must pass through this machine for scanning before being relayed to the mail server for distribution (i.e., it must be the first to receive all emails destined for your mail server). The same applies for outbound emails: The mail server must relay all outgoing emails to the gateway machine for scanning before they are conveyed to the external recipients via Internet (i.e. it must be the last 'stop' for emails destined for the Internet). In this way, GFI MailSecurity checks all your inbound and outbound mail before this is delivered to the recipients.

NOTE: You must install GFI MailSecurity in SMTP Gateway mode if you are running Lotus Notes or another SMTP/POP3 server.

NOTE: If you are running a Windows NT network, the machine running GFI MailSecurity can be separate from your Windows NT network - GFI MailSecurity does not require Active Directory when installed in SMTP mode.

Installing GFI MailSecurity in front of your firewall

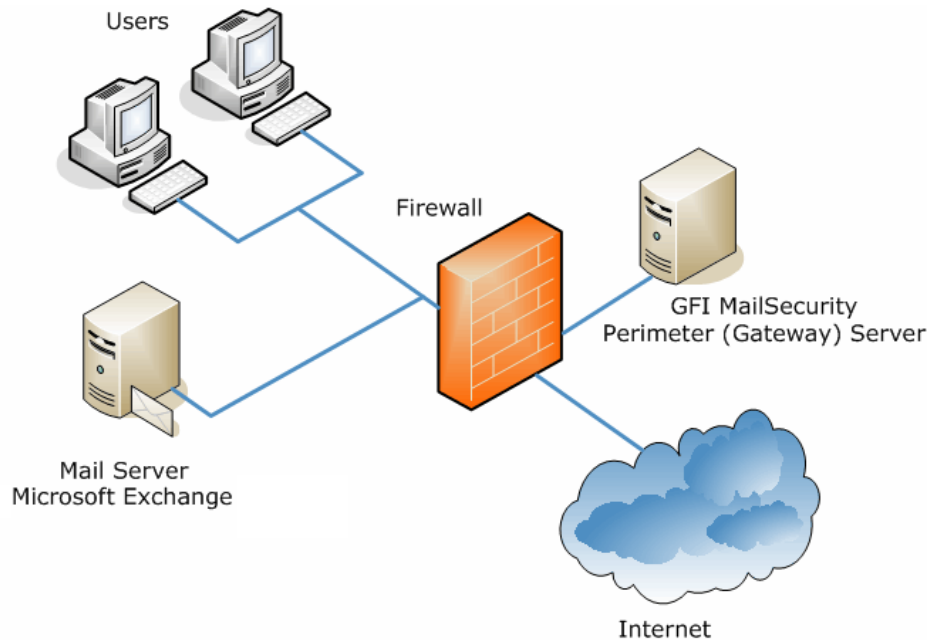


Figure 3 - Installing GFI MailSecurity on a separate machine on a DMZ

If running a Windows 2000/2003 firewall such as Microsoft ISA Server, a good way to deploy GFI MailSecurity is to install it on a separate machine in front of your firewall or on the firewall itself. This allows you to keep your corporate mail server behind the firewall. GFI MailSecurity will act as a smart host/mail relay server when installed on the perimeter network (also known as DMZ - demilitarized zone).

NOTE: In a Microsoft Exchange Server 2007/2010 environment, the mail relay server in the DMZ can be a machine running Microsoft Exchange Server 2007/2010 with the Edge Transport Server Role installed.

When GFI MailSecurity is not installed on your mail server:

- You can perform maintenance on your mail server whilst still receiving email from the Internet.
- Fewer resources are used on your mail server.
- Additional fault tolerance - if anything happens to your mail server, you can still receive email. This email is then queued on the GFI MailSecurity machine.

NOTE: GFI MailSecurity does not require a dedicated machine when not installed on the mail server. For example, you can install GFI MailSecurity on your firewall (i.e. on your ISA Server) or on machines running other applications such as GFI MailEssentials.

Installing GFI MailSecurity on an Active/Passive Cluster

NOTE: Installing GFI MailSecurity on a Microsoft Exchange Server 2007/2010 cluster environment is currently not supported.

To install GFI MailSecurity on an Active/Passive cluster you must install GFI MailSecurity on each node.

NOTE: Although you can install GFI MailSecurity on an Active/Passive cluster, bear in mind that you still need to configure and manage a GFI MailSecurity installation per node. The configuration settings and quarantine emails are not shared between nodes.

On each node, you have to do the following:

- Install GFI MailSecurity on the node local hard drive.
NOTE: Do not install GFI MailSecurity on the shared drive.
- Install the GFI MailSecurity WWW virtual directory on the node's Default Web Site.
- If you are installing on an IIS cluster, make sure you bind GFI MailSecurity to the Clustered SMTP Virtual Server instance.

The following steps show you how to install GFI MailSecurity in a typical Active/Passive Cluster environment. For this scenario, assume the cluster, named **MAILCLUSTER**, is made up of two nodes, named **Node1** and **Node2**.

1. Using the **Cluster Administrator** console make **Node1** active.
2. Install GFI MailSecurity on the local hard drive of **Node2** as described in the 'Installing GFI MailSecurity' section of this chapter. When you reach the **IIS Setup** step of the installation, select **Default Web Site** to host the GFI MailSecurity WWW virtual directory.
NOTE: The **Default Web Site** IP address of **Node2** should not be set to 'All unassigned'. You should configure the **Default Web Site** to use the IP address of the **MAILCLUSTER** machine.
3. When the GFI MailSecurity installation on **Node2** completes, you should be able to access the **Node2** configuration using the following URL: <http://Node2/MailSecurity/>
4. From the **Cluster Administrator** console, make **Node2** active.
5. Install GFI MailSecurity on the local hard disk of **Node1** as described in the 'Installing GFI MailSecurity' section of this chapter. When you reach the **IIS Setup** step of the installation, select **Default Web Site** to host the GFI MailSecurity WWW virtual directory.

NOTE: The **Default Web Site** IP address of **Node1** should not be set to 'All unassigned'. You should configure the **Default Web Site** to use the IP address of the **MAILCLUSTER** machine.

6. When the GFI MailSecurity installation on **Node1** completes, you should be able to access the **Node1** configuration using the following URL: <http://Node1/MailSecurity/>
7. To access the product configuration of the currently active node use the following URL: <http://MAILCLUSTER/MailSecurity/>.

NOTE: To access product configuration from a remote machine you must configure the **GFI MailSecurity SwitchBoard** application, making sure that the **MAILCLUSTER** name/IP is specified for **IIS Mode**. For more information,

refer to [Securing access to the GFI MailSecurity configuration/quarantine](#) section in this chapter.

NOTE: You will only be able to access the URL <http://MAILCLUSTER/MailSecurity/> if you assign the IP address of the **MAILCLUSTER** machine to the **Default Web Site** for **Node1** and **Node2** during the **IIS Setup** installation step.

8. The installation of GFI MailSecurity on an Active/Passive cluster is now complete.

NOTE: If Service Pack 2 for Microsoft Exchange Server 2003 is not installed on a Microsoft Exchange Server 2003 cluster installation, Internet Information Services Web sites that are hosted on the cluster will not start automatically when an Exchange Server 2003 virtual server fails over to a cluster node. More information about this issue can be found in [Microsoft Knowledge Base Article 885440](#).

Due to the above, the GFI MailSecurity configuration could become unavailable following a failover or moving of an Exchange Virtual Server from one node of the cluster to the other.

Installing Service Pack 2 for Exchange Server 2003 is thus recommended. Guidelines on how to install Exchange Server 2003 service packs in a clustered Exchange Server environment can be found in [Microsoft Knowledge Base Article 867624](#).

To uninstall GFI MailSecurity from the **MAILCLUSTER** cluster environment outlined above, follow these steps:

1. Using the **Cluster Administrator** console make **Node1** active.
2. Uninstall GFI MailSecurity from **Node2**.
3. Using the **Cluster Administrator** console make **Node2** active.
4. Uninstall GFI MailSecurity from **Node1**.
5. The uninstallation of GFI MailSecurity on an Active/Passive cluster is now complete.

Installing GFI MailSecurity on an Active/Active Cluster

Installing GFI MailSecurity on an Active/Active cluster is currently not supported.

2.3 Which installation mode should I use?

Active Directory mode

When installed in Active Directory mode, GFI MailSecurity creates user-based rules, such as Attachment Checking and Content Checking rules, based on the list of users available in Active Directory. This means that the machine running GFI MailSecurity must be behind your firewall and must have access to the Active Directory containing all your email users (i.e., the machine must be part of the Active Directory domain). You can install GFI MailSecurity in Active Directory mode directly on your mail server as well as on any other domain machine that is configured as a mail relay server in your domain.

SMTP mode

In SMTP mode, GFI MailSecurity will create user-based rules, such as Attachment Checking and Content Checking rules, based on the list of email users/addresses available on your mail server. This means that you must install GFI MailSecurity in SMTP mode if your machine does not have access to the Active Directory containing all your email users. This includes machines that are not part of your Active Directory domain (i.e., non-domain machines) as well as machines in a DMZ. However, you can still install GFI MailSecurity in SMTP mode on your mail server as well as on any other machine that has access to Active Directory containing all (email) users.

NOTE: Both installation modes have the same scanning features and performance. The only difference between Active Directory and SMTP installation mode is the way that GFI MailSecurity accesses/gathers the list of email users for generating its scanning rules and notifications.

2.4 Hardware requirements

The hardware requirements for GFI MailSecurity are:

- Pentium 4 (or equivalent) - 2Ghz
- 512MB RAM
- 1.5 GB of physical disk space

2.5 Software requirements

2.5.1 Supported Operating Systems

- Windows Server 2008 Standard or Enterprise (x86 or x64) (R1 or R2)
- Windows Server 2003 Standard or Enterprise (x86 or x64)
- Windows 2000 Server/Advanced Server (Service Pack 1 or higher)
- Windows XP professional
- Windows Small Business Server 2000
- Windows Small Business Server 2003
- Windows Small Business Server 2008

2.5.2 Supported Mail Servers

- Microsoft Exchange Server 2010, 2007, 2003, 2000 (SP1)
- Lotus Notes 5.5, 5.0, 4.5, 4
- Any SMTP/POP3 mail server

2.5.3 Other components

- Microsoft .Net framework 2.0
- MSMQ - Microsoft Messaging Queuing Service
- Internet Information Services (IIS) - SMTP and World Wide Web services
- Microsoft Data Access Components (MDAC) 2.8

2.6 Important installation notes

Windows XP

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

Windows Server 2008

When installing on Windows Server 2008, the following pre-requisites are required:

- Web Server (IIS) role
- ASP.NET
- Windows Authentication Services
- Microsoft SMTP Services

For more information, refer to:

<http://kbase.gfi.com/showarticle.asp?id=KBID001596>

Microsoft Exchange Server 2007/2010

If you are installing on Microsoft Exchange Server 2007/2010, you need to install one of the following roles;

- Edge Server Role,
- Hub Transport Role or,
- Mail Server and Hub Transport roles.

GFI MailSecurity cannot be installed on a Microsoft Exchange 2007/2010 machine with only Mailbox Server Role installed. In addition, IIS SMTP service is not required, since it has its own built in SMTP server.

Windows Small Business Server

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

Other installation configurations

Disable anti-virus software from scanning the GFI MailSecurity 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 mail server. For more information, please refer to:

<http://kbase.gfi.com/showarticle.asp?id=KBID001559>.

GFI MailSecurity directories should never be backed up using backup software.

2.7 Preparing to install GFI MailSecurity on an IIS mail relay server

In order to install GFI MailSecurity on a mail relay/gateway machine, it must be running the IIS SMTP Service and World Wide Web service. You must also configure the machine as an SMTP relay to your mail server. This means that the MX record of your domain must be pointing to the gateway machine. This section describes how you can configure your mail relay and install GFI MailSecurity.

About Windows 2000/2003 IIS SMTP & World Wide Web services

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

The World Wide Web service is also part of IIS. It uses the HTTP protocol to handle web client requests on a TCP/IP network.

The IIS SMTP service and World Wide Web service are included in every Windows 2000/2003/XP distribution.

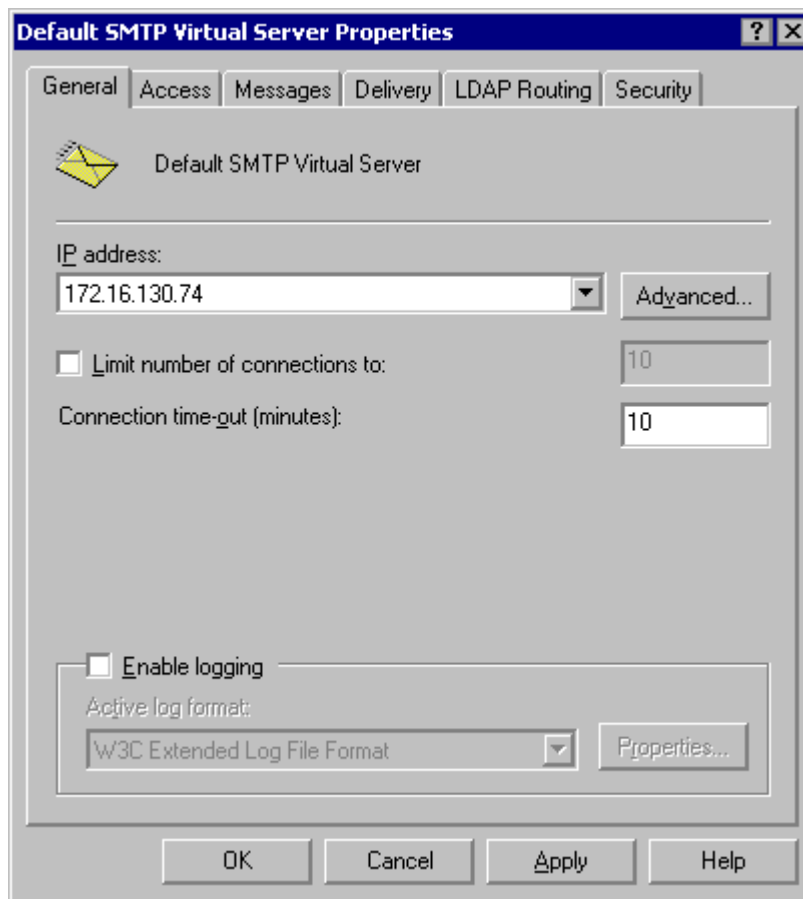
Step 1: Verify installation of IIS SMTP and WWW services

GFI MailSecurity uses the Windows 2000/2003/XP IIS SMTP service as its SMTP server.

1. On the taskbar, click **Start ► Settings ► Control Panel**. Double-click **Add/Remove Programs** and then click **Add/Remove Windows Components**.
2. From the dialog on display, locate and click the **Internet Information Services (IIS) component**, then click **Details**.
3. Select the **SMTP Service** check box and **World Wide Web Service** check box. Click **OK** to start the installation of the selected services. Follow the onscreen instructions and wait until the installation completes.

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

1. On the taskbar, click **Start ► Settings ► Control Panel**. Double-click **Administrative Tools** and then double-click **Internet Information Services**.
2. Expand the server name node, right-click the **Default SMTP Virtual Server** node and then click **Properties**.



Screenshot 2 - Assign an IP address to the mail relay server

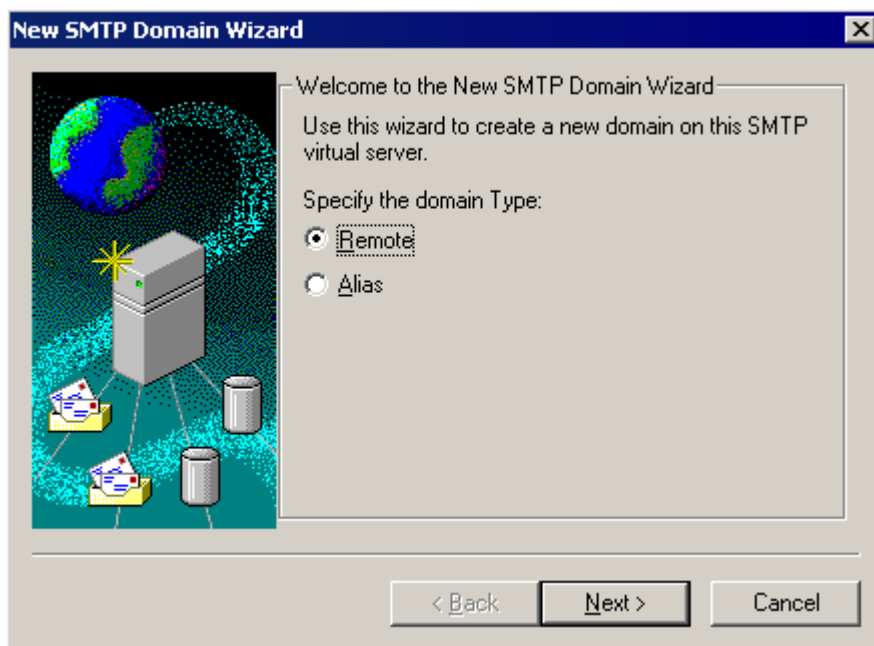
3. Assign an IP address to the SMTP relay server from the **IP address** list and then click **OK**.

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

Now you must configure the SMTP service to relay inbound messages to your mail server.

Start by creating a local domain in IIS to route mail:

1. On the taskbar, click **Start ► Settings ► Control Panel**. Double-click **Administrative Tools** and then double-click **Internet Information Services**.
2. Expand the server name node then expand the **Default SMTP Virtual Server** and then click **Domains**. By default, you should have a **Local (Default)** domain with the fully qualified domain name of the server.
3. Configure the domain for inbound message relaying as follows:
 - a) Right-click the **Domains** node, and then click **New ► Domain**.



Screenshot 3 - SMTP Domain Wizard - Selecting domain type

- b) Select **Remote** and then click **Next**.
- c) Type the domain name in the **Name** box and then click **Finish**.

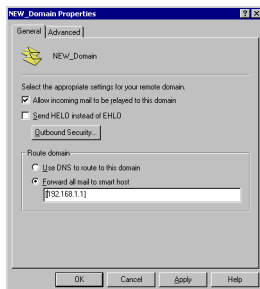
NOTE: Upon installation, GFI MailSecurity will import Local Domains from the IIS SMTP service. If you add additional Local Domains in IIS SMTP service, you must also add these domains to GFI MailSecurity because this does not detect newly added Local Domains automatically. You can add more/new Local Domains using the GFI MailSecurity configuration. For more information, refer to the [Adding Local Domains](#) section in the General Settings chapter of this manual.

Configure the domain to relay email to your mail server:

1. Right-click the domain you just created and then click **Properties**. Select the **Allow the Incoming Mail to be relayed to this domain** check box.
2. In the Route domain dialog box, click **Forward all email to smart host** and type the IP address (in square brackets) of the server which will handle the emails addressed to this new domain. For example, [123.123.123.123]

NOTE: The square brackets are used to differentiate an IP address from a hostname (which does not require square brackets), i.e., the server detects an IP address from the square brackets.

3. Click **OK**.

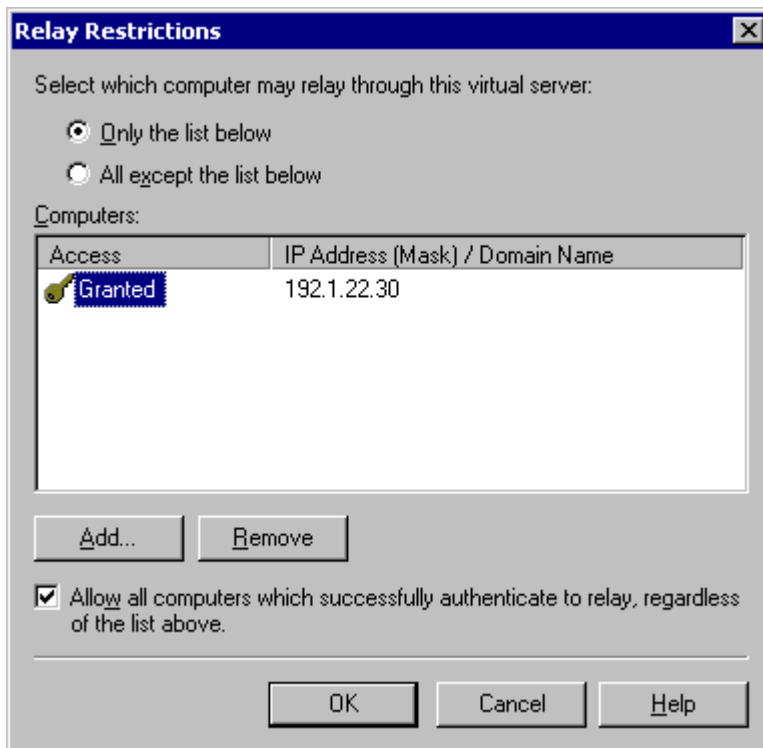


Screenshot 4 - Configure the new domain

Step 4: Secure your mail relay server

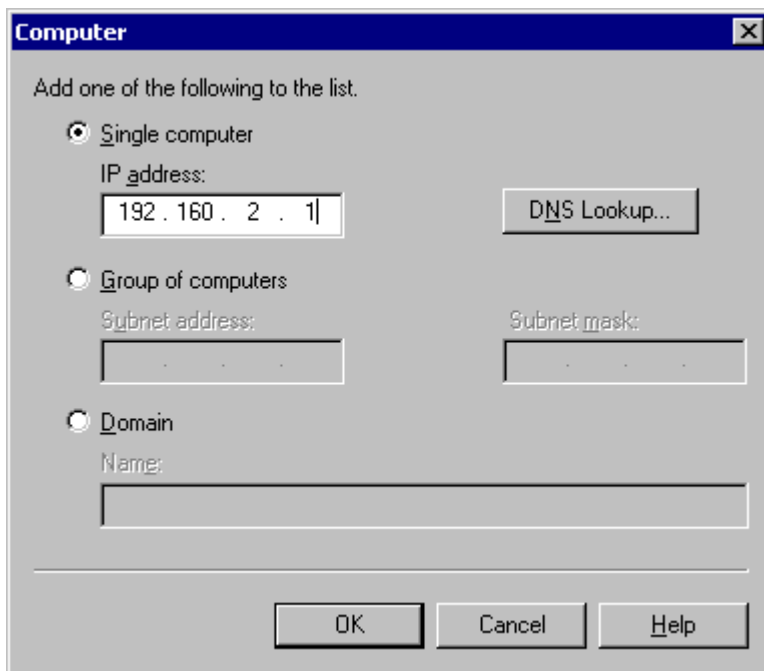
In this step, you will set up your SMTP virtual server's mail Relay Restrictions. This means that you must specify which machines may relay email through this virtual server (i.e., effectively limit the servers that can send email via this server).

1. Right-click the **Default SMTP Virtual Server** node and then click **Properties**.
2. In the properties dialog box, click the **Access** tab and then click **Relay** to open the **Relay Restrictions** dialog box.



Screenshot 5 - Relay Restrictions dialog

3. Click **Only the list below** and then click **Add** to specify the list of permitted computers.



Screenshot 6 - Specify machines which may relay email via virtual server

4. In the **Computer** dialog box, specify the IP of the mail server that will be forwarding the email to this virtual server and then click **OK** to add the entry to the list.

NOTE: You can specify the IP of a single computer, group of computers or a domain:

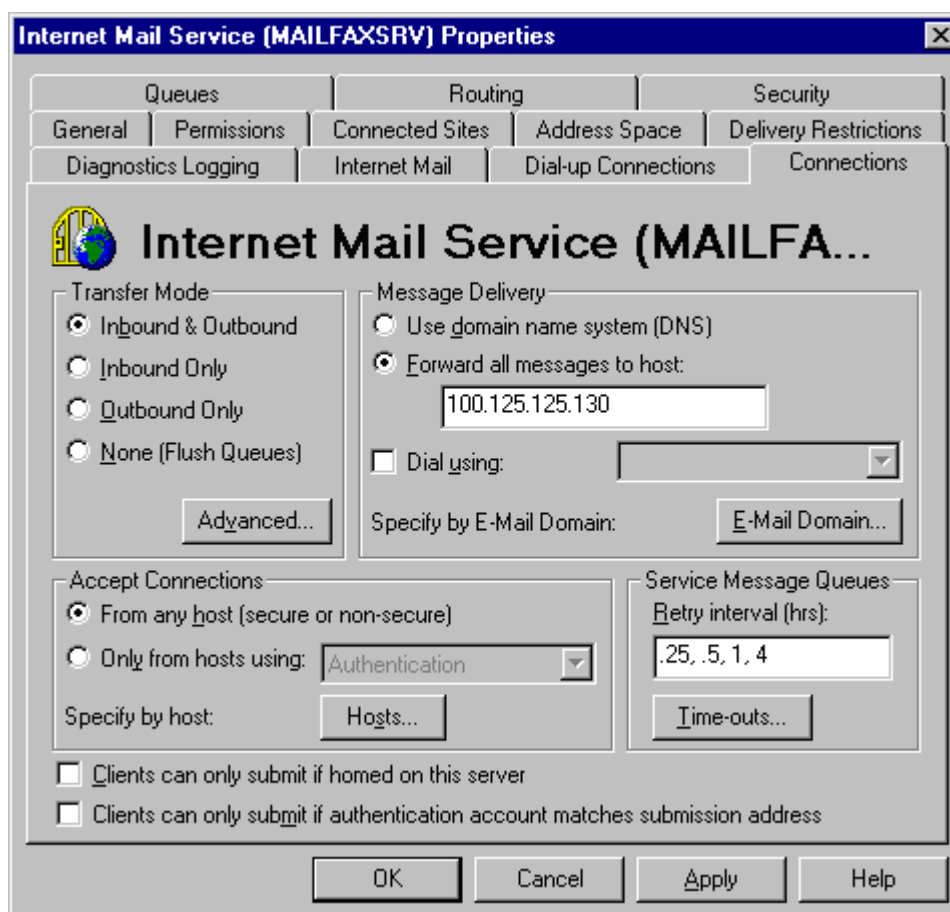
- **Single computer:** Select this option to specify one particular host that will relay email via this server. If you want to look up the IP address of a specific host, click **DNS Lookup**.
- **Group of computers:** Select this option to specify the base IP address for the computers that you want to relay.
- **Domain:** Select this option to include all the computers of a specified domain. This means that the domain controller will openly relay emails via this server. Please note that this option adds processing overhead, and may reduce SMTP service performance because it includes reverse DNS Lookups to verify the domain name of all IP addresses that try to relay.

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

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

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

1. Start the Microsoft Exchange Administrator and double-click on **Internet Mail Service** to open the properties configuration dialog box.



Screenshot 7 - The Microsoft Internet mail connector

2. Click the **Connections** tab and in the **Message Delivery** area click **Forward all messages to host**. Type the computer name or IP of the machine running GFI MailSecurity.

3. Click **OK** and restart the Microsoft Exchange Server from the services applet.

If you have Microsoft Exchange Server 2000/2003:

You will need to set up an SMTP connection that forwards all email to GFI MailSecurity:

1. Start the Exchange System Manager.
2. Right-click the **Connectors** Node, click **New ► SMTP Connector** and then specify the connector name.
3. Click **Forward all mail through this connector to the following smart host**, type in the IP of the GFI MailSecurity server (the mail relay/Gateway server) and then click **OK**.

NOTE: Always enclose the IP address within square brackets []. For example, [100.130.130.10].

4. Select the SMTP Server that must be associated to this SMTP Connector. Click the **Address Space** tab, and then click **Add**. Click **SMTP** and then click **OK** to accept the changes.

5. Click **OK**. All emails will now be forwarded to the GFI MailSecurity machine.

If you have Lotus Notes:

1. Double-click the **Address Book** in Lotus Notes.
2. Click on **Server** item to expand its sub-items.
3. Click **Domains** and then click **Add Domains**.
4. In the Basics section, click **Foreign SMTP Domain from the Domain Type** field and in the **Messages Addressed to** area, type "*" in the **Internet Domain** box.
5. Under the **Should be routed to** area, specify the IP of the machine running GFI MailSecurity in the **Internet Host** box.
6. Save the settings and restart the Lotus Notes server.

If you have an SMTP/POP3 mail server:

1. Start the configuration program of your mail server.
2. Search for the option to relay all outbound email via another mail server. This option will be called something like **Forward all messages to host**. Enter the computer name or IP of the machine running GFI MailSecurity.
3. Save the new settings and restart your mail server.

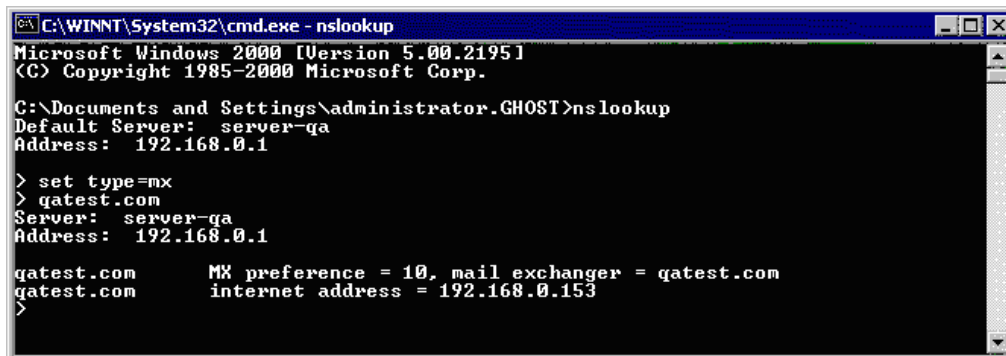
Step 6: The MX record of your domain must point to the mail relay server

NOTE: If your ISP manages the DNS server, ask this provider to update it for you.

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

Verify the MX record of your DNS server as follows:

1. Open the command prompt, type **nslookup** and press Enter.
2. Type **set type=mx** and press Enter.
3. Type your mail domain and press Enter.
4. The MX record should return a single IP that must correspond to the IP of the machine running GFI MailSecurity.



```

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

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

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

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

Screenshot 8 - Checking the MX record of your domain

Step 7: Test your new mail relay server

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

1. Test the IIS SMTP inbound connection of your mail relay server by sending an email from an external account to an internal user (you can use web-mail, for example MSN Hotmail, if you do not have an external account available). Verify that the email client received the email.
2. Test the IIS SMTP outbound connection of your mail relay server by sending an email to an external account from an email client. Verify that the external user received the email.

NOTE: Instead of using an email client, you can send email manually through Telnet. This will give you more troubleshooting information. For more information, refer to this Microsoft Knowledge Base article:

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

Step 8: Install GFI MailSecurity on the mail relay server

For information on how to install GFI MailSecurity, refer to [Installing GFI MailSecurity](#) section in this chapter.

2.8 Preparing to install GFI MailSecurity on your mail server

No additional configuration is required if you are installing GFI MailSecurity directly on your mail server. For information on how to install GFI MailSecurity, refer to [Installing GFI MailSecurity](#) section in this chapter.

2.9 Installing GFI MailSecurity

Before you install GFI MailSecurity, check the points below:

1. Make sure that you are logged on as Administrator or you are using an account with administrative privileges.
2. Save any pending work and close all open applications on the machine.
3. Check that the machine you are installing GFI MailSecurity on meets the system and hardware requirements specified earlier in this chapter.

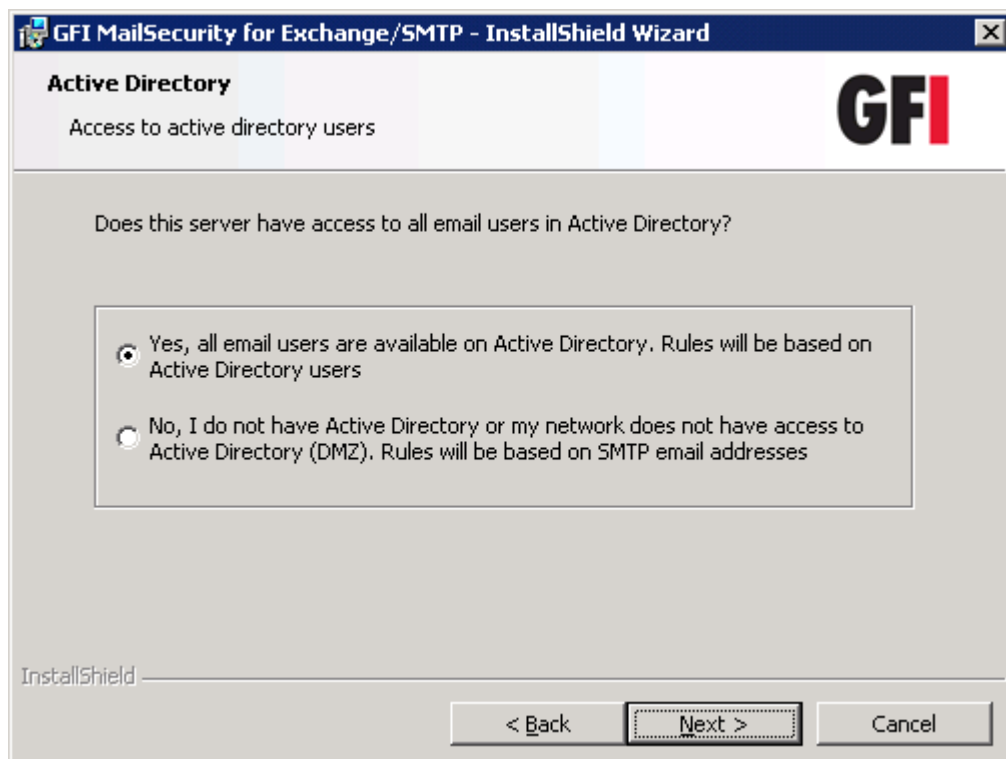
To install GFI MailSecurity follow these steps:

1. Run the GFI MailSecurity setup program by double-clicking on the **MailSecurity10.exe** file. The installation wizard will perform some unpacking operations and then display the **Welcome** page. Click **Next** to continue.

2. Read the license agreement displayed in the **License agreement** page and click **I accept the terms in the license agreement** if you accept the terms of the license agreement. Click **Next** to continue the installation.

NOTE: If upgrading from a previous version than GFI MailSecurity 10.1 SR8, you will be asked to upgrade to the Firebird database. Selecting import will prompt GFI MailSecurity to automatically launch the quarantine upgrade tool after the installation. If you select not to import the quarantine database, any previous quarantine data will not be used by the upgraded version. For information on the quarantine upgrade tool, refer to [Quarantine Upgrade tool](#) section in this manual.

3. Type the administrator email address in the **Administrator Email** box. If you bought a license for GFI MailSecurity, type it in the **License Key** box. If you do not have a license yet and want to evaluate GFI MailSecurity, leave the default evaluation license key in the **License Key** box. Click **Next** to continue the installation.



Screenshot 9 - Define if the server has access to all email users in the Active Directory

4. Setup will now ask you to select the mode that GFI MailSecurity will use to retrieve the list of your email users. You must select one of the following options:

- **Yes, all email users are available on Active Directory** - Select this option to continue installing GFI MailSecurity in Active Directory mode. In

this mode, GFI MailSecurity creates user-based rules, for example Attachment Checking rules, based on the list of users available in the Active Directory. This means that the machine on which GFI MailSecurity is being installed must be behind your firewall (for example, Mail Server) and must have access to the Active Directory containing all your email users (i.e., the machine on which GFI MailSecurity is being installed must be part of the Active Directory domain).

- **No, I do not have Active Directory or my network does not have access to Active Directory (DMZ)** - Select this option to continue installing GFI MailSecurity in SMTP mode. In this mode, GFI MailSecurity will create user-based rules, for example Attachment Checking rules, based on the list of email users/addresses imported from your mail server. You must select this mode if you are installing GFI MailSecurity on a machine that does not have access to the Active Directory containing the complete list of all your email users. This includes machines on a DMZ or machines that are not part of the Active Directory Domain. However, you can still choose this mode to install GFI MailSecurity on machines that do have access to the Active Directory containing all your email users.

Click **Next** to proceed with the installation.

Screenshot 10 - Define your SMTP server and GFI MailSecurity virtual folder details.

5. You now need to select the server where you want to host the GFI MailSecurity configuration pages. On this server, two virtual directories are created to host the configuration pages and the quarantine RSS feeds. You can specify custom virtual directory names if you want, or else leave the defaults.

NOTE: If you are installing on a Microsoft Exchange Server 2007/2010 machine, the IIS SMTP service is not required, since it has its own built in SMTP server. In such a case, the **SMTP Server Setup** area is not displayed and you can click **Next** to continue and go to step 7 directly.

GFI MailSecurity relies on the IIS SMTP service to send and receive SMTP mail. It binds to your default SMTP virtual server (i.e., the server specified in the MX record of your DNS Server). However, if you have multiple SMTP virtual servers on your domain, you can bind GFI MailSecurity to any available SMTP virtual server. To change the default SMTP connection, select the required server from the list of available SMTP Virtual Servers provided in this dialog box.

NOTE: After installing the product, you can still bind GFI MailSecurity to another SMTP virtual server from the GFI MailSecurity Configuration (**GFI MailSecurity ► Settings ► Bindings**). For more information, refer to [SMTP server bindings](#) section in this manual.

Click **Next** to continue the installation.

6. Setup will now search your network and will import a list of your Local Domains from the IIS SMTP service. GFI MailSecurity determines if an email is inbound or outbound by comparing the domain in a sender's address to the list of local domains. If the address exists in the list, then the email is outbound. Check that all your Local Domains have been included in the list on display. If not, make sure to add any unlisted domain after the installation completes. For more information, refer to the [Adding Local Domains](#) section in this manual. Click **Next** to continue.

7. Setup will now ask you to define the folder where you want to install GFI MailSecurity. GFI MailSecurity requires approximately 50 MB of free hard disk space. Additionally, you must also reserve approximately 200 MB for temporary files. Click **Change** to specify a new installation path or click **Next** to install in the default location and proceed with the installation.

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

8. The installation wizard has now collected all the required installation settings and is ready to install GFI MailSecurity. If you want to make changes to these settings, click **Back**. Otherwise, click **Install** to start the installation process.

9. During the installation, you are prompted that the setup needs to restart the SMTP services. Click **Yes** to restart these services and finalize the installation.

NOTE: If you are installing on a Microsoft Exchange Server 2007/2010 machine, you will not be prompted to restart the SMTP service.

10. When the installation completes, click **Finish** to close the installation wizard.

NOTE: If you are installing on a Microsoft Exchange Server 2007/2010 machine, the installation will launch the GFI MailSecurity Post-Installation

Wizard. Refer to the following section for information on how to use this wizard.

NOTE: If you are upgrading from a previous version (version 9 onwards) of GFI MailSecurity, you might be prompted to upgrade your quarantine database to a new Firebird database format. For more information, refer to the [Quarantine Upgrade tool](#) section in this manual.

2.10 GFI MailSecurity Post-Installation Wizard

NOTE: This section applies only when installing GFI MailSecurity on a Microsoft Exchange Server 2007/2010 machine.

IMPORTANT: You need to complete this wizard for GFI MailSecurity to work with Microsoft Exchange Server 2007/2010.

The GFI MailSecurity installation wizard launches the GFI MailSecurity Post-Installation Wizard when you click **Finish**. The GFI MailSecurity Post-Installation Wizard registers GFI MailSecurity with the local installation of Microsoft Exchange Server 2007/2010 so that it can process and scan the emails passing through the server.

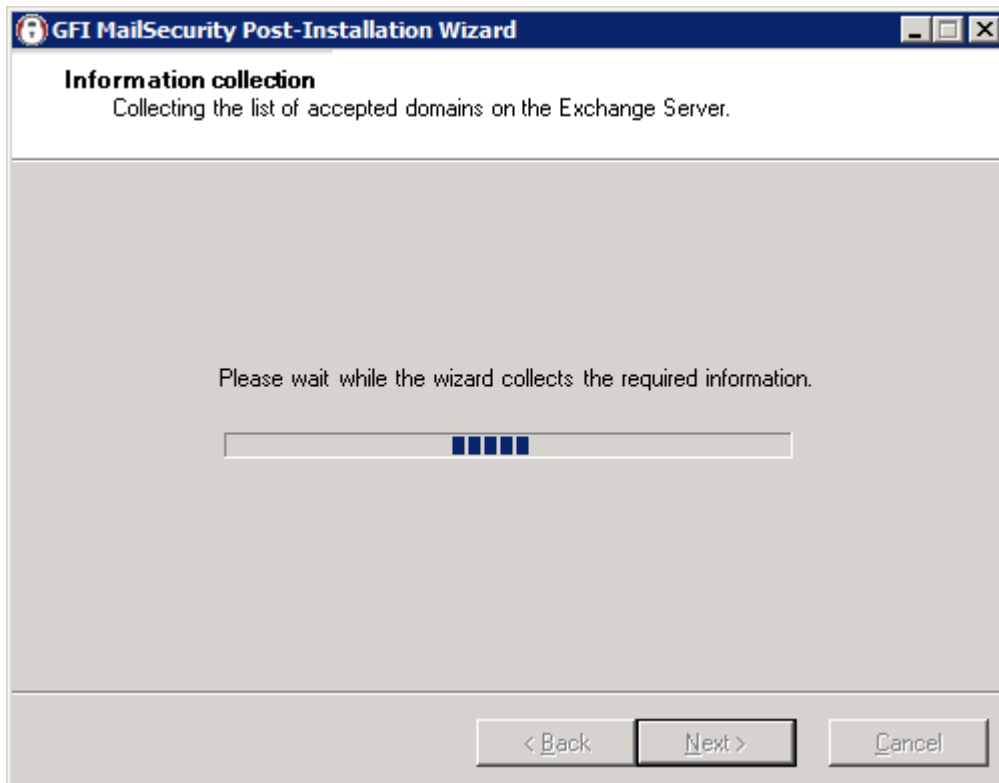
To complete the GFI MailSecurity Post-Installation Wizard, follow these steps:

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



Screenshot 11 - GFI MailSecurity Post-Installation Wizard welcome page

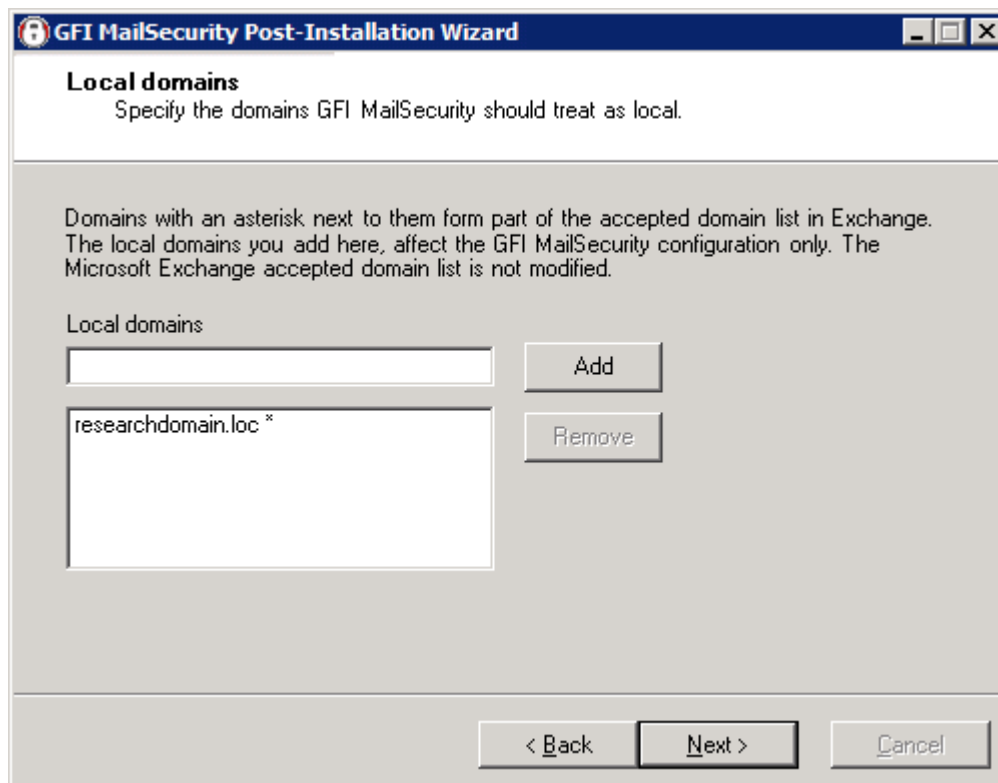
2. The wizard will collect information from the Microsoft Exchange Server 2007/2010 installation, such as the list of local domains and the server roles installed, for example Hub Transport Server Role.



Screenshot 12 - Collecting information from Microsoft Exchange Server 2007/2010

3. The wizard will display the accepted domain list collected from Microsoft Exchange Server 2007/2010. If you need to specify another local domain, type it in the **Local 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**.

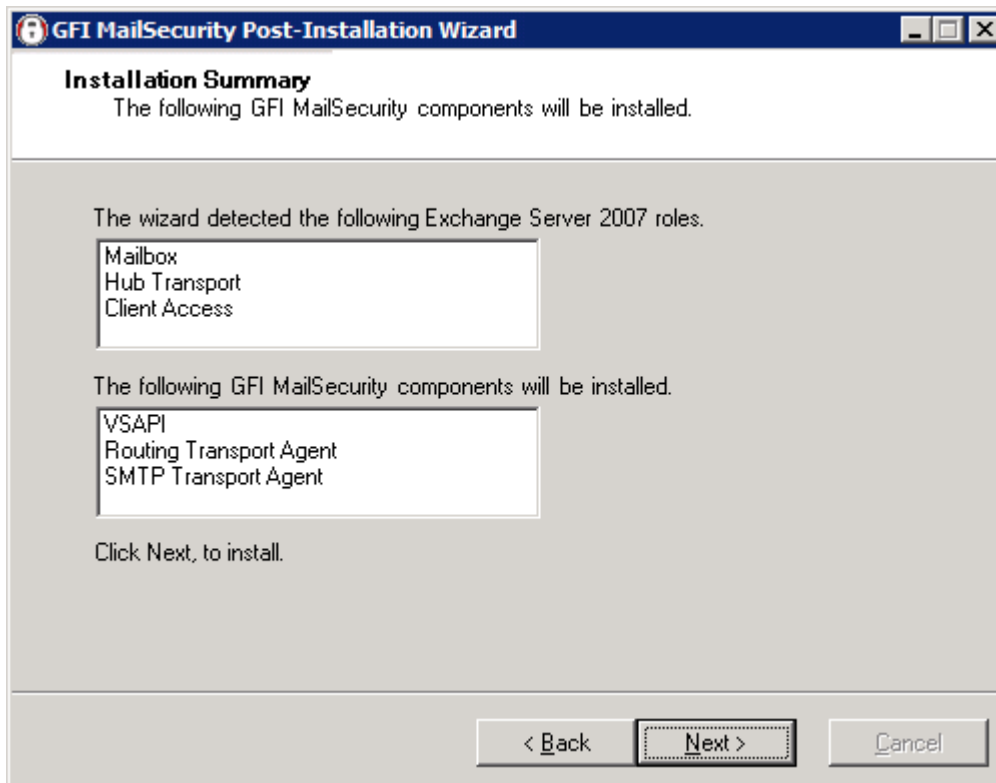
NOTE: The local domains you add from this page affect the GFI MailSecurity installation only. The Microsoft Exchange Server 2007/2010 accepted domains list is not modified.



Screenshot 13 - Local domains list

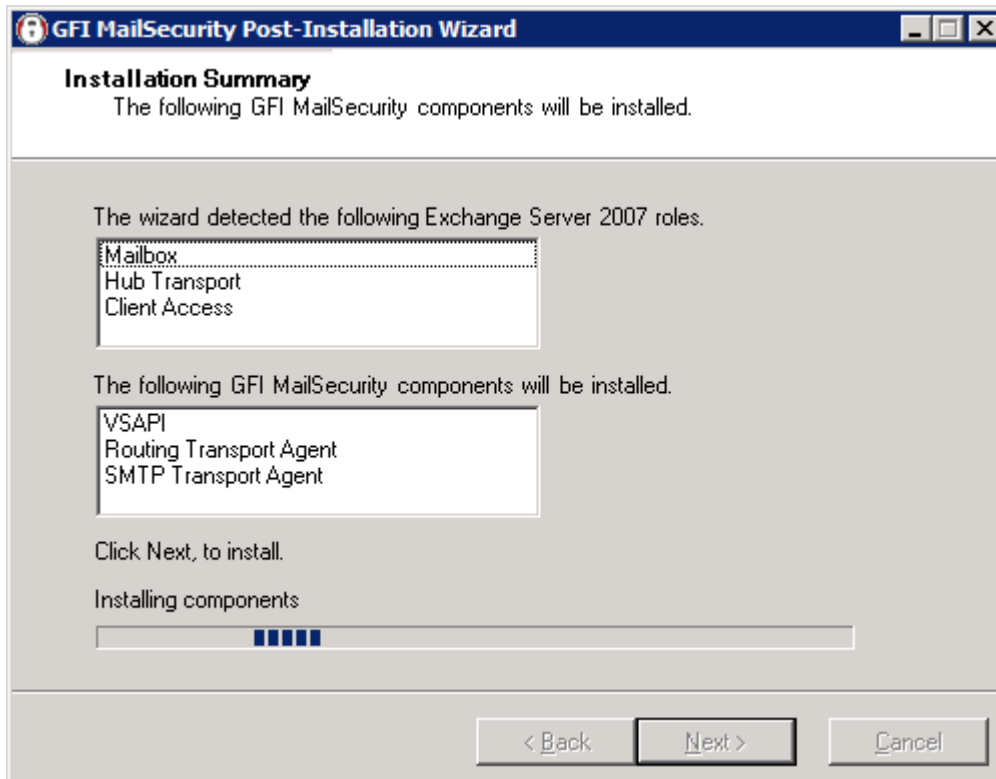
4. Click **Next** to continue.

5. The wizard displays a list of the Microsoft Exchange Server 2007/2010 server roles detected on this machine, and a list of the GFI MailSecurity components it needs to register for it to be able to process and scan emails passing through the server.



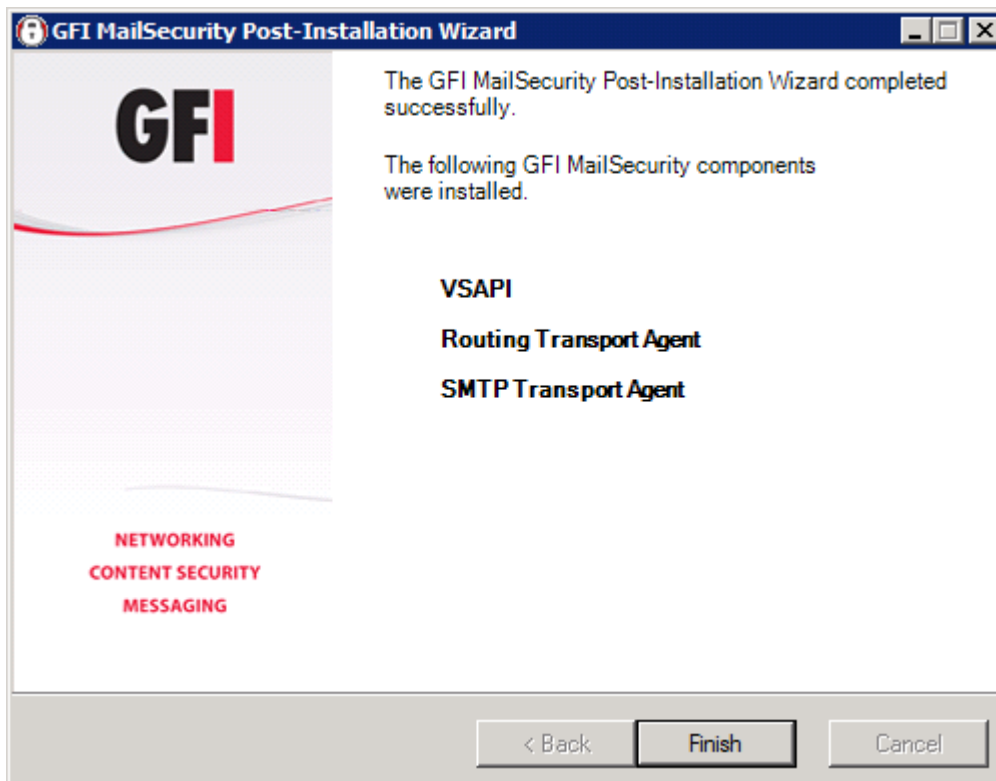
Screenshot 14 - Server roles detected and list of components to install.

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



Screenshot 15 - Installing the required GFI MailSecurity components

7. In the finish page, the GFI MailSecurity Post-Installation wizard will list the GFI MailSecurity components that it successfully installed. Click **Finish** to close the wizard and complete the installation of GFI MailSecurity on a Microsoft Exchange Server 2007/2010 machine.



Screenshot 16 - GFI MailSecurity Post-Installation Wizard finish page

2.11 Adding GFI MailSecurity to the Windows DEP Exception List

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform memory checks to help prevent malicious code from running on a system.

The DEP technology is available only on Microsoft Windows XP with Service Pack 2, Microsoft Windows Server 2003 (x32 Edition) with Service Pack 1 and Microsoft Windows Server 2003 (x64 Edition). On Microsoft Windows Server 2003 (x32 Edition) with Service Pack 1 and Microsoft Windows Server 2003 (x64 Edition), DEP is by default turned on for all programs and services except those that the administrator selects.

If you installed GFI MailSecurity on Microsoft Windows Server 2003 (x32 Edition) with Service Pack 1 or Microsoft Windows Server 2003 (x64 Edition), you will need to add the GFI MailSecurity scanning engine executable (**GFiScanM.exe**) and the Kaspersky Virus Scanning Engine executable (**kavss.exe**) to the Windows Data Execution Prevention (DEP) exception list.

To add the GFI executables in the DEP exception list follow these steps:

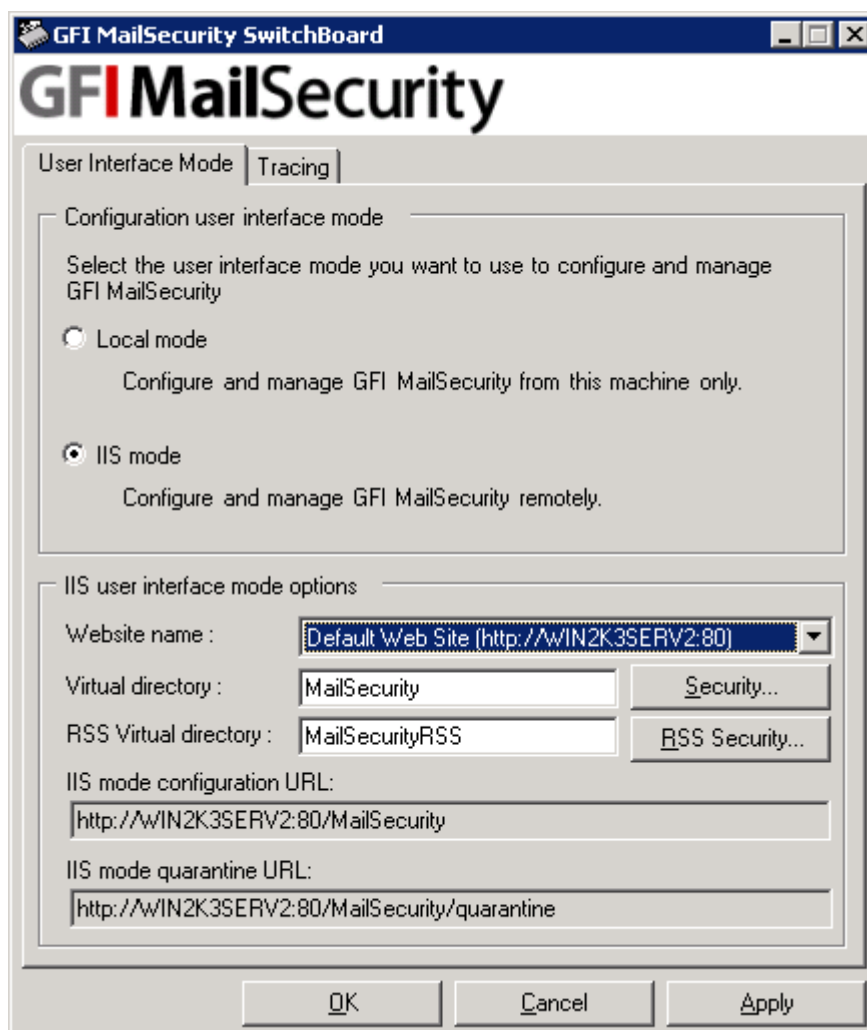
1. From the **Start** menu load the **Control Panel** and choose the **System** applet.
2. From the **Advanced** tab, click **Settings** under the **Performance** area.
3. Click the **Data Execution Prevention** tab.
4. Click **Turn on DEP for all programs and services except those I select**.
5. Click **Add** and from the dialog box browse to the GFI MailSecurity installation folder, <GFI\ContentSecurity\MailSecurity>, and choose **GFiScanM.exe**.
6. Click **Add** and from the dialog box browse to the GFI MailSecurity installation folder, <GFI\ContentSecurity\AntiVirus\Kaspersky\>, and choose **kavss.exe**.
7. Click **Apply** and **OK** to apply the changes.
8. Restart the "GFI Content Security Auto-Updater Service" and the "GFI MailSecurity Scan Engine" services.

2.12 Securing access to the GFI MailSecurity configuration/quarantine

The GFI MailSecurity configuration and quarantine store can be accessed through a web browser and thus it is imperative that you configure proper access security so that only authorized users can set-up rules and manage the quarantine store.

You can configure access security to the GFI MailSecurity configuration pages and quarantine store via the GFI MailSecurity SwitchBoard application. To configure access security, follow these steps:

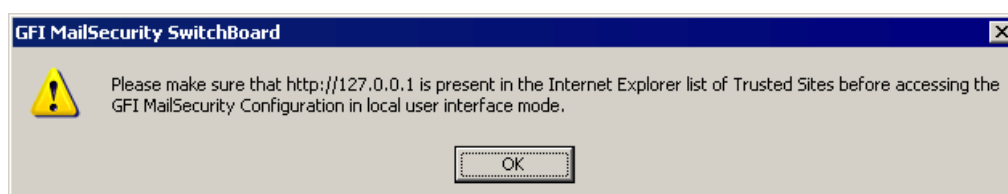
1. Click the **GFI MailSecurity SwitchBoard** shortcut found under **Start ► Programs ► GFI MailSecurity**.
2. The **GFI MailSecurity SwitchBoard** application is loaded. You now need to select whether you want to allow only local access to the Configuration and Quarantine Store or else both local and remote. To allow only local access, click **Local mode**, so that the Configuration and Quarantine Store can only be accessed when working directly on the server machine where GFI MailSecurity is installed. On the other hand, to allow both local and remote access, click **IIS mode**, so that authorized users, both from the local machine and other remote machines, can access the GFI MailSecurity Configuration and Quarantine Store.



Screenshot 17 - GFI MailSecurity SwitchBoard

3. If you selected **Local mode**, you do not need to configure anything else. If you selected **IIS mode** you now need to configure the Active Directory accounts or groups that have access to the Configuration and Quarantine Store, and you can change the virtual directory name where the GFI MailSecurity pages are stored.

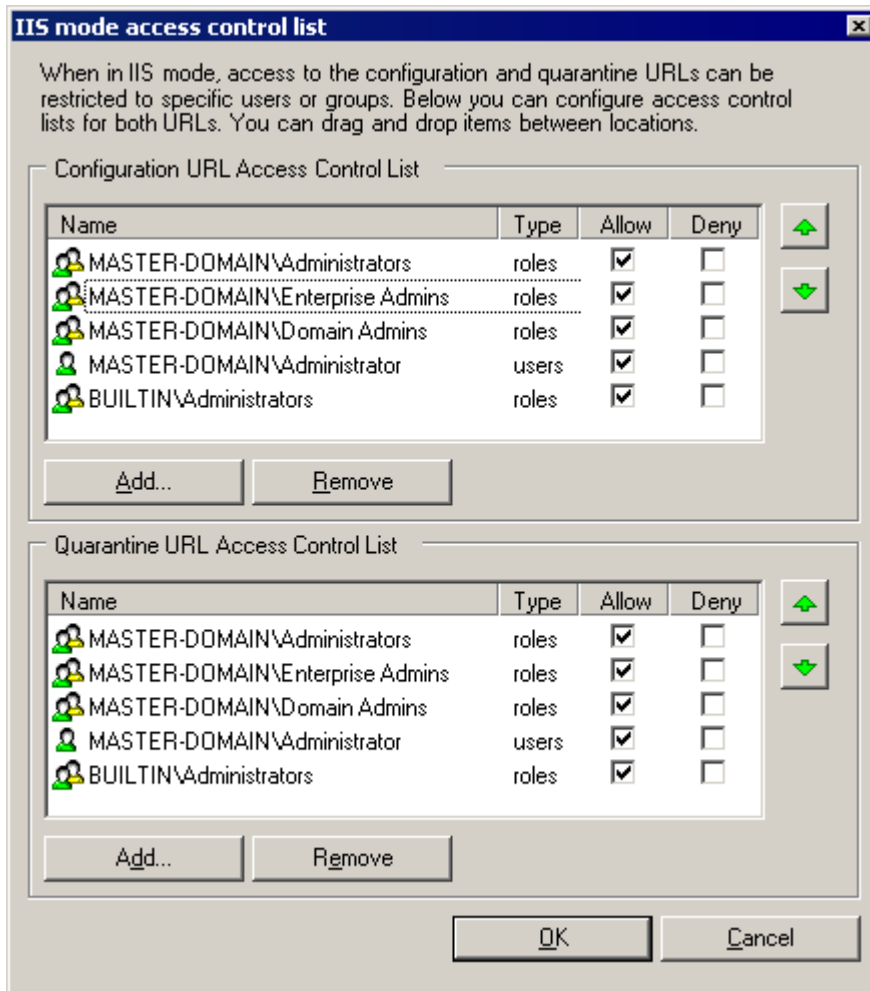
NOTE: If you select **Local mode** you need to add 'http://127.0.0.1' to the list of trusted sites in Internet Explorer. For further information, refer to [Adding local host to the trusted sites list](#) section below.



Screenshot 18 - Local host address must be added to trusted sites list

4. To configure access security, click **Security...** next to the **Virtual Directory** box.

5. In the **IIS mode access control list** dialog box you can configure who gets access to the configuration pages and the quarantine store in separate access control lists.



Screenshot 19 - Configuration / Quarantine store Access Control Lists

6. To configure the accounts that get access to the configuration pages, use the **Add** and **Remove** buttons underneath the **Configuration URL Access Control List**. If you want to deny access to a listed account without removing it from the list, select the check box under the **Deny** column.

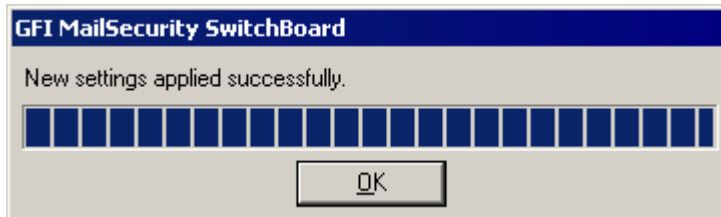
7. To configure the accounts that get access to the quarantine store, use the **Add** and **Remove** buttons underneath the **Quarantine URL Access Control List**. If you want to deny access to a listed account without removing it from the list, select the check box under the **Deny** column.

NOTE: To avoid reselecting the same accounts twice, once for each list, you can easily drag and drop accounts and groups between the two lists.

8. When ready click **OK**.

9. If you want to specify a different virtual directory name, you can do so by editing the entry in the **Virtual directory** box.

10. Click **OK** to save your changes. A progress bar shows you the progress while applying the new settings.



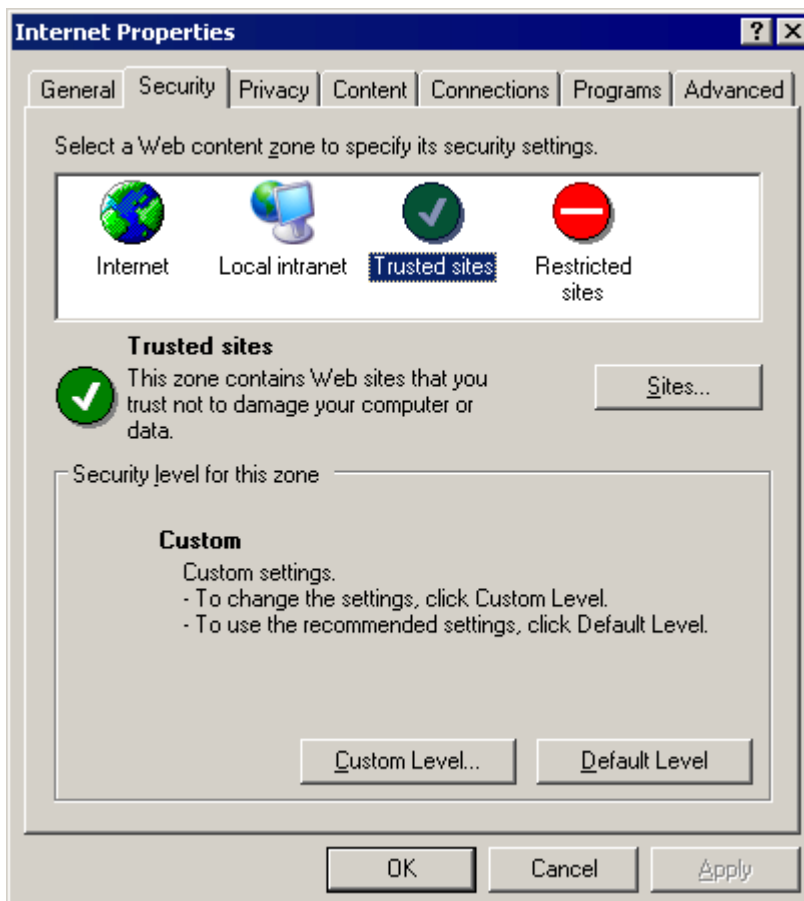
Screenshot 20 - New SwitchBoard settings successfully applied

11. When the process completes, click **OK**.

Adding local host to the trusted sites list

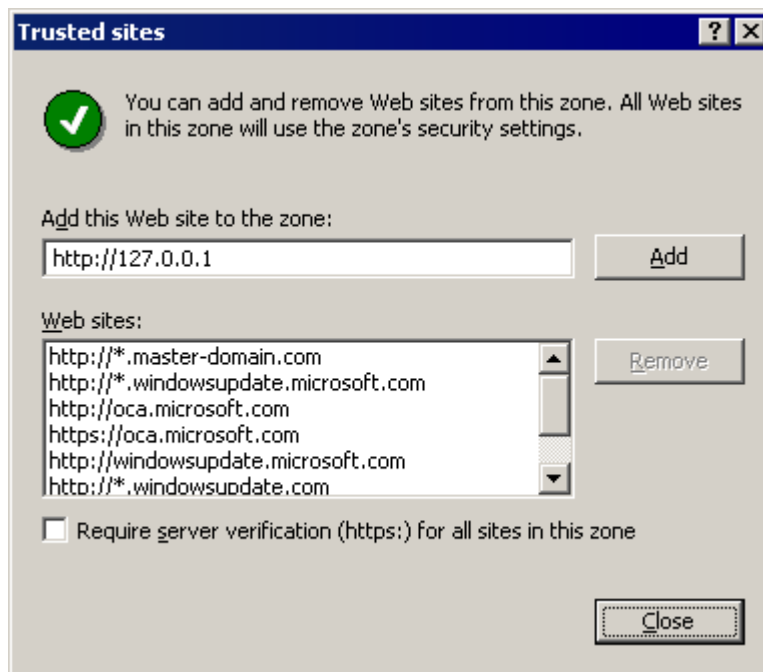
When you configure GFI MailSecurity to be accessible only locally, you need to add the local host address, 'http://127.0.0.1', to the list of trusted sites in Internet Explorer. To do this, follow these steps:

1. Click the **Control Panel** shortcut under the **Start** menu.
2. From the **Control Panel** open the **Internet Options** applet.
3. In the **Internet Properties** dialog box click the **Security** tab and then click the **Trusted sites** icon from the **Web content zone** list.



Screenshot 21 - Internet properties dialog

4. Click **Sites**.
5. In the **Trusted sites** dialog box specify 'http://127.0.0.1' in the **Add this Web site to the zone** box.
6. Click **Add**. The local host address is added to the **Web sites** list.



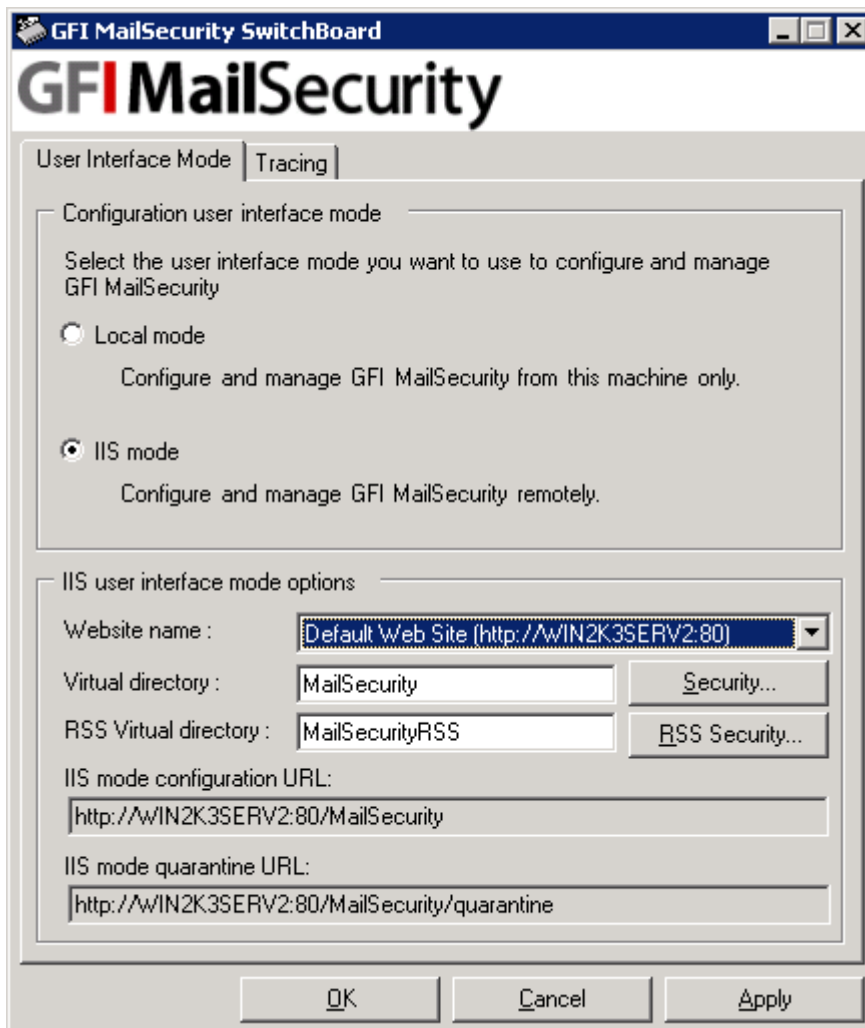
Screenshot 22 - Trusted sites dialog

7. Click **Close**.
8. Click **OK** in the **Internet Properties** dialog box to close it and save the new settings.

2.13 Securing access to the GFI MailSecurity Quarantine RSS feeds

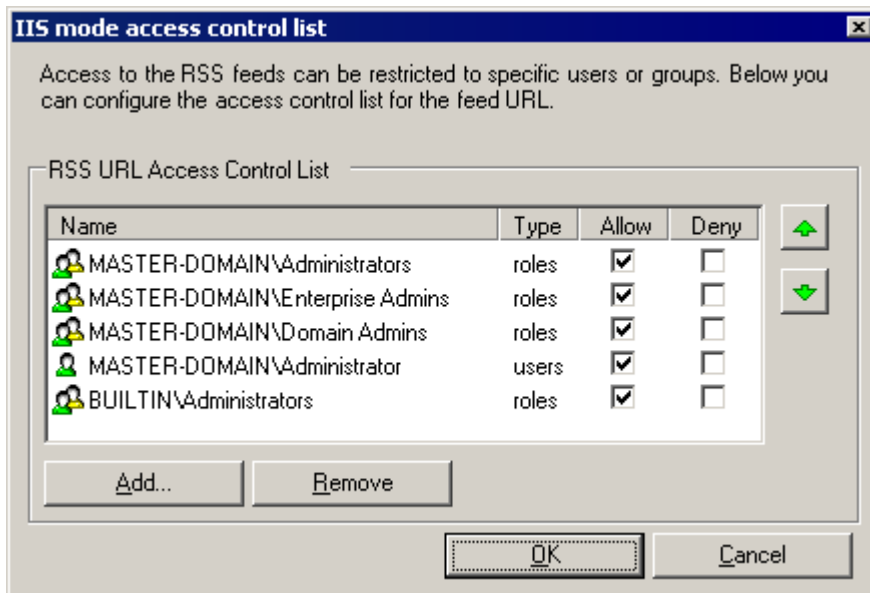
You can configure GFI MailSecurity to create quarantine RSS feeds on specific quarantine folders. To configure who can subscribe to the quarantine RSS feeds, follow these steps:

1. Click the **GFI MailSecurity SwitchBoard** shortcut found under **Start ► Programs ► GFI MailSecurity**.
2. In the **GFI MailSecurity SwitchBoard** dialog box, click **Security** next to the **RSS Virtual Directory** box.



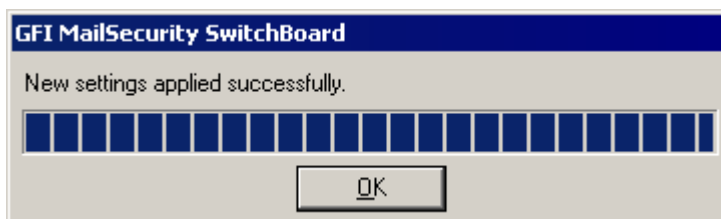
Screenshot 23 - GFI MailSecurity SwitchBoard

3. In the **IIS mode access control list** dialog box you can configure who can subscribe to the quarantine RSS feeds.



Screenshot 24 - Quarantine RSS feeds Access Control Lists

4. Use the **Add** and **Remove** buttons underneath the **RSS URL Access Control List**. If you want to deny access to a listed account without removing it from the list, select the check box under the **Deny** column.
6. When ready click **OK**.
7. If you want to specify a different virtual directory name, you can do so by editing the entry in the **RSS Virtual directory** box.
8. Click **OK** to save your changes. A progress bar shows you the progress while applying the new settings.



Screenshot 25 - New SwitchBoard settings successfully applied

9. When the process completes, click **OK**.

2.14 Accessing the GFI MailSecurity Configuration and Quarantine Store

This section will show you how to access the GFI MailSecurity Configuration and Quarantine Store from the local machine or a remote machine.

Accessing the configuration from the GFI MailSecurity machine

To access the GFI MailSecurity configuration or quarantine store from the same machine where GFI MailSecurity is installed, i.e. locally, follow these steps:

1. Click the **GFI MailSecurity** shortcut found under **Start ► Programs ► GFI MailSecurity**.
2. If you have configured GFI MailSecurity to be accessible only locally, via the GFI MailSecurity SwitchBoard application, a viewer application will automatically load up displaying the GFI MailSecurity configuration and quarantine store.



Screenshot 26 - GFI MailSecurity accessed under local mode only

Accessing the configuration from a remote machine

To access the GFI MailSecurity configuration or quarantine store from a remote machine, follow these steps:

1. Start Microsoft Internet Explorer.
2. In the address bar, specify the following address:

'http://<machine name>/<virtual directory name>' to access the configuration or 'http://<machine name>/<virtual directory name>/quarantine' to access the quarantine store directly.

For example:

'http://win2k3entsvr.master-domain.com/mailsecurity' for the configuration or 'http://win2k3entsvr.master-domain.com/mailsecurity/quarantine' for the quarantine store.

3. You will be prompted to specify a user name and password to authenticate and determine whether you have access to the page requested. If the

account specified has access, the GFI MailSecurity configuration or quarantine store is displayed.



Screenshot 27 - GFI MailSecurity accessed under IIS mode

2.15 Upgrading from GFI MailSecurity 8 to GFI MailSecurity 10.1

Due to fundamental architectural changes between GFI MailSecurity 10.1 and GFI MailSecurity 8, it is not possible to install GFI MailSecurity 10.1 on top of an existing installation of GFI MailSecurity 8.

This section therefore shows you how to:

- Replace your current GFI MailSecurity 8 installation with GFI MailSecurity 10.1.
- Convert and import the GFI MailSecurity 8 configuration settings to GFI MailSecurity 10.1's new configuration database format.

NOTE: If GFI MailSecurity 8 was installed in SMTP mode and GFI MailSecurity 10.1 is installed in Active Directory mode, you will not be able to convert and import the settings due to user-based rules. This also applies if

GFI MailSecurity 8 was installed in Active Directory mode and GFI MailSecurity 10.1 is installed in SMTP mode.

To upgrade from GFI MailSecurity 8 to GFI MailSecurity 10.1, follow these steps:

1. Uninstall GFI MailSecurity 8.
2. When the GFI MailSecurity 8 uninstallation completes, certain files are left behind under the root folder where GFI MailSecurity 8 was installed. One of these files is the avapicfg.rdb file located in the Data sub-folder.

NOTE: Do not delete this file since it contains the GFI MailSecurity 8 configuration settings. You will need this file to migrate the settings from GFI MailSecurity 8 to GFI MailSecurity 10.1.

3. Install GFI MailSecurity 10.1 as shown in the 'Install GFI MailSecurity' section of this chapter.

NOTE: To install GFI MailSecurity 10.1, you need to have the following installed on the machine:

- Microsoft .Net framework 1.1 / 2.0
- MSMQ - Microsoft Messaging Queuing Service.
- Internet Information Services (IIS) - SMTP service and World Wide Web service.

NOTE: Do not install GFI MailSecurity 10.1 to the same path where GFI MailSecurity 8 was installed, to prevent files such as avapicfg.rdb from being overwritten.

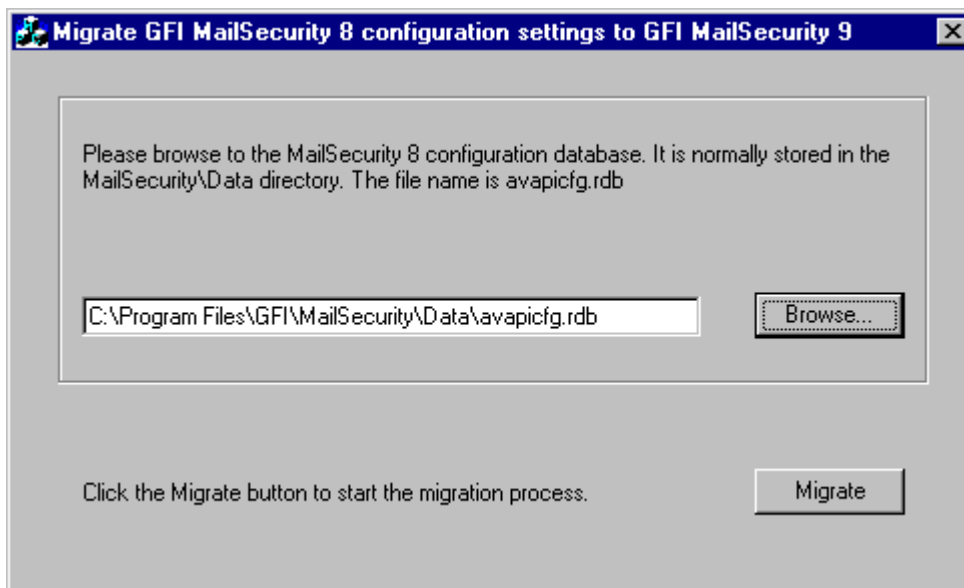
4. After the installation of GFI MailSecurity 10.1 is complete, you need to stop all GFI-related services along with the IIS Admin service, from the Services control applet. Then you can run the GFI MailSecurity 8 settings migration tool.

NOTE: You must stop the following services before going on to the next step:

- GFI Content Security Attendant Service
- GFI Content Security Auto-Updater Service
- GFI MailSecurity Attendant Service
- GFI MailSecurity Scan Engine
- IIS Admin
- Simple Mail Transfer Protocol (SMTP).

5. To convert and import the GFI MailSecurity 8 settings to the GFI MailSecurity 10.1 configuration database, you need to run the msec8upg.exe tool found in the GFI MailSecurity 10.1 folder, for example:

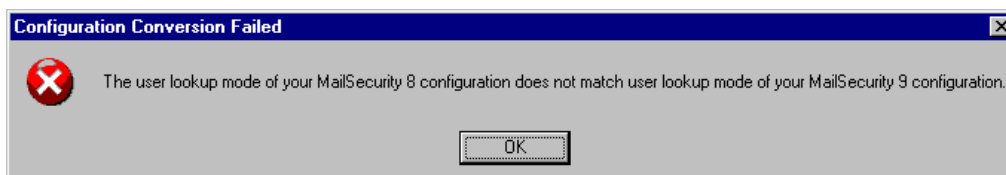
c:\program files\GFI\ContentSecurity\MailSecurity.




Screenshot 28 - GFI MailSecurity 8 configuration settings migration tool

6. Double-click the msec8upg.exe file.
7. When the tool loads, click **Browse**. Select the avapicfg.rdb file from the data sub-folder under the GFI MailSecurity 8 root folder.
8. Click **Migrate**.

NOTE: If you click **Migrate** and the user lookup mode of GFI MailSecurity 8 and GFI MailSecurity 10.1 do not match (for example GFI MailSecurity 8 was installed in SMTP mode and GFI MailSecurity 10.1 is installed in Active Directory mode or vice versa), an error like the one shown below will be displayed. In such a case, you will not be able to convert and import the settings due to user-based rules.



Screenshot 29 - User lookup mode mismatch.

9. When the migration process completes, a Configuration was successfully converted information dialog box will be displayed. Click OK to close the information dialog box and click the close button  to close the migration tool.
10. You now need to start all the services that you stopped in step 4 above, from the Services control applet.
11. Use the GFI MailSecurity 10.1 configuration to check that the GFI MailSecurity 8 settings were migrated correctly.

2.16 Upgrading from GFI MailSecurity 9 to GFI MailSecurity 10.1

NOTE: The upgrade process cannot be reverted. If you upgrade GFI MailSecurity to version 10.1, you cannot go back to version 9 of the product.

