

Installing GFI MailSecurity

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.

Typical deployment scenarios

Installing GFI MailSecurity on your mail server

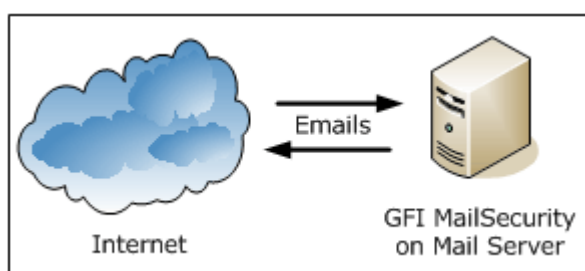


Figure 1 - Installing GFI MailSecurity on your mail server

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 installations:

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

Installing GFI MailSecurity on a mail relay server

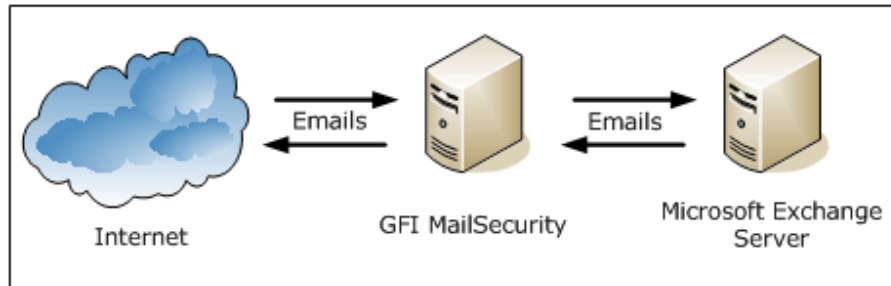


Figure 2 - Installing GFI MailSecurity on a mail gateway/relay server

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

NOTE 2: 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

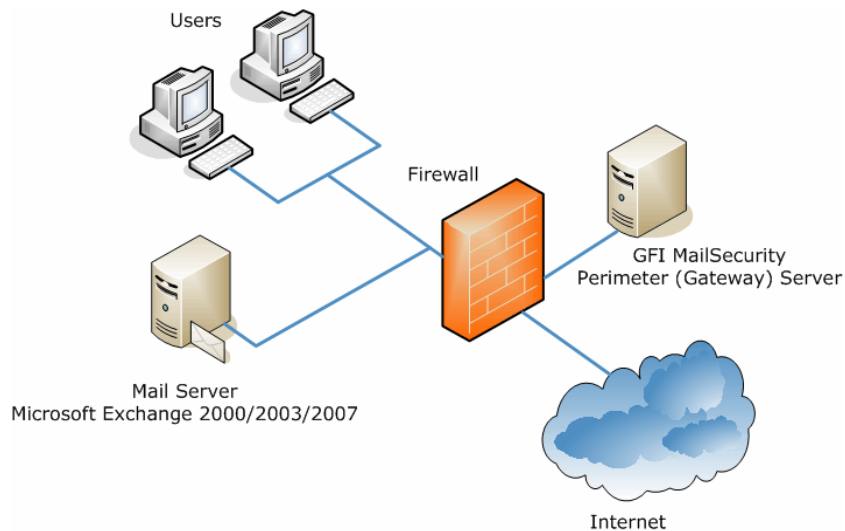


Figure 3 - Installing GFI MailSecurity on a separate machine on a DMZ

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 environment, the mail relay server in the DMZ can be a machine running Microsoft Exchange Server 2007 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 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 1: 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 the 'Securing access to the GFI MailSecurity configuration/quarantine' section in this chapter.

NOTE 2: 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.

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.

System requirements

To install GFI MailSecurity you need:

- Windows Server 2008/2003 (x32 or x64 Edition) or Windows 2000 Professional/Server/Advanced Server (Service Pack 1 or higher) or Windows XP

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

- Microsoft Exchange Server 2007, 2003, 2000 (SP1), 5.5, 5, 4, or Lotus Notes 4.5 and up, or any SMTP/POP3 mail server

NOTE 1: If you are installing on Microsoft Exchange Server 2007, you need to have either an Edge Server Role, Hub Transport Role or Mailbox Server Role and Hub Transport Server Role installed. GFI MailSecurity cannot be installed on a Microsoft Exchange 2007 machine with only Mailbox Server Role installed.

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

- Microsoft .Net framework 2.0
- MSMQ – Microsoft Messaging Queuing Service
- Internet Information Services (IIS) (x32 or x64 Edition) – SMTP service and World Wide Web service

NOTE: If installing on a Microsoft Exchange 2007 machine, the IIS SMTP service is not required, since it has its own built in SMTP server.

- Microsoft Data Access Components (MDAC) 2.8

IMPORTANT: 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>.

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

Hardware requirements

The hardware requirements for GFI MailSecurity are:

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

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.

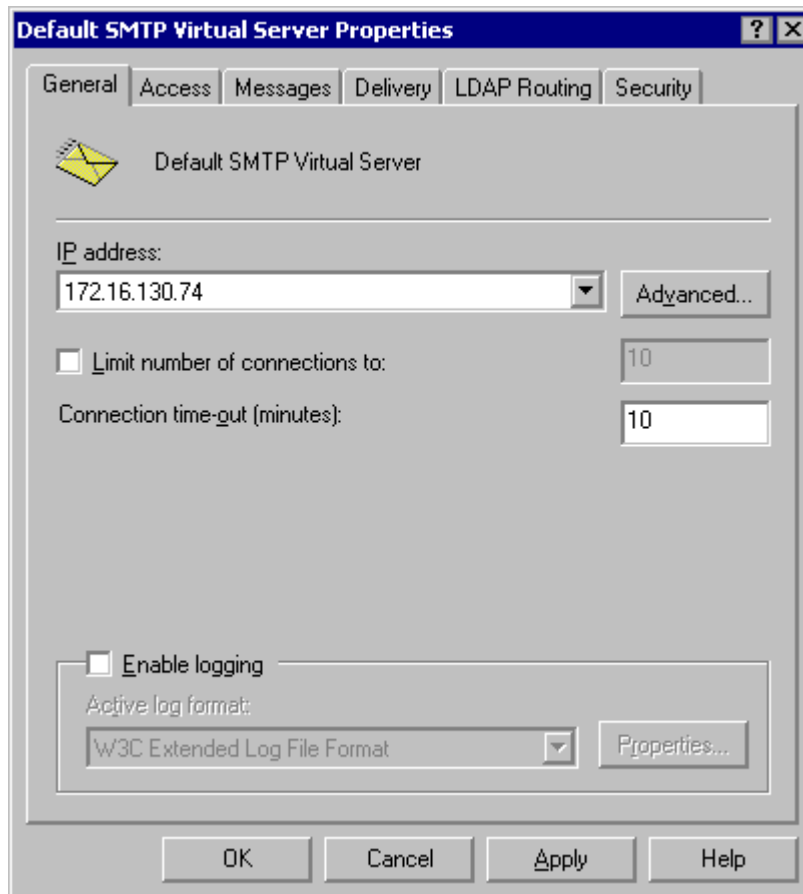
Step 1: Verify installation of IIS SMTP and WWW services

