

# 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 relative email addresses. This is required in order to generate the email monitoring rules which will filter inbound and outbound emails. GFI MailSecurity can define 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.

### Installing GFI MailSecurity on your mail server

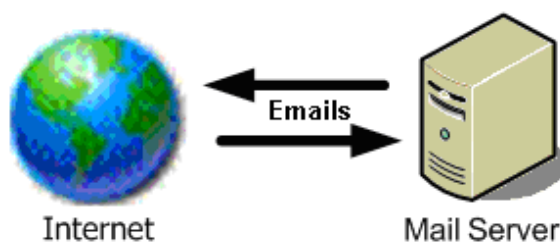


Figure 1 - Installing GFI MailSecurity on your mail server

GFI MailSecurity can be installed 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.

## 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 totally 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

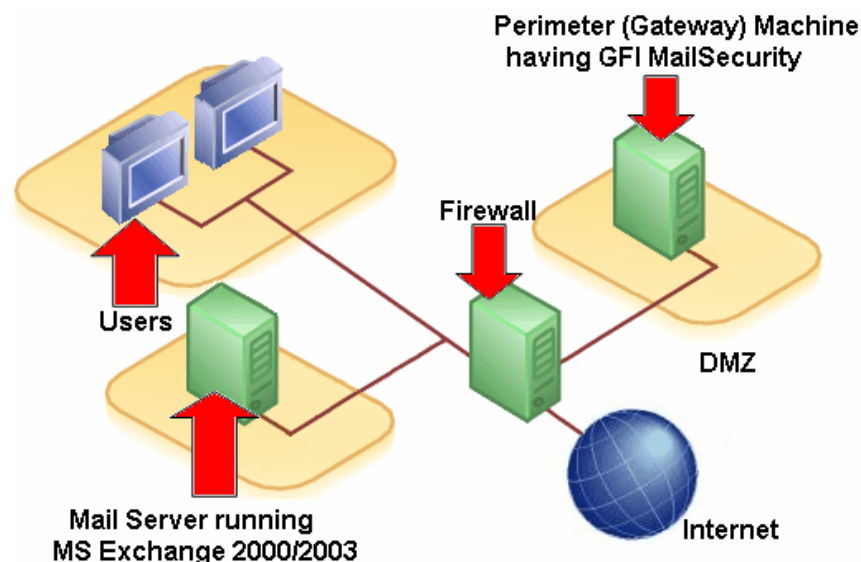


Figure 3 - Installing GFI MailSecurity on a separate machine on a DMZ

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).

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. You can, for example, 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

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.
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 9 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.
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/>.
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 9 on an Active/Active Cluster**

Installing GFI MailSecurity 9 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 email monitoring 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 which is configured as a mail relay server in your domain.

### **SMTP mode**

In SMTP mode, GFI MailSecurity will create email monitoring 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 which 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 which 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 monitoring/scanning rules and notifications.

---

## System requirements

To install GFI MailSecurity you need:

- Windows 2000 Professional/Server/Advanced Server (Service Pack 1 or higher) or Windows 2003 Server/Advanced Server or Windows XP.

**NOTE:** Since Windows XP has some speed limitations, installing GFI MailSecurity on a machine running Windows XP could affect its performance.

- Microsoft Exchange Server 2000 (SP1), 2003, 4, 5 or 5.5, Lotus Notes 4.5 and up, or any SMTP/POP3 mail server.
- When using Small Business Server, ensure you have installed Service Pack 2 for Exchange Server 2000 and Service Pack 1 for Exchange Server 2003.
- Microsoft .Net framework 1.1
- MSMQ – Microsoft Messaging Queuing Service.
- Internet Information Services (IIS) – SMTP service and World Wide Web service.

**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 which 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 a 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.

The machine must also be configured 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. For more information, please visit <http://support.microsoft.com/support/kb/articles/Q293/8/00.ASP>.

### **Installing and configuring IIS SMTP & World Wide Web services**

GFI MailSecurity uses the Windows 2000/2003/XP IIS SMTP service as its SMTP server. However, you must first configure this service as a mail relay server in order to enable GFI MailSecurity to scan all inbound and outbound emails before they reach your mail server.

#### **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, and has been designed to handle large amounts of mail traffic.

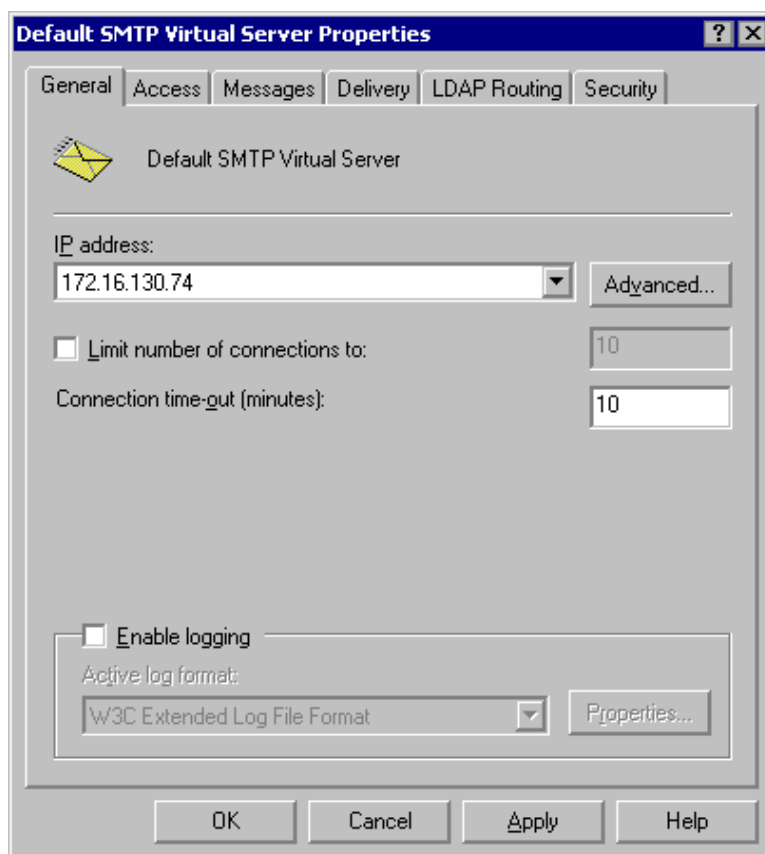
The World Wide Web service is also part of IIS. It uses the HTTP protocol to handle web client requests on a TCP/IP network.