If you are currently using GFI MailSecurity 9, you can upgrade your current installation. The GFI MailSecurity 9 configuration settings are kept. You need to enter the fully purchased license key after the upgrade completes. For information on how to obtain the new license key, visit <http://customers.gfi.com>.

To upgrade:

1. Launch the GFI MailSecurity 10.1 setup file on the machine on which you have installed GFI MailSecurity 9.
2. Setup will now proceed to install GFI MailSecurity 10.1 in exactly the same manner as a new installation. However, it will not let you change the destination folder.
3. To continue the installation, click **Install**. For a detailed description, of the installation procedure, refer to the [Installing GFI MailSecurity](#) section earlier in this chapter.

NOTE: During an upgrade you are also asked to upgrade your quarantine database to the new Firebird database format. For more information, refer to [Quarantine Upgrade tool](#) section in this manual.

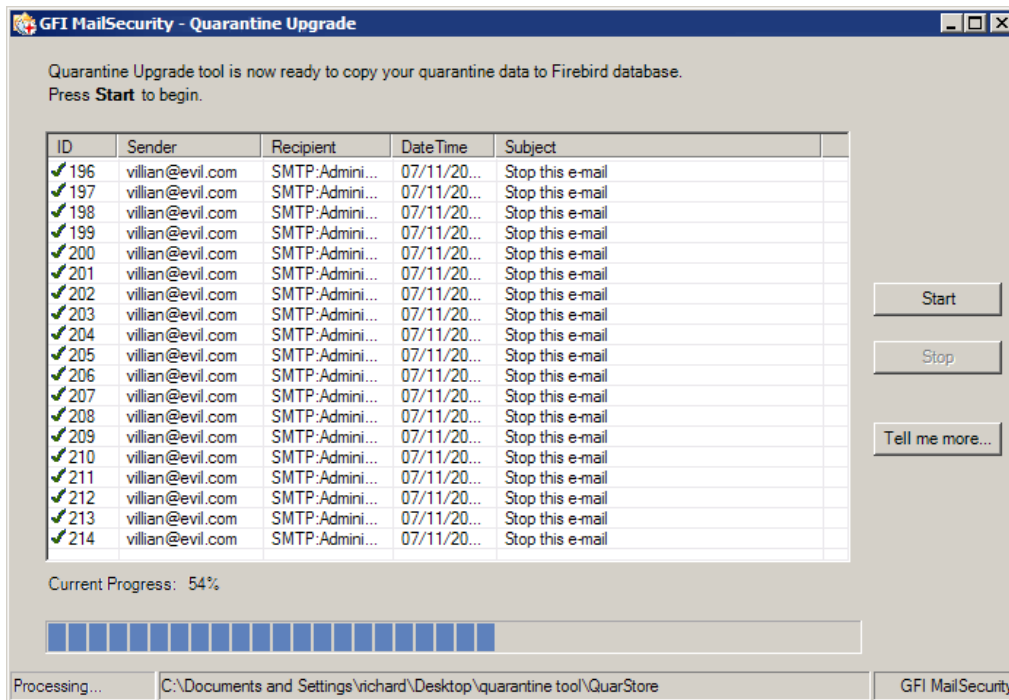
2.17 Quarantine Upgrade tool

Starting from GFI MailSecurity 10 SR8, Quarantine information is stored in a Firebird database format instead of Microsoft Access database. For upgrades between version 9 and 10 and between previous builds of version 10 to GFI MailSecurity 10 SR8, the Quarantine upgrade tool automates the migration of pre-existing quarantine data to the new Firebird database format.

NOTE: The old quarantine data will not be available until imported.

2.17.1 Using the quarantine upgrade tool

The Quarantine upgrade tool is automatically launched after installing the upgrade to GFI MailSecurity SR8. In case you need to launch it manually, navigate to the GFI MailSecurity installation folder (typically Program Files\GFI\ContentSecurity\MailSecurity\) and run QssUpgrade.exe



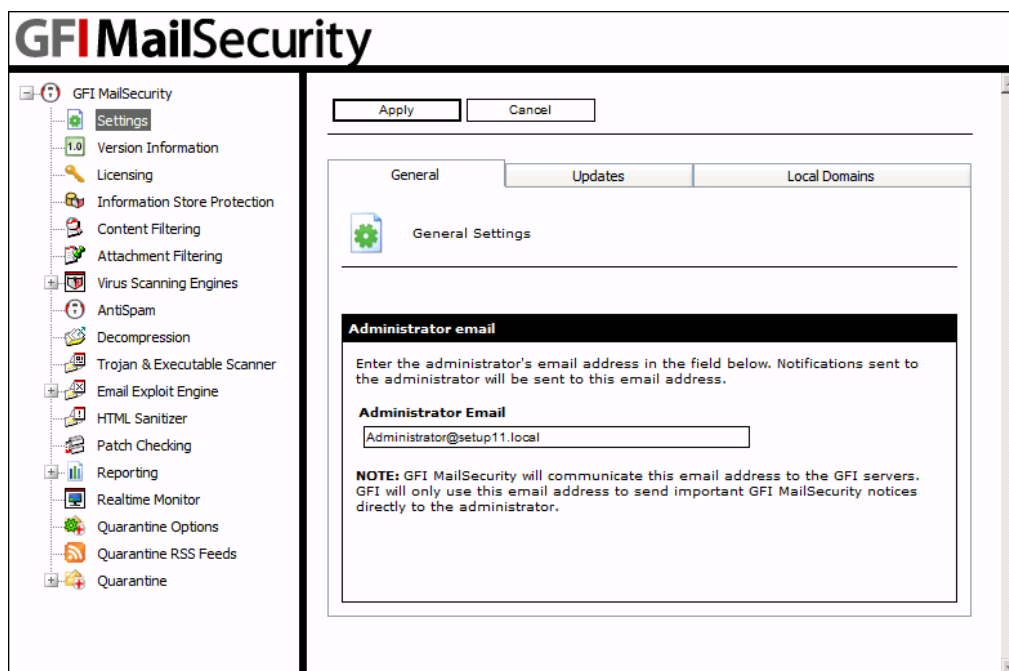
Screenshot 30 - Quarantine upgrade tool

1. Press **Start** button to start data migration.
2. Press **Pause/Continue** button to pause or continue data processing.
3. Press **Stop** button to cancel your data migration and restart at a later stage by pressing Start again.

NOTE: Upgrading your quarantine to the firebird database format might take long depending on the volume of your quarantine data.

3 General settings

3.1 Introduction to settings



Screenshot 31 - GFI MailSecurity general settings page

The **Settings** node allows you to configure a number of general options, including the administrator's email address, the Update URLs, the list of Local Domains, the SMTP server bindings and the management of the user list when GFI MailSecurity is installed in SMTP mode only. To configure the general settings, click the **GFI MailSecurity ► Settings** node.

3.2 Define the administrator's email address

GFI MailSecurity can be configured to send email notifications to the administrator whenever a security threat is found in an email. To set up the administrator's notification address:

1. Click the **Settings** node to open the **General Settings** page in the right window.
2. In the **General** tab, specify the email address where you wish to send email notifications addressed to the administrator in the **Administrator Email** box.
3. Click **Apply**.

3.3 Configuring proxy server settings for automatic updates

GFI MailSecurity will automatically search and download updates (for example, virus definitions updates and Trojan & Executable Scanner definitions updates) from the GFI update servers.

If the server on which GFI MailSecurity is installed, connects to the internet through a proxy server, you need to configure the proxy server settings as follows:

1. Click the **Settings** node to open the general settings page.
2. Click the **Updates** tab.
3. Select the **Enable proxy server** check box. In the **Proxy server** and **Port** boxes specify the Machine Name / IP of the proxy server and the port to connect on respectively. If the proxy server requires authentication, select the **Enable proxy authentication** check box and specify the user name and password in the **Username** and **Password** boxes respectively.

Proxy server settings

Configure proxy settings

☒ **Enable proxy server**

Proxy server:

Port:

Proxy authentication settings

Configure proxy authentication settings

☒ **Enable proxy authentication**

Username:

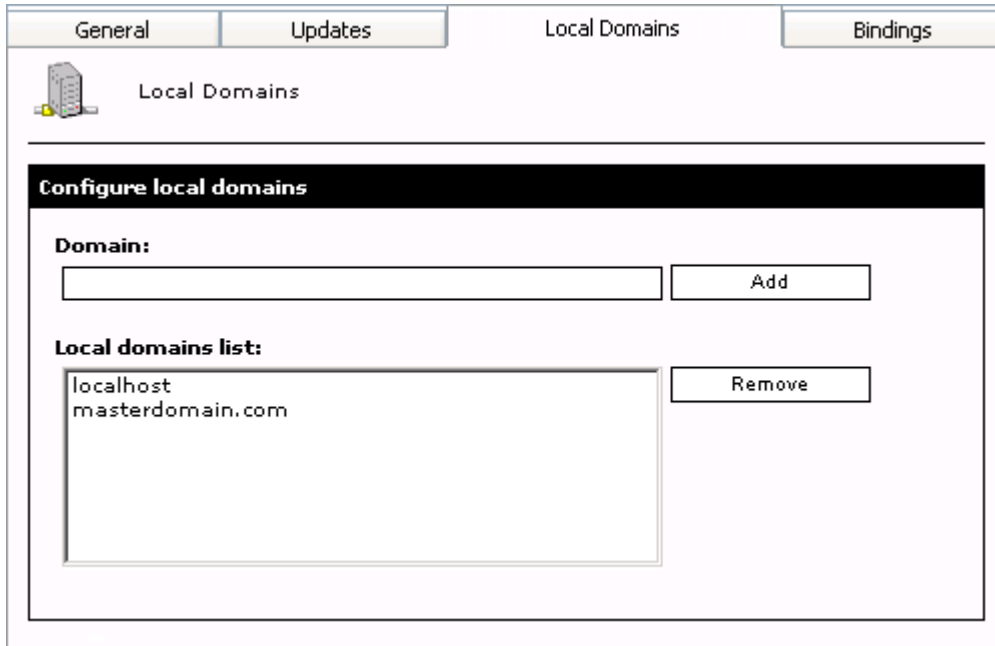
Password:

* For security reasons, the length in the password box above does not necessarily reflect the true password length

Screenshot 32 - Updates server proxy settings

4. Click **Apply**.

3.4 Adding Local Domains



Screenshot 33 - Local Domains list

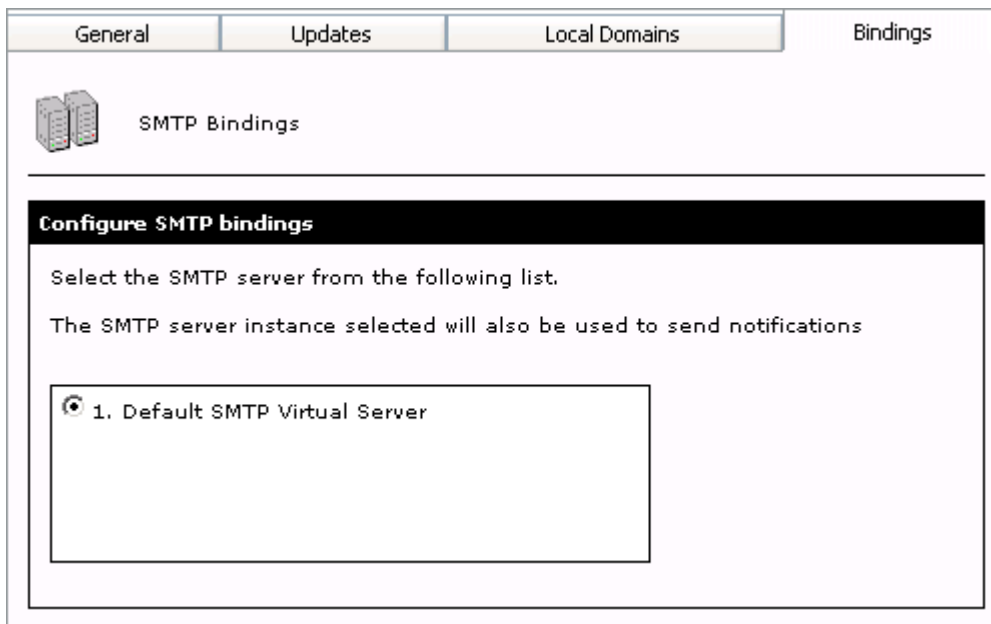
GFI MailSecurity needs to know what your local domains are to be able to classify an email as inbound or outbound. During installation, GFI MailSecurity will import local domains from the IIS SMTP service. If, however, you wish to add or remove local domains afterwards, you must follow these steps:

1. Click the **Settings** node to open the general settings page.
2. Click the **Local Domains** tab and specify the name of the domain in the **Domain** box.
3. Click **Add** to include the stated domain in the **Local domains list**. If you want to remove a listed domain, select it from the list and click **Remove**.
4. Click **Apply**.

NOTE: You can use the local domains option if you want to configure local mail routing in IIS differently, for example, to add domains that are local for mail routing purposes but which are not local for your mail server.

3.5 SMTP server bindings

NOTE: The SMTP Server bindings tab is not visible when GFI MailSecurity is installed on a Microsoft Exchange Server 2007/2010 machine.



Screenshot 34 - Binding GFI MailSecurity to a different SMTP Server

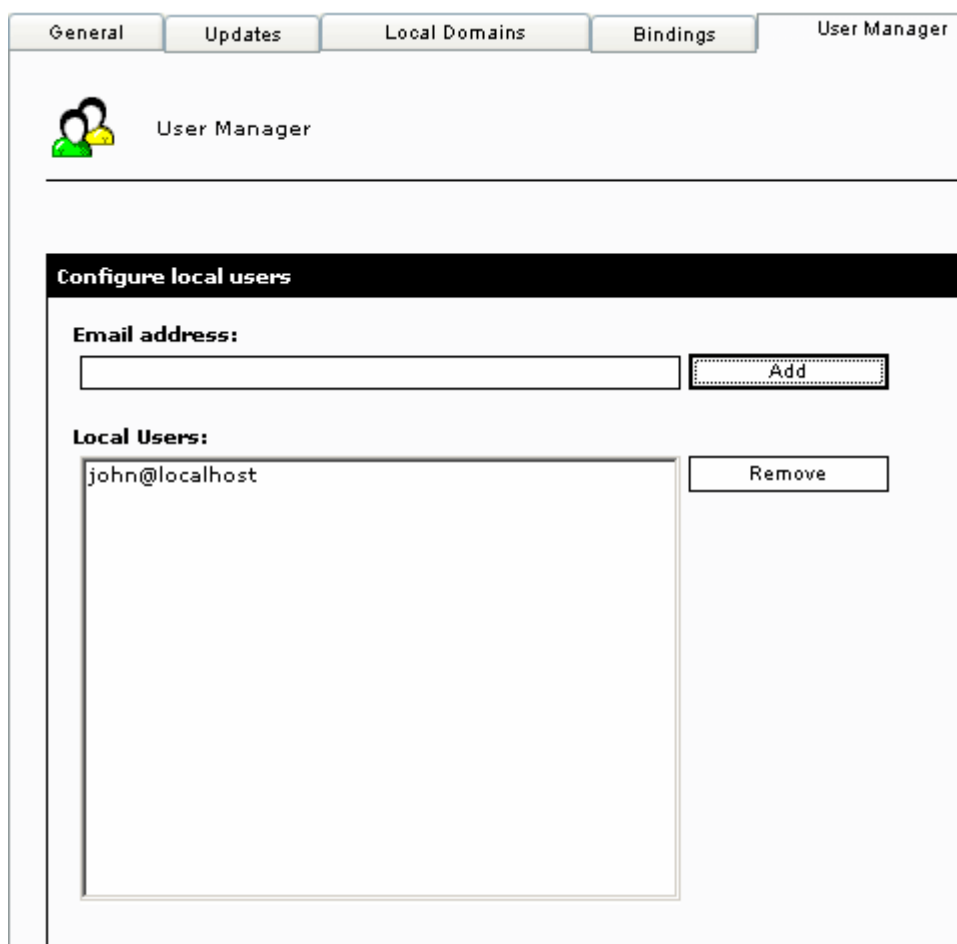
GFI MailSecurity relies on the IIS SMTP service to send and receive SMTP mail. By default, it binds to your default SMTP virtual server. However, if you have multiple SMTP virtual servers installed on your machine, you can select to which one you want to bind GFI MailSecurity. You can select your virtual SMTP server both during the installation stage as well as from the **Bindings** tab after the installation. To change the current SMTP Virtual Server:

1. Click the **Settings** node to open the general settings page in the right window.
2. Click the **Bindings** tab and select the required SMTP Virtual Server from the available list of servers present in your domain.
3. Click **Apply**.

3.6 Managing local users in SMTP mode

When you install GFI MailSecurity in Active Directory mode, the list of local users is stored in the Active Directory store. When you choose to install GFI MailSecurity in SMTP mode, the list of local users is stored in a database managed by GFI MailSecurity.

To populate and manage the user list when GFI MailSecurity is installed in SMTP mode, a **User Manager** is available under the **Settings** node.



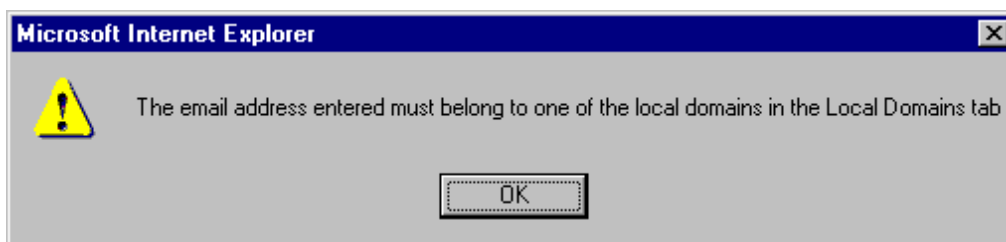
Screenshot 35 - User Manager

The **User Manager** tab displays the current list of local users, and it allows you to add or remove local users. The list of local users entered here is used when configuring user-based rules, such as Attachment Checking rules and Content Checking rules.

To add a new local user follow these steps:

1. Enter the email address in the **Email address** box.
2. Click **Add**.

NOTE: GFI MailSecurity uses the local domains list, configurable from the **Local Domains** tab, to determine whether a new email address is local or not. A notification dialog box is displayed if you enter a non-local user, as shown in the screenshot below.



Screenshot 36 - Non-local user entered

3. Repeat steps 1 and 2 to add more than one local user.
4. Click **Apply**.

To remove a local user follow these steps:

1. Select the local user you want to remove from the **Local Users** list.
2. Click **Remove**.
3. Repeat steps 1 and 2 to remove more than one local user.
4. Click **Apply**.

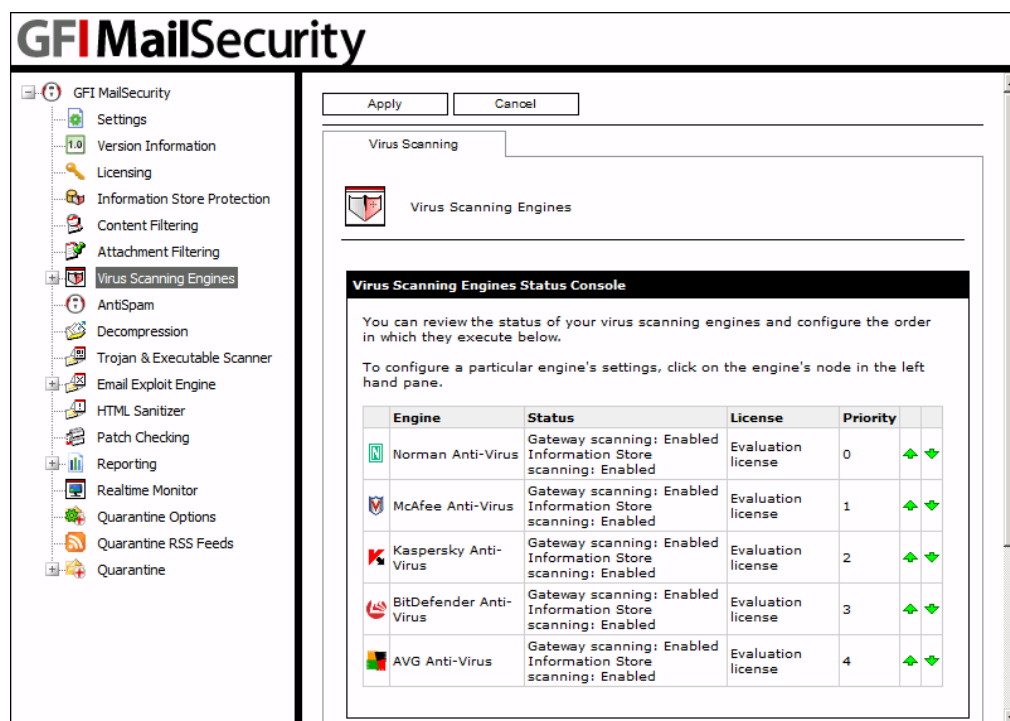
4 Configuring virus checking

4.1 Configuring Virus Scanning Engines

The virus-checking feature of GFI MailSecurity scans all SMTP traffic, inbound and outbound emails, for viruses using multiple Virus Scanning Engines. When GFI MailSecurity is installed on the Microsoft Exchange server machine, you can also configure GFI MailSecurity to scan the information store for viruses.

NOTE: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007/2010 machine, **Information Store Protection** is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

GFI MailSecurity ships with both Norman and BitDefender Virus Scanning Engine as standard. However, you can optionally license the AVG, Kaspersky and McAfee Virus Scanning Engines, which are supported as well. All of the aforementioned anti-virus packages are proven and reliable virus detection engines, which have received many awards and certifications, including the industry leading certifications of ICSSA.



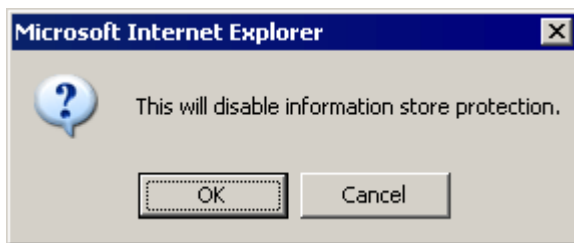
Screenshot 37 - Virus Scanning Engines status page

You can view the operational and license status of each Virus Scanning Engine along with the execution sequence of the installed Virus Scanning Engines by clicking on the **GFI MailSecurity ► Virus Scanning Engines** node.

The Virus Scanning Engines are listed in the same order of priority used by GFI MailSecurity to scan emails for viruses (Priority 0 being the highest or top priority).

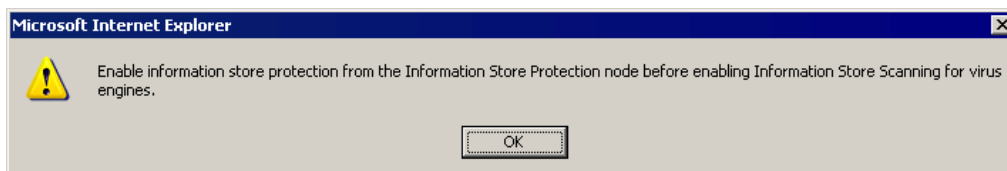
Each Virus Scanning Engine must be configured separately. To configure virus checking, click the required Virus Scanning Engine from the Status page on display in the right window. Alternatively, you can expand the **Virus Scanning Engines** node and click the required Virus Scanning Engine node (for example, Kaspersky).

NOTE: If you are running GFI MailSecurity on a Microsoft Exchange machine and the **Information Store Scanning** status is set to **Disabled** for all Virus Scanning Engines, the Information Store Scanning feature is disabled. The GFI MailSecurity configuration will inform you with a dialog that the Information Store Scanning feature is going to be disabled since you are trying to disable the only Virus Scanning Engine left which is set to scan the Information Store. If you click **OK**, the particular virus-scanning engine will have the Information Store Scanning feature disabled and so will the overall Information Store Scanning feature. If you click **Cancel**, the virus-scanning engine will not have the Information Store Scanning feature disabled and the overall Information Store Scanning feature will remain active since there is at least one virus-scanning engine that is still configured to scan the Information Store.



Screenshot 38 - Information Store Scanning will be disabled.

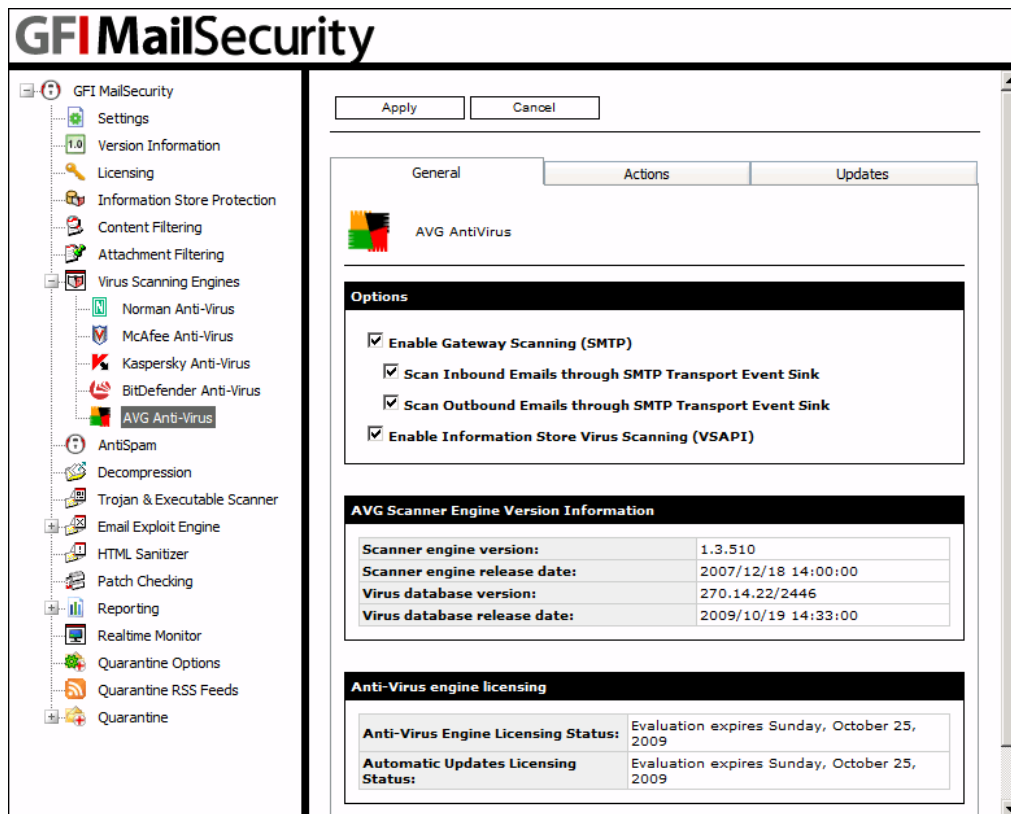
If the overall Information Store Scanning feature is disabled, you need to enable it from the **Information Store Protection** node before you can configure any Virus Scanning Engine to scan the Information Store. If you try to configure a Virus Scanning Engine to scan the Information Store and the feature is disabled from the **Information Store Protection** node, the GFI MailSecurity configuration will inform you about this with a dialog as shown in the screenshot below.



Screenshot 39 - Enable Information Store protection before configuring a Virus Scanning Engine

4.2 AVG configuration

NOTE: The AVG virus engine must be purchased separately: This engine is not included in the base product. As standard, GFI MailSecurity includes both the Norman and the BitDefender anti-virus engines. For pricing information on adding the AVG anti-virus engine, please visit the GFI website (www.gfi.com).



Screenshot 40 - Anti-virus Scanning Engines: AVG configuration page (General Tab)

To configure the AVG engine:

1. Expand the **GFI MailSecurity ► Virus Scanning Engines** node and then click **AVG**.
2. To scan SMTP traffic using this Virus Scanning Engine, select the **Enable Gateway Scanning (SMTP)** check box. You now need to select whether you want to scan inbound and outbound emails using this Virus Scanning Engine. To scan inbound emails select the **Scan Inbound Emails through SMTP Transport Event Sink** check box. To scan outbound emails select the **Scan Outbound Emails through SMTP Transport Event Sink** check box.
3. If you installed GFI MailSecurity on the Microsoft Exchange machine, you will also have the option to scan the Information Store using this Virus Scanning Engine. To scan the Information Store select the **Enable Information Store Virus Scanning (VSAPI)** check box.

NOTE: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007/2010 machine, information store scanning is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

4. The configuration settings required in the **Actions** and **Updates** tabs are identical for all the installed virus-scanning engines. For more information on how to configure these parameters, refer to the [Virus scanner actions](#) and 'Virus scanner updates' sections in this chapter.

5. After you have configured all the required parameters, click **Apply**. All changes and configuration settings will take effect immediately.

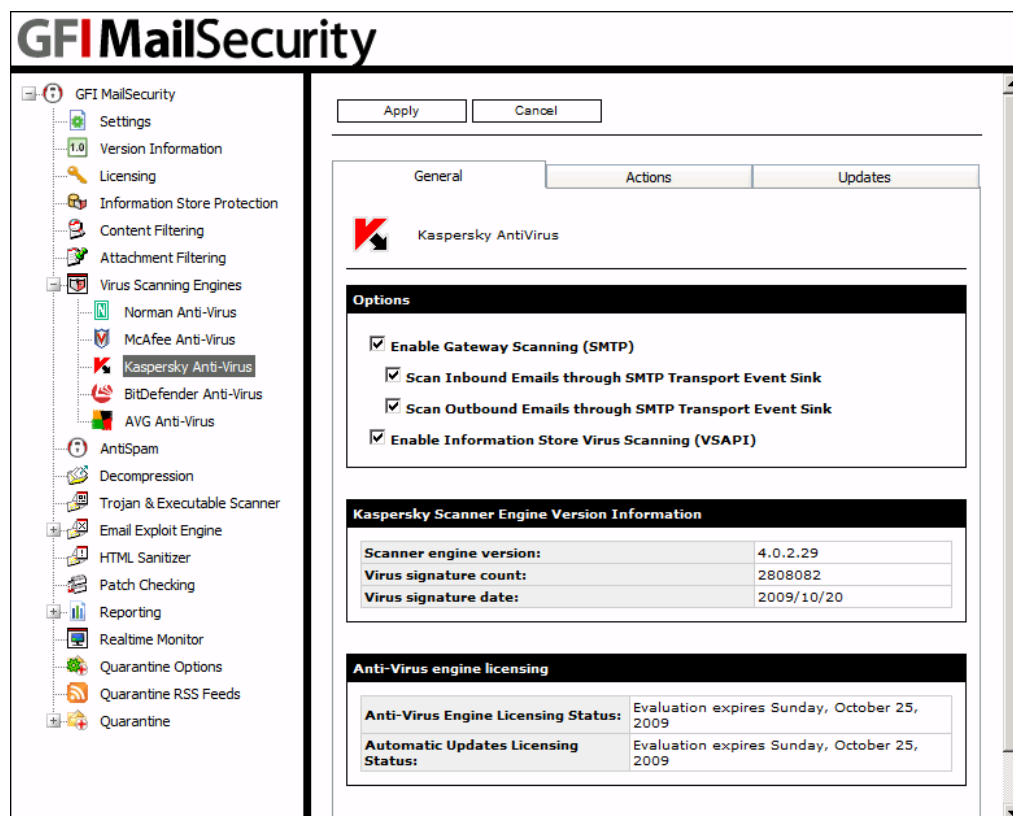
NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus database version and release date. License details for the current anti-virus engine are also displayed.

AVG web site

For more information about the virus patterns included in the AVG engine, visit the AVG website at <http://www.grisoft.com>.

4.3 Kaspersky configuration

NOTE: The Kaspersky virus engine must be purchased separately: This engine is not included in the base product. As standard, GFI MailSecurity includes both the Norman and the BitDefender anti-virus engines. For pricing information on adding the Kaspersky anti-virus engine, please visit the GFI website (www.gfi.com).



Screenshot 41 - Anti-virus Scanning Engines: Kaspersky configuration page (General Tab)

To configure the Kaspersky engine:

1. Expand the **GFI MailSecurity ► Virus Scanning Engines** node and then click **Kaspersky**.
2. To scan SMTP traffic using this Virus Scanning Engine, select the **Enable Gateway Scanning (SMTP)** check box. You now need to select whether you want to scan inbound and outbound emails using this Virus Scanning Engine. To scan inbound emails select the **Scan Inbound Emails through SMTP Transport Event Sink** check box. To scan outbound emails select the **Scan Outbound Emails through SMTP Transport Event Sink** check box.

3. If you installed GFI MailSecurity on the Microsoft Exchange machine, you will also have the option to scan the Information Store using this Virus Scanning Engine. To scan the Information Store select the **Enable Information Store Virus Scanning (VSAPI)** check box.

NOTE: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007/2010 machine, information store scanning is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

4. The configuration settings required in the **Actions** and **Updates** tabs are identical for all the installed Virus Scanning Engines. For more information on how to configure these parameters, refer to [Virus scanner actions](#) and [Virus scanner updates](#) sections in this chapter.

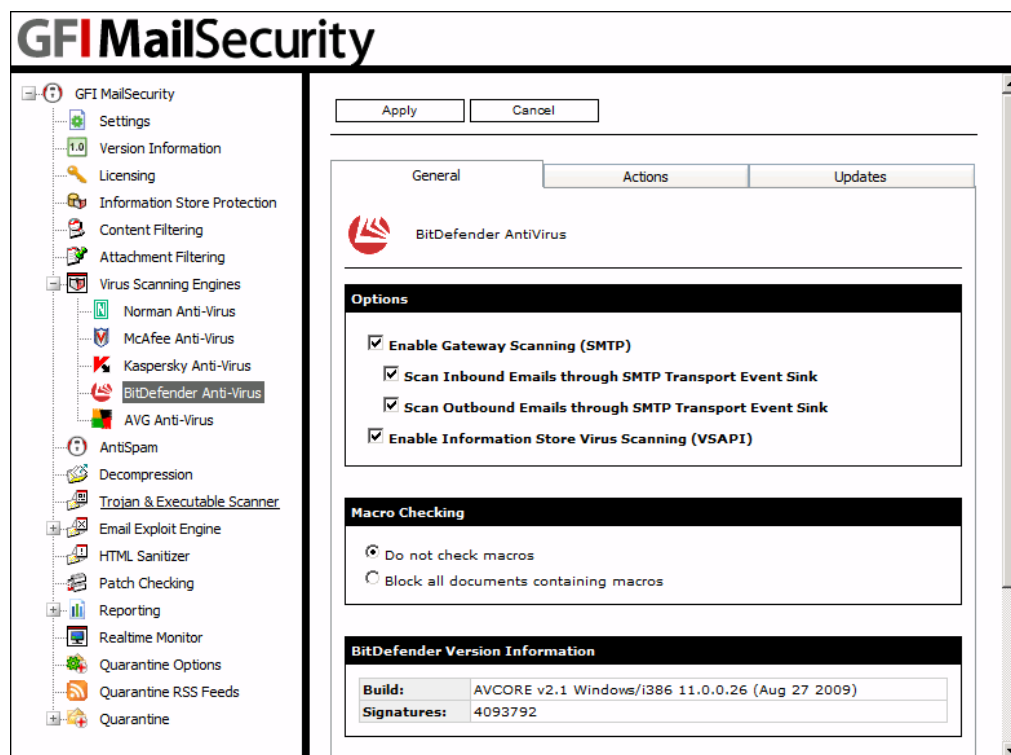
5. After you have configured all the required parameters, click **Apply**. All changes and configuration settings will take effect immediately.

NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus Scanning Engine version, virus signature count and the date of the current virus signature files. License details for the current anti-virus engine are also displayed.

Kaspersky web site

For more information about the virus patterns included in the Kaspersky engine, visit the Kaspersky website at <http://www.kaspersky.com>.

4.4 BitDefender configuration



Screenshot 42 - Virus Scanning Engines: BitDefender configuration page (General Tab)

To configure the BitDefender engine:

1. Expand the **GFI MailSecurity ► Virus Scanning Engines** node and then click **BitDefender**.

2. To scan SMTP traffic using this Virus Scanning Engine, select the **Enable Gateway Scanning (SMTP)** check box. You now need to select whether you want to scan inbound and outbound emails using this Virus Scanning Engine. To scan inbound emails select the **Scan Inbound Emails through SMTP Transport Event Sink** check box. To scan outbound emails select the **Scan Outbound Emails through SMTP Transport Event Sink** check box.

3. If you installed GFI MailSecurity on the Microsoft Exchange machine, you will also have the option to scan the Information Store using this Virus Scanning Engine. To scan the Information Store select the **Enable Information Store Virus Scanning (VSAPI)** check box.

NOTE: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007/2010 machine, information store scanning is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

4. BitDefender Control also allows you to block or ignore emails with attachments that contain macros. This feature can be configured by selecting one of the following options:

- **Do not check macros** - Select this option if you want GFI MailSecurity to ignore macros and only scan emails for viruses.
- **Block all documents containing macros** - Select this option if you want to quarantine all emails that contain a macro (even if the macro is a genuine one).

NOTE: Quarantining of emails depends on the Actions configured in the Virus Scanning Engine. If you select **Delete item** in the **Actions** tab of the Antivirus Engine, all emails containing macros will still be DELETED (i.e. they are NOT Quarantined).

5. The configuration settings required in the Actions and Updates tabs are identical for all the installed Virus Scanning Engines. For more information on how to configure these parameters, refer to the [Virus scanner actions](#) section and [Virus scanner updates](#) section in this chapter.

6. After you have configured all the required parameters, click **Apply**. All changes and configuration settings will take effect immediately.

NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus Scanning Engine version and the virus signature count. License details for the current anti-virus engine are also displayed.

BitDefender website

For more information about the virus patterns included in the BitDefender engine, visit the BitDefender website at <http://www.bitdefender.com>

4.5 McAfee configuration

NOTE: The McAfee engine is purchased separately: the engine is not included in the base product. As standard, GFI MailSecurity includes both the

Norman and the BitDefender anti-virus engine. For pricing information on adding the McAfee anti-virus engine, please visit the GFI website (www.gfi.com).

The configuration options of the McAfee Virus Scanning Engine are identical to those of the BitDefender engine. For more information on how to configure these options, refer to [BitDefender configuration](#) section earlier in the manual.

NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus Scanning Engine version, virus signature count and the date of the current virus signature files. License details for the current anti-virus engine are also displayed.



Screenshot 43 - Virus Scanning Engines: McAfee configuration page (General Tab)

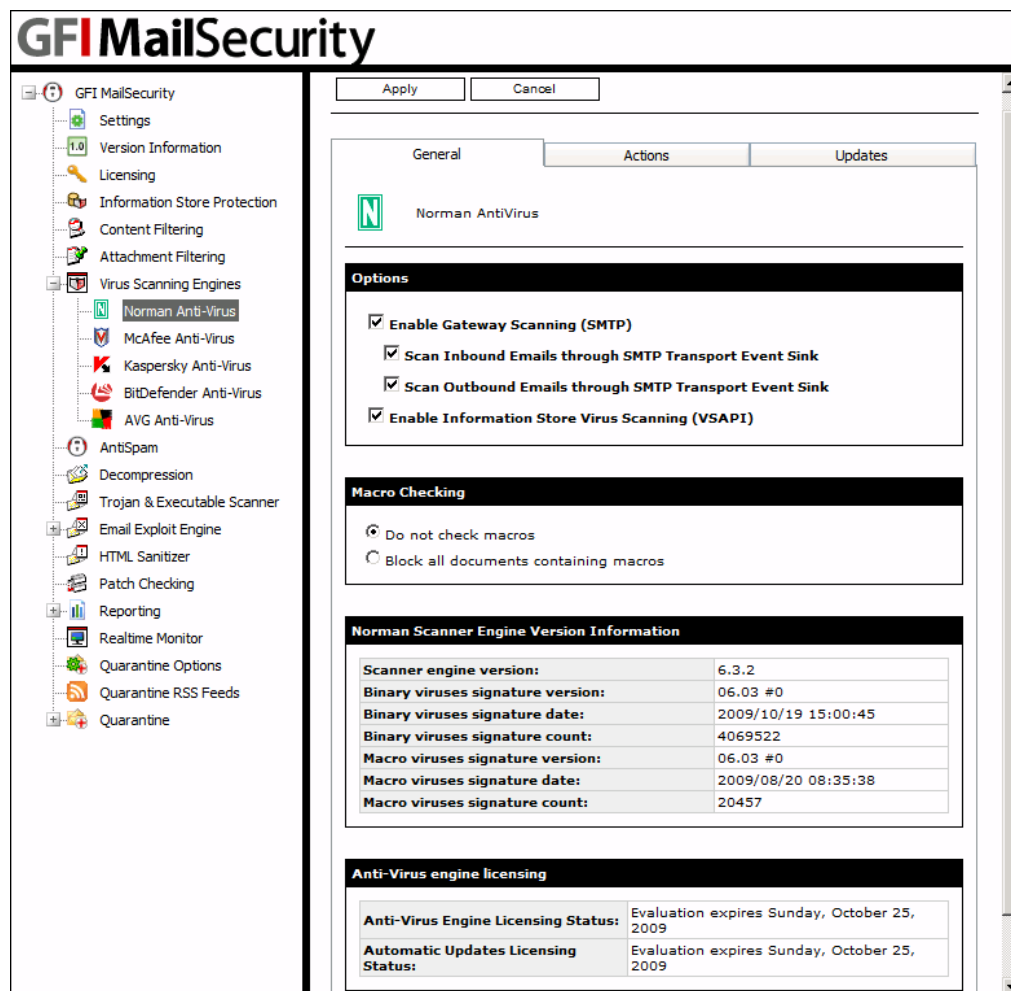
McAfee website

For more information about the virus patterns included in the McAfee engine, visit the McAfee website at <http://www.mcafee.com>

4.6 Norman configuration

The configuration options of the Norman Virus Scanning Engine are identical to those of the BitDefender engine. For more information on how to configure these options, refer to [BitDefender configuration](#) section earlier in the manual.

NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus Scanning Engine version, virus signature count and the date of the current virus signature files. License details for the current anti-virus engine are also displayed.

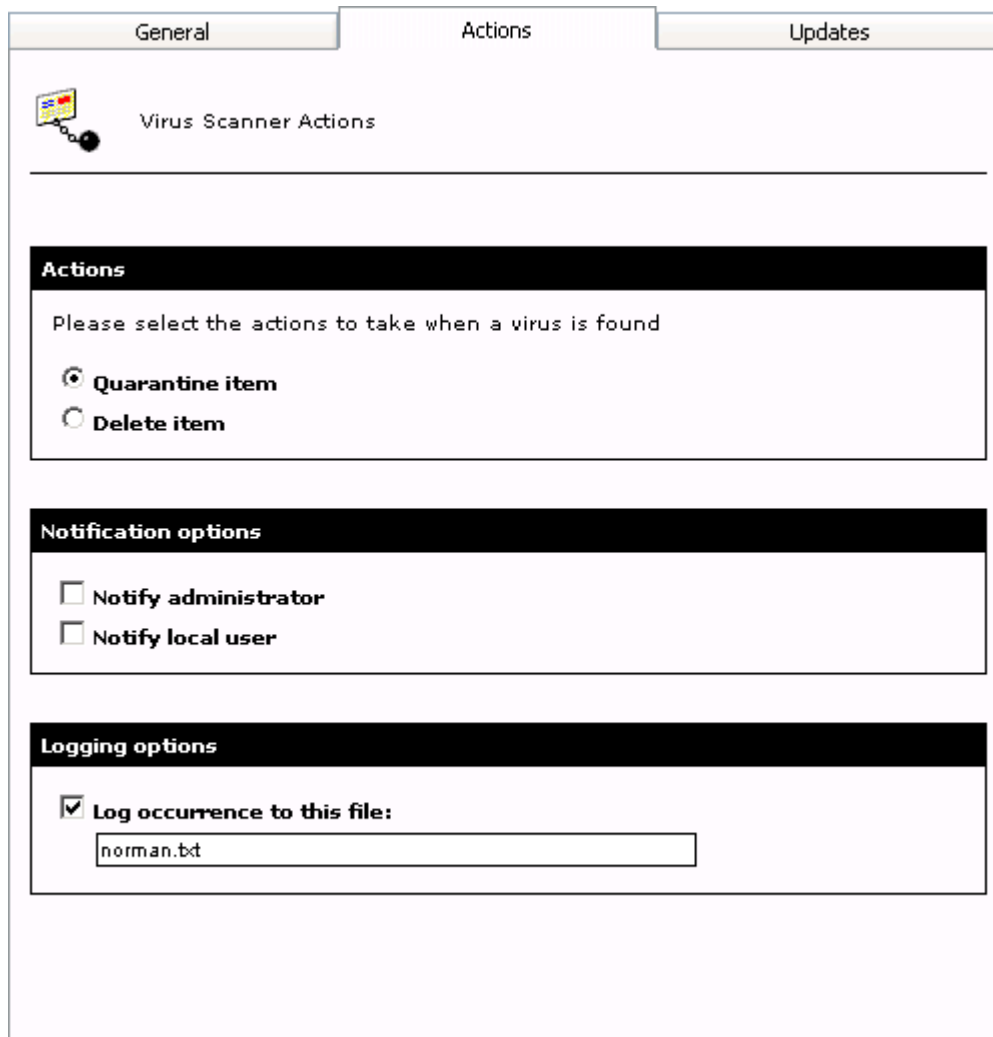


Screenshot 44 - Virus Scanning Engines: Norman configuration page

Norman website

For more information about the virus patterns included in the Norman Virus Control (NVC) engine, visit the NVC website at <http://www.norman.com>

4.7 Virus scanner actions



General Actions Updates

Virus Scanner Actions

Actions

Please select the actions to take when a virus is found

☒ Quarantine item

☐ Delete item

Notification options

☐ Notify administrator

☐ Notify local user

Logging options

☒ Log occurrence to this file:

norman.bt

Screenshot 45 - Virus Scanning Engine: Configuration page (Actions Tab)

In GFI MailSecurity, you can configure what each of the installed Virus Scanning Engines should do whenever an infected email is detected. To configure the actions of a virus scanner:

1. Select the virus scanner that you want to configure and click the **Actions** tab.
2. Choose one of the following options:
 - **Quarantine item** - Select this option if you want to quarantine all virus-infected emails detected by this Virus Scanning Engine. You can subsequently review (approve/delete) all the quarantined emails.
 - **Delete item** - Select this option to delete all virus-infected emails detected by this Virus Scanning Engine.

NOTE: This option overrides the settings configured in the **General** tab. i.e. If in the **General** tab, you selected **Block all emails containing a macro** (i.e. quarantine all emails even the ones having a genuine macro) but at the same

time you have enabled the **Delete item** option, ALL emails containing a macro will be deleted.

3. To send email notifications whenever an infected email is detected, enable any of the following options:

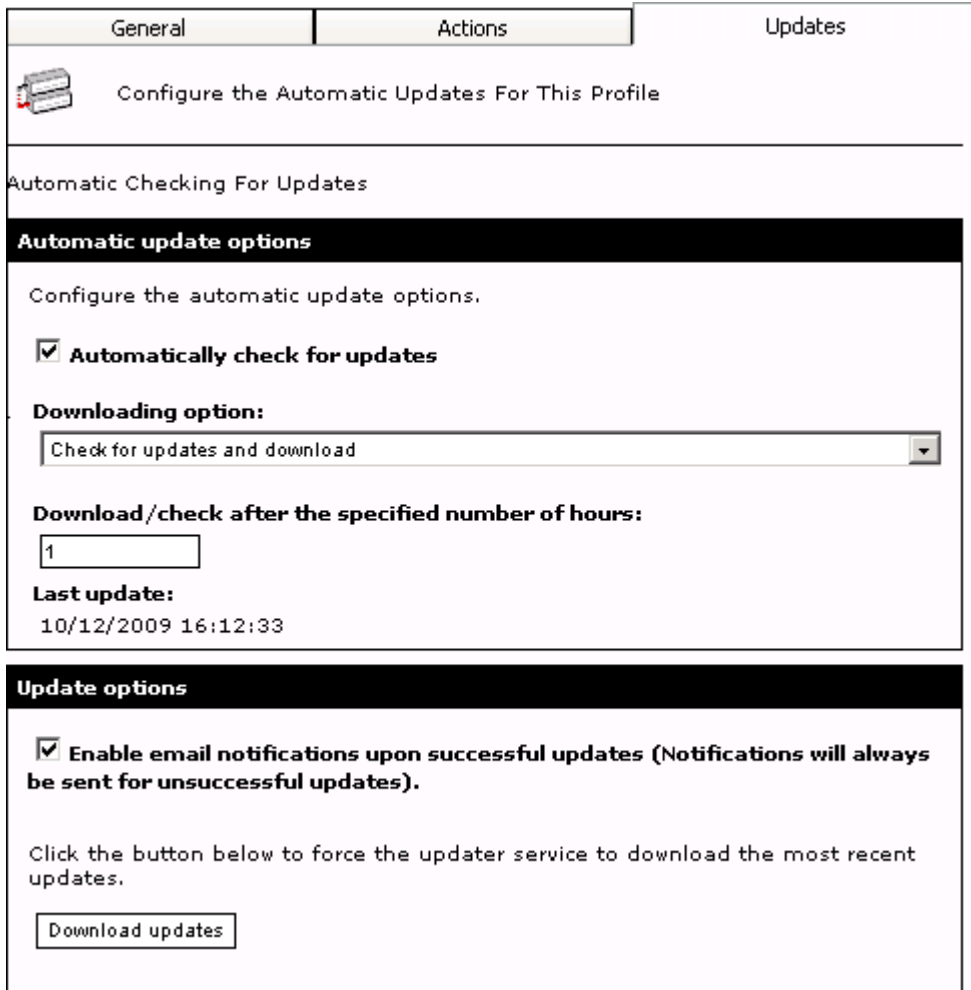
- **Notify local user** - Select this option if you want to notify the email local users when this filter detects a virus.

NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.

- **Notify administrator** - Select this option if you want to notify the administrator whenever this virus scanner detects an infected email.

4. Select the **Log occurrence to this file** check box and specify a log file name in the box below, if you want to log the virus scanning activity to a log file. You can specify either the file name only or else the full path to a custom location on disk.

4.8 Virus scanner updates



The screenshot shows the 'Updates' tab of the 'Virus Scanning Engines' configuration page. At the top, there are three tabs: 'General', 'Actions', and 'Updates'. Below the tabs is a header area with a server icon and the text 'Configure the Automatic Updates For This Profile'. The main content area is titled 'Automatic Checking For Updates'. It contains a section 'Automatic update options' with the instruction 'Configure the automatic update options.' and a checked checkbox for 'Automatically check for updates'. Below this is a 'Downloading option:' dropdown menu set to 'Check for updates and download'. Further down is a 'Download/check after the specified number of hours:' field with the value '1'. At the bottom of this section, it shows 'Last update: 10/12/2009 16:12:33'. The next section is 'Update options', which has a checked checkbox for 'Enable email notifications upon successful updates (Notifications will always be sent for unsuccessful updates)'. Below this is a text instruction 'Click the button below to force the updater service to download the most recent updates.' and a 'Download updates' button.

Screenshot 46 - Virus Scanning Engines: Configuration page (Updates Tab)

You can configure GFI MailSecurity to download virus scanner updates automatically or to notify the administrator whenever new updates are available. To configure the automatic updates of a particular virus scanner:

1. Select the virus scanner that you want to configure and from the right window, click the **Updates** tab.
2. Select the **Automatically check for updates** check box to enable the auto-update feature.
3. From the **Downloading options** list, select one of the following:
 - **Only check for updates** - Select this option if you want GFI MailSecurity to just check and notify the administrator whenever updates are available for this virus scanner. This option will NOT download the available updates.
 - **Check for updates and download** - Select this option if you want GFI MailSecurity to check and automatically download any updates available for this virus scanner.

4. Specify how often you want GFI MailSecurity to check/download updates for this Virus Scanning Engine, by specifying an interval value in hours.






Triggering the virus update manually

To check/download updates for the current Virus Scanning Engine immediately, click **Download updates**.

4.9 Setting the Virus Scanning Engines scan priority

To configure the execution order of the Virus Scanning Engines, follow these steps:

1. Click the **GFI MailSecurity ► Virus Scanning Engines** node.

Engine	Status	License	Priority		
 AVG Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	0	▲	▼
 BitDefender Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	1	▲	▼
 Norman Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	2	▲	▼
 McAfee Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	3	▲	▼
 Kaspersky Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	4	▲	▼

Screenshot 47 - Virus Scanning Engines: scan priority list

2. In the right pane, the Virus Scanning Engines are listed in descending order of priority.

