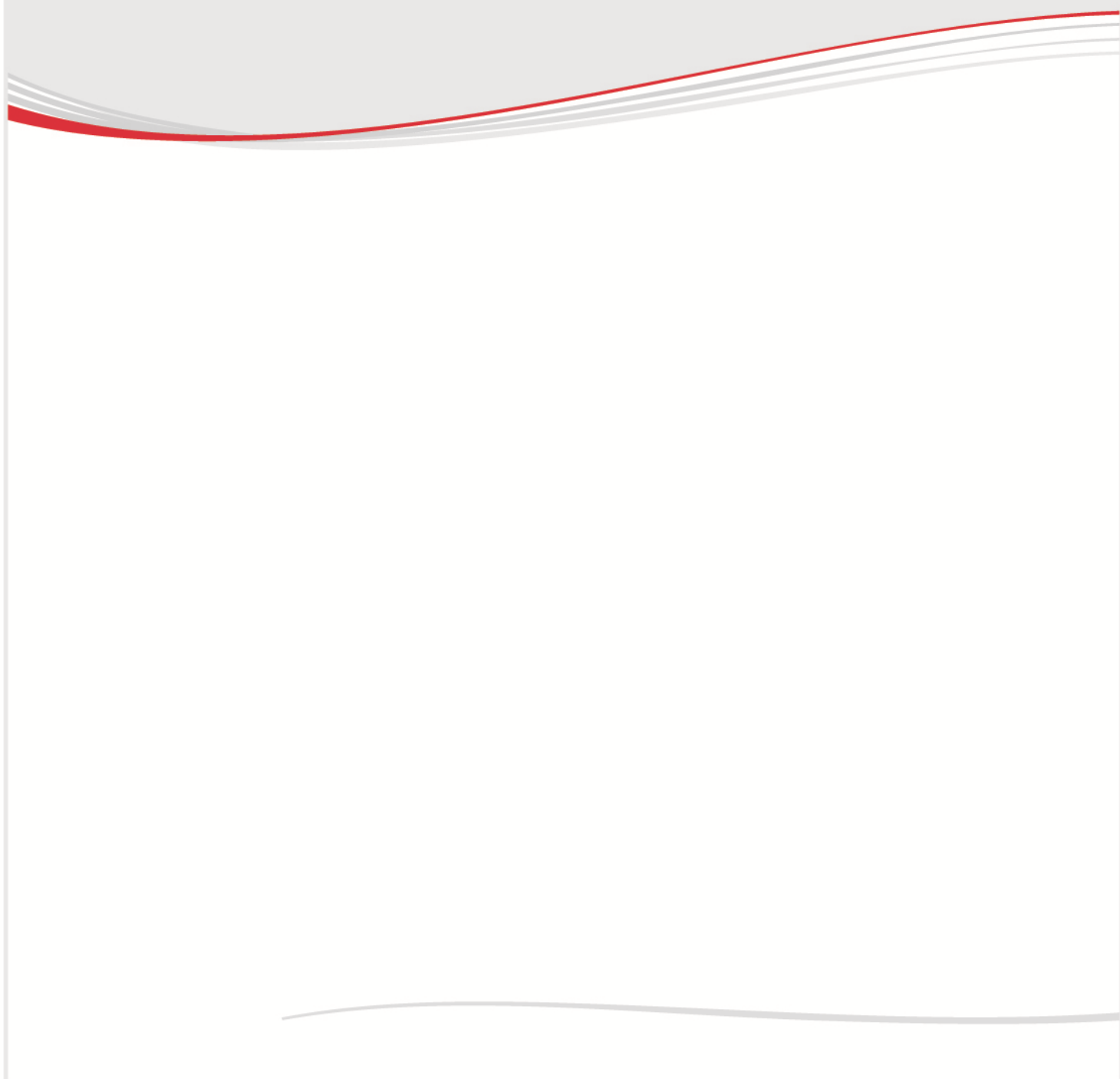


**"Highest Performance
Lowest Price"**

Microsoft
GOLD CERTIFIED
Partner



**GFI MailSecurity 2011 for
Exchange/SMTP
Getting Started Guide**





<http://www.gfi.com>

info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI MailSecurity is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Document Version: MSEC-GSG-EN-1.01.001

Last updated: April 11, 2011

Contents

1	Introduction	1
1.1	Introduction to GFI MailSecurity.....	1
1.2	Using this manual	1
1.3	Terms and conventions used in this manual.....	2
2	About GFI MailSecurity	3
2.1	GFI MailSecurity components.....	3
2.2	How GFI MailSecurity works.....	4
2.3	Licensing.....	6
3	Typical deployment scenarios	7
3.2	Which installation mode should I use?.....	9
4	System requirements	11
4.1	Hardware requirements	11
4.2	Software requirements.....	11
5	Pre-install actions	13
5.1	Installing on your mail server	13
5.2	Installing on an IIS mail relay server	13
6	New installations	21
6.1	GFI MailSecurity Post-Installation Wizard.....	24
7	Upgrade from earlier versions	27
7.1	Upgrading from GFI MailSecurity 8 or earlier.....	27
7.2	Upgrading from GFI MailSecurity 9 or later.....	28
7.3	Upgrading the Quarantine.....	29
8	Post-install actions	31
8.1	Add GFI MailSecurity to the Windows DEP Exception List.....	31
8.2	Securing access to the GFI MailSecurity configuration/quarantine.....	31
8.3	Securing access to the GFI MailSecurity Quarantine RSS feeds	35
8.4	Configuring virtual directory names	36
9	Accessing the GFI MailSecurity Configuration and Quarantine Store	37

9.1	Accessing the configuration from the GFI MailSecurity machine	38
9.2	Accessing the configuration from a remote machine	39
10	Testing your GFI MailSecurity system.....	41
10.1	Introduction	41
10.2	Step 1: Create a Content Filtering rule.....	41
10.3	Step 2: Send an inbound test email	41
10.4	Step 3: Send an outbound test email	41
10.5	Step 3: Confirm that test emails were blocked.....	41
11	Uninstalling GFI MailSecurity	43
11.1	Introduction	43
11.2	Uninstall GFI MailSecurity.....	43
11.3	Uninstalling GFI MailSecurity from an Active/Passive Cluster	43
12	Troubleshooting	45
12.1	Introduction	45
12.2	Knowledge Base	45
12.3	Web Forum	45
12.4	Common issues	45
12.5	Request technical support	46
12.6	Build notifications	46
13	Appendix - Installing on a Microsoft Exchange 2003 cluster	47
14	Glossary	49
	Index	51

1 Introduction

1.1 Introduction to GFI MailSecurity

Email is frequently used as a means for distributing harmful content (for example, through email attachments). GFI MailSecurity acts as an email firewall to protect an email system against malicious email attacks. The software uses various methods to block malicious emails, such as multiple virus scanning engines and link scanning technology. Using the GFI MailSecurity web-based interface, you can easily configure and optimize the software for your requirements. Blocked emails can then be reviewed and the appropriate action taken accordingly.

1.2 Using this manual

The aim of this 'Getting Started Guide' is to help you install and run GFI MailSecurity on your network with minimum configuration effort. It describes:

1. The various environments and email infrastructures supported by this product.
2. How to install the software.
3. How to run the product using default settings.

1.2.1 Administration and Configuration Manual

Detailed administration and configuration guidelines are provided in a separate manual called **GFI MailSecurity Administration and Configuration Manual**. This is installed with the product or downloadable separately from the GFI web site:

<http://www.gfi.com/mailsecurity/manual/>

This Administration and Configuration manual complements this Getting Started Guide by providing more detailed information on how to use and customize the features provided in GFI MailSecurity.

1.2.2 Manual structure

This manual contains the following chapters:

Chapter 1	Introduction Introduces this manual.
Chapter 2	About GFI MailSecurity Provides basic information about GFI MailSecurity.
Chapter 3	Typical deployment scenarios Describes the various environments how GFI MailSecurity can be installed.
Chapter 4	System requirements Defines system specifications required to install GFI MailSecurity.

Chapter 5	Pre-install actions Describes the actions that need to be taken before installing GFI MailSecurity in various environments.
Chapter 6	New installations Provides information on how to install GFI MailSecurity.
Chapter 7	Upgrade from earlier versions Describes how to upgrade older versions of GFI MailSecurity to the latest version.
Chapter 8	Post-install actions Defines the actions that need to be taken after installing GFI MailSecurity.
Chapter 9	Accessing the GFI MailSecurity Configuration and Quarantine Store Provides information on how to access the GFI MailSecurity interface.
Chapter 10	Testing your GFI MailSecurity system Describes how to test your GFI MailSecurity installation.
Chapter 11	Uninstalling GFI MailSecurity Provides information on how to uninstall GFI MailSecurity.
Chapter 12	Troubleshooting Contains information on how to deal with any problems encountered while using GFI MailSecurity. Also provides extensive support information.
Chapter 13	Appendix - Installing on a Microsoft Exchange 2003 cluster Describes how to install GFI MailSecurity in a Microsoft Exchange 2003 Active/Passive cluster.
Chapter 14	Glossary Defines technical terms used within GFI MailSecurity.

1.3 Terms and conventions used in this manual

The following terms and conventions are used in the documentation of this manual:

NOTE: Additional information and references essential for correct operation.



Important notifications and cautions regarding potential issues that are commonly encountered.



Step by step navigational instructions to access a specific task.

Bold Names of items to select such as nodes, menu options or command buttons.

<Italics> Parameters and values that you must replace with the applicable value, such as custom paths and filenames.

For any technical terms and their definitions as used in this manual, refer to the [Glossary](#) chapter.

2 About GFI MailSecurity

2.1 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 server, it will also scan the Microsoft Exchange information store. If you install GFI MailSecurity on a Microsoft Exchange Server 2007/2010 machine with Hub Transport and Mailbox Server Roles, 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 configured.

GFI MailSecurity web interface

Through the GFI MailSecurity web interface, you can:

- Monitor email scanning activity
- Manage scanning and filtering engines
- Configure GFI MailSecurity settings
- Review quarantined emails

GFI MailSecurity Switchboard

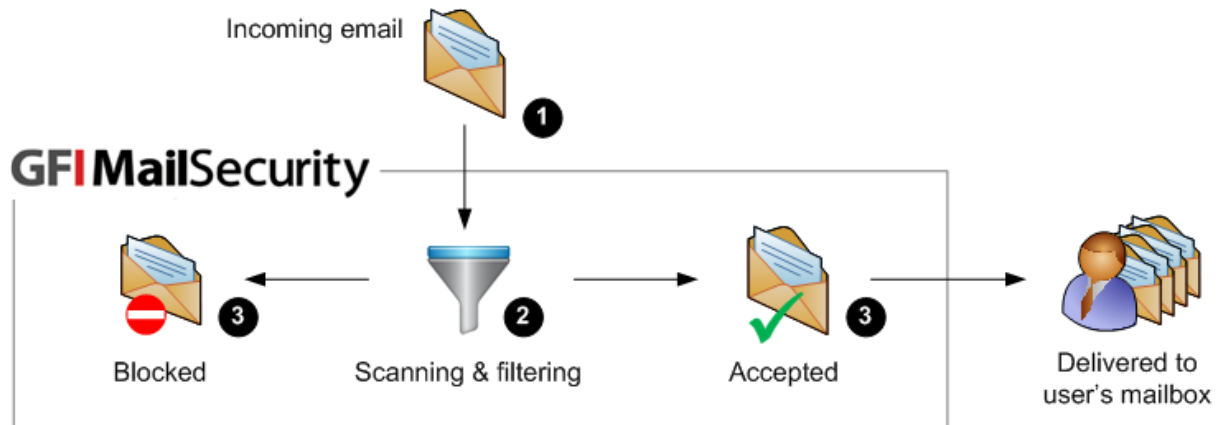
Use the GFI MailSecurity Switchboard to configure:

- How to launch GFI MailSecurity
- Website and Virtual Directory names for the web interface and quarantine
- Tracing options to create log files for debugging purposes.