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

To install and configure the IIS SMTP service as a mail relay server, you must:

#### **Step 1: Verify the Installation of the SMTP and World Wide Web Services**

1. Go to **Start ► Settings ► Control Panel**. Double-click on **Add/Remove Programs** and then click on **Add/Remove Windows Components**.
2. From the dialog on display, locate and click on the **Internet Information Services (IIS) component**; then click on the **Details** button.
3. Make sure that the **SMTP Service** and **World Wide Web Service** check-boxes are selected. If not, click on these check-boxes and click on the **OK** button. This should start the installation of the selected services. Follow the onscreen instructions and wait until the installation completes.



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

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

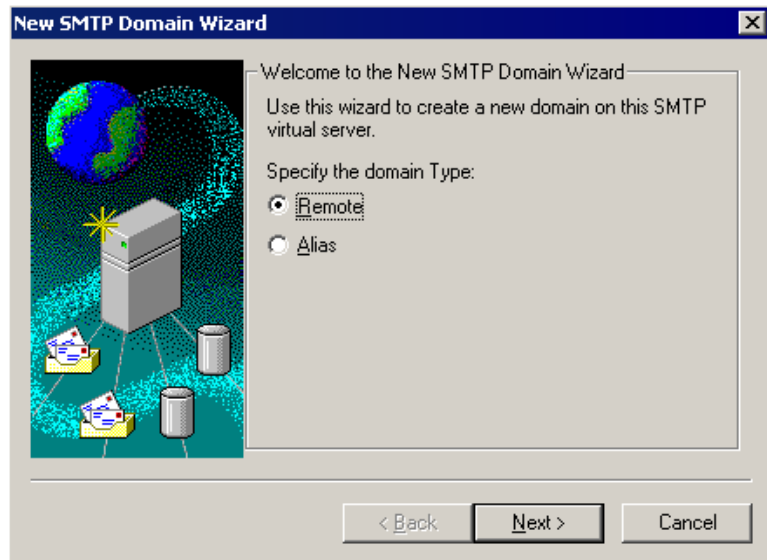
1. Go to **Start ▶ Programs ▶ Administrative Tools** and click on **Internet Information Services (IIS) Manager**.
2. Expand the server name node. Right click on the **Default SMTP Virtual Server** node and select **Properties**.
3. Assign an IP address to the SMTP relay server and click on the **Apply** button to accept the changes and exit.

## 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. Go to **Start ▶ Programs ▶ Administrative Tools** and click on **Internet Information Services (IIS) Manager**.
2. Expand the server name node, and then expand the Default SMTP Virtual Server. By default, you should have a Local (Default) domain with the fully qualified domain name of the server.
3. Configure the domain for inbound message relaying as follows:
  - a) Right-click the Domains node and go to **New ▶ Domain**.