NOTE: The priority assigned to each virus scanner determines the sequence when each anti-virus engine gets to scan the content. The scanner with priority 0 is the first to start scanning an email. Upon completion, the Virus Scanning Engine with priority 1 scans the email and so on. This means that the Virus Scanning Engine listed at the top of the list is the first to scan emails, if it is enabled.

3. To change the virus scanning execution priority, click the (up) ▲ or (down) ▼ arrows to respectively increase or decrease the priority of the virus scanner. Repeat the same procedure until the virus scanner reaches the desired position in the priority/execution sequence list.

4.10 Configuring Virus Scanning optimizations

From the **GFI MailSecurity ► Virus Scanning Engines** node you can instruct GFI MailSecurity to stop virus scanning an item if a number of virus scanning engines already detected a virus in that item.

To enable this option, select the **Stop virus scanning the current item, if viruses are detected by** check box, and specify the number of virus scanners that need to detect a virus to stop virus scanning, in the box. Click **Apply**.

Virus Scanning Optimizations

- ☒ Stop virus scanning the current item, if viruses are detected by:
 - virus scanners
- ☒ Stop scanning even for non-virus related threats.

Screenshot 48 - Configure virus scanning optimizations

For example, if you select this option and enter 2 in the box, virus scanning on an item that contains a virus is performed by at most two virus-scanning engines, if they detect it. Emails that do not contain a virus are scanned by all enabled virus-scanning engines anyway.

If you want to streamline further the path taken by items containing a virus, select the **Stop scanning even for non-virus related threats** check box and click **Apply**. This option will instruct GFI MailSecurity to stop further scanning of the current item, such as with Attachment Checking and so on, since the amount of virus-scanning engines you specified have detected a virus.

4.11 Configuring Information Store Scanning

NOTE: The **Information Store Protection** node is only available if you install GFI MailSecurity on the Microsoft Exchange machine.

NOTE: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007/2010 machine, **Information Store Protection** is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

This section will show you how to enable or disable Information Store Scanning, and select the scan method used by VSAPI (Virus Scanning API).

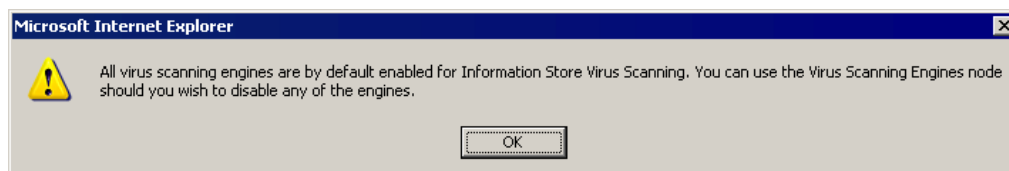
To configure the Information Store Scanning feature, follow these steps:

1. Click the **GFI MailSecurity ► Information Store Protection** node.
2. In the **Information Store Virus Scanning** tab, you can enable or disable Information Store Scanning by selecting/clearing the **Enable Information Store Virus Scanning** check box accordingly. The status of the Virus Scanning Engines used to scan the Information Store is also displayed.



Screenshot 49 - Information Store Protection node

NOTE: When you disable Information Store Virus Scanning, the Information Store Scanning option of all Virus Scanning Engines is disabled automatically. When you enable Information Store Virus Scanning, the Information Store Scanning option of all Virus Scanning Engines is enabled automatically. This setting does not affect the Gateway scanning option of each Virus Scanning Engine. The GFI MailSecurity configuration will prompt you about this action as shown in the screenshot below. If you need to enable or disable the Information Store Scanning option for a specific Virus Scanning Engine, please refer to the [Configuring Virus Scanning Engines](#) section earlier in this chapter.



Screenshot 50 - All Information Store Virus Scanning Engines have been enabled.

3. To configure what VSAPI scan method to use, click the **VSAPI Settings** tab.



Screenshot 51 - VSAPI scan settings

4. From the VSAPI Settings tab, you can enable background Information Store Scanning, by selecting the **Enable background scanning** check box. This option will cause all the contents of the Information Store to be scanned, which depending on the amount of items stored in the Information Store could result in a huge processing load on the Exchange server. For this reason, it is recommended that this option be only enabled during periods of low server activity such as during the night.

5. Select a VSAPI scan method from the following:

- **On-access scanning** - New items in the Information Store are scanned as soon as they are accessed by the email client. This scan method will thus introduce a short delay before the email client can display the contents of a new message.
- **Pro-active scanning** - New items added to the Information Store are added to a queue for scanning. When a mail client tries to access an item that is still in the queue, it will be allocated a higher scanning priority so that it is scanned as soon as possible. This is the default and recommended mode of operation, since in general the delay associated with on-access scanning is avoided because new items are added to the queue immediately and are usually scanned before a mail client requests access to the item.

6. To save and instruct GFI MailSecurity to make use of the new settings, click **Apply**.

5 Configuring Content Filtering

5.1 Introduction

The Content Filtering feature allows you to set up rules to filter emails containing particular keywords or a combination of keywords in an email. A rule is composed of:

- Keywords to block in the email body, subject or attachment
- Actions to take when a keyword is found
- The users to which a rule applies.

NOTE: Although this feature can be used as a filter against spam email, it is recommended to use dedicated software to block spam. For more information, refer to:

<http://kbase.gfi.com/showarticle.asp?id=KBID003342>

Content Filtering

Configure content filtering settings

This filter generates alerts as well as blocks, quarantines and moves to specific folders all inbound/outbound emails containing listed keywords.
NOTE: This is NOT an anti-spam feature. For more information [click here](#).

Remove Selected Enable Selected Disable Selected Add Rule...

<input type="checkbox"/>	Rule	Status	Priority		
<input type="checkbox"/>	CONTENT POLICY: Block Racial Content	Enabled	0	↑	↓
<input type="checkbox"/>	CONTENT POLICY: Block Sexual Content	Enabled	1	↑	↓
<input type="checkbox"/>	CONTENT POLICY: Block Profanities	Disabled	2	↑	↓

Screenshot 52 - Content Filtering page

To configure keyword-blocking rules, navigate to the **Content Filtering** node from the GFI MailSecurity Configuration. This page allows you to view, create, enable, disable or delete rules.

5.2 Creating a Content Filtering rule

1. Navigate to **GFI MailSecurity ► Content Filtering** node and click **Add Rule....**

General | Body | Subject | Actions | Users/Folders

Content Checking Options

Rule name

Please specify a friendly name for this rule:

Email checking

This rule can be applied to both inbound and outbound emails. Select below:

☒ Check inbound emails

☒ Check outbound emails

PGP Encryption

This rule can be set to block any PGP encrypted mail. Enable or disable this option below:

☐ Block PGP encrypted emails

Screenshot 53 - Content Filtering: General Tab

- Specify a name for the rule in the **Rule name** text box.
- Select which emails to scan.

Check inbound emails	Select this option to scan incoming emails
Check outbound emails	Select this option to scan outgoing emails

- To block emails encrypted using PGP technology, select **Block PGP encrypted emails**.

NOTE: PGP encryption is a public-key cryptosystem often used to encrypt emails.

- Select the **Body** tab to specify the keywords in the email body to block.
- Select **Block emails if content is found matching these conditions** checkbox to enable scanning of body for keywords.

Condition entry

Edit condition:

AND

OR

AND NOT

OR NOT

Add Condition

Update

Conditions list

All these conditions are validated as a single condition using the OR operator for each entry. Clicking on an entry will copy the condition text in the condition entry above for editing.

Current conditions:

Remove

Screenshot 54 - Content Filtering: Body Tab- setting conditions

7. From the **Condition entry** area, key in keywords to block in the **Edit condition** box. You can also use conditions **AND**, **OR**, **AND NOT** and **OR NOT** to use a combinations of keywords.

8. To add the keyword or combination of keywords keyed in, click **Add Condition**.

NOTE 1: To modify an entry in the **Conditions list**, select it and make the required changes in the **Condition entry** box. Click **Update** to apply changes.

NOTE 2: To remove an entry from the **Conditions list**, select it and click **Remove**.

Conditions list

All these conditions are validated as a single condition using the OR operator for each entry. Clicking on an entry will copy the condition text in the condition entry above for editing.

Current conditions:

Remove

Options

☐ Match whole words only
 ☐ Apply above conditions to attachments

Attachment filtering

☒ Check all attachments having file extensions in this list
 ☐ Check all except attachments having file extensions in this list

File extension entry:
(eg. txt)
(eg. jpg)

Add

File extensions:

Remove

Screenshot 55 - Content Filtering: Body Tab- configuring other options

9. From the **Options** area, configure other settings:

Match whole words only	Block emails when the keywords specified match whole words.
Apply above conditions to attachments	Select this option to apply this rule also to text in attachments. In the Attachment filtering area specify the attachments to apply or exclude from this rule.

10. Select the **Subject** tab to specify keywords to block in the email subject.

General Body **Subject** Actions Users/Folders

Content Checking Actions

☒ **Enable subject content checking**

Block emails with the following phrases in the 'Subject' field

Enter phrase:

Phrases:

Options
☐ **Match whole words only**

Screenshot 56 - Content Filtering: Subject Tab

11. Select **Enable subject content checking** to enable scanning for keywords in the email subject.

12. In the **Enter phrase** text box, specify keywords to block, and click **Add**.

NOTE: To remove an added keyword, select it from the **Phrases** box and click **Remove Selected**.

13. From the **Options** area, configure how keywords are matched. Select **Match whole words only** to block emails where the keywords specified match whole words in the subject.

14. Click the **Actions** tab to configure what should be done when this rule is triggered.

15. To block an email that matches the rule conditions, select **Block attachment and perform this action** and select one of the following options:

Quarantine email	Stores emails containing the keyword(s) in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information about Quarantine refer to the Quarantine chapter in this manual.
Delete email	Deletes emails containing the blocked keyword(s).
Move to folder	Moves the email to a folder on disk. Key in the full folder path where to store blocked emails.

16. You can configure rule to send email notifications to the administrator and/or user whenever an email containing an attachment is blocked. To do this, from the **Notification options** area select:

Notify administrator	Notify the administrator whenever the rule is triggered.
-----------------------------	--

Notify local user Notify the email local recipients about the blocked email.

17. To log the activity of this rule to a log file, select **Log rule occurrence to this file**. In the text box specify:

- Path and file name to a custom location on disk where to store the log file, or
- The file name only. The log file will be stored in the following default location:
`<GFI MailSecurity installation path>\ContentSecurity\MailSecurity\DebugLogs\<filename.txt>`

18. By default, the rule is applied to all email users. GFI MailSecurity, however, allows you to apply this rule to a custom list of email users. To specify the users to apply this rule to, select **Users/Folders** tab

Screenshot 57 - Content Filtering: Users/Folders Tab

19. Specify the users to apply this rule to.

Only this list	Apply this rule to a custom list of email users, groups or public folders.
All except this list	Apply this rule to all email users except for the users, groups or public folders specified in the list.

20. To add email users, user groups and/or public folders to the list, click **Add**.

21. In the **User Lookups** window, specify the name of the email user/user group or public folder that you wish to add to the list and click **Check Names**. Matching users, groups or public folders are listed below.

NOTE: You do not need to input the full name of the users, groups or public folder. It is enough to enter part of the name. GFI MailSecurity will list all the names that contain the specified characters. For example, if you input 'sco', GFI MailSecurity will return names like 'Scott Adams' and 'Freeman Prescott', if they are available.

22. Select the check box next to the name(s) that you want to add to the list and click **OK**.

NOTE 1: To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

NOTE 2: If no names are included in the list, GFI MailSecurity automatically applies this rule to all email users.

24. Repeat steps 21 to 23 to add all the required users to the list.

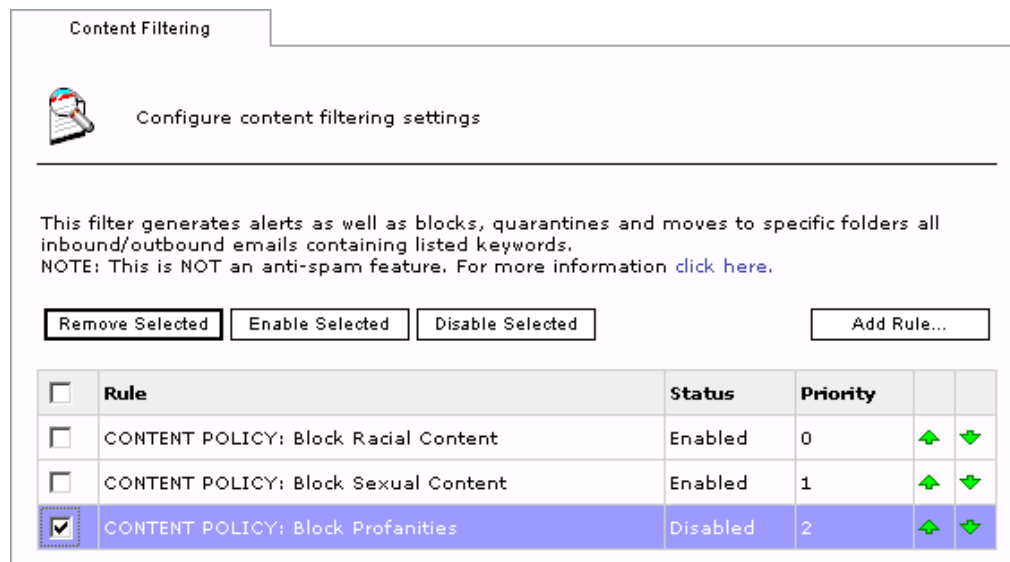
25. Click **Apply**.

5.3 Enabling/disabling rules

Enabled rules are rules that are active and GFI MailSecurity uses them during scanning. Disabled rules are rules that are inactive and are not currently used by GFI MailSecurity during email scanning.

1. Navigate to the **GFI MailSecurity ► Content Filtering** node.
2. From the Content Filtering page, select the checkbox of the rule(s) to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly.

5.4 Removing content filtering rules



Screenshot 58 - Selecting a Content Filtering rule for removal



1. Navigate to the **GFI MailSecurity ► Content Filtering** node.
2. From the Content Filtering page, select the checkbox of the rule(s) that you want to remove.
3. Click **Remove Selected**.

5.5 Modifying an existing rule

1. Click the **GFI MailSecurity ► Content Filtering** node.
2. From the Content Filtering page, click the name of the rule to modify.
3. Perform the required changes in the rule properties and click **Apply** to apply changes.

5.6 Changing the rule priority

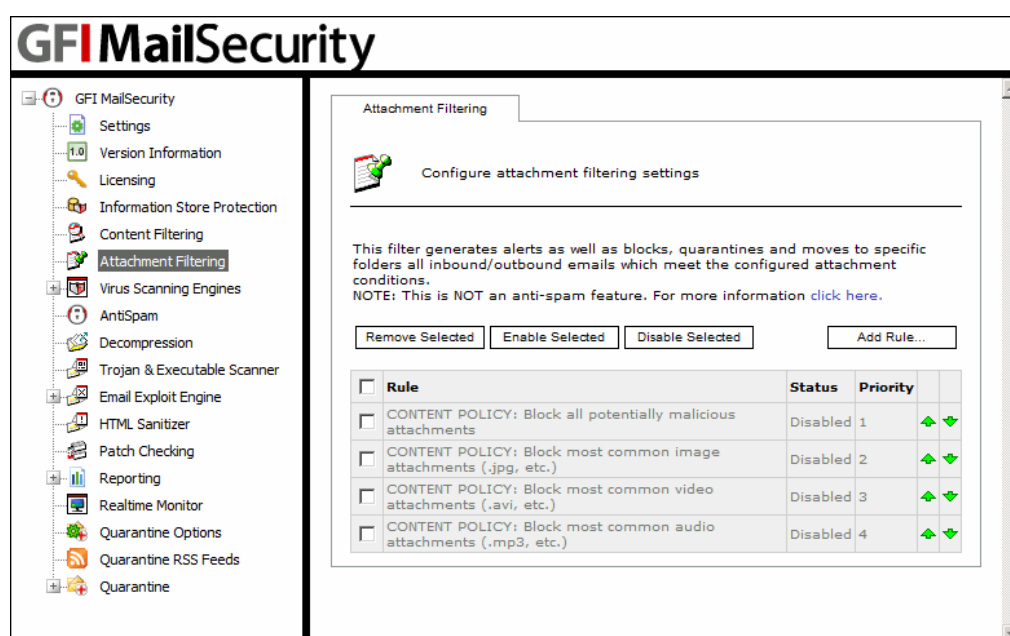
Content Filtering rules are applied in the same order, from top to bottom as they are listed in the Content Filtering page (that is, rule with priority value 1 is checked first). To change the sequence/priority of rules:

1. Navigate to **GFI MailSecurity ► Content Filtering**.
2. From the Content Filtering page, click the (up)  or (down)  arrows to respectively increase or decrease the priority of the rule.
3. Repeat step 2 until rules are placed in the desired sequence.

6 Configuring Attachment Filtering

6.1 Introduction to Attachment Filtering

This chapter explains how to set up Attachment Filtering in GFI MailSecurity. The Attachment Filtering feature allows you to set up a policy regarding what types of email attachments you will allow on your mail server. To set up such a policy, GFI MailSecurity uses the concept of 'Rules'. A rule is a condition that you set, such as, "block all executable attachments". This means that an Attachment Filtering rule allows you to block attachments of a certain type.



Screenshot 59 - Attachment Filtering page


In GFI MailSecurity, you can configure attachment rules from the **Attachment Filtering** node. This page contains the options that enable you to create, delete, enable or disable rules. In addition, it lists all the existing attachment rules, including their status and the order in which these rules are applied to emails (i.e. priority).

6.2 Creating an Attachment Filtering rule

To create an Attachment Filtering rule:

1. Click the **GFI MailSecurity ► Attachment Filtering** node.
2. From the Attachment Filtering page (in the right window), click **Add Rule**.

General
Actions
Users/Folders

 Attachment Checking

Rule display name

Rule name:

Email checking

☒ Check inbound emails
☒ Check outbound emails

Attachment blocking

☐ Block all
☒ Block this list
☐ Block all except this list

Enter filenames with optional wildcards:
 (eg, *.vbs)
 (eg, *letter.vbs)
 (eg, happy*.exe)
 (eg, orders.mdb)

Options

☐ Block all files greater than the following size in Kb:

Screenshot 60 - Attachment Filtering: General Tab

3. Specify the name of the rule and select whether to apply this rule to inbound and/or outbound emails by selecting the respective check boxes.
4. Decide on the type of attachment blocking required:
 - **Block all** - Select this option to block email attachments of any type.
 - **Block this list** - Select this option to block ONLY the listed attachment types.

- **Block all except this list** - Select this option to block attachment types that are not included in the list.

NOTE: To add an attachment type to the list, input the required full file name or file extension in the box next to the **Add** button. When ready, click **Add**. You can use asterisk (*) wildcards to replace characters or strings in the attachment type/extension. For example, specifying *orders*.mdb blocks all mdb files which contain the string 'orders' in the file name. Specifying *.jpg will block all jpg files.

NOTE: To remove an entry from the list, select it and click **Remove Selected**.

5. Additionally, you can specify a file size in kilobytes as a threshold. This has the effect of blocking all attachments with a file size bigger than the one you specify irrespective of whether it matches an entry in the list. To enable this option, select the **Block all files greater than the following size in Kb** check box and specify the maximum file size (in KB) allowed without blocking.

General Actions Users/Folders

Attachment Checking Actions

Actions

☒ Block attachment and perform this action:

☒ Quarantine email

☐ Delete email

☐ Move to folder:

Notification options

☒ Notify administrator

☒ Notify local user

Logging options

☒ Log rule occurrence to this file:

attachment.txt

Screenshot 61 - Attachment Filtering: Actions Tab

6. After you have specified what the attachment rule should check for, you must specify what this rule should do whenever it finds the specified

attachment(s). Click the **Actions** tab to open the rule actions configuration page.

7. Select the **Block attachment and perform this action** check box if you want to quarantine, delete or move the blocked emails to a particular folder. Additionally, select one of the following options:

- **Quarantine email:** Select this option to quarantine the email containing the attachment for review by an administrator. For more information, refer to [Quarantine](#) chapter in this manual.
- **Delete email:** Select this option to delete the email and attachment completely.
- **Move to folder:** This option will move the email to the specified folder. Input the folder name in the box provided underneath this option.

NOTE: Please note that you cannot configure actions to affect a single attachment within an email. Actions will always affect the whole email containing the attachment.

8. You can configure an attachment rule to send email notifications to the administrator and/or user whenever an email containing an attachment is blocked. You can configure the required notifications by selecting any of the following options:

- **Notify local user:** Select this option if you want to notify the email local users when this filter blocks an attachment.

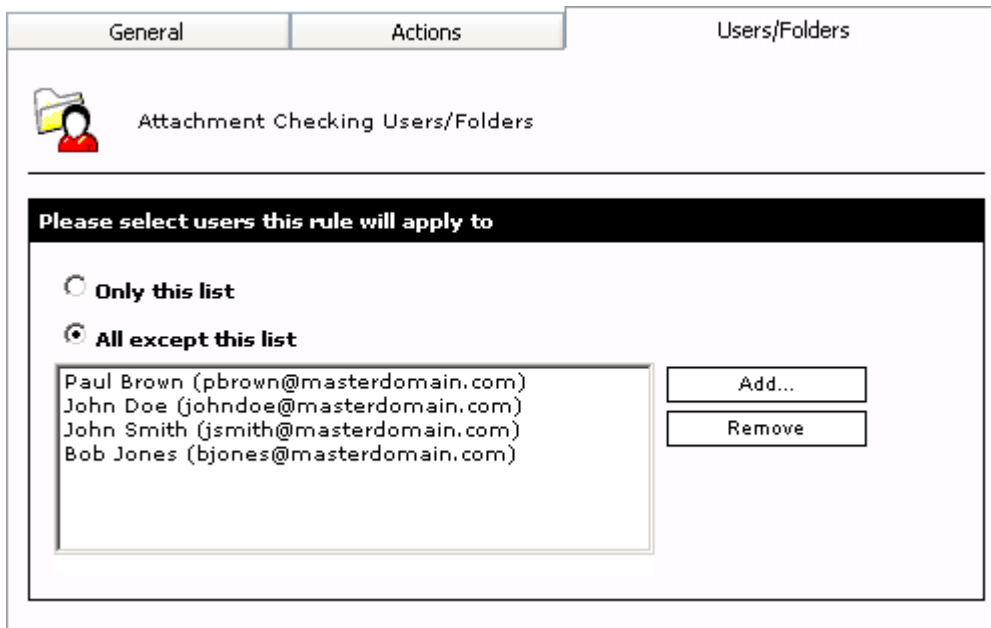
NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.

- **Notify administrator:** Select this option if you want to send email notifications to the administrator whenever an email containing an attachment is blocked. The administrator's email address is specified during the installation of GFI MailSecurity but can still be changed from the GFI MailSecurity configuration (**GFI MailSecurity ► Settings node ► General** tab). For more information refer to [Define the administrator's email address](#) section in this manual.

9. Select the **Log rule occurrence to this file** check box and specify a log file name in the box below, if you want to log all rule activity to a log file. You can specify either the file name only or else the full path to a custom location on disk.

NOTE: You can configure an attachment rule using any combination of actions. For example, you can opt not to block emails containing the attachment, but to simply notify the user or log the occurrence to file.

10. Now, you must specify the users to whom this rule applies. By default, GFI MailSecurity will apply the rule to all email users. However, if you want this rule to affect a selection of users only, click the **Users/Folders** tab.

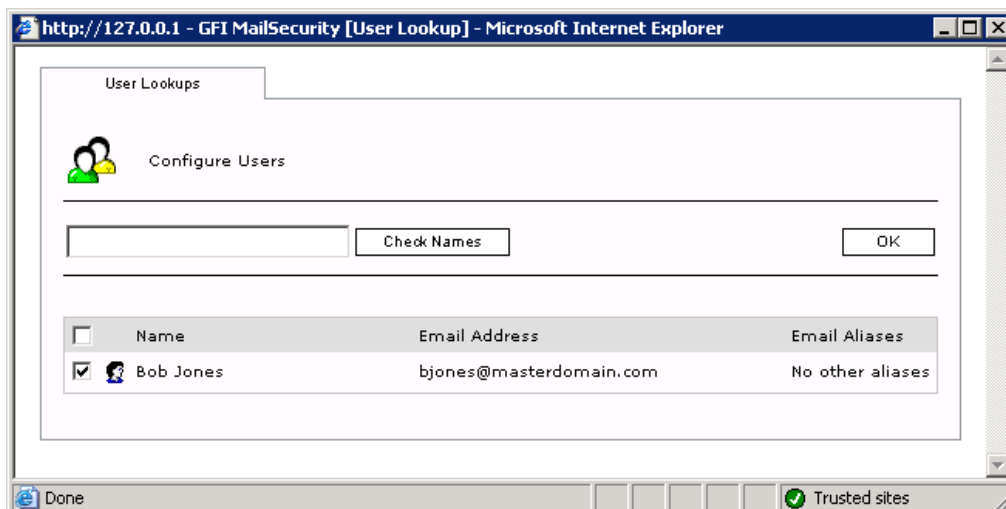


Screenshot 62 - Attachment Filtering: Users/Folders Tab

11. Choose one of the following options:

- **Only this list** - Select this option if you want to apply this rule to all email users/groups or public folders present in the list.
- **All except this list** - Select this option if you want to apply this rule to all email users, groups or public folders NOT present in the list.

12. To add email users, user groups and/or public folders to the list, click **Add**.



Screenshot 63 - Add users to an attachment Filtering rule

13. In the add users window, specify the name of the email user/user group or public folder that you wish to add to the list.

14. Click **Check Names** to query the Active Directory or the imported list of SMTP addresses (depending on how you installed GFI MailSecurity), to

check if the specified entry exists. Any user, group or public folder that matches will be listed below.

NOTE: You do not need to input the full name of the user/user group or public folder. It is enough to enter at least three characters. GFI MailSecurity will list all the names that contain the specified characters. For example, if you input 'ott', GFI MailSecurity will return names like 'Scott Adams' and 'Freeman Prescott', if they are available.

15. Select the check box at the start of the listed name(s) to indicate the ones that you wish to add to the list and click **OK**.

NOTE: You can select all the listed names at once by selecting the check box next to the **Name** column heading at the top-left of the list.

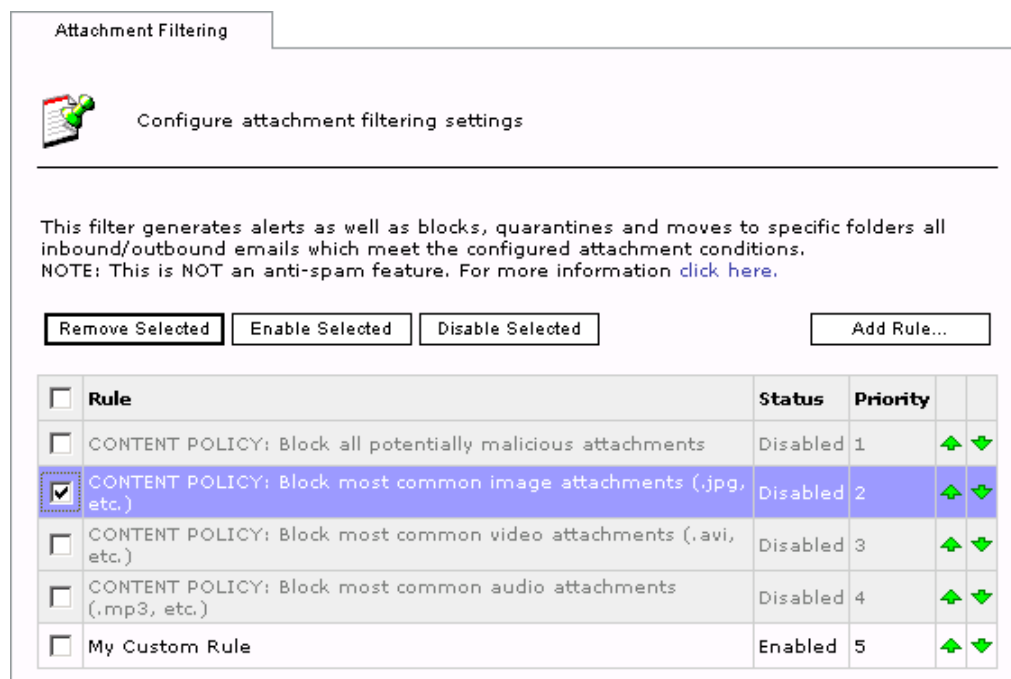
NOTE: Repeat steps 12 to 15 to add all the users you want to the list.

NOTE: To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

NOTE: If no names are included in the list, GFI MailSecurity will automatically apply this rule to all the email users in Active Directory/SMTP address list.

16. Click **Apply**.

6.3 Removing attachment rules



Screenshot 64 - Selecting an attachment Filtering rule for removal

To Remove an Attachment Filtering rule:

1. Click the **GFI MailSecurity ► Attachment Filtering** node.
2. From the Attachment Filtering page (in the right window), select the check box of the rule(s) that you want to remove.

NOTE: You can select all check boxes in one go by selecting the check box next to the **Rule** column heading at the top-left of the list.

3. Click **Remove Selected** to delete the selected rules.

6.4 Make changes to an existing rule

To modify an existing rule:

1. Click the **GFI MailSecurity ► Attachment Filtering** node.
2. From the Attachment Filtering page (in the right window), click the name of the rule that you want to modify.
3. Make the required changes (for example, Rename the rule, etc.) in the rule properties and click **Apply** to accept the changes you made. Changes will take effect immediately.

6.5 Enabling/disabling rules

You can check and change the status of a rule (i.e. enabled/disabled) from the Attachment Filtering page. To enable or disable an existing rule:

1. Click the **GFI MailSecurity ► Attachment Filtering** node.
2. From the Attachment Filtering page (in the right window), select the check box of the rule(s) that you want to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly. The status change is displayed immediately under the **Status** column.

6.6 Changing the rule priority

Attachment Filtering rules are applied in the same order, from top to bottom, as they are listed in the Attachment Filtering page. However, you can change the sequence/priority of a rule as follows:

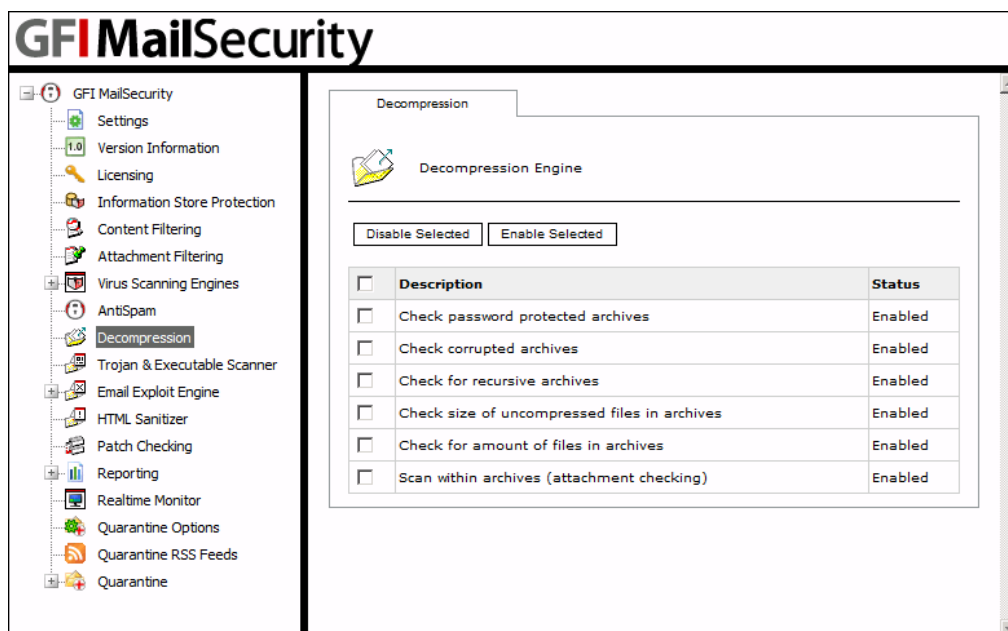
1. Click the **GFI MailSecurity ► Attachment Filtering** node.
2. From the Attachment Filtering page (in the right window), click the (up) ▲ or (down) ▼ arrows to respectively increase or decrease the priority of the required rule(s). Repeat until the rule reaches the desired position in the list (i.e. until the rule is assigned the desired priority).

NOTE: You can check the priority of rules from the Attachment Filtering page. The priority value of each rule is displayed in the **Priority** column.

7 Decompression engine

7.1 Introduction to the Decompression engine