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

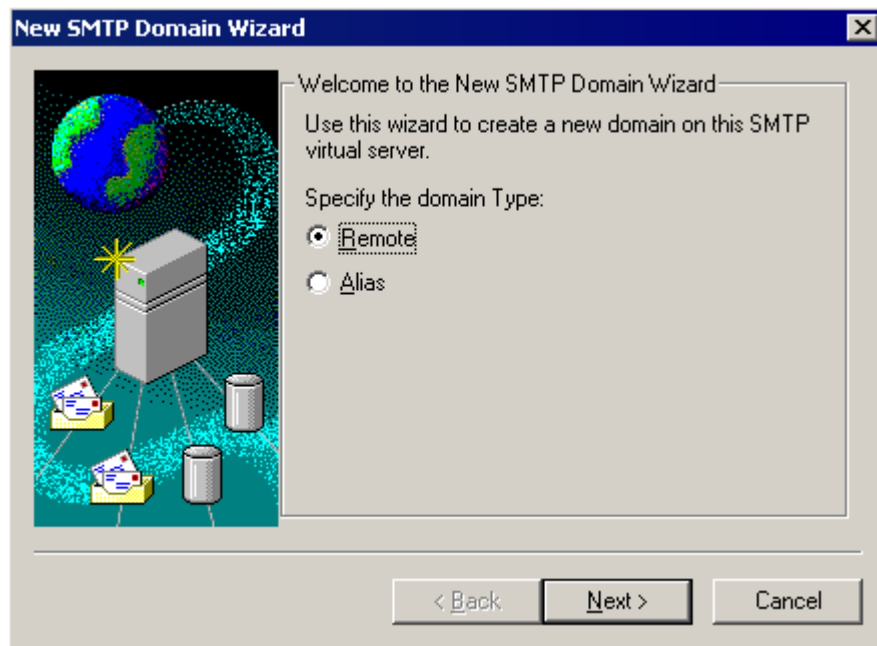
3. Assign an IP address to the SMTP relay server from the **IP address** list and then click **OK**.

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**.

IMPORTANT NOTE ABOUT LOCAL DOMAINS

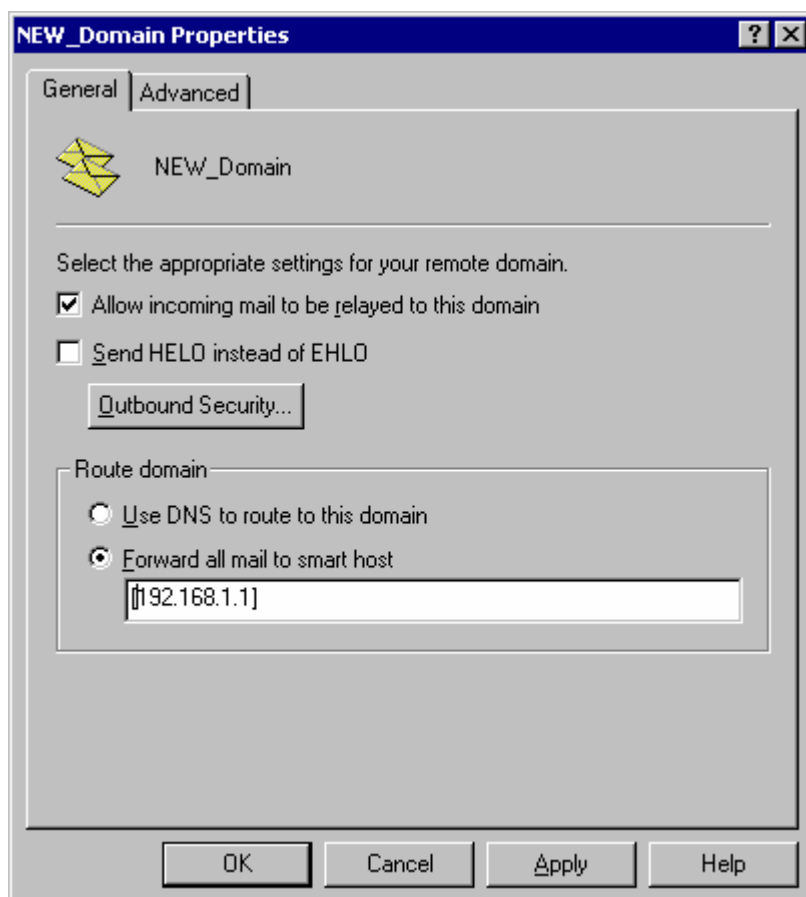
NOTE: Upon installation, GFI MailSecurity will import Local Domains from the IIS SMTP service. If you add additional Local Domains in IIS SMTP service, you must also add these domains to GFI MailSecurity because this does not detect newly added Local Domains automatically. You can add more/new Local 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**.

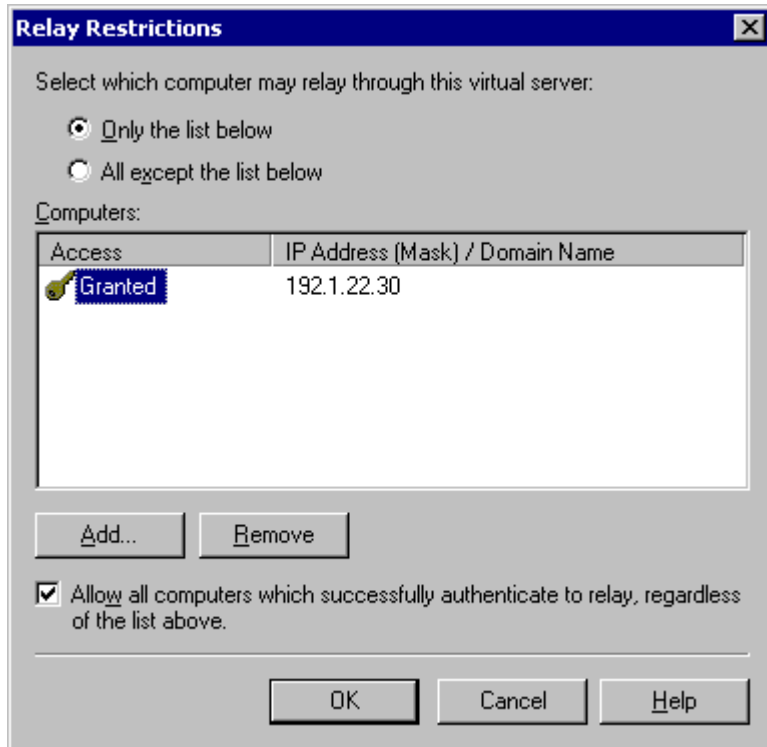


Screenshot 4 - Configure the new domain

Step 4: Secure your mail relay server

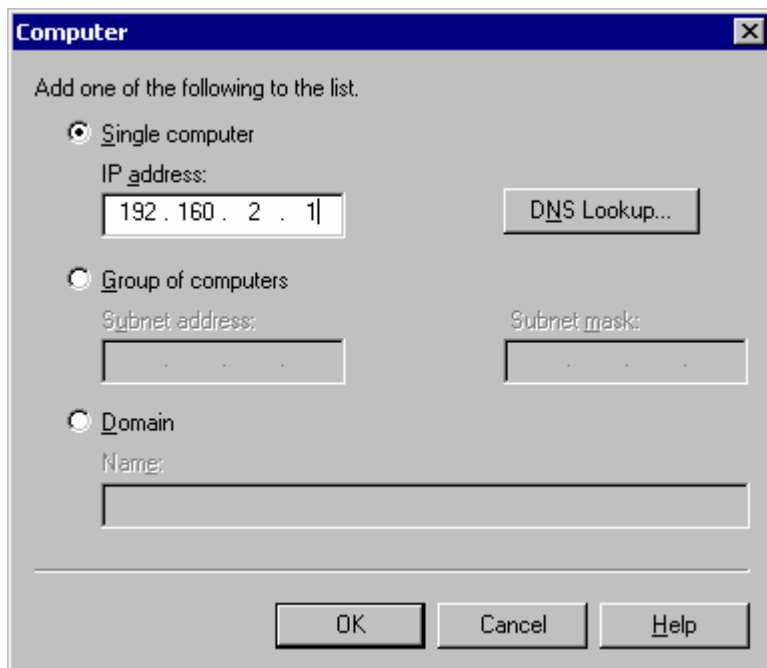
In this step, you will set up your SMTP virtual server's mail Relay Restrictions. This means that you must specify which machines may relay email through this virtual server (i.e., effectively limit the servers that can send email via this server).