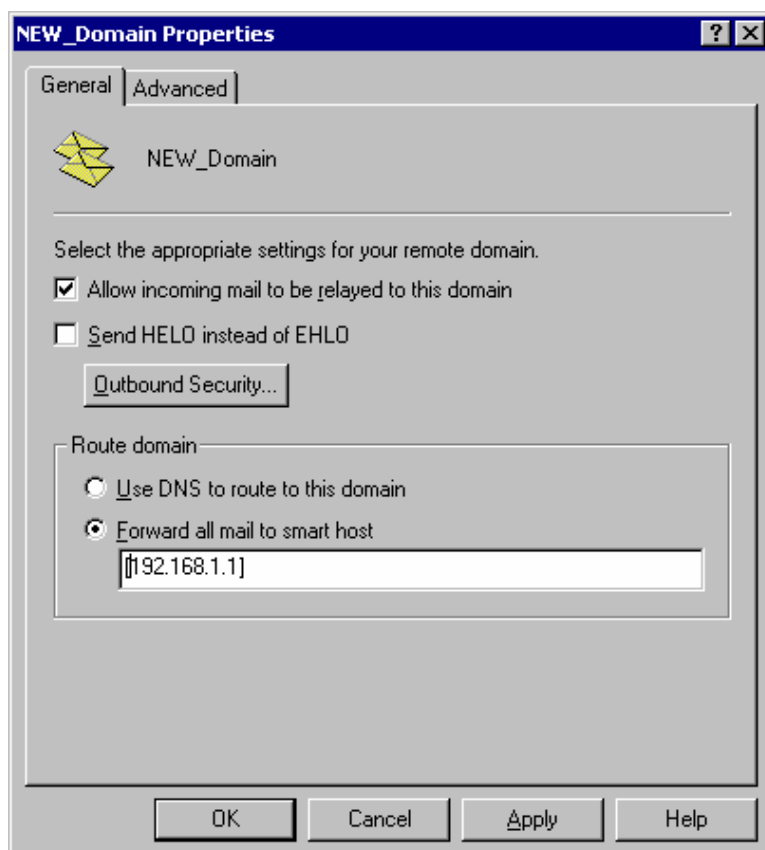


Screenshot 3 - SMTP Domain Wizard - Selecting domain type

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

### 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.



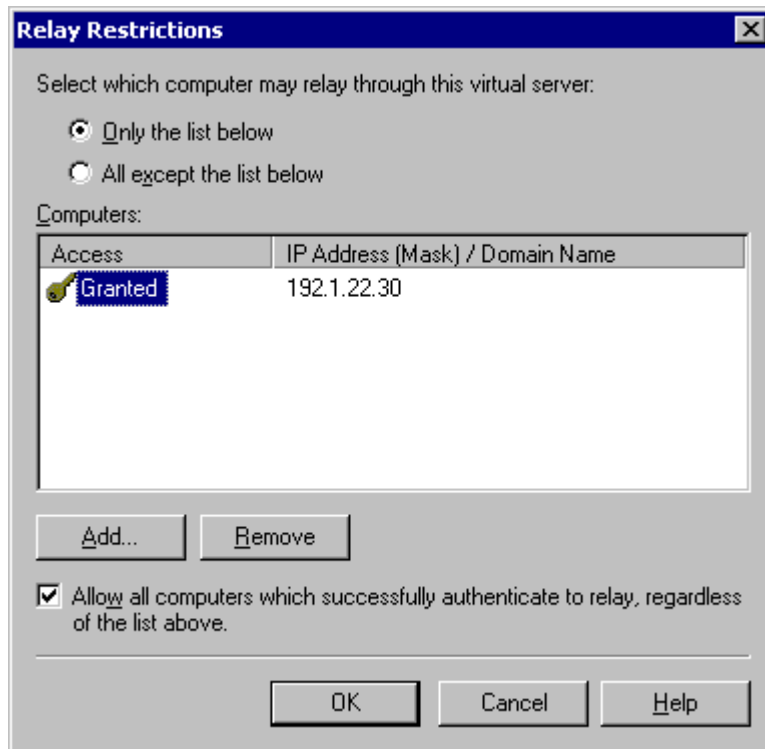
Screenshot 4 - Configure the new domain

### Configure the domain to relay email to your mail server:

1. Right click on the domain that you have just created and select **Properties**. Select the **Allow the Incoming Mail to be relayed to this domain** check-box.
2. In the Route domain dialog box, select the **Forward all email to smart host** option and specify the IP address (in square brackets) of the server which will handle the emails addressed to this new domain. E.g., [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 on the **OK** button to save the entries and close the dialog.

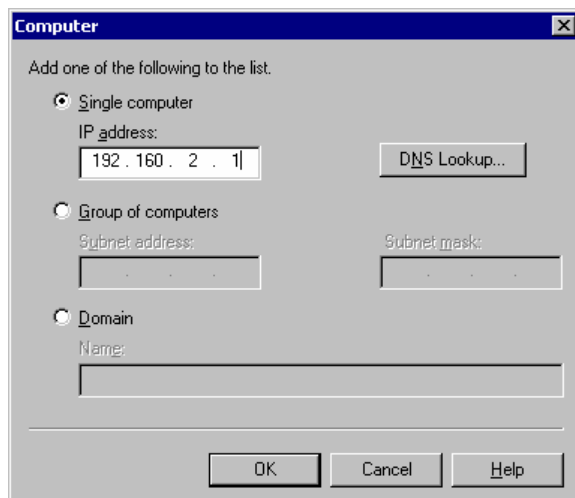


Screenshot 5 - Relay Restrictions dialog

#### 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 on **Default SMTP Virtual Server** and select **Properties**.
2. In the properties window, click on the **Access** tab and then click on the **Relay** button to open the relay restrictions dialog.
3. Click on the **Only the list below** option and then click on the **Add** button to specify the list of permitted computers.



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

4. In the newly opened dialog, state the IP of the mail server that will be forwarding the email to this virtual server and click on the **OK** button to add the entry to the list.