2.2 How GFI MailSecurity works

This section provides a high-level overview on how GFI MailSecurity works.

2.2.1 Incoming email



Screenshot 1 -Incoming email

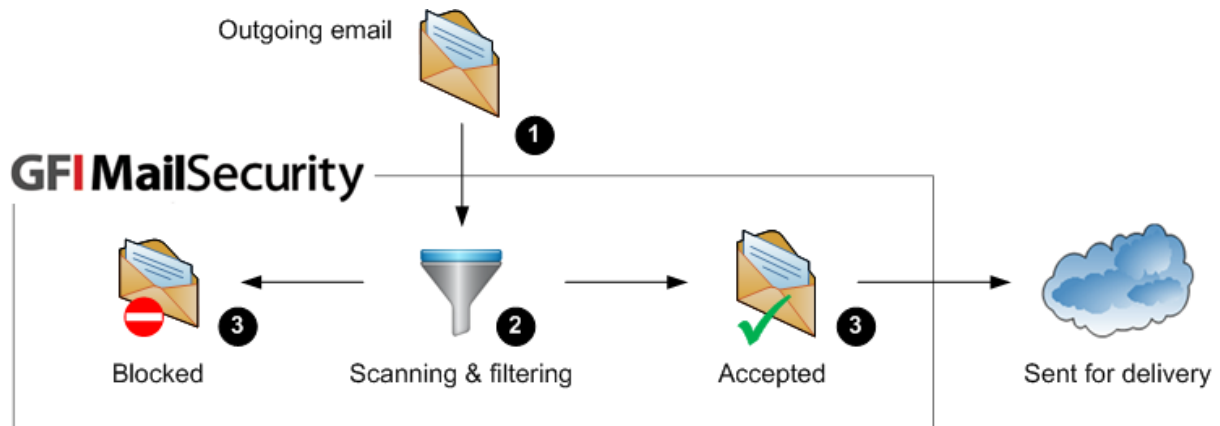
- 1 Incoming email is relayed to the GFI MailSecurity machine.
- 2 Email is scanned by GFI MailSecurity using the email scanning engines and filters configured to scan inbound emails.

EMAIL SCANNING ENGINE	DESCRIPTION
Virus Scanning Engines	Scan emails for viruses and malicious code. Some engines also include other features, such as macro checking, link scanning and Sandbox technology.
Content and attachment filtering	Block emails that match any rules containing pre-configured conditions within the email body or attachments.
Decompression engine	Analyzes compressed attachments for potentially malicious content.
Trojan & executable scanner	Analyzes the function of executable files for malicious code.
Email exploit engine	Checks if attachments contain any exploits.
HTML Sanitizer	Scans and removes html code with email body and attachments.

- 3 GFI MailSecurity applies the appropriate action depending on the scan results.

SCAN RESULT	ACTION
Accepted	If the email is safe, delivery to the user's mailbox is allowed.
Blocked	When a compromised email is detected, the appropriate action is taken by GFI MailSecurity depending on which action is configured (for example, the email is quarantined).

2.2.2 Outgoing email



Screenshot 2 -Outgoing email

- 1 Outgoing email is relayed to the GFI MailSecurity machine.
- 2 Email is scanned by GFI MailSecurity using the email scanning engines and filters configured to scan outbound emails.

EMAIL SCANNING ENGINE	DESCRIPTION
Virus Scanning Engines	Scan emails for viruses and malicious code. Some engines also include other features, such as macro checking, link scanning and Sandbox technology.
Content and attachment filtering	Block emails that match any rules containing pre-configured conditions within the email body or attachments.
Trojan & executable scanner	Analyzes the function of executable files for malicious code.
Email exploit engine	Checks if attachments contain any exploits.
HTML Sanitizer	Scans and removes html code with email body and attachments.

- 3 GFI MailSecurity applies the appropriate action depending on the scan results.

SCAN RESULT	ACTION
Accepted	If the email is safe, delivery to the user's mailbox is allowed.
Blocked	When a compromised email is detected, the appropriate action is taken by GFI MailSecurity depending on which action is configured (for example, the email is quarantined).

2.2.3 Other features

Apart from scanning incoming and outgoing emails, GFI MailSecurity also includes the features listed below.

FEATURE	DESCRIPTION
Internal emails scanning	Attachment Filtering and Content Filtering can be configured to scan internal emails when GFI MailSecurity is installed on the Microsoft Exchange server.

Information Store Protection	Scans the Microsoft Exchange information store using the Virus Scanning Engines.
Directory Harvesting	Deletes emails addressed to nonexistent users from the Quarantine Store.
Quarantine Store	A central repository within GFI MailSecurity where all blocked emails are retained until review.

2.3 Licensing

For information on licensing, refer to:

<http://www.gfi.com/products/gfi-mailsecurity/pricing/licensing>.

3 Typical deployment scenarios

This chapter explains the different scenarios how GFI MailSecurity can be installed and configured. You can install GFI MailSecurity:

- directly on your mail server, or
- on a separate machine configured as a mail relay/gateway server.

3.1.1 Installing GFI MailSecurity on your mail server

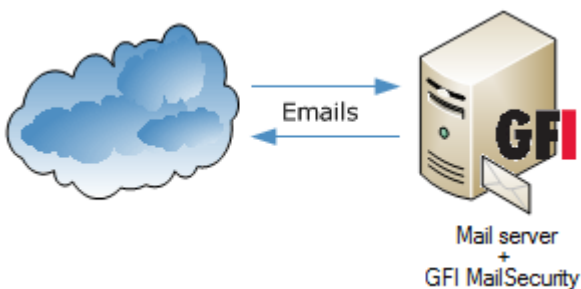


Figure 1 - Installing GFI MailSecurity on your mail server

You can install GFI MailSecurity directly on your mail server, without any additional configuration.

NOTE: In Microsoft Exchange 2007/2010 environments, GFI MailSecurity can only be installed on the servers with the following roles:

- Edge Server Role, or
- Hub Transport Role, or
- Hub Transport and Mailbox Roles - with this configuration GFI MailSecurity can also scan internal emails for viruses.

3.1.2 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 (that is, on a server that is not the 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 emails. This means that all inbound email must pass through this machine for scanning before being relayed to the mail server for distribution. The same applies for outbound emails, where the mail server must relay all outgoing emails to the gateway machine for scanning before they are conveyed to the external recipients via Internet.

3.1.3 Installing GFI MailSecurity in front of your firewall

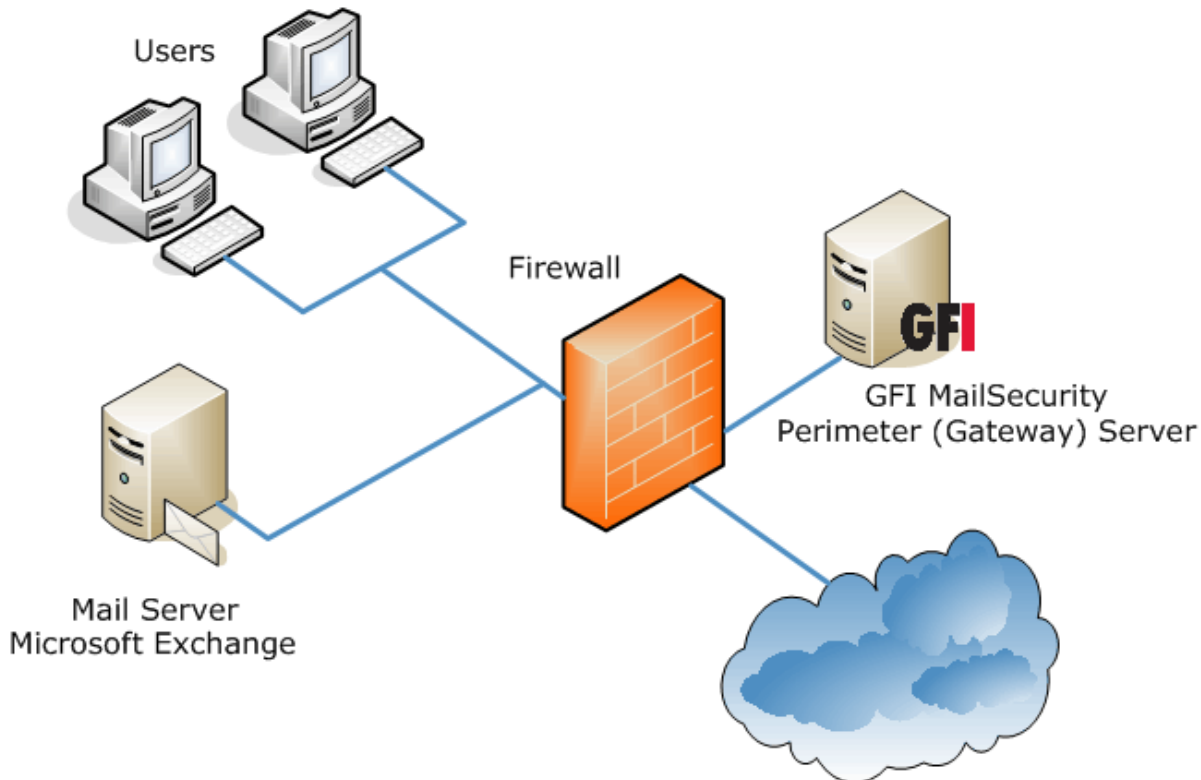


Figure 3 - Installing GFI MailSecurity on a separate machine on a DMZ

Recommendation: If utilizing a firewall, 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 since emails are 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 machine or on machines running other applications such as GFI MailEssentials.

3.2 Which installation mode should I use?

A core requirement of GFI MailSecurity is a list of the local mailboxes to protect. GFI MailSecurity can access the list of email users using two modes chosen during the installation:

- Active Directory mode
- SMTP mode

NOTE: Both 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.



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

3.2.1 Active Directory mode

To use this mode, the machine running GFI MailSecurity must be behind your firewall and must have access to the Active Directory containing ALL your email users (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.

3.2.2 SMTP mode

Use this mode when the machine running GFI MailSecurity 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 and machines in a DMZ.

4 System requirements

4.1 Hardware requirements

The minimum hardware requirements for GFI MailSecurity are:

- 2GHz processor
- 512MB RAM
- 1.5GB of physical disk space (installation only)

4.2 Software requirements

4.2.1 Supported Operating Systems

- Windows Server 2008 Standard or Enterprise (x86 or x64) (including R2 edition)
- Windows Server 2003 Standard or Enterprise (x86 or x64)
- Windows XP professional
- Windows Small Business Server 2003 / 2008

4.2.2 Supported Mail Servers

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

4.2.3 Other required components

- Internet Information Services (IIS) SMTP and World Wide Web services
- Microsoft .NET framework 2.0
- MSMQ - Microsoft Messaging Queuing Service - for more information how to install MSMQ, refer to:

<http://msdn.microsoft.com/en-us/library/aa967729.aspx>

- Microsoft Data Access Components (MDAC) 2.8 - this is included by default on Windows Server 2003 or later. This can be downloaded from:

<http://www.microsoft.com/Downloads/details.aspx?familyid=6C050FE3-C795-4B7D-B037-185D0506396C&displaylang=en>

4.2.4 Important notes

Windows XP

Since the version of Internet Information Services (IIS) in Windows XP limits only up to 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 server roles and services must be enabled:

- 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>

Windows Small Business Server 2003

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

Microsoft Exchange Server 2007/2010

In a Microsoft Exchange Server 2007/2010 environment, install GFI MailSecurity on a machine with one of the following roles:

- Edge Server Role, or
- Hub Transport Role, or
- Hub Transport and Mailbox Roles - with this configuration GFI MailSecurity can also scan internal emails for viruses.