The Decompression engine decompresses and analyzes archives attached to an email.



Screenshot 65 - The decompression engine filters list

The following is a list of archive filters included in the decompression engine:

- Check password protected archives
- Check corrupted archives
- Check for recursive archives
- Check size of uncompressed files in archives
- Check for amount of files in archives
- Scan within archives

You can configure each of the above listed filters separately. This means that you can specify what each decompression filter should do with emails containing particular archives.

7.2 Configuring the decompression engine filters

Check password protected archives



General Actions

Decompression engine

☐ Check password protected archives

Actions

Please select the action to take when this rule is violated.

☒ Quarantine

☐ Automatically Delete

Screenshot 66 - Configuring password protected archives options

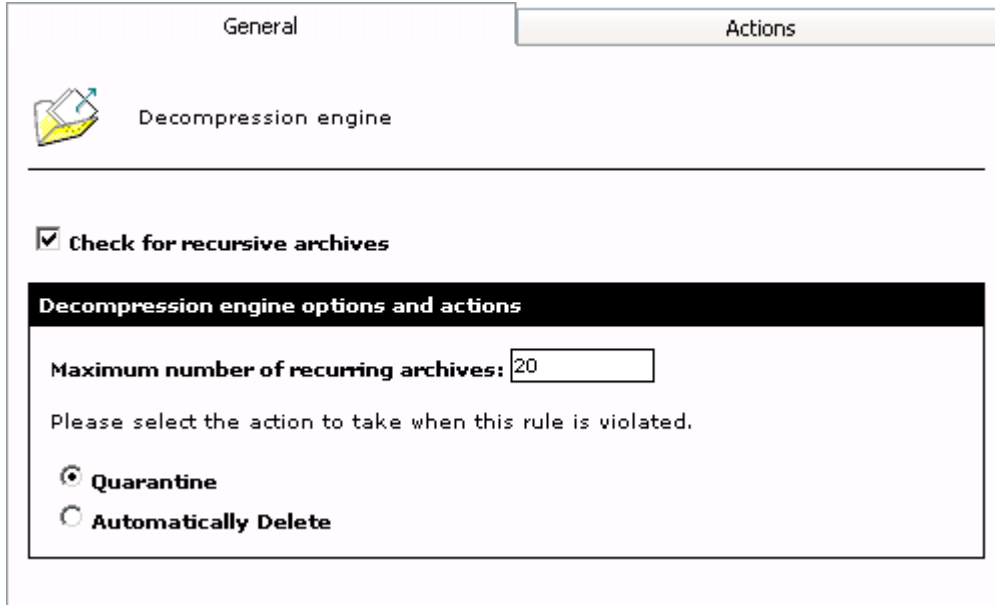
This filter allows you to quarantine or delete emails that contain password-protected archives. To configure this filter:

1. Click the **GFI MailSecurity ► Decompression** node.
2. From the list of available filters (in the right window), click on **Check password protected archives**.
3. Select the **Check password protected archives** check box to enable this filter.
4. Specify what to do with emails containing password-protected archives by selecting one of the following options:
 - **Quarantine** - Select this option to quarantine the emails that contain a password-protected archive. The administrator can later review these quarantined emails and approve or delete them accordingly.
 - **Automatically Delete** - Select this option to delete emails containing password-protected archives.
5. Click the **Actions** tab to configure any actions to be performed whenever an email containing a password-protected archive is detected and blocked. For more information on how to configure actions refer to [Configuring decompression filter actions](#) section in this chapter.
6. Click **Apply**.


Check corrupted archives

This filter allows you to quarantine or delete emails that contain corrupted archives. The configuration options of this filter are identical to those of the [Check password protected archives](#).

Check for recursive archives



General Actions

 Decompression engine

☒ **Check for recursive archives**

Decompression engine options and actions

Maximum number of recurring archives:

Please select the action to take when this rule is violated.

☒ **Quarantine**

☐ **Automatically Delete**

Screenshot 67 - Configuring recursive archives options

This filter allows you to quarantine or delete emails that contain recursive archives. Recursive archives, also known as nested archives, are archives that contain other/multiple levels of sub-archives (i.e. archives within archives). A high number of archive levels can indicate a malicious archive: Recursive archives can be used in a DoS (Denial of Service) attack, since most content scanning and anti-virus packages crash while attempting to scan nested archive levels.

To configure this filter:

1. Click the **GFI MailSecurity ► Decompression** node.
2. From the list of available filters (in the right window), click on **Check for recursive archives**.
3. Select the **Check for recursive archives** check box to enable this filter and specify the maximum number of nested archives permitted.

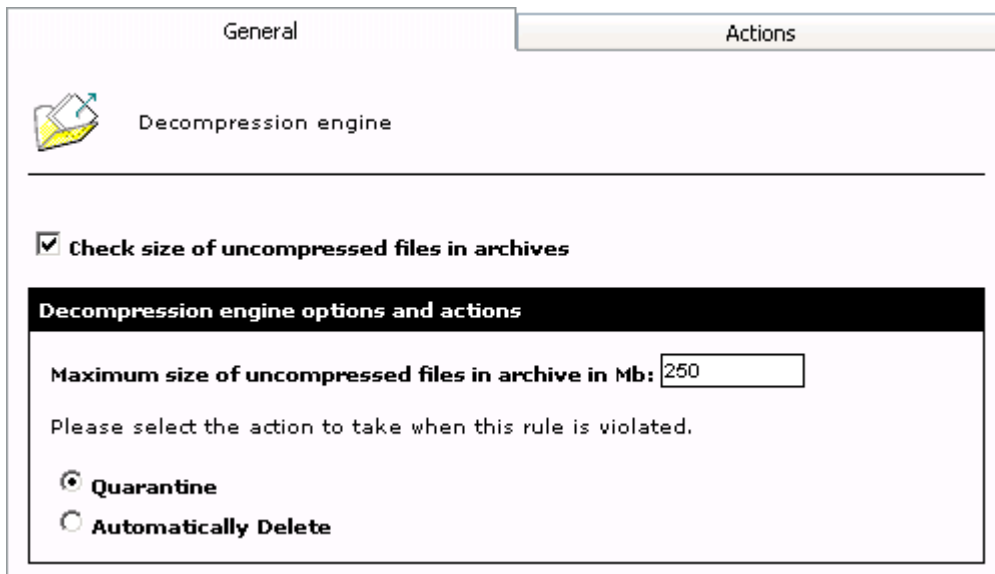
IMPORTANT: If you disable the **Check for recursive archives** rule, GFI MailSecurity will not scan or quarantine recursive archives, thus bypassing the anti-virus checking.

4. Decide on what to do with emails containing nested archives that exceed the specified limit by selecting one of the following options:
 - **Quarantine** - Select this option to quarantine the emails that contain recursive archives. The administrator can later review these quarantined emails and approve or delete them accordingly.
 - **Automatically Delete** - Select this option to delete emails containing recursive archives that exceed the specified nesting limit.
5. Click the **Actions** tab to configure any actions to be performed whenever an email containing a recursive archive is detected and blocked. For more

information on how to configure actions refer to the [Configuring the decompression engine filters](#) section in this chapter.

6. Click **Apply**.

Check size of uncompressed files in archives



General Actions

Decompression engine

☒ **Check size of uncompressed files in archives**

Decompression engine options and actions

Maximum size of uncompressed files in archive in Mb:

Please select the action to take when this rule is violated.

☒ **Quarantine**

☐ **Automatically Delete**

Screenshot 68 - Configuring checks for the size of uncompressed files in archives

This filter allows you to block or delete emails with archives that exceed the specified physical size when uncompressed. Hackers sometimes use this method in a DoS (Denial of Service) attack: By sending an archive that can be uncompressed to a very large file, they can often crash content security or anti-virus software.

To configure this filter:

1. Click the **GFI MailSecurity ► Decompression** node.
2. From the list of available filters (in the right window), click on **Check size of uncompressed files in archives**.
3. Select the **Check size of uncompressed files in archives** check box to enable this feature and specify the maximum size (in MB) allowed for uncompressed files, received within an archive.

IMPORTANT: If you disable the **Check size of uncompressed files in archives** rule, GFI MailSecurity will not scan or quarantine archive attachments, thus bypassing the anti-virus checking.

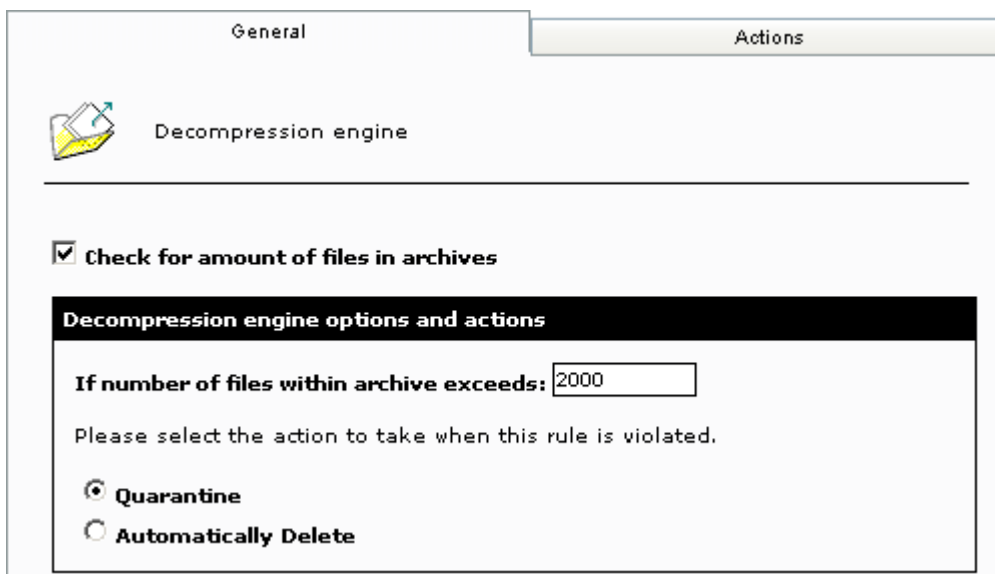
4. Decide on what to do with emails containing archived files that exceed the specified size when un-compressed.

- **Quarantine** - Select this option to quarantine the emails that contain these archives. The administrator can later review these quarantined emails and approve or delete them accordingly.
- **Automatically Delete** - Select this option to delete emails containing archived files that when un-compressed, exceed the specified size limit.

5. Click the **Actions** tab to configure any actions to be performed whenever this filter detects and blocks emails containing an archive. For more information on how to configure actions refer to [Configuring the decompression engine filters](#) section in this chapter.

6. Click **Apply**.

Check for amount of files in archives



General Actions

Decompression engine

☒ Check for amount of files in archives

Decompression engine options and actions

If number of files within archive exceeds:

Please select the action to take when this rule is violated.

☒ Quarantine

☐ Automatically Delete

Screenshot 69 - Configuring the amount of files in archive check

This filter allows you to quarantine or delete emails that contain an excessive amount of compressed files within an attached archive. You can specify the number of files allowed in archive attachments from the configuration options included in this filter.

To configure this filter:

1. Click the **GFI MailSecurity ► Decompression** node.
2. From the list of filters (in the right window), click on **Check for amount of files in archives**.
3. Select the **Check for amount of files in archives** check box to enable this filter and specify the maximum amount of files allowed in an archive.

IMPORTANT: If you disable the **Check for amount of files in archives** rule, GFI MailSecurity will not scan or quarantine archive attachments, thus bypassing the anti-virus checking.

4. Decide on what to do with emails containing archives that exceed the specified limit of contained files by selecting one of the following options:
 - **Quarantine** - Select this option to quarantine the emails that contain these archives. The administrator can later review these quarantined emails and approve or delete them accordingly.

- **Automatically Delete** - Select this option to delete emails containing archived files that when uncompressed contain more files than the limit specified.

5. Click the **Actions** tab to configure any actions to be performed whenever this filter detects and blocks emails containing an archive. For more information on how to configure actions, refer to [Configuring the decompression engine filters](#) section in this chapter.

6. Click **Apply**.

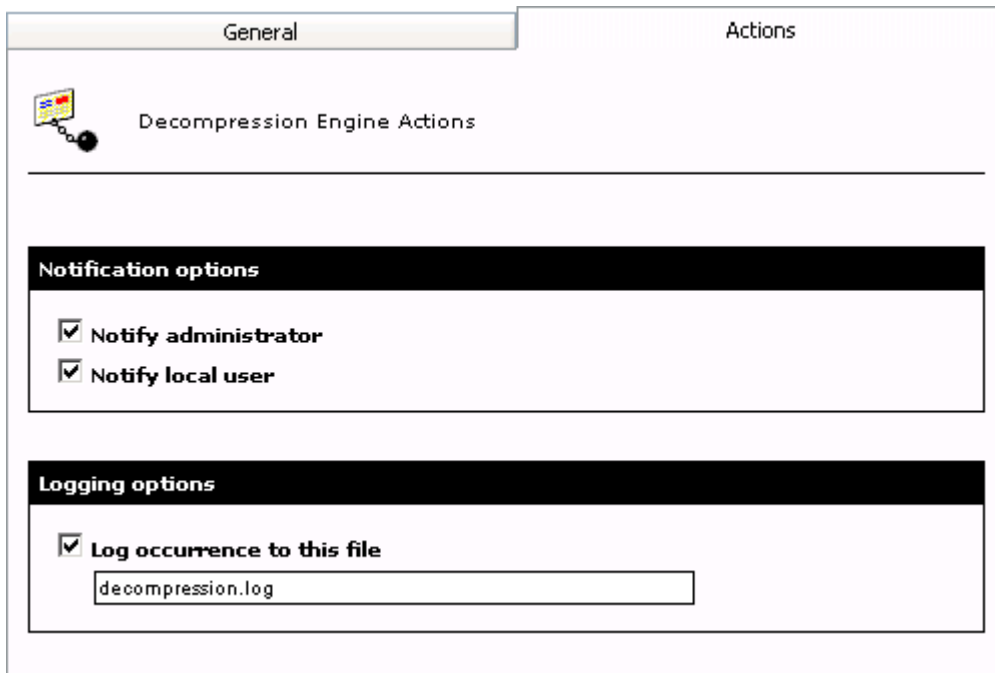
Scan within archives

Through the **Scan within archives** option, you can disable Attachment Filtering and Content Filtering of files in archives.

Configure this option as follows:

1. Click the **GFI MailSecurity ► Decompression** node.
2. From the list of filters (in the right window), click on **Scan within archives**.
3. Select the **Scan within archives** check box to scan any archive attachments present in an email using the decompression and attachment scanning rules.

7.3 Configuring decompression filter actions



Screenshot 70 - Decompression filter actions

To configure the actions to be performed whenever a particular filter blocks emails containing archives:

1. Click the **GFI MailSecurity ► Decompression** node and from the right window select the required filter.

2. Click the **Actions** tab and select any of the following actions:

- **Notify local user** - Select this option if you want to notify the email local users when the email contains an archive file that infringes a decompression engine rule.

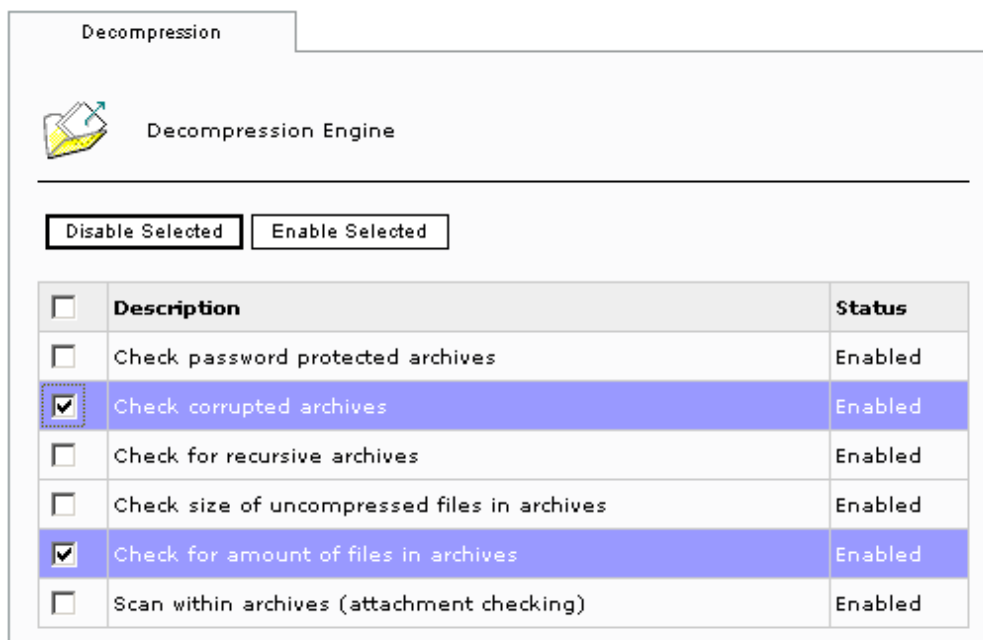
NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.

- **Notify administrator** - Select this option to send email notifications to the administrator whenever an email containing an archive is quarantined.

Log occurrence to this file - Select this option to log the event whenever the selected decompression filter blocks an email. In the box below, specify either a file name only or the full path to the log file.

3. Click **Apply**.

7.4 Enable/disable decompression filters



Screenshot 71 - Decompression tool filters list

To enable or disable any of the available decompression filters:

1. Click the **GFI MailSecurity ► Decompression** node.
2. In the right window, select the check box of the filter(s) that you want to enable or disable.
3. Click **Enable selected** or **Disable selected** accordingly.

NOTE: You can select all check boxes in one go by selecting the check box next to the **Description** column heading at the top-left of the list.

8 The Trojan & Executable Scanner

8.1 Introduction to the Trojan & Executable Scanner

GFI MailSecurity includes an advanced Trojan and Executable Scanner, which is able to analyze and determine the function of an executable file. This scanner can subsequently quarantine any executables that perform suspicious activities (such as a Trojan).

What is a Trojan horse?

The Trojan horse got its name from the old mythical story about how the Greeks gave their enemy a huge wooden horse as a gift during the war. The enemy accepted this gift and brought it into their fortress. During the night, Greek soldiers crept out of the horse and attacked the city.

In computers a Trojan horse is a way of penetrating a victim's computer undetected, allowing the attacker unrestricted access to the data stored on that computer. Subsequently the attacker can manipulate the data and can cause great damage to the victim, just like the citizens of Troy.

A Trojan can be a hidden program that runs on your computer without your knowledge. Furthermore, hackers sometimes hide Trojans into legitimate programs that you normally use.

Difference between Trojans and viruses

The difference between Trojans and viruses is that Trojans are often 'one-off' ('tailor made') executables, targeted to obtain information from a specific target (user/system). In general, a hacker deploys a Trojan to create a backdoor on a system, thus gaining unrestricted access to the system. Signature based anti-virus software, are unable to detect one-off Trojans. Indeed any application that only uses signatures to detect malicious software will not be effective in detecting such threats. These include specialized anti-Trojan software. The main reason is that signature based software can only detect known viruses and Trojans. That is why such applications need frequent updates.

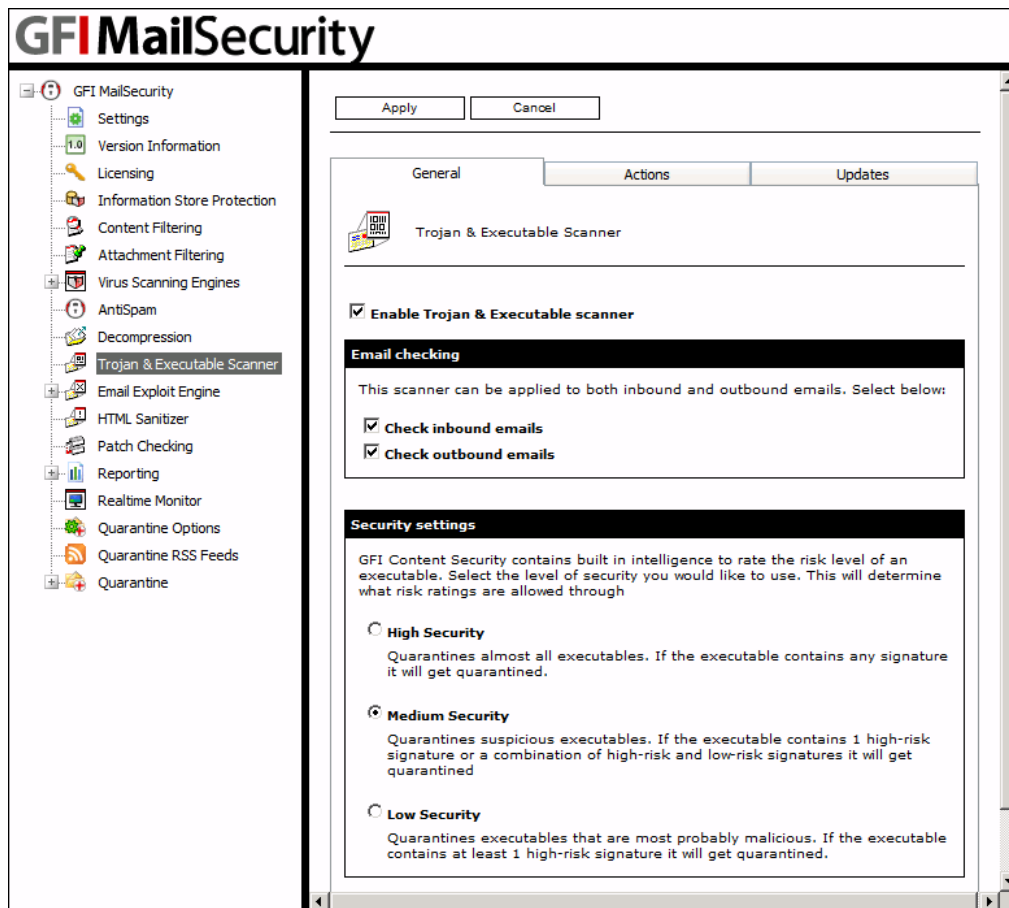
How does the Trojan & Executable Scanner work?

GFI MailSecurity is able to rate the risk-level of an executable file by decompiling the executable, and detecting in real time what the executable might do. Subsequently, it compares capabilities of the executable to a database of malicious actions and then rates the risk level of this executable file. With the Trojan & Executable scanner, you can detect and block potentially dangerous, unknown or one-off Trojans before they penetrate your network.

8.2 Configuring the Trojan & Executable Scanner

From the **Trojan & Executable Scanner** node, you can define the level of security that you require and the actions you want GFI MailSecurity to take on emails containing malicious executable files.

Configuring the security level



Screenshot 72 - Trojan and Executable Scanner: General Tab

To configure the Trojan & Executable Scanner:

1. Click the **GFI MailSecurity ► Trojan & Executable Scanner** node.
2. From the configuration options (in the right window), select the **Enable Trojan & Executable Scanner** check box to activate this filter.
3. Specify the emails you want to check for Trojans and other malicious executables by selecting any of the following options:
 - **Check inbound emails** - Select this option to scan inbound emails for Trojans and malicious executable files.
 - **Check outbound emails** - Select this option to scan outbound emails for Trojans and malicious executable files.
4. Choose the required level of security by selecting one of the following options:
 - **High Security** - Select this option to quarantine almost all executables. If the executable file contains any known malicious signature it will get immediately quarantined.
 - **Medium Security** - Select this option to quarantine only suspicious executables. If the executable contains one high-risk signature or a combination of high-risk and low-risk signatures it will be quarantined.

- **Low Security** - Select this option to quarantine all malicious executables. If the executable contains at least one high-risk signature, it will be immediately quarantined.

Configuring actions

Screenshot 73 - Trojan and Executables Scanner: Actions Tab

5. Click the **Actions** tab to configure the actions you want GFI MailSecurity to take on emails containing a malicious executable. Select any of the following options:

- **Notify local user** - Select this option if you want to notify the email local users when this filter detects a malicious executable.

NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.

- **Notify administrator** - Select this option to send email notifications to the administrator whenever an email containing malicious executable is quarantined.
- **Log occurrence to this file** - Select this option to log the event whenever the Trojan & Executable Scanner detects an infected email. In the edit box below, specify either the file name only or the full path to the log file.

6. Click **Apply**.

8.3 Trojan & Executable Scanner updates

You can configure GFI MailSecurity to download Trojan & Executable Scanner updates automatically or to notify the administrator whenever new updates are available. To configure automatic updates:

1. Click the **GFI MailSecurity ► Trojan & Executable Scanner** node.
2. Click the **Updates** tab in the Trojan & Executable Scanner page (in the right window).
3. Select the **Automatically check for updates** check box to enable the auto-update feature.
4. From the **Downloading options** list, select one of the following download options:
 - **Only check for updates** - Select this option if you want GFI MailSecurity to just check and notify the administrator whenever updates are available for the Trojan & Executable Scanner. This option will NOT download the available updates.
 - **Check for updates and download** - Select this option if you want GFI MailSecurity to check and automatically download any updates available for the Trojan & Executable Scanner.
5. Specify how often you want GFI MailSecurity to check/download updates for the Trojan & Executable Scanner, by typing an interval in hours.
6. Click **Apply**.

Automatic update options

Configure the automatic update options.

☒ **Automatically check for updates**

Downloading option:

Check for updates and download

Download/check after the specified number of hours:

1

Last update:

10/12/2009 16:20:52

Update options

☒ **Enable email notifications upon successful updates (Notifications will always be sent for unsuccessful updates).**

Click the button below to force the updater service to download the most recent updates.

Download updates

Screenshot 74 - Trojan and Executable Scanner: Updates tab

Triggering the Trojan & Executable Scanner update manually



To check/download updates for the Trojan & Executable Scanner immediately, click **Download updates**.

9 The Email Exploit Engine

9.1 Introduction to e-mail exploits

What is an exploit?

An exploit uses known vulnerabilities in applications or operating systems to compromise the security of a system, for example, execute a program or command, or install a backdoor. It "exploits" a feature of a program or the operating system for its own use.

What is an e-mail exploit?

An email exploit is an exploit launched via email. An email exploit is essentially an exploit that can be embedded in an email, and executed on the recipient's machine either once the user opens or receives the email. This allows the hacker to bypass firewalls and anti-virus products.

Difference between Anti-Virus software & Email Exploit Detection software

Anti-virus software is designed to detect malicious code. It does not necessarily analyze the method used to execute the code.

The Email Exploit Detection Engine analyses emails for exploits - i.e., it scans for methods to execute a program or command on the user's system. The Email Exploit Engine does not check whether the program is malicious or not. Rather, it assumes a security risk if an email is using an exploit in order to run a program or command - whether or not the actual program or command is malicious.

In this manner, the Email Exploit Engine works like an intrusion detection system (IDS) for email. The Email Exploit Engine might cause more false-positives, but it is more secure than a normal anti-virus package, simply because it uses a different way of checking for e-mail threats.

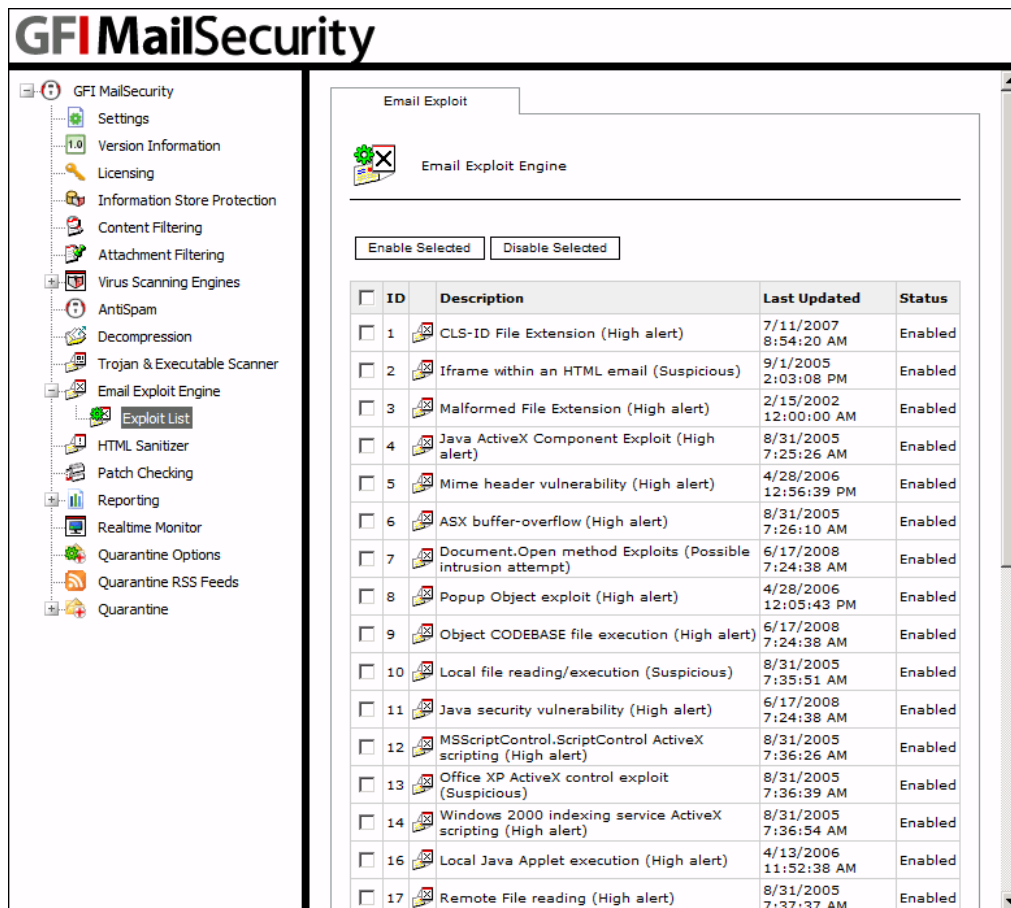
Furthermore, the Email Exploit Engine is optimized for finding exploits in email, and can therefore be more effective at this job than a general-purpose anti-virus engine.

9.2 Configuring the Email Exploit Engine

Enable/Disable email exploits

To enable/disable emails exploits:

1. Click the **GFI MailSecurity ► Email Exploit Engine ► Exploit List** node.
2. From the Email Exploit Engine page (in the right window), select the check box of the exploit(s) that you want to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly. The status change is displayed immediately in the exploits **Status** column.

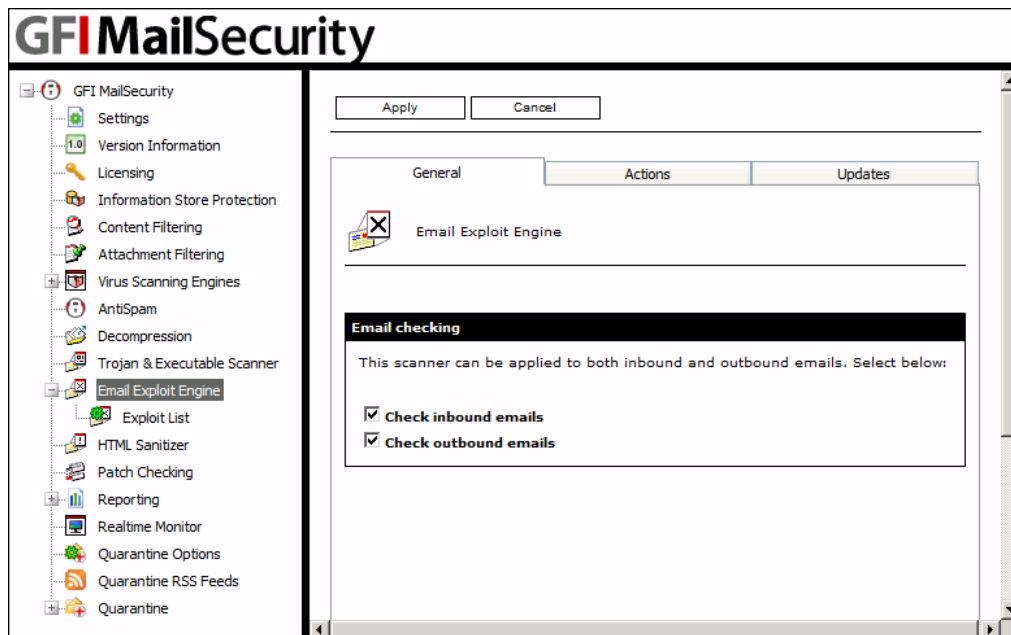


Screenshot 75 - Email Exploit list

Configuring the Email Exploit Engine properties

To configure the **Email Exploit Engine** properties:

1. Click the **GFI MailSecurity ► Email Exploit Engine** node.
2. From the **General** tab, select whether you want to check inbound and/or outbound emails for email exploits, by selecting the **Check inbound emails** check box and **Check outbound emails** check box accordingly.



Screenshot 76 - Email Exploit Engine: General Tab

3. Click on the **Actions** tab, to set what actions you want GFI MailSecurity to take on emails containing email exploits.

4. You can choose either one of the following options:

- **Quarantine email:** Select this option to quarantine the email containing the email exploit for review by an administrator. For more information, refer to [Quarantine](#) chapter in this manual.
- **Delete email:** Select this option to delete the email containing the email exploit completely.

5. When an email exploit is detected, you can also choose to inform the administrator and/or user by sending email notifications. You can configure the required notifications by selecting any of the following options:

- **Notify local user:** Select this option if you want to notify the email local users when this filter detects an email exploit.

NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.

- **Notify administrator:** Select this option if you want to send email notifications to the administrator whenever an email containing email exploits is detected. The administrator's email address is specified during the installation of GFI MailSecurity but can still be changed from the GFI MailSecurity configuration (**GFI MailSecurity ► Settings node ► General tab**). For more information refer to the [Define the administrator's email address](#) section in the General Settings chapter.

Screenshot 77 - Email Exploit Engine: Actions Tab

6. Select the **Log occurrence to this file** check box if you want to log all email exploits detected to a log file. In the box below, specify either a file name only or the full path to the log file.

7. Click **Apply**.

9.3 Email Exploit Engine updates

You can configure GFI MailSecurity to download Email Exploit Engine updates automatically or to notify the administrator whenever new updates are available. To configure automatic updates:

1. Click the **GFI MailSecurity ► Email Exploit Engine** node.
2. Click the **Updates** tab.
3. Select the **Automatically check for updates** check box to enable the auto-update feature.
4. From the **Downloading option** list, select one of the following download options:
 - **Only check for updates** - Select this option if you want GFI MailSecurity to just check and notify the administrator whenever updates are available

for the Email Exploit Engine. This option will NOT download the available updates.

- **Check for updates and download** - Select this option if you want GFI MailSecurity to check and automatically download any updates available for the Email Exploit Engine.

5. Specify how often you want GFI MailSecurity to check/download updates for the Email Exploit Engine, by typing an interval in hours.

6. Click **Apply**.

Automatic update options

Configure the automatic update options.

☒ **Automatically check for updates**

Downloading option:

Check for updates and download

Download/check after the specified number of hours:

1

Last update:

10/12/2009 16:20:50

Update options

☒ **Enable email notifications upon successful updates (Notifications will always be sent for unsuccessful updates).**

Click the button below to force the updater service to download the most recent updates.

Download updates

Screenshot 78 - Email Exploit Engine: Updates Tab

Triggering the Email Exploit Engine update manually

To check/download updates for the Email Exploit Engine immediately, click **Download updates**.

10 The HTML Sanitizer

10.1 Introduction to the HTML Sanitizer

The HTML Sanitizer scans and cleans from scripting code the email body parts that have the MIME type set to “text/html” and all the attachments that have an extension of “.htm” or “.html”. The HTML is cleaned from all the scripts, rendering it harmless. The HTML sanitization process is an automated process, which does not require administrator intervention.

Why remove HTML scripts?

The introduction of HTML mail has allowed senders to include scripts in email that can be triggered automatically upon opening mail. HTML scripts are used in a number of headline hitting viruses, such as the KAK worm. Moreover, HTML scripts are often utilized in one-off attacks directed towards particular users and particular companies. Consequently, it is best if all scripts are removed from within HTML emails.

The HTML Sanitizer included in GFI MailSecurity provides automated protection against HTML scripting threats.

10.2 Configuring the HTML Sanitizer



Screenshot 79 - HTML Sanitizer configuration page

Configure the HTML Sanitizer as follows:

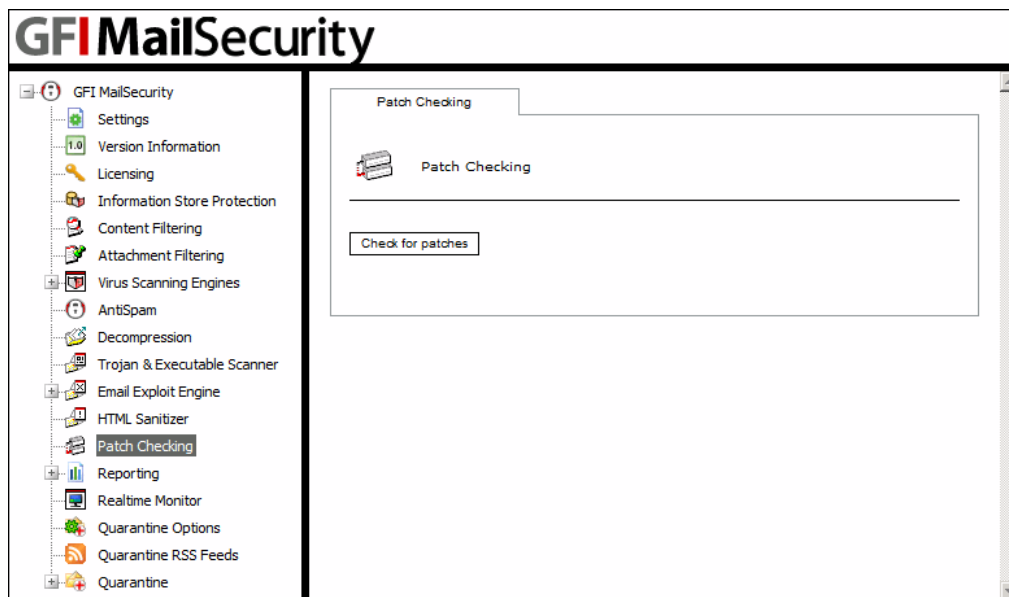
1. Click the **GFI MailSecurity ► HTML Sanitizer** node.
2. From the **HTML Sanitizer** configuration page, select the **Enable the HTML Sanitizer** check box to enable the HTML Sanitizer.
3. Select the emails you want to check for HTML scripts and clean by selecting any of the following options:

- **Check inbound emails** - Select this option to scan and clean HTML scripts from all inbound emails.
 - **Check outbound emails** - Select this option to scan and clean HTML scripts from all outbound emails.
4. Click **Apply**.

11 Patch Checking

11.1 Introduction to Patch Checking

The Patch Checking feature verifies if there are any software patches available for your version of GFI MailSecurity by directly connecting/querying the GFI Update Servers.



Screenshot 80 - List of available patches