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:

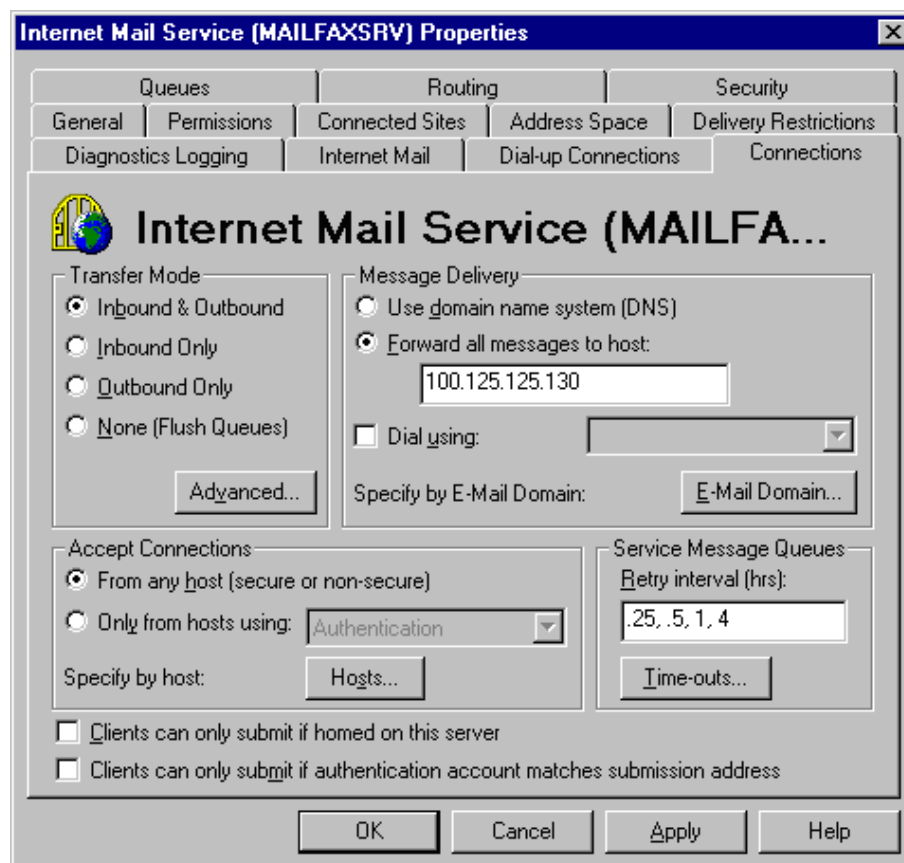
- **Single computer:** Select this option to specify one particular host that will relay email via this server. If you want to look up the IP address of a specific host, click **DNS Lookup**.
- **Group of computers:** Select this option to specify the base IP address for the computers that you want to 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.

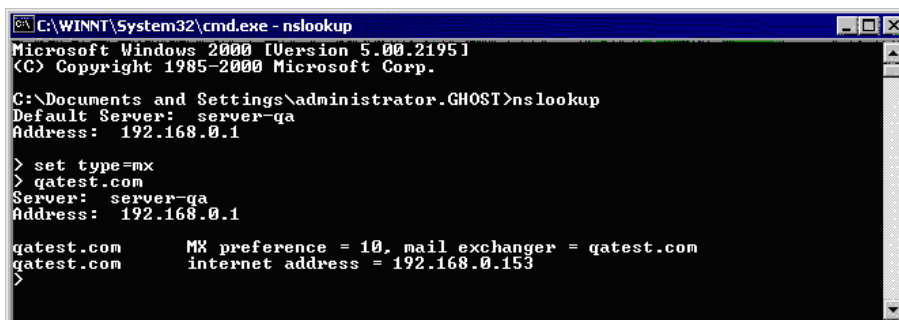
Step 6: The MX record of your domain must point to the mail relay server

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-ga
Address:  192.168.0.1

> set type=mx
> gatest.com
Server:  server-ga
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 the 'Installing GFI MailSecurity' section in this chapter.

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 the 'Installing GFI MailSecurity' section below.

Installing GFI MailSecurity

Before you install GFI MailSecurity, check the points below:

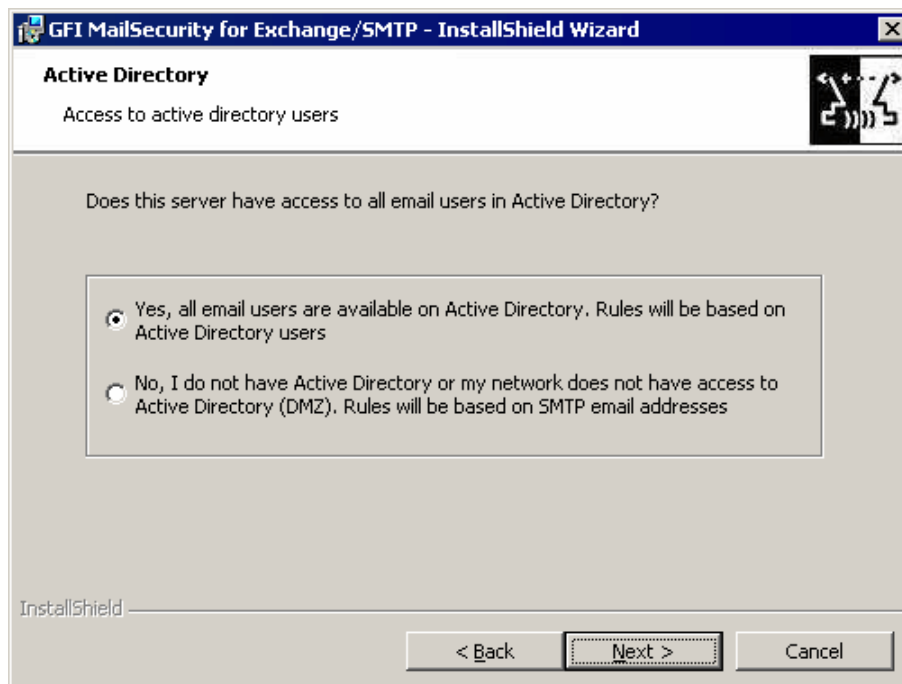
1. Make sure that you are logged on as Administrator or you are using an account with administrative privileges.

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.
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.

NOTE: When you use the evaluation license key, you will be able to use GFI MailSecurity for 10 days. If later you decide to buy GFI MailSecurity, you will not need to install GFI MailSecurity again – entering the purchased license key will be sufficient.



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

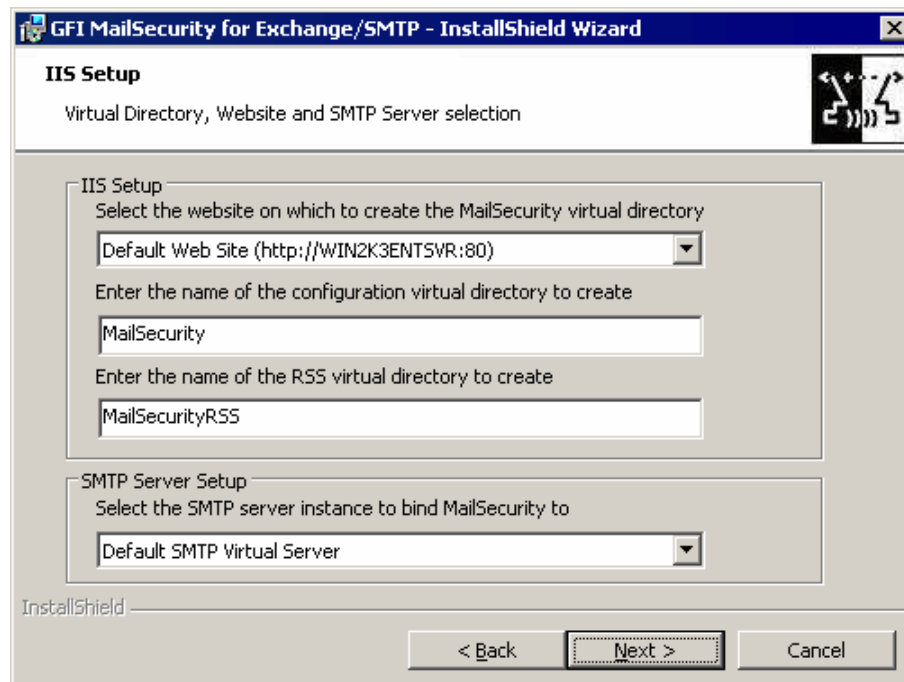
4. Setup will now ask you to select the mode that GFI MailSecurity will use to retrieve the list of your email users. You must select one of the following options:

- **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 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 the 'SMTP server bindings' section in the 'General Settings' chapter.