NOTE: IIS SMTP service is not required, since Microsoft Exchange 2007/2010 have an inbuilt SMTP server.

4.2.5 Other installation notes

1. Disable anti-virus software from scanning the GFI MailSecurity directories. Anti-virus products might 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, refer to:

<http://kbase.gfi.com/showarticle.asp?id=KBID003316>.

2. GFI MailSecurity directories should not be backed up using backup software since this effects operation of the software.

5 Pre-install actions

5.1 Installing 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 [New installations](#) chapter.

5.2 Installing 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 to configure your mail relay to install GFI MailSecurity.

5.2.1 Step 1: Install the IIS SMTP service

If the IIS SMTP service is not installed, ensure to install it on the mail relay server, as described in the following sub-sections.

Windows Server 2003

1. Navigate to **Start ► Control Panel ► Add or Remove Programs ► Add/Remove Windows Components**.
2. Select **Internet Information Services (IIS)** and click **Details**.
3. Select the **SMTP Service** option and click **OK**.
4. Click **Next** to finalize your configuration.

Windows Server 2008

Enabling IIS SMTP service

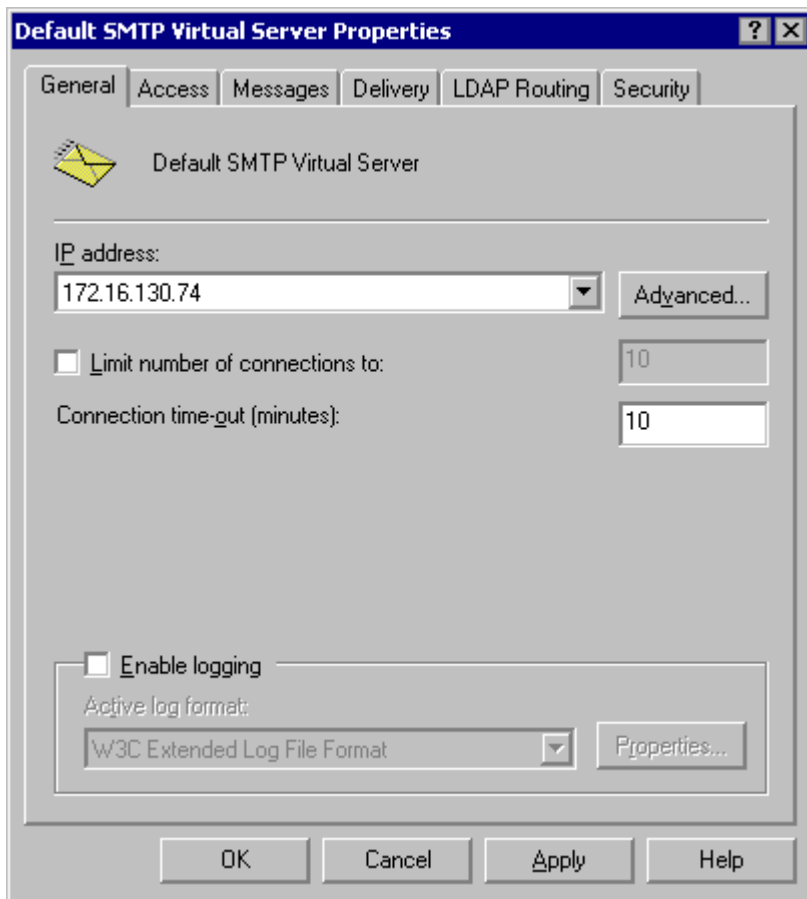
1. Launch the Windows Server Manager.
2. Navigate to the **Features** node and select **Add Features**.
3. From the **Add Features Wizard** select **SMTP Server** checkbox.

NOTE: The SMTP Server feature might require the installation of additional role services and features. Click **Add Required Role Services** to proceed with installation.

4. In the following screens click **Next** to configure any required role services and features, and click **Install** to start the installation.
5. Click **Close** to finalize the configuration.

5.2.2 Step 2: Specify mail relay server name and IP address

1. From **Control Panel**, open **Administrative Tools** and launch **Internet Information Services**.
2. Expand the server name node, right-click the **Default SMTP Virtual Server** node and click **Properties**.



Screenshot 3 - Assign an IP address to the mail relay server

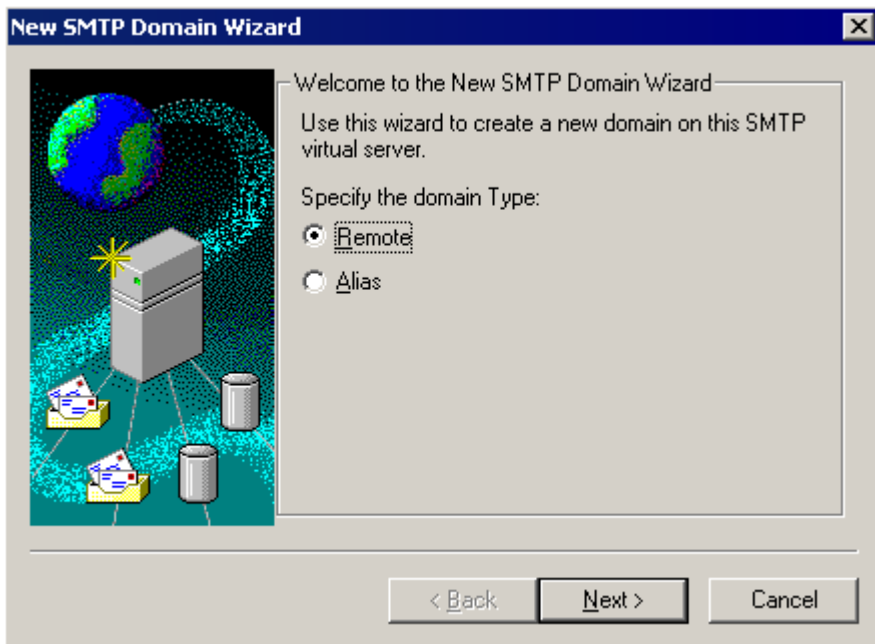
3. Key in the IP address of the SMTP relay server in the **IP address** list and click **OK**.

5.2.3 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. From **Control Panel** open **Administrative Tools** and launch **Internet Information Services**.
2. Expand the server name node and navigate to **Default SMTP Virtual Server ► 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 click **New ► Domain**.



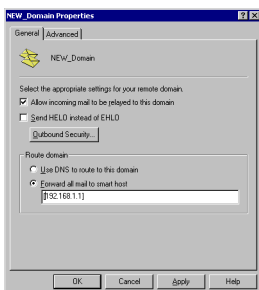
Screenshot 4 - SMTP Domain Wizard - Selecting domain type

- 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 Local Domains using the GFI MailSecurity configuration. For more information, refer to the 'Adding Local Domains' section in the GFI MailSecurity Administration & Configuration manual.

5.2.4 Step 4: 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.



Screenshot 5 - Configure the new domain

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]

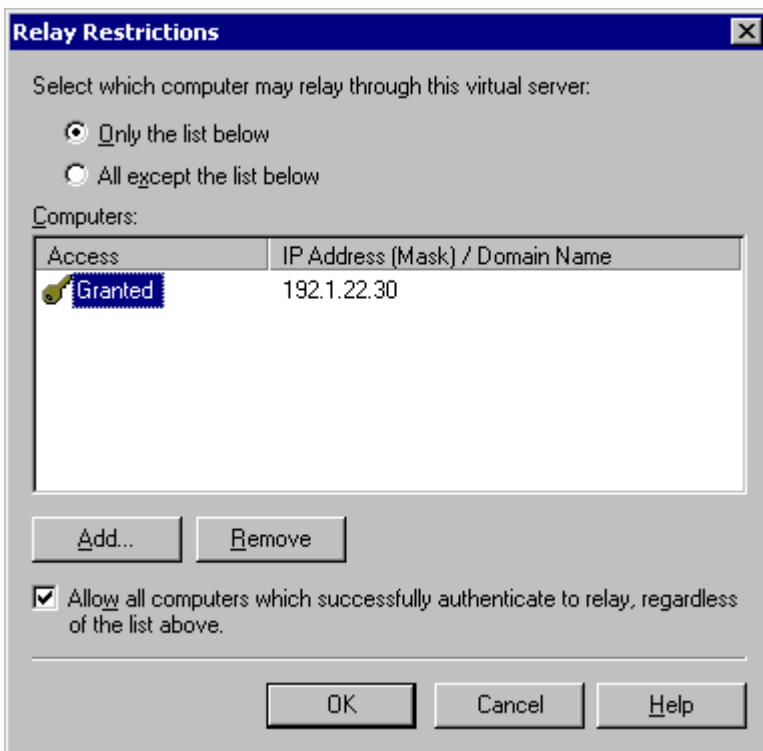
NOTE: The square brackets are used to differentiate an IP address from a hostname (which does not require square brackets).

3. Click **OK**.

5.2.5 Step 5: Secure your mail relay server

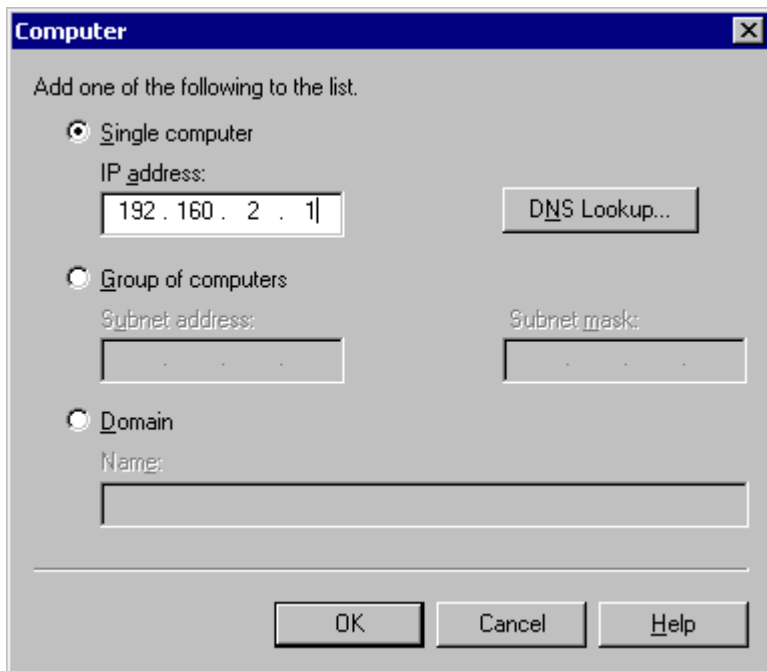
In this step, you will set up your SMTP virtual server's mail Relay Restrictions. This means that you must specify which machines may relay email through this virtual server (effectively limiting the servers that can send email via this server).

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 6 - Relay Restrictions dialog

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



Screenshot 7 - 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. 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. 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.

Click **OK** to add entry to the list.

5.2.6 Step 6: 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:

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 8 - 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.

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.

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.

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 similar to **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.