If software updates are present on the GFI Servers, this feature lists them out for you to download. In addition, the list of available updates includes links to information about each patch as well as to the relative GFI Knowledge Base articles if available.

NOTE: In order to keep GFI MailSecurity running efficiently, we recommend that you periodically check for software updates. These updates would help to ensure better performance and enhance the functionality of GFI MailSecurity.

11.2 Downloading and installing software patches

To check for GFI MailSecurity software updates:

1. Click the **GFI MailSecurity ► Patch Checking** node, and click **Check for patches** in the right pane window, to connect to the GFI Update Server and check for available updates.
2. If software patches exist for your version of GFI MailSecurity, these are listed in the right window. Otherwise, you will be informed that no software patches are available. From the list of available software updates (in the right window), click the **Download** link included in the last column of each patch. This will start the download process. Repeat the same procedure for all the listed updates.
3. After all downloads are complete, you can start installing the software updates. Since the software patches vary in file format (i.e. could be DLL files,

EXE files, etc.), you must read the relative patch information for the installation instructions. To access the installation instructions and other information relevant to a patch, click the **Information** link provided in the list of available updates (in the right window of GFI MailSecurity).

NOTE: It is important that you follow the exact patch instructions provided in the information link. An incorrect patch installation might cause a product malfunction or degrade its performance.

NOTE: If available, GFI MailSecurity also includes links to Knowledge Base articles related to the listed patches. This is denoted by the **KB Article** caption in the KB link column of the patch. To access the Knowledge Base information, click the **KB Article** caption/link.

NOTE: GFI MailSecurity sends an email notification to the administrator whenever new software patches are discovered.

12 Quarantine

12.1 Introduction to the Quarantine Store

As outlined earlier in the manual, you can configure GFI MailSecurity to quarantine the emails that fail any of the content policy or content security checks. You can then review the quarantined emails and either approve or delete them.

You can approve/delete quarantined emails either directly from the Quarantine Store or through a Quarantine Action Form.

- Approve/Delete directly from the Quarantine Store (recommended). For more information on how to review emails in the Quarantine Store, refer to the 'Approving emails from the Quarantine Store' section, further on in this chapter.
- Approve/Delete from a Quarantine Action Form. GFI MailSecurity sends the Quarantine Action Form through email to the administrator (on the administrator's email address) or to a specific email address, belonging to an authorized person who can review quarantined emails. For more information, refer to the 'Enable email approval via HTML approval forms' section further on in this chapter.

12.2 The Quarantine Store

To access the GFI MailSecurity Quarantine Store, click the **GFI MailSecurity** ► **Quarantine** node. From the **Quarantine** node, the administrator/authorized user can search for quarantined emails as well as approve or delete emails.

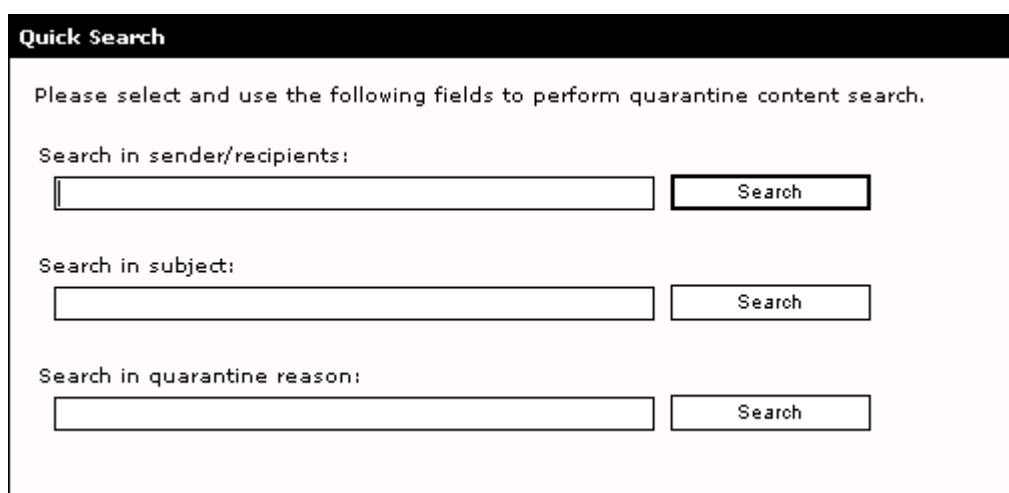
When you click the **Quarantine** node, GFI MailSecurity displays the following:

- **Quick Search** - You can search for quarantined emails by sender, recipient, subject or quarantine reason.
- **Quarantined Items** - You can see how many emails are currently stored in the Quarantine Store and the amounts that match each quarantine search folder, be it default or custom. To view the quarantined emails contained in a search folder, click on the quarantine search folder name. Refer to the 'Grouping quarantined emails in Search Folders' section further on in this chapter, for information on how to create and use search folders. To access this information from the navigation panel, expand the Quarantine node and click on a sub-node.



Screenshot 81 - Quarantine Store status page

Searching for emails in the Quarantine Store



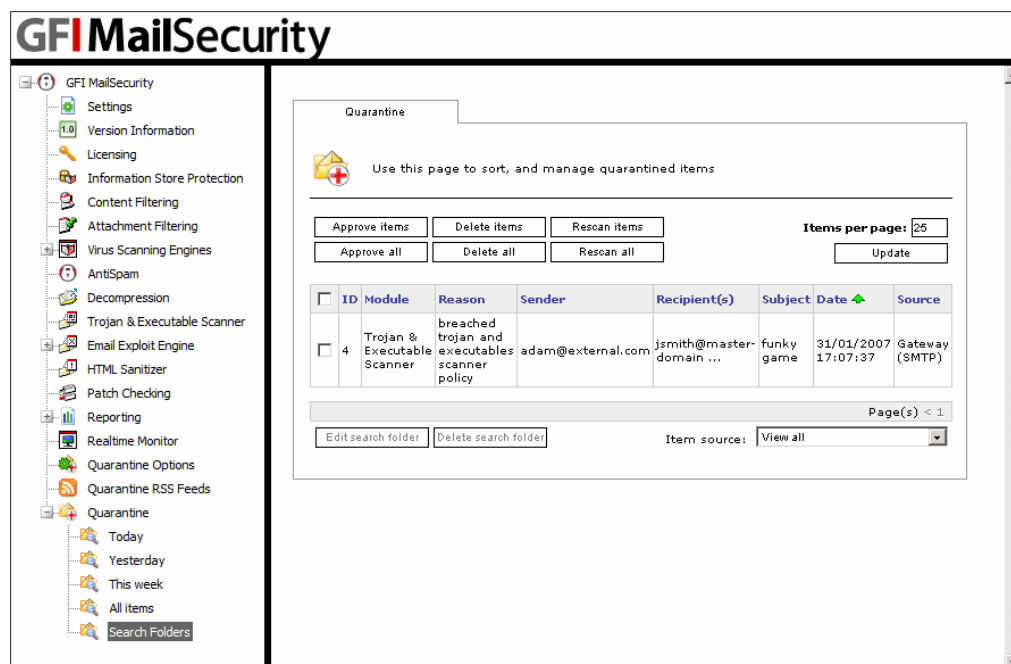
Screenshot 82 - Quarantine Store: Quick Search

To search for emails in the GFI MailSecurity Quarantine Store, follow these steps:

1. Click on either the **GFI MailSecurity ► Quarantine** node or the **GFI MailSecurity ► Quarantine ► Search Folders** node.

2. From the **Quick Search** area, use one of these methods to perform the search:

- **Search in sender/recipients** - Specify an email address and click **Search** to find quarantined emails sent from or received by that email address.
- **Search in subject** - Specify a keyword or phrase and click **Search** to find quarantined emails that contain that specific word/string in the subject.
- **Search in quarantine reason** - Specify a keyword or phrase and click **Search** to find quarantined emails that contain that specific word/string in the quarantine reason.



Screenshot 83 - Quick search results

12.3 Search Folders

What is a search folder?

A Search Folder is a special type of folder that has a search query associated to it. The contents of the search folder are the quarantined emails that match the search query. The content of a search folder is thus dynamic and changes automatically as emails that match the search folder criteria are quarantined or deleted.

Why are search folders useful?

The main benefit of search folders is that they help you organize your quarantined emails. In this way, it is easier for the administrator to identify and then approve or delete blocked emails.

Each search folder can have different search criteria, thus you can virtually split the Quarantine Store into subdivisions containing emails with specific

characteristics in each group. For example, you can create a search folder that collects only emails that were quarantined by the Virus Scanning Engines. A good idea is to create a search folder for each GFI MailSecurity module, so that instead of viewing one huge list of quarantined emails, you split them up into logical groups.

Grouping quarantined emails in Search Folders

To create a new search folder, follow these steps:

1. Click on either the **GFI MailSecurity ► Quarantine** node or the **GFI MailSecurity ► Quarantine ► Search Folders** node.
2. From the right panel, click **New search folder**.
3. In the **Search folder name** box, type a name for the new search folder, for example, "Emails blocked by Attachment Rules".
4. If you installed GFI MailSecurity on the Microsoft Exchange Server machine, you can limit the emails in this search folder to those blocked from a particular source. From the list under the **Item source** area, you can select one of the following:
 - **Information store (VSAPI)** - Only quarantined items forming part of the Information Store will be displayed.
 - **Information store (Transport)** - This option is only available when GFI MailSecurity is installed on a Microsoft Exchange Server 2007/2010 machine with the Hub Transport Server Role installed. Only quarantined items forming part of the Information Store that were scanned through the Hub Transport Agent will be displayed.
 - **Gateway (SMTP)** - Only inbound or outbound quarantined emails, SMTP traffic, will be displayed.
 - **Any** - All quarantined items will be displayed irrespective of the source.
5. You can now configure auto-purge settings for this search folder. If you configure auto purging on a search folder, GFI MailSecurity will delete any emails in that search folder that are older than the number of days you specify.


To enable auto-purging, select the **Enable Auto-purging** check box and specify a value in the **days(s)** box.

NOTE: Configure auto purging with great care since emails purged from the Quarantine Store are not recoverable.

6. Specify the search criteria that will determine the contents of this folder. You can select any of the following options:
 - **Quarantine reason** - Select this option to include all the emails containing a specific keyword or phrase in the quarantine reason. Type a keyword in the box next to this option.
 - **Item subject** - Select this option to include all the emails containing a specific keyword or phrase in the email subject. Type a keyword/phrase in the box next to this option.

- **Sender** - Select this option to include **ONLY** the emails sent from a particular email address. Type the sender email address in the box next to this option.
- **Recipient** - Select this option to include **ONLY** the emails sent to a particular email address. Type a recipient email address in the box next to this option.
- **Quarantined by** - Select this option to group emails quarantined by a specific (but not necessarily unique) filter in this search folder. Select a filter from the list next to this option (for example, Attachment Checking).

NOTE: Since GFI MailSecurity can block an email for multiple security threats or content policy infringements, you can choose to include only emails that were blocked by one specific filter. This is possible by selecting the **only** check box next to the filters list.

- **Item direction** - Select this option to limit the items included in this search folder to either Inbound or Outbound emails.
- **NOTE:** Leave this option unselected if you want to include both Inbound and Outbound emails in this Search Folder.
- **NOTE:** This option is only enabled when GFI MailSecurity is not installed on a Microsoft Exchange machine, or if it is, the Item source selected was Gateway.
- **Date** - Select this option to group emails by date. Specify a date in the relevant box or alternatively click the calendar  button and select the required date from the calendar window.

Specify a Date Range

You can also group emails by Date Range. To do so, click **Date Range**, and then specify a start date in the **Day from** box and an end date in the **Day to** box.

Specify time

In addition to the date, you can also specify the time or time range of the emails you want to include in this folder. To specify the time, select the time check box and input a time value in the relevant box.

Specify time range

To specify a time range for a particular day, click **Date Range** and specify the same date value in both the **Day** boxes. Subsequently specify the required start time in the **Time from** box and the end time in the **Time to** box.

7. Click **Save folder** to create the search folder.

New Search Folder



Use this page to create and edit search folders.

Define a new folder

Search folder name:

Item source

Please select item source.

Auto-Purging

With the auto-purge option, you can automate the management of the items stored in this search folder. Items that have been quarantined for at least the number of days you specify will be automatically deleted from the quarantine system.

☒ Enable Auto-purging

Automatically purge items older than:

 day(s)

Keyword search

Quarantine reason:

☐

Item subject:

☐

Sender:

☐

Recipient:

☐

Search options

Quarantined by:

☐ ☐ only

Item direction:

☐

Date filter

☐ Date:

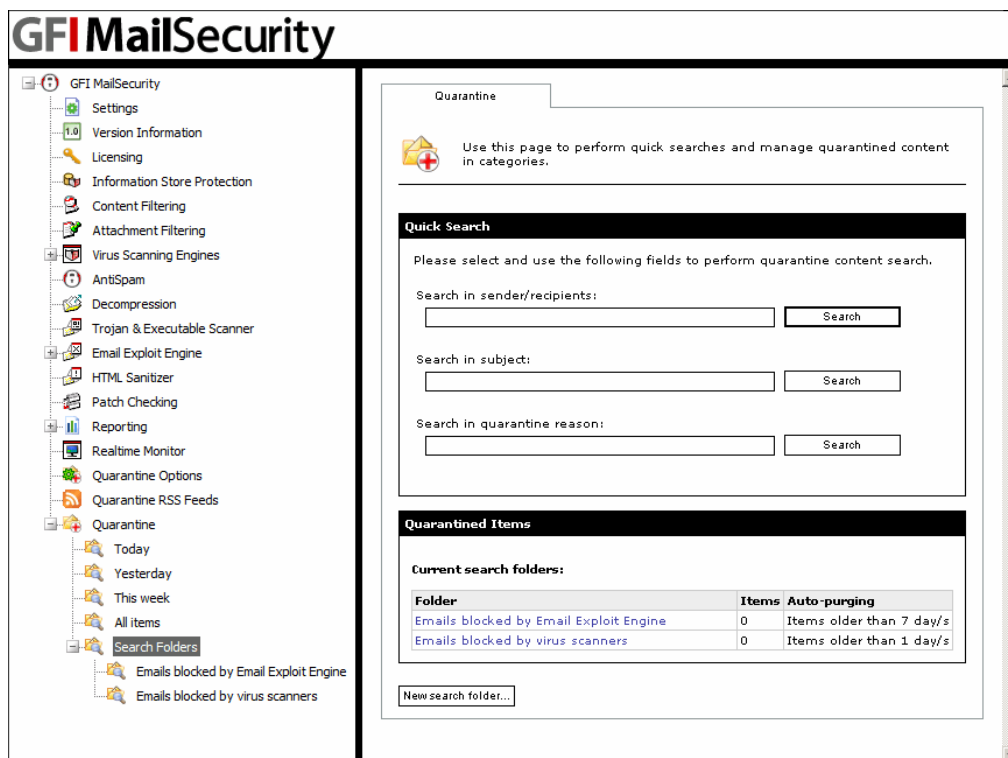
Day:



Time: (hh:mm:ss:am/pm)

Date range

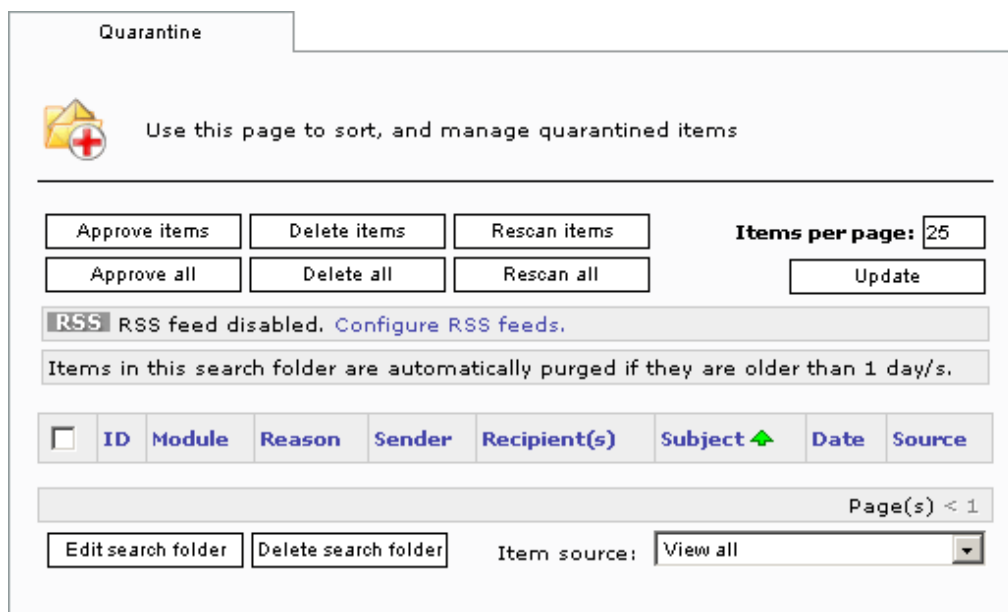
Screenshot 84 - New Search Folder properties page



Screenshot 85 - Search Folder Contents Summary

NOTE: Click the **Search Folder** node to view the amount of emails matching each Search Folder.

Changing Search Folder properties



Screenshot 86 - Search Folder options

To modify the properties, search criteria and auto-purge settings of an existing search folder:

1. Expand the **GFI MailSecurity ► Quarantine ► Search Folders** node.
2. Click on the Search Folder you want to modify and from the right pane, click **Edit search folder**.
3. Make the required changes to the search folder properties. For more information on how to configure search folder options, refer to the 'Grouping quarantined emails in Search Folders' section earlier in this chapter.
4. Click **Save folder**.

Deleting Search Folders

To delete an existing search folder:

1. Expand the **GFI MailSecurity ► Quarantine ► Search Folders** node.
2. Click on the Search Folder you want to delete and from the right pane, click **Delete search folder**.

NOTE: - When you delete a search folder, no emails are actually deleted from the quarantine store. This is because a search folder is just a query that retrieves matching emails from the Quarantine Store. In other words, a search folder is just a visual grouping of emails that match certain criteria, but the actual email is not physically stored in the search folder. However, you can still approve or delete emails from within a search folder by using the **Approve items / Delete items** buttons.


12.4 Approving emails from the Quarantine Store

You can approve emails from any sub-node underneath the **Quarantine** node including the Search Folders. You can also use Quick Search to look for specific emails that you want to approve. To approve emails:

1. Expand the **GFI MailSecurity ► Quarantine** node and select the sub-node that contains the email(s) you want to approve (for example, select the **Today** node if you want to approve emails that were quarantined today). Alternatively, you can use Quick Search to look for the emails that you want to approve.

NOTE: You can approve an email that was quarantined today from the **Today** node, the **This Week** node, the **All Emails** node as well as from any Search Folder that contains the email. The difference between the mentioned nodes is the amount of emails that are present within.

Quarantine


Use this page to sort, and manage quarantined items

Approve items

Delete items

Rescan items

Approve all


Delete all

Rescan all

Items per page: 25

Update

RSS RSS feed disabled. [Configure RSS feeds.](#)

<input type="checkbox"/>	ID	Module	Reason	Sender	Recipient(s)	Subject	Date 	Source
<input type="checkbox"/>	6	Attachment Checking	triggered rule "content policy: block most common image attachments (.jpg, ...	meredith@external.co ...	jackb@master-domain, ...	party pic	02/02/2007 14:07:56	Gateway (SMTP)
<input type="checkbox"/>	5	Attachment Checking	triggered rule "content policy: block all potentially malicious attachments ...	paul@external.com	jackb@master-domain, ...	funny video	02/02/2007 14:02:09	Gateway (SMTP)
<input type="checkbox"/>	4	Trojan & Executable Scanner	breached trojan and executables scanner policy	adam@external.com	jsmith@master-domain ...	funky game	31/01/2007 17:07:37	Gateway (SMTP)

Edit search folder

Delete search folder

Page(s) < 1

Item source:

View all

Screenshot 87 - List of Quarantined Emails in selected Search Folder

NOTE: You can sort the quarantined emails by clicking on any of the column headings. If you click the same column heading, the sort order switches between ascending and descending.

2. Select the check box of the email(s) you want to approve and click **Approve items**.

NOTE: If you want to approve all the listed emails, you do not need to select all the check boxes individually. Just click **Approve all**.

NOTE: To refresh the information, click **Update**.

NOTE: If an email matches more than one search folder, the administrator does not need to approve the same email from each search folder. If you approve an email from a search folder, GFI MailSecurity removes it from the Quarantine Store and so it does not list in any of the other search folders.

12.5 Deleting emails from the Quarantine Store

To delete emails from the Quarantine Store:

1. Expand the **GFI MailSecurity ► Quarantine** node and select the sub-node that contains the email(s) you want to delete (for example, select the **Today** node if you want to delete emails that were quarantined today). Alternatively, you can use Quick Search to look for the emails that you want to delete.

NOTE: You can delete an email that was quarantined today from the **Today** node, the **This Week** node, the **All Emails** node as well as from any Search Folder that contains the email. The difference between the mentioned nodes is the amount of emails that are present within.

2. Select the check box of the email(s) you want to delete and click **Delete items**.

NOTE: If you want to delete all the listed emails, you do not need to select all the check boxes individually. Just click **Delete all**.

NOTE: To refresh the information, click **Update**.

NOTE: If an email matches more than one search folder, the administrator does not need to delete the same email from each search folder. If you delete an email from a search folder, GFI MailSecurity removes it from the Quarantine Store and so it does not list in any of the other search folders.

12.6 Rescanning emails from the Quarantine Store

The Quarantine Store allows you to submit quarantined emails for rescanning. This option is provided mostly to cater for virus outbreak scenarios.

For example, an email is quarantined on Monday because it infringed a Content Checking rule. The same email also contained a newly released virus. However, since the virus signatures had not yet been updated when it passed through GFI MailSecurity, it did not infringe any virus scanning rules.

A few hours after this email was quarantined, the virus signatures are updated. The next day, the administrator comes across this email while going through the quarantine store. If rescanning of quarantined items was not possible, the administrator would have only two options, delete the email, or approve it and release a virus unknowingly.

With the rescan option, the administrator can choose to submit the email for rescanning. This time around, since the virus signatures were updated, the email will infringe both a virus scanner rule, as well as the same Content Checking rule.

When the administrator finds the same email in the Quarantine Store, the reason for quarantining will be that a virus was detected. The administrator will then most probably choose to delete the email.

To rescan emails from the Quarantine Store:

1. Expand the **GFI MailSecurity ► Quarantine** node and select the sub-node that contains the email(s) you want to rescan (for example, select the **Today** node if you want to rescan emails that were blocked today). Alternatively, you can use Quick Search to look for the emails that you want to rescan.

2. Select the check box of the email(s) you want to rescan and click **Rescan items**.

NOTE: If you want to rescan all the listed emails, you do not need to select all the check boxes individually. Just click **Rescan all**.


NOTE: To refresh the information, click **Update**.

12.7 View the full security threat report of an email

To view the full security threat report of a quarantined email, follow these steps:

1. Expand the **GFI MailSecurity ► Quarantine** node and select the sub-node that contains the email(s) you want to view (for example, select the **Today** node if you want to view emails that GFI MailSecurity quarantined today). Alternatively, you can use Quick Search to look for the emails that you want to view.
2. GFI MailSecurity lists the quarantined emails in a table. GFI MailSecurity can quarantine an email for one or more security reasons, but it only displays the top security threat under the **Reason** column.

Quarantine


Use this page to sort, and manage quarantined items

Approve items

Delete items

Rescan items

Approve all

Delete all

Rescan all

Items per page: 25

Update

RSS

RSS feed enabled. Use the URL associated with the RSS icon to subscribe to the feed.

<input type="checkbox"/>	ID	Module	Reason	Sender	Recipient(s)	Subject	Date	Source
<input type="checkbox"/>	8	Trojan & Executable Scanner	breached trojan and executables scanner policy	adam@external.com	jackb@master-domain. ...	free game and funny pics	07/02/2007 09:49:48	Gateway (SMTP)

Edit search folder

Delete search folder

Page(s) < 1

Item source: View all

Screenshot 88 - A quarantined email

3. To view the full security threat report, click on the row of the quarantined email you want to view. GFI MailSecurity will list all the body parts of the email such as plain text body, HTML body, and any attachments.


4. To return to the list of quarantined emails, click **Back**.

NOTE: From this page you can also approve, delete, or re-scan the particular email you are currently viewing, by clicking the respective button. If you want to delete an email and inform the intended recipients of the action taken, click **Delete and Notify** instead of **Delete**.

NOTE: If you want to download the quarantined item, click **Download Item**.

NOTE: Unless the source of the item is **Information Store (VSAPI)**, you can approve a sanitized version of the email by clicking **Sanitize and Approve**. When you click this option, GFI MailSecurity removes the email from the quarantine store and sends it to the intended recipients, but before doing so, all the body parts that have a security threat are removed from the email, thus rendering it safe.

Quarantined email


Showing details for quarantined item 8

Approve

Sanitize and Approve

Rescan

Delete

Delete and Notify

Download item

Back

Item Information

Source:

Gateway (SMTP)

Subject:

Free game and funny pics

From:

adam@external.com

To:

jackb@master-domain.com

Date:

07/02/2007 09:49:48

Module:

Trojan & Executable Scanner






Scan Modules:

Trojan & Executable Scanner

Attachment Checking

Content Checking

Attachments

Filename (size)	Threat Description
 coolgame.exe (1008Kb) ⓘ	Breached Trojan and Executables scanner policy
<div>Module</div> <div>Threat</div>	
Trojan & Executable Scanner	File 'coolgame.exe' breached the following Trojan & Executable Scanner rule/s: "Checks if the executable tries to change keyboard, mouse or display settings (CheckUIChange)"
Attachment Checking	File "coolgame.exe" triggered rule "CONTENT POLICY: Block all potentially malicious attachments" (Claimed extension "exe" listed in "block" extension list)
 fun 03.jpg (22.91Kb) ⓘ	Triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)"
 fun 04.gif (22.91Kb) ⓘ	Triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)"
 fun 02.jpg (22.91Kb) ⓘ	Triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)"
<div>Module</div> <div>Threat</div>	
Attachment Checking	File "fun 02.jpg" triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)" (Claimed extension "jpg" listed in "block" extension list)
 fun 01.jpg (22.91Kb) ⓘ	Triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)"

Message Text

Text Body

HTML Body

Please click here to see quarantined content

The message body might contain malicious content. Instead of displaying the message body, the threat description is being shown. The following table shows the threat details for this message body. To view the actual message body, please click the link above.

Plugin	Threat
Content Checking	Words in body triggered rule "CONTENT POLICY: Block Sexual Content" (Words found: jack)

Screenshot 89 - Viewing the full security threat report of a quarantined email

12.8 Enable email approval via HTML approval forms



Screenshot 90 - Quarantine Options configuration page

You can configure GFI MailSecurity to send HTML Quarantine Action Forms through email to the administrator or an authorized user. The Quarantine Action Form makes it possible for the administrator to approve or delete quarantined emails directly from the email client without accessing the Quarantine Store. To enable the sending of HTML Quarantine Action Forms, follow these steps:

1. Click the **GFI MailSecurity ► Quarantine Options** node.
2. Select the **Send quarantine approval forms by email** check box to enable the sending of HTML Quarantine Action Forms through email.
3. Specify to whom you want to send the HTML Quarantine Action Forms (i.e. specify who will review/approve the quarantined emails) by selecting one of the following options:
 - **Send to administrator** - Select this option to send the HTML Quarantine Action Forms to the administrator (i.e. using the email address specified during the installation stage or configured in the **GFI MailSecurity ► Settings node ► General tab**). For more information on how to configure the administrator's email address, refer to [Define the administrator's email address](#) section in this manual.
 - **Send to the following email address** - Select this option to send the HTML Quarantine Action Forms to a specified email address/user group or public folder. Type the recipient in the box provided underneath this option.

NOTE: In the HTML Quarantine Action Form, you can click **More details** to view all the information related to the quarantined email.

4. Click **Apply**.

How to approve or delete quarantined emails from an email client

When GFI MailSecurity quarantines an email, the administrator receives an email containing an HTML Quarantine Action Form. The form contains details related to the quarantined email including the reason why it was blocked and any attachments that were included in the email.

Notification: GFI MailSecurity detected a threat. - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: Administrator Sent: Tue 10/13/2009 4:22 PM