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 the 'General Settings' chapter. 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 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 machine, the installation will launch the GFI MailSecurity Post-Installation Wizard. Refer to the following section for information on how to use this wizard.

GFI MailSecurity Post-Installation Wizard

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

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

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 so that it can process and scan the emails passing through the server.

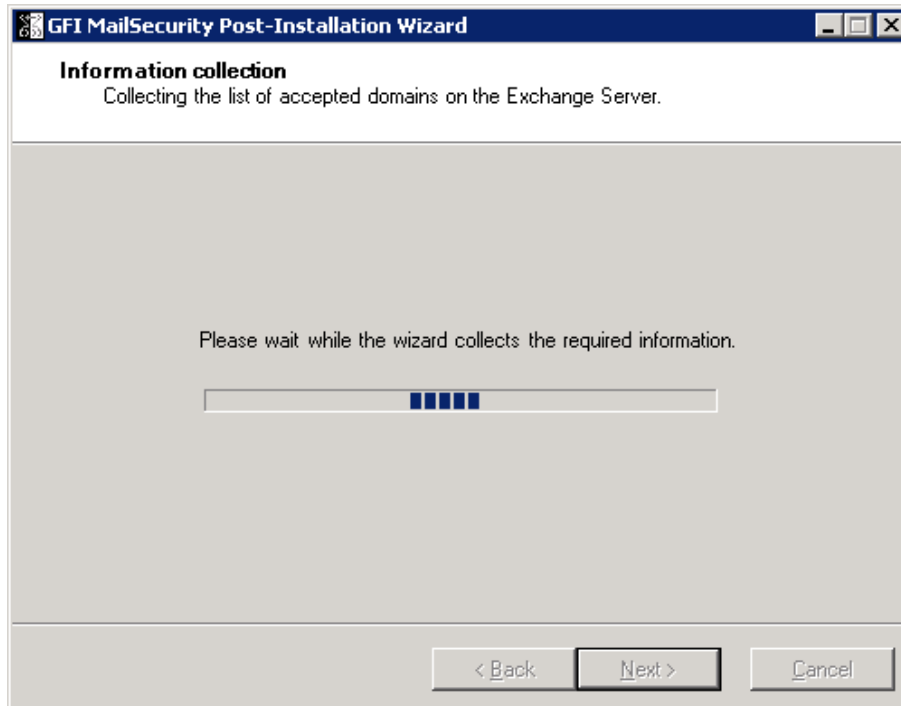
To complete the GFI MailSecurity Post-Installation Wizard, follow these steps:

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



Screenshot 11 - GFI MailSecurity Post-Installation Wizard welcome page

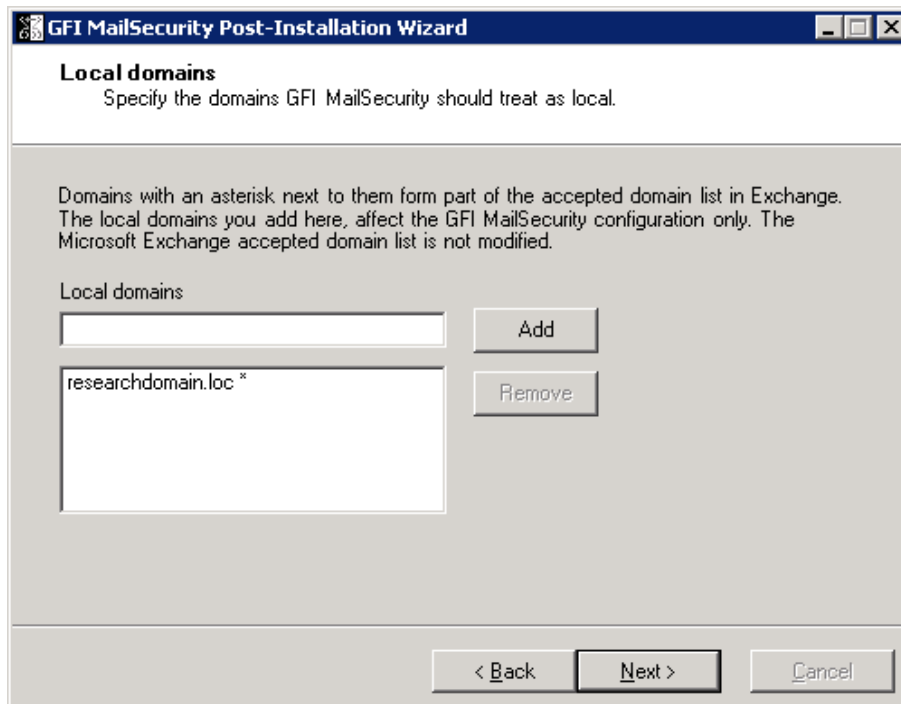
2. The wizard will collect information from the Microsoft Exchange Server 2007 installation, such as the list of local domains and the server roles installed, for example Hub Transport Server Role.



Screenshot 12 – Collecting information from Microsoft Exchange Server 2007

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

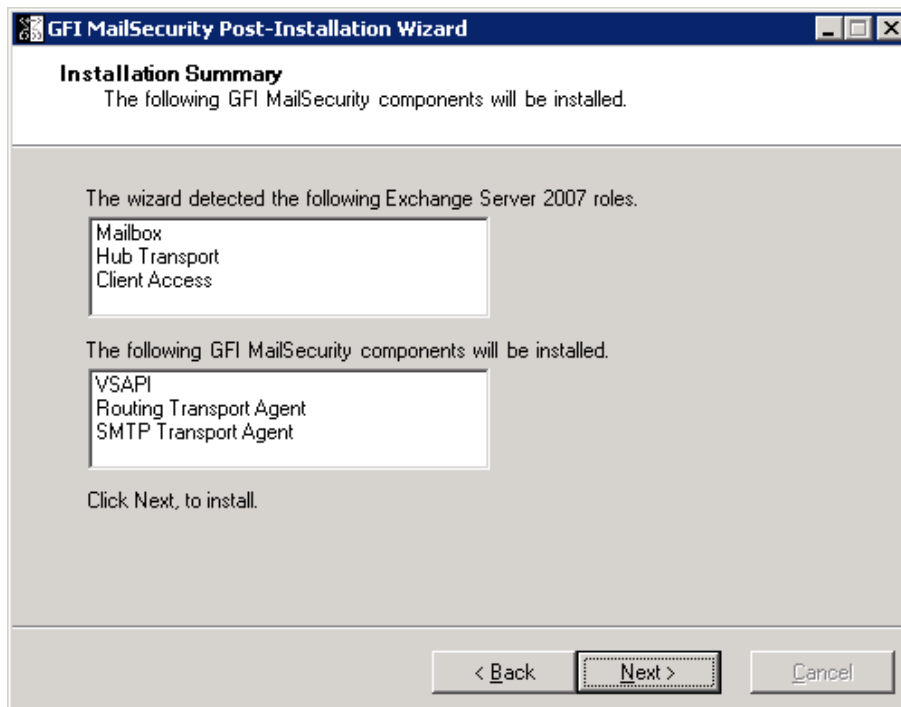
NOTE: The local domains you add from this page affect the GFI MailSecurity installation only. The Microsoft Exchange Server 2007 accepted domains list is not modified.