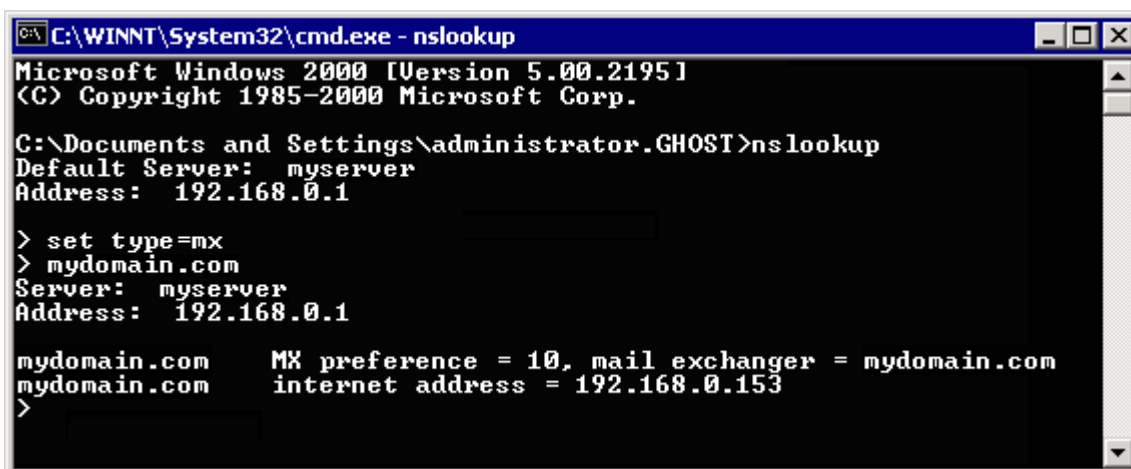
5.2.7 Step 7: Modify the MX record of your domain to point to the mail relay server

NOTE: If your ISP manages the DNS server, ask 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 hit **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: myserver
Address: 192.168.0.1

> set type=mx
> mydomain.com
Server: myserver
Address: 192.168.0.1

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

Screenshot 9 - Checking the MX record of your domain

5.2.8 Step 8: 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. Verify that the email client receives the email.
2. Test the IIS SMTP outbound connection of your mail relay server by sending an email to an external account from an internal email client. Verify that the external user receives 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:

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

6 New installations

Before you install GFI MailSecurity, check the points below:

1. Make sure that you are logged on 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 software and hardware requirements specified earlier in this chapter.

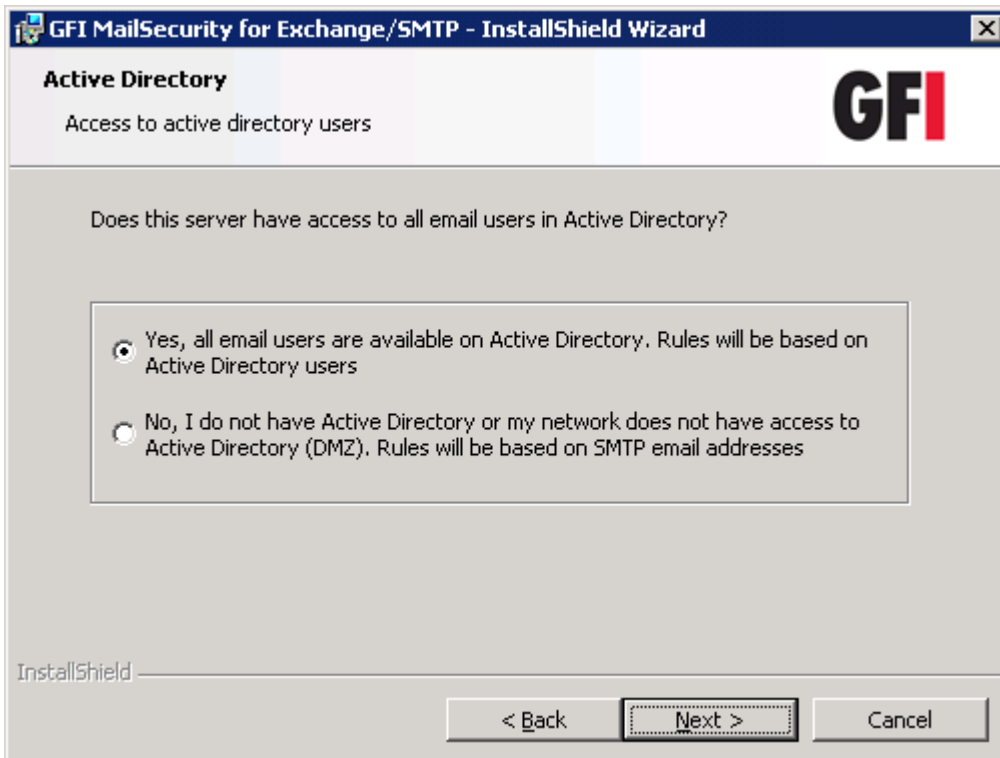
To install GFI MailSecurity follow these steps:

1. Run the GFI MailSecurity setup program by double-clicking on the **MailSecurity2011.exe** file.
2. Click **Next** in the **Welcome** page.
3. Select whether to check for newer versions/builds of GFI MailSecurity and click **Next**.
4. 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.
5. When upgrading from a previous version than GFI MailSecurity 10.1 SR8, you will be asked to upgrade the Quarantine database from Microsoft Access to a Firebird database. Select **Import** to automatically launch the Quarantine upgrade tool after the installation is complete. For more information how to use the quarantine upgrade tool, refer to [Upgrading the Quarantine](#) section in this manual.



If you select not to import the quarantine database, any quarantined emails will not be imported in the new installation.

6. Key in the administrator's email address in the **Administrator Email** text box. Enter the license key in the **License Key** text box or use the default license key for evaluation purposes. Click **Next** to continue the installation.



Screenshot 10 - Define if the server has access to all email users in the Active Directory

7. 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

Active Directory mode

GFI MailSecurity will retrieve the list of users from Active Directory. Selecting this option means that GFI MailSecurity is being installed behind your firewall and that it has access to the Active Directory containing ALL your email users.

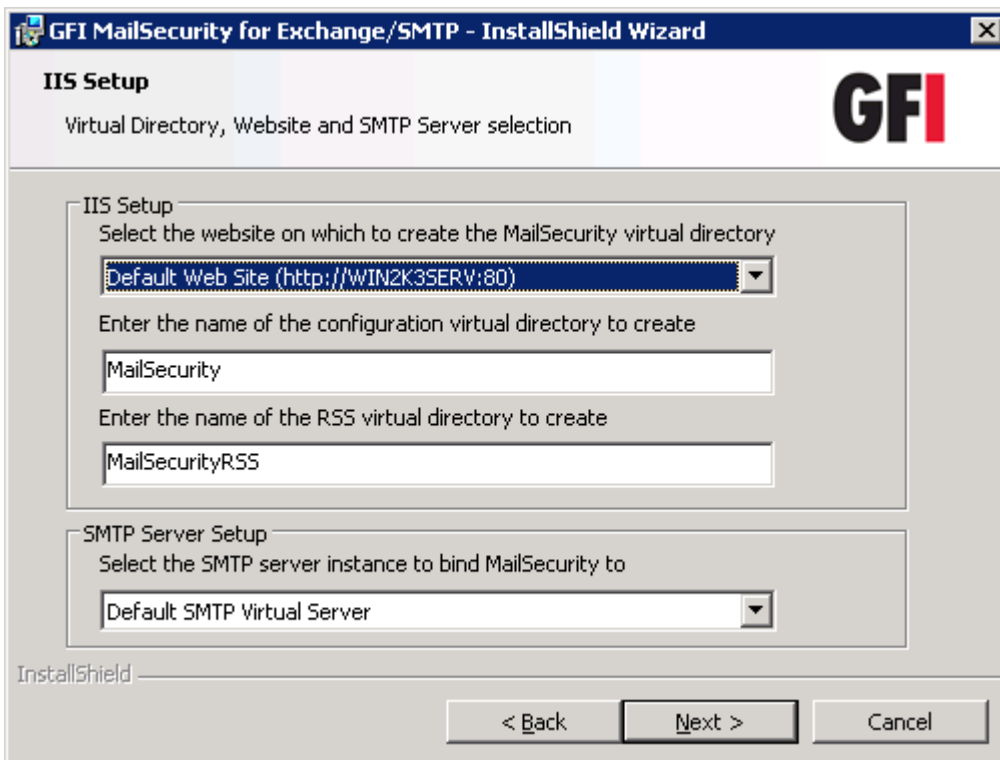
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ)

SMTP mode

GFI MailSecurity will retrieve the list of email users/addresses from your mail server. 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.

NOTE: For more information on which installation mode to use, refer to section [Which installation mode should I use?](#)

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



Screenshot 11 - Define your SMTP server and GFI MailSecurity virtual folder details.

8. In the IIS Setup dialog, configure the following options:

<p>The website to create the GFI MailSecurity virtual directory</p>	<p>Select the website where you want to host the GFI MailSecurity virtual directories.</p>
<p>The GFI MailSecurity Configuration virtual directory</p>	<p>Specify a name for the GFI MailSecurity virtual directory.</p>
<p>The GFI MailSecurity Quarantine RSS feeds virtual directory</p>	<p>Specify a name for the GFI MailSecurity Quarantine RSS feeds virtual directory.</p>
<p>SMTP Server Setup</p>	<p>Select the SMTP Server that GFI MailSecurity binds to. By default, GFI MailSecurity binds to your default SMTP virtual server (that is, the server specified in the MX record of your DNS Server). If you have multiple SMTP virtual servers on your domain, you can bind GFI MailSecurity to any available SMTP virtual server.</p> <p>NOTE 1: If you are installing on a Microsoft Exchange Server 2007/2010 machine this option is not shown since the IIS SMTP service is not required as Microsoft Exchange has its own built-in SMTP server.</p> <p>NOTE 2: After installation, you can still bind GFI MailSecurity to another SMTP virtual server from the GFI MailSecurity Configuration. For more information, refer to the 'SMTP server bindings' section in the GFI MailSecurity Administration & Configuration manual.</p>

Click **Next** to continue.

9. Setup now imports a list of your Local Domains from the IIS SMTP service. If any Local Domain is not listed, make sure to add it after installation completes. For more information, refer to the 'Adding Local Domains' section in the GFI MailSecurity Administration & Configuration manual. Click **Next** to continue.

NOTE: When installing on a Microsoft Exchange 2007/2010 machine, this screen is not displayed. Local domains are configured in the Post-Installation Wizard.

10. Setup will now ask you to select a folder where to install GFI MailSecurity. Click **Change...** to specify a new installation path or click **Next** to install in the default location and proceed with the installation.

11. Click **Install** to start the installation process.

NOTE: If you are prompted to restart the SMTP services, click **Yes** and finalize the installation.

12. On completion, click **Finish**.

NOTE: When installing on a Microsoft Exchange Server 2007/2010 machine, the installation launches the GFI MailSecurity Post-Installation Wizard. For information on how to use this wizard, refer to [GFI MailSecurity Post-Installation Wizard](#) chapter.