**NOTE:** In this dialog you can specify the IP of a single computer, group of computers or a domain:

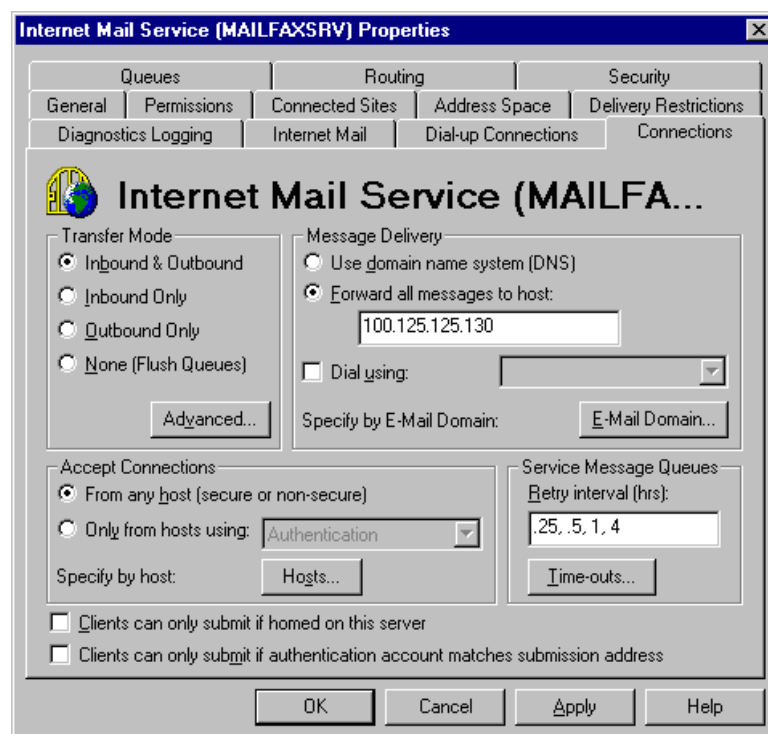
- **Single computer:** Select this option to specify one particular host that will relay email via this server. You can look up the IP address of a specific host by clicking on the **DNS Lookup** button.
- **Group of computers:** Select this option to specify the base IP address for the computers that 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. Launch Microsoft Exchange Administrator and double-click on **Internet Mail Service** to open the properties configuration dialog.



Screenshot 7 - The Microsoft Internet mail connector

2. Click on the **Connections** tab and in the **Message Delivery** section; select **Forward all messages to host**. Enter the computer name or IP of the machine running GFI MailSecurity.

3. Click on the **OK** button and restart MS Exchange Server. This can be done from the services applet.

### **If you have Microsoft Exchange Server 2000/2003:**

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

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

**NOTE:** Always enclose the IP address within square brackets [ ]. E.g., [100.130.130.10].

4. Select the SMTP Server that must be associated to this SMTP Connector. Click on the **Address Space** tab, and click on the **Add** button. Select **SMTP** and click on the **OK** button to accept the changes.
5. Click on the **OK** button to exit. All emails will now be forwarded to the GFI MailSecurity machine.

### **If you have Lotus Notes:**

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

### **If you have an SMTP/POP3 mail server:**

1. Start-up 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. If necessary, click on the **OK** button and restart your mail server.

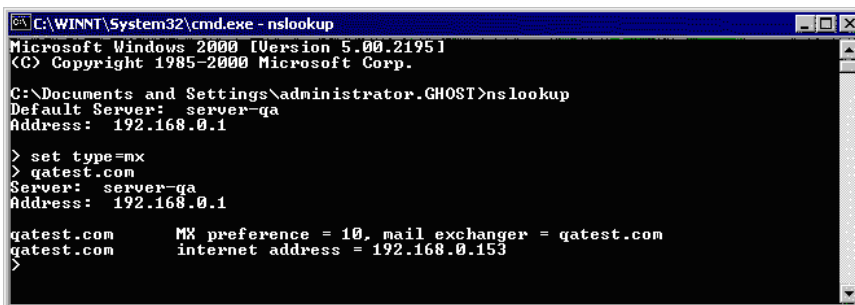
### **Step 6: Point the MX record of your domain to the mail relay server**

Because 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.

#### **Update the MX record of your DNS server as follows:**

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

1. Open the command prompt and type in **nslookup**.
2. Now type **set type=mx** and enter your mail domain.
3. The MX record should return a single IP which 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 5 SMTP inbound connection of your mail relay server by sending an email from an external account to an internal user (you can use webmail, e.g. MSN Hotmail, if you don't have an external account available). Verify that the email client received the email.
2. Test the IIS 5 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 use Telnet to manually send an email. 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 in this chapter.

---

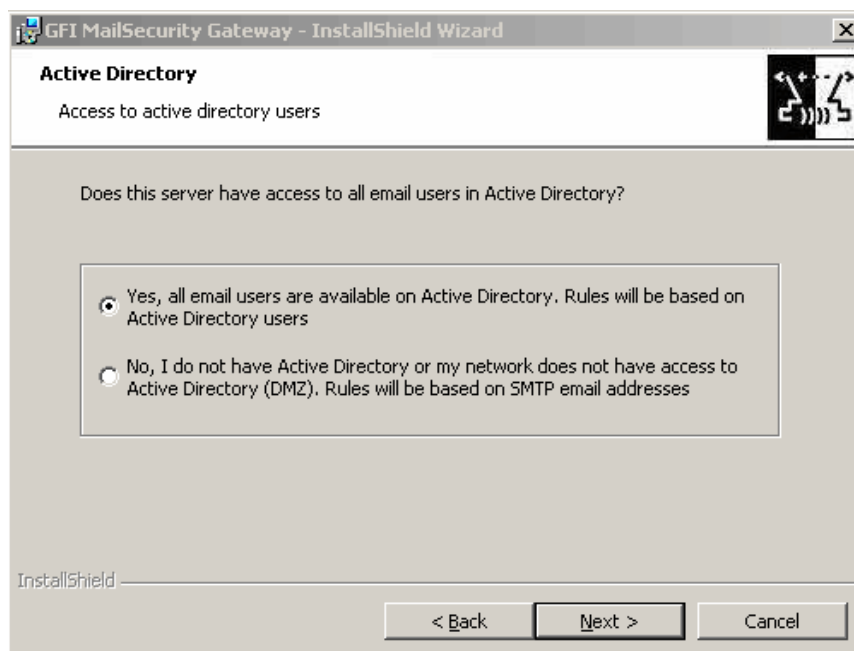
## Installing GFI MailSecurity

**NOTE:** Before you install GFI MailSecurity, make sure to:

Log on as Administrator or use an account with administrative privileges.