Screenshot 13 - Local domains list

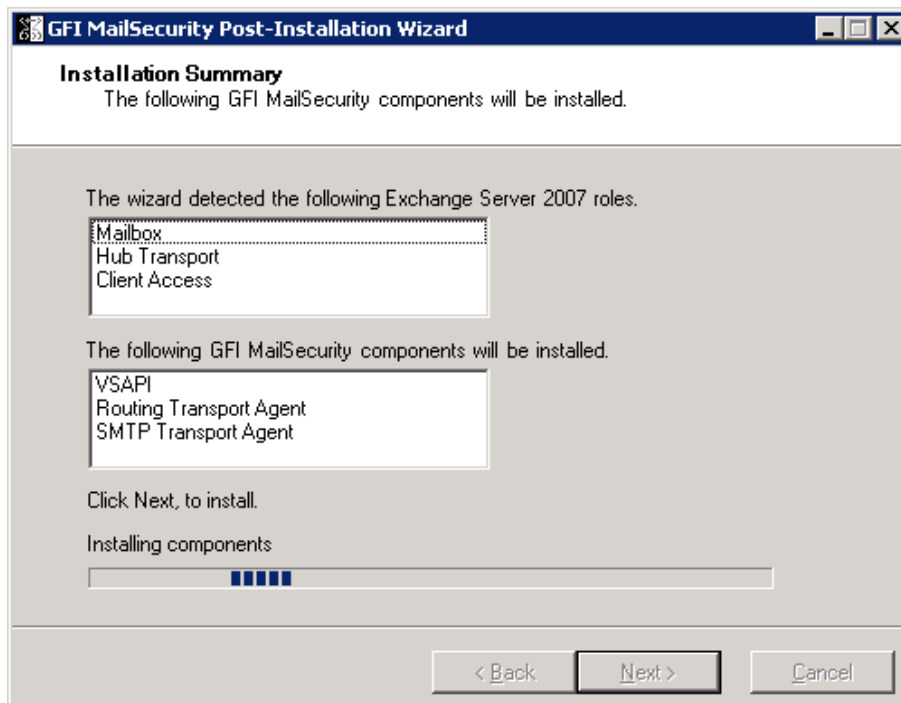
4. Click **Next** to continue.

5. The wizard displays a list of the Microsoft Exchange Server 2007 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.



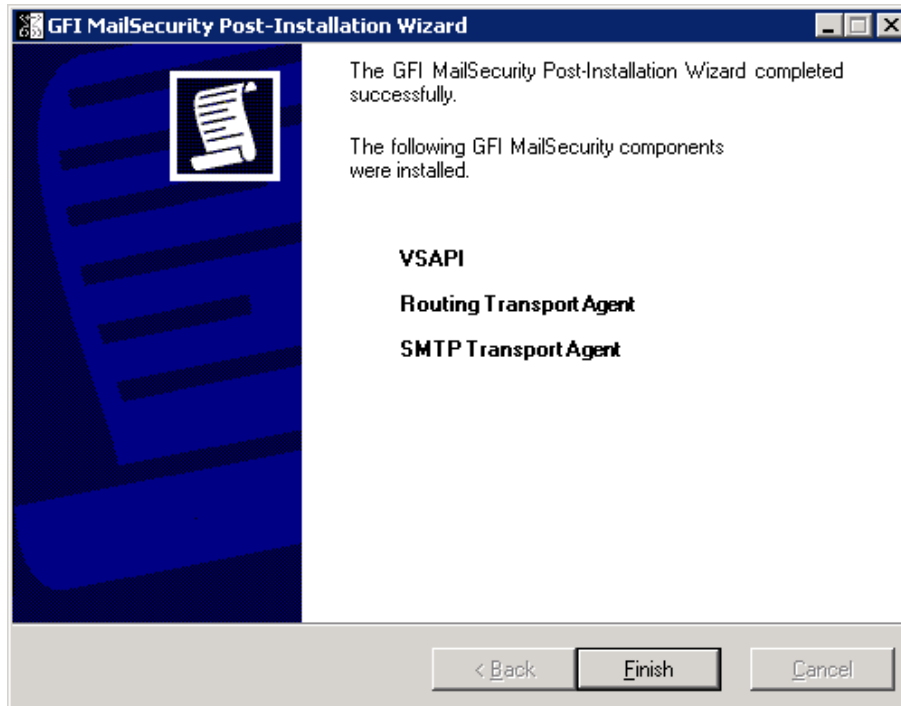
Screenshot 14 - Server roles detected and list of components to install.

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 machine.



Screenshot 16 - GFI MailSecurity Post-Installation Wizard finish page

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**.

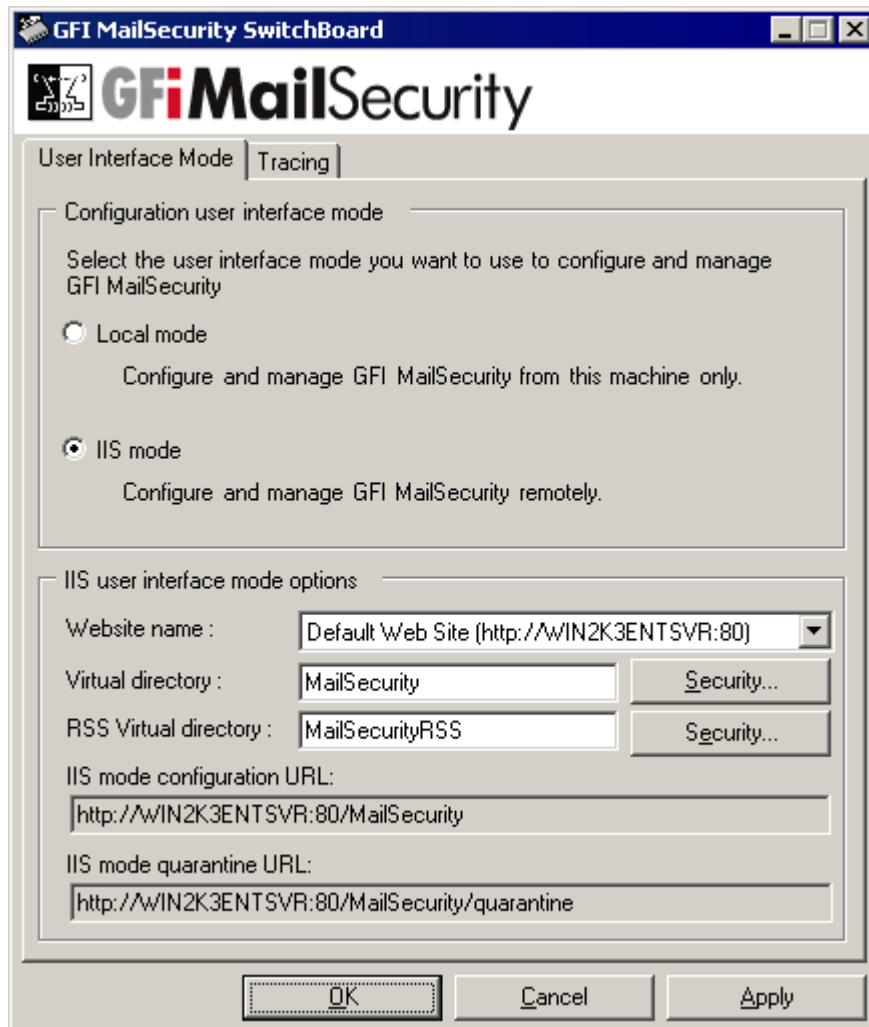
5. Click **Add** and from the dialog box browse to the GFI MailSecurity installation folder, <GFI\ContentSecurity\MailSecurity>, and choose **GFiScanM.exe**.
6. Click **Add** and from the dialog box browse to the GFI MailSecurity installation folder, <GFI\ContentSecurity\AntiVirus\Kaspersky\>, and choose **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.