6.1 GFI MailSecurity Post-Installation Wizard

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

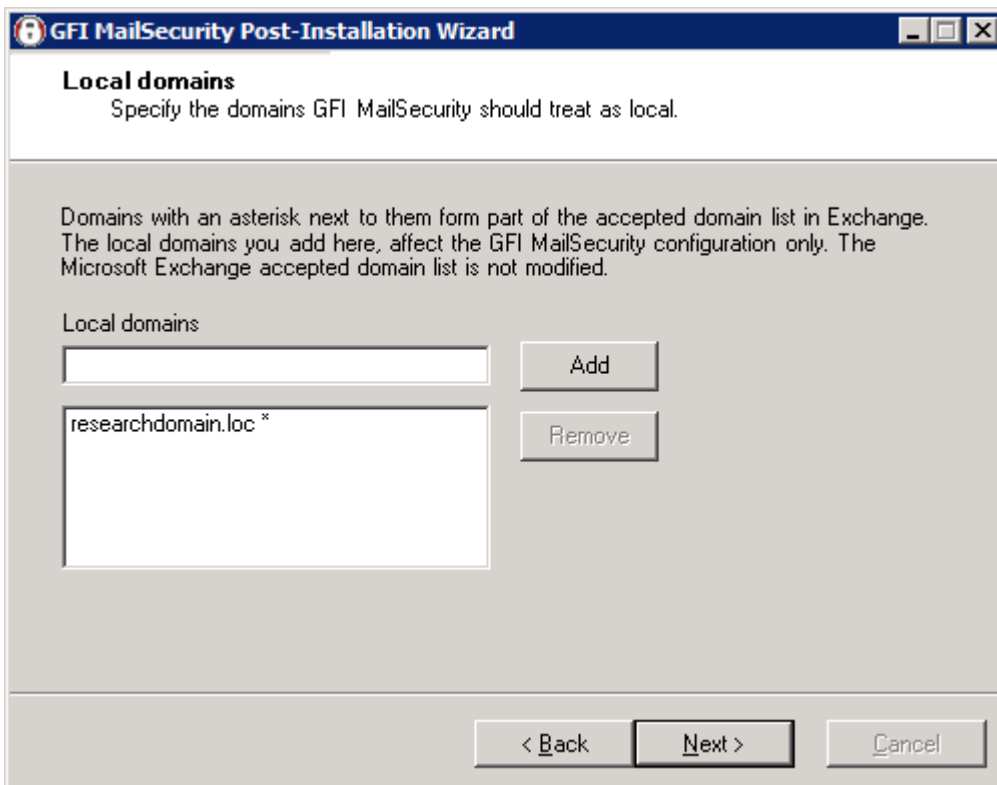


GFI MailSecurity will not work with Microsoft Exchange Server 2007/2010 if the Post-Installation wizard is not completed.

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 emails passing through the server.

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

The wizard collects information from the Microsoft Exchange Server 2007/2010 installation, such as the list of local domains and the server roles installed.

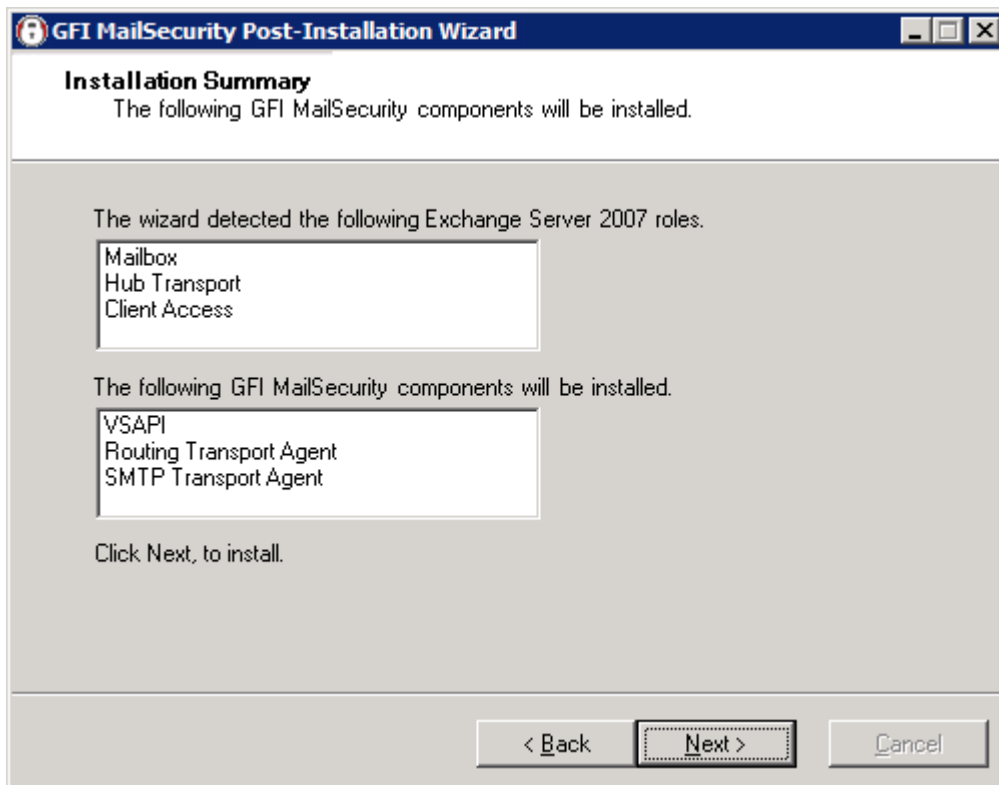


Screenshot 12 - Local domains list

2. The wizard displays the accepted domain list collected from Microsoft Exchange Server 2007/2010. Only emails sent to or received from these domains will be scanned by GFI MailSecurity. If there are any other local domains, type each domain in the **Local domains** box and click **Add**. If you want to remove a domain from this page, select it from the list and click **Remove**.

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

Click **Next** to continue.



Screenshot 13 - Server roles detected and list of components to install.

3. A list of the Microsoft Exchange Server 2007/2010 server roles detected on the machine and a list of the GFI MailSecurity components that need to be registered are displayed. Click **Next** to install the required GFI MailSecurity components.
5. Click **Finish** to close the wizard.

7 Upgrade from earlier versions

7.1 Upgrading from GFI MailSecurity 8 or earlier

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

This section shows you how to:

- Replace your current GFI MailSecurity 8 installation with a newer version.
- Convert and import the GFI MailSecurity 8 configuration settings to the new configuration format.

To upgrade from GFI MailSecurity 8, follow these steps:

1. Uninstall GFI MailSecurity 8.
2. When the GFI MailSecurity 8 uninstallation completes, some files are left in the root folder where GFI MailSecurity 8 was installed. One of these files is the **avapicfg.rdb** located in the Data sub-folder. You will need this file to migrate the settings from GFI MailSecurity 8 to the new GFI MailSecurity installation.
3. Install GFI MailSecurity as shown in the [New installations](#) section of this chapter.

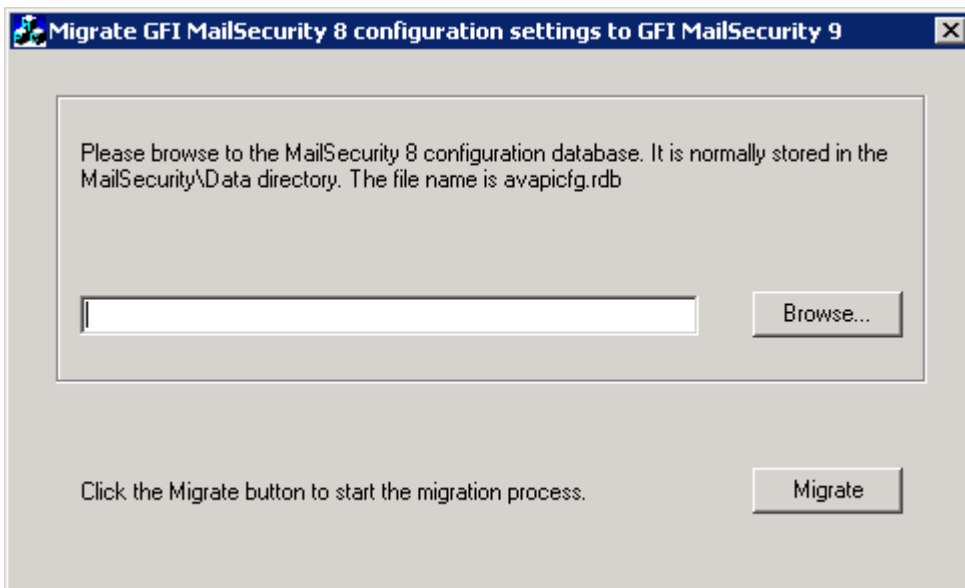


Do not install GFI MailSecurity to the same path where GFI MailSecurity 8 was installed to prevent files such as avapicfg.rdb from being overwritten.




Ensure that the new GFI MailSecurity installation is installed using the same mode as GFI MailSecurity 8. It is not possible to import settings if for example GFI MailSecurity 8 was installed in SMTP mode and the new installation is installed in Active Directory mode.

4. After the new installation of GFI MailSecurity is complete, stop the following services:
 - 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. Navigate to *<new GFI MailSecurity installation path>* \GFI\ContentSecurity\MailSecurity and run the **msec8upg.exe** tool.



Screenshot 14 - GFI MailSecurity 8 configuration settings migration tool

6. In the migration dialog, click **Browse** and select the **avapicfg.rdb** file from the Data sub-folder under the GFI MailSecurity 8 root folder.
7. Click **Migrate**.
8. When the migration process completes, click **OK** to close the information dialog box and click the close button  to close the migration tool.
9. You now need to start all the services stopped in step 4 above.
10. From the GFI MailSecurity configuration page check that the GFI MailSecurity 8 settings were migrated correctly.

7.2 Upgrading from GFI MailSecurity 9 or later

If you are currently using GFI MailSecurity 9, you can upgrade your current installation while retaining your existing configuration settings.



Upgrades cannot be undone, that is, you cannot downgrade to an earlier version once you have installed the latest version.

NOTE 1: On upgrading an existing installation, licensing reverts to trial version and a new fully purchased license key for GFI MailSecurity 10.1 is required. For more information on new license keys, refer to:

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

NOTE 2: You cannot change the installation path during GFI MailSecurity upgrades.

7.2.1 Upgrade procedure

1. Launch the GFI MailSecurity setup file on the machine where you have installed GFI MailSecurity 9.
2. Setup will now proceed to install GFI MailSecurity in the same way as a new installation. For more information refer to the [New installations](#) section earlier in this chapter.