To: John Smith
Cc:
Subject: Notification: GFI MailSecurity detected a threat.

GFI MailSecurity **Quarantine Action Form**

Dear Administrator,

On the 13 October 2009 GFI MailSecurity quarantined the following item.

Item ID	7
Highest Priority Module	Attachment Checking
Subject	callcall
From	jackb@external.com
To	jsmith@masterdomain.com

Threats detected

	Filename	Reason
🚫	funny.mp3 (25B)	Attachment Checking : Triggered rule "CONTENT POLICY: Block all potentially malicious attachments"

Please select from the following options:

Screenshot 91 - HTML approval form

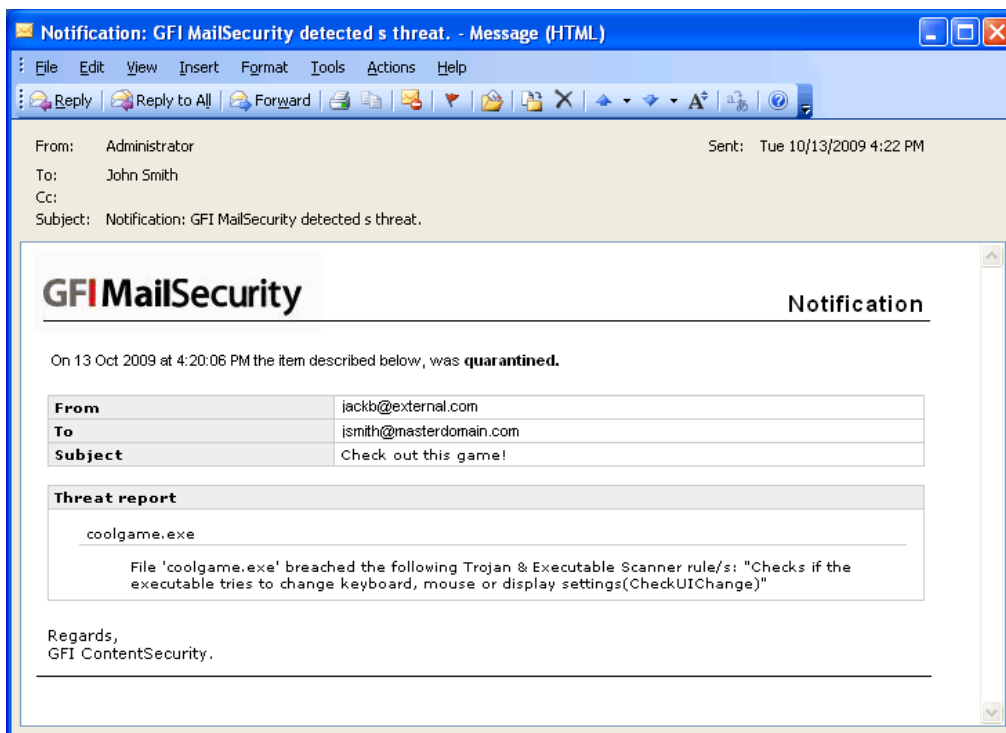
Through the HTML Quarantine Action Form, the administrator can approve or delete the email mentioned in the form by clicking on **Approve** or **Delete** accordingly. If the administrator approves the quarantined email, GFI MailSecurity will forward the quarantined email to the intended recipient and remove it from the Quarantine Store. In addition, if the email was inbound, the recipient will receive an email describing the status change of the quarantined email (i.e. approved or deleted). This email is mostly required to inform the user when the quarantined email is deleted.

12.9 Quarantined mail from the user point of view

The quarantining of mail is largely transparent to the mail user. For both inbound and outbound mail, users will receive the quarantined mail as soon as the administrator approves it.

If you select to notify the local user, via the notification options group under the actions tab of a particular node, the local user will receive an email to inform him that an email was quarantined as shown in the following screenshot.

NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by the 'notify local users' setting.



Screenshot 92 - Quarantined email user notification

12.10 Enable quarantine RSS feeds

What is RSS?

Really Simple Syndication (RSS) is a protocol used by websites that update their content frequently, for example news sites, weblogs and so on, to inform end users of what is new or updated on the website.

The website publishes an XML file, called an RSS feed, that complies with the schema defined in the RSS standard. End users make use of a special application, called a feed reader or aggregator, to subscribe to the different RSS feeds. The aggregator reads the XML file from the URL specified when subscribing, parses the content and displays a list of updated articles. The entries usually include a summary of the article and a link to view the full article.

How does GFI MailSecurity use RSS?

The quarantine store is like a website that is updated frequently with new blocked content. To facilitate the work of the administrator in keeping an eye on the GFI MailSecurity quarantine store, RSS feeds can now be enabled on the quarantine folders.

If you enable RSS feeds on a quarantine folder, the administrator can use an RSS feed reader to subscribe to the quarantine folder RSS feed. Through the RSS feed reader, the administrator is periodically informed of new blocked content in the quarantine store.

NOTE: For a list of freely available RSS feed readers please visit <http://kbase.gfi.com/showarticle.asp?id=KBID002661>. The RSS feed readers listed support authentication and have been tested with the quarantine RSS feeds feature of GFI MailSecurity.

How do I configure RSS on a quarantine folder?

To enable RSS feeds on specific quarantine folders, follow these steps:

1. Click the **GFI MailSecurity ► Quarantine RSS Feeds** node.

GFI MailSecurity

Quarantine RSS Feeds

Configure RSS feeds on the quarantine search folders

GFI MailSecurity uses RSS (Really Simple Syndication) feeds to inform you when new items are blocked in the quarantine.

To read Quarantine RSS Feeds you can use an RSS feed reader program to subscribe to the feed. To subscribe to a feed, copy the URL associated with the orange RSS button to the left of the Quarantine folder you want to monitor and use it to create a new subscription in the RSS feed reader.

NOTE: Only users given access privilege through the GFI MailSecurity SwitchBoard tool are allowed to subscribe to the Quarantine RSS feeds. Please visit <http://kbase.gfi.com/showarticle.asp?id=KBID002661> for a list of freely available RSS feed readers which are known to support authentication and have been tested out with the GFI MailSecurity Quarantine RSS Feeds.

☐ **Enable Quarantine RSS Feeds**
If the above checkbox is unchecked, no feeds will be generated regardless of the individual filter's settings

RSS Feeds

OPML To subscribe to all enabled feeds, copy the URL associated with the orange OPML button.

Default quarantine folder	RSS Feed Status	Interval	Maximum Items
Today	Disabled	10 minutes	100
Yesterday	Disabled	10 minutes	100
This Week	Disabled	10 minutes	100
All Items	Disabled	10 minutes	100

Custom quarantine folder	RSS Feed Status	Interval	Maximum Items
Emails blocked by Email Exploit Engine	Disabled	10 minutes	100
Emails blocked by virus scanners	Disabled	10 minutes	100

Screenshot 93 - Quarantine RSS feeds

2. Select the **Enable Quarantine RSS Feeds** check box.
3. Under the **RSS Feeds** area you can view a list of all the quarantine search folders, both default and custom, currently configured. To configure RSS feeds for a particular quarantine folder, click **Edit** to the right of the quarantine folder entry.

RSS Feeds

OPML To subscribe to all enabled feeds, copy the URL associated with the orange OPML button. [Edit...](#)

Default quarantine folder	RSS Feed Status	Interval	Maximum Items
RSS Today	Enabled	10 minutes	100

☒ **Enable Quarantine RSS feeds on this folder**

Refresh feed content every:
10 minutes

Feed should contain at most:
100 items

Please use the following address to subscribe to this feed.

<http://MIN2K3JENTSVR:80/MailSecurityRSS/issfeed.aspx?feedName=today.xml&uniqueid=B6639C8A-B27E-403C-A63E-319CC>

NOTE: If you give everyone access to the RSS feeds from the GFI MailSecurity SwitchBoard application or disable NTLM security on the RSS feeds virtual directory, anyone will be able to subscribe to this feed. If you suspect unauthorized users managed to get a copy of this URL, click the 'Reset Feed URL' button to generate a new URL and click the 'Apply' button. You then need to modify the RSS subscription to point to the new URL.

[Reset Feed URL](#)

Custom quarantine folder	RSS Feed Status	Interval	Maximum Items
RSS Yesterday	Disabled	10 minutes	100
RSS This Week	Disabled	10 minutes	100
RSS All Items	Disabled	10 minutes	100

Screenshot 94 - Quarantine folder RSS feed

4. Select the **Enable Quarantine RSS feeds on this folder** check box.
5. Specify an interval in minutes in the **Refresh feed content every** box. The default value is 10 minutes.
6. Specify the maximum number of items you want the feed to include in the **Feed should contain at most** box.

NOTE: By default, the GFI MailSecurity quarantine RSS feeds require authentication and thus only the users configured in the GFI MailSecurity SwitchBoard tool can subscribe to the RSS feeds. For more information, refer to [Securing access to the GFI MailSecurity Quarantine RSS feeds](#) section in this manual.

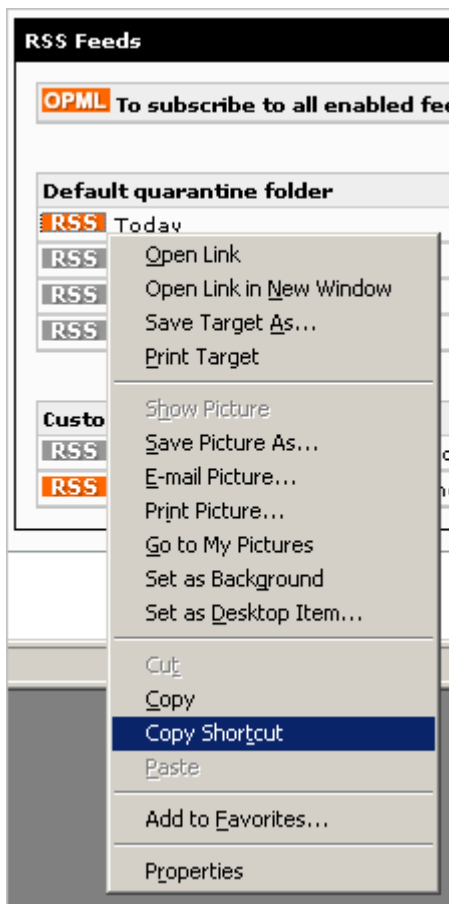
NOTE: If you give everyone access to the RSS feeds from the GFI MailSecurity SwitchBoard application or disable NTLM security on the RSS feeds virtual directory, anyone will be able to subscribe to the feeds. If you suspect unauthorized users managed to get a copy of a quarantine folder RSS feed URL, click the **Reset Feed URL** button for the specific quarantine folder and then click **Apply**. You then need to update the RSS subscription in your RSS feed reader application to point to the new URL. If you suspect that all RSS feed URLs might have been discovered, click **Edit** to the right of the **OPML** entry, click **Reset all the URLs** and then click **Apply**. You then need to update all the RSS subscriptions in your RSS feed reader to point to the new URLs.

7. Click **Apply**.

How do I subscribe to a quarantine search folder RSS feed?

To subscribe to an RSS feed follow these steps:

1. Right-click on the RSS icon to the left of the quarantine search folder to which you want to subscribe.



Screenshot 95 - Copy RSS feed URL

2. Click **Copy Shortcut**.
3. Use your favorite RSS feed reader application to create a new RSS feed subscription. Use the RSS feed URL copied in the previous step to specify the location of the feed.

NOTE: If you want to subscribe to all the enabled quarantine search folder RSS feeds in one go, copy the shortcut of the OPML icon. RSS feed reader applications usually have an option to import RSS feeds from an OPML file. An OPML file is an XML file that contains a list of RSS feeds, in this case all the quarantine search folder RSS feeds that are enabled.

12.11 Enable the Directory Harvesting filter on quarantined emails

Since GFI MailSecurity is usually installed as a first line of defense against email-based threats, it will process a lot of spam email because server level

spam filters, such as GFI MailEssentials, are usually installed behind GFI MailSecurity.

For this reason, GFI MailSecurity will process a lot of spam email. Some of the spam email contains malicious attachments such as viruses, trojans and so on, and will thus be blocked by GFI MailSecurity and stored in the quarantine store for review.

Spam email quarantined by GFI MailSecurity will thus clutter the quarantine store with many useless emails, making the administrative review process more complex.

To eliminate malicious spam email from the quarantine store you can enable the Directory Harvesting filter on the quarantine store. The Directory Harvesting filter will scan emails that GFI MailSecurity blocks before they are stored in the quarantine store. If all the recipients of the blocked email are non-local or do not exist on the organizations Active Directory or email server, GFI MailSecurity will delete the blocked email instead of storing it in the quarantine store.

The Directory Harvesting filter determines if a user exists or is local, by performing user lookups against the Active Directory or LDAP server you configure.

To enable the Directory Harvesting filter on the quarantine store, follow these steps:

1. Click the **GFI MailSecurity ► Quarantine Options** node.
2. Click the **Directory Harvesting** tab.

Quarantine Mode
Directory Harvesting

Directory Harvesting

If you enable directory harvesting protection on the quarantining system, GFI MailSecurity will delete items that have only non-existent recipients, instead of storing them in the quarantine.

This feature will automatically keep your quarantine store clean from malicious spam email.

☒ **Enable directory harvesting protection**

Lookup options

☐ Use native Active Directory lookups

☒ **Use LDAP lookups**

LDAP Settings

Server:

Port: ☐ Use SSL

Base DN: ▼

☐ Anonymous bind Update DN list

User:

Password:

* For security reasons, the length in the password box above does not necessarily reflect the true password length

Email address test

Email address:

Test

Logging options

☐ Log occurrence to this file:

Screenshot 96 - Directory Harvesting filter

3. Select the **Enable directory harvesting protection** check box.

4. If you installed GFI MailSecurity in AD mode, click **Use native Active Directory lookups** and skip to step 7. If you want, you can choose to use LDAP lookups, as outlined in the next step.

5. If you installed GFI MailSecurity in SMTP mode, click **Use LDAP lookups**.

6. Specify the LDAP server name or IP in the **Server** box and the port number, default 389, in the **Port** box. If your LDAP server requires authentication, ensure that the **Anonymous bind** check box is clear and enter the authentication details in the **User** and **Password** boxes.

7. Click **Update DN list** to populate the **Base DN** list and select the appropriate entry from the list.

8. To test your LDAP configuration settings, specify a valid email address in the **Email address** box and click **Test**. If the lookup succeeds, **Email address found** is displayed underneath the **Email address** box.

NOTE: If you installed GFI MailSecurity 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, we recommend that you perform Directory Harvesting checks using LDAP lookups (i.e. click **Use LDAP lookups** and specify your LDAP server details).

NOTE: When GFI MailSecurity 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, you must use LDAP lookups in order to enable the Directory Harvesting filter 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: When connecting to an Active Directory using LDAP (i.e. when GFI MailSecurity is 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: In an Active Directory, normally the LDAP server is the Domain Controller.

9. If you want to keep a log of the emails that GFI MailSecurity deletes through the Directory Harvesting filter, select the **Log occurrence to this file** check box and specify a log file name in the box below.

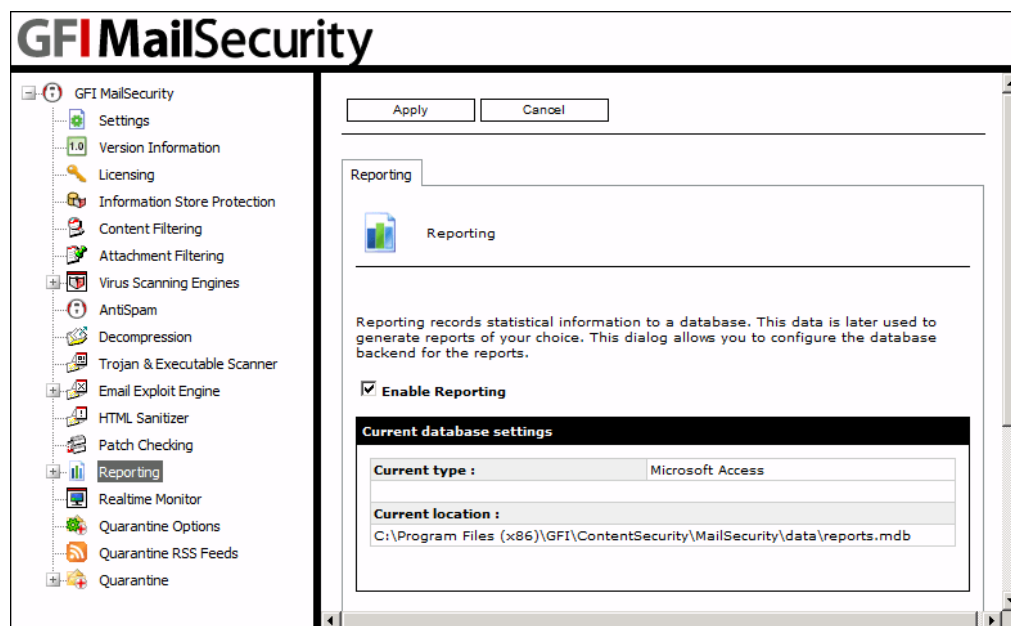
10. Click **Apply**.

13 Reporting

13.1 Introduction to GFI MailSecurity Reporting

Through the reporting option, you can configure GFI MailSecurity to log statistical data, such as the amount of emails being processed and quarantined, into a database. You can then buy the GFI MailSecurity ReportPack add-on, to generate informative reports based on the data collected in the database.

13.1.1 Configuring the statistical information database

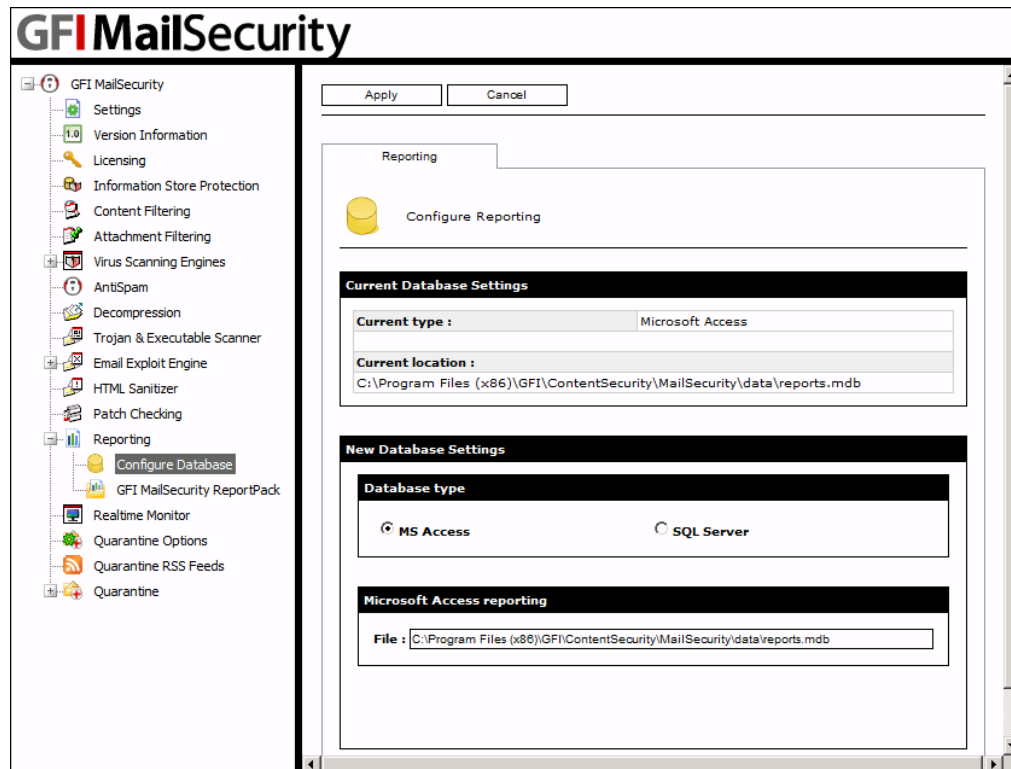


Screenshot 97 - Reporting page

To configure the reporting option:

1. Click the **GFI MailSecurity ► Reporting** node.
2. To enable data logging for reporting purposes, select the **Enable Reporting** check box. If clear this check box, no reporting data will be logged.
3. In the reporting page, you can see the details of the currently configured reporting database, such as the database type and the location of the database. To change the current database settings, expand the **Reporting** node and click the **Configure Database** sub-node.
4. In the Configure Reporting page, you can configure the reporting database as follows:

13.1.2 Configuring a Microsoft Access database backend



Screenshot 98 - Configuring a Microsoft Access database backend


1. Click **MS Access** and type the complete path including the filename of the database file in which the statistical data must be stored. If you only specify a filename, the database file is created in the default path i.e.

C:\Program Files\GFI\ContentSecurity\MailSecurity\data\<filename.mdb>

2. Click **Apply**.

13.1.3 Configuring a Microsoft SQL Server database backend

Reporting


 Configure Reporting

Current Database Settings

Current type : Microsoft Access

Current location :
 C:\Program Files\GFI\ContentSecurity\MailSecurity\data\reports.mdb

New Database Settings

Database type

☐ MS Access
 ☒ SQL Server

SQL server reporting

☒ **Detected server :** WIN2K3SQL

☐ **Manually specified server :**

User : sa

Password :

Get Database List

Database : IMSECDB

Screenshot 99 - Configuring SQL Server Database backend

1. Click **SQL Server**.
2. Click **Detected server** and then select the SQL Server from the **Server** list or else click **Manually specified server** and in the box type the IP or server name where Microsoft SQL Server is hosted.
3. Type the name of a user that is authorized to access the Microsoft SQL Server in the **User** box.
4. Type the password for this account in the **Password** box.
5. Click **Get Database List** to extract the database information from this server and populate the **Database** list.

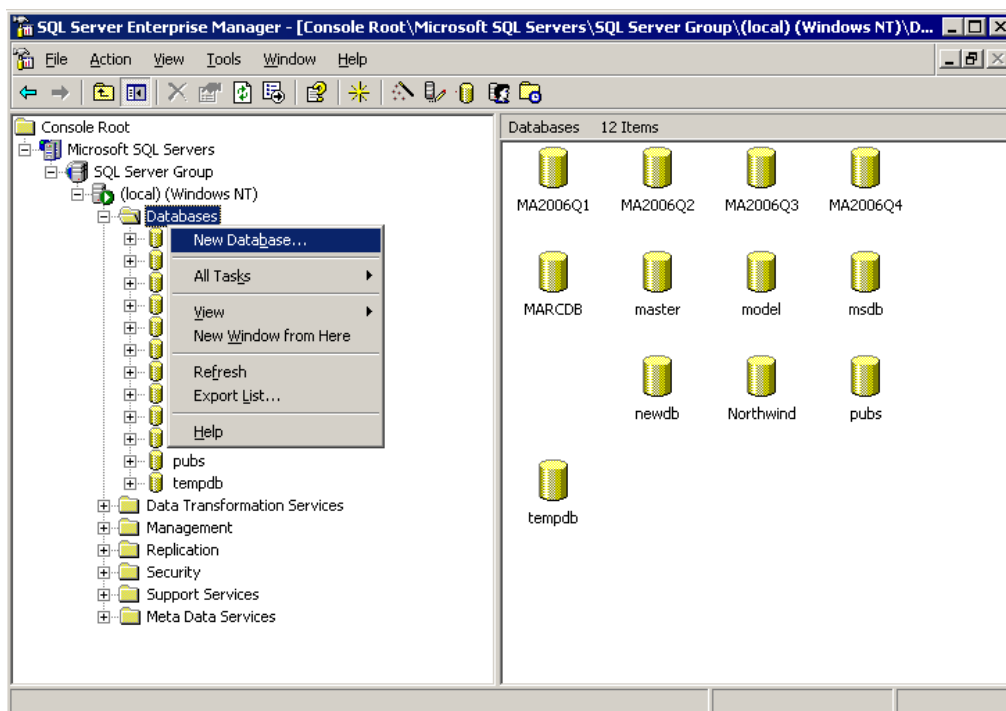
6. From the **Database** list, select the database where you want to store the statistical data.

7. Click **Apply**.

NOTE: Make sure that you have already created the database on Microsoft SQL Server before configuring this option.

Creating a new database on Microsoft SQL Server 2000

1. Open the SQL Server Enterprise Manager (**Start ► Programs ► Microsoft SQL Server ► Enterprise Manager**) and expand the Microsoft SQL Server node where you want to create the database.

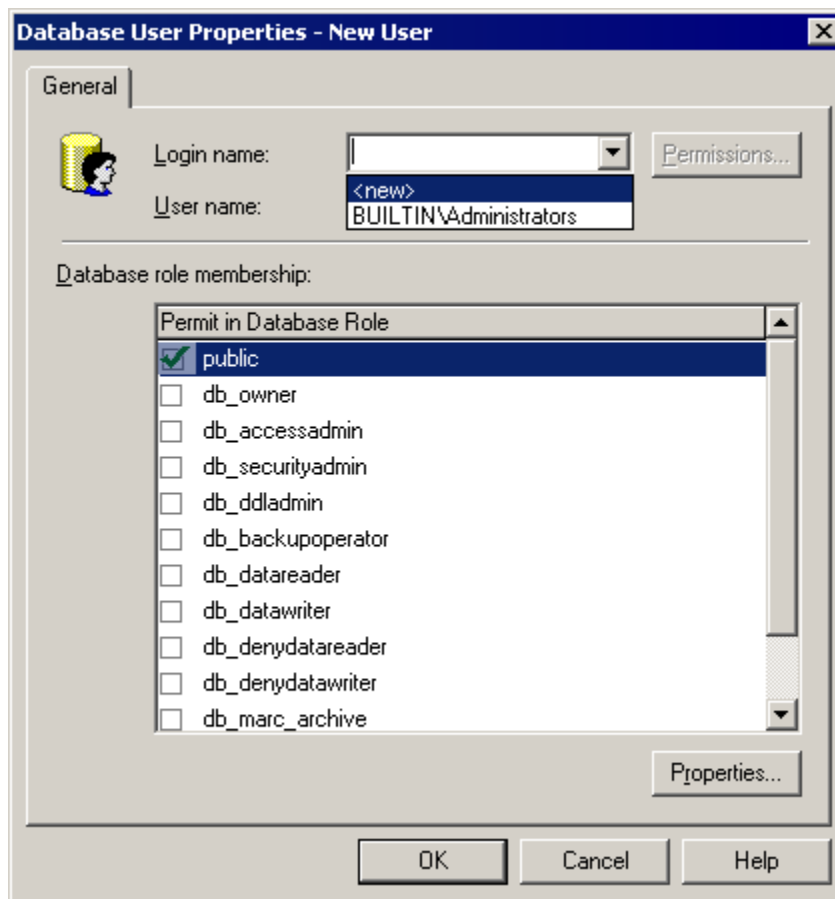


Screenshot 100 - Creating a new database

2. Right-Click the **Databases** node and then click **New Database**.

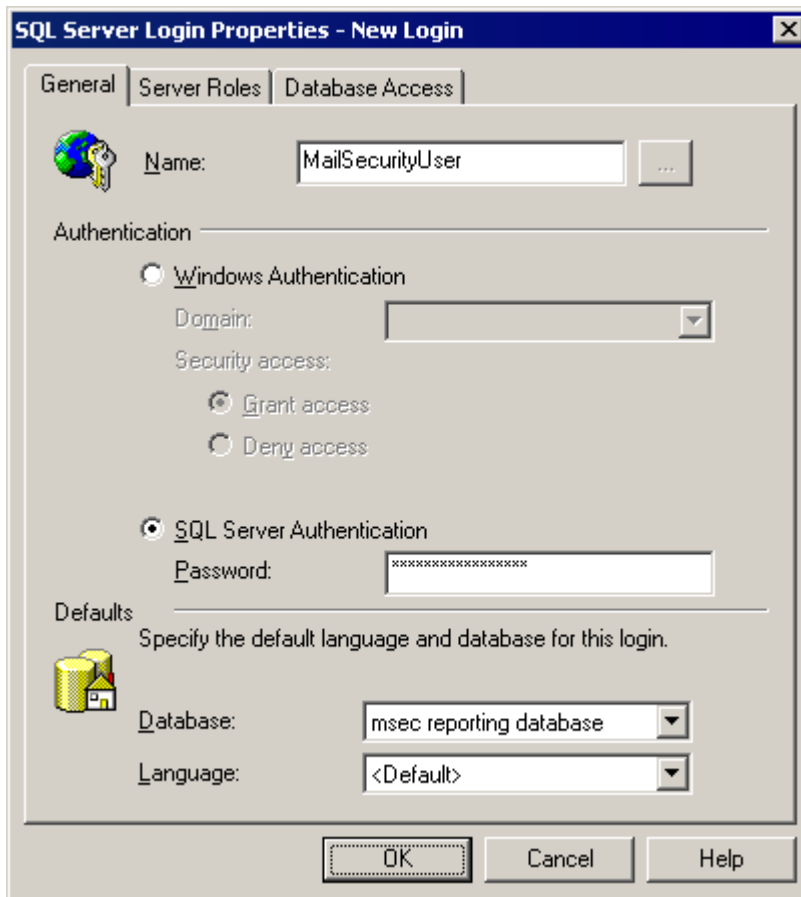
3. Type the database name in the dialog box, for example, 'MailSecurityReports', and then click **OK**.

4. Expand the newly created database node, right-click the **Users** sub-node and then click **New Database User**.



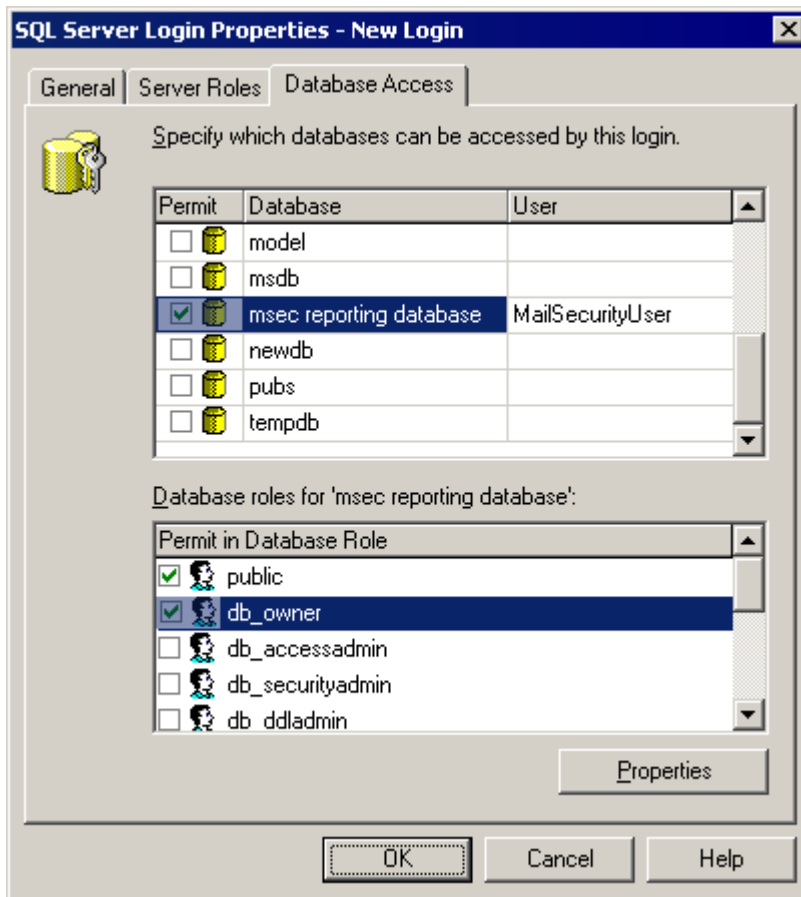
Screenshot 101 - Creating a login

5. From the **Login name** list, select **<new>**.



Screenshot 102 - Specifying authentication mode

6. In the **SQL Server Login Properties** dialog box, type the login name, for example, 'MailSecurityUser', in the **Name** box. Under the **Authentication** area, click **SQL Server Authentication** and then type a password in the **Password** box.
7. Select the database you have just created from the **Database** list.
8. Click the **Database Access** tab.
9. Select the check box near the Database you have just created.

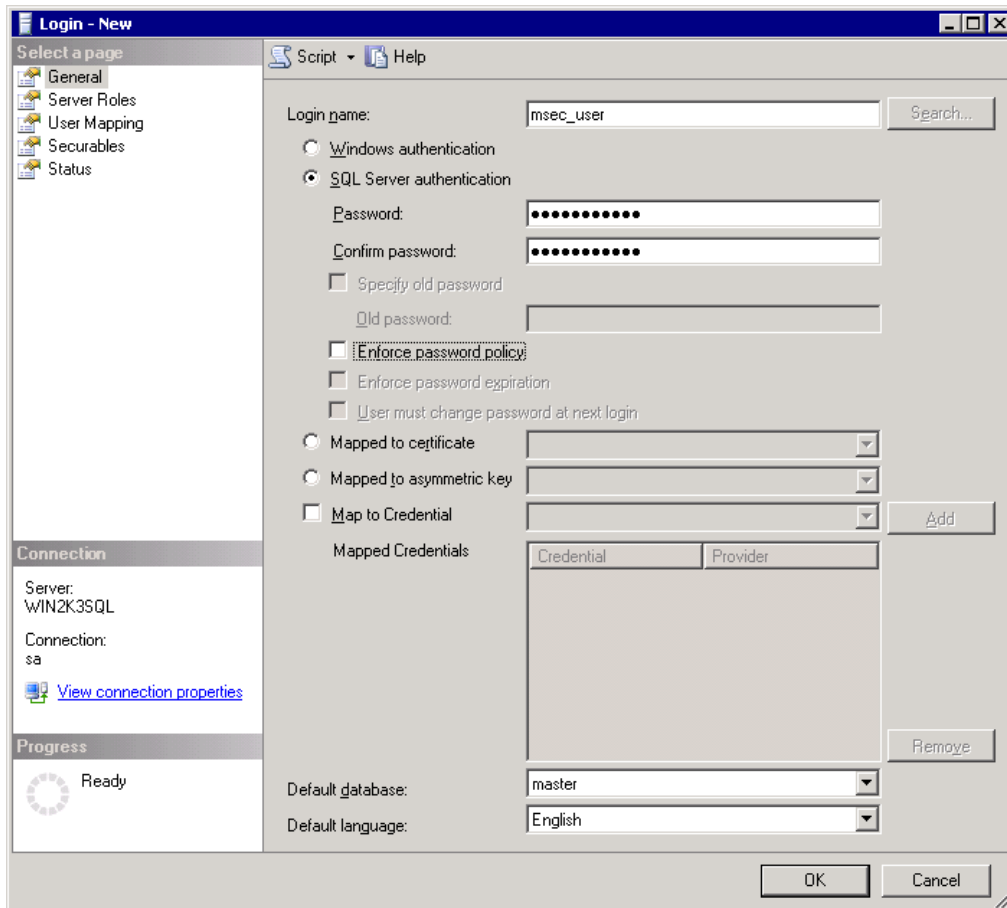


Screenshot 103 - Enabling the db_owner field

10. In the **Database roles for** list, select **db_owner**. Click **OK** to save your settings.

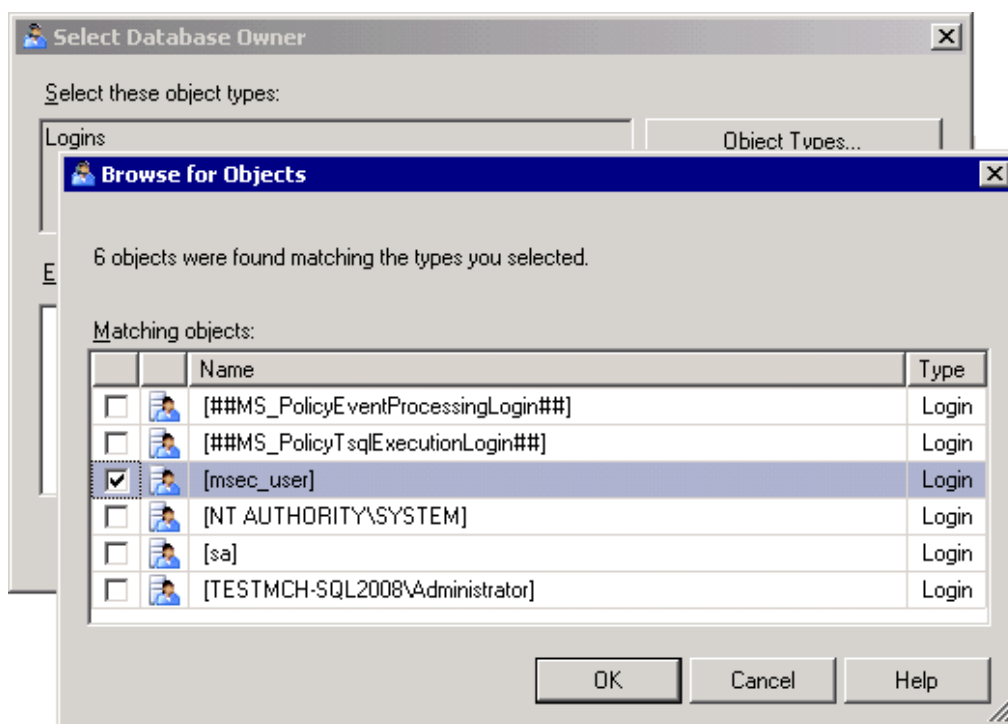
Creating a new database in Microsoft SQL Server 2008

1. On the SQL server machine, click **Start ► All Programs ► Microsoft SQL Server 2008 ► SQL Server Management Studio**.
2. Enter the database administrator credentials.
3. From the left panel expand **SQL Server node ► Security**.
4. Right-click **Logins** and select **New Login**.
5. Enter a valid user login name (example msec_user).
6. Select authentication type and click **OK** to apply changes.



Screenshot 104 - Create new SQL login

7. From the left panel right-click **Databases** folder and select **New Database**.
8. In the new database dialog, enter a valid name (example MSECDB).
9. Click the owner browse button to enter a login name and in the **Select Database Owner** dialog, click **Browse**.



Screenshot 105 - Browse for object dialog

10. Select the user created in step 5 and click **OK**.
11. Click **OK** to close the **Select Database Owner** dialog.
12. Click **OK** in the **New Database** dialog to apply changes.

14 Realtime Monitor

14.1 About the Realtime Monitor

Through the Realtime Monitor page, you can monitor the GFI MailSecurity email processing activity in a 'Live' environment. Therefore, you can use this option to check the status of each email and determine whether an email was successfully processed, not processed or quarantined.

GFI MailSecurity

Realtime Monitor

The Realtime Monitor shows all the scanning activity in chronological order.

GFI MailSecurity Statistics

Number of processed items	3
Number of quarantined items	0
Number of unprocessed emails in the last 24 hours	0

For more information on how to reprocess unprocessed emails [click here...](#)

GFI MailSecurity Activity Log

☒ Enable Auto-Refresh. Refresh time interval in seconds: 10 Refresh

Event

- 10/20/2009 6:15:57 PM - Item was processed ok
- 10/20/2009 6:15:56 PM - Item was processed ok
- 10/20/2009 6:15:55 PM - Recipients:
- 10/20/2009 6:15:55 PM - Subject: GFI ContentSecurity - New Norman Anti-Virus update files downloaded and installed.
- 10/20/2009 6:15:55 PM - Sender: Administrator@setup11.local
- 10/20/2009 6:15:55 PM - Processing new item
- 10/20/2009 6:15:55 PM - Recipients:
- 10/20/2009 6:15:55 PM - Subject: Your GFI MailSecurity evaluation will expire in 5 day(s)!
- 10/20/2009 6:15:55 PM - Sender: Administrator@setup11.local
- 10/20/2009 6:15:55 PM - Processing new item
- 10/20/2009 6:15:51 PM - Item was processed ok
- 10/20/2009 6:15:31 PM - Recipients:
- 10/20/2009 6:15:31 PM - Subject: GFI ContentSecurity - New Kaspersky Anti-Virus update files downloaded and installed.
- 10/20/2009 6:15:31 PM - Sender: Administrator@setup11.local
- 10/20/2009 6:15:31 PM - Processing new item

Screenshot 106 - Realtime Monitor page

14.2 Monitoring email activity

Click the **GFI MailSecurity ► Realtime Monitor** node to open the Realtime Monitor page. This page displays the GFI MailSecurity email statistics and event log.

The GFI MailSecurity Statistics area shows the:

- **Number of processed items** - number of emails which were successfully scanned by the product.
- **Number of quarantined items** - number of emails which were directed to quarantine.

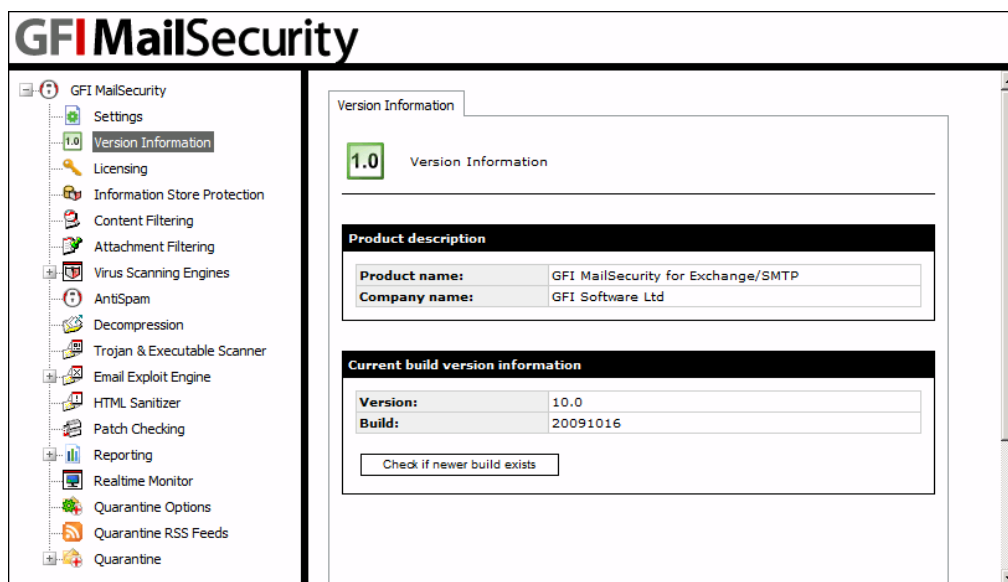
- **Number of unprocessed emails in the last 24 hours** - number of emails that are not processed by GFI MailSecurity and not delivered to the recipient. One reason this can happen is when the email is corrupted spam and therefore could not be processed successfully. A copy of these emails can be found at <..\GFI\Content Security\MailSecurity\FailedMails> folder.

NOTE: For more information about unprocessed emails refer to: <http://kbase.gfi.com/showarticle.asp?id=KBID003263>

- In the GFI MailSecurity Activity Log select the **Enable Auto-Refresh** check box and specify a time interval in seconds for automatic refresh of the Realtime Monitor. Alternatively, click on **Refresh** to refresh the activity manually.
- In the **Event** area, the page displays the date and time when GFI MailSecurity receives and scans an email, as well as the sender, recipient and subject of every email scanned.

15 Miscellaneous

15.1 Version Information



Screenshot 107 - Version Information page

To view the GFI MailSecurity version information, click the **GFI MailSecurity ► Version Information** node. The version information page displays the GFI MailSecurity version number currently installed and the build information. To check whether you have the latest build of GFI MailSecurity installed on your machine, click **Check if newer build exists**.

NOTE: Please, always quote your GFI product Version and Build information when requesting for GFI support.

16 Advanced topics

16.1 Customizing the notification templates

GFI MailSecurity sends notification emails to the administrator/user whenever an event that needs attention occurs.

There are two types of notifications:

- **Administrative notifications** - GFI MailSecurity sends these notifications, for example, when a license is going to expire, when a new patch is available, and when new anti-virus engine updates are available.
- **End user notifications** - GFI MailSecurity sends these notifications to the sender/recipient of an email when an email gets quarantined or modified.

The notification email message is generated from templates stored in sub-folders in the **ContentSecurity\MailSecurity\Templates** folder.

Each template sub-folder can contain an HTML body template (html.txt), a text body template (text.txt), and a subject template (subject.txt).

NOTE: The template folder names and template file names are predefined and therefore you cannot change them.

The templates contain the text of the notification message, as well as field names that are replaced by dynamic values upon generation of the notification message.

There are two types of template:

- **Tag-based templates** - These templates use tags (in the form "[TAGNAME]") to indicate fields which need to be replaced with dynamic data.
- **XSL-based templates** - These templates are an XSL style sheet, and are used in conjunction with dynamically created XML data to generate the notification message.

NOTE: Always take a backup of the template you are going to modify. In this way, you can always recover from the backup template if your modified template does not work as expected.

NOTE: Before modifying XSL-based templates, make sure you are proficient in XML and XSL. If you modify an XSL template and it is not well formed, for example, the notification services module will fail to send notification emails. To check whether an XSL based template is well formed, you can rename the template filename with an extension of ".xml" and load it in Microsoft Internet Explorer. If the template is well formed, the browser will load it correctly. If it contains errors, the browser will highlight the exact line where the problem is located.

Variables used in XSL-based notification templates

Notify user and notify manager notifications (in notifyuser folder and notifymanager folder respectively)

Node	Description
"itemsenderemailaddress"	The sender's email address.
"itemsubject"	The quarantined email subject.
"itemdeliverytime"	The date and time the message was delivered.
"itemrecipients/recipient"	The message recipients. Use xsl:for-each to enumerate.
"action"	Action taken on message by GFI MailSecurity.
"shortdate"	Date when email was processed. Short date format.
"longdate"	Date when email was processed. Long date format.
"time24"	Time when email was processed. 24 hour format.
"time12"	Time when email was processed.
"infringedrules/rule"	List of rules infringed. Use xsl:for-each to enumerate.
"itemmessageid"	The message ID of the email processed.
"itemscandirection"	0 - Inbound : 1 - Outbound : 4 - Mixed

The listing on the next page shows a typical notify manager XSL template, which will generate the following HTML output.

HTML Output