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:

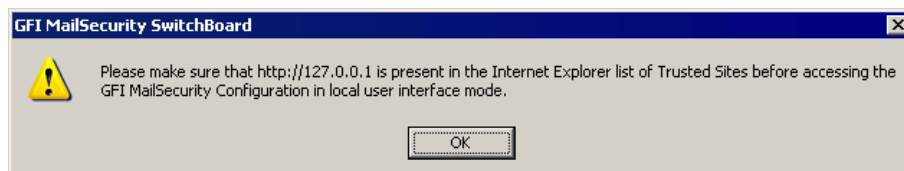
1. Click the **GFI MailSecurity SwitchBoard** shortcut found under **Start ▶ Programs ▶ GFI MailSecurity**.
2. The **GFI MailSecurity SwitchBoard** application is loaded. You now need to select whether you want to allow only local access to the Configuration and Quarantine Store or else both local and 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.

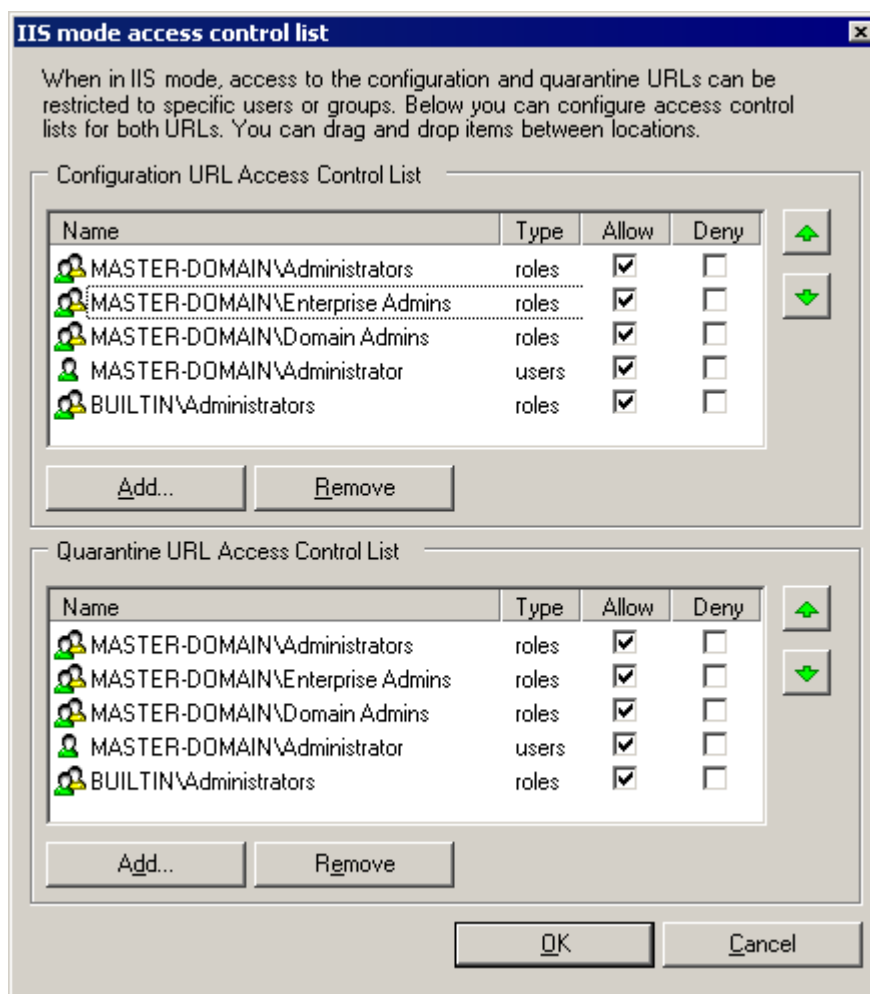
NOTE: If you select **Local mode** you need to add 'http://127.0.0.1' to the list of trusted sites in Internet Explorer. For further information, refer to the 'Adding local host to the trusted sites list' section below.



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.

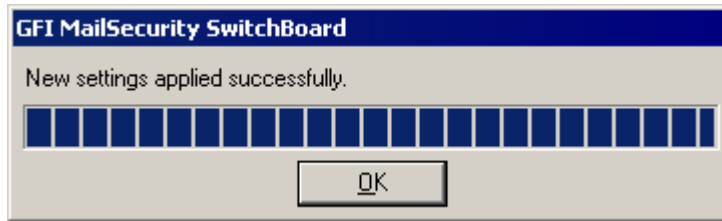
7. To configure the accounts that get access to the quarantine store, use the **Add** and **Remove** buttons underneath the **Quarantine URL Access Control List**. If you want to deny access to a listed account without removing it from the list, select the check box under the **Deny** column.

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.



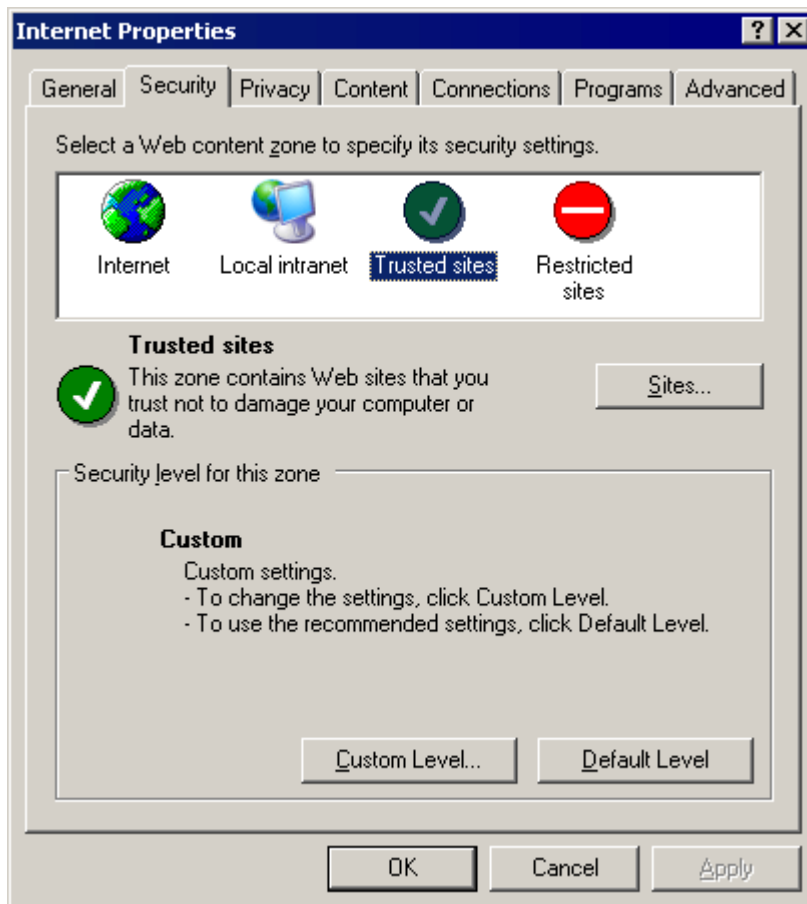
Screenshot 20 - New SwitchBoard settings successfully applied