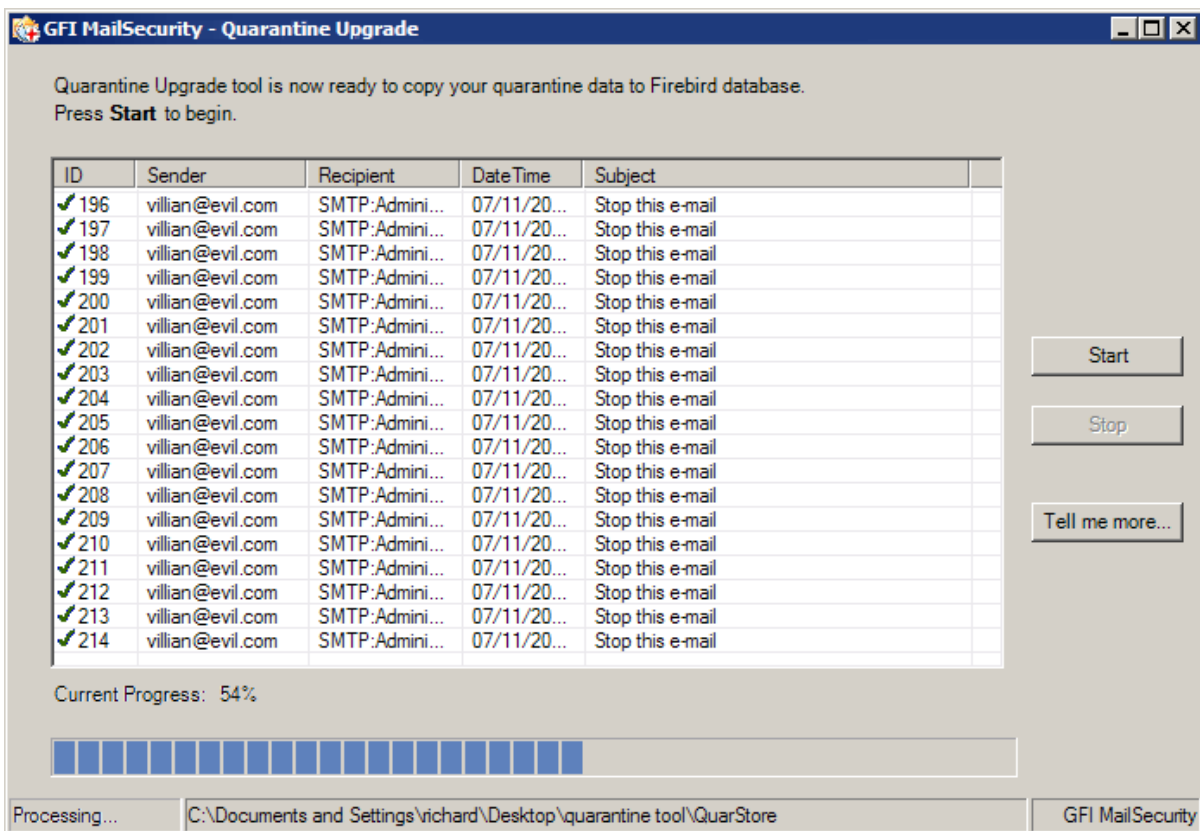
7.3 Upgrading the Quarantine

Starting from GFI MailSecurity 10 SR8, Quarantine information is stored in a Firebird database format. When upgrading from versions 9 or 10, GFI MailSecurity includes a Quarantine Upgrade Tool to automate migration from the old database to the new database format.



The old quarantine data will not be available until imported.

7.3.1 Using the Quarantine upgrade tool



Screenshot 15 - Quarantine upgrade tool

1. Open the Quarantine Upgrade tool from `<GFI MailSecurity installation path>\ContentSecurity\MailSecurity\` and launch **QssUpgrade.exe**.
2. Click **Start** to start data migration.

Duration of the upgrade depends on the volume of data in your quarantine.

8 Post-install actions

8.1 Add 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.

This section applies only when installing GFI MailSecurity on:

- Microsoft Windows XP with Service Pack 2
- Microsoft Windows Server 2003 with Service Pack 1 or 2

If you installed GFI MailSecurity on an operating system that includes DEP, you will need to add the GFI MailSecurity scanning engine (**GFiScanM.exe**) and the Kaspersky Virus Scanning Engine (**kavss.exe**) executables.

NOTE: The Kaspersky Virus Scanning Engine is optional. If you are not purchasing the engine, do not add kavss.exe to the DEP exception list.

To add the GFI executables in the DEP exception list:

1. From **Control Panel** and open 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: *<GFI MailSecurity installation path>\GFI\ContentSecurity\MailSecurity*, and choose **GFiScanM.exe**.
6. Click **Add** and from the dialog box browse to: *<GFI MailSecurity installation path>\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.

8.2 Securing access to the GFI MailSecurity configuration/quarantine

The GFI MailSecurity configuration and quarantine store can be accessed through a web browser. It is imperative that you configure proper security so that only authorized users can access the software.

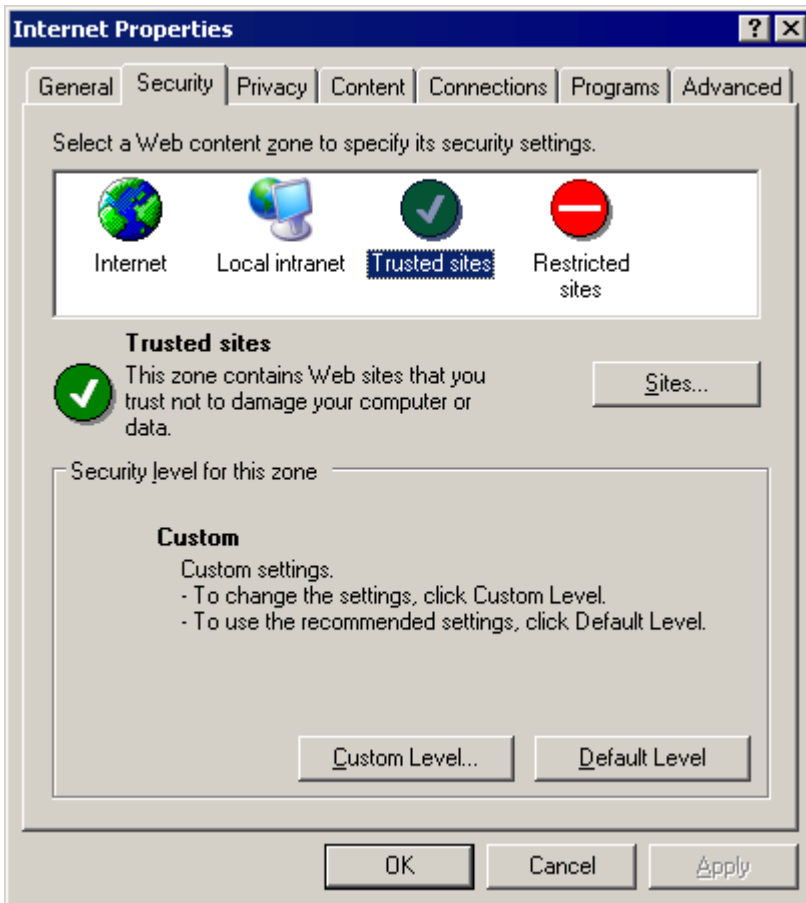
8.2.1 Local access only

You can configure GFI MailSecurity to be accessed only from the machine where it is installed.

1. Navigate to **Start ► Programs ► GFI MailSecurity ► GFI MailSecurity SwitchBoard**.
2. Select **Local mode** to allow access to GFI MailSecurity only from the GFI MailSecurity server (local machine).
3. Click **OK**.

To use this option you must add the local host address 'http://127.0.0.1' to the list of trusted sites in Internet Explorer.

1. Navigate to **Start ► Control Panel ► Internet Options**.
2. From the **Internet Properties** dialog select **Security** tab and click the **Trusted sites** icon from the **Web content zone** list.



Screenshot 16 - Internet properties dialog

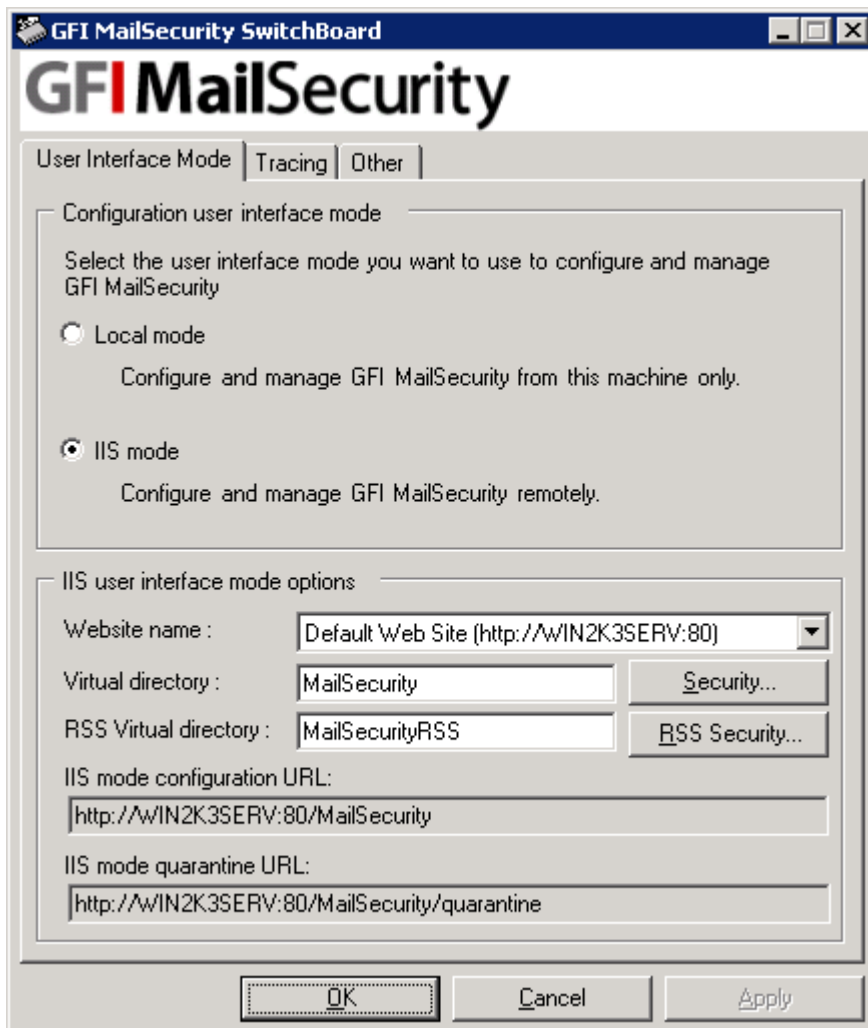
3. Click **Sites**.
4. From the **Trusted sites** dialog specify **http://127.0.0.1** in the **Add this Web site to the zone** text box.
5. Click **Add**.
6. Click **Close** and **OK** to apply settings.

8.2.2 Local and remote access

You can configure GFI MailSecurity to be accessed from both the machine where it is installed and other machines on the network.

1. Navigate to **Start ► Programs ► GFI MailSecurity ► GFI MailSecurity SwitchBoard**.
2. Select **IIS mode** to allow access to GFI MailSecurity both from the GFI MailSecurity server and from remote machines.

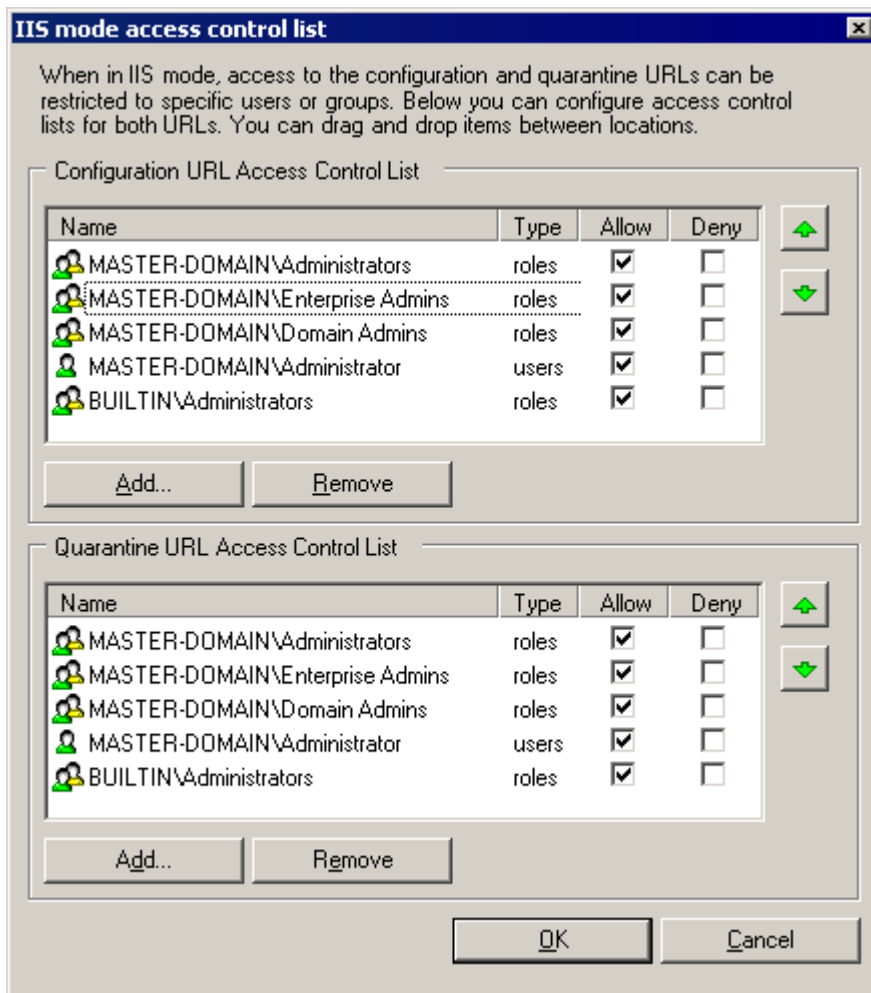
NOTE: You can also configure IIS to use https for the GFI MailSecurity configuration. For more information how to do this refer to <http://kbase.gfi.com/showarticle.asp?id=KBID002515>.