Save any pending work you might have on the machine and close all open applications.

1. Run GFI MailSecurity set-up by double-clicking on **MailSecurityGW.exe** and as soon as the intro dialog shows up, click on the **Next** button
2. Confirm the License agreement and click on the **Next** button.
3. Enter your Name, Company, and License key. If you are evaluating the product, leave the license key as default (i.e. **'Evaluation'**). Click on the **Next** button.
4. Specify the administrator's email address or the address where email notifications are to be sent.



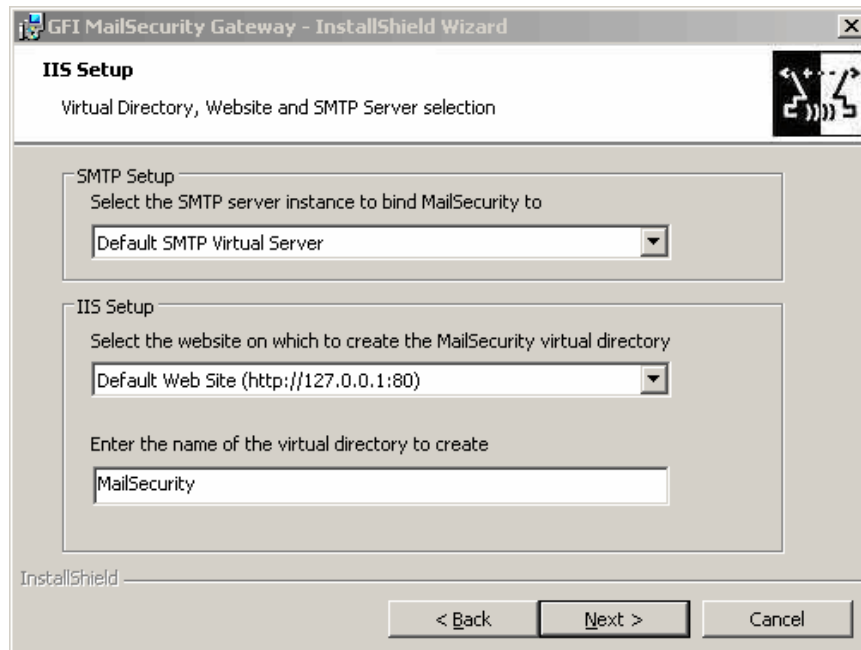
Screenshot 9 - Define if the server has access to all email users in the Active Directory

5. Setup will now ask you to select the mode which 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 email monitoring 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 (e.g., 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 the active directory.....** – Select this option to continue installing GFI MailSecurity in **SMTP mode**. In this mode, GFI MailSecurity will create email monitoring rules based on the list of email users/addresses imported from your mail server. You **MUST** select this mode if you are installing this software on a machine which 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 which are not part of the Active Directory Domain. However, you can still choose this mode to

install GFI MailSecurity on machines which do have access to the Active Directory containing all your email users.

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



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

6. 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.

**NOTE 1:** For more information on IIS SMTP service settings refer to the 'Installing and configuring the IIS SMTP & World Wide Web services' section in this manual.

**NOTE 2:** After installing the product, you can still bind GFI MailSecurity to another SMTP virtual server from the GFI MailSecurity Configuration (**Console Root ▶ Settings ▶ Bindings**). For more information, refer to the 'SMTP server bindings' section in the General Settings chapter.

GFI MailSecurity can be configured and monitored remotely using a web browser. To be able to monitor and configure GFI MailSecurity remotely, you must specify the web location (i.e., the server) where the installation will create its virtual directory. To change this setting, select the required location from the available list. Finally, specify the name of the virtual directory or click on the **Next** button to leave as default (i.e., GFI MailSecurity).

7. 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 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 on the **Next** button to continue.

8. In order for GFI MailSecurity to handle high volumes of event processing, it requires MSMQ (Message Queuing Service) to be installed. Although this service is included in every version of Windows 2000/2003 and XP, it is not always installed by default.



Screenshot 11 - MSMQ installation dialog

The installation wizard will now check if this service is already installed on your system and if not, a dialogue will inform you that the installation of this service is required. Click on the **Next** button to confirm and continue with the installation of this service.

**NOTE:** You cannot continue installing GFI MailSecurity without having MSMQ installed. Clicking on the **Cancel** button will interrupt the installation process of both the MSMQ service and GFI MailSecurity.

9. Setup will now ask you to define the folder where GFI MailSecurity is to be installed. GFI MailSecurity requires approximately 40 MB of free hard disk space. In addition to this, you must reserve approximately 200 MB for temporary files. Click on the **Change** button to specify a new installation path or click on the **Next** button to leave as default and proceed with the installation.

10. 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 on the **Back** button. Otherwise click on the **Install** button to start the installation process.

11. Upon completion, setup will inform you that it requires to restart the SMTP services. To instantly restart these services and finalize the installation, click on the **Yes** button.