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

Adding local host to the trusted sites list

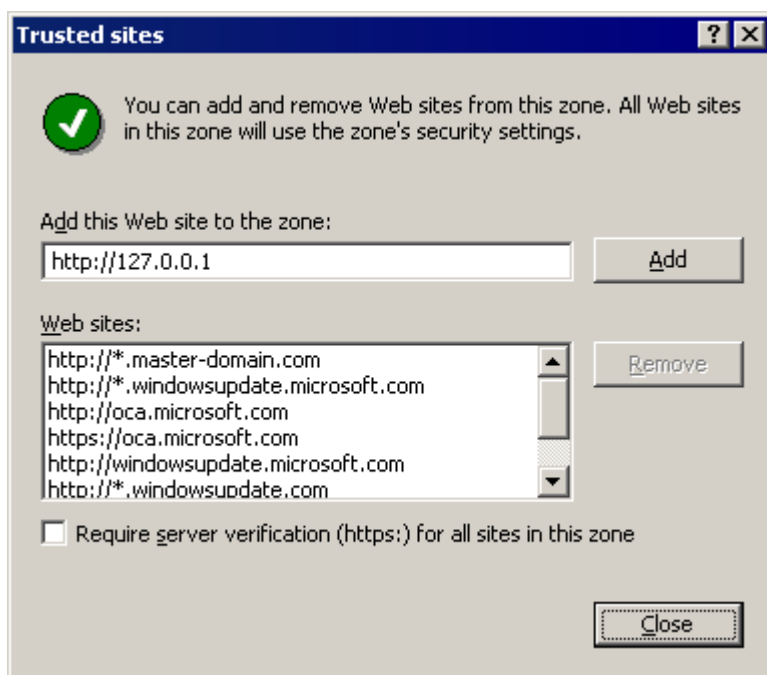
When you configure GFI MailSecurity to be accessible only locally, you need to add the local host address, 'http://127.0.0.1', to the list of trusted sites in Internet Explorer. To do this, follow these steps:

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.



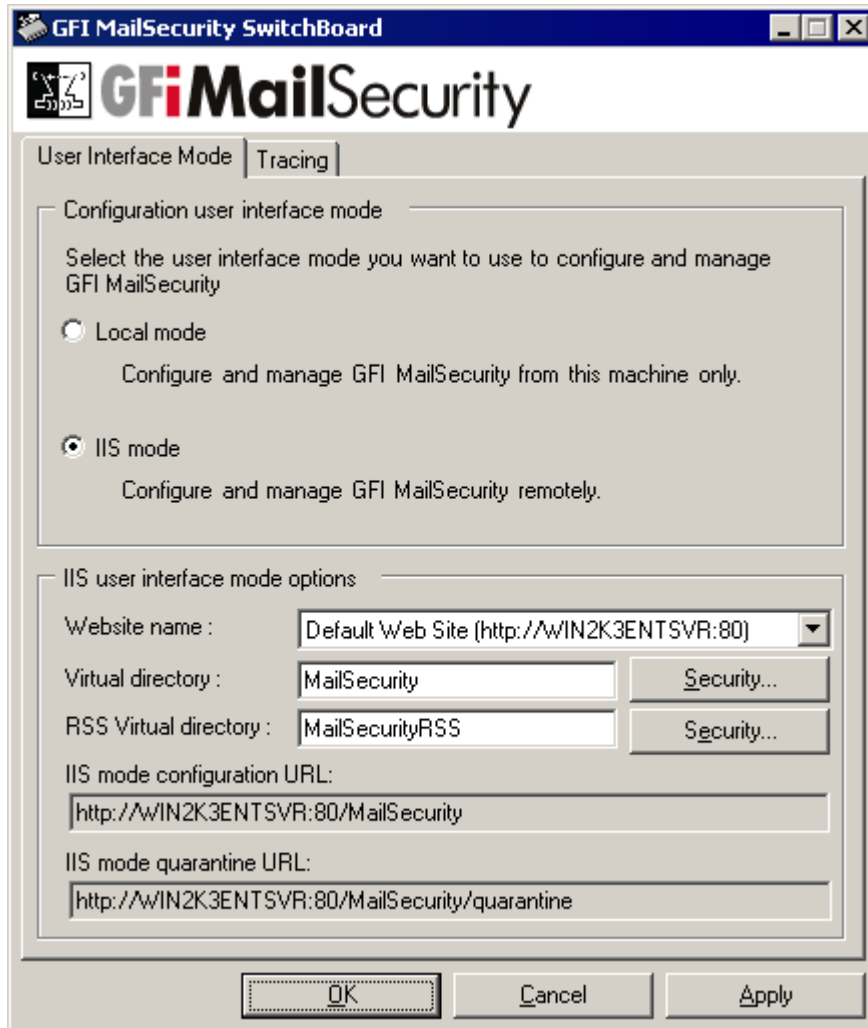
Screenshot 22 - Trusted sites dialog

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

Securing access to the GFI MailSecurity Quarantine RSS feeds

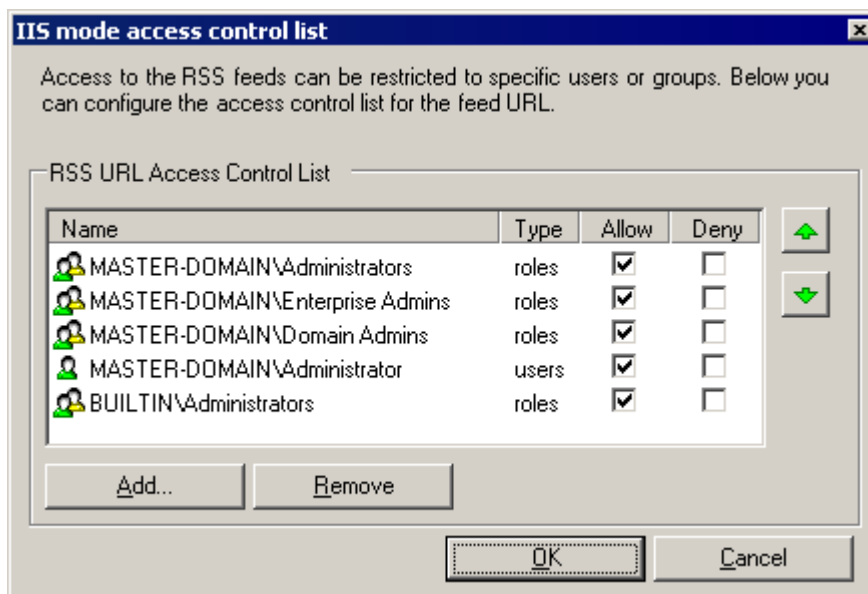
You can configure GFI MailSecurity to create quarantine RSS feeds on specific quarantine folders. To configure who can subscribe to the quarantine RSS feeds, follow these steps:

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.



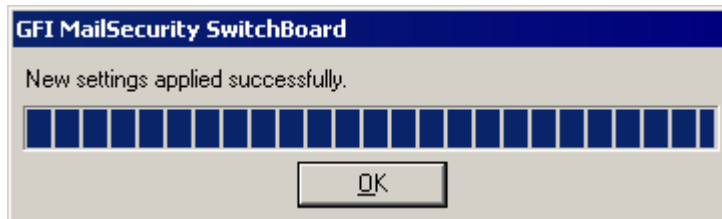
Screenshot 23 - GFI MailSecurity SwitchBoard

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**.