Screenshot 17 - GFI MailSecurity SwitchBoard

Configure the Active Directory accounts or groups to allow access to the Configuration and Quarantine Store.

1. From the GFI MailSecurity Switchboard, click **Security....**



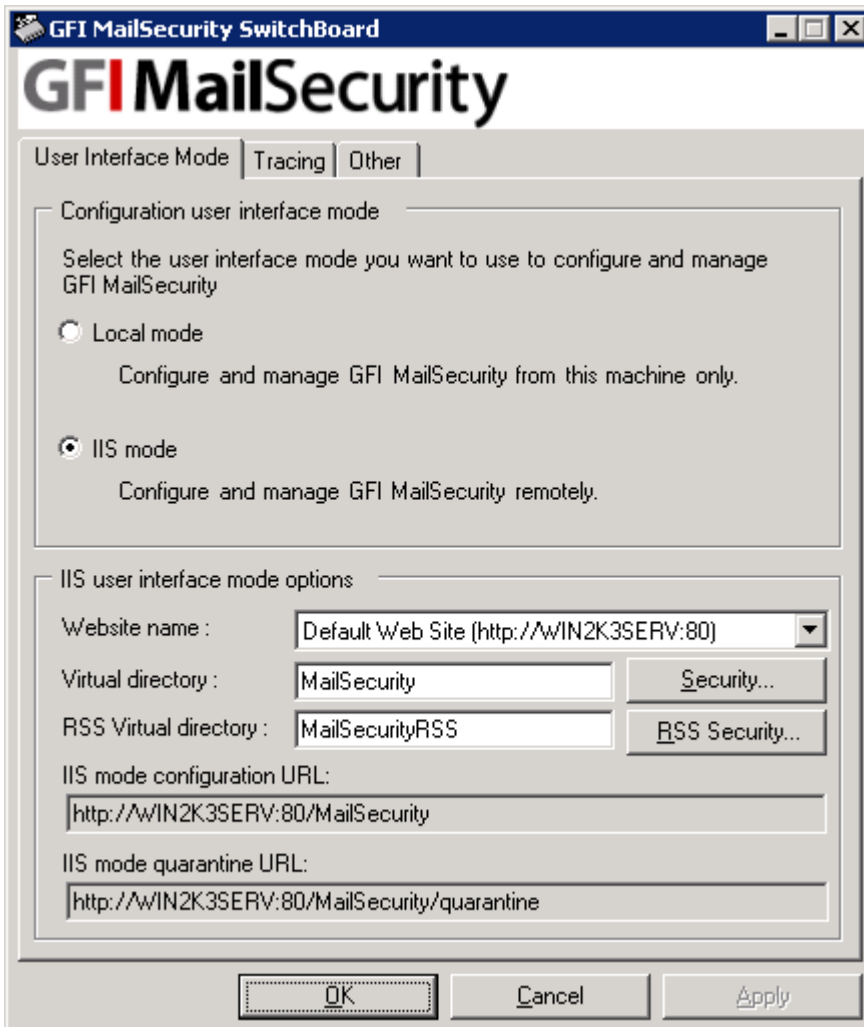
Screenshot 18 - Configuration / Quarantine store Access Control Lists

2. In the **IIS mode access control list** dialog, configure the users to allow access to the GFI MailSecurity configuration and the quarantine store in separate access control lists.
 3. To allow access to a particular user or group, select **Allow** checkbox. To deny access, select the check box under the **Deny** column.
 4. If there are users or groups to allow access to but are not listed, click **Add** to specify and add to the list.
- NOTE:** You can drag and drop accounts and groups between the GFI MailSecurity configuration and the quarantine store lists to avoid configuring the same users/groups twice.
5. On completion, click **OK**.
 6. Click **OK** and wait while applying new settings.
 7. Click **OK** to finalize configuration.

8.3 Securing access to the GFI MailSecurity Quarantine RSS feeds

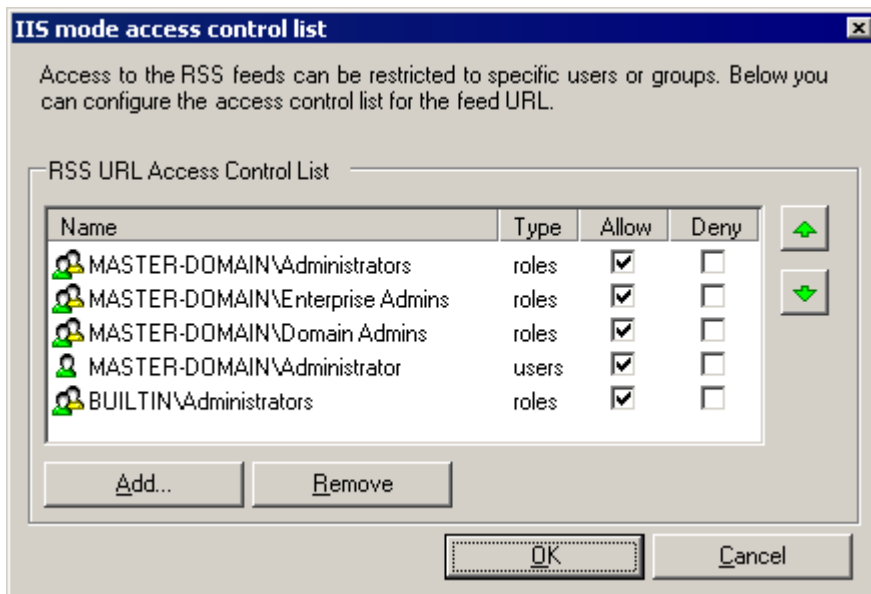
You can configure GFI MailSecurity to create quarantine RSS feeds on specific quarantine folders. To configure who can subscribe to the quarantine RSS feeds:

1. Navigate to **Start ► Programs ► GFI MailSecurity ► GFI MailSecurity SwitchBoard**.



Screenshot 19 - GFI MailSecurity SwitchBoard

2. Click **RSS Security....**



Screenshot 20 - Quarantine RSS feeds Access Control Lists

3. In the **IIS mode access control list** dialog box, configure which users/groups can subscribe to the quarantine RSS feeds. Click **Add** or **Remove** buttons to add or remove users or groups from the list. For each entry, select **Allow** or **Deny** checkboxes to allow or deny access.
4. Click **OK** to finalize access permissions.
5. Click **OK** and wait while applying the new settings.
6. On completion, click **OK**.

8.4 Configuring virtual directory names

By default, the virtual directory names of GFI MailSecurity and Quarantine RSS are **MailSecurity** and **MailSecurityRSS** respectively. You can customize these virtual directory names.

NOTE: If GFI MailSecurity is configured to be accessed only from the local machine, the GFI MailSecurity Configuration virtual directory is not configurable.

1. Launch the **GFI MailSecurity SwitchBoard** from **Start ► Programs ► GFI MailSecurity ► GFI MailSecurity SwitchBoard**.
2. From the **IIS user interface mode options** area, specify custom virtual directory names for:
 - **GFI MailSecurity virtual directory** - key in a custom name in the **Virtual directory** field.
 - **Quarantine RSS virtual directory** - key in a custom name in the **RSS Virtual directory** field.
3. Click **OK** to apply changes.
4. Click **OK** and wait while applying the new settings.
5. When the process completes, click **OK**.

9 Accessing the GFI MailSecurity Configuration and Quarantine Store

This section provides information on how to access the GFI MailSecurity Configuration and Quarantine Store from the local or a remote machine.

The GFI MailSecurity Configuration loads depending on the access mode configured in the GFI MailSecurity SwitchBoard application.

IIS mode (default)	GFI MailSecurity loads in your default web browser using the IIS setup settings configured during installation.
---------------------------	---

Local mode	GFI MailSecurity loads in an html viewer application.
-------------------	---

For more information how to configure these settings refer to chapter [Securing access to the GFI MailSecurity configuration/quarantine](#).

9.1 Accessing the configuration from the GFI MailSecurity machine

Navigate to **Start ► Programs ► GFI MailSecurity** and click **GFI MailSecurity**. The GFI MailSecurity Configuration loads depending on how it is configured in the GFI MailSecurity SwitchBoard application.



Screenshot 21 - GFI MailSecurity accessed in local mode

9.2 Accessing the configuration from a remote machine

To access the GFI MailSecurity configuration or quarantine store from a remote machine ensure that GFI MailSecurity is set to IIS mode (default setting) in the GFI MailSecurity Switchboard.

9.2.1 Accessing the configuration

1. Start Microsoft Internet Explorer.
2. In the address bar, key in the following address to access the GFI MailSecurity configuration:

`http://<GFI MailSecurity server name>/<GFI MailSecurity virtual directory name>`

where:

- *<GFI MailSecurity server name>* is the fully qualified domain name of the server where GFI MailSecurity is installed
- *<GFI MailSecurity virtual directory name>* is the name configured for the GFI MailSecurity virtual directory (by default: MailSecurity).

For example: `http://msecsvr.mydomain.com/MailSecurity`

3. You will be prompted to specify a user name and password to authenticate.

NOTE: The specified credentials must be allowed access to the GFI MailSecurity configuration to be able to log in. Permissions can be configured from the GFI MailSecurity SwitchBoard.

9.2.2 Accessing the quarantine

1. Start Microsoft Internet Explorer.
2. In the address bar, specify the following address to access the GFI MailSecurity configuration:

`http://<GFI MailSecurity server name>/<GFI MailSecurity virtual directory name>/quarantine`

where *<GFI MailSecurity server name>* is the fully qualified domain name of the server where GFI MailSecurity is installed, and *<GFI MailSecurity virtual directory name>* is the name configured for the GFI MailSecurity virtual directory (by default: MailSecurity).

For example: `http://msecsvr.mydomain.com/mailsecurity/quarantine`

3. You will be prompted to specify a user name and password to authenticate.

NOTE: The specified credentials must be allowed access to the GFI MailSecurity quarantine store to be able to log in. Permissions can be configured from the GFI MailSecurity SwitchBoard.

4. From the left pane, select the node to display.

Quarantine

Use this page to perform quick searches and manage quarantined content in categories.

Quick Search

Please select and use the following fields to perform quarantine content search.

Search in sender /recipients:

Search in subject:

Search in quarantine reason:

Quarantined Items

Folder	Items
Today	52
Yesterday	0
This week	52
All items	52

Screenshot 22 - Accessing the quarantine

10 Testing your GFI MailSecurity system

10.1 Introduction

GFI MailSecurity is now ready to start protecting your mail system from threats. This section shows you how to create a custom content filtering rule and test the operation of GFI MailSecurity by breaching this rule.