```
<HTML>
<BODY>
On 04 August 2005 an email was blocked which has violated the following
rules:<P></P>
<B>BitDefender Anti-Virus</B><BR/>
<P>
The following action(s) were taken: <B>Quarantined</B>
</P>
Additional information:
<P>
<table border="1">
<tr>
<td>Subject</td><td><B>Sample email subject</B></td>
</tr>
<tr>
<td>Sender</td><td><B>samplesender@sampldomain.com</B></td>
</tr>
<tr>
<td colspan="2" align="center">Recipients</td>
</tr>
<tr>
<td colspan="2"><B>samplerrecipient@localdomain.com</B></td>
</tr>
</table>
</P>
Regards,<BR/>
GFI ContentSecurity.
</BODY>
```

</HTML>

XSL Template

```
<?xml version="1.0"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
version="1.0">
<xsl:output method="html" omit-xml-declaration="yes" standalone="no"/>
<xsl:template match="/properties">
<HTML>
<BODY>
On <xsl:value-of select="longdate"/> an email was blocked which has violated
the following rules:<P/>
<xsl:for-each select="infringedrules/rule">
<B><xsl:value-of select="."/></B><BR/>
</xsl:for-each>
<P>
The following action(s) were taken: <B><xsl:value-of select="action"/></B>
</P>
Additional information:
<P>
<table border="1">
<tr>
<td>Subject</td>
<td><B><xsl:value-of select="itemssubject"/></B></td>
</tr>
<tr>
<td>Sender</td>
<td><B><xsl:value-of select="itemsenderemailaddress"/></B></td>
</tr>
<tr>
<td colspan="2" align="center">Recipients</td>
</tr>
<xsl:for-each select="itemrecipients/recipient">
<tr>
<td colspan="2"><B><xsl:value-of select="."/></B></td>
</tr>
</xsl:for-each>
</table>
</P>
Regards,<BR/>
GFI ContentSecurity.
</BODY>
</HTML>
</xsl:template>
</xsl:stylesheet>
```

16.2 Setting Virus Scanning API Performance Monitor Counters

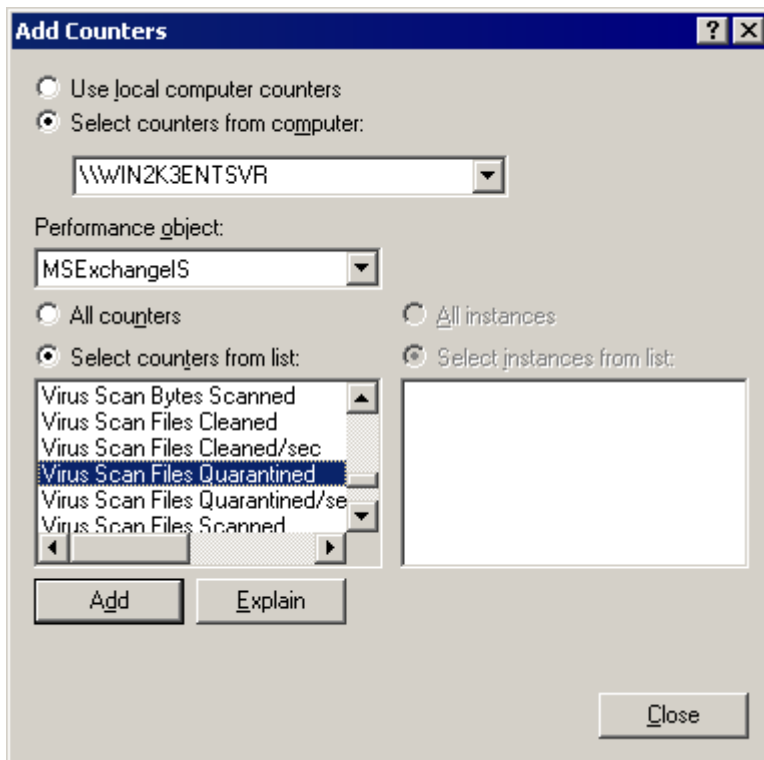
When you install GFI MailSecurity on the Microsoft Exchange machine directly, you can use the Performance Monitor MMC to keep an eye on Virus Scanning API performance through the performance monitor counters made available by Microsoft Exchange.

NOTE: The VSAPI performance monitor counters are only available on a Microsoft Exchange Server 2007/2010 machine with the Mailbox Server Role installed.

16.2.1 Performance counter in Windows 2003 Server

To add and view, the performance monitor counter in Windows 2003 Server, follow these steps:

1. Click on **Start ► Control Panel**.
2. In the **Control Panel** window, double-click **Administrative Tools**.
3. In the **Administrative Tools** window, double-click **Performance**, to start the Performance monitor MMC.
4. Press Ctrl+I to load the **Add Counters** dialog box.
5. From the **Performance object** list, select **MSExchangeIS**.
6. Click **Select counters from list**.
7. Select one of the **Virus Scan** counters as listed below.
8. Click **Add**.
9. Repeat step 7 and 8 to add all the performance counters you want.
10. Click **Close**.



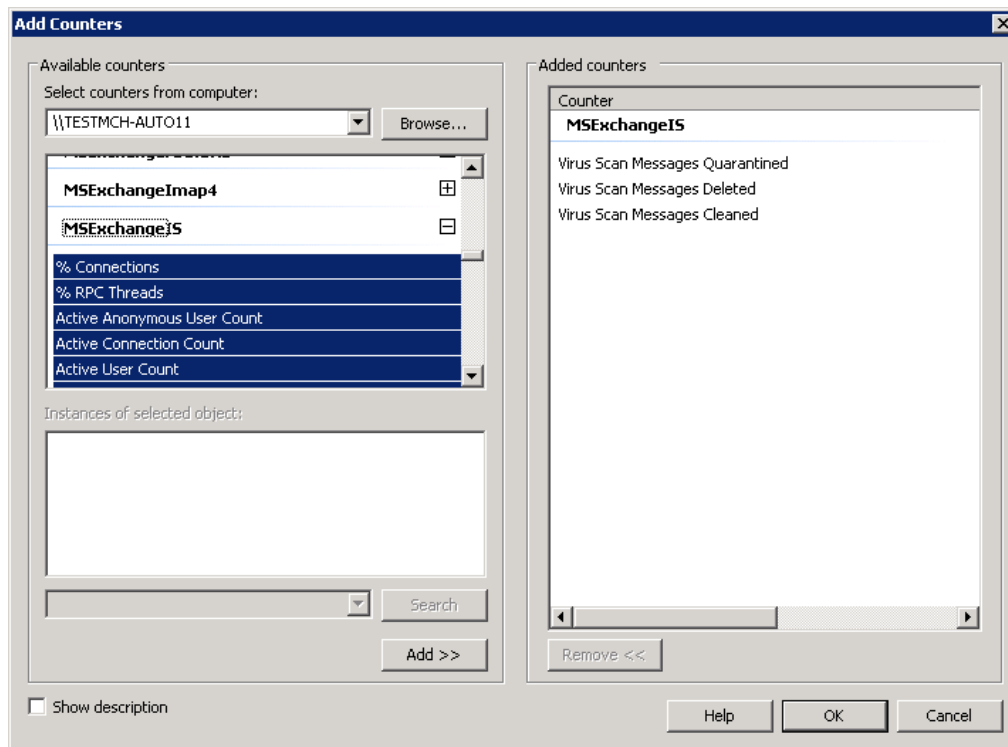
Screenshot 108 - Adding VSAPI performance monitor counters

The information provided below is also available from the following link:
<http://support.microsoft.com/kb/285696>

16.2.2 Performance counter in Windows 2008 Server

To add and view, the performance monitor counter in Windows 2008 Server, follow these steps:

1. Click on **Start ► Control Panel**.
2. In the **Control Panel** window, double-click **Administrative Tools**.
3. Double-click **Reliability and Performance Monitor**.
4. In the monitor dialog, expand **Monitoring Tools** and select **Performance Monitor**.
5. From the right panel click the **Add** button to add a new counter.
6. From the **Select counters from computer** drop down, select the computer to monitor.
7. From the list identify and expand **MSExchangeIS**.
8. Select the process to monitor and click **Add**.
9. Repeat step 8 for each process.



Screenshot 109 - Adding VSAPI performance monitor counters in Windows 2008 Server

10. Click **Ok** to apply changes.

16.2.3 Performance monitor counters

The following VSAPI Performance Monitor counters are available:

- **Virus Scan Messages Processed** - This is a cumulative value of the total number of top-level messages that are processed by the virus scanner.
- **Virus Scan Messages Processed/sec** - This counter represents the rate at which top-level messages are processed by the virus scanner.
- **Virus Scan Messages Cleaned** - The total number of top-level messages that are cleaned by the virus scanner.
- **Virus Scan Messages Cleaned/sec** - The rate at which top-level messages are cleaned by the virus scanner.
- **Virus Scan Messages Quarantined** - The total number of top-level messages that are put into quarantine by the virus scanner.
- **Virus Scan Messages Quarantined/sec** - The rate at which top-level messages are put into quarantine by the virus scanner.
- **Virus Scan Files Scanned** - The total number of separate files that are processed by the virus scanner.
- **Virus Scan Files Scanned/sec** - The rate at which separate files are processed by the virus scanner.

- **Virus Scan Files Cleaned** - The total number of separate files that are cleaned by the virus scanner.
- **Virus Scan Files Cleaned/sec** - The rate at which separate files are cleaned by the virus scanner.
- **Virus Scan Files Quarantined** - The total number of separate files that are put into quarantine by the virus scanner.
- **Virus Scan Files Quarantined/sec** - The rate at which separate files are put into quarantine by the virus scanner.
- **Virus Scan Bytes Scanned** - The total number of bytes in all of the files that are processed by the virus scanner.
- **Virus Scan Queue Length** - The current number of outstanding requests that are queued for virus scanning.
- **Virus Scan Folders Scanned in Background** - The total number of folders that are processed by background scanning.
- **Virus Scan Messages Scanned in Background** - The total number of messages that are processed by background scanning.

17 Troubleshooting

17.1 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

17.2 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/>.

17.3 Web Forum

User to user technical support is available via the web forum. The forum can be found at: <http://forums.gfi.com/>.

17.4 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.

17.5 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>.

18 Index

- Active Directory, 5, 6, 9, 10, 20, 21, 29, 36, 38, 44, 77, 78, 123, 125
- Active/Passive cluster, 8, 9
- anti-virus, 1, 11, 47, 48, 50, 51, 52, 53, 54, 58, 83, 84, 85, 89, 95, 141
- ASP.Net, 11
- AVG, 1, 47, 48, 49, 50
- Bayesian, 3
- BitDefender, 1, 47, 48, 50, 51, 52, 53, 54, 142
- Database**, 127, 129, 130, 132, 133
- Decompression engine, 81
- decompression filter, 2, 86
- DEP, 27, 28
- DMZ, 7, 10, 21, 125
- DNS, 16, 18, 22
- Domain, 16
- DoS, 83, 84
- Edge Server, 5
- email, 1, 2, 3, 5, 6, 7, 9, 10, 14, 15, 16, 17, 18, 19, 20, 21, 22, 41, 43, 45, 55, 56, 58, 61, 68, 69, 73, 74, 76, 77, 78, 81, 82, 83, 86, 87, 91, 95, 96, 97, 98, 101, 104, 105, 107, 108, 109, 112, 113, 114, 115, 116, 117, 118, 119, 122, 123, 125, 137, 138, 141, 142, 143
- Email, 1
- Exploit Engine, 95, 96, 97, 98, 99
- firewall, 1, 7, 9, 21, 125
- gateway, 1, 5, 6, 12
- Harvesting, 122, 123, 124, 125
- HTML Sanitizer, 2, 101
- Hub Transport, 2, 5, 23, 47, 49, 51, 52, 59, 108
- ICSA, 47
- IIS, 8, 9, 10, 11, 12, 13, 14, 16, 19, 22, 28, 29, 30, 33, 36, 37, 43, 44
- Internet, 6, 7, 9, 10, 11, 12, 13, 16, 17, 18, 29, 31, 32, 35, 37, 141
- IP, 8, 9, 12, 13, 14, 16, 17, 18, 42, 125, 129
- ISP, 18
- Kaspersky, 1, 27, 28, 47, 48, 50, 51
- Lotus Notes, 6, 10, 18
- Mailbox, 2, 5, 47, 49, 51, 52, 59, 144
- McAfee, 1, 47, 52, 53
- Microsoft Exchange, 2, 5, 7, 9, 10, 11, 12, 16, 17, 22, 23, 24, 25, 27, 43, 47, 48, 49, 51, 52, 59, 108, 109, 144
- MIME, 101
- MSMQ, 10, 37
- Net framework, 10, 37
- Norman, 1, 47, 48, 50, 53, 54
- Performance, 28, 144, 146
- POP3, 4, 6, 10, 18
- Post-Installation, 22, 23, 27
- proxy, 41, 42
- Quarantine, 28, 29, 30, 32, 34, 39, 40, 55, 68, 76, 82, 83, 84, 85, 97, 105, 106, 107, 108, 112, 113, 114, 115, 117, 118, 120, 121, 123
- RSS Feeds, 2, 21, 32, 33, 34, 119, 120, 121, 122
- Service Pack, 9, 10, 11, 27
- SMTP, 5, 6, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 36, 37, 38, 41, 43, 44, 47, 49, 50, 52, 77, 78, 108, 125
- SMTP relay, 12
- SQL, 129, 130, 132, 133
- Switch Board, 35
- trojan, 2
- Trojan, 2, 41, 89, 90, 91, 92, 93
- Virtual directory**, 30, 34
- virus, 1, 2, 47, 52, 58, 89, 101, 123
- Web content zone**, 31
- Windows NT, 6
- Windows XP, 10, 11, 27
- Wizard, 14, 23, 27
- XSL, 141, 142, 143