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:

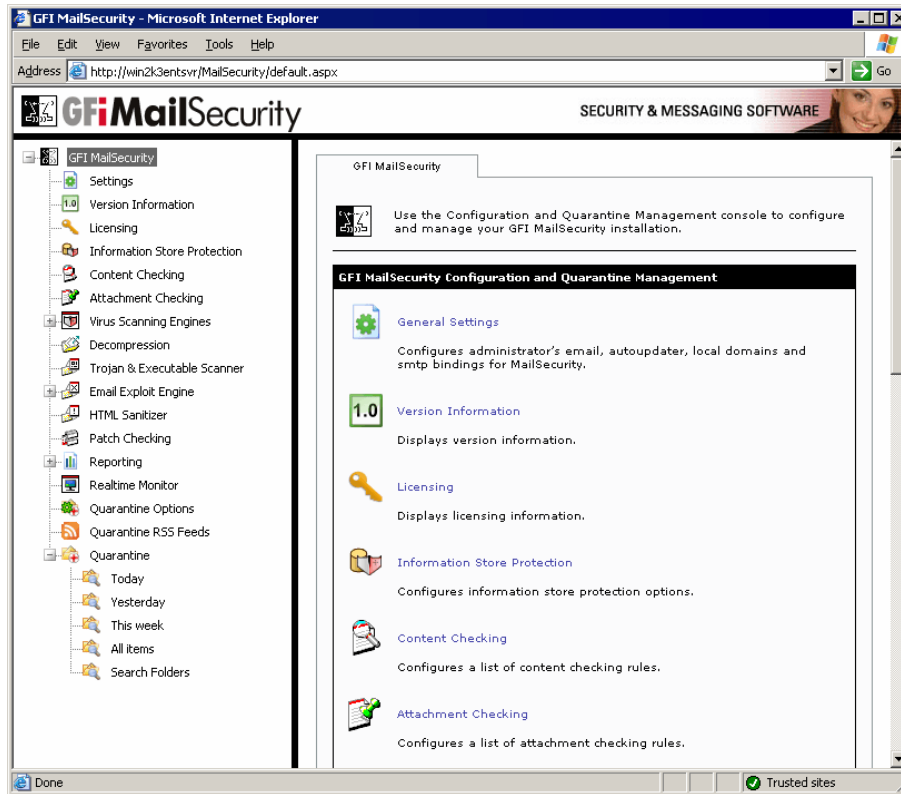
1. Start Microsoft Internet Explorer.
2. In the address bar, specify the following address:

'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

Entering your license key after installation

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



Screenshot 28 - License key information

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

Entering the license key should not be confused with the process of registering your company details on our website. This is important, since it allows us to give you support, and notify you of important product news. Register at <http://www.gfi.com/pages/regfrm.htm>.

Upgrading from GFI MailSecurity 8 to GFI MailSecurity 10

Due to fundamental architectural changes between GFI MailSecurity 10 and GFI MailSecurity 8, it is not possible to install GFI MailSecurity 10 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.
- Convert and import the GFI MailSecurity 8 configuration settings to GFI MailSecurity 10's new configuration database format.

NOTE: If GFI MailSecurity 8 was installed in SMTP mode and GFI MailSecurity 10 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 is installed in SMTP mode.

To upgrade from GFI MailSecurity 8 to GFI MailSecurity 10, 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.

3. Install GFI MailSecurity 10 as shown in the 'Install GFI MailSecurity' section of this chapter.

NOTE: To install GFI MailSecurity 10, 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 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 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.

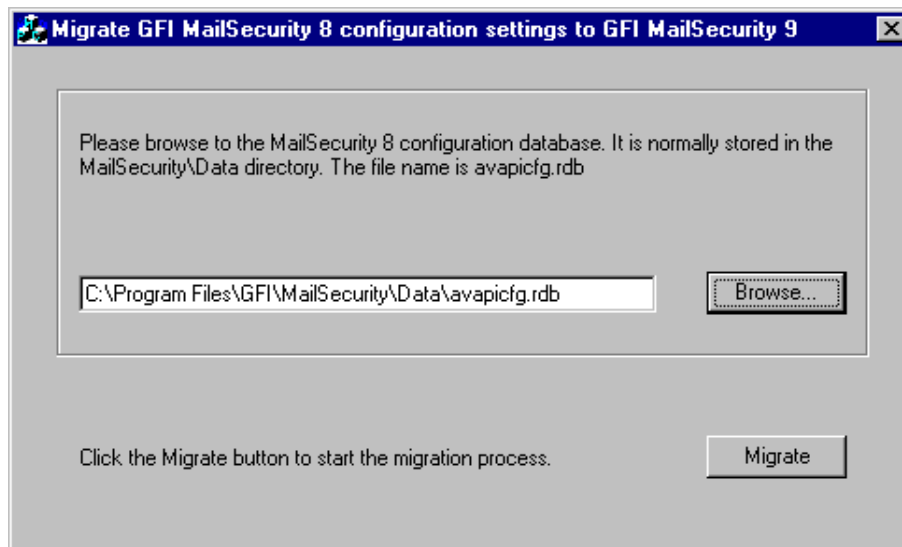
NOTE: You must stop the following services before going on to the next step:

- 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 configuration database, you need to run the msec8upg.exe tool found in the GFI MailSecurity 10 folder, for example:

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



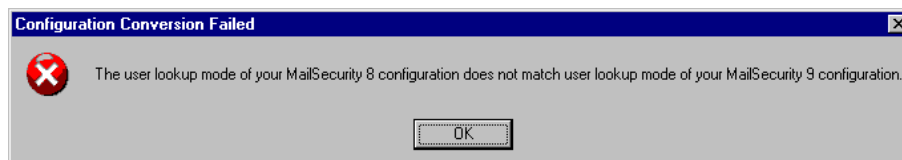
Screenshot 29 - GFI MailSecurity 8 configuration settings migration tool

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 do not match (for example GFI MailSecurity 8 was installed in SMTP mode and GFI MailSecurity 10 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 30 - 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 configuration to check that the GFI MailSecurity 8 settings were migrated correctly.

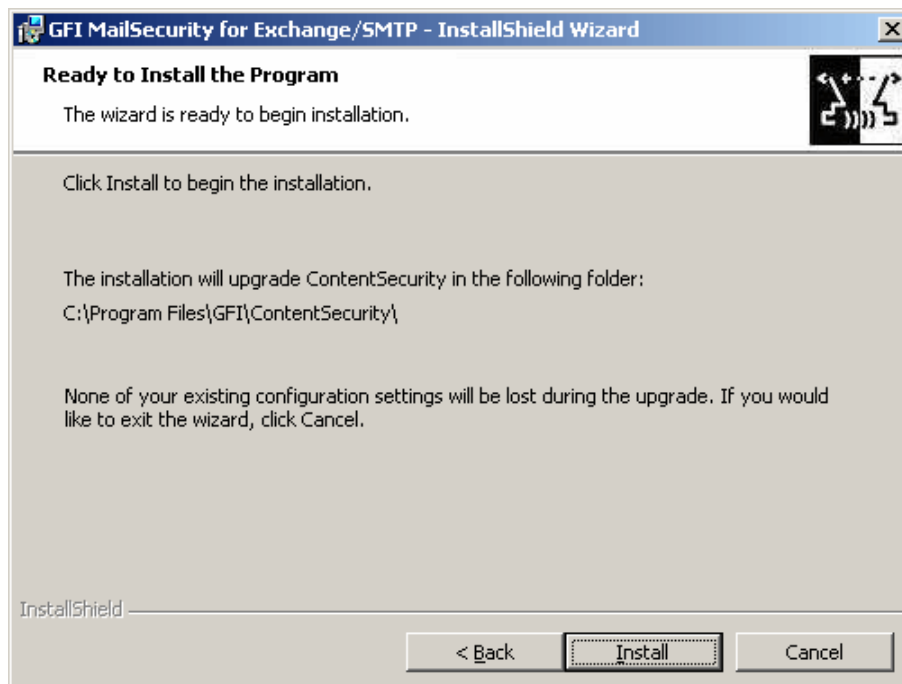
Upgrading from GFI MailSecurity 9 to GFI MailSecurity 10

NOTE: The upgrade process cannot be reverted. If you upgrade GFI MailSecurity to version 10, 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 setup file on the machine on which you have installed GFI MailSecurity 9.
2. Setup will now proceed to install GFI MailSecurity 10 in exactly the same manner as a new installation. However, it will not let you change the destination folder.



Screenshot 31 - Upgrading from GFI MailSecurity 9 to GFI MailSecurity 10

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.