---

## 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 Service Pack 2 and on Microsoft Windows 2003 Service Pack 1. On Microsoft Windows 2003 Service Pack 1, 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 2003 Service Pack 1, 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 enter 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 the **Settings** button under the **Performance** group.
3. Change to the **Data Execution Prevention** tab.
4. Enable **Turn on DEP for all programs and services except those I select:** radio button.
5. Click the **Add** button and from the dialog go to the GFI MailSecurity installation folder, <GFI\ContentSecurity\MailSecurity>, and choose **GFiScanM.exe**.
6. Click the **Add** button and from the dialog go to the GFI MailSecurity installation folder, <GFI\ContentSecurity\AntiVirus\Kaspersky>, and choose **kavss.exe**.
7. Click the **Apply** and **OK** buttons 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

The GFI MailSecurity configuration is entirely web-based. For this reason it is imperative that proper access security is configured so that only authorized users get access to the setting-up of rules and 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 on 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, select the **Local mode** option, 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, select the **IIS mode** option, so that authorized users both from the local machine and other remote machines can access the GFI MailSecurity Configuration and Quarantine Store.



Screenshot 12 - GFI MailSecurity SwitchBoard

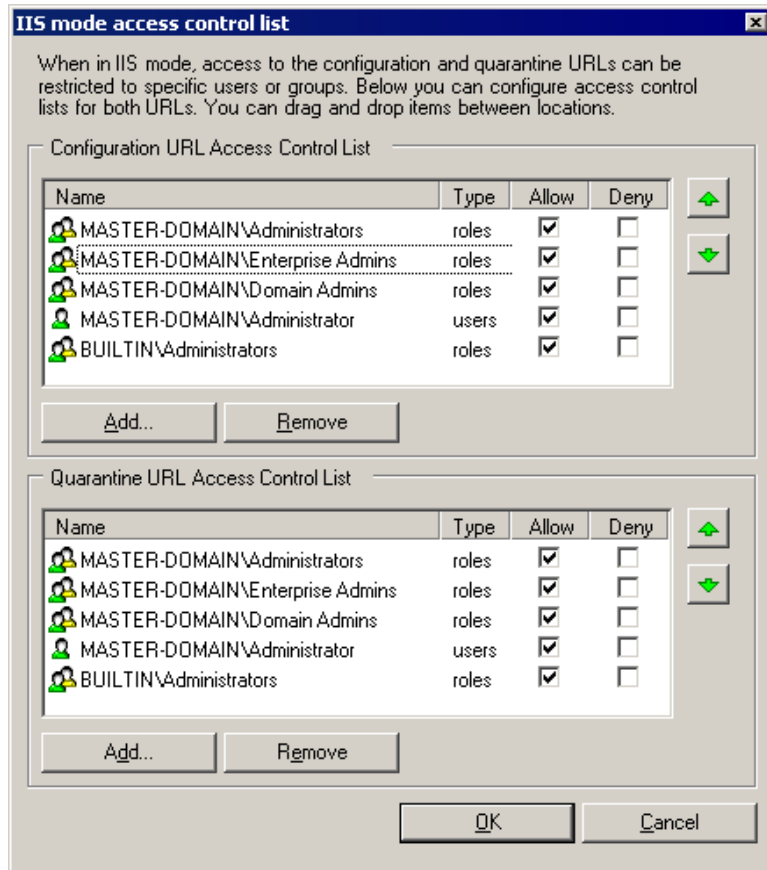
3. If you selected the **Local mode** option, you do not need to configure anything else. If you selected the **IIS mode** option you now need to configure the Active Directory accounts or groups which have access to the Configuration and Quarantine Store, and you can also change the virtual directory 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' below.



Screenshot 13 - Local host address must be added to trusted sites list

4. To configure access security, click the **Security...** button.
5. The **IIS mode access control list** dialog is displayed. This dialog allows you to configure who gets access to the configuration pages and the quarantine store in separate access control lists.



Screenshot 14 - Configuration / Quarantine store Access Control Lists

6. To configure the accounts which 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.

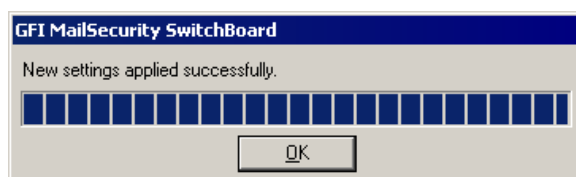
7. To configure the accounts which get access to the quarantine store, use the **Add** and **Remove** buttons underneath the **Quarantine URL Access Control List**. If you want to deny access to a listed account without removing it from the list, select the check box under the **Deny** column.

**NOTE:** So as 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 the **OK** button to close the dialog.

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

10. Click the **OK** button to save your changes. A popup dialog will display the progress while applying the new settings.