10.2 Step 1: Create a Content Filtering rule

1. Launch the GFI MailSecurity console.
2. Navigate to **GFI MailSecurity ► Scanning & Filtering ► Content Filtering** node.
3. Click **Add Rule...**
4. In **Rule name** key in 'Test Rule'.
5. Select the **Subject** tab and select **Enable subject content filtering**.
6. In **Enter phrase** key in 'Threat test' and click **Add**.
7. Select the **Actions** tab, enable **Block email and perform this action** and select **Quarantine email**.
8. Click **Apply** to save the rule.

10.3 Step 2: Send an inbound test email

1. From an external email account, create a new email and key in "Threat test" as the subject.
2. Send the email to one of your internal email accounts.

10.4 Step 3: Send an outbound test email

1. From an internal email account, create a new email and key in "Threat test" as the subject.
2. Send the email to an external email account.

10.5 Step 3: Confirm that test emails were blocked

Confirm that GFI MailSecurity is working by ensuring that both inbound and outbound test emails were blocked and quarantined. To do this:

1. From GFI MailSecurity, navigate to **GFI MailSecurity ► Quarantine ► Today**.
2. Ensure that both inbound and outbound test emails are listed, with reason being **triggered rule "test rule"**.

NOTE: When test is completed successfully, delete or disable the "test rule" created in step 1.

Quarantine

Use this page to sort, and manage quarantined items

Approve items

Delete items

Rescan items

Items per page:

Approve all

Delete all

Rescan all

Update

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

<input type="checkbox"/>	ID	Module	Reason	Sender	Recipient(s)	Subject	Date ▲	Source
<input type="checkbox"/>	65	Content Filtering	triggered rule "test rule"	administrator@master ...	external@webmail.com	threat test	9/23/2010 8:40:26 AM	Gateway (SMTP)
<input type="checkbox"/>	56	Content Filtering	triggered rule "test rule"	external@webmail.com	administrator@master ...	threat test	9/23/2010 8:28:35 AM	Gateway (SMTP)

Page(s) < 1

Edit search folder

Delete search folder

Item source:

Screenshot 23 - Ensuring that test emails are blocked and quarantined

11 Uninstalling GFI MailSecurity

11.1 Introduction

This chapter describes how to uninstall GFI MailSecurity for all supported operating systems.

NOTE 1: If you are planning to uninstall and reinstall GFI MailSecurity to fix problems encountered during installation, it is recommended to first read the [Troubleshooting](#) chapter in this manual.

NOTE 2: Third-party components which are required by GFI MailSecurity, such as Microsoft .NET Framework or Microsoft Messaging Queuing Service, will not be uninstalled.

11.2 Uninstall GFI MailSecurity

1. Exit GFI MailSecurity.
2. From the **Control Panel** select:
 - **Add or Remove Programs** - Windows Server 2003, Windows SBS 2003.
 - **Programs and Features** - Windows Server 2008, Windows SBS 2008.
3. From the list of installed software select **GFI MailSecurity for Exchange/SMTP** and click **Remove** or **Uninstall**.
4. Follow on-screen instructions to uninstall GFI MailSecurity.

11.3 Uninstalling GFI MailSecurity from an Active/Passive Cluster

To uninstall GFI MailSecurity from a **MAILCLUSTER** cluster environment, 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**.

12 Troubleshooting

12.1 Introduction

The troubleshooting chapter explains how you should go about resolving any 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

12.2 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, 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/>.

12.3 Web Forum

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

12.4 Common issues

ISSUE ENCOUNTERED	POSSIBLE CAUSE AND SOLUTION
<p>1. When migrating the GFI MailSecurity 8 settings to the new installation using msec8upg.exe tool, the following error is shown:</p> <p>“The user lookup mode of your MailSecurity 8 configuration does not match user lookup mode of your MailSecurity 9 configuration.”</p>	<p>Cause</p> <p>The user lookup mode of the GFI MailSecurity 8 installation is different from the user lookup mode of the new installation.</p> <p>Solution</p> <ol style="list-style-type: none"> 1. Uninstall the new GFI MailSecurity installation. 2. Re-install the new GFI MailSecurity installation in the appropriate mode. 3. Retry importing the GFI MailSecurity 8 configuration as described in Upgrading from GFI MailSecurity 8 or earlier.
<p>Error when receiving emails:</p> <p>"Body type not supported by Remote Host"</p>	<p>This error occurs when emails are relayed from the IIS SMTP server to the Microsoft Exchange server. This happens because Microsoft Exchange Server versions 4.0, 5.0, and 5.5 are not able to handle 8-bit MIME messages. For instructions how to turn off 8BITMIME in Windows Server 2003 refer to:</p> <p>http://support.microsoft.com/default.aspx?scid=kb:en-us:Q262168.</p>
<p>Legitimate emails are moved to the failedmails folder</p>	<p>Cause</p> <p>When GFI MailSecurity is not able to scan incoming emails, these emails are not delivered to the recipient(s) since they may contain malicious content. GFI MailSecurity moves these emails to the failedmails folder, which is located in: <GFI MailSecurity installation path>\Content Security\MailSecurity\</p>

Solution

If any legitimate emails are moved to the failedmails folder, these can be manually re-processed for delivery. For more information how to do this in various environments refer to:

<http://kbase.gfi.com/showarticle.asp?id=KBID003263>

GFI MailSecurity returns the following error:

“The file was blocked by the attachment filtering module at file type checking stage. The attachment claimed to be a <filetype 1> which is identified as being an attachment in category <filetype 1>. The file was detected to belong to the category <filetype 2>.”

Cause

An attached file is detected as being a file with multiple file-types.

Solution

For information how to resolve this issue refer to:

<http://kbase.gfi.com/showarticle.asp?id=KBID001922>.

NOTE: The solution to this issue requires changes in the Windows Registry. It is important to follow the steps described in the solution with attention as incorrect configuration can cause serious, system-wide problems.

12.5 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 visit: <http://www.gfi.com/company/contact.htm>.

NOTE: Before you contact our Technical Support team, 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.

12.6 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>.

13 Appendix - Installing on a Microsoft Exchange 2003 cluster

A Microsoft Exchange cluster can be set up in one of 2 modes: active/active or active/passive. This appendix describes how to install GFI MailSecurity on a Microsoft Exchange 2003 Active/Passive cluster

NOTE: Installing GFI MailSecurity on a Microsoft Exchange 2003 Active/Active cluster is currently not supported.

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

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

The following steps are required on each node:

- 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 be set 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 be set to 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 in 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.



WARNING: 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. For more information about this issue refer to:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;885440>

Due to this, 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. It is therefore recommended to install Service Pack 2 for Microsoft Exchange Server 2003. For more information on how to install Microsoft Exchange Server 2003 service packs in a clustered Exchange Server environment refer to:

<http://support.microsoft.com/kb/867624/en-us>.

14 Glossary

Active Directory	A technology that provides a variety of network services, including LDAP directory services.
AD	See Active Directory
Anti-virus software	Software that detects malware such as Trojan horses in emails, files and applications.
Botnet	A network of infected computers that run autonomously and are controlled by a hacker/cracker.
Decompression engine	A scanning module that decompresses and analyzes archives attached to an email.
Demilitarized Zone	An internet-facing section of a network that is not part of the internal network. Its purpose typically is to act as a gateway between internal networks and the internet.
Directory harvesting	Email attacks where known email addresses are used as a template to create other email addresses.
Domain Name System	A database used by TCP/IP networks that enables the translation of hostnames to IP addresses and provides other domain related information.
DMZ	See Demilitarized Zone
DNS	See Domain Name System
DNS MX	See Mail Exchange
Email headers	Information that precedes the email text (body) within an email message. This includes the sender, recipient, subject, sending and receiving time stamps, etc.
Exploit	An attack method that uses known vulnerabilities in applications or operating systems to compromise the security of a system.
Gateway	The computer (server) in a LAN that is directly connected to an external network. In GFI MailSecurity, gateway refers to the email servers within the company that first receive email from external domains.
HTML Sanitizer	A filtering module within GFI MailSecurity that scans and removes html scripting code from emails.
HTTP	Hypertext Transfer Protocol - A protocol used to transfer hypertext data between servers and internet browsers.
IIS	See Internet Information Services
Internet Information Services	A set of Internet-based services created by Microsoft Corporation for internet servers.
LDAP	See Lightweight Directory Access Protocol
Lightweight Directory Access Protocol	An application protocol used to query and modify directory services running over TCP/IP.
Mail Exchange	The DNS record used to identify the IP addresses of the domain's mail servers.

Malware	All malicious types of software that are designed to compromise computer security and which usually spread through malicious methods.
Microsoft Message Queuing Services	A message queue implementation for Windows Server operating systems.
MIME	See Multipurpose Internet Mail Extensions
MSMQ	See Microsoft Message Queuing Services
Multipurpose Internet Mail Extensions	A standard that extends the format of e-mail to support text other than ASCII, non-text attachments, message bodies with multiple parts and header information in non-ASCII character sets.
PGP encryption	A public-key cryptosystem often used to encrypt emails.
Public folder	A common folder within Microsoft Exchange that allows users to share information.
Quarantine Store	A central repository within GFI MailSecurity where all blocked emails are retained until they are reviewed by an administrator.
Recursive archives	Archives that contain multiple levels of sub-archives (that is, archives within archives). Also known as nested archives.
RSS feeds	A protocol used by websites to distribute content (feeds) that frequently changes (for example news items) with its subscribers.
Secure Sockets Layer	A protocol to ensure an integral and secure communication between networks.
Simple Mail Transport Protocol	An internet standard used for email transmission across IP networks.
SMTP	See Simple Mail Transport Protocol
SSL	See Secure Sockets Layer
Trojan horse	Malicious software that compromises a computer by disguising itself as legitimate software.
Virus scanning engine	A virus detection technology implemented within antivirus software that is responsible for the actual detection of viruses.
Zombie	An infected computer that is made part of a Botnet through malware.

Index

A

Active Directory, 9, 22, 27, 49
Active/Passive cluster, 47, 48
anti-virus, 12
ASP.Net, 12

D

Database, 21, 29
DEP, 31
DMZ, 8, 22, 49
DNS, 17, 19, 23
Domain, 9, 14, 15, 17, 19, 23, 25, 39

E

Edge Server, 7, 12
email, 3, 7, 8, 9, 15, 16, 17, 19, 20, 21, 22, 49

F

firewall, 8, 22

G

gateway, 7, 13, 17, 19

H

Hub Transport, 3

I

IIS, 11, 12, 13, 15, 17, 20, 23, 27, 34, 37, 47,
48
Internal email, 41
Internet, 7, 8, 11, 14, 18, 19, 32, 39
IP, 14, 15, 17, 18, 19, 47, 48
ISP, 19

K

Kaspersky, 31

L

Licensing, 6
Lotus Notes, 9, 18, 19

M

Microsoft Exchange, 2, 3, 8, 12, 17, 18, 23,
24, 25, 26, 47, 48
Microsoft Exchange Server, 45
MSMQ, 11, 50

N

Net framework, 11

P

Performance, 9, 17
perimeter server, 49
POP3, 11
Post-Installation, 24

Q

Quarantine, 2, 21, 23, 29, 31, 34, 35, 36, 37,
39, 47

R

RSS Feeds, 23, 35, 36

S

Service Pack, 31, 48
SMTP, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19,
20, 23, 27, 47
SMTP relay, 13
SMTP Server, 13, 45



V

Virtual directory, 39, 47

W

Web content zone, 32

Windows XP, 11, 31

Wizard, 15, 24, 25