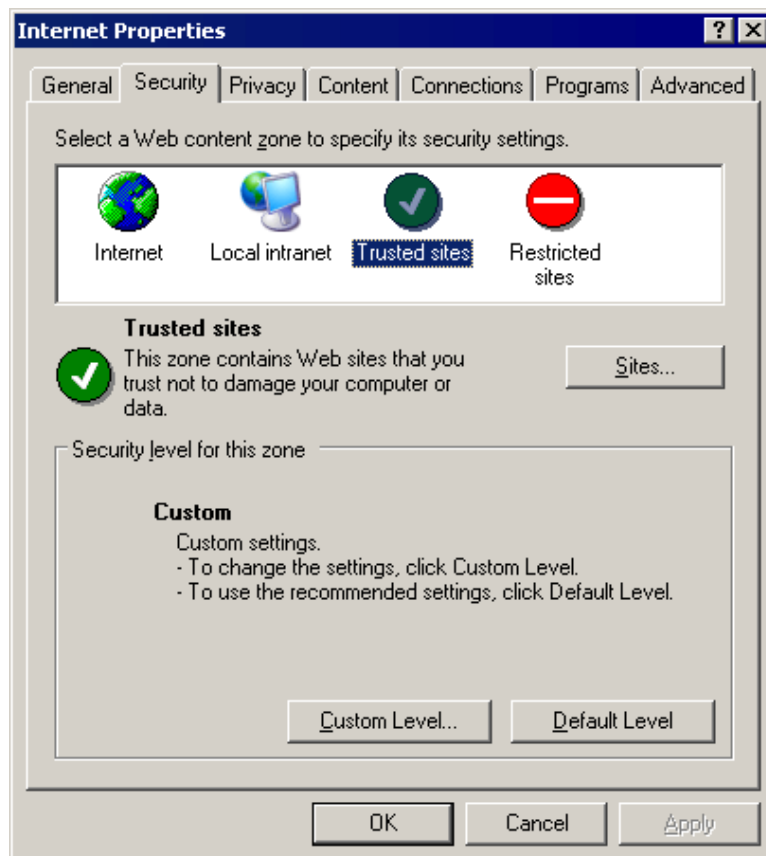
Screenshot 15 - New SwitchBoard settings successfully applied

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

### Adding local host to the trusted sites list

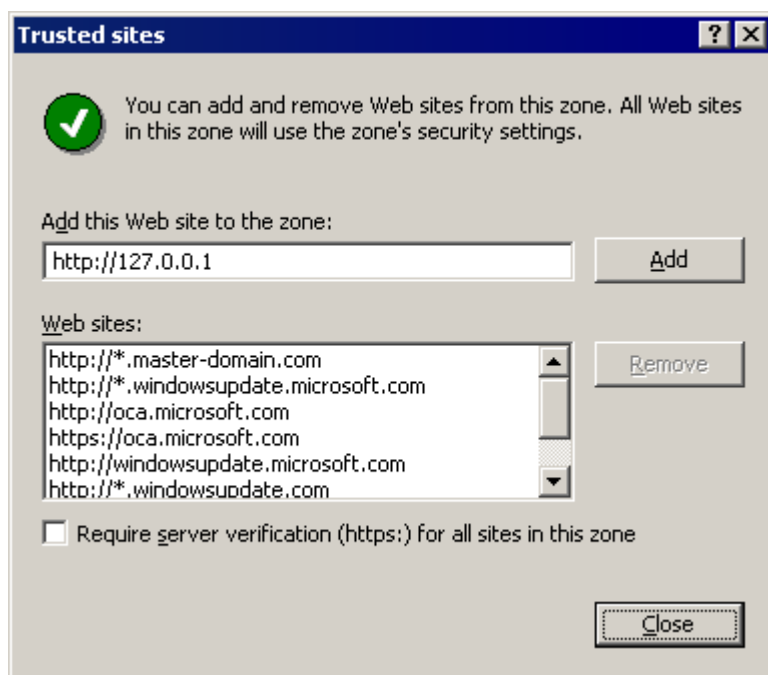
When you configure GFI MailSecurity to be accessible only locally, you need to add the local host address, 'http://127.0.0.1', to the list of trusted sites in Internet Explorer. To do this, follow these steps:

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



Screenshot 16 - Internet properties dialog

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



Screenshot 17 - Trusted sites dialog

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

---

## 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 on 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 18 - GFI MailSecurity accessed when set to local only access

## Accessing the configuration from a remote machine

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

1. Load 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:

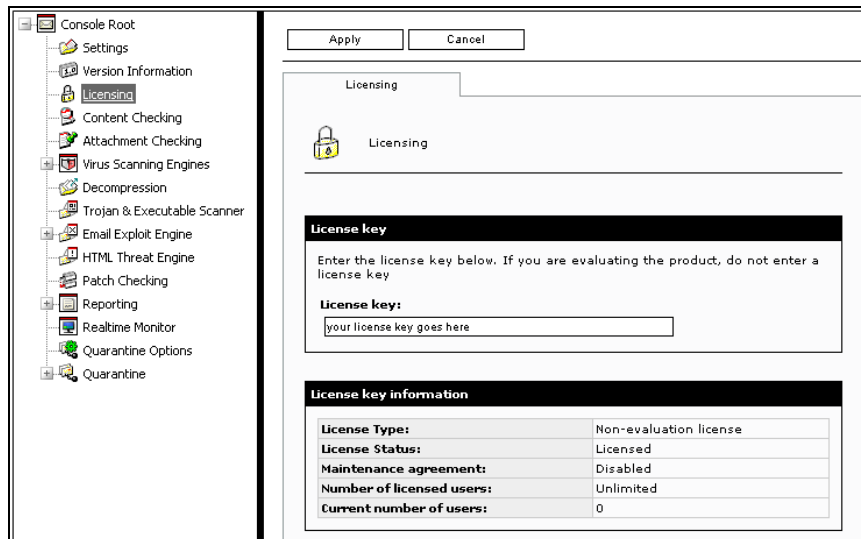
'http://win2k3entsvr.master-domain.com/mailsecurity' for the configuration or 'http://win2k3entsvr.master-domain.com/mailsecurity/quarantine' for the quarantine store.

3. You will be prompted to specify a user name and password so as 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 will be displayed.



Screenshot 19 - GFI MailSecurity accessed from a remote machine

## Entering your license key after installation



Screenshot 20 - License key information

If you have purchased GFI MailSecurity, you can enter your License key by clicking on the **Licensing** node under the **Console Root**.

If you are evaluating GFI MailSecurity with an evaluation key, the product will time out after 60 days. If you then decide to purchase GFI MailSecurity, you can just enter the purchased license key here without having to re-install.

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/reqfrm.htm>.

---

## Upgrading from GFI MailSecurity 8 to GFI MailSecurity 9

Due to fundamental architectural changes between GFI MailSecurity 9 and GFI MailSecurity 8, it is not possible to install GFI MailSecurity 9 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 9.
- Migrate the GFI MailSecurity 8 configuration settings to GFI MailSecurity 9's new configuration database format.

**NOTE:** If GFI MailSecurity 8 was installed in SMTP mode and GFI MailSecurity 9 is installed in Active Directory mode, you will not be able to migrate the settings due to user-based rules. This also applies if GFI MailSecurity 8 was installed in Active Directory mode and GFI MailSecurity 9 is installed in SMTP mode.

To upgrade from GFI MailSecurity 8 to GFI MailSecurity 9, follow these steps:

1. Uninstall GFI MailSecurity 8.
2. When the GFI MailSecurity 8 uninstallation completes, certain files will be left behind under the root folder where GFI MailSecurity 8 had been 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 9.

3. Install GFI MailSecurity 9 as shown in the 'Install GFI MailSecurity' section of this chapter.

**NOTE:** To install GFI MailSecurity 9, you need to have the following installed on the machine:

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

**NOTE:** Do not install GFI MailSecurity 9 to the same path where GFI MailSecurity 8 was installed, so as to prevent files such as `avapicfg.rdb` from being overwritten.

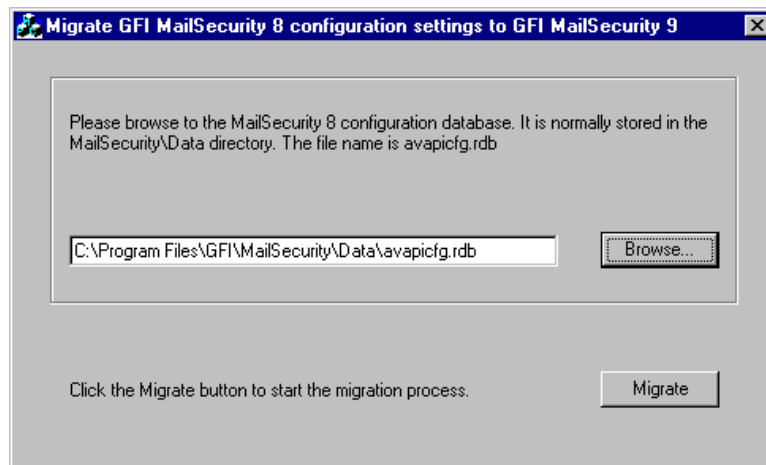
4. After the installation of GFI MailSecurity 9 is complete, you need to stop all GFI-related services along with the IIS Admin service, from the Services control applet. After that, you can run the GFI MailSecurity 8 settings migration tool.

**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 migrate the GFI MailSecurity 8 settings to the GFI MailSecurity 9 configuration database, you need to run the msec8upg.exe tool found in the GFI MailSecurity 9 folder, for example:

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



Screenshot 21 - GFI MailSecurity 8 configuration settings migration tool

6. Double-click the msec8upg.exe file.


7. When the tool loads, click on the **Browse** button. Select the avapicfg.rdb file from the data sub-folder under the GFI MailSecurity 8 root folder.

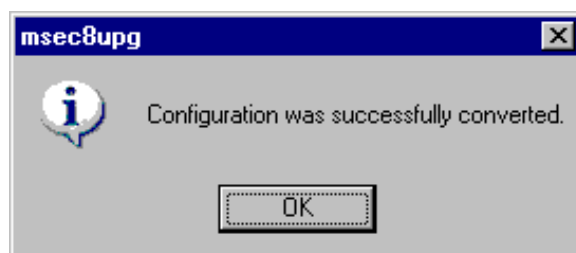
8. Click the **Migrate** button.

**NOTE:** If you click the migrate button and the user lookup mode of GFI MailSecurity 8 and GFI MailSecurity 9 do not match (for example GFI MailSecurity 8 was installed in SMTP mode and GFI MailSecurity 9 is installed in Active Directory mode or vice versa), an error like the one shown below will be displayed and you will not be able to migrate the settings due to user-based rules.



Screenshot 22 - User lookup mode mismatch.

9. When the migration process completes, a **Configuration was successfully converted** information dialog will be displayed. Click the **OK** button to close the information dialog and click on the close button  to close the migration tool.



Screenshot 23 - Settings migrated successfully

10. You now need to start all the services that you stopped in step 4 above; this must be done from the Services control applet.

11. Use the GFI MailSecurity 9 configuration to check that the GFI MailSecurity 8 settings were migrated correctly.